

# Grundlagen IP, NAT, UDP, TCP

Marcel Jess

mjess@informatik.tu-cottbus.de

**Abstract:** Dieses Dokument behandelt die grundlegenden Themen im Bereich der Computernetzwerke. Es gibt einen Überblick darüber, wie Computernetzwerke strukturiert sein können und im allgemeinen arbeiten. Dabei werden wichtige Begriffe und grundlegende Verfahren zu diesem Thema näher erläutert.

## 1 Einführung

Jeder der sich schon einmal mit Rechnern beschäftigt hat, weiß wie vielfältig ihr Einsatzgebiet ist und was für Möglichkeiten sie bieten uns das Leben leichter zu machen. Eine wichtige Eigenschaft ist die, dass Daten die in digitaler Form auf einem Rechner vorliegen, praktisch gesehen beliebig oft vervielfältigt werden können, ohne dabei Qualitätsverluste (z.B. bei Musik) befürchten zu müssen. Doch es nützt nichts, wenn man Daten auf einem Rechner beliebig oft vervielfältigt und sie dann doch in diesem einen Rechner "gefangen" sind, obwohl sie weiteren Personen oder sogar der ganzen Welt zur Verfügung stehen sollten. Genau aus diesem Grund wurde schon bald eine schnelle und sichere Kommunikationsart zwischen unterschiedlichen Rechnern benötigt, die jegliche Art von Daten auf die unterschiedlichsten Systeme übertragen konnte. Eine solche Kommunikationsverbindung bezeichnet man heute als Netzwerk. Ein solches Netzwerk ist in der Größe frei skalierbar und kann somit auf die individuellen Anforderungen abgestimmt werden. Außerdem ist es auch möglich gleichzeitig auf gemeinsam genutzte Daten zuzugreifen. Doch was für Netzwerke gibt es?

Wie sieht das Grundkonzept der Übertragung aus?

Wie ist so ein Netzwerk eigentlich aufgebaut?

Und was bedeuten die Begriffe: IP, NAT, UDP, TCP?

Fragen über Fragen auf die ich nun in den folgenden Abschnitten näher eingehen werde.

## 2 Was für Netzwerke gibt es?

Netzwerke können nach zwei verschiedenen Kriterien unterschieden werden. Zum einen nach ihrer logischen Struktur und zum anderen nach ihrer räumlichen Ausdehnung.

Bei der logischen Struktur unterscheidet man hauptsächlich Peer-to-Peer Netzwerke (Abb. 2.1) und Netzwerke mit Servern (Abb. 2.2). Das Peer-to-Peer Netzwerk ist die einfachste Möglichkeit Rechner zu vernetzen, dieses Netzwerk besteht aus gleichberechtigten Rechnern und man hat dadurch keine Möglichkeit Daten zentral abzulegen:

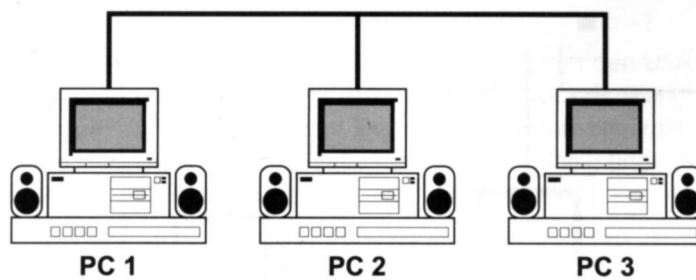


Abbildung 2.1: Peer-to-Peer-Netzwerke mit gleichberechtigten Rechnern [BW01]

Bei Netzwerken mit Servern hingegen besteht diese Möglichkeit, denn diese bilden die zentrale Verwaltungs- und Speichereinheit. Daher besteht in diesem Netzwerk eine Hierarchie wobei der oder die Server den anderen Rechnern übergeordnet sind. Dabei verwaltet der Server in einer zentralen Datenbank die Nutzer und deren Zugriffsrechte. Das heißt jeder Nutzer der auf die zentralen Daten zugreifen möchte muss sich beim Server über einen Rechner anmelden:

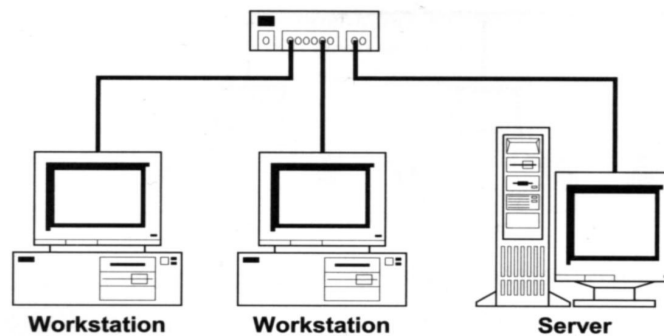


Abbildung 2.2: Serverbasiertes Netzwerk mit hierarchischer Struktur [BW01]

Wie bereits erwähnt, werden Netzwerke auch nach ihrer räumlichen Ausdehnung unterschieden. Hier unterscheidet man hauptsächlich LAN und WAN. Das LAN ist die Abkürzung für Lokal Area Network. Man beschreibt damit ein Netzwerk was auf einen Raum oder ein Gebäude beschränkt ist, also mit anderen Worten lokal ist. Hierbei ist es nicht von Bedeutung wie viele Server in diesem Netz aktiv sind.

Die Abkürzung WAN hingegen steht für Wide Area Network, was als eine Erweiterung der LAN zu betrachten ist. Dieser Begriff beschreibt also ein überregionales Netzwerk, welches aus mehreren in sich geschlossenen LAN's besteht, die untereinander verbunden sind.

Hierbei können die einzelnen LAN's auf verschiedene Gebäude, Stadtteile oder Länder verteilt sein. Das bekannteste Beispiel eines WAN ist das Internet, welches noch weitere besondere Eigenschaften hat.

### **3 Das Grundkonzept der Adressen (IP)**

Nach diesen grundlegenden Begriffserläuterungen soll jetzt im folgenden das Grundkonzept der IP-Adressen betrachtet werden.

Die Grundidee ist eigentlich recht einfach zu verstehen. Es ist im Grunde wie im richtigen Leben. Wenn man mit jemandem kommunizieren möchte, muss man als erstes wissen wen speziell man eigentlich ansprechen möchte aus der Gesellschaft. Genauso ist es in einem Netzwerk, auch wenn ein Rechner mit einem anderen in Verbindung treten möchte. Um dies zu realisieren muss jeder Rechner im Netzwerk eindeutig zu identifizieren sein. Da die Rechner im Grunde nur mit „0“ und „1“ arbeiten basiert diese eindeutige Erkennung auf Zahlen die leicht binär dargestellt werden können. So bekommt jeder Rechner im Netzwerk eine eigene Adresse, und zwar eine sogenannte IP-Adresse. Jeder der schon einmal im Internet gesurft ist weiß, dass man diese Adresse benötigt um sich in das größte Netzwerk der Welt einklinken zu können. Aus diesem Grunde steht IP auch für den Begriff „Internet Protokoll“. Die IP-Adresse selbst besteht aus einem 32 Bit Wert der wiederum in vier Felder von je 8 Bit eingeteilt wird.

Jedes Feld kann durch die 8 Bit die ihm zur Verfügung stehen eine beliebige Zahl zwischen 0 und 255 annehmen. Die Felder an sich werden mit einem Punkt voneinander getrennt. Eine solche IP-Adresse könnte nun speziell z.B. so aussehen: „255.98.162.5“.

Theoretisch lassen sich mit dieser Methode gut und gerne 4,2 Mrd. verschiedene IP-Adressen generieren. Nun wurde ja bereits erwähnt, dass es sich beim Internet im Grunde um ein WAN handelt, was aus LAN's besteht. Daher ist es nur logisch und sinnvoll die Rechner die sich in einem LAN befinden zu einem Teilnetz zusammenzufassen und somit mehr Ordnung und Struktur in diese Vielzahl von Adressen zu bringen. Um dies zu realisieren ist jede IP-Adresse in einen sogenannten Präfix und einen Suffix eingeteilt (Abb. 3.1).

Der Präfix identifiziert das physikalische Netzwerk an das der Rechner angeschlossen ist. Dieser Teil wird auch "Netzwerknummer" genannt. Der Suffix identifiziert nun einen ganz speziellen Rechner in diesem Netzwerk. Eine solche Unterteilung der IP-Adresse kann z.B. wie folgt aussehen:

<i>Netzwerkpräfix</i>	<i>Suffix</i>
10000001 00110100	00000110 00000000
(129.52.	6.0)

Abbildung 3.1: Bestandteile einer IP-Adresse [Ha02]

Da es ja verschieden große LAN's gibt, unterteilt man diese und somit auch ihre IP-Adressen weiterhin in sogenannte Netzwerkklassen (Abb. 3.2). Insgesamt unterscheidet man 5 Netzwerkklassen.

Um diese näher zu erläutern wird im folgenden die IP-Adresse durch Variablen dargestellt, dies sieht dann so aus: "aaa.bbb.ccc.ddd" [1]. Die erste Netzwerkklassen sind die sogenannten Klasse A-Netze. Diese Netze enthalten für das Feld "aaa" in der IP-Adresse die Werte von 0 bis 127, dies bedeutet, dass es nur 128 Klasse A-Netze gibt (Abb. 3.3)! Aber dafür können die restlichen Felder zur Identifizierung der Endgeräte (z.B. ein spezieller Rechner) in diesen Netzwerken genutzt werden, was in Zahlen etwa 17 Mio. Endgeräte sein würden. Die Klasse B-Netze nutzen die Werte 128-191 an der Stelle aaa und zusätzlich die Werte bbb für die Netzwerknummer. Damit stehen in diesem Netz 16382 Netzwerke zur Verfügung, wobei jedes Netzwerk ca. 64000 Geräte beherbergen kann (durch die restlichen beiden Felder in der IP-Adresse). Die Klasse C-Netze nutzen die Werte 192 bis 223 für das Feld aaa und zusätzlich die Felder bbb und ccc als Netzwerknummer. Das bedeutet, dass ca. 2 Mio. Netzwerke entstehen und pro Netzwerk können 254 Endgeräte angesprochen werden. Diese drei Klassen sind die primären Klassen die verwendet werden. Die Klassen D und E teilen sich den restlichen Wertebereich für das Feld aaa. Sie sind hauptsächlich reserviert für besondere Aufgaben und Funktionen oder aber auch für spätere Anwendungen. Im folgenden nun noch einmal einen kurzen tabellarischen Überblick zu der eben angesprochenen Klasseneinteilung:

<i>Klasse</i>	<i>Wertebereich</i>
A	0 bis 127
B	128 bis 191
C	192 bis 223
D	224 bis 239
E	240 bis 255

Abbildung 3.2: Dezimalwertebereich des ersten Bytes nach Adressklassen [Ha02]

<i>Klasse</i>	<i>Max. Netzwerke</i>	<i>Max. Hosts pro Netzwerk</i>
A	128	16777216
B	16384	65536
C	2097152	256

Abbildung 3.3: Charakteristika der IP-Adressen [Ha02]

Diese eben erwähnten Netzwerkklassen können bei Bedarf nun noch in kleinere Subnetze weiter unterteilt werden. Damit nun aber eindeutig entschieden werden kann welcher Teil der IP- Adresse die Netzwerknummer und welches die eigentliche Rufnummer ist, gibt es die sogenannte Sub-Mask. Sie hat die gleiche Struktur wie die IP-Adresse, aber besteht nur aus 24 Bit. Diese Sub-Mask markiert den Teil der IP-Adresse, der die Netzwerknummer repräsentiert. Für ein Klasse B-Netz müssten die Werte der Sub-Mask dann so aussehen : 255.255.0.0. So, damit sollten die IP-Adressen mit ihren Präfixen, Suffixen und auch ihrer Unterteilung ausreichend erläutert worden sein. Da das Grundkonzept der Adressen jetzt klar ist, werden nun im folgenden einige Kommunikationsarten zwischen Rechnern anhand von Protokollen (mit ihren Vor- und Nachteilen) etwas näher beleuchtet.

#### **4 Wie funktioniert ein Netzwerk? (TCP/IP & UDP)**

Ganz allgemein kann man sagen, dass ein Netzwerk im wesentlichen aus zwei Teilen besteht. Der eine Teil ist die Hardware, welche die physikalische Verbindung zwischen den Rechnern herstellt und über die dann später die Daten übertragen werden. Zur Hardware zählen z.B. Netzwerkkarten, Server, Router und Verbindungskabel. Die Möglichkeiten der Vernetzung im Hardwarebereich sind groß und hängen hauptsächlich vom Verwendungszweck des Netzwerkes und vom Geldbeutel ab. Doch dieser Hardwarebereich soll in dieser Ausarbeitung keine größere Rolle spielen, denn der zweite Teil, die Software, ist wie ich finde sehr viel interessanter und auch komplexer.

Nehmen wir zum allgemeinen Verständnis wieder ein Beispiel: Damit Menschen untereinander Informationen austauschen können müssen sie zumindest eine gemeinsame Sprache sprechen. Des weiteren übermitteln wir die Information, die wir an einen anderen Menschen weitergeben möchten nicht in einem Zuge, sondern wir zerlegen sie in Worte und übermitteln diese nach und nach an unseren Partner mit dem wir kommunizieren. Dieser setzt die Worte wieder zur ursprünglichen Information zusammen.

Genau nach diesem Prinzip funktioniert auch der Informationsaustausch zwischen zwei Rechnern. Dabei liegt die Sprache in der sich die Rechner "unterhalten" oder besser gesagt Informationen austauschen logischerweise in Softwareform vor. Diese spezielle Software wird auch Protokoll genannt. Wie auch im richtigen Leben wo es verschiedene Sprachen gibt, so gibt es auch bei der Rechnerkommunikation eine Vielzahl verschiedener Protokolle.

Einige ermöglichen eine Kommunikation von unterschiedlichen Rechnerarten über verschiedene Netzwerktypen, andere wiederum sind auf bestimmte Netzwerke, Aufgaben und besondere Systeme zugeschnitten. Beide Rechner müssen jedoch über mindestens ein gemeinsames Protokoll verfügen damit sie Informationen austauschen können.

Auf zwei dieser Protokolle möchte ich im folgenden genauer eingehen. Das eine ist das TCP/IP (was eigentlich aus zwei Protokollen besteht: 1. TCP und 2. IP) und das andere ist das UDP. Beide Protokolle zerlegen die zu übertragenden Informationen in kleine Stückchen. Diese Stückchen werden dann jeweils mit der Absender- und der Empfänger-IP (und eventuell weiteren Informationen) zu einem Netzwerkpaket zusammengeschnürt und verschickt (so wie es bei den meisten Netzwerken gemacht wird). Bei größeren Netzwerken (wie z.B. dem Internet) werden die einzelnen Pakete durch ein sogenanntes Routing intelligent über verschiedene Server und Router geschleust, bis das Paket die Zieladresse erreicht hat. Der Empfänger muss die Pakete sammeln und wieder zusammen setzen bevor er mit den Daten weiter verfahren kann. Ich gehe zunächst einmal auf das wichtigste und verbreitetste Protokoll ein, das TCP/IP Protokoll. Die Abkürzung TCP/IP bedeutet "Transmission Control Protocol / Internet Protocol", wobei dieser Überbegriff für eine Reihe unterschiedlicher Protokolle steht die aus dem Bereich der UNIX-Betriebssysteme stammen. Diese Protokollfamilie wurde Mitte der 70er Jahre entwickelt. TCP/IP schafft ein heterogenes Netzwerk mit offenen Protokollen, die unabhängig von unterschiedlichen Betriebssystemen, Hardware-Architekturen und Netzwerken sind. Das heißt sie sind bestens für eine Vielzahl von unterschiedlichen Rechnern geeignet, die auch in unterschiedlichen Netzen beheimatet sein können. So kann man sagen, dass das TCP/IP die Fähigkeit hat mehrere kleine Netze (LAN's) zu einem WAN zu verbinden. Aufgrund dieser Eigenschaften bildet das TCP/IP die Grundlage des Internets. Dieses Protokoll hat durch seine umfassende Leistungsfähigkeit den Vorteil, dass es individuell einsetzbar ist. Des weiteren können Daten durch die TCP-Verbindung jederzeit in beide Richtungen fließen. Außerdem gewährleistet es eine sehr sichere Übertragung. Diese wird mit verschiedenen Verfahren gewährleistet, die an dieser Stelle kurz erwähnt werden sollen. Eines der wichtigsten ist die Neuübertragung, denn empfängt TCP Daten schickt es dem Sender eine Bestätigung (ACK = Acknowledgement). Vor jeder Datenübertragung startet TCP einen Timer. Läuft der Timer vor Ankunft einer Bestätigung ab, überträgt der Sender die Daten nochmals. Ein weiteres Verfahren ist, dass zu jedem Paket bei jeder Übertragung noch Kontrollinformationen hinzu kommen, diese werden auch TCP-Header genannt. Der Header jedes Paketes enthält Informationen anhand derer, u.a. die Paketgröße überprüft wird. Durch diese Mechanismen garantiert TCP/IP eine korrekte und sichere Übertragung. Ein Nachteil dieser Kontrolle ist, dass die Datenmenge bei jeder einzelnen Übermittlung größer wird und somit das Gesamtnetz zusätzlich belastet.

Ganz im Gegensatz zu dem eben beschriebenen umfangreichen TCP, besitzt des UDP (User-Datagram-Protokoll) nur einen minimalen Kontrollmechanismus und garantiert keineswegs eine sichere oder korrekte Übertragung. Das UDP wurde definiert um auch Anwendungsprozessen die direkte Möglichkeit zu geben, Datagramme (Pakete) zu versenden. Der Funktionsumfang des UDP-Protokolls ist daher gegenüber dem TCP-Protokoll eingeschränkt. Er beschränkt sich auf den Transportdienst und dem Multiplexen von Verbindungen. Bei diesem Transportdienst ist die korrekte Datenübermittlung an den Empfänger nicht sichergestellt, da er ohne Bestätigungsmechanismus arbeitet. Verlorengegangene Datenpakete können daher nicht erneut gesendet werden. Im Gegensatz zu TCP baut UDP auch keine aktive Verbindung zwischen den Stationen auf, sondern schickt die einzelnen Datenpakete völlig unabhängig voneinander ins Netz. Durch Verwendung von sogenannten »Ports« können in einem Rechner mehrere Kommunikationsziele ausgewählt werden. Diese Funktion wird »Multiplexing« genannt (Abb. 4.1). (Multiplexing ist ein Verfahren zur zeitgleichen oder zeitlich geschichteten Übertragung von Signalen oder Elementen mehrerer Nachrichten).

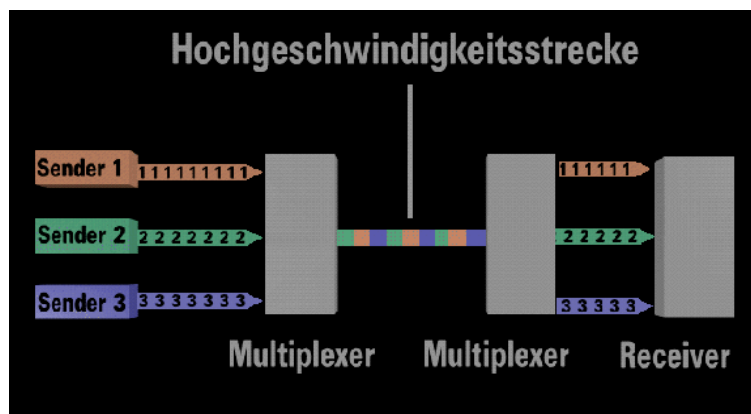


Abbildung 4.1: Multiplexing Verfahren [3]

Die Ports werden durch Nummern identifiziert, wobei diese Nummern teilweise für bestimmte Prozesse reserviert sind. Da das UDP-Protokoll nur unter bestimmten Implementationen eine minimale Fehlerbehandlung hat, obliegt es den höheren Schichten, Fehler zu erkennen und gegebenenfalls erneut ein Datensegment anzufordern. Demzufolge ist der UDP-Header sehr viel kleiner als beim TCP-Protokoll und belastet so das Netzwerk nur minimal. Einsatzgebiete für UDP sind z.B. die Versendung von Videostreams, da es hierbei auf eine flüssige und schnelle Datenübertragung ankommt und kleinere Datenaussetzer nicht wirklich von Bedeutung sind. Zum Abschluss dieses Abschnitts, soll an dieser Stelle noch kurz auf das NAT-Protokoll eingegangen werden, welches nun im folgenden beschrieben wird.

## 5 Das Grundkonzept vom NAT-Protokoll

Die Abkürzung NAT bedeutet Network Address Translation. Wie der Name schon sagt werden hier offenbar Adressen "übersetzt", das bedeutet im Klartext folgendes: Gewöhnlich werden die Netzwerkpakete ja von ihrer Quelle über verschiedene Links zu ihrem Ziel geleitet, dabei wird das Paket im eigentlichen Sinne nicht verändert. Würde nun einer dieser Links NAT verwenden, dann würde er die Quelle oder das Ziel (Sender- oder Empfänger IP) dieses Paketes verändern, wenn es an diesem Link eintrifft. Wie man sich nun leicht denken kann wurde das System nicht dafür entworfen so zu arbeiten. Sondern es ist folgendermaßen gedacht.

Gewöhnlich wird sich der Link, der NAT verwendet, daran erinnern wie er das Paket verändert hat und wenn ein Antwortpaket aus der anderen Richtung kommt, wird er genau das Umgekehrte darauf anwenden. Im Normalfall ist es ja so, die meisten Internetanbieter vergeben an jeden der sich ins Internet einwählen möchte eine einzelne IP-Adresse. Nun ist es ja möglich, Pakete mit welcher Quelladresse auch immer zu verschicken, aber nur Pakete mit dieser Antwortadresse werden zu einem zurückgesendet. Stellen wir uns nun vor wir haben ein Heimnetzwerk, aber nur ein Rechner verfügt über einen Internetanschluss (wir haben nur eine IP-Adresse), aber wir wollen über alle Rechner auf das Internet zugreifen können. Um dies zu realisieren benötigt man NAT, denn damit ist es möglich das Ziel von eintreffenden Paketen im Netzwerk zu verändern. Damit wird also die Möglichkeit eröffnet von außen die Rechner die hinter dieser einen IP-Adresse stehen zu erreichen. So kann man also ein LAN mit lokal eindeutigen IP-Adressen durch NAT mit einer einzigen globalen IP-Adresse im Internet repräsentieren. Es bildet also eine "Schnittstelle" zwischen dem lokalen und dem globalen Netz (Abb. 5.1).

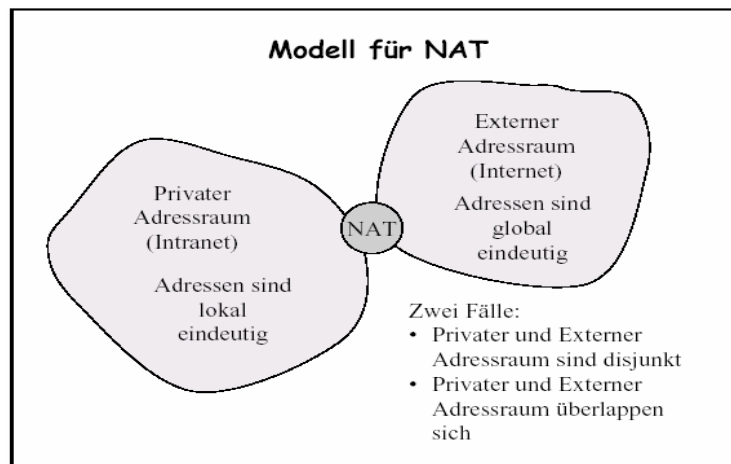


Abbildung 5.1: NAT-Modell [4]

Das Protokoll wird also zum routen (weiterleiten) von Paketen zwischen lokalen und globalen Netzen genutzt.

Damit sollten die Grundlagen von NAT, sowie die vielfältigen und unterschiedlichen Kommunikationsarten zwischen Rechnern ausreichend erläutert worden sein. Fassen wir nun zusammen.

## **6 Zusammenfassung**

Damit die Rechner in einem Netzwerk kommunizieren können benötigen sie in jedem Falle eine IP (Internet Protokoll) – Adresse, wodurch jeder Rechner eindeutig in einem Netzwerk “ansprechbar“ ist, diese Adresse ist 32 Bit lang. Die Informationen, die man übertragen möchte werden durch ein sogenanntes Protokoll in Pakete zerlegt und eventuell mit Zusatzinformationen bestückt. Wobei jedes Paket immer die IP-Adresse des Senders und des Empfängers enthält. Anhand dieser Informationen wird das Paket über verschiedene Server u.s.w. geleitet bis es beim Empfänger eintrifft. Weiterhin wissen wir, dass es durch NAT möglich ist mehrere Rechner die sich in einem Netzwerk befinden mit dem Internet zu verbinden auch wenn man nur eine IP-Adresse zur Verfügung hat. Weiterhin haben wir die Protokolle TCP/IP und UDP kennengelernt. Wobei TCP das leistungsstärkere Protokoll ist und durch viele Verfahren sicherstellt, dass die Daten auch den Empfänger erreichen. Dadurch ist die Übertragung aber auch langsamer und die zu übertragenden Datenmengen größer. Das UDP besitzt hingegen wenige Kontrollmechanismen und kann daher eine schnellere Übertragung ermöglichen. Dafür gibt es jedoch keine Garantie, dass die Daten wirklich beim Empfänger ankommen. Daher ist es besonders geeignet für die Versendung von Videostreams, da es hierbei auf eine flüssige Datenübertragung ankommt und kleinere Datenaussetzer nicht wirklich von Bedeutung sind. So kann man zusammenfassend sagen, dass im Grunde die Vergabe der IP-Adressen und deren Verfügbarkeit für die Netzwerke von enormer Bedeutung sind. Um der immer stärkeren Knappheit der IP-Adressen entgegenzuwirken ist bereits die IP-Version 6 in Arbeit, wo die IP-Adressen aus 128 Bit bestehen sollen. Insgesamt wurde hiermit ein umfangreicher Überblick über die grobe Funktionsweise von Netzwerken und deren Protokolle gegeben.

## **Literaturverzeichnis**

- [BW01] Jürgen Brebeck, Peter Winkler: PCs vernetzen Gewusst wie!, 1. Auflage, Markt&Technik Verlag, München, 2001
- [Ha02] <http://www.rnks.informatik.tu-cottbus.de> Unter: Lehre, Vorlesungsskripte und Lehrmaterialien, WS 2002/2003 “Proseminar Internet“, Vortrag „IP-Adressen“ von Birka Harmuth
- [3] <http://klever.multimedia.fhaugsburg.de/fha/Vorlesungen/Datenkommunikation/Studenten/SS2003/GruppeB/weinrot/UDP>
- [4] <http://www.tik.ee.ethz.ch/~plattner/Kursunterlagen/TCP-IP/nat.pdf>