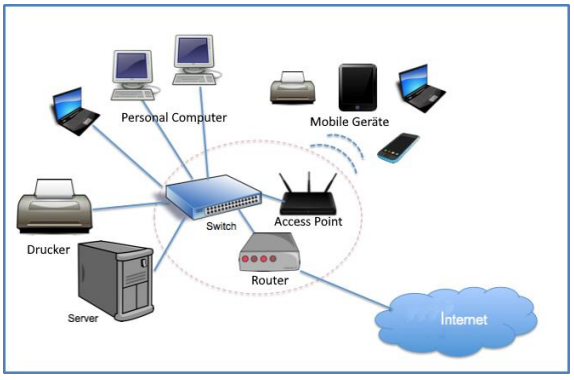
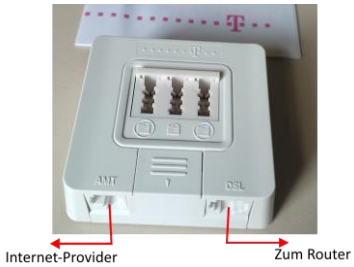
Inhalt

Netzwerk- Fachbegriffe

Netzwerk  	Ein "Netzwerk" verbindet vernetzte Geräte miteinander, die danach Daten miteinander austauschen, oder gemeinsam dieselben Daten nützen können. Das größte Netzwerk der Welt ist das "Internet". Es besteht aus vielen kleinen Einzel-Netzwerken, die durch Router miteinander verbunden sind.
TCP/IP	(Ausgesprochen: "ti-ßi-pi-ei-pi") ist die am meisten verbreitete Netzwerksprache der Welt.

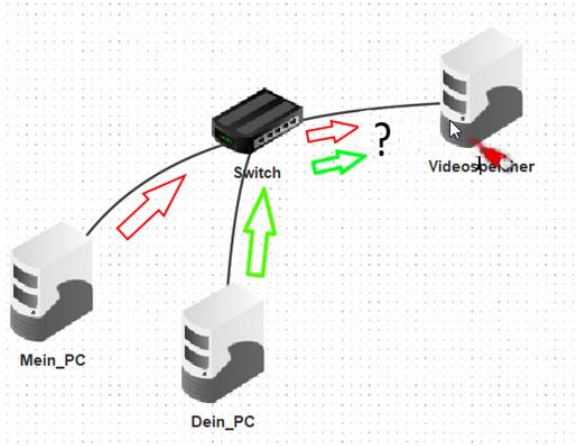
	Praktisch alle vernetzen Geräte sprechen TCP/IP.
TCP/IP-Adresse (oft einfach IP-Adresse genannt)	Jedes Gerät im Netzwerk benötigt eine eindeutige, aus vier Feldern bestehende IP-Adresse. Die vier Felder können sind durch Punkte getrennt.
Ethernet 	Die Bezeichnung für das am häufigsten verwendete kabelgebundene Netzwerk. Normalerweise verwendet man Kupferkabel, für besondere Zwecke auch Glasfasern. Ein Ethernet-Kabel aus Kupfer kann maximal etwa 100m lang gemacht werden, mit Glasfasern gehen auch viele km Länge.
WLAN, WIFI "Wireless LAN" 	Eine Erweiterung von Ethernet zur Vernetzung über Funk ("die Luft") statt über Kabel. Die Verbindung zwischen dem Ethernet-Teil und dem WLAN-Teil macht ein "Access Point". Er wird mit einem Ethernet-Kabel ans übrige Netzwerk angeschlossen. Man erkennt Access-Points meistens leicht an ihren Antennen.
LAN "Local Area Network" "Heimnetz"	Ein eher kleines Netz, das eine Wohnung, ein Haus oder ein Firmengebäude vernetzt. Ein Beispiel sind die Netzwerke, die zu Hause oder in der Schule aufgebaut sind.
WAN "Wide Area Network" "Internet"	Ein Netzwerk das LAN-Netzwerke zu einem großen Netz verbindet. Das Internet ist das größte WAN der Welt
Switch, Hub 	Ein "Netzwerkverteiler" mit vielen Ethernet-Anschlüssen, das alle Geräte im LAN-Netzwerk miteinander verbindet.
Router "Gateway"	Geräte, die ganze LAN-Netze miteinander verbinden. Um das eigene Netz (LAN) mit dem Internet (WAN) zu verbinden, benötigt man einen Router. Es gibt viele Hersteller von Routern, in Deutschland wurde die "Fritzbox" der Berliner

	Firma AVN sehr bekannt, es gibt aber auch sehr gute Router von vielen anderen Firmen. Ein anderes Wort für "Router" ist "Gateway". Im Bezug auf IP-Vernetzung ist das dasselbe.
DHCP-Server "**D**ynamic **H**ost **C**onfiguration **P**rotocol"	Ein DHCP-Server dient zur Verwaltung von TCP/IP-Adressen in einem LAN. Er macht das Führen von Listen von TCP/IP-Adressen überflüssig. Wenn ein Gerät keine IP Adresse hat, im Netzwerk aber ein DHCP Server installiert wurde, kann sich das Gerät eine IP Adresse von diesem DHCP Server zuweisen lassen.
DNS-Server "**D**omain **N**ame **S**ervice"	Ein DNS Server dient zur Verwaltung von Computernamen in einem LAN oder WAN. Er macht das Führen von Listen mit Netzwerkadressen und Computernamen überflüssig
"Privates" Netz	Ein eigenes kleines LAN-Netzwerk, das man selber bei sich zu Hause aufgebaut hat.
"Öffentliches" Netz, Internet	Das weltweit größte WAN Netzwerk. Es besteht aus vielen kleinen LAN Netzwerken, die durch "Router" verbunden wurden. Um sein "Privates" Netzwerk ans Internet anzuschließen, benötigt man einen "Router", und muss dafür sorgen, dass die im LAN verwendeten IP Adressen "kompatibel" zum Internet sind. Das ist der Fall, wenn man "private" IP Adressen verwen
Internet-Provider	Eine Firma, die private Netze von Haushalten und Firmen an das Internet anschließen kann.
DSL "**D**igital **S**ubscriber **L**ine" 	Kabelverbindung, mit der Internet-Provider die Internetverbindung an private Gebäude anschließen. Irgendwo im Haus wird dazu eine Anschlussdose montiert. In diese wird dann das Verbindungskabel zum DSL Anschluss des Routers gesteckt.

Die Sache mit den Netzwerkpaketen

Ein etwa 600 Megabyte große Video im LAN kopieren, das dauert in einem 100Mbit Netzwerk etwa eine Minute. Es kann je nachdem wie schnell das Netz ist auch mal etwas mehr oder weniger sein, aber so ungefähr kommt das hin.

So schaut beispielsweise ein sehr kleines Netzwerk aus drei Computern aus.

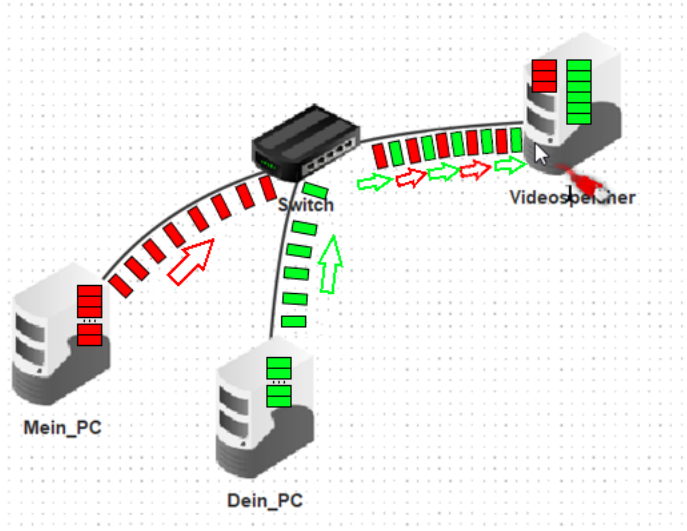


Und jetzt stell dir vor, "Mein_PC" möchte das Video auf einen dritten Computer ("Videospeicher") kopieren, und zwar ungefähr gleichzeitig, wo "Dein_PC" ein anderes Video auch dahin kopieren möchte. Zu "Videospeicher" führt aber nur eine Netzwerkleitung.

Wie ist das jetzt, wenn Mein_PC zu kopieren begonnen hat, aber noch nicht fertig ist? Muss "Dein_PC" jetzt eine Minute warten? Oder wenn "Dein_PC" zuerst zu kopieren begonnen hat … muss Mein_PC dann warten, bis Dein_PC fertig ist, damit er die Leitung zum Videospeicher benützen kann?

Nein, muss er nicht. Beide PCs zerteilen das Video in "Netzwerkpakete", jedes ist nur etwa 1500 Bytes groß. Insgesamt werden pro Video etwa 400.000 solche Pakete durchs Netzwerk geschickt werden. Das Übertragen solch eines Netzwerkpaketes dauert nur einen Sekundenbruchteil. Und dann wechseln sich die beiden PCs einfach ab: jeder überträgt ein Paket, und dann lässt er den anderen ein Paket übertragen, dann kommt er wieder dran, und so weiter, bis beide alles übertragen haben, was sie brauchen.

Und der Videospeicher-Rechner der die Pakete empfängt, der setzt sie einfach wieder zusammen, und am Ende hat er wieder die unzerhackten Video-Dateien.



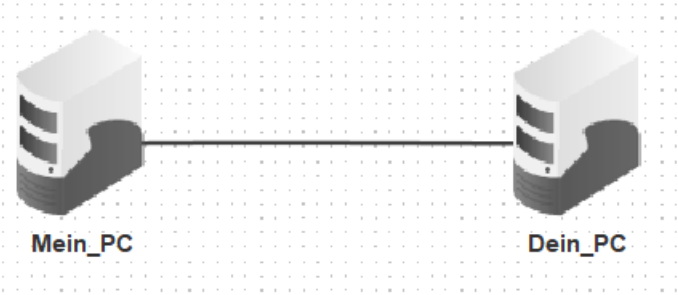
Auf diese Weise kommt jeder schnell wieder dran, und keiner muss lang warten. Aber, wenn man mit der Stoppuhr nachmisst, würde man sehen, dass die Übertragung jetzt doppelt so lang dauert, wie wenn ein PC die Leitung ganz für sich allein hätte.

Und wie ist es jetzt bei drei, vier, fünf Computern? Genau gleich. Die Computer teilen sich das Netzwerk gleichmäßig, jeder kommt genau so oft dran wie die anderen. Aber insgesamt dauert das Übertragen einer bestimmten Datei immer länger, je mehr Computer gleichzeitig das Netzwerk nützen.

Merke: Netzwerke verteilen ihre Geschwindigkeit schön gleichmäßig auf alle Computer, die es gleichzeitig benützen wollen. Keiner muss ewig lang warten, bis er drankommt. Aber: je mehr Computer gleichzeitig etwas im Netzwerk machen wollen, desto länger dauert es, bis alle endlich fertig sind. Der Benutzer sagt dann: "das Netzwerk wird langsam".

Unser erstes kleines Netzwerk

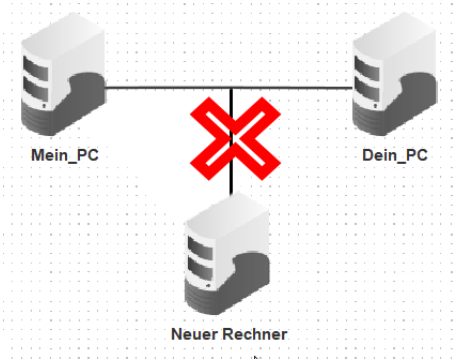
Das kleinste Netzwerk, das man mit Ethernet bauen kann, besteht aus genau zwei Geräten, und einem Stück Ethernet-Kabel dazwischen eingesteckt. Das können zwei Computer sein, oder ein Computer und ein Drucker mit Netzwerkanschluss, oder ein Computer und ein Router. Wichtig: es können nur zwei sein.

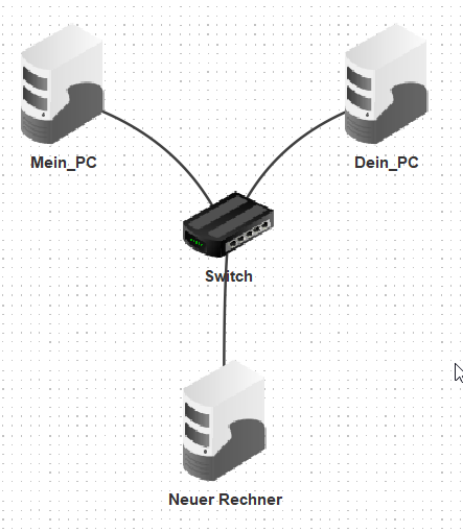


Man braucht dazu nur ein Ethernet-Netzwerkkabel, und muss den beiden Geräten eine passende IP-Adresse zuweisen.

Netzwerkverteiler: "Switches".

Leider geht das Verbinden mit einem billigen Kabel nur mit genau zwei Geräten, man kann im Ethernet keine weitere Abzweigung für ein drittes Gerät einbauen. Ab drei Geräten, muss zwingend ein Switch ("Netzwerkverteiler") hinzugefügt werden.





So geht das nicht! So geht das.

Die kleinsten Switches, die man kaufen kann, haben 4 oder 5 Anschlüsse, und die Größten 48 oder gar noch mehr.

Wenn das nicht ausreicht, kann auch mehrere Switches parallelschalten. Dazu verbindet man die Switches mit einem kurzen Stück Ethernet-Kabel (rot eingezeichnet).

5 Anschlüsse

48 Anschlüsse

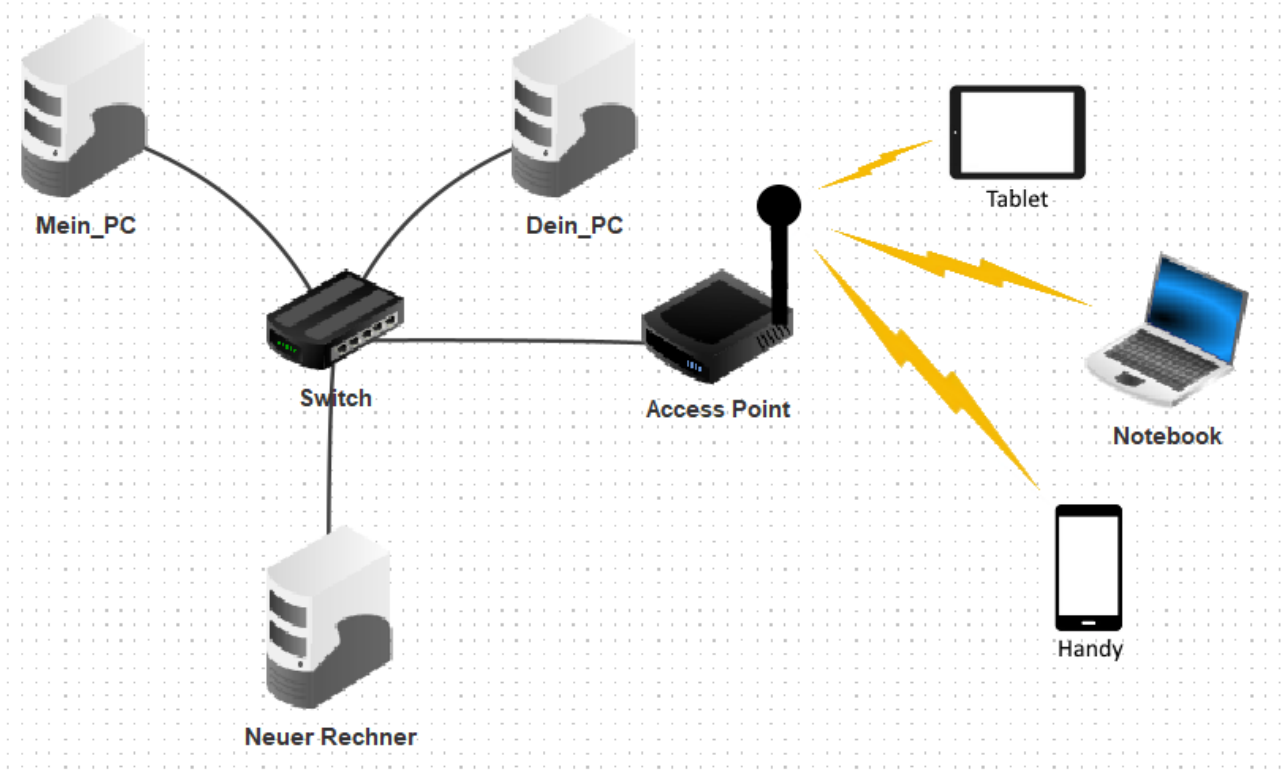
48 + 48 = 96 Anschlüsse

Die beiden verbundenen Switches verhalten sich dann wie ein einziger großer Switch mit 96 Anschlüssen. Selbstverständlich müssen die Switches dazu nicht identisch sein, man kann, wenn man nur ein paar Anschlüsse zu wenig hat, auch einen kleinen Switch und einen großen Switch zusammenschalten.

Man verliert dabei aber immer einen Anschluss pro Switch, nämlich den, wo das rote Verbindungskabel eingesteckt ist.

Switches sind aus der Sicht des IP-Netzwerks "unsichtbar", sie benötigen nicht einmal unbedingt eine eigene IP-Adresse.

Netzwerk ohne Kabel: WLAN (WiFi)



WLAN erweitert das kabelgebundene Ethernet Netzwerke um Funkstrecken. Das ist praktisch, weil man damit herumlaufen kann und keine Kabel im Weg sind. Man kann zu jedem kabelgebundenen LAN einen oder mehrere Funkempfänger ("Access-Points") hinzufügen, um alle oder einige Geräte mit WLAN zu versorgen.

Jetzt können auch Endgeräte, die gar keinen Stecker für das Ethernet haben, z.B. Handys und Tablets, an das Netzwerk angeschlossen werden.

Man kann am Access-Point sein WLAN entweder einfach "offen" einstellen, dann kann sich jeder jederzeit damit verbinden, ohne ein Passwort einzugeben. Oder man schaltet im Access-Point "WPA" oder "WPA2" Sicherheit ein, und legt dabei ein geheimes Passwort fest. Nur wer das Passwort kennt, kann sich mit dem WLAN verbinden.

Man kann ein Netzwerk aufbauen, das nur WLAN-Geräte beinhaltet, dann braucht man weder Kabel noch Switches. WLANs sind aber wesentlich langsamer und störanfälliger wie Kabelnetzwerke, und haben nur eine geringe Reichweite. Deswegen ist es oft sinnvoll, wichtige oder weit entfernte Computer über Kabel anzuschließen. Alle Access-Points haben dafür auch noch mindestens einen Anschluss für Ethernet-Kabel, dort kann man dann einen Switch für ein kabelgebundenes LAN hinzufügen.

Wenn man alles richtig macht, können am Ende alle Geräte mit allen anderen Geräten im LAN Daten austauschen, egal ob ein bestimmtes Gerät nun über Kabel oder über Funk angeschlossen ist.

Man hört es meistens nicht gerne, aber WLAN-Verbindungen machen wesentlich mehr Probleme als Kabelverbindungen. Die Ursache liegt darin, dass Funkübertragung wesentlich schwieriger und störanfälliger als Übertragung über Kabel ist. Die meisten Probleme äußern sich als "langsames Internet" oder "Verbindungsabbrüche".

Es gibt viele Ursachen für WLAN Störungen, und das Aufbauen eines billigen zusätzlichen Kästchens ("Repeater") hilft leider nur manchmal, hin und wieder schadet es sogar.

Für eine richtige WLAN-Diagnose muss man noch viel mehr lernen als ds was ich hier im Unterricht durchnehmen kann, das könnte vielleicht einmal ein eigener Kurs im Informatik-Unterricht werden.

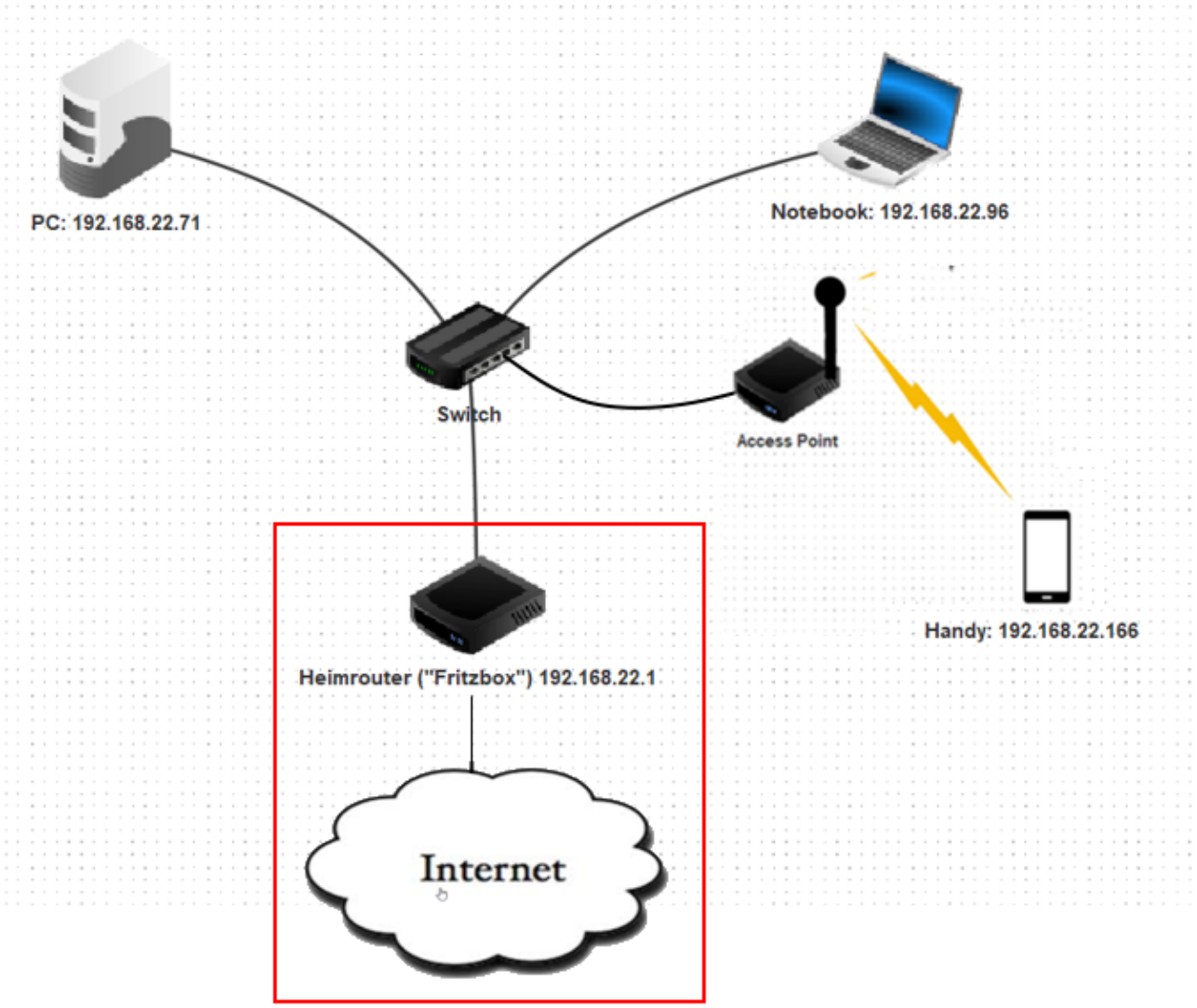
Anbindung an das Internet: der "Router"

Bisher haben wir uns nur in unserem eigenen kleinen LAN-Netzwerk bewegt. Um Daten zwischen deinen eigenen Geräten auszutauschen, zum Beispiel zwischen deinem Handy und deinem PC, würde das schon reichen. Jetzt wollen wir uns mit aber auch noch mit dem Internet verbinden.

Dazu muss man einen Vertrag mit einem Provider abschließen, einen "Router" anschließen, und für das eigene Netzwerk korrekte "private" IP-Adressen verwenden.

Der Internet-Provider verlang jeden Monat eine Gebühr. Eingeschlossen ist meistens ein Miet-Router, den man nach Abschluss des Vertrages per Post geschickt bekommt.

Der Router ist vom Provider bereits so eingestellt, dass man ihn nur noch anstecken und einschalten muss.



In Deutschland sind die Router der Firma AVM ("Fritzbox") sehr verbreitet, es gibt aber auch Router von vielen anderen Herstellern. Hier ein paar Bilder von Routern:

In Firmennetzen kommen, wie schon bei den Switchen, oft sehr viel größere und leistungsstärkere Router zum Einsatz.

Weil der Router so wichtig ist für die Verbindung in das Internet, ist es üblich, ihm entweder die niedrigste oder die höchste mögliche IP-Adresse zu geben. Erinnere dich: die 0 und die 255 sind reserviert, also ist im Heimnetz meistens die 1 oder die 254 die Adresse des Routers.

IP-Adressen für kleine "private" Netzwerke

Jedes Gerät, das am Netzwerk teilnehmen soll, benötigt eine IP -Adresse aus dem Bereich der "Privaten" IP Adressen, und eine Subnetz-Maske. Da diese Adressen sehr versteckt arbeiten, wissen viele nichts davon. Trotzdem sind sie wichtig, wenn man verstehen will, wie man IP Netzwerke aufbaut, und wie man vorgehen muss, um Netzwerk-Fehler zu finden.

Die am meisten verbreitete Norm sind IP-Adresse und Subnetz-Masken nach "IPv4" / "private Adressen". Solche Netze sind ohne Weiteres für Internet-Anbindung geeignet.

IP Adressen bestehen immer aus vier Feldern, die mit einem Punkt voneinander getrennt sind. Hier ein Beispiel:

IP-Adresse: 192.168.022.???

Feld 1 Feld 2 Feld 3 Feld 4

Subnetz-Maske: 255.255.255.000

Nach Internet-Norm beginnen die meisten privaten Netzwerke mit 192.168, und haben die Subnetzmaske 255.255.255.0. Man kann mit ihnen maximal 254 Geräte ans Internet anschließen, für zu Hause reicht das. Größere Firmen-Netzwerke beginnen oft mit 172 oder mit 10., und haben Subnetzmasken wie 255.255.252.0. Mit diesen IP-Adressen und Subnetzmasken kann man viele viele tausend Geräte abdecken, das reicht auch für größere Firmen

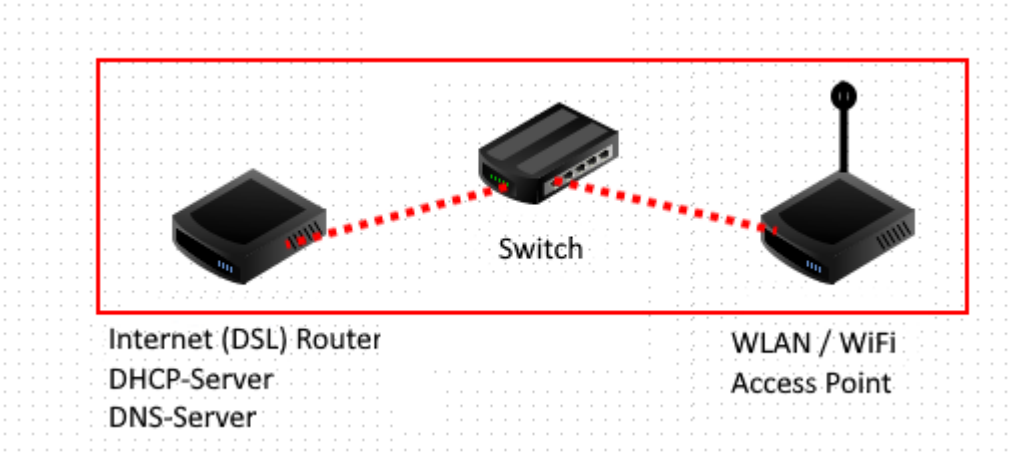
Einige wichtige Regeln:

- Aus computertechnischen Gründen (jedes Feld ist genau ein "Computer-Byte" groß. Ein "Computer-Byte" kann nur Zahlen von 0 bis 255 aufnehmen) stehen in den Feldern immer **nur Zahlen zwischen 0 und 255**.
- Die IP-Adressen eines bestimmten Netzwerks **beginnen immer gleich** (z.B. 192.168.22), und **enden bei jedem Gerät anders** (ich habe deswegen oben "???" geschrieben). Beispiele: 192.168.22.14, 192.168.22.15, 192.168.22.27, uns so weiter.
- Die Adressen **"0" und "255"** sind für die interne Netzwerkverwaltung **reserviert**, du darfst sie daher nicht als IP-Adresse für ein Gerät verwenden. 192.168.22.0 wäre also verboten, ebenso 192.168.22.255. Die übrigen Zahlen (also von 1 bis 254) kannst Du beliebig an Geräte vergeben.
- Die Reihenfolge, in der die IP-Adressen vergeben werden, ist egal, es dürfen auch Lücken in den Adressen sein. Es ist also nicht nötig, dass die Geräte genau 192.168.22.1, 192.168.22.2, 192.168.22.3 und so weiter hochgezählt werden. Du darfst aber jede Adresse nur ein einziges Mal vergeben.
- Es ist üblich, dem Internet-Router entweder die niedrigste oder die höchste **zulässige** Adresse zu geben, das wäre in meinem Beispielnetz 192.22.121.1 oder 192.168.22.254. Die Router-Adresse darfst du nicht an ein anderes Gerät vergeben.
- Die **Subnetz-Maske** ist in kleinen Netzwerken, die mit 192.168 beginnen, meistens 255.255.255.0, und **muss bei allen Geräten gleich sein**.

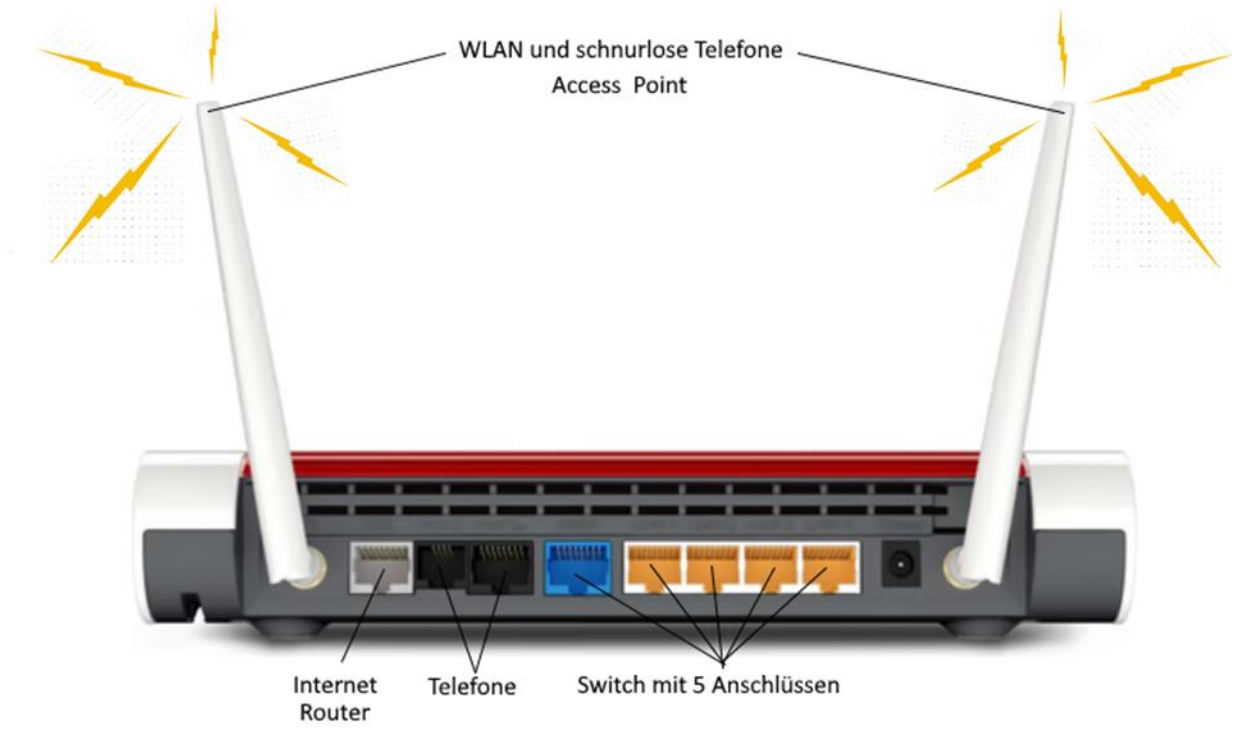
Netzwerk zu Hause

In großen Firmen-Netzwerken findet man Switches, Router, Access Points, DHCP Server und DNS Server tatsächlich als eigene Geräte, oft braucht man auch mehrere davon.

Zu Hause, wo man Platz sparen möchte, und wo das Netz vergleichsweise klein ist, kauft man zusammen mit dem Internet-Anschluss vom Internet-Provider ein Gerät, in das alle nötigen Geräte (Switch, Router, Access Point) und Dienste (DHCP-Server, DNS-Server, Firewall) zusammen eingebaut sind.



Die Rückseite eines solchen Routers schaut z.B. so aus:



Das Kästchen hat also alles, was die einzelnen Geräte gebraucht hätten: Antennen fürs WLAN, Stecker-Anschlüsse für Ethernet-Kabel (blau und gelb), einen Anschluss fürs Internet (grau), wo die DSL-Leitung, die vom Internet-Provider kommt, eingesteckt werden muss.

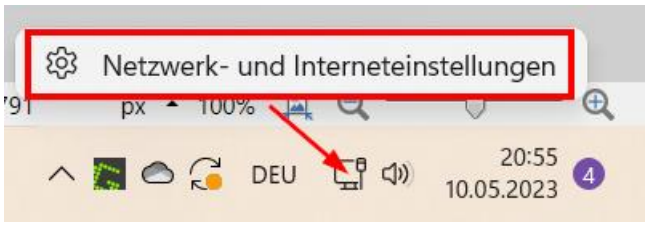
Dazu kommen bei Geräten für zu Hause oft auch noch Anschlüsse für Telefone, die gibt es mit Kabelanschluss (Schwarz) oder drahtlos ("DECT", die funktionieren so wie WLAN über eine Antenne).

Beachte, dass diese Farben nicht genormt sind. So ist zum Beispiel bei Routern der Firma "Asus" der Internet-Anschluss blau gefärbt. Was genau wo eingesteckt werden muss steht im Handbuch, das zu jedem Router mitgeliefert wird.

Die IP-Adresse des eigenen Gerätes feststellen

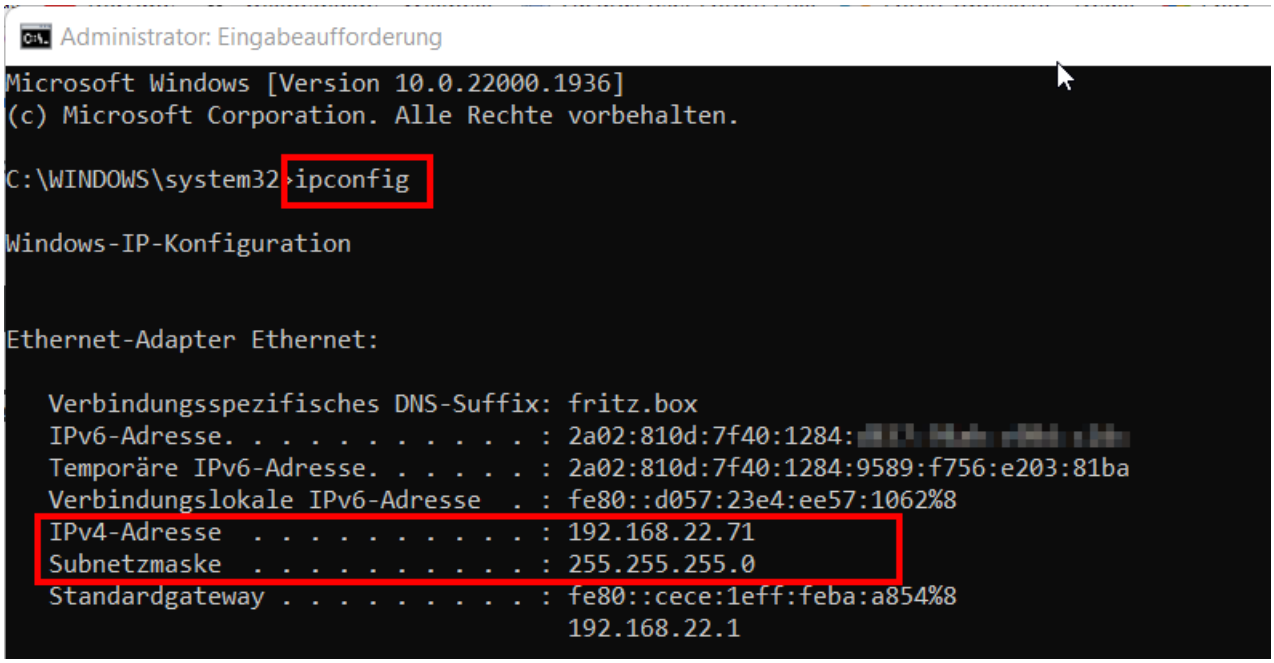
Jedes Gerät im Netzwerk, egal ob PC, Notebook, Handy, Tablet, Netzwerk-Drucker oder Router muss also eine IP-Adresse haben. Informatiker wollen sicher wissen, wie die IP-Adressen ihrer Geräte lauten, man braucht sie bei der Fehlersuche.

Schauen wir doch erst mal auf einem Windows-PC nach. Klicke mit der rechten Maustaste auf das Netzwerksymbol unten in der Taskleiste, und wähle "Netzwerk- und Interneteinstellungen".

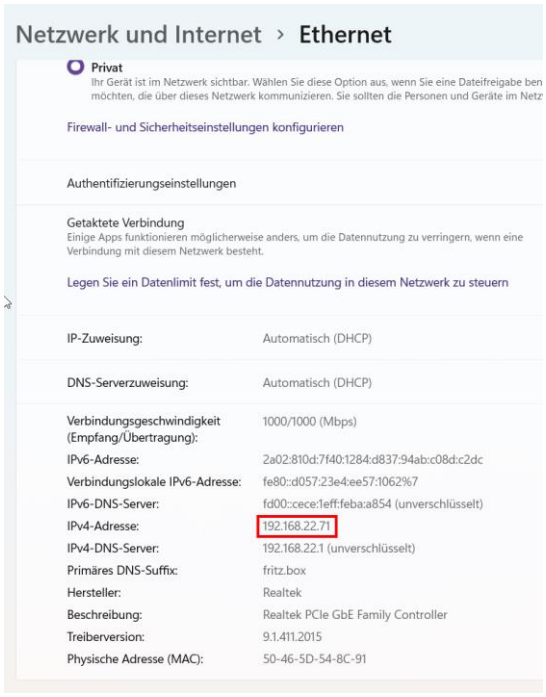


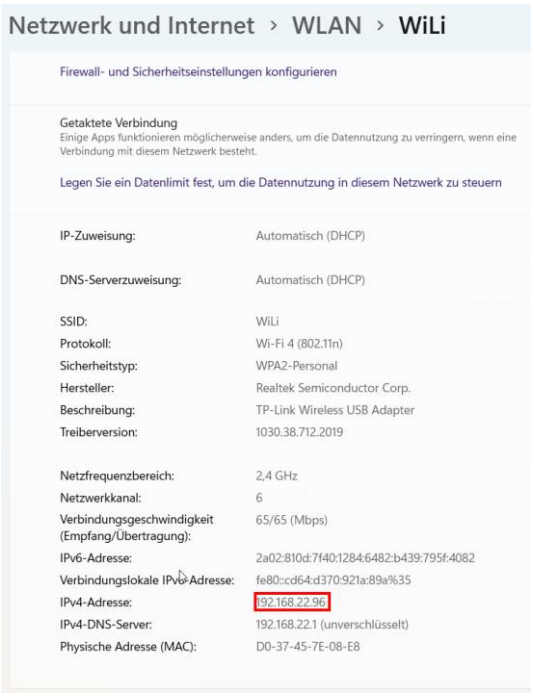
Wenn dein PC mit einem Kabel funktioniert, geht’s weiter bei "Ethernet". Wenn dein Notebook über WLAN verbunden ist, geht’s weiter bei "WLAN - Eigenschaften".

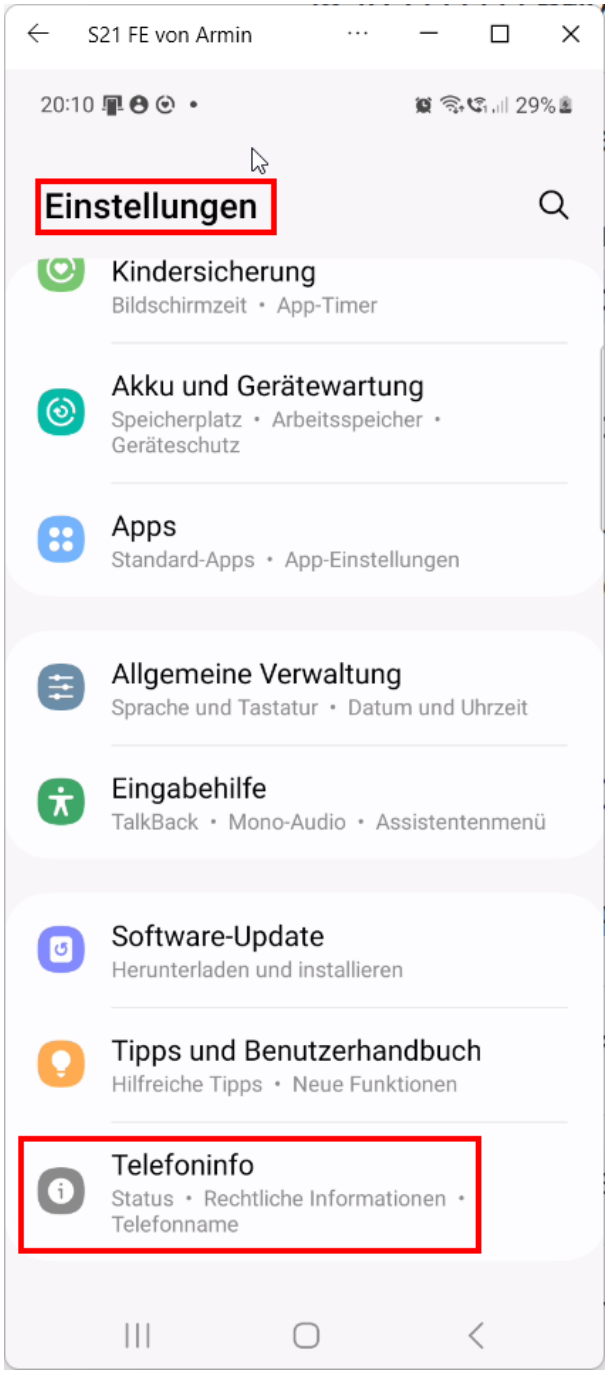
Du kannst aber auch den Kommandozeilen-Befehl "ipconfig" verwenden.

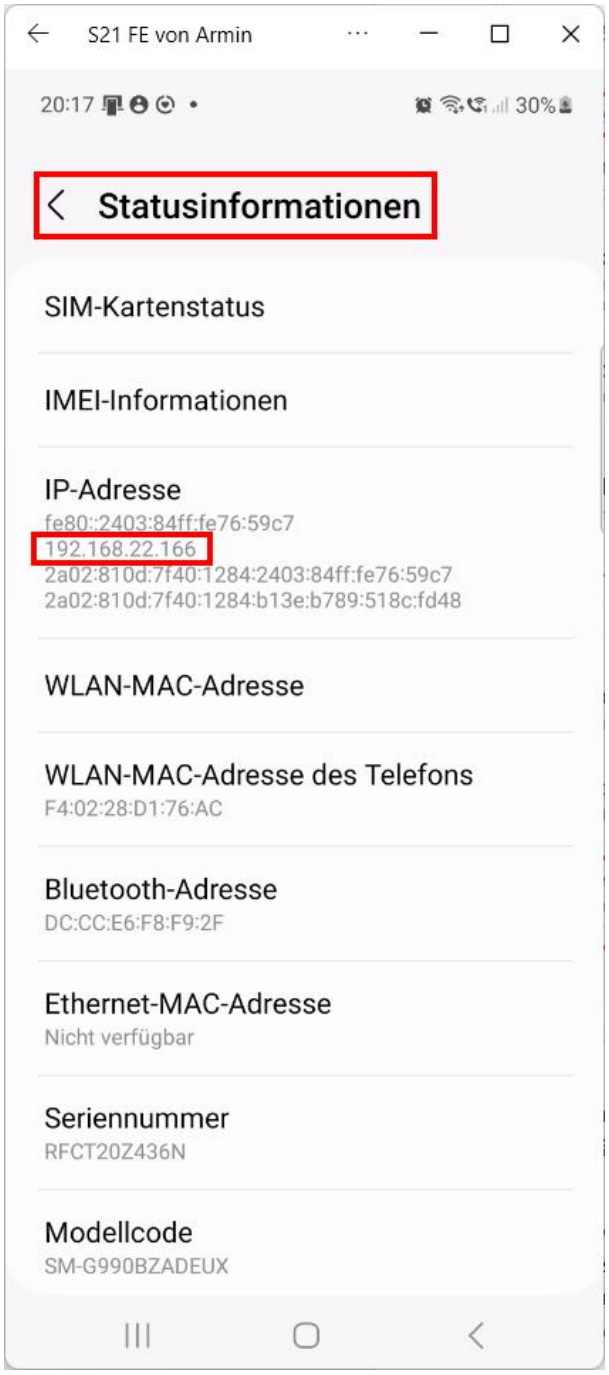


Wie ist das nun bei Smartphones? Genau gleich. Du findest die IP-Adresse bei Android Telefonen unter "Einstellungen" – "Telefoninfo" – "Statusinformationen".









Mein Telefon hat also die IP-Adresse "192.168.22.166".

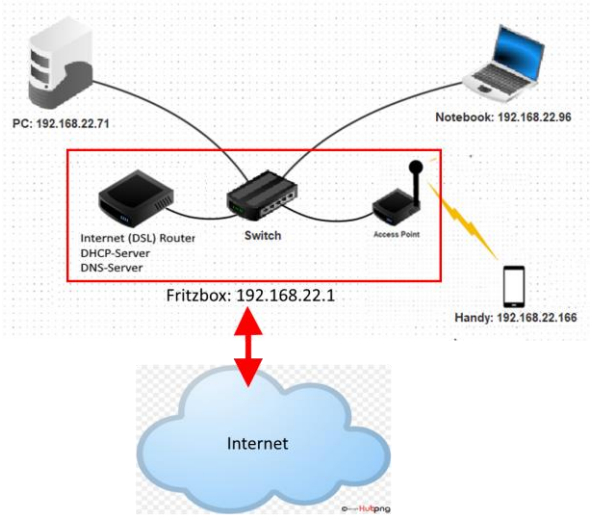
Netzwerkverbindung testen: "Ping"

Netzwerke sind relativ empfindlich. Kabel können zerdrückt oder abgerissen werden, oder ein Mitschüler steckt sie wieder mal aus, um jemanden zu ärgern. WLANs haben nur geringe Reichweite, und oft werden sie gestört, zum Beispiel von Mikrowellen-Herden, Funk-Videokameras, Funk-Kopfhörern oder Bluetooth-Geräten.

Netzwerkverbindungen testen ist daher etwas, was ein Informatiker unbedingt können muss.

Praktisch alle Computer haben deswegen ein kleines Testprogramm dabei, mit dem man die Verbindung zu einem anderen Computer testen kann. Es heißt "Ping".

Ich mache gleich ein richtiges Beispiel, und ein richtiges Netzwerk, rein zufällig ist es das bei mir daheim, das Netzwerk sieht so aus:

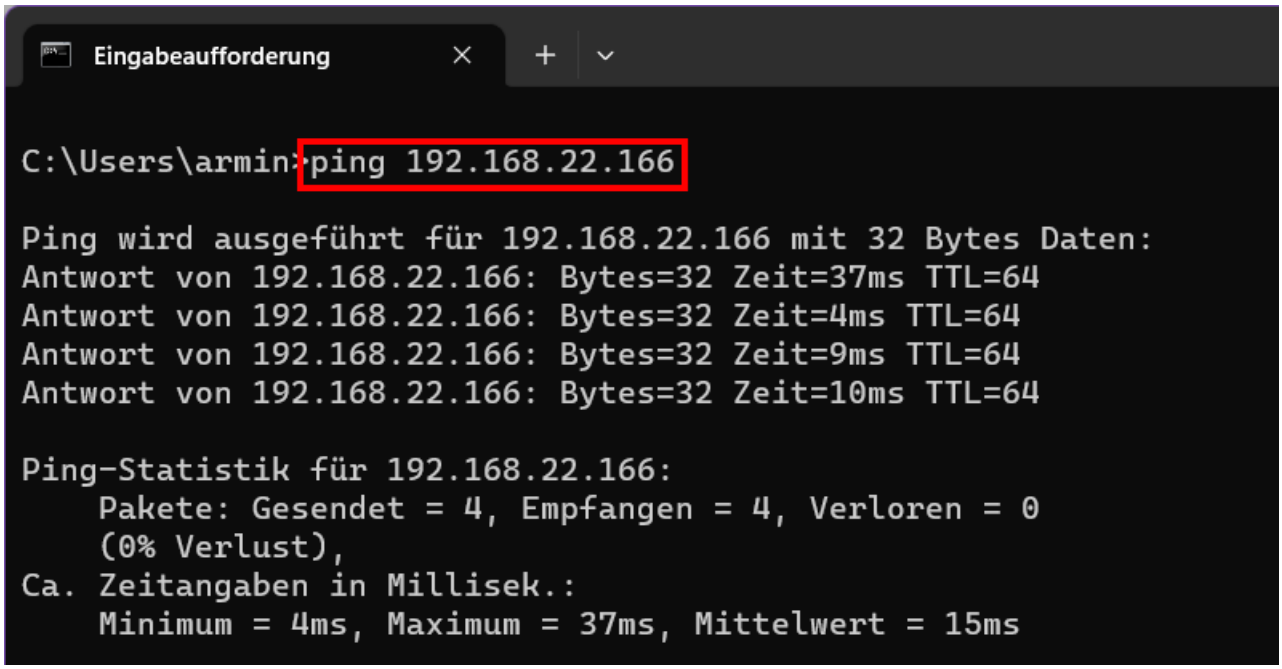


Man braucht für so einen Test also die IP-Adresse, die man testen möchte. Hier gibt es vier davon:

Handy:	192.168.22.166	(Android)
PC:	192.168.22.71	(Windows)
Notebook:	192.168.22.96.	(Windows)
Router:	192.168.22.1	(AVM Fritzbox)

Test mit einem Windows- oder Linux PC

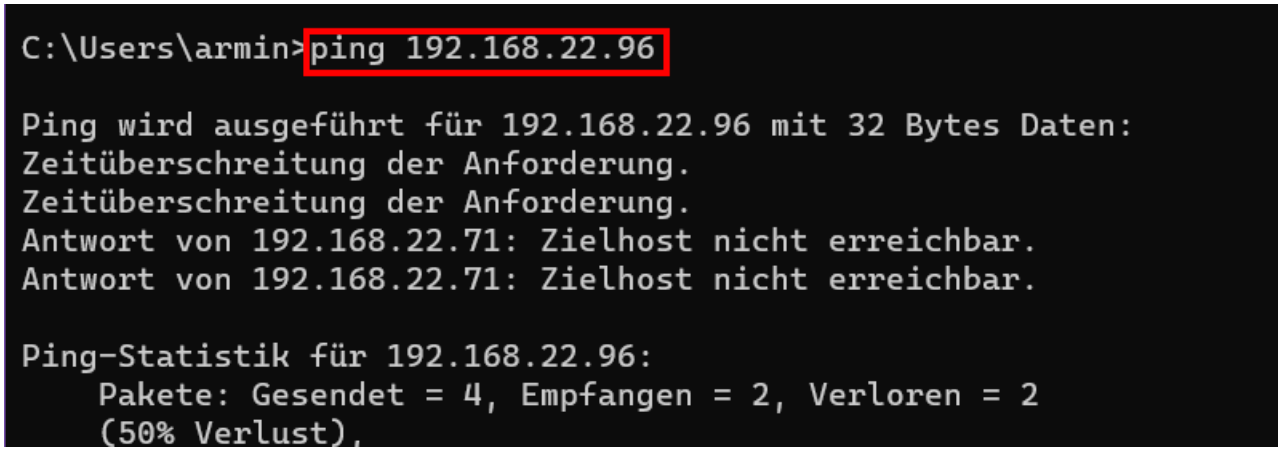
Testen wir erst einmal mit einem Windows-PC, da ist das Ping Tool immer schon mit dabei. Öffne eine Eingabeaufforderung ("Kommandozeile", "Cmd"), und gib den Befehl "Ping", Abstand (Leertaste), dann die IP-Adresse, die du testen möchtest, und dann [Enter] ein.



Wenn du danach positive Ping-Antworten bekommst, ist die Verbindung OK. Bekommst du Fehlermeldungen ("Timeout"), dann ist etwas faul. Erst einmal ein erfolgreicher Test. Vom Handy (192.168.22.166) bekomme ich vier Antworten mit Zeitangaben von 4 bis 37ms.

Der PC 192.168.22.71 konnte das Handy 192.168.22.166 tadellos erreichen, die Verbindung zwischen diesen beiden Geräten ist also in Ordnung.

Natürlich wollen wir auch sehen, wie das ist, wenn ein Test fehlschlägt. Ich schalte also das Notebook (192.168.22.96) aus, jetzt kann es sicher keine Ping Testpakete beantworten. Dann teste ich:

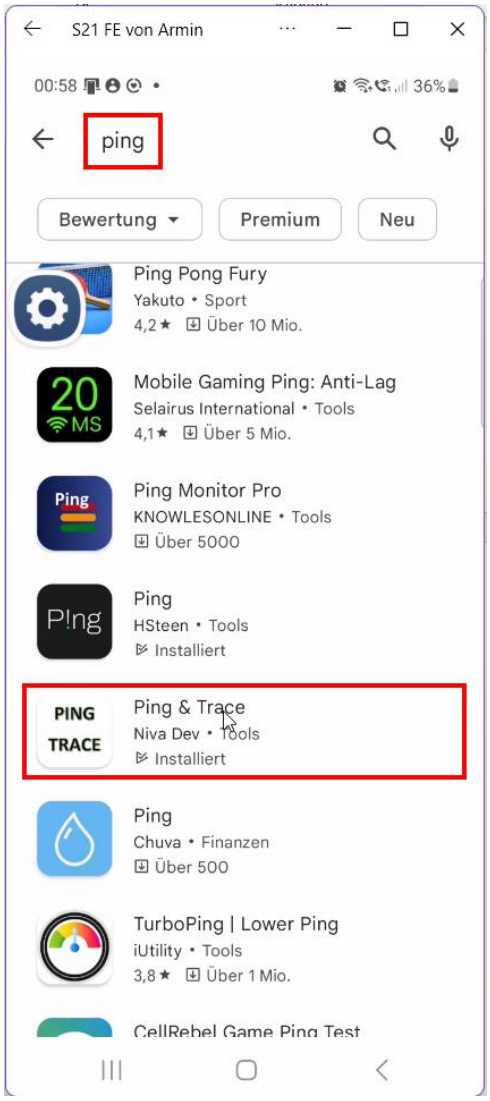


Vom Notebook 192.168.22.96, den ich ja absichtlich abgeschaltet habe, bekomme ich also keine Antwort, und der Ping Test gibt nur Fehlermeldungen wie "Zeitüberschreitung" und "Zielhost nicht erreichbar" aus.

Mit einem Handy oder einem Tablet testen

Kann man solche Tests auch mit dem Handy oder mit einem Tablet machen? Na klar, nur … bei Android ist keine "Ping" App mit dabei. Man kann sich aber eine aus dem Play Store holen. Da gibt es sehr viele davon. Ich schlage dir die App "Ping & Trace" von "Niva Dev" vor. Sie derzeit (Mai 2023) gratis, werbefrei und klaut keine Daten. Trotzdem funktioniert sie super. Leider ist sie aber in Englisch geschrieben – da man aber nur ganz wenige Wörter braucht solltest du trotzdem damit zurechtkommen.

Wir holen uns also die "Ping & Trace" App aus dem Android Play Store.



Nachdem du die "Ping & Trace" App geladen hast, öffnest du sie.

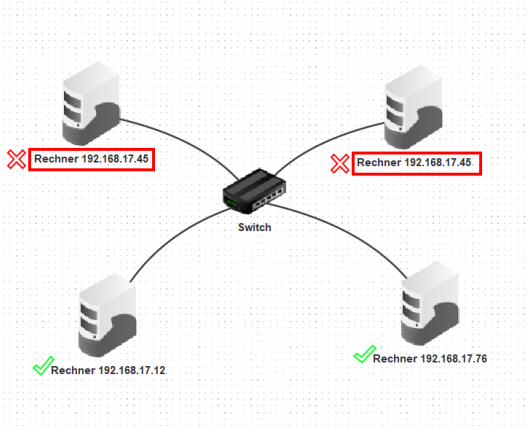
Dann gibst du bei (1) die IP-Adresse des Gerätes ein, zu dem du testen möchtest. Schau oben nach: mein PC hatte die IP-Adresse 192.168.22.71. Den wollen wir testen. Also gibst du oben die 192.168.22.71 ein, dann drückst du den roten Knopf rechts unten bei (2). Es dauert dann ein bisschen, dann erscheinen die Zeilen bei (3). Dort kannst du dann nachsehen, ob die Verbindung geklappt hat oder nicht.

Bingo! Vier positive Antworten, der PC ist also erreichbar. Und was ist mit dem Notebook, das ja immer noch abgeschaltet ist? Gleich mal nachsehen, die IP-Adresse war 192.168.22.96:

Keine erfolgreichen Versuche. Keine Antwort. Vier Pakete gesendet ("4 packets transmitted"), null empfangen ("0 received"). Also keine einzige Antwort kam zurück, das Notebook ist nicht erreichbar.

Häufig gemachte Fehler bei IP-Adressen

Was passiert, wenn man einen Fehler macht? Zwei Fehler kommen häufig vor:



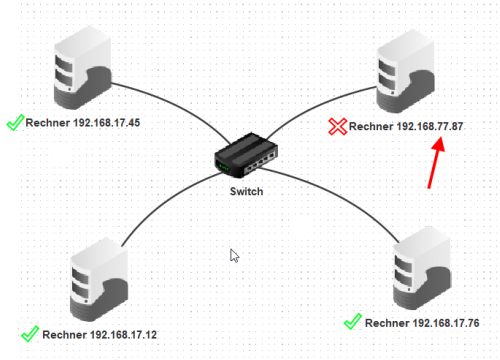
Fehler 1: doppelte IP Adresse ("IP Adresskonflikt")

Die beiden oberen Rechner, denen jemand dieselbe IP Adresse gegeben hat, würden beide nicht im Netzwerk funktionieren. Die unteren beiden Rechner, die eindeutige IP Adressen bekommen haben, würden ganz normal funktionieren.

Besonders fatal ist es, wenn man einem Gerät die IP-Adresse des Routers zuweist. Dann funktioniert das Netzwerk überhaupt nicht mehr.

Fehler 2: falsche Netzwerk-Adresse

In diesem Netz sind die Geräteadressen alle okay, wir haben die 45, die 87, die 12 und die 76, keine ist doppelt. Aber bei einem Computer wurde eine falsche Netzwerkadresse eingegeben, blöder Tippfehler, 77 statt 17.



Dieser eine Computer wird keine Netzwerkverbindung bekommen, alle anderen funktionieren ohne Probleme.

Fehler 3: falsche Subnetz-Maske

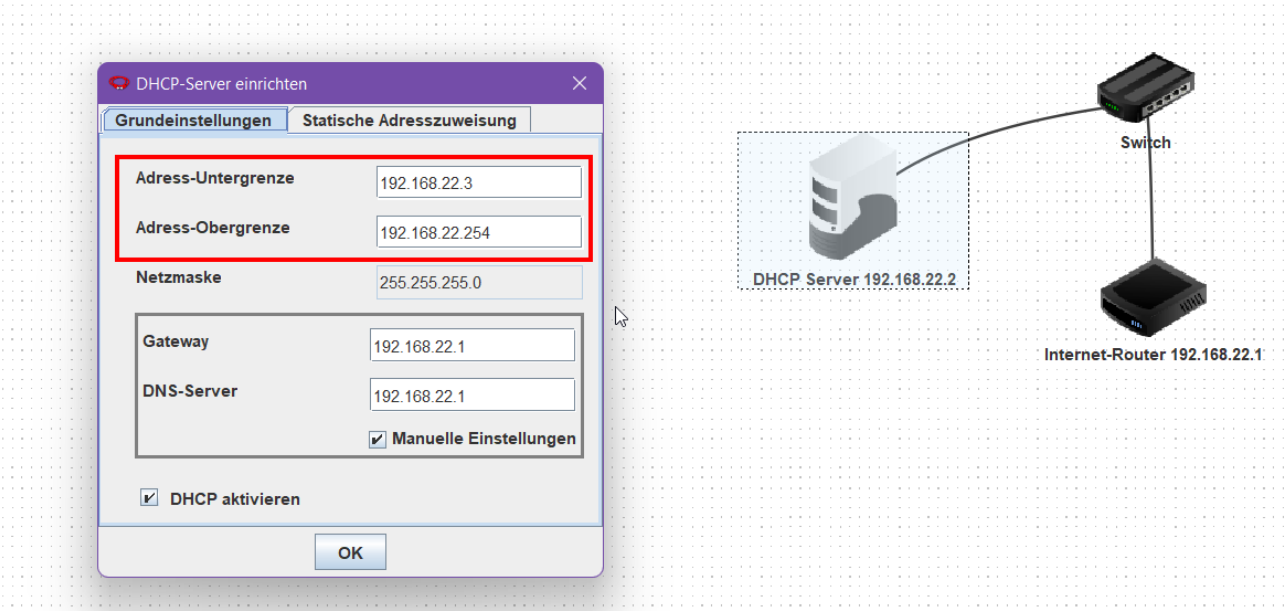
Alle Geräte in einem LAN Netzwerk müssen **die selbe Subnetz-Maske** haben. Für kleine, private Netze (die mit 192.168 beginnen) ist die Subnetzmaske fast immer 255.255.255.0

Der DHCP-Server

Wir erinnern uns: eigentlich müsste man die IP-Adressen aller Geräte von Hand eintragen, eine in jedes Gerät. Und dabei darauf achten, dass man ja keine IP-Adresse einträgt, die schon ein anderer Rechner hat. Dazu hat keiner so richtig Lust, also installiert man einen DHCP-Server im Netzwerk, der das für uns erledigt.

Wir können das super ausprobieren in Filius. Am besten beginne ich ein ganz neues Netz, und installiere den DHCP-Server und das Internet-Gateway als allererstes.

Zur Erinnerung: mein Netzwerk war 192.168.22.0, mögliche Adressen sind also 192.168.22.1 bis 192.168.22.254. Zwei Geräte im Netz kann man aus technischen Gründen typischer Weise **nicht** vom DHCP-Server Adressen holen lassen: das Standard-Gateway (den Router, der ins Internet führt, oder – genauer – Router allgemein), und den DHCP-Server selber. Die 192.168.22.1 und die 192.168.22.2 darf ich also nicht an Geräte herausrücken. Die anderen Adressen aber schon, deswegen reicht mein DHCP-Bereich (Adress-Untergrenze bis Adress-Obergrenze) von 192.168.22.3 bis 192.168.22.254.



Tipp: erfahrene Netzwerker würden dir wahrscheinlich raten, erst bei der 10 oder der 20 zu beginnen, dann hast du die Adressen 3 bis 9 (19) noch für irgendwelche "Spezialaufgaben" reserviert. Aber ich wollte es nicht zu kompliziert machen.

Beachte auch, dass dieser DHCP den Geräten auch gleich eine Subnetz-Maske, ein Standard-Gateway und die Adresse des DNS-Servers senden kann.

Für diese beiden Zusatzfelder gilt dasselbe wie für die IP-Adresse: der DHCP-Server selbst, und das Standard-Gateway, die ja keine IP-Adresse vom DHCP-Server holen können, bekommen auch diese Optionen nicht, man muss sie auf diesen beiden Computern also von Hand eintragen. Auf allen "normalen" Geräten wird das aber automatisch erledigt.

Und was ist jetzt zu Hause? Wo ist da mein DHCP-Server? Weil man daheim immer einen braucht, haben alle Internet-Router, die für Heimanschlüsse verkauft werden, einen DHCP-Server schon mit eingebaut.

Der DNS-Server

Ganz im Ernst: mag hier irgendjemand seine Rechner mit der IP-Adresse ansprechen? Kennt man sie überhaupt, von allen wichtigen Rechnern, auch von denen im Internet? Normalerweise nicht.

Namen sind doch sowieso viel einfacher zu merken. Die Lösung für das Problem ist wieder eine Tabelle, sie enthält in der linken Spalte die Computernamen und in der rechten Spalte die IP-Adressen. Wenn man bei irgendeinem Befehl, also z.B. bei PING, keine IP-Adresse eingibt,

sondern etwas anderes, sucht der Computer in der DNS-Tabelle, ob er dort eine Zeile mit dem Computernamen finden kann.

Handy.linder.lan	192.168.22.166
PC.linder.lan	192.168.22.71
Notebook.linder.lan	192.1687.22.96
Fritz.box	192.168.22.1

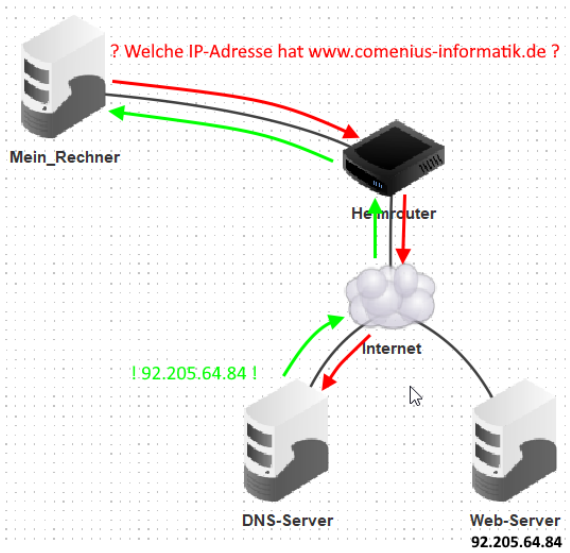
Die Tabelle wird von einem "DNS-Server" verwaltet. Zu Hause macht das auch der Internet-Router so nebenbei mit.

HTTP-Server: der Kern vom Internet!

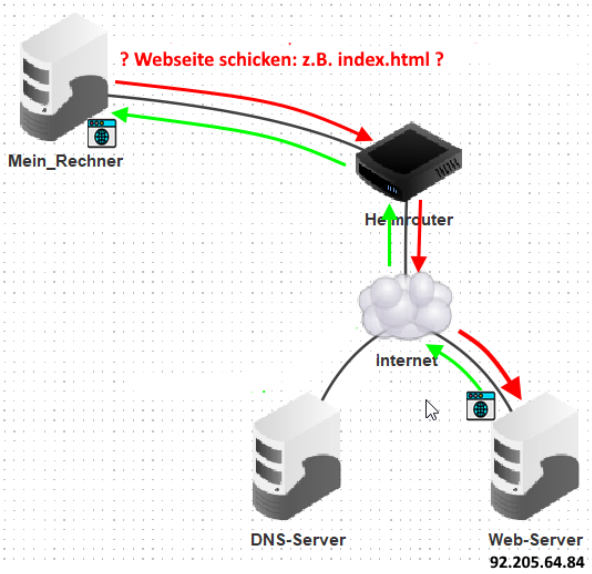
Das Internet besteht aus Seiten, die von "Webservern" bereitgestellt werden. Das Programm, welches Webseiten vom Internet laden und anzeigen kann, heißt "Browser". Die meisten sagen aber lieber den Namen, den der Hersteller "seinem" Browserprogramm gegeben hat, also "Internet Explorer", "Safari", "Edge", "Firefox", "Chrome", "Opera", und es gibt noch viele mehr.

Die genaue Vorgehensweise zum Anzeigen einer Internetseite geht wie folgt:

- Der Anwender gibt in die Adresszeile des Browsers den Internet-Namen (URL) der Seite ein, z.B. www.comenius-informatik.de.
- Der Browser fragt bei einem DNS Server nach der IP-Adresse dieser Seite, und bekommt z.B. 92.205.64.84 als Antwort. Man nennt diese "Umwandeln" von einem Namen in eine Adresse "**Namensauflösung**".
- Der Browser sendet die Aufforderung, die Seite vom Computer mit der Internet-Adresse 92.205.64.84 zu laden, an sein Standard-Gateway (den Router in seinem LAN)
- Der Router sendet die Anforderung über seine WAN Schnittstelle ins Internet, welches die Anfrage zu dem Webserver mit der IP Adresse 92.205.64.84 weiterleitet
- Der Webserver empfängt die Anforderung, lädt die Seite von seinem internen Datenspeicher und sendet sie zurück an den Computer, der die Seite angefordert hat.
- Das Internet sendet die Antwortseite weiter, bis sie an der WAN Schnittstelle des eigenen Routers eintrifft.
- Der eigene Router vermittelt die Seite im LAN weiter an den Computer, der die Anfrage gestellt hat
- Auf diesem Computer zeichnet der Browser die Seite auf dem Bildschirm an.



Phase 1: "Namensauflösung"



Phase 2: Webseite ausliefern

Tipp am Schluss: IPv6 Adressen

Ein kleiner Tipp am Schluss, gut für die Zukunft.

Das IP-Adresssystem mit den vier Feldern (IPv4), das wir in diesem Kurs gelernt haben, wird nach und nach abgelöst von einem Nachfolger (IPv6) mit 8 Byte langen Adressen. Die meisten Geräte bekommen inzwischen zwei Adressen, eine IPv4 Adresse (z.B. 192.168.22.132) und eine IPv6 Adresse (z.B. 2a02:810d:7f40:1284:51c8:9278:8756:b450).

Meistens gibt es pro Gerät sogar noch zwei oder drei zusätzliche IPv6 Adressen. Wofür sie gut sind - das ist dann aber Teil eines eigenen Kurses.