

Heimnetzwerke: Einrichten, absichern und gemeinsam surfen

In der heutigen Zeit sind in vielen Haushalten kleine Heimnetzwerke zu finden, die ihre Verbreitung durch das Nutzen eines DSL-Anschlusses entstanden sind. Solche Netzwerke bestehen sehr häufig aus einem Router, der z.B. vom Provider subventioniert bereitgestellt worden ist, und mehreren PCs und Laptops.

Diese Erklärung soll helfen das heimische Netzwerk mit gängigen Methoden einzurichten, die auch dem aktuellen Stand der Sicherheit entsprechen.

Anfangs werden Grundlagen zu den Netzwerken geschaffen, um ein Verständnis für die weiteren Erklärungen zu schaffen. Im Weiteren wird dann näher auf die Einrichtung der PCs und eines Routers eingegangen.

Die Erklärung erfolgt beispielhaft für ein Netzwerk aus zwei PCs, die sowohl drahtlos, als auch drahtgebunden am Netzwerk teilhaben sollen. Die Namen und Adressen sind dem hiesigen Netzwerk angepasst, für dein Netzwerk wirst du also deine entsprechenden Adressen und Namen verwenden.

1 Grundlagen

Um einen Einstieg in die Netzwerkthematik zu schaffen, bedienen wir uns dem Modell einer Stadt, oder einem Modell eines Stadtteils mit Häusern, Straßen und einer entsprechenden Verwaltung dazu. Städte sind grundlegend in Verkehrswege und Wohnorte gegliedert.

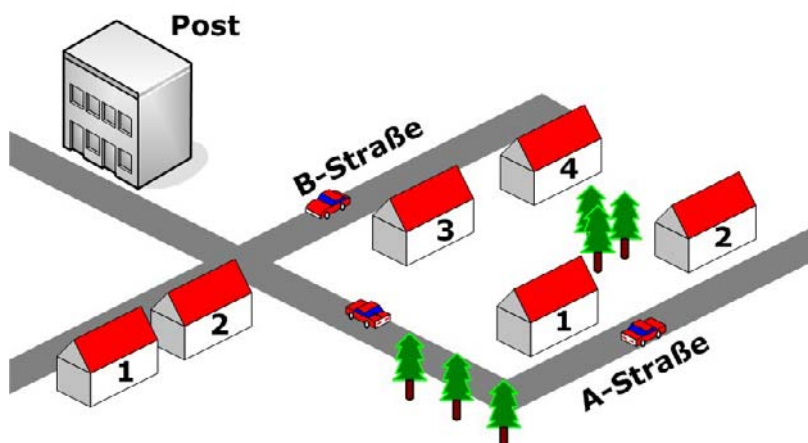


Bild 1: Stadtmodell

Verkehrswege stellen dabei die Verbindung zwischen Orten dar, bieten also die Möglichkeit sich zu bewegen. Häuser und Wohnungen sind feste Standorte, in denen man wohnen oder arbeiten kann. Ihre Lage wird durch postalische

Adressen (Ort, Straße, Hausnummer) fest definiert. Die Analogie zum Themenkomplex der Netzwerke liegt nahe, da dort eine ähnliche Verwaltung genutzt wird. Aus Straßen werden Kabel- oder Funknetze, aus Häusern Rechner oder Drucker (Host und Client), und aus der Verwaltung werden Server oder ein Router (Host und Gateway).

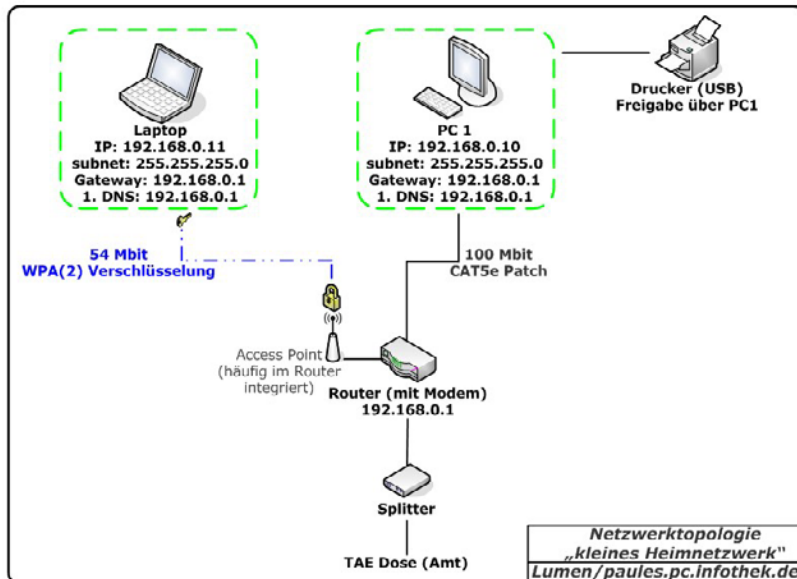


Bild 2: Netzwerktopologie

1.1 Adressen

Im Stadtmodell werden Adressen durch Postleitzahlen, Straßennamen und Hausnummern definiert. In einem Rechnernetz werden diese durch **IP-Nummern** realisiert. IP-Nummern bestehen zurzeit aus 4-stelligen Zahlenblöcken (IPv4), die das Netz, Subnetz und den Host definieren. Anhand der IP-Nummern werden also Rechner eindeutig identifiziert. Für Heimnetzwerke werden **Klasse-C Netze** benutzt, die wie hier mit 192.168. beginnen. Jedes Subnetz kann 254 Hosts beinhalten, wenn das Netzwerk also ein Subnetz von 192.168.0.x hat, können 254 Rechner oder Geräte integriert werden.

Können Router größere Bereiche aufspannen, z.B. von 192.168.0.1 - 192.168.2.254, dann können entsprechend mehr Hosts integriert werden.

Für kleine Heimnetzwerke reicht aber ein IP-Bereich völlig aus, gängige IP-Bereiche sind:

- 192.168.0.x
- 192.168.1.x
- 192.168.2.x
- 192.168.100.x
- 192.168.178.x

Die letzte IP eines Bereiches, die 192.168.x.255 wird **Broadcast** genannt. Über diese IP werden z.B. DHCP Anfragen gesendet, sie dient dem Netzwerk als Verteiler und „Ansprechpartner“ für gewisse Dienste und Befehle.

1.2 DNS

In einer Stadt werden Adressen so angewendet wie sie existieren, ein Brief an Müller wird auch an Müller geschickt. In einem Haus wird es selten Dopplungen geben. Rechner können mit Namen nicht umgehen, wenn dein PC wie hier im Beispiel PC1 oder Laptop heißt, kann der Rechner damit nichts anfangen. Damit aber trotzdem eine Kommunikation zu Stande kommt, werden die Namen zuerst in Adressen aufgelöst. Für diese **Namensauflösung** ist der **Domain Name Service** (DNS) zuständig, der eine Liste der Rechner mit ihren Namen und IP-Adressen führt. Eine entsprechende Suche oder Anfrage vom PC1 an den Laptop würde also entsprechend umgewandelt werden, so dass nur IPs benutzt werden. Dieser Vorgang verläuft im Hintergrund, als Benutzer bekommst du davon nichts mit.

1.3 ARP

Das **Address Resolution Protocol** (ARP) löst IP-Adressen in MAC-Adressen auf, damit Rechner miteinander kommunizieren können. Dies stellt die zweite Stufe der Adressauflösung dar. Die Rechner wandeln die IP-Adressen (z.B. 192.168.0.1) in MAC-Adressen um (z.B. 00-10-B5-03-82-23). Dabei wird vorher vom Rechner angefragt, wie die MAC-Adressen der anderen Geräte im Netzwerk lauten. Hat er die benötigten Daten, legt er ebenfalls eine Tabelle mit diesen Daten an, und kann Anfragen nacheinander in IP- und MAC-Adressen übersetzen.

1.4 WAN, LAN und WLAN

Netzwerke werden in ihrer topografischen Ausdehnung kategorisiert.

Eine **Wide Area Network** (WAN) umschreibt ein großräumiges, auch globales Netzwerk, das entsprechende Dienste und Möglichkeiten vielen Benutzern zur Verfügung stellt. Ein **Local Area Network** (LAN) hingegen ist ein räumlich stark begrenztes Netzwerk, wie es zum Beispiel in einem Firmengebäude oder einer Wohnung vorhanden ist. Es kann also direkt einem Ort zugeordnet werden. Die Zwischenstufe **Metropolitan Area Network** (MAN) umschreibt Netze in städtischer Größenordnung, sie fassen also bestimmte größere Gebiete zusammen. Das Stadtmodell würde also für die beiden Straßen ein LAN symbolisieren, Pakete die mit der Post (Gateway) versandt werden, gehören dann zum WAN.

Ein **WLAN** ist daher das Selbe wie ein LAN, nur werden hier keine Kabel, sondern Funkwellen zur Erzeugung des Netzwerks benutzt. Im Sprachgebrauch

wird unter LAN ein **wired** LAN, also kabelgebundenes Netzwerk bezeichnet, WLAN (*wireless* LAN) immer als Funknetzwerk. Sauberer wäre jedoch die Bezeichnung als wired LAN über Kupferkabel, und wireless LAN (es gibt auch wired LAN über Glasfaser: LWL, Lichtwellenleiter). Aufgrund der Funkwellen ist die Bandbreite aber deutlich geringer, entsprechend schnelle Funknetze die an ein Kabel rankommen gibt es derzeit nicht. Kabelgebundene Netzwerke werden über **Switches** und **Hubs** erweitert, bei Funknetzen geschieht dies über sogenannte **Repeater**. Alle drei Geräte greifen das Signal auf, und verstärken es. Damit ist es möglich die Netzwerke deutlich zu vergrößern. Die Kabellänge im wired LAN (Kupfer) wird mit 100 m zwischen zwei Verstärkern angegeben, in einem WLAN sind maximal 100 m (Freifläche) genehmigt. In Räumen kann die Ausbreitung durch Wände und Störquellen aber auch auf 15 m reduziert werden, hier machen Repeater durchaus Sinn. Wird in Gebäuden nur an bestimmten Orten ein WLAN benötigt, ist die Erweiterung über Kabel kein Problem, zwischen zwei **Access Points** (WLAN Basisstation) können Kabel gezogen werden (Kostensparnis).

Die Reichweitenerhöhung mit reinen Funklösungen geschieht im Regelfall über **WDS** (Wireless Distribution System), allerdings ist dort häufig nur WEP als Verschlüsselung möglich. Von daher bieten sich die bereits erwähnten Erweiterungen über Kabel (Kupfer oder Stromnetz) mit Kanaladaptation wie im *Bild 3* gezeigt. Die Funknetze haben dabei wegen starker Dämpfung nur eine sehr geringe Ausdehnung, z.B. 15 m.

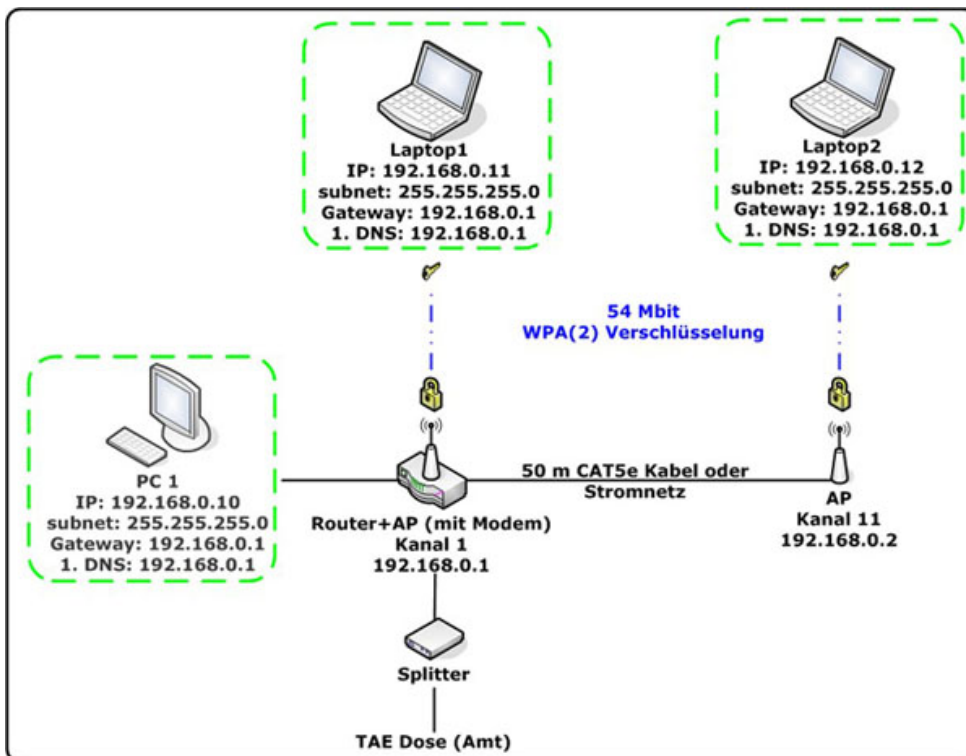


Bild 3: Ungleichmäßige WLAN Ausdehnung

Eine Restriktion des Netzwerks ist seine **Bandbreite**. Je mehr Benutzer auf ein Netzwerk treffen, desto geringer wird die Bandbreite für den Einzelnen. Am Einfachsten wird das zwischen WAN und LAN klar. Daheim kann man 100 MBit, oder vielleicht sogar 1 GBit/s übertragen, also rund 10 bis 125 MB/s. Die Anzahl der Benutzer ist sehr klein, anteilig würden 3 Benutzer also grob gesagt jeweils 33 MBit/s von 100 bekommen. Im WAN, also Internet treten deutlich mehr Benutzer auf, die sich ebenfalls eine Bandbreite wie 1 GBit/s teilen müssen, da der Server (z.B. eine Webseite) nicht schneller angebundnen ist. Greifen jetzt 1.000 Benutzer in etwa zeitgleich auf diesen Server zu, wird die Bandbreite entsprechend geteilt. Dem einzelnen Benutzer werden jetzt nur noch 0,125 MB/s, oder 128 kByte/s zugeteilt, was in etwa DSL1000 entspricht. Um solche Dienste also anbieten zu können, werden die DSL Geschwindigkeiten im Vorfeld gedrosselt. Das Netz wird dann „fair“ verteilt. Weitere Einschränkungen ergeben sich aus der **Leitungslänge** (Wellenwiderstand und Dämpfung), sowie der **Bandbreite am DSL-Knoten**, die hier aber nicht näher beschrieben werden.

1.5 Host und Client

Als **Host** werden Rechner und Geräte bezeichnet, die für andere Dienste bereitstellen. **Clients** hingegen können solche Dienste nicht bereitstellen, sondern greifen auf die Ressourcen und Dienste eines Hosts zu. In unserem Netzwerkbeispiel agieren Rechner sowohl als Client und Host, der Router ist immer nur Host.

Laptop und PC1 sind aus der Sicht des Routers Clients, sie greifen auf seinen Dienst zur Freigabe und Weiterleitung des Internets zu. Beherrscht der Router weitere Dienste wie FTP, Drucker, oder sogar die Verwaltung einer Netzwerkfestplatte (NAS, Network Attached Storage), können die Clients diese Dienste ebenfalls benutzen.

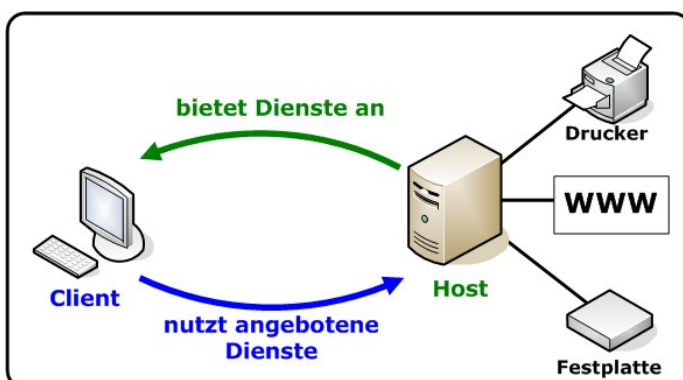


Bild 4: Host und Client Prinzip

PC1 arbeitet hier ebenfalls als Host, er verwaltet nämlich einen Drucker über USB, den er als Netzwerkdrucker dem Netzwerk zur Verfügung stellt. Der Laptop kann also als Client auf den PC mit seinem Druckerserver zugreifen, nimmt den Dienst zum Drucken in Anspruch.

1.6 Gateway


Ein **Gateway** ermöglicht es unterschiedlichen Netzwerken miteinander zu kommunizieren. Diese Aufgabe übernimmt der Router, der das LAN und WAN ansteuert, und entsprechende Pakete verwaltet (im Stadtmodell die Post). Der Router fängt die gesendeten und empfangenen Pakete ab, und ändert ihre Quelle und ihr Ziel so ab, das sie jeweils in beiden Netzwerken funktionieren. Dieses **Remapping** wird ebenfalls im Hintergrund ausgeführt, als Benutzer musst du dich nicht darum kümmern.

2 Rechner einrichten

2.1 Netzwerk mit Router und Internet

Alle gängigen Router besitzen einen **DHCP-Server**, vergeben also die IPs selbständig an die angeschlossenen Rechner. Da im alltäglichen Betrieb aber durchaus weitere Einstellungen nötig werden, empfiehlt es sich **feste IPs** zu vergeben (Ausnahme: Routerhersteller schreibt explizit DHCP vor). Feste IPs besitzen zudem den Vorteil einer eindeutigen Zuordnung von PCs zu entsprechenden Nutzern und Räumen. Damit die IP korrekt für das Netzwerk vergeben wird, benötigst du die IP des Routers. Die **IP des Routers** findest du im **Handbuch**, oder auf der **Unterseite** des Gerätes.

Um die IPs für die PCs im Netzwerk zu vergeben, gehst du in die *Systemsteuerung*, und klickst dort auf *Netzwerkverbindungen*. In dem sich jetzt öffnenden Menü wählst du die entsprechende *Netzwerkverbindung* wie im *Bild 5: Netzwerkumgebung* gezeigt.

 *Tip: Arbeitest du öfters mit Netzwerken, kannst du das Menü Netzwerkumgebung auch in das Startmenü integrieren (Rechtsklick Taskleiste -> Eigenschaften -> Startmenü -> Anpassen -> Erweitert).*

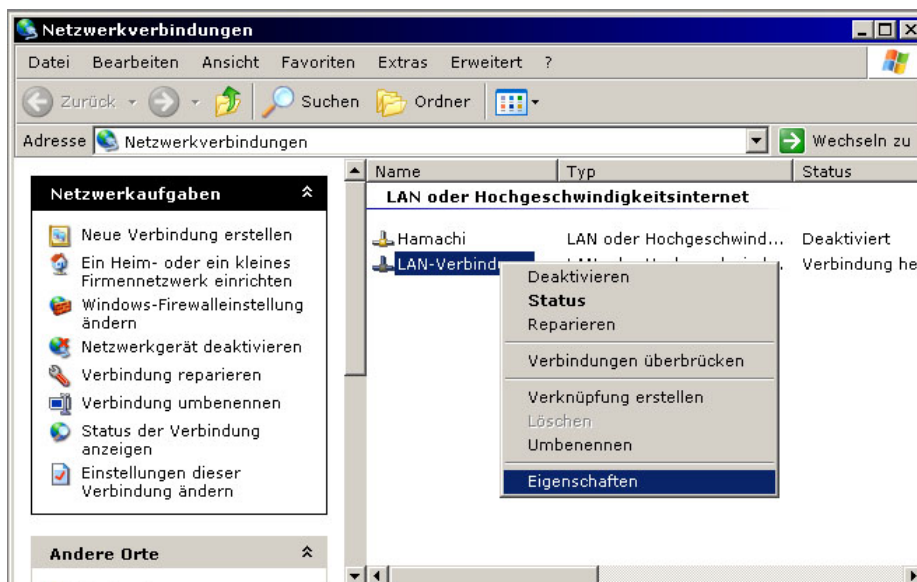


Bild 5: Netzwerkumgebung

2 Rechner einrichten

In den Eigenschaften der Netzwerkverbindung klickst du doppelt auf *Internetprotokoll (TCP/IP)*, und vergibst manuell die passenden IPs für den Rechner. Beispielhaft ist das im *Bild 7: TCP/IP der Netzwerkkarte* aufgezeigt.

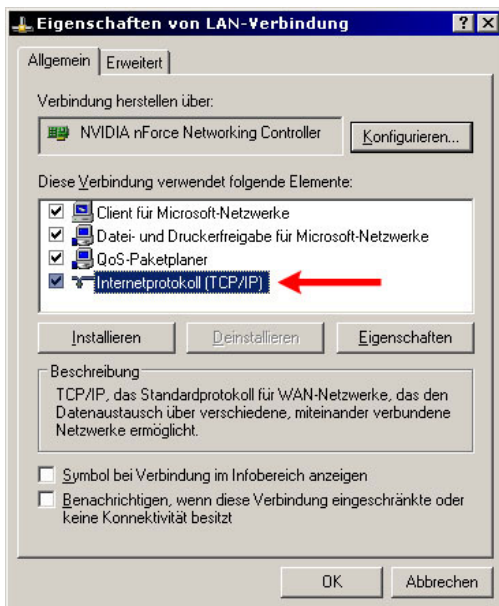


Bild 6: Eigenschaften der Netzwerkkarte



Hinweis: Die IP Bereiche müssen angeglichen werden, benutzt dein Router den Bereich 192.168.2.x statt der hier gezeigten 192.168.0.x, musst du die IPs auch so angepasst eingeben.

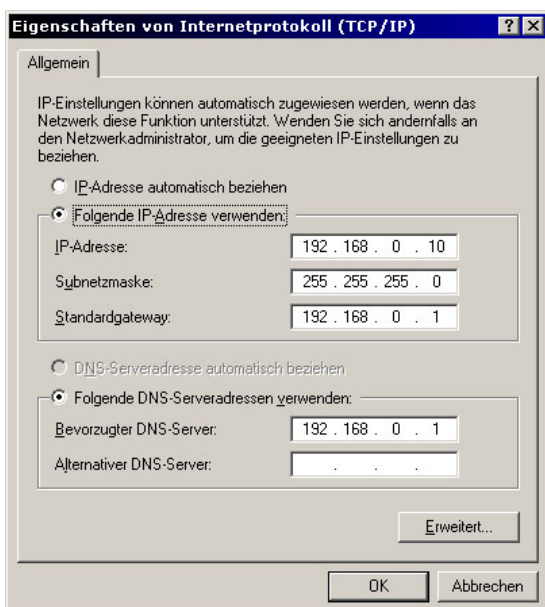


Bild 7: TCP/IP der Netzwerkkarte

Nach dieser Einstellung ist die Einrichtung der Netzwerkkarte vorerst abgeschlossen. Erweiterte Einstellungen für ein WLAN werden später aufgezeigt, nachdem der Router für WLAN konfiguriert wurde. Da in einem Netzwerk kein Rechner eine Internetverbindung herstellt, schaltest du im *Internet Explorer* unter *Extras* -> *Internetoptionen* -> *Verbindung* jegliche Verbindungen ab, wie im *Bild 8* gezeigt.

2 Rechner einrichten

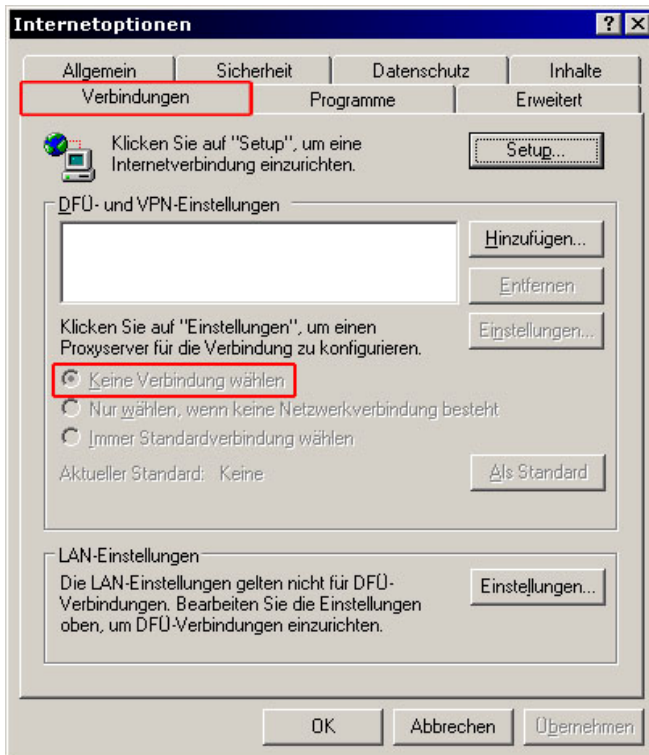


Bild 8: Internet Explorer Verbindungen

Jetzt überprüfst du mit Windows-Bordmitteln, ob das Netzwerk bereits funktionstüchtig ist. Dafür öffnest du das Startmenü, gibst bei Ausführen `cmd` ein, und klickst **OK** (oder **Enter**-Taste). In der sich jetzt öffnenden *Kommandozeile* führst du die beiden gezeigten Befehle aus. Sind die IP-Adressen korrekt vergeben, und funktioniert der Ping, dann ist der Router erreichbar. Im 3. Abschnitt wird nun der Router eingerichtet.

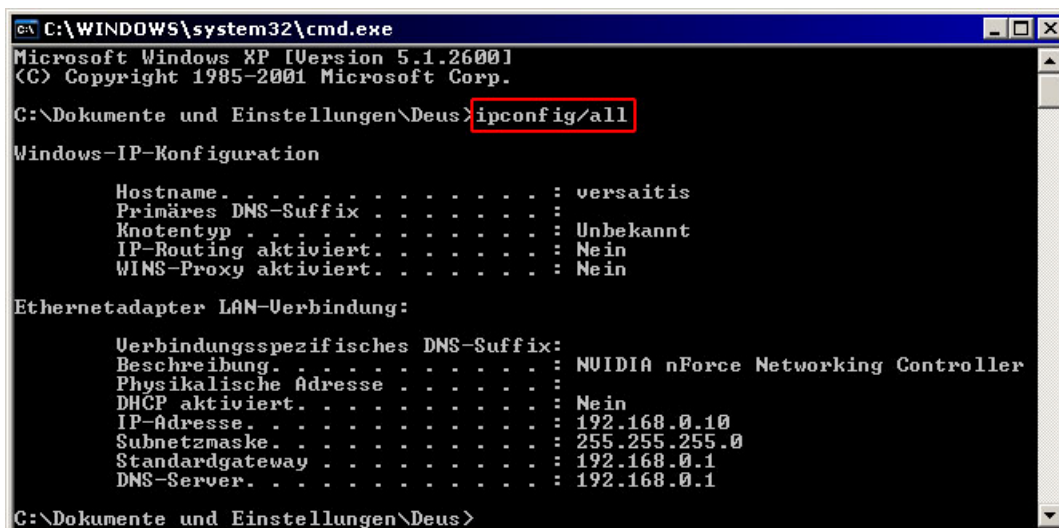


Bild 9: Eingabeaufforderung (1)

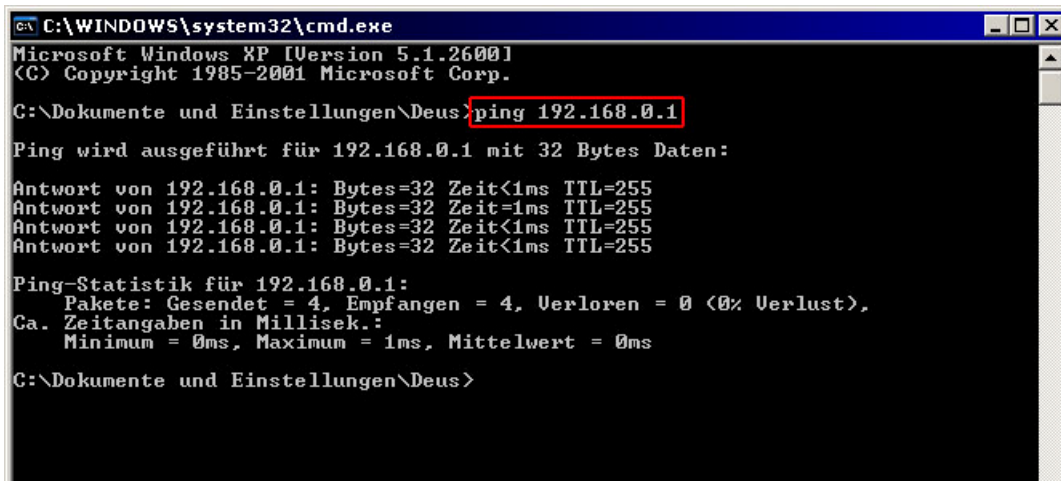


Bild 10: Eingabeaufforderung (2)

2.2 Netzwerk ohne Router oder Internet

Willst du nur zwei Rechner verbinden um einen Datenaustausch vorzunehmen, oder eine Netzwerkparty veranstalten, entfällt die Routerkonfiguration vollständig. Dann ist es nur notwendig die entsprechenden IPs an den Rechnern zu vergeben. In einem solchen Falle ist es zwingend notwendig feste IPs zu vergeben, da es keinen DHCP-Server gibt der IPs zuordnen könnte.

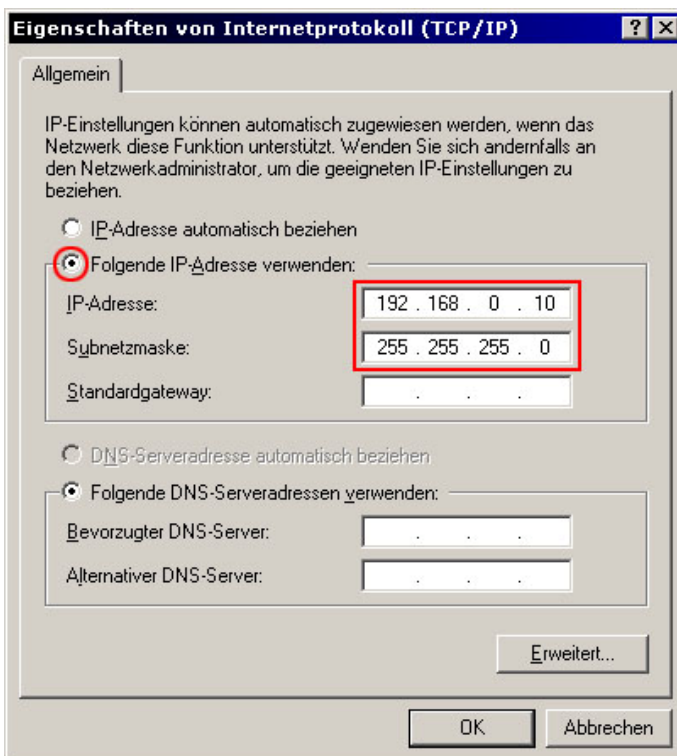


Bild 11: TCP/IP ohne Router

Die IPs werden wie gezeigt ebenfalls einmalig vergeben, es fallen *Standardgateway* und *DNS-Server* weg. Der PC mit dem du dich verbinden möchtest, hat dann beispielsweise die IP 192.168.0.11.

Die Überprüfung in der *Kommandozeile* wird dann mit den entsprechenden IPs im Netzwerk ausgeführt.

2.3 Windows Vista einrichten

Mit der Einführung von Windows Vista im Jahr 2007 ändern sich auch einige Menüs. Daher wird dir hier gezeigt, wie du dich in Vista zu den entsprechenden Menüs durchklickst, und welche Einstellungen es dort gibt.

IPs vergeben

Die Netzwerkumgebung wurde unter Vista in *Netzwerk- und Freigabecenter* umgetauft. Über dieses Menü sind jetzt diverse Änderungen möglich. Um in das Netzwerkcenter zu gelangen, gibt es folgende Möglichkeiten:

- Rechts unten in der *Systray* einen Klick oder Rechtsklick auf das Netzwerksymbol, dort *Netzwerk- und Freigabecenter* wählen.
- Wenn schon im Startmenü verfügbar, dort Rechtsklick auf *Netzwerke*, und ebenfalls das Center auswählen.
- Bist du im Netzwerk-Menü, dann gibt es oben in der dynamischen Leiste den entsprechenden Eintrag



Bild 12: Button für das Center

- In der Systemsteuerung findet sich ebenfalls ein Punkt für das Netzwerkcenter

In dem sich jetzt öffnenden Fenster findest du oben eine Anzeige des derzeitigen Netzes, darunter finden sich die Optionen zur Konfiguration deines PCs. Klicke dort im mittleren Bereich *Netzwerk* auf *Status anzeigen*.

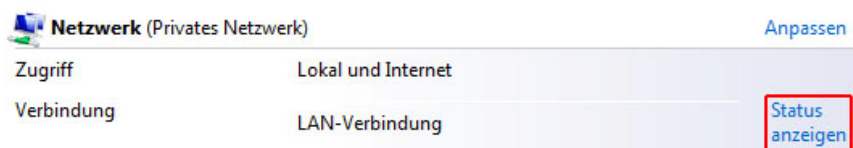


Bild 13: Status der Verbindung im Center

Das nächste Fenster ähnelt schon mehr den bekannten Bereichen aus Windows XP, hier wählst du im unteren Bereich *Eigenschaften* aus. Da diese Änderung eine administrative Änderung ist, erscheint der gewohnte *UAC*-Dialog, der dich nach den Administratorrechten fragt.

2 Rechner einrichten

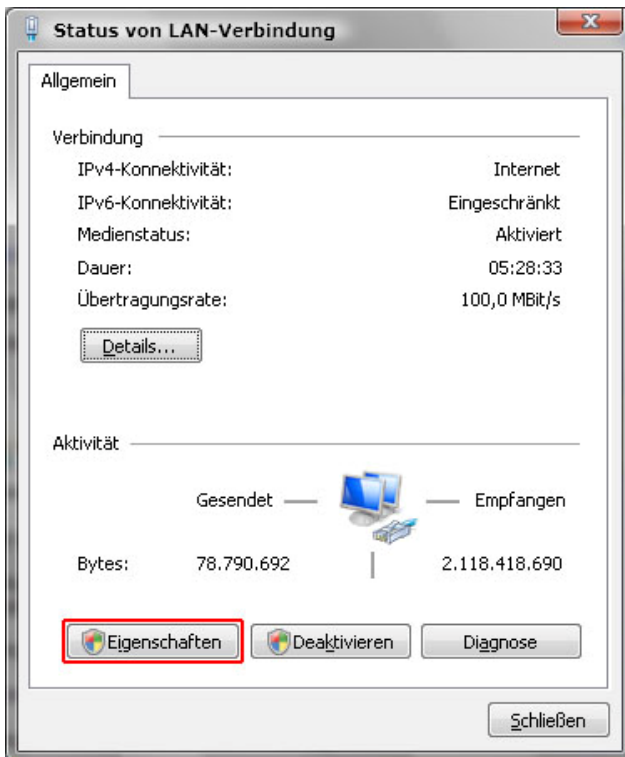


Bild 14: Status der LAN-Verbindung (Vista)

Jetzt sieht es wieder sehr bekannt aus, ähnliche Menüs findest du ebenfalls im XP. Neu ist die direkte Vorbereitung für IPv6. Zurzeit wählst du aber noch *IPv4* aus, und gehst in dieses Menü über einen Doppelklick, oder den Button *Eigenschaften*. Die Vergabe der IP ist identisch mit der weiter oben gezeigten Methode.

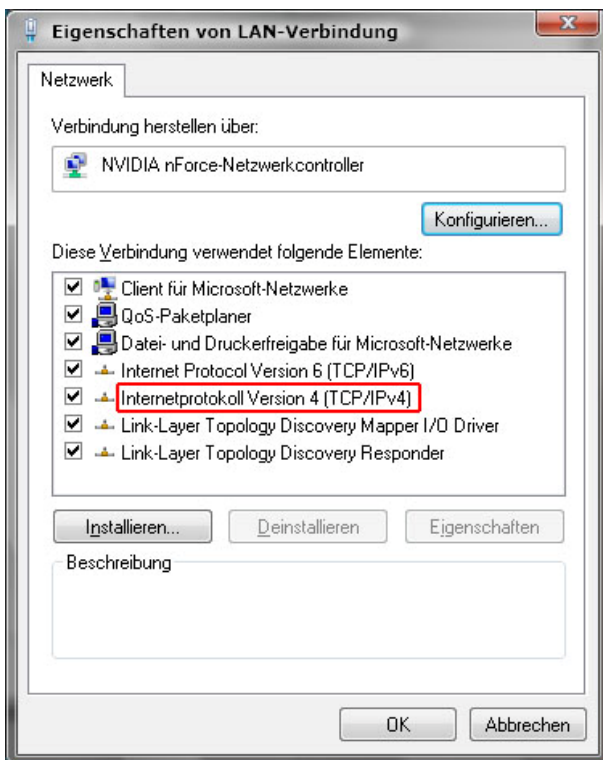


Bild 15: Eigenschaften der LAN-Verbindung (Vista)

Öffentliche und private Netze

In Windows Vista wurde eine Separierung der Netzwerktypen vorgenommen. Damit eine höhere Sicherheit gegeben ist, wurden die Netzwerke in **öffentliche** und **private** Netzwerke unterteilt, die unterschiedliche Eigenschaften bzgl. Freigaben und Rechten haben.

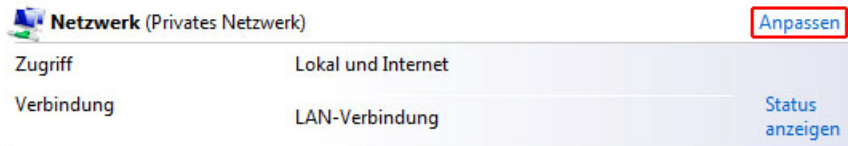


Bild 16: Netzwerktyp anpassen

Ist der *Standorttyp* auf *Öffentlich* gesetzt, können keine Freigaben getätigt werden, und zudem findet der Rechner keine anderen Clients im Netzwerk. Für andere Rechner ist der Vista-PC dann ebenfalls unsichtbar.

Erst wenn der Typ auf *Privat* gesetzt wurde, sind Freigaben und das Zusammenarbeiten mit anderen PCs im Netzwerk uneingeschränkt möglich. Eine Überbrückung dieser Restriktion ist möglich, muss aber gesondert eingestellt werden. Für Heimnetzwerke die den Datenaustausch bewusst benutzen, ist die Einstellung Privat völlig okay.

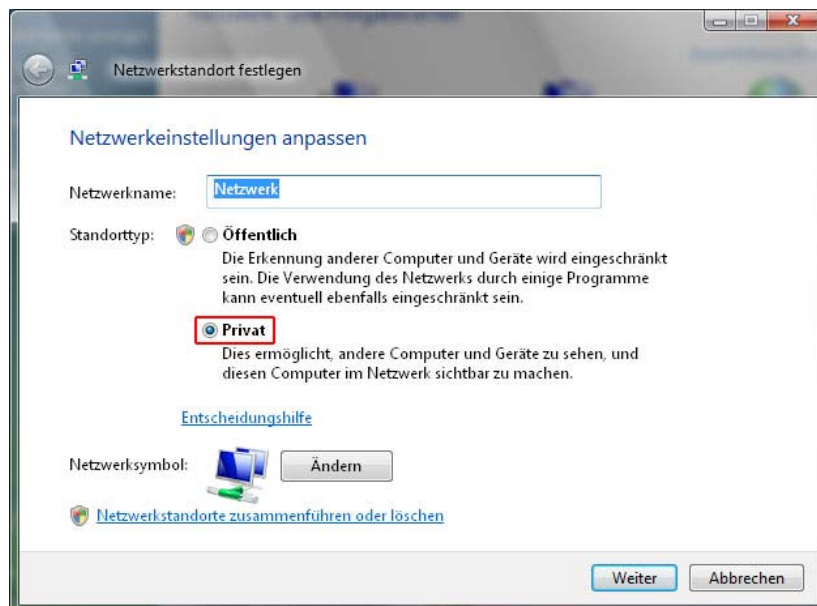


Bild 17: Netzwerkstandort festlegen

Der *Netzwerkname* ist die Bezeichnung des hiesigen Netzwerkes, benötigst du Freigaben die auf älteren Betriebssystemen liegen, musst du erst die *Arbeitsgruppe* im Untermenü *Netzwerkerkennung* ändern. Die *Arbeitsgruppe* muss dann mit der des älteren Betriebssystems übereinstimmen.



Hinweis: Die Änderung der Arbeitsgruppe hat immer noch einen Neustart des Rechners zur Folge.

3 Router und WLAN einrichten

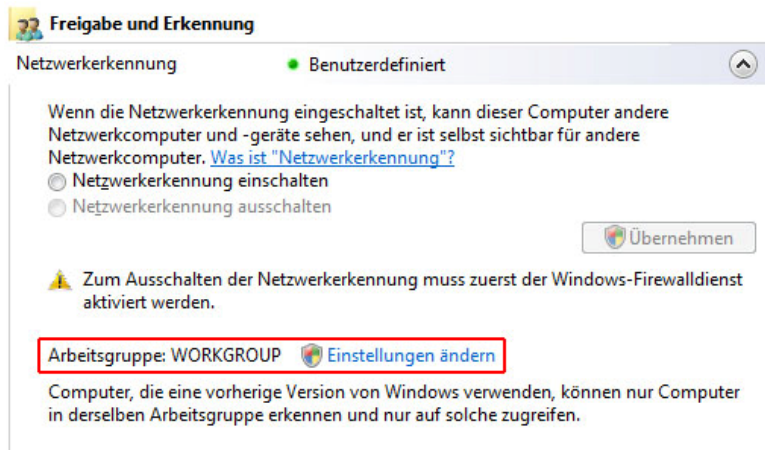


Bild 18: Netzwerkerkennung

Netzwerkübersicht

Sind in einem Netzwerk mehrere Vista-PCs verfügbar, dann bietet Windows Vista die Möglichkeit einer Netzwerkübersicht. Diese Übersicht listet alle verfügbaren PCs auf, und zeigt sie in einem übersichtlichen Schema mit Knotenpunkten an. Diese Übersicht erreichst du im *Netzwerkcenter* über den Link *Gesamtübersicht anzeigen*.

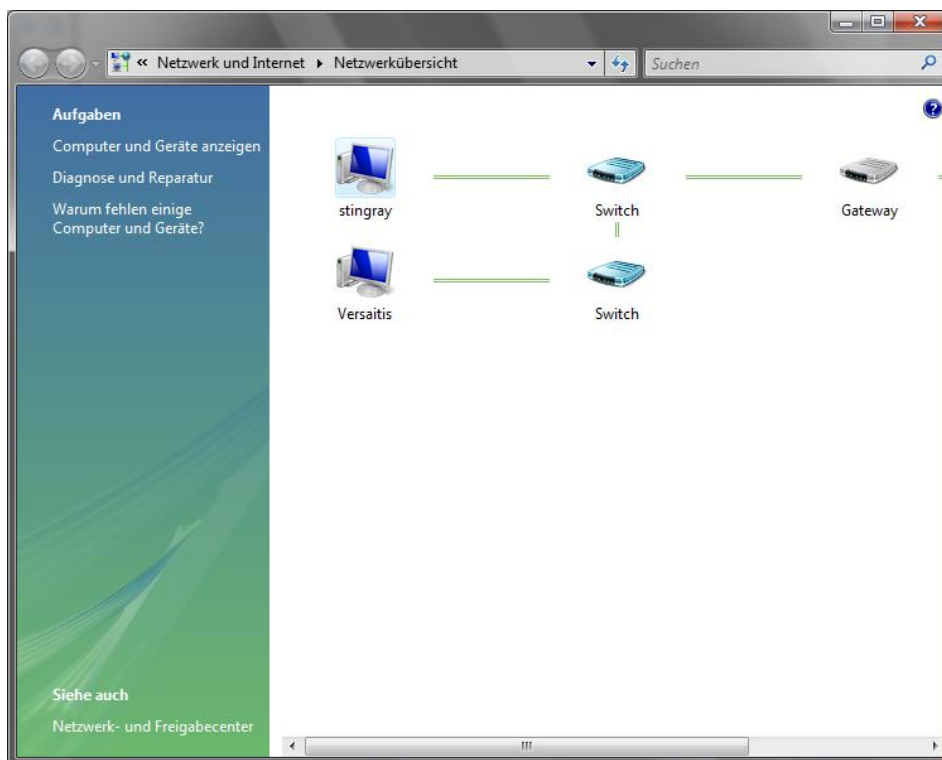


Bild 19: Netzwerkübersicht

3 Router und WLAN einrichten

Der Router agiert in diesem Netzwerk als Gateway, und verteilt somit das Internet auf alle PCs die online dürfen oder möchten. Damit der Router sich am DSL-Netzwerk anmelden kann, benötigt er die **ISP-Daten** (Internet Service Provider). Diese und weitere Einstellungen die im Alltag notwendig sind, werden nun erklärt.

Um das Konfigurationsmenü aufzurufen, gibst du im Regelfall die IP des Routers im *Internet Explorer* an. Benutzer und Passwort für die Routerkonfiguration sollten sich in der Anleitung des Gerätes finden lassen.

3.1 DHCP

Da du im Netzwerk feste IPs benutzt, benötigst du den DHCP-Server des Routers nicht mehr. Router besitzen dafür entweder ein eigenes Menü wie in *Bild 20* gezeigt, oder in einem Punkt in einem Menü wie LAN.

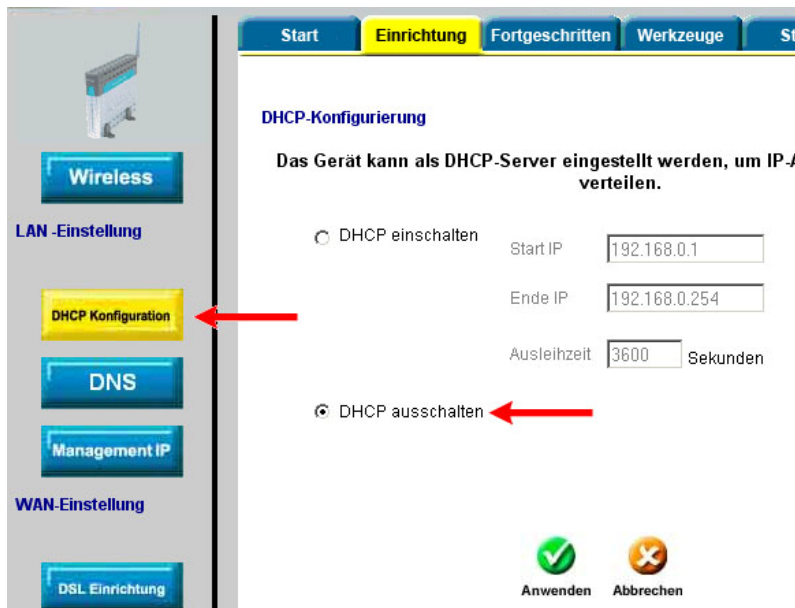


Bild 20: DHCP im Router

Sobald der DHCP deaktiviert ist, werden keine IPs mehr im Netzwerk vergeben. Rechner die also bisher darauf zurückgegriffen haben, können jetzt nicht mehr im Netzwerk agieren. Diese müssen also auch mit einer festen IP konfiguriert werden. Die DHCP Konfiguration im Router benötigt keine weiteren Einstellungen.

3.2 WAN

Im *WAN-* oder *Verbindungs*menü gibst du die **DSL-Daten** deines Providers ein, damit der Router eine Verbindung zum Internet herstellen kann. Für Deutschland wählst du hier *PPPoE*, und gibst dann deinen *Benutzernamen* und das *Passwort* ein, welches du von deinem Provider bekommen hast. Hast du einen der wenigen Anschlüsse mit einer festen IP bekommen, musst du von einer **dynamischen** auf eine **statische** IP wechseln. Der Regelfall sind jedoch **dynamische** IP-Vergaben mit einer Gültigkeit von 24 Stunden.

Der *MTU-Wert* bestimmt die maximale Paketgröße, die über die Verbindung gesendet werden darf. Dieser Wert ist vom Provider abhängig, und wird nach dem Erstellen der Verbindung mit der *MTU.zip* (in der Infothek zu finden) herausgefunden. AOL schreib hier einen MTU Wert von **1400** vor, bekommst du also keine Verbindung aufgrund des MTUs, kannst du auch pauschale 1400

versuchen. Kleinere MTU Werte als sie der Provider vorschreibt erzeugen im Regelfall keinerlei Probleme, **bis 1300** sind keine Änderungen feststellbar.

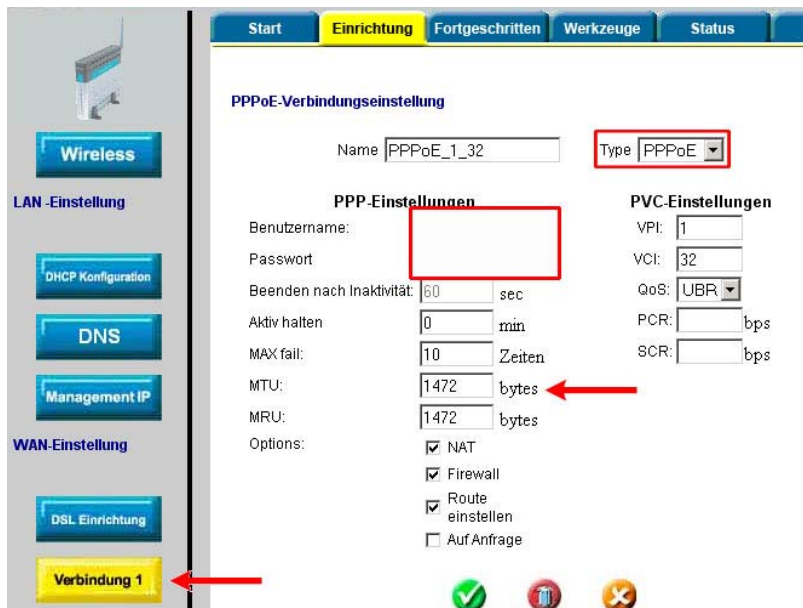


Bild 21: DSL Verbindungsdaten

i *Tip: Ein zu großer MTU Wert macht sich häufig durch nicht vollständig, oder gar nicht ladende Seiten wie Ebay bemerkbar.*

Die Zeitangabe bei *Aktiv halten* (manchmal auch *Idle Time*) umschreibt, wie lange der Router bei Inaktivität die Verbindung hält. Stellst du dort **30 min** ein, wird nach 30 min ohne Verkehr die Verbindung beendet. Die Eingabe **0** hält den Router im Regelfall permanent online, was bei DSL ohne Zeitbindung das Sinnvollste ist. Der Haken bei *Auf Anfrage* weist den Router an, bei einer Anfrage von einem PC die Verbindung aufzubauen, sich also zu verbinden.

Wenn der Router permanent online ist, spielt diese Einstellung keine größere Rolle.

3.3 WLAN einrichten und absichern

Routereinstellungen

Die Einrichtung des WLAN beginnt mit dem Router. Einige Router bieten ab Werk eine verschlüsselte WLAN-Verbindung, einrichten solltest du das WLAN aber immer mit einem Kabel am Router.

In einem entsprechenden Menü gibst du eine gewünschte *SSID* ein, und stellst danach die *WPA*, oder *WPA2 Verschlüsselung* ein. Die *SSID* ist der Name des Netzwerkes, kann also beliebig vergeben werden. *WEP* sollte **nicht** mehr verwendet werden, da es als unsicher gilt. *WPA(2)* bietet deutlich besseren Schutz, der mit entsprechenden Passwörtern sehr schwer zu knacken ist. Als Methode bietet sich in kleinen Heimnetzwerken *PSK* (Pre-shared Key) an. *PSK* bietet dir die Eingabe eines Strings, also einer Zeichenfolge an. Dieses

Passwort sollte **mindestens 10 besser 15 bis 20 Stellen** besitzen, und **hart** sein. Harte Passwörter sind solche wie P5mn98qw091v8f45 (mit der Veröffentlichung nicht mehr zu benutzen), Weiche hingegen alle die man im Duden oder beim Benutzer finden kann. Der Name des Hundes ist also eher ungeeignet. Das Knacken eines solchen Passworts dauert seine Zeit, wer es noch sicherer haben will wechselt alle 2 Wochen das Passwort.

Die Daten zu SSID und dem Passwort solltest du auf einem Zettel stehen haben, den du z.B. unter den Router legst. Für die Einrichtung der anderen PCs sind diese Daten ebenfalls notwendig, alle PCs die sich an deinem Router anmelden wollen, müssen diese Daten kennen.

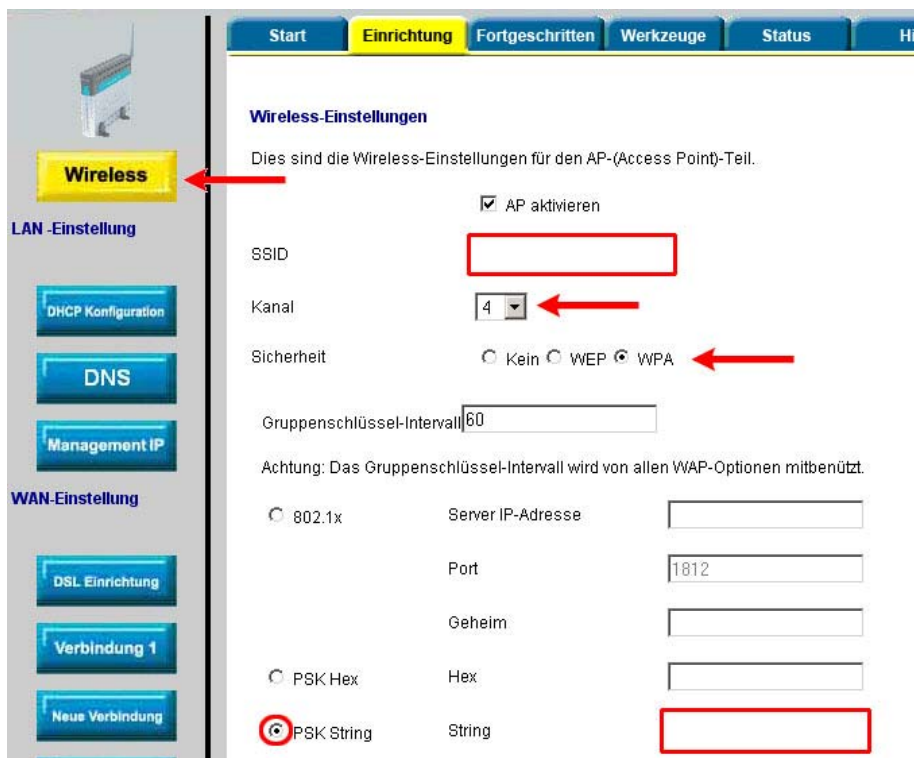


Bild 22: Access Point aktivieren

Der *Kanal* ist ein eingeschränkter Bereich im 2,4 GHz Funknetz.

In Deutschland sind 13 Kanäle möglich, die sich aber überlagern. Gibt es in deiner Umgebung mehrere Funknetze die sich überschneiden und gegenseitig stören, solltest du einen störungsärmeren Kanal wählen. Günstige Kombinationen von Kanälen sind z.B. **1 - 6 - 11** oder **2 - 7 - 13**.

Kanäle haben eine gewisse Breite im Funknetz, und mit diesen Kombinationen kannst du nahezu ausschließen, dass sich benachbarte Kanäle treffen.

Rechnereinstellungen

Wie bereits erwähnt wurde, benötigen alle Rechner die Daten des WLANs, um sich damit verbinden zu können. Die Dateneingabe kann entweder über eine *Windows-Maske*, oder ein *spezielles Programm* zum WLAN Stick oder der Karte erfolgen. Exemplarisch wird hier die Einrichtung über *Windows* erklärt.

3 Router und WLAN einrichten

! *Hinweis: Benutzt du eine Software des Herstellers, ist es sinnvoll in der Dienstverwaltung die Konfigurationsfreie drahtlose Verbindung zu beenden, und zu deaktivieren.*

Gehe in die *Eigenschaften* der *Netzwerkumgebung*, und wähle dort die *drahtlose Verbindung* aus, die dir angezeigt wird. Über *Rechtsklick* -> *Eigenschaften* öffnest du die *Konfiguration* der Verbindung.

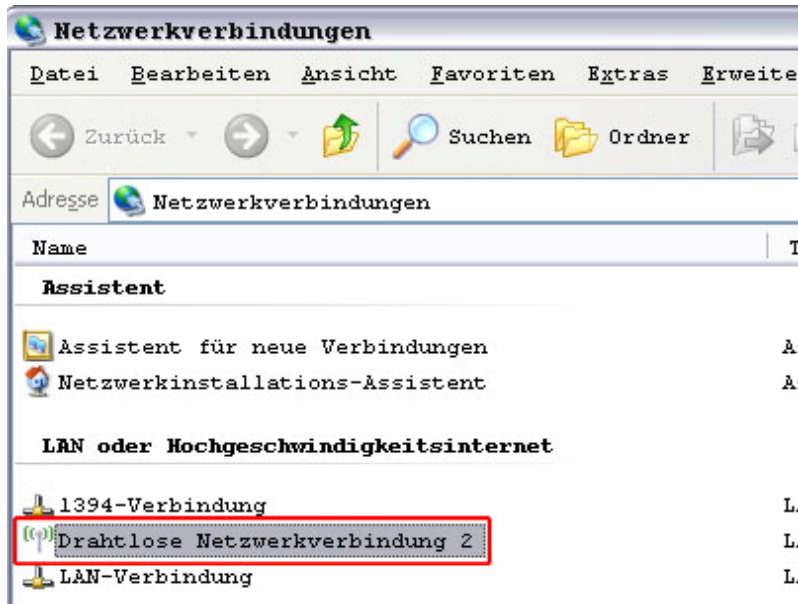


Bild 23: Netzwerkeigenschaften des WLAN

Hier wählst du den Reiter *Drahtlosnetzwerke*, überprüfst ob Windows die Konfiguration verwaltet, und legst unten ein neues Netzwerk mit *Hinzufügen* an.

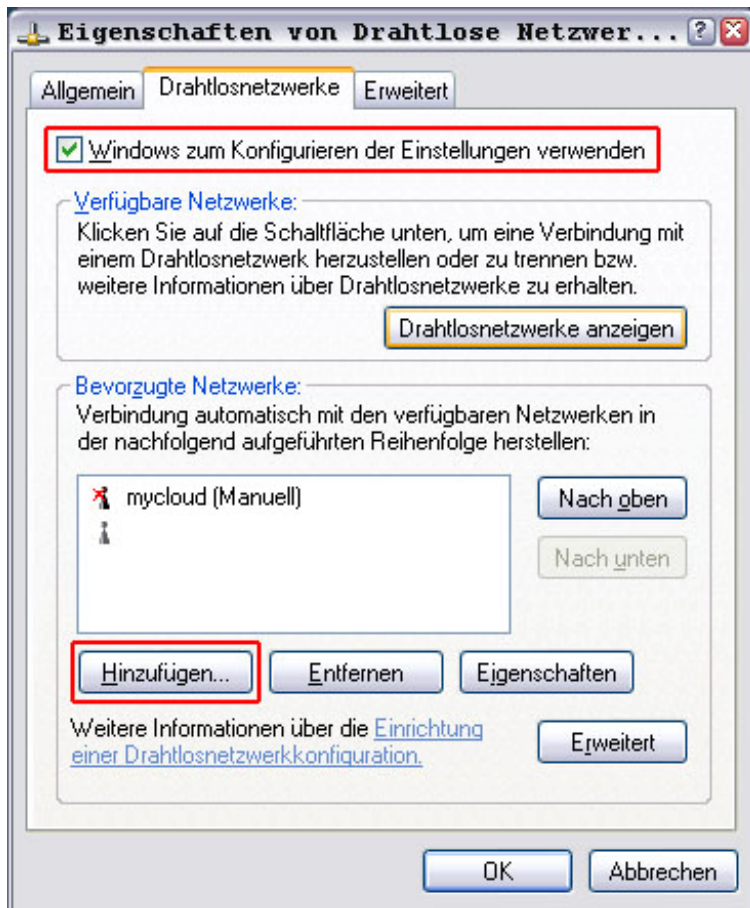


Bild 24: Anlegen des Netzwerkes

In dem sich jetzt öffnenden Fenster kannst du die Verschlüsselungsdaten vom WLAN eingeben. Für die oben gezeigte Einstellung, benutzt du die Einstellung wie im *Bild 25* gezeigt. *SSID* und *Passwort* stehen ja auf deinem Zettel. Unterstützt dein Netzwerk *AES* (Advanced Encryption Standard), und nicht nur *TKIP* (Temporal Key Integrity Protocol), solltest du dieses verwenden, da es einen besseren Schutz gegen Auslesen besitzt.

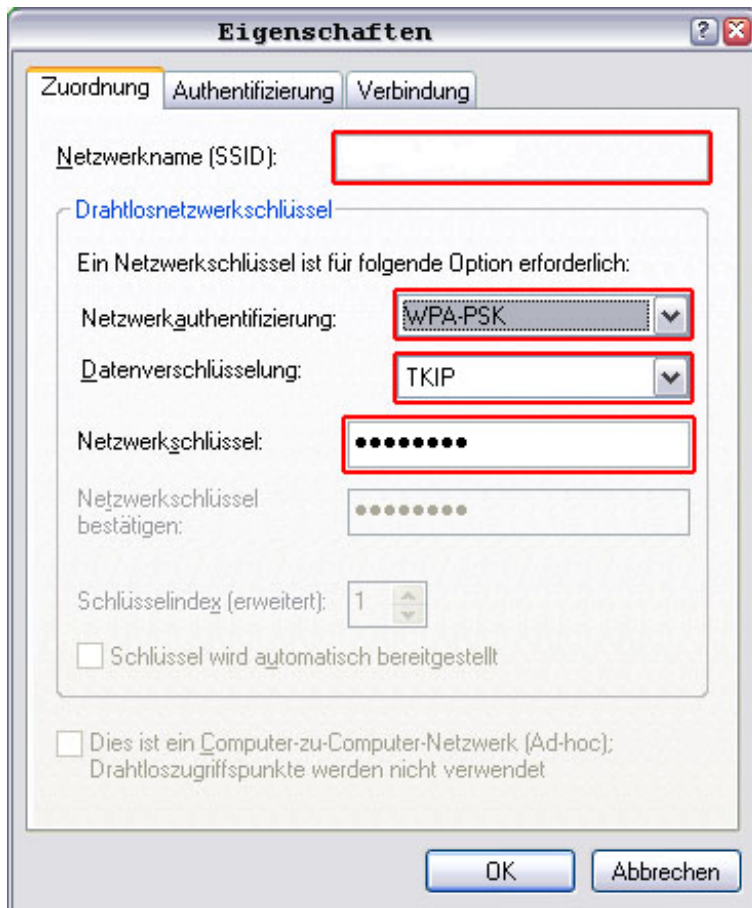


Bild 25: WLAN



Tip: Willst du mehr über die Verschlüsselungen wissen, kannst du bei Level1 eine PowerPoint Präsentation laden.

http://ftp.level1.com/levelone_de/events/Sicherheit_im_WLAN.ppt

3.4 Sonstige Einstellungen

Router beherrschen viele Funktionen, die aber im Einzelfall auch hinderlich oder gefährlich sein können. Einstellungen die gesetzt werden sollten, um den täglichen Betrieb sicherer zu gestalten werden in diesem Abschnitt näher behandelt.

MAC-Filter

MAC-Filter sind eine Erweiterung von Sicherheitseinstellungen, die für den Einzelfall durchaus noch sinnvoll sind. *Noch* daher, da MAC-Adressen prinzipiell zu fälschen sind. Möchte man aber bestimmten Rechner oder Benutzern wie Kindern den Zugang zum Internet verwehren, und haben diese ebenfalls ein eingeschränktes Benutzerkonto, ist es sinnvoll diesen zu nutzen.

MAC Adressen sind globale eindeutige Kennungen von Netzwerkadaptern, die eine Karte zweifelsfrei identifizieren sollen. Dementsprechend greift der MAC Filter nur auf eine Netzwerkkarte.

3 Router und WLAN einrichten

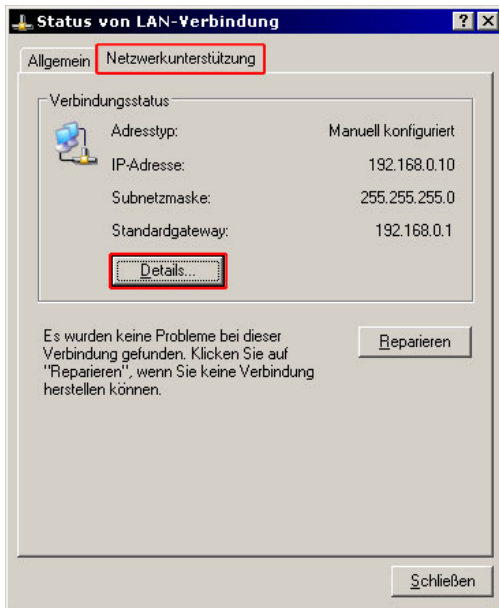


Bild 26: Status der LAN-Verbindung

In den *Eigenschaften* der *Netzwerkumgebung* gehst du per Doppelklick auf die gewünschte Verbindung in das Informationsmenü der Verbindung. Dort wählst du den Reiter *Netzwerkunterstützung*, und dann *Details*.



Bild 27: Details der LAN-Verbindung

Die MAC-Adresse wird auch **physikalische Adresse** genannt, der entsprechende Wert in der zweiten Spalte wird übernommen und im Router hinterlegt.

Wireless Management



Bild 28: MAC-Filter

Bietet der Router eine entsprechende MAC-Liste nur für WLAN an, kannst du kabelgebundenen PCs leider keine Restriktion über die MAC vorschreiben. Du kannst entscheiden ob MAC-Adressen die eingetragen entweder einen Zugang erhalten, oder diesen verwehrt bekommen. Bei einer übersichtlichen Menge an PCs die ins Netz dürfen, ist es günstiger die erlaubten MACs zu definieren. Sollen dagegen in einem größeren Netzwerk nur bestimmte Teilgruppen wie Kinder ausgeschlossen werden, kann es günstiger sein diesen den Zugang zu untersagen.

Universeller Plug`n`Play

UPnP ist ein Dienst, der **automatisch** Ports öffnen kann. Sofern der Dienst in Windows XP ebenfalls aktiviert und eingerichtet ist, darf der Router angeforderte Ports öffnen, wenn sie der Rechner benötigt. Die Funktion hat den Vorteil, dass man sich um keine Portfreigaben kümmern muss, da Programme alle Ports bekommen die sie benötigen. Dieser Dienst kann aber genauso leicht von Schädlingen ausgenutzt werden, die eine Internetverbindung herstellen wollen um Inhalte nachzuladen.

UPnP

Um UPnP zu aktivieren, markieren Sie UpnP und wählen dann eine Verbindung

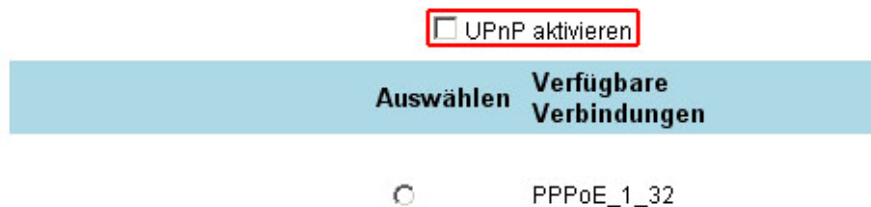


Bild 29: UPnP im Router

UPnP sollte also nicht aktiviert sein, und der Dienst **SSPD-Suchdienst** deaktiviert sein.

Einige Geräte die für den Netzwerkbetrieb gedacht sind, beispielsweise Kameras, beherrschen ebenfalls UPnP. Diese Geräte können bei aktiviertem UPnP ebenfalls Ports öffnen, und Daten nach draußen senden. Jeder der dann deine IP (Online IP, nicht die Klasse-C) hat, kann auf die Geräte zugreifen. Bei Kameras oder

Netzwerkfestplatten unter Umständen ein herbes Sicherheitsleck das unangenehm enden kann.

Erweiterte WLAN-Einstellungen

Der **Access Point** im Router bietet dir auch noch weitere Einstellungen für die Konfiguration an.

Die *verborgene SSID* bringt nur etwas, wenn keiner nach ihr sucht. Will man das Netzwerk finden, benötigt man mit normalen Mitteln entsprechend die Daten dazu. Besitzt man diese nicht, ist das Netzwerk weder sichtbar, noch erreichbar. Gegen gezielte Angriffe die über Suchsoftware laufen, hilft diese Methode aber eher weniger.

Die *Antennenleistung* ist ein sinnvoller Punkt. Je höher die Sendeleistung ist, desto größer wird die Ausdehnung des WLAN-Netzes. Drossle die Leistung am besten so weit, wie es für einen **stabilen** Betrieb möglich ist. Je kleiner die Ausdehnung des Netzes, desto näher müssen potenzielle Fremdsurfer an deinen Router heran. Bei einem Einfamilienhaus müssten sie dann z.B. auf dem Grundstück stehen, und das fällt definitiv auf.

Wireless-Leistung

Dies ist die Wireless-Leistungsfunktion für den AP (Access Point)-Teil

Strahl-Intervall	<input type="text" value="200"/>	(msec, Bereich:1~1000, Grundeinstellung:200)
DTIM:	<input type="text" value="2"/>	(Bereich:1~25,Grundeinstellung:2)
Verborgene SSID	<input type="checkbox"/> Aktiviert	
Antennensendeleistung	<input type="text" value="Full"/>	
Domäne	ETSI	
RTS-Schwelle	<input type="text" value="4096"/>	
Frag-Schwelle	<input type="text" value="4096"/>	
b/g-Modus	<input type="text" value="11g Only"/>	

Bild 30: Erweiterte WLAN-Einstellungen

Der *b/g-Modus* stellt eine Zugangskontrolle für Geräte unterschiedlicher Standards dar. Lässt du nur *g-Modus* Geräte zu, werden 54 MBit (oder 108/125, je nach Gerät) angestrebt, und Geräte eines älteren Standards nicht integriert. Ein *mixed Mode* erlaubt hingegen die Einbindung neuerer und älterer Adapter, wobei dann die geringere Geschwindigkeit gewählt wird.

Router-Dienste deaktivieren

Router bieten auch die Möglichkeit Ports und Dienste von außen zu gewährleisten. Dazu gehört unter anderem auch das **Remote Management**, also das Konfigurieren des Routers von außen. Die Punkte *Remote Web* und

Remote Telnet sollten also tunlichst gemieden werden, die Konfiguration des Routers vom heimischen Netz aus vollzogen werden.

Die *dmz* (demilitarized Zone) mappt im Regelfall allen ankommenden Verkehr erstmal auf eine gewählte IP. Die *dmz* hilft aber im Regelfall nicht, und öffnet eher Sicherheitslücken, als dass sie weiterhilft. Benötigt man Ports, sollten diese **nicht** über die *dmz* freigeschalten werden.

Einstellungen Erweiterte Sicherheit

Firewall und NAT Dienst aktivieren

Wählen Sie ihre WAN-Verbindung

DMZ aktivieren

Wählen Sie eine LAN IP-Adresse

Remote Web

IP-Adresse IP-Netzmaske

Remote Telnet

IP-Adresse IP-Netzmaske

Ankommende ICMP PING erlauben

Bild 31: Erweiterte Sicherheit im Router

Die *Unterdrückung des ankommenden Pings* ist sinnvoll, um anderen Leuten zu verschleiern, dass man existiert. Wird ein Ping auf eine nicht existierende IP gesandt, dann kommt eine **Zeitüberschreitung**, der Ping wird „fallen gelassen“. Kommt jedoch eine Antwort, dann ist das für entsprechende Leute oder Programme ein Anreiz die IP über den gesamten Portbereich auf Lücken zu scannen.



Tipp: Bist du dir nicht sicher ob dein Router Ports vernünftig schließt dann nutze die vielen Porttests die in der Infothek zu finden sind.