

Werner Geers  
 Berufliche Informatik  
 ISBN:978-3-427-60080-0  
 Bestellnr.:60080



Das nachfolgende Skript wurde aus dem folgenden Lehrbuch entnommen:

Geers/Beckermann/Rieger  
 Informationsverarbeitung  
 mit Office 2003  
 ISBN: 978-3-427-61273-5  
 Bestellnr.: 61273



Autor dieses Skripts

**Dipl.- Ing. Jens Rieger**

Ich bedanke mich herzlich bei Jens, dass er dieses Skript zur Verfügung stellt.

**Zusatzinformationen**

(c) by Jens Rieger

<b>13</b>	<b>Netzwerke .....</b>	<b>560</b>
13.1	Grundlagen zu vernetzten Systemen.....	560
13.1.1	Vorbemerkungen .....	560
13.1.2	Einteilung der unterschiedlichen Netzwerke .....	560
13.1.3	Aufbau und Organisation von vernetzten Systemen .....	570
13.1.4	Sinn und Zweck vernetzter Systeme .....	572
13.1.5	Einsatzgebiete für vernetzte Systeme .....	575
13.2	Installation von Netzwerken .....	577
13.2.1	Direktverbindung zweier PCs.....	577
13.2.2	Einrichtung eines Peer-to-Peer-Netzwerkes.....	586
13.3	Einrichtung eines zentralen Internetzuganges.....	599

Dieses Skript darf im Unterricht in Verbindung mit dem oben angegebenen Lehrbuch oder einem anderen Lehrbuch desselben Schulbuchautors eingesetzt werden.

## 13 Netzwerke

### 13.1 Grundlagen zu vernetzten Systemen

#### 13.1.1 Vorbemerkungen

Das Kapitel Netzwerke ist so aufgebaut, dass es durchaus möglich sein soll, im Bedarfsfall direkt mit dem zweiten Teil, also mit der praktischen Einrichtung von Netzwerken, oder mit dem dritten Unterkapitel, der Einrichtung eines zentralen Internetzuganges, zu beginnen. Die vorangestellten Grundlagen bieten wichtige Informationen, die zum Verständnis des insgesamt doch sehr komplexen Gesamthemas „Netzwerke“ beitragen sollen, allerdings nicht zwingend den Kapiteln 13.2 und 13.3 vorangestellt sein müssen.

Die Grundlagen unserer heutigen lokalen und globalen Netzwerke liegen gerade einmal etwas mehr als 20 Jahre zurück. Der Siegeszug der Automobile hat etwa 100 Jahre erfordert. Computer haben es innerhalb der letzten 2 Jahrzehnte geschafft, dasselbe hohe Beschäftigungsniveau der Automobilindustrie zu erreichen.

Im Jahre 1981 hat IBM - eine der renommiertesten Großrechner-Hersteller-Firmen - den ersten PC (Personal Computer) auf den Markt gebracht, den Urvater des IBM-kompatiblen PC-Systems. Ein derartiger IBM-PC der frühen 80er Jahre verfügte über zwei Diskettenlaufwerke und 64 KB Arbeitsspeicher. Eine 10 MB große Festplatte galt damals als gigantisch und kostete so viel wie unsere heutigen PCs. Programme wie Word oder Multiplan passten auf eine 360 KB-Diskette.

Neben der **PC-Welt** von IBM gab es und gibt es die Welt der **Apple-PCs**. Diese hatten nicht nur hinsichtlich der graphischen Benutzeroberfläche, die für die Benutzer der IBM-kompatiblen PCs erst mit der Einführung des Betriebssystems **Windows** erfolgte, die Nase vorn. Auch und gerade im Hinblick auf die Verbindung (Vernetzung) von Apple-PCs hat man sich im Hause Apple frühzeitig Gedanken gemacht. Bei den hohen Preisen von Festplatten, Druckern und anderen Peripheriegeräten kam man zwangsläufig auf die Idee, diese teuren Medien gemeinsam zu nutzen. Sehr schnell folgte die Erkenntnis, dass es eine Fülle von Daten gibt, die man am effektivsten gemeinsam nutzen kann. Mit einfachen Umschaltboxen wurden erste Verbindungen zwischen PCs erstellt und genutzt. Dies war die Geburtsstunde der so genannten **Peer-to-Peer-Netzwerke**, die einfache direkte Verbindung zwischen zwei oder mehr PC-Systemen. Die so genannten **Stand-Alone-PC-Systeme** der frühen 80er Jahre waren von *statischen* Datenbeständen gekennzeichnet. Die Aktualisierung von Informationen erfolgte durch das Übertragen der Daten per Diskette oder anderer Speichermedien. Mit dem Anwachsen der Datenbestände wurde die Aktualisierung aber immer schwieriger.

Der Wunsch und das Bedürfnis nach einer *dynamischen* Verknüpfung von Datenbeständen und die Möglichkeit des gemeinsamen Zugriffs auf eine ständig aktuelle Datenzentrale war die Grundmotivation für die so genannten serverbasierten Netzwerklösungen: **Client-Server-Netzwerke**.

#### 13.1.2 Einteilung der unterschiedlichen Netzwerke

Jeder von uns kennt Netzwerke: das Wassernetzwerk, das Telefonnetzwerk, das Elektrizitätsnetzwerk. Die gemeinsame Grundlage all dieser Netzwerke ist der Verbund mehrerer einzelner Endgeräte (z. B. Computer) zum Zweck des Austauschs und der gemeinsamen Nutzung von Systemkomponenten.

Die Klassifikation von Computer-Netzwerken kann nach den folgenden Kriterien, die in **organisatorische** und **technische Kriterien** gegliedert wurden, unterschieden werden:

• **Organisatorische Kriterien**

- **Geographische Erstreckung** des Netzwerks (z. B. LAN oder WAN)
- **Netzwerkklassen** (z. B. Peer-to-Peer-Netze und Client-Server-Netze)

• **Technische Kriterien**

- **Netzwerktopologie**  
Die Netzwerktopologie beschreibt die Struktur eines Netzwerkes, also die Art, wie die physische Verbindung der Computersysteme vorgenommen wird. Die Standard-Netzwerktopologien sind: Bus-, Stern- und Ring-Netzwerk.
- **Übertragungsmedium/Hardware**  
Beim Einsatz der notwendigen Hardware ist neben der Wahl der Netzwerkkarten u. a. auf die Möglichkeit verschiedener Kabelverbindungen zu achten (z. B. Koaxial-, Twisted-Pair- und Glasfaserkabel).
- **Technologie**  
Die bekanntesten Technologien lokaler Netzwerke sind Ethernet und Token Ring.
- **Zugriffsverfahren**  
Grundsätzlich lassen sich **zentrale** (das so genannte Polling) und **dezentrale Zugriffsweisen** auf das Übertragungsmedium unterscheiden. Die Unterteilung der dezentralen Zugriffsweisen in **stochastische** und **deterministische** führt uns zu den wichtigen Zugriffsverfahren CSMA/CD und Token Passing.

**Geographische Erstreckung des Netzwerks**

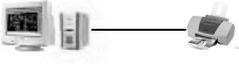
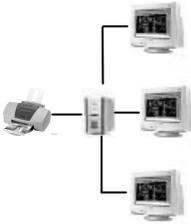
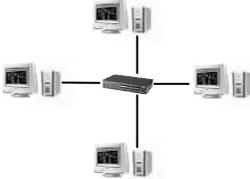
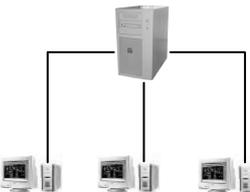
Die Unterscheidung bzw. Bezeichnung von Netzwerken aufgrund ihrer Ausdehnung ist nicht fest definiert, wird allerdings sehr häufig verwendet. Die folgenden Erklärungen und Beispiele sollen die jeweiligen Zusammenhänge verdeutlichen.

<b>L</b> ocal <b>A</b> rea <b>N</b> etwork	Oft werden Netzwerke, die Computer innerhalb von Räumen, Gebäuden oder Gebäudegruppen verbinden, als lokale Netzwerke bezeichnet. Dazu gehören demnach sowohl private Netzwerke als auch der Zusammenschluss von Computern eines Betriebes. <i>Das Netzwerk in einem Unternehmen, einer Verwaltungseinheit, einer Schule oder in einem Privathaushalt.</i>
<b>M</b> etropolitan <b>A</b> rea <b>N</b> etwork	In einer Region vorhandene lokale Netzwerke werden miteinander verbunden. Dabei sind i. d. R. andere Anforderungen z. B. an die Datenübertragungsraten und Ausfallsicherheiten als bei einem LAN zu stellen. <i>In der Region Hannover werden alle staatlichen Netzwerke zu einem gemeinsamen Netzwerk zusammengeschlossen: MAN-Hannover.</i>
<b>W</b> ide <b>A</b> rea <b>N</b> etwork	Ein überregionales, meist weltweites Netz schließt die Computer verschiedener Betriebe oder anderer Benutzer zusammen. <i>Das bekannteste weltweite Netz ist das Internet.</i>

Es lassen sich auch teilweise weitere Bezeichnungen für die Ausbreitung von Netzwerken als die oben genannten finden. So wird z. B. die private Heimvernetzung von Hausgeräten mit dem Begriff **PAN** (personal area network) in Verbindung gebracht und bei dem Begriff Internet auch von einem **GAN** (global area network) gesprochen.

## Netzwerkclassen

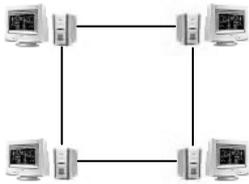
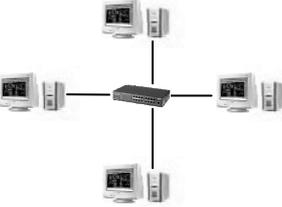
In ihren einfachsten Formen können Computersysteme zunächst als Einplatz- oder Mehrplatzsysteme aufgebaut werden. Mehrplatzsysteme beinhalten Komponenten, die Vorstufen einer Vernetzung darstellen. Bezogen auf die logischen Verbindungen der Computer untereinander sind die wichtigen Netzwerkclassen dann die Peer-to-Peer- und Client-Server-Netze.

<p><b>Einplatzsystem</b></p> 	<p>Bei einem Einplatzsystem ist die Zentraleinheit des Computers mit anderen Komponenten verbunden wie</p> <ul style="list-style-type: none"> <li>• Dialogterminal (Tastatur und Bildschirm),</li> <li>• Diskettenlaufwerk, Festplatte,</li> <li>• CD-ROM-Laufwerk,</li> <li>• Drucker.</li> </ul>
<p><b>Mehrplatzsystem</b></p> 	<p>Bei einem Mehrplatzsystem ist die Zentraleinheit des Computers mit anderen Komponenten verbunden wie</p> <ul style="list-style-type: none"> <li>• Dialogterminals (Tastatur und Bildschirm),</li> <li>• Diskettenlaufwerk, Festplatte,</li> <li>• CD-ROM-Laufwerk,</li> <li>• Drucker.</li> </ul> <p>Die Zentraleinheit wird von mehreren Teilnehmern genutzt, da die einzelnen Dialogterminals keine eigene „Intelligenz“ haben. Das System wird durch ein Multi-User-Betriebssystem gesteuert, welches in der Lage ist, die Prozessorzeit auf die verschiedenen Benutzer zu verteilen (Time-Sharing-Verfahren).</p>
<p><b>Peer-to-Peer-Netze</b></p> 	<p>Bei einem Peer-to-Peer-Netzwerk sind die einzelnen Rechner im Netzwerk gleichberechtigt. Jeder Computer kann sowohl Server- als auch Clientfunktionen übernehmen. Er stellt also Informationen im Netz zur Verfügung und kann Informationen von anderen Rechnern im Netz abrufen. Der Nachteil dieses Systems liegt sicherlich darin, dass keine zentrale Daten- und Zugriffsverwaltung erfolgt. So können z. B. auf den einzelnen Computern unterschiedliche Datensätze vorhanden sein und bei einer größeren Anzahl von Clients der Einrichtungs- bzw. Verwaltungsaufwand höher sein als in einem serverbasierten Netz.</p>
<p><b>Client-Server-Netze</b></p> 	<p>Bei diesem System stellen ein oder mehrere Computer, so genannte Server, Informationen (Programme, Daten) und Hardware (z. B. Drucker) im Netz zur Verfügung. Die angeschlossenen Rechner (Clients) können die Informationen abrufen und nutzen. Durch eine zentrale Benutzerverwaltung kann der Verwalter des Netzwerkes (Administrator, Supervisor) an die einzelnen Client-Anwender bestimmte Zugriffsrechte vergeben (bzw. verweigern), sodass der einzelne Benutzer z. B. bestimmte Programme aufrufen oder bestimmte Daten bearbeiten darf.</p>

Eine Sonderform der Client-Server-Netze stellen die so genannten **Cluster-Netze** dar. Wie der Begriff Cluster (übersetzt: Gruppe) bereits andeutet, werden mehrere Server so zusammengefasst, dass diese für die Clients nur als ein Server erkennbar sind.

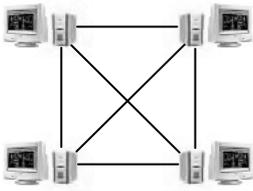
Netzwerktopologien

Die Struktur eines Netzes wird nach bestimmten Netzwerktopologien (Netzwerkarchitektur) aufgebaut. Die im Folgenden dargestellten Möglichkeiten sind Grundstrukturen. In der Praxis werden die Netze häufig als Kombinationen dieser Grundstrukturen eingerichtet.

<p style="text-align: center;"><b>Ringnetz</b></p> 	<p>Bei einem Ringnetz sind die Computer in Form eines Ringes miteinander verbunden. Jeder Computer ist mit je zwei Nachbargeräten verbunden. Die Nachrichten wandern von einer Station zur anderen, bis ein Computer erkennt, dass eine Nachricht für ihn bestimmt ist. Der Rechner nimmt die Information dann aus dem Ring.</p> <p>Eine Leitungsunterbrechung führt zum Ausfall des gesamten Netzes. Die Betriebssicherheit kann durch einen Doppelring mit zwei getrennten Leitungen erhöht werden.</p> <p>Die bekannteste Ringtopologie ist das 1985 von IBM vorgestellte <b>Token-Ring</b>-Verfahren, das sicherstellt, dass nie zwei Netzknoten gleichzeitig senden. Dafür wird ein bestimmtes Kennzeichen, das Token, von Station zu Station geschickt.</p> <p>Ein Vorteil liegt hier im Vergleich zum Sternnetz z. B. in der Einsparung von Kabellängen (auch bei einem Einsatz eines Doppelringes).</p>
<p style="text-align: center;"><b>Sternnetz</b></p> 	<p>Bei einem Sternnetz sind mehrere Computer stern- oder strahlenförmig mit einem Server oder einem Hub bzw. Switch verbunden. Die Zentrale bildet den Netzknoten. Das Netz ist bei Störungen dieser zentralen Komponente nicht mehr funktionsfähig.</p> <p>Der zentrale Netzknoten, z. B. der Server, kann nacheinander alle Rechner abfragen, ob sie senden wollen. Die Leistungsfähigkeit des gesamten Sternnetzes hängt wesentlich von der Leistungsfähigkeit des Servers ab. Die Vorteile des Sternnetzes bestehen z. B. darin, dass relativ leicht weitere Komponenten hinzugefügt werden können und dass der Ausfall einer Leitung nur einen teilnehmenden Rechner betrifft. Der Fehler im Netz kann daher leicht erkannt werden.</p> <p>Auch unsere Telefonnetze stellen bis zum Endteilnehmer Sternnetze dar.</p>
<p style="text-align: center;"><b>Busnetz</b></p> 	<p>Bei einem Busnetz sind die einzelnen Rechner, also der Server und die Clients (Arbeitsplatzrechner), durch ein Netzkabel, dem Bus, miteinander verbunden. Dieser, an beiden Enden mit einem Endwiderstand versehene, zentrale Bus übernimmt die Steuerung und Nachrichtenübermittlung.</p> <p>Dieser Netztyp ist die technisch einfachste Form der Vernetzung und eignet sich für ein relativ kleines Netz, in dem die Computer nur gelegentlich miteinander kommunizieren.</p> <p>Da jedoch bereits bei kleineren Kabel- oder Anschlussproblemen der gesamte Bus ausfällt und sich die Fehlersuche schwieriger gestaltet als in den zuvor genannten Topologien, liegen die Betriebskosten hier häufig höher.</p>

### Netzwerktopologien (Fortsetzung):

#### Maschennetz



In einem Maschennetz kann jeder Teilnehmer mit zwei oder mehreren Teilnehmern direkt verbunden sein. Handelt es sich um ein vollständig vermaschtes Netz, ist sogar jeder Teilnehmer mit allen anderen Teilnehmern direkt verbunden.

Ein solches Netzwerk ist extrem unempfindlich gegen Ausfälle von Leitungen und sonstigen Störungen, da die einzelnen Verbindungen unabhängig voneinander sind. Bei Ausfall einer Datenleitung kann der Datenverkehr umgeleitet werden.

Da viele Datenleitungen benötigt werden, verursacht das Netz relativ hohe Kosten.

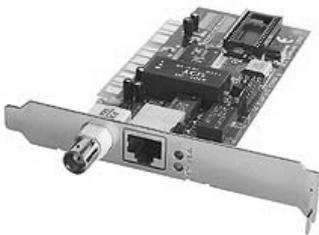
Ein wesentliches Kriterium für die Wahl der Netzform ist sicherlich die Funktionsfähigkeit des Netzes. Daher werden vor allem in Betrieben Netzwerke bevorzugt, die beim Ausfall einer Leitung nicht zum Ausfall des gesamten Netzes führen. Weitere wichtige Gesichtspunkte neben den Kosten für die Einrichtung eines Netzwerkes sind die Wartungs-, Pflege- und Verwaltungskosten, die neben dem Personaleinsatz eigener Mitarbeiter häufig unterschätzt werden und daher in der Planung eines Netzwerkes bereits sehr früh gründlich bedacht werden müssen.

#### Hardware für den Netzwerkbetrieb

Betrachtet man den Grundaufbau eines (zunächst beliebigen) Netzwerkes, dann benötigt man i. d. R. die folgenden Grundelemente:

#### Hardware zum Aufbau eines Netzwerkes:

##### Netzwerkkarte



Mindestens 2 Computersysteme sind mit je einer Netzwerkkarte auszustatten. Netzwerkkarten gibt es mit den Anschlusssystemen ISA und PCI und den Datenübertragungsraten von **10 MBit/s** und **100 MBit/s**. Häufig wird in diesem Zusammenhang vereinfacht von 10- bzw. 100-MBit-Karten gesprochen.

Bei der nebenstehend abgebildeten Netzwerkkarte handelt es sich um eine 10-MBit Karte, die sowohl mit einem **RJ-45**- und einem **RG-58**-Anschluss versehen ist. Darüber hinaus gewinnen Netzwerkkarten mit Glasfaserverbindungen immer mehr an Bedeutung.

Ein weiteres wichtiges Kriterium ist die Datenübertragungsart, bei der zwischen dem **Halb-Duplex**- (Daten werden über 2 Adern nacheinander gesendet und empfangen) und dem **Voll-Duplex-Verfahren** (gleichzeitiges Senden und Empfangen über 2 Leitungen bzw. 4 Adern) unterschieden wird.

Die Preise der Netzwerkkarten sind abhängig von den oben genannten Leistungsdaten und beginnen bei ca. 25 €.

Beim Kauf (grundsätzlich jeder Erweiterungskarte) sollte man allerdings darauf achten, dass die passenden Treiber für die verwendeten Betriebssysteme beigelegt oder aber (z. B. im Internet) gut erhältlich sind.

**Hardware zum Aufbau eines Netzwerkes (Fortsetzung):**

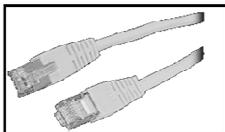
Die wichtigen Medien zur Datenübertragung in Computer-Netzwerken sind derzeit **Kupfer**, **Glasfaser** und **Luft**. An dieser Stelle kann also eine Unterscheidung zwischen der **leitergebundenen** (Kupfer und Glasfaser) und der **leiterungebundenen Übertragung** (Luft) vorgenommen werden. Die Verbindung zwischen den Netzwerk-Computern kann im Wesentlichen mit den drei folgenden Kabelarten erstellt werden:

**Koaxialkabel**



Dieses Kabel (auch **10Base2** genannt) ist mit dem Fernsehantennenkabel vergleichbar. Es hat eine spezielle Spezifikation: **RG58**. Die Steckverbindungen werden mit so genannten **BNC-Steckern** bzw. -Kupplungen oder T-Steckern hergestellt. Die Datenübertragungsraten sind auf 10 MBit/s begrenzt und die Verkabelung erinnert an eine Bus-Linie (s. auch **Busnetz** unter **Netzwerktopologien**). An den jeweiligen Endpunkten müssen 50 Ohm-Abschlusswiderstände angebracht werden.

**Twisted Pair**

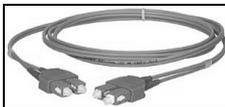


Die zweite Kabelart - **Twisted Pair** = „**paarweise verdreht**“ wird häufig abgekürzt als TP-Kabel bezeichnet oder auch abhängig von der Datenrate **10BaseT** oder **100BaseT** genannt und ist mit dem gebräuchlichen Telefonkabel vergleichbar. Die Spezifikation lautet: **RJ-45**. Die Anschlüsse dieses Kabels werden sehr leicht mit den ISDN-Telefonanschlusskontakten verwechselt.

Es gibt bei dieser Kabelart verschiedene Ausführungen, die sich unter anderem in der jeweiligen Abschirmung unterscheiden. So besitzen die einzelnen verdrehten Adernpaare beim **UTP-Kabel** (Unshielded TP) keine zusätzliche Einzelabschirmung, während diese beim **STP-Kabel** (Shielded-TP) vorhanden ist. Ist ein TP-Kabel zusätzlich durch einen Gesamtmantel (Screen) abgesichert, so spricht man von einem **S/UTP-** bzw. einem **S/STP-Kabel**.

Die Anschlüsse werden entweder nach dem so genannten CAT 5-Standard (mit einer Datenübertragungsrates bis zu 100 MBit/s) oder CAT 7-Standard (bis zu 1 GBit/s) gefertigt.

**Glasfaserkabel**



Die dritte Kabelart stellt das **Glasfaserkabel** dar (Lichtwellenleiter: **LWL-Verkabelung**). Die augenblickliche Standardübertragungsgeschwindigkeit liegt hier bei 100 MBit/s, kann allerdings auch über 1 Gbit/s liegen.

Diese Verkabelungsart ist noch relativ teuer und in der freien Verkabelung sehr anfällig. Kabelsegmente, die frei zugänglich sind, können sehr leicht beschädigt werden.

Die Sicherheit dieser Kabel (sowohl gegen Störstrahlungen als auch gegen Abhören) ist dagegen jedoch sehr gut.

Da die Übertragung der Lichtimpulse nur unidirektional (also nur in eine Richtung) erfolgt, sind für eine Verbindung mindestens zwei Lichtwellenleitungen erforderlich.

Zentrale Verkabelungen werden i. d. R. mit LWL-Verkabelung gefertigt.

### Hardware zum Aufbau eines Netzwerkes (Fortsetzung):

Sollen mehr als 2 Computer miteinander verbunden werden, dann sollte man sich mit den jeweiligen Vor- und Nachteilen der verschiedenen Netzwerktopologien beschäftigen. Die hier aufgeführten Geräte werden besonders mit der Stern-Topologie in Verbindung gebracht.

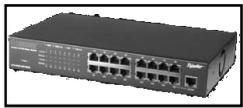
#### Hub, Bridge, Switch, Router oder Gateway



Bei einem **Hub** (übersetzt „Mittelpunkt“ bzw. „Nabe“) handelt es sich um ein Gerät, das mehrere Rechner in einem Netzwerk sternförmig miteinander verbindet und dazu dienen kann, den Datenverkehr in einem Netzwerk zu regeln.

In einem Stern-Netzwerk ist jede Workstation durch ein Kabel z. B. an einen Hub angeschlossen, an dem je nach Ausführung die entsprechende Anzahl der benötigten Anschlüsse (z. B. 4 für sehr kleine oder 24 für größere Netzwerke) vorhanden ist.

Hubs gibt es mit verschiedenen Leistungsmerkmalen, dabei wird u.a. auf die Möglichkeit der Signalverstärkung (**aktiv – passiv**), der Erweiterbarkeit („**stackable Hubs**“) oder des modularen Aufbaus geachtet.



An die Ports (Ausgänge) eines solchen Knotenpunktes können aber auch wiederum ganze Netzwerke (oder Netzwerk-Segmente) angeschlossen werden. Werden z. B. zwei lokale Netzwerke (Subnetze) miteinander verbunden, so spricht man von einer **Bridge** (Brücke), die auf der Schicht 2 des OSI-Schichtenmodells arbeitet und durch kontrolliertes Weiterleiten der Daten die Bandbreite des gesamten Netzwerkes optimieren kann.



Ein **Switch** arbeitet wie eine Bridge auf der Schicht 2 des OSI-Schichtenmodells und ist im Vergleich dazu in der Lage, eine Lastverteilung der unterschiedlichen Verbindungen bereits innerhalb eines Netzwerk-Segementes zu steuern und damit die Bandbreite zu verbessern.

Stellt z. B. ein Standard-Hub allen Verbindungen dieselbe Übertragungsbreite zur Verfügung, so kann ein Switch zwischen mehr und weniger ausgelasteten Verbindungen die Kapazitäten variieren und anpassen.



Ein **Router** ist ein Verbindungselement zwischen zwei oder mehreren Netzwerken, ist auf der Schicht 3 des OSI-Schichtenmodells einzuordnen und enthält bestimmte Funktionalitäten, um einen optimalen Weg der Datenpakete von einem zu einem anderen Rechner (also eine optimale „Route“) zu ermitteln.

Bei einem **Gateway** (übersetzt „Eingang“ bzw. „Tor“) handelt es sich um eine Verbindungsstelle verschiedener Netzwerke mit z. B. unterschiedlichen Protokollen und ermöglicht durch die Umsetzung der Daten auf bis zu allen 7 Schichten des OSI-Modells die Kommunikation der ansonsten heterogenen Netzwerke. Diese Funktionalität muss nicht zwingend durch ein Zusatzgerät bereitgestellt werden, sondern kann auch z. B. von einem Betriebssystem übernommen werden.

### Mögliche Zusatz-Hardware zum Aufbau eines Netzwerkes:

#### Wireless LAN



Die drahtlose Vernetzung (**Wireless LAN**) stellt eine weitere Verbindungsalternative dar. Hierzu verwendet man spezielle Netzwerkkarten, die mittels Antennen und so genannten **Access Points** die Verbindung im Funkfrequenzbereich von 2,4 GHz herstellen. Die Übertragungsbandbreite liegt nur bei 10 MBit/s. Der Vorteil besteht darin, dass keine baulichen Maßnahmen erforderlich sind. Die Reichweite ist jedoch begrenzt. Die Kosten sind im Vergleich zur Kabelkomponente noch vergleichsweise hoch.

Im Privathaushalt ist die „Point-to-Point“-Verbindung ausreichend. In einem größeren Netzwerk können Bereiche wie Lager, Labor, etc. mit Access Points wie dem DWL-1000AP der Firma D-Link so eingebunden werden, dass der Anwender lückenlos die Bereiche wechseln kann. Der Anschluss wird entweder über einen PCMCIA-Steckplatz (Einsteckkarte, die besonders bei Notebooks gebräuchlich ist), einen PCI-Slot (spezieller Einsteckplatz auf dem Motherboard des PCs) oder einen USB-Adapter drahtlos realisiert.

**Bluetooth** – steht für einen noch relativ neuen Standard im Nahbereich der drahtlosen, funkbasierten Datenübertragung.

Mittels eines Bluetooth-Sende-Empfängers können theoretisch sämtliche elektronischen Geräte, z. B. angefangen von der Mikrowelle über das Faxgerät, das Handy oder dem PC miteinander verbunden werden. Bluetooth erkennt die in der Reichweite (ca. 10 m im Umkreis) befindlichen Geräte und stellt die Verbindung her. So wie heute nach dem Einstecken eines USB-Kabels das angeschlossene Gerät sofort dem System bekannt gemacht wird, werden mit Bluetooth Geräte miteinander verbunden.

Diese neue technologische Entwicklung wurde im Mai 1998 von der **Bluetooth Special Interest Group (SIG)** erstmals der Öffentlichkeit vorgestellt. Der vom Mobilfunkanbieter Ericsson gegründeten Initiative schlossen sich namhafte Unternehmen wie IBM, Intel, Nokia und Toshiba an. Die Idee, eine preiswerte, energiesparende und schnelle Funkverbindung, die Kabel auf kurzer Distanz vollständig ersetzt, ist verblüffend. Bluetooth könnte zum globalen Standard werden, allerdings gibt es noch einige Probleme bei der Umsetzung, da die Geräte verschiedener Hersteller noch nicht aufeinander abgestimmt sind und sich gegenseitig stören können.

#### Ericson Bluetooth Empfänger



#### Ericson Mobile Festplatte mit Bluetooth-Modul



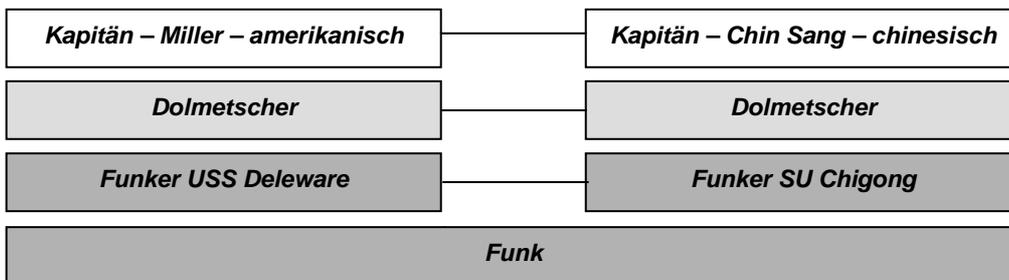
### OSI-Schichtenmodell

Die Übertragungstechnik in einem Netzwerk ist nur schwer zu veranschaulichen. Die Kommunikation zwischen vernetzten Systemen läuft nach dem **OSI-Schichtenmodell** ab.

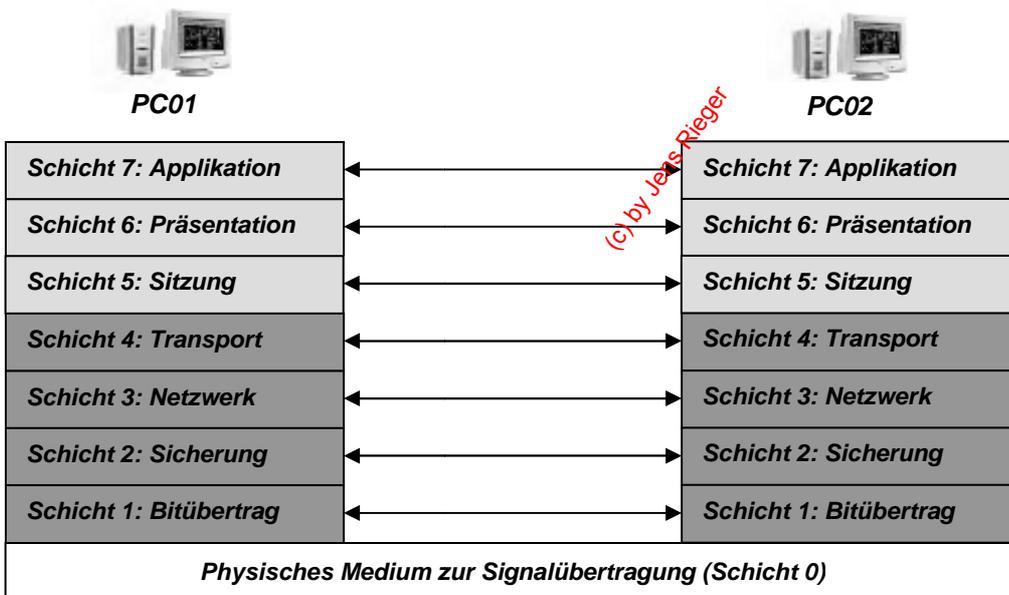
**Open Systems Interconnection Reference Model (OSI)** ist ein Kommunikations-Modell, das von der **International Standards Organization (ISO)** entwickelt wurde. Es listet die Aufgaben auf, die von Netzwerk-Komponenten erledigt werden müssen, damit Datenkommunikation überhaupt funktionieren kann.

Ein kleines Beispiel soll verdeutlichen, welche Aufgaben im OSI-Schichtenmodell vereint werden. Angenommen die Kapitäne eines amerikanischen und eines chinesischen Unterseebootes wollen miteinander in Kontakt treten, dann geschieht dies üblicherweise durch die beiden Funker. Der Kontakt wird über das Medium „Funk“ hergestellt.

Ein Dolmetscher dient als Vermittlungsschicht zwischen den beiden Gesprächspartnern, den Kapitänen. Die Funker folgen dabei ganz speziellen technischen Vorgaben, die Dolmetscher halten sich an die Regeln der Sprachen und die Kapitäne halten sich an die Regeln der christlichen Seefahrt und ihre Dienstvorschriften.



Mit dem obigen Bild vor Augen ist das folgend dargestellte OSI-Schichten-Modell etwas leichter zu verstehen.



Genau wie im Beispiel der Kommunikation zwischen beiden Kapitänen, kommunizieren die einzelnen Schichten eines Netzwerkes nach bestimmten Regeln, die von der OSI festgelegt wurden.

Die Schichten 1 bis 4 werden auch **transportorientierte Schichten** und die Schichten 5 bis 7 **anwendungsorientierte Schichten** genannt.

Unterschieden wird darüber hinaus zwischen der **horizontalen Kommunikation** (z. B. zwischen der Schicht 7 des PC01 und der Schicht 7 des PC02) und der **vertikalen Kommunikation** (z. B. das Durchlaufen eines Datenpaketes des PC01 durch alle Schichten des OSI-Schichtenmodells).

### Übertragungstechnik (Protokolle, Ethernet und Token Ring)

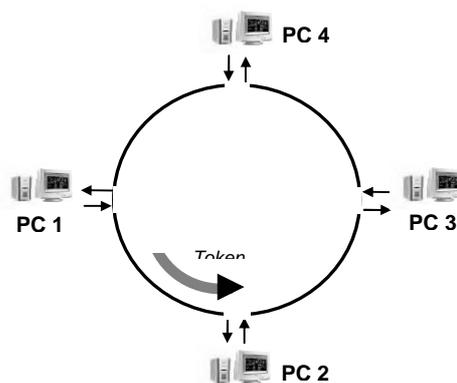
Das OSI-Modell beschreibt dabei nur grob, welche Aufgaben von den Netzwerkkomponenten erfüllt werden müssen. Die spezielle Aufgabendefinition erfolgt in den **Netzwerkprotokollen**, z. B. TCP/IP (Internet-) oder NetBEUI (Microsoft-) oder IPX (Novell-Protokoll), die auch als Kommunikationsregeln bezeichnet werden könnten.

**Ethernet** und **Token Ring** sind die am meisten verbreiteten Übertragungstechniken in Netzwerken (zu vergleichen mit der Funktechnik im U-Boot-Beispiel).

Der Begriff Ethernet setzt sich aus den englischen Bezeichnungen für „Äther“ und „Netz“ zusammen, die Regeln für Ethernet wurden von dem Institute of Electrical and Electronics Engineers in der Spezifikation 802.3 festgelegt. Die Festlegung stellt Regeln für die Netzwerk-Topologie von Ethernet-Netzwerken, für die Übertragungsmedien, die verwendet werden können, und dafür, wie die Elemente des Netzwerks zusammenarbeiten sollten, auf.

Das Token Ring Netzwerk ist durch eine ringförmige Anordnung gekennzeichnet. Kernpunkt dieses Netzwerkes ist das so genannte **Token**, das eine besondere Bitfolge darstellt und als eine Art Sendeberechtigung verstanden werden kann. Die eingebundenen Netzwerkstationen geben dieses Token nun jeweils weiter zur nächsten Station und können, vergleichbar mit einer in sich geschlossenen Eisenbahnstrecke, bei Bedarf an diesen „Zug“ Informationen anhängen, sofern dieser noch frei ist bzw. noch keine Daten eines anderen Senders enthält. Außerdem sind in dem verschickten Datenpaket Informationen zum Empfänger abgelegt, so dass beim Anhalten des Zuges an den einzelnen Stationen geprüft werden kann, ob die Station der Zieladresse entspricht. Erreicht das Token wieder den Absender des Datenpaketes, so kann diese Station das „leere“ Token weiterschicken oder zunächst überprüfen, ob der angekommene Inhalt dem abgeschickten entspricht, um das Versenden ggf. zu wiederholen.

#### Darstellung eines Beispiels für einen Token Ring:



### Zugriffsverfahren (vor allem: CSMA/CD und Token Passing)

Zugriffsverfahren regeln den Verkehr der Informationen in einem Netzwerk. Die klassischen Verfahren sind **CSMA/CD** und **Token Passing**.

Mit **CSMA/CD** (Carrier Sense Multiple Access/Collision Detection) wird bei Ethernet gewährleistet, dass in einem in sich geschlossenen Netzwerksegment - einer so genannten *Collision Domain* - nicht mehrere Stationen gleichzeitig senden. Wie bei der Nutzung des Übertragungsmediums „Sprechfunk“, bei dem man vor Betätigung der Sendetaste in die Sprechfrequenz hineinhören soll, um festzustellen, ob jemand auf dieser Frequenz sendet, stellt CSMA/CD dieselbe Prüfung im Netzwerk sicher. Falls doch zwei Workstations gleichzeitig Informationen senden, wird dies als **Kollision** bezeichnet. Die beteiligten Stationen versuchen nach unterschiedlichen Zeiten erneut, ihre Information abzusetzen. Die steigende Zahl der Nutzer in einem Ethernet-Netzwerk führt zu immer häufigeren Kollisionen. Daher werden große Netzwerke in viele in sich abgeschlossene Netzsegmente aufgeteilt, die Kollisionen minimieren helfen sollen.

Mit **Token Passing** („vorbeiziehender Zug“) bezeichnet man das Zugriffsverfahren im Token-Ring-Netzwerk. Da nur der Besitzer des Token sendeberechtigt ist, regelt sich die Zugriffsreihenfolge durch das Token-Prinzip (s. o.).

### 13.1.3 Aufbau und Organisation von vernetzten Systemen

Die erste und einfachste Vorstufe unserer heutigen Netzwerkbetriebssysteme waren so genannte **Disk-Server**. Ein PC wurde mittels eines speziellen Netzwerkbetriebssystems zum Disk-Server - große gemeinsame Festplatte - umgewandelt. Die Kunden (**Netzwerk-Clients** genannt) konnten mit verschiedenen Kommunikations- und Ankoppelungsverfahren, mittels unterschiedlicher Kabelverbindungen, auf die Daten des Disk-Servers zugreifen. Das größte Problem dieser Verbindung lag in der mangelhaften Kontrolle der Zugriffe und der Datennutzung. Die Weiterentwicklung der Betriebssysteme brachte die Möglichkeit, PCs auf gleichberechtigter Basis miteinander zu verbinden. Bei dieser Art der Verbindung spricht man von so genannten **Peer-to-Peer-Netzwerken**. Auch sie haben den großen Nachteil, dass die Zugriffskontrolle nur begrenzt möglich ist. Als Optimierung der Disk-Server und der Peer-to-Peer-Netzwerke sind so genannte **serverbasierte Netzwerkbetriebssysteme** entwickelt worden. Lange Zeit war die Firma **Novell** führender Anbieter von Netzwerksoftware. Microsoft hat aber auch in diesem Marktsegment mit seinen Netzwerk-Betriebssystemen **Windows NT**, **Windows 2000** und **Windows XP** den einstigen Marktführer Novell abgelöst. Als ein weiteres wichtiges Betriebssystem, das sehr gute Netzwerkfunktionalitäten besitzt und sich gerade im Serverbereich etabliert hat, ist **Linux** zu nennen, das hier stellvertretend für die gesamte „**Unix-Welt**“ genannt sein soll.

Ein serverbasiertes Netzwerkbetriebssystem besteht aus

- einem oder mehreren **Netzwerkservern**,
- einem **Netzwerkbetriebssystem** und
- mehreren **Workstation-PCs**, den Clients,

die mittels einer speziellen „**Client-Server-Software**“ mit dem Server kommunizieren können. In der einfachsten und gebräuchlichsten Netzwerkanwendung stellt ein File-Server (Zentralrechner mit einer großen Festplatte) seine Speicherkapazitäten allen Benutzern des Netzwerkes zur Verfügung. Voraussetzung ist, dass der jeweilige Nutzer einer Workstation von der Benutzerverwaltung des Netzwerkbetriebssystems erkannt und akzeptiert wird. Die Zugangs- und Zugriffskontrolle wird häufig durch das Netzwerkbetriebssystem sichergestellt.

Neben der klassischen File-Server Netzwerkanwendung gibt es eine Vielzahl weiterer sinnvoller Nutzungsmöglichkeiten für Netzwerkanwendungen, die von den gängigen Netzwerkbetriebssystemen entweder von Hause aus bereits enthalten sind oder mit Zusatzprogrammen gesondert geladen werden müssen.

Gerade diese beschriebene Bedeutung der Betriebssysteme, die den jeweiligen Anforderungen entsprechend bestimmte Leistungsmerkmale und Funktionalitäten mitbringen sollen, lässt erkennen, dass nicht allein die Wahl des Betriebssystems, sondern auch die Bereitschaft zur Weiterentwicklung ein wichtiges Maß für den erfolgreichen Betrieb eines Netzwerkes darstellt. In diesem Zusammenhang kommt es ganz besonders darauf an, nicht nur die reinen Anschaffungskosten für den Betrieb eines Netzwerkes zu kalkulieren, sondern z. B. auch die Kosten für fachliche Aus- und Weiterbildungen und mögliche oder absehbare Systemumstellungen bzw. -erweiterungen in die **Planung eines Netzwerkes** einzubeziehen.

Versteht man den gesamten komplexen Bereich der Informationstechnologie als einen Dienstleistungsbereich, so soll mit dessen Hilfe entweder eine Arbeitserleichterung oder eine Verbesserung der Arbeitsergebnisse angestrebt werden. Um dieses „Instrument“ jedoch sinnvoll einzusetzen, bedarf es immer mehr einer sorgfältigen Planung. Viele Firmen entschließen sich daher auch dazu, diese Planungen nicht allein durchzuführen, sondern erfahrene Berater-Firmen heranzuziehen, die sie bei entsprechenden Projekten, z. B. für die Konzeption, Einrichtung und den Betrieb eines Netzwerkes, unterstützen.

### Typische Server-Dienste

In der folgenden Tabelle werden die wichtigsten Server-Dienste dargestellt:

Wichtige Server-Dienste:	
<b>File-Server</b>	Ein zentraler PC mit einem Festplattenstapel dient als große, gemeinsame Festplatte für alle Nutzer des Netzwerkes. Man verwendet hierbei i. d. R. SCSI-Festplatten, deren Übertragungsgeschwindigkeit höher ist, da die Anzahl der Dateizugriffe im Netzwerk wesentlich höher ist als bei Einzelplatz-PCs.
<b>Print-Server</b>	Entweder ist auf einem File-Server ein zusätzlicher Print-Server installiert, oder ein eigenständiger PC dient als Print-Server. An ihm sind meist mehrere Drucker angeschlossen, die dann allen Nutzern des Netzwerkes zur Verfügung gestellt werden. Insbesondere für teure Farb-Laserdrucker bzw. Hochleistungsdrucksysteme werden Printserver eingesetzt. Print-Server-Boxen übernehmen heute die Aufgaben von Printservern. Mit ihnen kann ein handelsüblicher Drucker direkt mit einem Netzwerk verbunden werden und von allen Nutzern als Netzwerkdrucker installiert werden.
<b>Applications-Server</b>	Dieser Server stellt ein Anwendungsprogrammpaket in einem Unternehmen zentral zur Verfügung. Die Programme liegen nur zentral auf dem Applikationsserver. Der lokale Nutzer erhält die Programme und erforderlichen Daten über das Netzwerk. Die Arbeit für Programmupdates wird deutlich vereinfacht.
<b>CD-ROM-Server</b>	Einen PC, der mittels spezieller Festplattencontroller mit mehreren CD-ROM-Laufwerken ausgestattet ist und im Netzwerk verfügbar ist, bezeichnet man als CD-ROM-Server. Kataloge und Service-Dokumentationen können im CD-ROM-Server allen Mitarbeiterinnen und Mitarbeitern eines Unternehmens zur Verfügung stehen, ohne dass für jeden PC eine eigene CD vorhanden ist.

Wichtige Server-Dienste (Fortsetzung):	
<b>Mail-Server</b>	Ein Mail-Server übernimmt den zentralen Postverteildienst in einem Netzwerk. Ein externer Postversender schickt seine Mail an den Mail-Server. Dieser PC ist in der Regel immer erreichbar. Sobald der Postempfänger sich mit seinem PC im Netzwerk anmeldet, überstellt der Mail-Server automatisch die zwischenzeitlich empfangenen Mails.
<b>Web-Server</b>	Ein Web-Server ermöglicht den angeschlossenen „Clients“ die Verbindung ins <b>Internet</b> oder <b>Intranet</b> .
<b>Datenbank-Server</b>	Ein Server, der mit einem geeigneten Datenbankprogramm - z. B. SQL-Server der Fa. Oracle - große Datenbestände zentral verwaltet und verfügbar hält.
<b>Proxy-Server</b>	Ein solcher Server ist auf jedem PC mit Internetzugang in der Regel aktiv. Er speichert die Internetseiten zwischen. Beim erneuten Aufruf der Seite wird diese nicht aus dem Internet, sondern vom Proxy-Server gelesen. Ein „richtiger“ Proxy-Server übernimmt diese Service-Funktion innerhalb eines Netzwerkes. Die Zugriffe ins Internet werden reduziert und die Geschwindigkeit des Seitenaufbaus ist höher, da die Übertragungsgeschwindigkeit im Netzwerk wesentlich höher ist als direkt aus dem Internet.

#### 13.1.4 Sinn und Zweck vernetzter Systeme

Die unterschiedlichen Serverdienste, die in Netzwerken eingesetzt werden, machen den Sinn und Zweck vernetzter Systeme deutlich. Die gemeinsame Nutzung teurer Peripheriegeräte (**Ressource-sharing**), die gemeinsame Nutzung von Anwenderprogrammen (**Software-sharing**) sowie der gemeinsame Zugriff auf Datenbestände (**Data-sharing**) und die Verlagerung arbeitsintensiver Operationen auf spezielle Computersysteme sind klassische Gründe für den Einsatz von Netzwerken.

Durch die Festlegung von Zugriffsrechten wird die Datensicherheit erhöht. Es kommt zu einer Verbesserung der Benutzerführung. Der externe Zugriff auf einzelne Arbeitsplätze (**Remote-control**) ermöglicht Wartungsarbeiten an weit entfernten Client-PCs. Der Austausch von Nachrichten (**Electronic Mail**) ist die gebräuchlichste Anwendung in der Welt der Netzwerke.

Die folgenden Aspekte sind (hier als Zielvorstellungen formuliert) für viele Unternehmen ausschlaggebend, um in Netzwerktechnologien zu investieren:

- **Netzwerke fördern die Kommunikation** innerhalb der Unternehmen – gut informierte Mitarbeiterinnen und Mitarbeiter sind der Schlüssel für die Informationsgesellschaft.
- Netzwerke steigern die **Effektivität und Kreativität** der Mitarbeiter durch den Informationsverbund. Mitarbeiter, die über die ganze Welt verteilt sind, arbeiten an gemeinsamen Projekten. Alle Informationen stehen allen „Berechtigten“ im Netzwerk frei zur Verfügung.
- Netzwerke **schützen die Informationen** der Unternehmen durch effektive, standardisierte Datenschutz- und Datensicherungsmechanismen.
- Netzwerke **optimieren die IuK-Leistungen** (IuK – Informations- und Kommunikationstechnik) von Unternehmen.

Die Kommunikation innerhalb von Unternehmen und die Kommunikation zwischen den Unternehmen sind Grundlagen des globalen Handelns. Einzige Voraussetzung für die Teilnahme und Teilhabe am E-Business ist der Anschluss an das globale Datennetz.

## Kommunikation und Zusammenarbeit mit vernetzten Systemen

Eigentlich braucht man gar keine vernetzten Systeme. Viele Menschen sind auch heute noch dieser Auffassung. Sicher, man kann Daten auch per Diskette oder CD von einem Computer zum anderen transportieren. Das Kopieren mittels externer Datenspeicher ist möglich; aber ...!

Wie schafft man es, dass alle Mitarbeiter immer über einen aktuellen Datenbestand verfügen? Wie kann man Termine gemeinsam und zeitgleich bearbeiten? Wie ist das Auftragserfassungssystem immer auf dem Laufenden? Wie kann man große Dateien – größer als 1.4 MB – transportieren? Wie kann man gemeinsam an einem Projekt arbeiten, obwohl Mitarbeiter in Amerika und andere in Australien wohnen und arbeiten?

Die Art des Arbeitens am und mit dem Computer ändert sich, wenn man im Netzwerk arbeitet. Vielfach merkt der Anwender gar nicht, dass er an einem langen Kabel hängt. Die Art und Weise der Kommunikation zwischen den Mitarbeitern ändert sich nicht nur technisch. Ein funktionierendes E-Mail-System verändert die Kommunikation und die Zusammenarbeit nachhaltig. Zeit und Terminplanung sind wesentlich effektiver, weil der nächste freie Termin für alle Einzuladenden direkt ablesbar ist und die Einladung und Zusage elektronisch erfolgen kann.

Die Bereitschaft, Informationen zu teilen und frühzeitig allen Beteiligten zur Verfügung zu stellen, wird durch Netzwerke größer; erfordert aber einen Lernprozess bei allen Beteiligten. Die Weitergabe eines Ergebnisprotokolls per Fotokopie war und ist sehr aufwendig. Die Versendung desselben Protokolls mittels Anhängsel (Attachment) an einer E-Mail dauert nur Sekundenbruchteile. Jederzeit über alle wichtigen Informationen zu verfügen und diese in aktuelle Dateien mittels „Drag-and-Drop-Technik“ (Markieren-Kopieren-Einfügen zwischen unterschiedlichen Anwendungsprogrammen) einzubinden, vereinfachen die Büroarbeit um ein Vielfaches.

## Zentrale Benutzerverwaltung

Wer darf was im Netzwerk? Wie kann man verhindern, dass Unbefugte an meine geheimen Daten kommen? Wie kann man irrtümliche Löschungen von Unwissenden verhindern?

Die zentrale **Zugangskontrolle** eines Netzwerkbetriebssystems übernimmt genau diese Aufgaben. Die Benutzer eines Netzwerkes werden verschiedenen Gruppen zugeordnet. Rechte und Zuordnungen werden i. d. R. nicht auf Benutzerebene, sondern auf Gruppenebene zugewiesen. Durch dieses Verfahren ist die Administration (Wartung und Pflege) der Benutzerverwaltung sehr einfach und effizient.

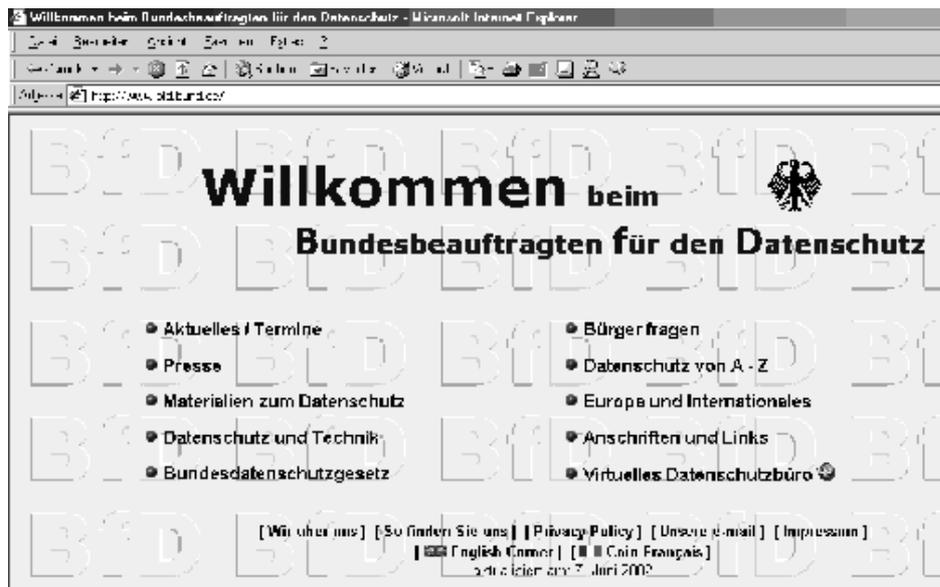
Ein weiterer entscheidender Vorteil einer zentralen Benutzerverwaltung ist die Tatsache, dass ein Anwender mit seinem „Login“ (Anmeldename und Passwort) sich an jedem beliebigen Rechner des Netzwerkes anmelden kann. Er erhält „seine“ Rechner-Umgebung (Desktopeinstellungen – Programmstruktur) und kann auf seine Daten zugreifen.

## Datenschutz, Datensicherheit und Datensicherung

Wer sich mit der Netzwerktechnik beschäftigt, muss sich neben den offensichtlichen Vorteilen, z. B. der zentralen Datenhaltung, auch Gedanken über die damit verbundenen möglichen Gefahren des Datenmissbrauchs machen. Hierzu werden im **Bundesdatenschutzgesetz (BDSG)** gesetzliche Regelungen getroffen, die nicht dem Schutz der Daten an sich, sondern dem Schutz des Bürgers vor missbräuchlicher Verwendung der über ihn gespeicherten Daten dienen.

Informationen können hierzu auf der Homepage des **Bundesbeauftragten für Datenschutz (BfD)** unter [www.bfd.bund.de](http://www.bfd.bund.de) abgerufen werden.

### Informationen zum Datenschutz:



Werden personenbezogene Daten automatisiert verarbeitet, so sind die folgenden **Kontrollarten des Datenschutzes** (auch häufig als die 10 Gebote des Datenschutzes bezeichnet) im Bundesdatenschutzgesetz festgeschrieben und machen bereits ansatzweise deutlich, wie wichtig dieses Thema ist und in welchen Bereichen der Datenschutz wirken kann.

### Kontrollarten des Datenschutzes:

- **Zugangskontrolle:** Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren,
- **Datenträgerkontrolle:** zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können,
- **Speicherkontrolle:** die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern,
- **Benutzerkontrolle:** zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können,
- **Zugriffskontrolle:** zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können,
- **Übermittlungskontrolle:** zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können,

**Kontrollarten des Datenschutzes (Fortsetzung):**

- **Eingabekontrolle:** zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind,
- **Auftragskontrolle:** zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können,
- **Transportkontrolle:** zu verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können,
- **Organisationskontrolle:** die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

Der Datenschutz, die Datensicherheit und die Datensicherung sind allerdings in vielen Unternehmen Stiefkinder der Datenverarbeitung. Hand aufs Herz, wann haben Sie die letzte Datensicherung Ihrer Textdateien erstellt? Verfügen Sie über Sicherungskopien aller Ihrer Programme? Wie viele Daten würde der Super-Gau Ihrer Festplatte in diesem Moment kosten?

Egal wie die Regelungen für die Datensicherung in Unternehmen auch organisiert sind, immer dann, wenn dem einzelnen Computernutzer die Aufgabe der Datensicherung und des Datenschutzes übertragen wird, gibt es ein hohes Sicherheitsrisiko. Das Problem besteht sehr häufig darin, dass dieses Risiko von den meisten Anwendern, aber auch (oder besonders) bei vielen Verantwortlichen, unterschätzt wird, da der Netzwerkbetrieb „ja bislang immer einwandfrei funktionierte“ und alle präventiven Maßnahmen zur Vermeidung eines größeren Schadens durch Datenverlust eher als „Zeitverschwendung“ angesehen werden und darüber hinaus auch noch Kosten verursachen.

In Netzwerken sollten allerdings planmäßig die Datenbestände des File-Servers ebenso wie die Datenbestände der Workstations zentral gesichert werden. Leistungsstarke Sicherungslaufwerke (Bandlaufwerke – Streamer-Tapes – Jazz-Laufwerke – CD-Brenner) können hierzu eingesetzt werden. Nach einem festgelegten **Sicherungskonzept** werden die Daten gesichert und an einem sicheren Ort aufbewahrt. Somit ist gewährleistet, dass Unternehmensdaten auch bei Datenverlusten rekonstruierbar sind und ggf. bei juristischen Auseinandersetzungen oder z. B. für mögliche spätere Regelungen mit Steuerbehörden verfügbar sind.

### 13.1.5 Einsatzgebiete für vernetzte Systeme

Die Einsatzgebiete von vernetzten Systemen sind nahezu grenzenlos. Der einzelne PC auf dem häuslichen Schreibtisch und das Notebook für unterwegs sind oft die Initialzündung für den Vernetzungswunsch. Das Netzwerk zwischen beiden Systemen ermöglicht die einfache Aktualisierung des Terminkalenders, die Übertragung der aktuell geänderten Adressdatenbank bzw. der Auftragsdatenbank.

Die Computer des Vorgesetzten und seiner Mitarbeiter können als kleines vernetztes System zum Überspielen von Textdateien, zum Mailing, zur Verwaltung eines gemeinsamen Datenpools, zur Nutzung gemeinsamer Vorlagen und Vordrucke usw. dienen. Sie sehen, ein Netzwerk bietet schon in einem 2-Personen-Office eine schier unerschöpfliche Ideenquelle für die Organisation.

Was für zwei gut ist, entlastet kleine und mittelständische Unternehmen erst recht. Hier kommen weitere Vorzüge hinzu. In Handelsunternehmen werden so genannte geschlossene **Warenwirtschaftssysteme** geschaffen. Ein Artikel ist somit im Netzwerk von der Beschaffung bis zum Verkauf jederzeit verfügbar, d. h. sein Aufenthaltsort mit jeweiligem Status und entsprechendem „Sachbearbeiter“ ist sofort abrufbar.

Komplexe **betriebswirtschaftliche Programmpakete** für die Bereiche – Produktionsplanung – Lagerhaltung – Auftragsbearbeitung – Finanzbuchhaltung – Lohn- und Gehaltsbuchhaltung – Management-Informationssysteme usw. sind erst im Zusammenspiel eines Netzwerkes effektiv.

Die Schaffung eines **Intranet** (firmeninternes Internet), das nur von den Mitarbeitern und Angehörigen des Netzwerkes genutzt werden kann, wird von vielen Unternehmen als Meilenstein in der Netzwerknutzung bezeichnet. Das Intranet kann demnach Firmeninterna von der Geburtstagsliste über aktuelle Projektentwicklungen bis zur interaktiven Mitarbeiterfortbildung beinhalten und führt gekoppelt mit speziellen Softwarepaketen sogar hin zu einer „gläsernen Firma“, die zu jedem Zeitpunkt z. B. auch die Arbeitszeitbelastungen, Gehälter und besonderen Fähigkeiten (Skills) der Mitarbeiter preisgibt.

Bevor auf die sicherlich deutlich gegebenen Vorteile eines Intranet hingewiesen wird, soll an dieser Stelle aber auch betont werden (und das gilt grundsätzlich für alle Netzwerke), dass neben dem sicheren Umgang mit den Daten und der Informations-Philosophie der Firma an sich, besonders auf den **administrativen Aufwand** und die Pflege eines solchen Netzwerkes geachtet werden muss. Als Stichwort sei in diesem Zusammenhang nur die „**Aktualität der Daten**“ angesprochen, denn wie im Internet auch hängt die Akzeptanz und die Häufigkeit der Nutzung sehr stark von der Aktualität der bereitgestellten Informationen ab und es schließt sich sofort die Frage an, wer für diese Informationen verantwortlich ist und wer die Daten entsprechend pflegt.

Trotz der soeben angesprochenen Einschränkungen bzw. Punkte, die es zu beachten gilt, liegen die Vorteile eines Intranet auf der Hand:

- Die Internet-Technologie macht es möglich, dass auf zentral gelagerte Datenbestände von den unterschiedlichsten Betriebssystemen her zugegriffen werden kann.
- Mit **Java** (einer objektorientierten Programmiersprache für das Internet) gibt es eine Sprache, die es ermöglicht, umfangreiche Programme zu schreiben, die plattformübergreifend (auf PCs, Apple, im Bereich der mittleren Datentechnik und auf Großrechnersystemen) einsetzbar sind.
- Da in die Entwicklung der Internet-Technologien viel Idealismus gesteckt wurde und mit der Hoffnung auf und in die Zukunft gearbeitet wurde, stehen für die verschiedensten Anwendungsbereiche preiswerte Software-Produkte zur Verfügung, deren Quellcode oft direkt verfügbar ist.
- Der Einsatz von Internet-Technologien erzeugt einen starken Trend (bzw. den Versuch) zur Vereinheitlichung. Gemeint ist damit das sinnvolle Prüfen und Einsetzen der immer weiterentwickelten oder neuen Produkte (Hardware und Software). Wenn in allen Segmenten eines innerbetrieblichen Netzwerkes z. B. dieselben Browser und dieselben Übertragungsprotokolle verwendet werden, dann reduziert sich u. a. der nötige Schulungsaufwand für die Mitarbeiterinnen und Mitarbeiter.

## 13.2 Installation von Netzwerken

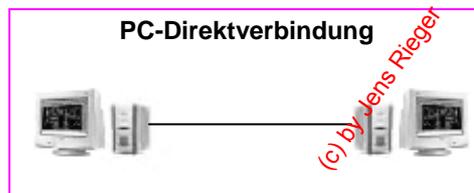
Nachdem einige theoretische Grundlagen der Vernetzung von Computersystemen behandelt worden sind (die, wie bereits zu Beginn des Kapitels erwähnt, nicht zwingend zur hier beschriebenen praktischen Durchführung durchgearbeitet werden müssen), wollen wir an dieser Stelle die Installation verschiedener privater Netzwerke vorstellen. Dabei soll zunächst auf eine Direktverbindung zweier PCs und dann auf die Erweiterung zu einem Peer-to-Peer-Netzwerk eingegangen werden.

Ein wichtiger Grundsatz soll dabei sein, die unterschiedlichen (zurzeit gebräuchlichen) Betriebssysteme in ein Netzwerk aufzunehmen und nicht von einer „reinen Windows XP- oder Windows 2000-Welt“ auszugehen, die es in der Praxis ja häufig nicht gibt. So haben wir dann auch berücksichtigt, dass es trotz ständig wachsender Verbreitung des derzeit aktuellen Betriebssystems Windows XP z. B. noch eine Vielzahl von Windows 98- oder Windows ME-Systemen gibt, die ebenfalls ihre Berechtigung haben und durchaus geeignet sind für den Aufbau und den Betrieb eines stabilen (privaten) Netzwerkes.

Voraussetzung für die Installation eines Netzwerkes ist grundsätzlich eine gute Planung. Das heißt nicht, dass sich diese über Tage hinziehen, viel Literatur gewälzt und eine Menge Papier beschrieben sein muss. Allerdings sollten die Anforderungen an das Netzwerk insofern gestellt sein, als dass sich der Einsatz der notwendigen Hard- und Software auch lohnt.

### 13.2.1 Direktverbindung zweier PCs

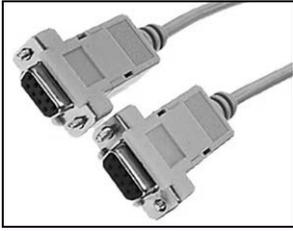
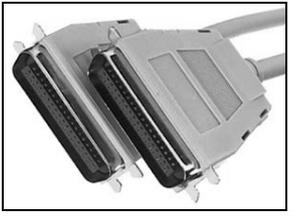
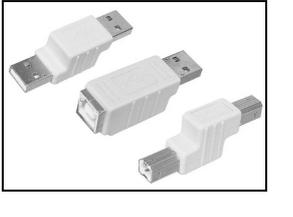
Die Direktverbindung zweier PCs ist im Grunde bereits ein Peer-to-Peer-Netzwerk, da beide PCs gleichberechtigt sind. Allerdings stellt es bei dem Einsatz von seriellen oder parallelen Verbindungskabeln (den so genannten „Nullmodem-Kabeln“) eine besondere Form dar, weil für eine solche Verbindung keine Netzwerkkarten vorhanden sein müssen.



Für eine PC-Direktverbindung werden jedoch spezielle Kabel verwendet. Selbst, wenn diese Kabel die gleiche oder ähnliche Form und Anschlüsse aufweisen wie andere Netzwerkkabel, so ist doch die Kabelbelegung und die damit verbundene Signalzuweisung auf diesen speziellen Fall der Computerverbindung abgestimmt. Wie der dazugehörige Name „Crossover“ bereits andeutet, handelt es sich dabei um „verdrehte“ bzw. „gekreuzte“ Leitungen, die bei einem Einsatz als „normale Patchkabel“ schon so manches Netzwerk oder Teile davon (zumindest für die Zeit bis zum Erkennen dieses Irrtums) lahmgelegt haben.

Als dritter wichtiger Punkt ist noch die für diesen Sonderfall notwendige Software (z. B. *Interlink* oder *Laplink*) hinzuweisen, ohne die beide PC nicht wüssten, wie sie miteinander Daten austauschen können.

Folgende Kabelalternativen stehen für eine Direktverbindung zweier PCs zur Verfügung:

	<p><b>Seriellles Verbindungskabel/Nullmodem</b></p> <p>Das serielle Verbindungskabel dient zur Kopplung zweier Datenendeinrichtungen, wobei die Schnittstellenleitungen für die Nutz- und die Steuerdaten über Kreuz geführt werden.</p>
	<p><b>Paralleles Computer-Verbindungskabel</b></p> <p>Diese noch immer verwendete Leitung ist gut für den Einsatz von <i>Interlink</i> und ähnlichen Anwendungen geeignet, mit denen ohne zusätzliche Hardware (wie z. B. Netzwerkkarten) Daten von einem PC zum anderen übertragen werden können.</p>
	<p><b>USB-Kabel</b></p> <p>Die geringe Übertragungsgeschwindigkeit der seriellen Schnittstelle war für die Maus und das Modem zwar ausreichend, moderne Peripheriegeräte erfordern schnellere Verbindungen. Daher wurde von einigen führenden IT-Firmen gemeinsam der Universal Serial Bus (USB) entwickelt, der heute in fast allen Geräten vorhanden ist. Er kann Daten theoretisch mit 12 Megabyte pro Sekunde (USB 1.1) bzw. 480 Mbit/s (USB 2.0) transportieren und ist damit wesentlich schneller als die bisherigen seriellen Schnittstellen.</p> <p>Außerdem können bis 127 Geräte wie Tastatur, Maus, Modem, ISDN- oder analoge Telefone und Telefonanlagen, Scanner oder digitale Kameras daran angeschlossen werden.</p>
	<p><b>Patchkabel RJ-45</b></p> <p>Hierbei handelt es sich um kurze Twisted-Pair-Verbindungskabel (TP-Kabel), die in unterschiedlichen Längen (0,5 m; 1 m; 2 m; 5 m; 10 m) erhältlich sind.</p> <p>Die speziellen Patchkabel (Crossover-Kabel) werden verwendet, wenn nur zwei PCs miteinander vernetzt werden sollen.</p>

Bei einer PC-Direktverbindung können also zwei Personalcomputer ohne zusätzliche Geräte miteinander verbunden werden. Diese Verbindungsgeräte, z. B. ein Hub oder ein Switch, müssen erst dann verwendet werden, wenn mehr als zwei Computer miteinander verbunden werden sollen.

### Serielle und parallele PC-Direktverbindung

Von den oben dargestellten Kabeltypen geraten die beiden erstgenannten (das serielle und das parallele Verbindungskabel) zunehmend in den Hintergrund. Diese werden häufig nur noch dann eingesetzt, wenn auf älteren Systemen Probleme auftreten und eine Datensicherung vorgenommen werden soll, die die Kapazität von Disketten übersteigt. Für den Einsatz eines seriellen oder parallelen Crossover-Kabels ist nämlich kein Windows-Betriebssystem notwendig. Die zum Datenaustausch notwendigen Programme sind so klein, dass sie auf eine Diskette passen und somit z. B. in Verbindung mit einer Startdiskette ermöglichen, dass Daten von einem PC zu einem anderen PC übertragen werden können. Beispielhaft sei hier die Verbindung zweier PCs über den Parallel-Port mit einer MS-DOS-Version ab 6.0 und den beiden Programmen *Interlink* und *Interserver* angesprochen. Der große Nachteil dieser Verbindungen besteht allerdings in ihrer geringen Datenübertragungsrate. Während diese bei einer seriellen PC-Direktverbindung theoretisch bis zu etwa 100 kBit/s und bei einer parallelen ca. 700 kBit/s betragen kann, so bietet eine Verbindung mittels 10/100 MBit-Netzwerkkarte die Möglichkeit wesentlich kürzerer Datenübertragungszeiten.

Die aufgeführten Werte zu den verschiedenen Verbindungsarten stellen theoretische Angaben dar, praktisch lassen sich folgende Vergleichswerte angeben, um z. B. eine Datei mit der Größe von 1 MByte zu übertragen:

Serielle PC-Direktverbindung	Parallele PC-Direktverbindung	Netzwerkkarten (100 MBit/s)-PC-Verbindung
ca. 6 Minuten	ca. 50 Sekunden	ca. 0,3 Sekunden

Unter dem oben angeführten Aspekt der langen Übertragungszeiten und der wohl gesicherten Annahme, dass es sich bei der Datenübertragung häufig um größere Datenmengen als einmalige 1 MByte große Dateien handelt, wollen wir hier auf eine interessante Alternative einer PC-Direktverbindung eingehen, ohne extra Netzwerkkarten einbauen zu müssen.

### PC-Direktverbindung mit USB

Im Vergleich zu der seriellen und parallelen PC-Direktverbindung sind hier weitaus höhere Datenübertragungsraten möglich (die Übertragung der 1 MByte großen Datei aus dem obigen Beispiel dauert dann nur ca. 5 Sekunden). Es gibt jedoch verschiedene Möglichkeiten für eine USB-Verbindung, sodass beim Kauf eines dafür notwendigen USB-Kabels (häufig als *USB-Link* oder *USB Net Cable* bezeichnet) darauf geachtet werden muss, welche Funktionalität jeweils unterstützt bzw. für welchen Anwendungsfall das Kabel vorgesehen ist. Einerseits kann die USB-Verbindung in Windows integriert werden, andererseits gibt es ein USB-Kabel mit dazugehöriger Software, die zusammen sozusagen ein eigenes USB-Netzwerk darstellen.

Der letztgenannte Fall zur PC-Direktverbindung lässt sich sehr einfach durchführen und wird hier deshalb kurz aufgezeigt:

Notwendig ist ein spezielles USB-Link-Kabel (3 Meter lang), das etwa in der Mitte über einen USB-Chip (Bridge) verfügt und an beiden Enden USB-Stecker vom Typ A aufweist, die dann jeweils direkt an die zu verbindenden PCs angeschlossen werden können, ohne dass diese geöffnet werden müssen. Ein weiterer großer Vorteil besteht darin, dass diese Verbindung im laufenden Betrieb durchgeführt werden kann, d. h., die zu verbindenden PCs brauchen beide nicht heruntergefahren und neu gestartet zu werden.

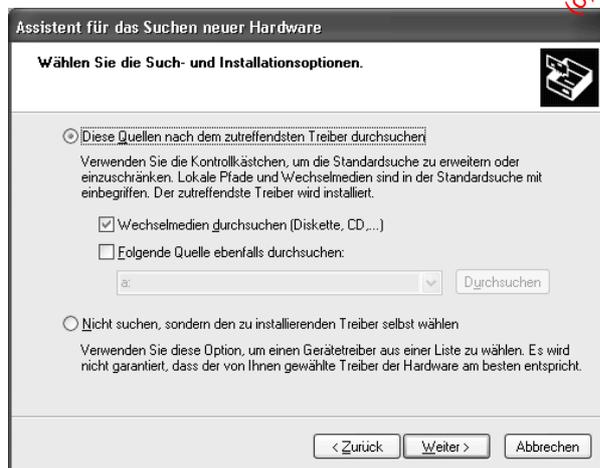
Außerdem können auf den PCs durchaus unterschiedliche Windows-Betriebssysteme vorhanden sein. In unserem Beispiel handelt es sich um Windows XP und Windows ME.

### Bearbeitungsschritte:

- Stellen Sie die zu verbindenden PCs (oder wie in diesem Beispiel PC und Laptop) so zueinander auf, dass Sie das USB-Kabel problemlos an beide PCs anschließen können. Verwenden Sie dazu die freien USB-Anschlüsse an der Frontseite oder Rückseite des PCs.
- Schließen Sie das USB-Kabel während des laufenden Betriebes an beiden PCs an oder starten Sie die PCs nach erfolgtem Anschluss neu.
- Der Hardware-Assistent erscheint, da das neue USB-Gerät automatisch erkannt wird. Aktivieren Sie den Radio-Button **Software von einer Liste oder bestimmten Quelle installieren** und klicken Sie auf die Schaltfläche **Weiter**.



- Klicken Sie auf die Schaltfläche **Weiter**, wenn sich der dem USB-Link-Kabel beigelegte Treiber auf einer CD oder Diskette befindet und diese eingelegt ist, oder wählen Sie den entsprechenden Ort des Treibers aus (z. B. nach dem Kopieren auf die Festplatte) und klicken dann auf die Schaltfläche **Weiter**.



**Bearbeitungsschritte (Fortsetzung):**

- Es erscheinen darauf die Meldungen, dass die Software für ein neues USB-Gerät gesucht und dann installiert wird.



- Die Installation kann durch eine Windows-Warnmeldung unterbrochen werden, da das Betriebssystem erkennt, dass möglicherweise einige VB-Programmteile (Programmabschnitte in der Programmiersprache **Visual Basic**) angepasst werden.



- Setzt man die Installation fort, so wird ein **Wiederherstellungspunkt** gesetzt, durch den das System wieder auf den jetzt aktuellen Stand zurückgesetzt werden kann.

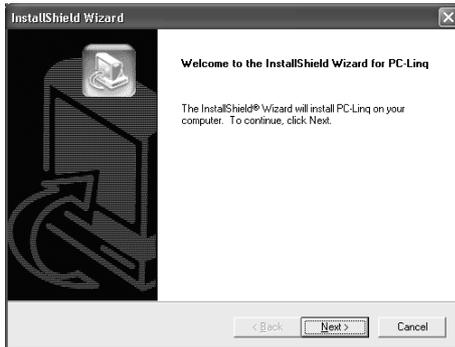


© by Jens Rieger

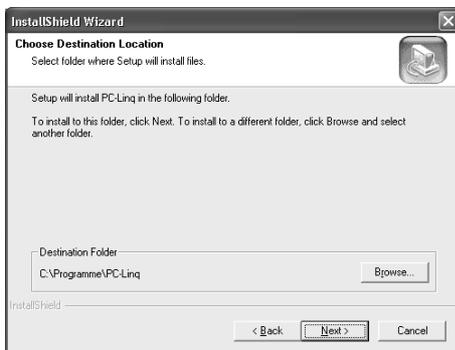
Der Treiber für diese PC-Direktverbindung wurde somit installiert, in der Regel sind die beige-fügten Programme so ausgelegt, dass die noch ausstehende Installation der Software (zum Bedienen bzw. Nutzen der eingerichteten Verbindung) automatisch gestartet wird. Sollte dies nicht erfolgen, so ist das entsprechende (Setup-) Programm manuell zu starten.

### Bearbeitungsschritte:

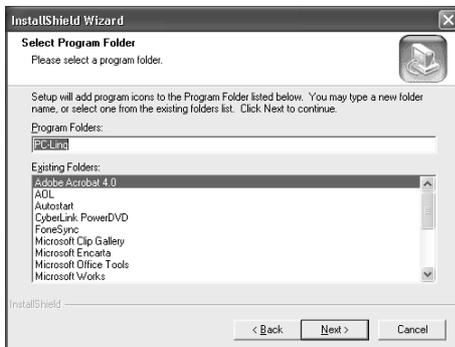
- Klicken Sie bei dem **InstallShield Wizard**, der Sie bei der zu installierenden Software unterstützen soll, auf die Schaltfläche **Next**.



- Sie können den vorgegebenen Zielordner, in den zu kopierende oder zu installierende Dateien abgelegt werden sollen, übernehmen oder einen eigenen Ordner wählen bzw. erstellen, indem Sie auf die Schaltfläche **Browse** klicken.



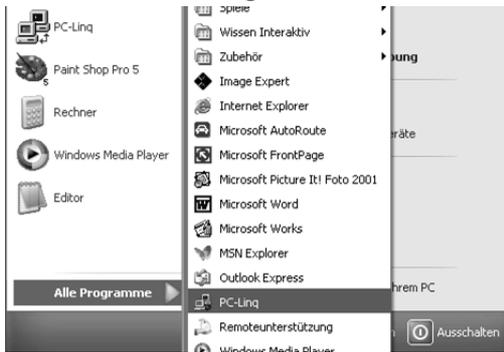
- Nach dem Klicken auf die Schaltfläche **Next** werden Sie aufgefordert, einen Programmordner auszuwählen, dessen Name Sie übernehmen oder selbst wählen können.



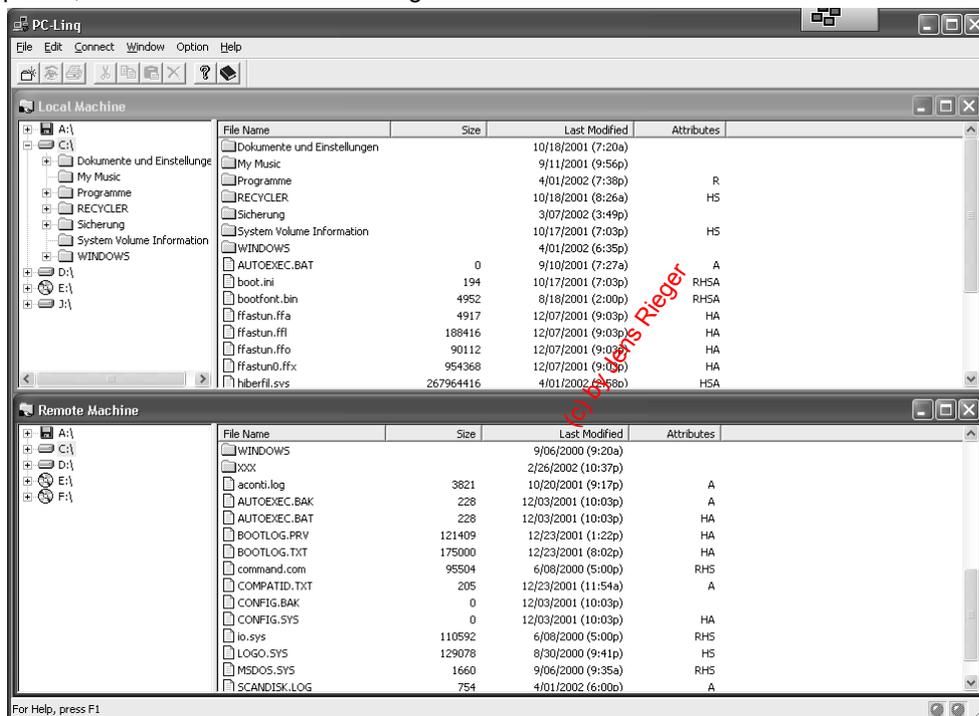
Die Installation ist damit abgeschlossen und Sie können das Programm zur Nutzung der PC-Direktverbindung (hier PC-Linq) aufrufen.

**Bearbeitungsschritte (Fortsetzung):**

- Klicken Sie auf die Schaltfläche **Start** und die Direktauswahl zu **PC-Linq** oder auf die Schaltfläche **Alle Programme** und dann **PC-Linq**.



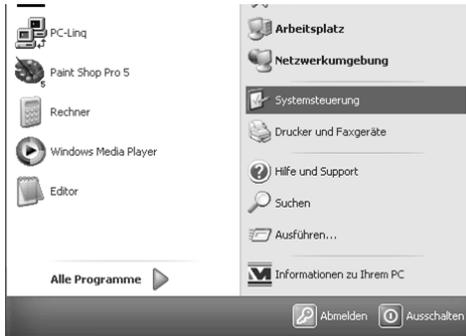
- Sie erkennen zwei Bereiche, die einen Zugriff auf den eigenen PC (**Local Machine**) und den angeschlossenen PC (**Remote Machine**) ermöglichen. So können Sie (vergleichbar mit dem Windows-Explorer) Dateien von einem PC auf den anderen PC kopieren, um z. B. eine Datensicherung vorzunehmen.



Anhand der Programmdarstellung lässt sich bereits erkennen, dass es sich bei dieser Lösung zur Verbindung zweier PCs noch um keine umfangreiche Netzwerkfunktionalität im eigentlichen Sinne handelt. Verdeutlichen lässt sich diese Aussage durch die folgend dargestellte Überprüfung:

### Bearbeitungsschritte:

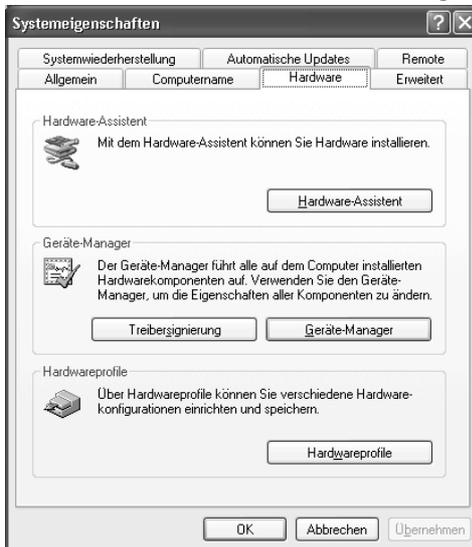
- Rufen Sie den Hardwareassistenten auf, indem Sie nacheinander auf die Schaltflächen **Start – Systemsteuerung ...**



- ... und dann auf **System** klicken.



- Wählen Sie in den Systemeigenschaften das Registerblatt **Hardware** und klicken Sie dort auf die Schaltfläche **Geräte-Manager**.



(c) by Jens Rieger

**Bearbeitungsschritte (Fortsetzung):**

- Klicken Sie auf das Pluszeichen vor dem USB-Symbol  und Sie erkennen dort die neue PC-Verbindung als **USB Bridge Cable** (und nicht als Eintrag unter den Netzwerkkarten bzw. Netzwerkadaptern).

**Einbau und Einrichtung einer Netzwerkkarte**

In der einleitenden Beschreibung zu dieser einfachsten Verbindung zweier PCs wurde bereits darauf hingewiesen, dass für den Fall eines Crossover-Patchkabel-Einsatzes eine **Netzwerkkarte** notwendig ist. Da diese auch eine Voraussetzung für die nachfolgend behandelten Netzwerke darstellen, soll bereits hier kurz auf diese wichtige Netzwerkkomponente eingegangen werden.

Die Netzwerkkarte ist eine Zusatzkarte, die in einen Einsteckplatz des PCs eingebaut werden muss. Man verwendet für einfache Anwendungen so genannte Ethernet Karten, die es sowohl als PCI- bzw. ISA-Steckkarten gibt. Die Übertragungsrate der Karten wird in Megabit pro Sekunde (**MBit/s** oder in der internationalen Schreibweise **mbps**) angegeben. In der Bezeichnung von Netzwerkkarten findet man daher häufig die Kurzform MBit. Mit einer 10 MBit-Karte zum Preis von ca. 10 € können maximal 1,25 MByte pro Sekunde übertragen werden. 100 MBit-Karten für ca. 20 € haben einen Datendurchsatz von ca. 12,5 MByte pro Sekunde. Eigentlich reichen für kleine Netzwerke 10 MBit-Karten völlig aus, gäbe es nicht z. B. die sehr datentransferhungrigen Computerspiele. Beim Kauf eines neuen PCs sollte man die wenigen Euro für eine Netzwerkkarte gleich investieren, auch wenn man noch nicht an Netzwerke denkt. Der Selbsteinbau ist von jedem Laien leistbar.

**Bearbeitungsschritte:**

- Schalten Sie den PC aus und ziehen Sie alle Kabelverbindungen ab. Bevor Sie das Gehäuse aufschrauben, fassen Sie einmal an einen Heizkörper oder verwenden Sie ein Antistatik-Armband aus dem Fachhandel, um die evtl. vorhandene statische Aufladung abzubauen. Das schützt die sensiblen Bauteile vor statischer Überspannung.
- Suchen Sie einen freien PCI oder ISA-Steckplatz (PCI sind kleinere weiße Steckplätze und ISA die etwas größeren schwarzen Steckplätze, die auf neueren Mainboards allerdings i. d. R. nicht mehr zu finden sind.). Öffnen Sie die Blende und schieben die Netzwerkkarte in den Steckplatz hinein. Wichtig ist, dass sie parallel eingesteckt ist. Verschrauben Sie die Karte.

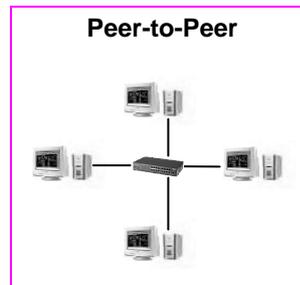
**Bearbeitungsschritte (Fortsetzung):**

- Verschließen Sie das Gehäuse und schließen Sie die Kabelverbindungen wieder an.
- Bevor Sie den PC wieder einschalten, prüfen Sie, ob die Diskette bzw. CD, die mit der Netzwerkkarte ausgeliefert wurde, bereitliegt. Wenn Sie den PC jetzt einschalten, dann wird die Karte durch „Plug-and-Play“ erkannt. Das System fordert die Aktualisierung des Treibers an. Liegt die Diskette bzw. CD im Laufwerk, dann erfolgen alle erforderlichen Schritte automatisch.
- Sollte das Betriebssystem die Netzwerkkarte nicht automatisch erkennen, dann wird es etwas schwieriger. Wechseln Sie in die Systemsteuerung. Rufen Sie die Hardwareerkennung auf und wählen sie den Unterpunkt „Netzwerkkarte“ aus. Sie können zwar aus der Liste der aufgeführten Treiber den vermeintlich richtigen Treiber auswählen, da die Treiberversionen aber häufig modifiziert werden, ist die mitgelieferte Diskette oder CD empfehlenswert bzw. die Aktualisierung aus der Treiberdatenbank des Herstellers im Internet. Klicken Sie die Schaltfläche „Diskette“ an; wenn die Diskette im Laufwerk liegt, wird in der Regel die Treiberinformation der dazugehörigen Karte angezeigt. Markieren Sie die Karte und klicken Sie auf weiter. Das Betriebssystem wird nun automatisch den Treiber installieren. Gegebenenfalls müssen Sie die Windows-Installations-CD einlegen, weil zusätzliche Komponenten erforderlich sind.
- Starten Sie den Rechner neu. Wechseln Sie erneut in die Systemsteuerung, wählen Sie den Bereich **System** aus und dort den **Gerätemanager**. Wenn die Karte richtig installiert ist, dann ist die Netzwerkkarte weder rot noch gelb gekennzeichnet.
- Nun haben Sie eine installierte Netzwerkkarte. Nach dem Neustart des PCs taucht vielleicht zum ersten Mal das nebenstehende Icon „Netzwerkumgebung“ auf der Desktop-Oberfläche auf.

**13.2.2 Einrichtung eines Peer-to-Peer-Netzwerkes**

Der Begriff **Peer-to-Peer** (häufig auch **P2P** abgekürzt) steht in diesem Zusammenhang für eine Gruppe von Computern, die **gleichberechtigt** zu einem Netzwerk zusammengeschlossen sind. In diesem Punkt besteht der wesentliche Unterschied zu einem **Client-Server**-basierten Netzwerk, denn gleichberechtigt bedeutet hier, dass jeder PC sowohl Serverfunktionen übernehmen als auch als Client dienen kann.

Seit der Version Windows 3.1 können alle IBM-kompatiblen PCs diese Form der Vernetzung verwenden. Die Folgeversionen von Windows haben diese Verbindungsmöglichkeit weiter perfektioniert. Sofern man lediglich ca. 10 PCs miteinander verbinden will, um gemeinsam auf Daten und Peripheriegeräte zuzugreifen, ist dies eine praktikable Lösung, die nicht nur im Privatbereich häufig verwendet wird.



War der einzelne PC im Privathaushalt noch vor wenigen Jahren eine Seltenheit, so gehört er in fast jedem Haushalt heute zur Standardausrüstung. In den ersten Jahren wurde der PC für den Vater gekauft und von den Kindern mitbenutzt, dies gehört zum Teil bereits der Vergangenheit an. In immer mehr Haushalten befinden sich mehr als ein PC; und genau dann beginnen die Überlegungen auch im Privatbereich, eine sinnvolle Verbindung zwischen den einzelnen PCs herzustellen. Die gemeinsame Nutzung von Modem bzw. ISDN-Karte oder eines Druckers bzw. die Sicherung der Daten auf einem speziellen Sicherungs-PC (Backup-System) und nicht zuletzt die Möglichkeit von Netzwerkspielen, stellen sinnvolle Anwendungsbeispiele dar.

### Protokoll und Kommunikation

Damit unterschiedliche Geräte oder verschiedene Software-Produkte zusammenarbeiten können, muss es Konventionen (Vereinbarungen) geben, die von den beteiligten Geräten verstanden und eingehalten werden. Die Konventionen werden festgelegt, indem nationale und internationale Normungsgremien beraten und Entschlüsse fassen. Die Festlegungen, die in den Gremien getroffen werden, werden zu Protokollen zusammengefasst. Die grundlegenden Netzwerkprotokolle (zum Beispiel **NetBEUI** oder **TCP/IP**) werden wie Treiber in den Hauptspeicher geladen. Protokolle kommen insbesondere bei der Datenfernübertragung (DFÜ) und in Netzwerken zum Einsatz. NetBEUI ist die Abkürzung für *Netbios Extended User Interface*. Damit ist ein auf Netbios aufgesetztes Protokoll gemeint, das 1985 von IBM eingeführt wurde. Die Identifikation der einzelnen PCs im Netzwerk erfolgt über eindeutige Netzwerknamen. Nur mit dem Protokoll NetBEUI ist es möglich, alle im Netzwerk befindlichen Netzwerkcomputer in der Netzwerkumgebung von Windows zu sehen. Ist das Protokoll NetBEUI nicht geladen, dann kann zwar die Netzwerkkommunikation über andere Protokolle erfolgen, die Anzeige der Netzwerkrechner ist jedoch nur mittels NetBEUI möglich.

Neben NetBEUI ist für die Kommunikation im Internet das Protokoll **TCP/IP** (**T**ransmission-**C**ontrol-**P**rotocoll/**I**nternet-**P**rotocoll) erforderlich. Die folgenden Schritte zeigen, wie einfach das Hinzufügen von Protokollen ist. Die Geschwindigkeit – die Performance – leidet in der Regel nicht unter dem Laden mehrerer Protokolle.

### IP – Adressen, geheimnisvolle Zahlenfolgen

Abgeleitet aus dem Namen handelt es sich hier also um **Internet-Protokoll-Adressen**. Das Internet als größtes Netzwerk basiert auf dem Prinzip, dass jeder Rechner – in der Anfangsphase handelte es sich bei den Internet-Computern nur um Großrechner-Systeme – eine eindeutige Nummer hat. Das heißt nicht, dass die jeweilige IP-Nummer für alle Rechner immer gleich bleiben muss; wichtig ist allerdings, dass zu keinem Zeitpunkt zwei gleiche IP-Adressen vorhanden sein dürfen, damit immer erkennbar ist, um welchen Rechner es sich bei einer Kommunikation im Netzwerk handelt.

Diese Identifikationsnummern bestehen aus vier Zahlenblöcken, die jeweils durch einen Punkt voneinander getrennt werden (z. B. 192.168.0.1). Nun wird in der digitalen Welt des Computers grundsätzlich mit den Werten 0 oder 1 gearbeitet (dem **dualen Zahlensystem**), während wir Menschen uns jedoch lieber in der uns vertrauten Welt des **dezimalen Zahlensystems** bewegen. Zur Erklärung der IP-Adressen wollen wir hier jedoch eine kurze Umrechnung durchführen, denn die bereits angesprochenen vier Zahlenblöcke bestehen genauer gesagt aus jeweils 8 Bit (also insgesamt 32 Bit) und lassen sich daher dem oben gewählten Beispiel entsprechend wie folgt darstellen (z. B. 11000000.10101000.00000000.00000001). Zur besseren Übersicht sind in der folgenden Tabelle noch einmal beide Schreibweisen dargestellt.

### Darstellung der gleichen IP-Adresse in verschiedenen Zahlensystemen (Bsp.):

Im dezimalen Zahlensystem:	192	168	0	1
Im dualen Zahlensystem:	11000000	10101000	00000000	00000001

Zur Kontrolle der aufgeführten Zahlenwerte können Sie für jede 8-Bit-Zahlenfolge folgende einfache Umrechnung durchführen:

### Bearbeitungsschritte:

- Notieren Sie die folgende Tabelle, die sich aus dem dualen Zahlensystem ergibt ...

128	64	32	16	8	4	2	1

- und tragen Sie die 8 Bit aus der dualen Zahlenfolge in die zweite Zeile der Tabelle ein (hier ist es der erste Zahlenblock aus dem obigen Beispiel).

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

- Multiplizieren Sie nun die Zahlen spaltenweise ( $128 \times 1$  und  $64 \times 1$  usw.) und bilden Sie die Summe aus all diesen Einzelwerten ( $128 + 64 + 0 + 0 + 0 + 0 + 0 + 0 = 192$ ). Sie erkennen, dass Ihr Ergebnis dem Zahlenwert aus dem dezimalen Zahlensystem entspricht (hier: 192) und können diese Umrechnung zur Kontrolle nun auch für die anderen 8-Bit-Blöcke durchführen.

Ein weiteres wichtiges Ergebnis wird aus der dargestellten Umrechnung deutlich, denn der maximale „Wertebereich“ (von dual geschrieben 00000000.00000000.00000000.00000000 bis 11111111.11111111.11111111.11111111) ergibt einen theoretischen Adressbereich in dezimaler Schreibweise von **0.0.0 bis 255.255.255.255**). Bei dieser Schreibweise betrachten wir die 8-Bit-Blöcke jeweils einzeln und erkennen, dass der Wertebereich von 0 bis 255 genau 256 Zahlen entspricht, d. h. vereinfacht  $2^8 = 256$ . Wollen wir nun also wissen, wie viele Adressen in dem uns vorgegebenen Rahmen überhaupt vergeben werden können, so nehmen wir die duale Schreibweise (und einen Taschenrechner) zur Hilfe und berechnen für alle 32 Bit (4 Blöcke mit jeweils 8 Bit) den Wert in dezimaler Schreibweise zu  $2^{32} = 4294967296$ . Wir könnten demnach theoretisch über 4 Milliarden verschiedene IP-Adressen vergeben. In der Praxis stoßen wir hier allerdings auf Probleme, da diese Adressen in verschiedene Netze aufgeteilt wurden und diese bereits in großer Anzahl vergeben worden sind.

Gehen wir bei unseren Betrachtungen weiterhin vom Internet aus, so kann jeder im Internet verfügbare Computer – auch **Host** genannt – über seine IP-Nummer eindeutig identifiziert werden. Genau so verhält es sich grundsätzlich auch in einem LAN, allerdings gibt es für die Einrichtung und Nutzung eines privaten Netzwerkes die Besonderheit, dass bereits bestimmte IP-Adressen (Adressbereiche) frei verfügbar sind, und zwar unabhängig davon, ob die gleichen Adressen an irgendeiner anderen Stelle der Welt bereits genutzt werden.

Solange diese Rechner in privaten Netzwerken arbeiten, also ohne eine direkte Verbindung zum Internet dem „Rest der Welt“ unbekannt sind, gilt ja auch immer noch der Grundsatz, dass in einem Netzwerk nicht zwei gleiche IP-Adressen vorkommen dürfen.

Folgende private IP-Netze wurden festgelegt:

Private IP-Netze:		
10.0.0.0	bis	10.255.255.255
172.16.0.0	bis	172.31.255.255
192.168.0.0	bis	192.168.255.255

### Subnet Mask

Zur Beschreibung eines Netzwerkes gehören i. d. R. allerdings nicht nur die Adressen der einzelnen Rechner, die so genannten **Host-IDs**, sondern auch die Erkennungsnummer des Netzwerkes selber, die **Netzwerk-ID** (oder auch Net-ID genannt).

Dazu wird die IP-Adresse in zwei verschiedene Bereiche aufgeteilt, die jedoch in der jeweiligen Größe variieren können. Um eine Zuordnung treffen zu können, benutzt man die **Subnet Mask** (Subnetzmaske), die in ihrer Schreibweise der IP-Adresse entspricht (also auch aus vier 8-Bit-Blöcken besteht, die theoretisch jeweils Werte von 0 bis 255 annehmen können). Vereinfacht ausgedrückt kennzeichnen die Blöcke der Subnet Mask, die den Wert 255 enthalten, die Blöcke der IP-Adresse, die die Netzwerk-ID enthalten, während die Subnet Mask-Blöcke mit dem Wert 0 die Stellen in der IP-Adresse mit den Host-IDs kennzeichnen.

Bei dem Beispiel einer IP-Adresse 192.168.0.1 und einer Subnet Mask 255.255.255.0 bedeutet dies also, dass die Zahlenfolge 192.168.0 die Kennnummer des Netzwerkes darstellt und dass in diesem Netzwerk maximal 256 unterschiedliche Adressen an die Hosts vergeben werden können. Der Wert von maximal 256 Host-IDs ist nur theoretisch möglich, da bestimmte IP-Adressen (die kleinste Host-ID als Bezeichnung für das Netzwerk an sich und die höchste Host-ID für einen Broadcast) bereits reserviert sind und damit nicht für die Adressierung eines Rechners zur Verfügung stehen.

Die dargestellte Subnet Mask 255.255.255.0 steht für ein so genanntes **Class-C Netzwerk**. Ein **Class A-Netzwerk** hätte die Subnet Mask 255.0.0.0 und ein **Class-B-Netzwerk** die Subnet Mask 255.255.0.0.

### Domain Name Service (DNS)

War die Darstellung der Adressen in dezimaler Schreibweise im Vergleich zum dualen Zahlensystem für uns bereits eine Vereinfachung, so können wir besonders bei der Nutzung des Internets noch einen Schritt weiter gehen. Für uns Menschen ist es noch einfacher, nicht die IP-Adresse, sondern (möglichst einfache) Namen, die so genannten **URL's** – Uniform Resource Locator – zu behalten und anzugeben. Hinter ihnen stehen dann i. d. R. IP-Nummern, nämlich die Adresse des Computers, auf der die Seite gespeichert ist, die wir im Internet suchen. Unter der URL: <http://www.nibis.de> wird z. B. der Niedersächsische Bildungsserver in Hildesheim erreicht. Für die Auflösung der eingegebenen Namen werden **DNS-Server** eingesetzt, die entsprechende Einträge in ihren Tabellen zur Umsetzung der Namen in IP-Adressen verwalten können.

## Voraussetzungen und praktische Einrichtung eines P2P-Netzwerkes

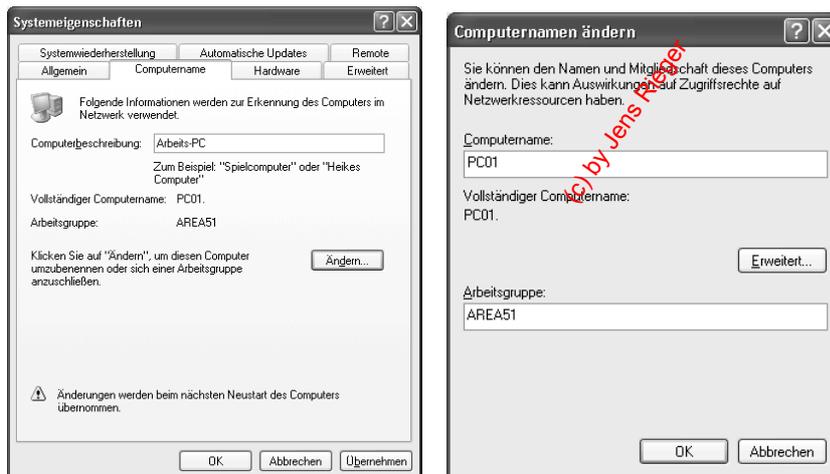
Gehen wir bei unseren folgenden Betrachtungen davon aus, dass nicht ein einmaliger (oder selten angestrebter) Datenaustausch zwischen zwei einzelnen PCs das Ziel ist, sondern dass wir uns in einer wie folgt dargestellten Situation befinden:

- Es sind mindestens 2 PCs vorhanden, die miteinander (dauerhaft) vernetzt sein sollen.
- Es liegt eine heterogene „PC-Landschaft“ vor: mindestens ein PC ist mit dem Betriebssystem Windows XP und mindestens ein weiterer mit Windows 98 ausgestattet.
- Für alle zu vernetzenden PCs stehen Netzwerkkarten zur Verfügung, die auch bereits installiert sind.
- Es gibt zwar verschiedene Netzwerksysteme, wir gehen bei den folgenden Betrachtungen jedoch von dem **Ethernet**, der derzeit gebräuchlichsten Implementierung aus.
- Dabei konzentrieren wir uns auf die Vernetzung mittels **Twisted-Pair-Kabel (TP-Kabel)** und vernachlässigen die Verbindung mit Koaxialkabel, die für neu zu vernetzende (private) Systeme in der Regel nicht mehr verwendet wird.
- Die eingebauten Netzwerkkarten enthalten einen entsprechenden **RJ-45-Anschluss**.
- Es steht ein **Hub** oder ein **Switch** zur Verfügung, der zunächst als „Verteiler“ der Daten eingesetzt bzw. angesehen werden soll und alle zu vernetzenden PCs sind (mittels TP-Kabel-Verbindung von der Netzwerkkarte zum „Verteiler“) angeschlossen.

Ausgehend von einem PC mit dem Betriebssystem Windows XP sollen nun die ersten Schritte zur Einrichtung eines Peer-to-Peer-Netzwerkes beschrieben werden:

### Bearbeitungsschritte:

- Öffnen Sie über **Start – Systemsteuerung und System** das Fenster **Systemeigenschaften**.



- Über die Schaltfläche **Ändern** können Sie hier die hier genannten Einstellungen vornehmen oder eigene Angaben wählen.
- Sie sollten allerdings darauf achten, dass die Computernamen und IP-Adressen der zu vernetzenden PCs verschieden sind, der Name der Arbeitsgruppe (hier: AREA51) auf allen PCs jedoch gleich gewählt wird!

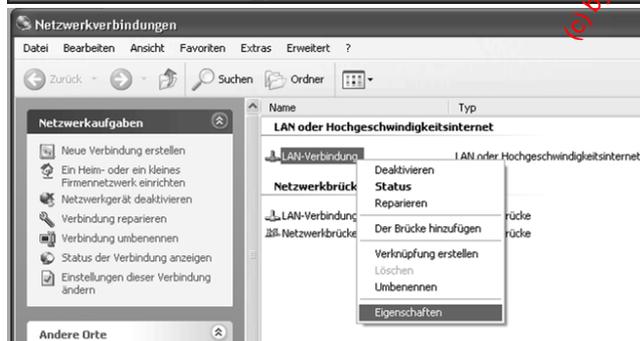
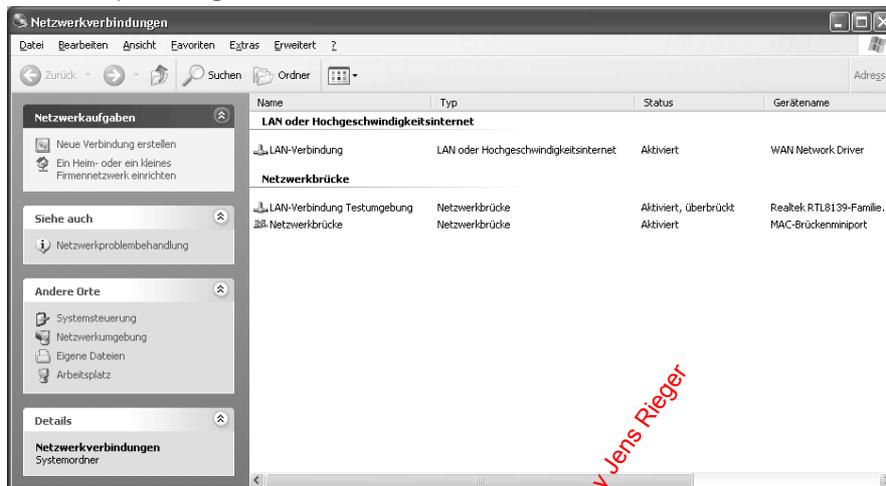
**Bearbeitungsschritte (Fortsetzung):**

- Die Meldung, dass die hier getroffenen Einstellungen erst nach einem Neustart wirksam werden, kann zunächst ignoriert werden (Klicken auf die Schaltfläche OK), da noch weitere Einstellungen notwendig sind.



Dazu gehört das Eintragen einer IP-Adresse, die (vergleichbar mit einer Hausnummer) das Finden und Ansprechen eines PCs ermöglicht. Wir wählen hier zunächst die für kleine private Netzwerke häufig vorteilhafte Variante der festen IP-Adressen:

- Klicken Sie auf die Schaltfläche **Start** und dann mit der rechten Maustaste auf **Netzwerkumgebung** (alternativ dazu können Sie auch vom Desktop aus direkt mit der rechten Maustaste auf das Symbol Netzwerkumgebung klicken) und wählen Sie dann den Menüpunkt **Eigenschaften**.



- Klicken Sie dann mit der rechten Maustaste auf die **LAN-Verbindung** und wählen den Menüpunkt **Eigenschaften** (In dem oben dargestellten Beispiel besteht eine weitere LAN-Verbindung Testumgebung, die bereits zusätzlich eingetragen worden und auf einem „neuen“ XP-System nicht vorzufinden ist.).

### Bearbeitungsschritte (Fortsetzung):



- Von hier aus werden die wichtigen Eigenschaften der LAN-Verbindung angezeigt und (falls notwendig) bearbeitet. Wählen Sie durch Anklicken das **Internetprotokoll (TCP/IP)** aus und klicken dann auf die Schaltfläche **Eigenschaften**.



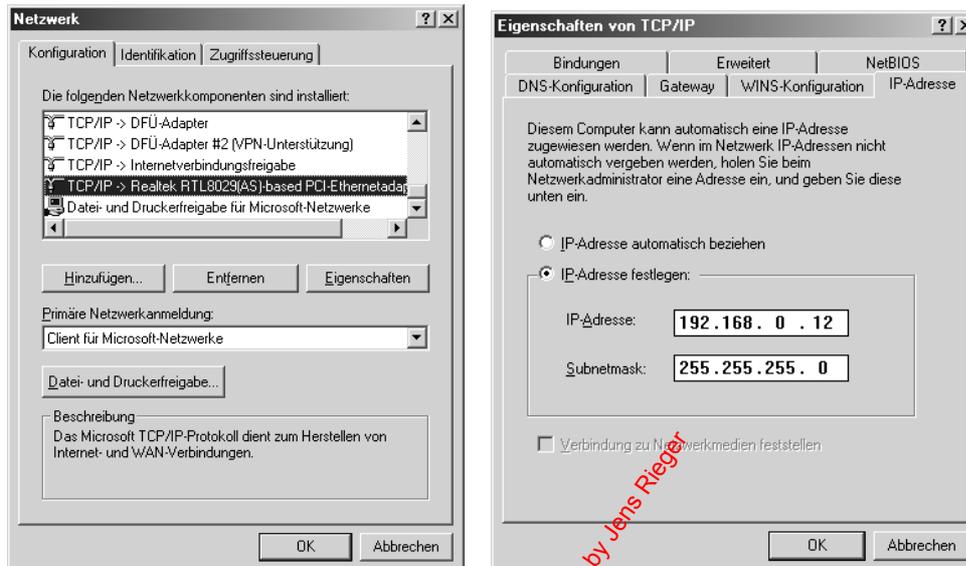
(c) by Jens Rieger

- Aktivieren Sie hier den Radio-Button **Folgende IP-Adresse verwenden**, um der Netzwerkkarte (dieses PCs und unter dieser LAN-Verbindung) eine feste IP-Adresse zuzuweisen und geben Sie die in dem Beispiel dargestellte IP-Adresse **192.168.0.11** und die Subnetzmaske **255.255.255.0** ein.
- Klicken Sie in dem Fenster **Eigenschaften von Internetprotokoll (TCP/IP)** auf die Schaltfläche **OK** und im Fenster **Eigenschaften von LAN-Verbindung** auf die Schaltfläche **Schließen**.
- Sie haben nun die wichtigsten Einstellungen an einem PC Ihres neuen Netzwerkes vorgenommen. Führen Sie diese Schritte an einem weiteren PC durch, wählen Sie dazu wiederum die Arbeitsgruppe mit dem Namen **AREA51**, aber verschiedene Computernamen und IP-Adressen (z. B. **192.168.0.12**, **192.168.0.13** usw.).

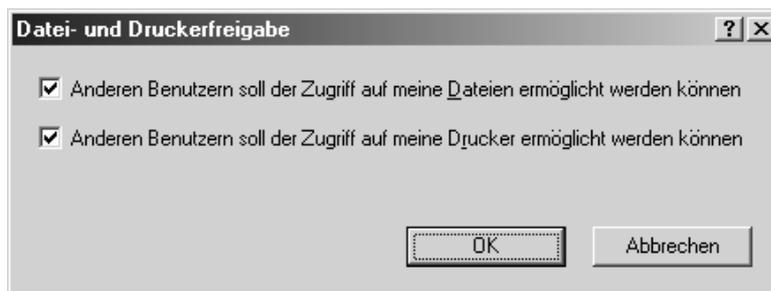
Sie werden feststellen, dass die Einrichtung eines Netzwerk-PCs, z. B. mit dem Betriebssystem Windows 98, vergleichbar mit der Vorgehensweise bei Windows XP ist. Allerdings lassen sich unter Windows 98 oder Windows ME zu einer Netzwerkkarte keine unterschiedlichen LAN-Verbindungen eintragen, sodass man nach dem Aufruf der **Netzwerkumgebung** mit der rechten Maustaste und dem Wählen des Menüpunktes **Eigenschaften** direkt zu den Einstellungen des Netzwerkes gelangt. Von dort aus können die den oben genannten Angaben entsprechenden Konfigurationsdaten und Identifikationsdaten eingerichtet werden!

#### Bearbeitungsschritte:

- Wählen Sie an Ihrem PC mit dem „alternativen“ Betriebssystem (hier Windows ME) nach dem Aufruf der **Netzwerkumgebung** mit der rechten Maustaste und dem Wählen des Menüpunktes **Eigenschaften** auf der Registerkarte **Konfiguration** das TCP/IP-Protokoll zu der in Ihrem PC befindlichen Netzwerkkarte (hier Realtek) und klicken Sie dann auf die Schaltfläche **Eigenschaften**.

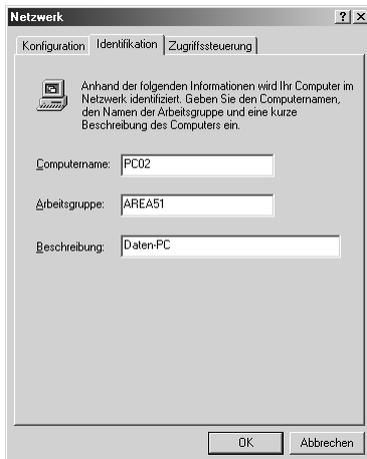


- Tragen Sie die dargestellten Angaben für die IP-Adresse (**192.168.0.12**) und für die Subnetmask (**255.255.255.0**) unter dem entsprechenden Registerblatt zur **IP-Adresse** ein und bestätigen Sie die Eingaben mit **OK**.
- Damit auch andere Benutzer auf Ihre Dateien und Drucker zugreifen können, klicken Sie im Netzwerk-Fenster auf die Schaltfläche **Datei- und Druckerfreigabe** und aktivieren beide Punkte durch Anklicken.

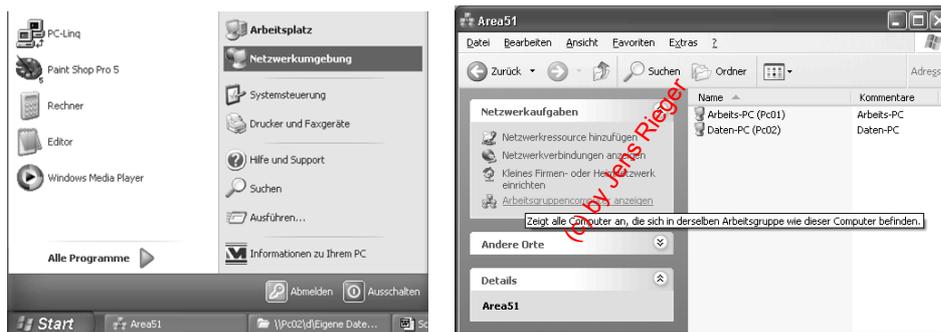


### Bearbeitungsschritte (Fortsetzung):

- Wählen Sie die Registerkarte **Identifikation** und geben Sie den Computernamen **PC02**, die Arbeitsgruppe **AREA51** und eine beliebige Beschreibung (als optionaler Eintrag, z. B. **Daten-PC**) ein.



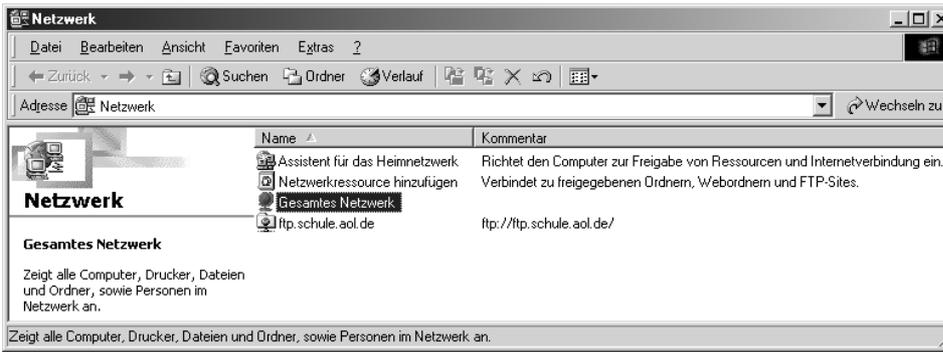
- Wechseln Sie jetzt wieder zu Ihrem Arbeits-PC (PC01) mit dem Betriebssystem Windows XP und rufen Sie den über **Start – Netzwerkumgebung** zu erreichenden und dort unter **Netzwerkaufgaben** befindlichen Menüpunkt **Arbeitsgruppencomputer anzeigen** auf.



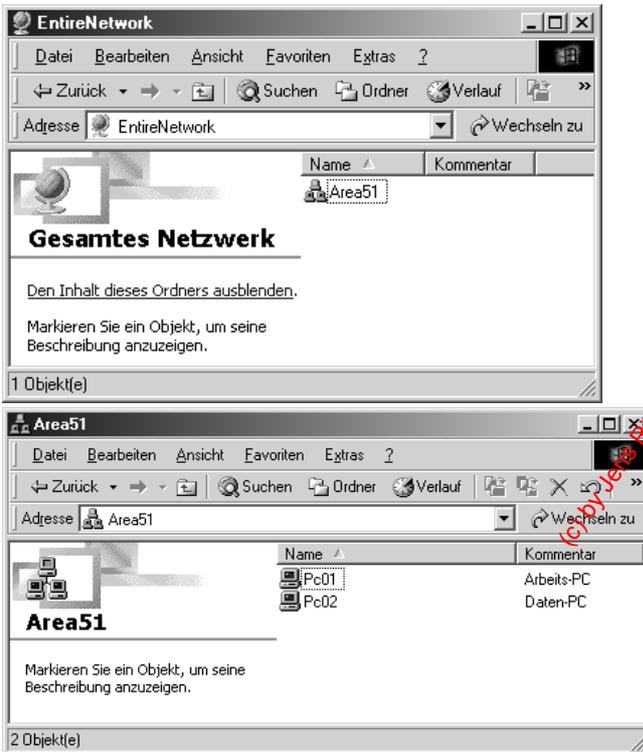
- Hier sehen Sie bereits beide PCs in dem von Ihnen eingerichteten Netzwerk. Zur Kontrolle betrachten wir das Netzwerk jetzt aus der Sicht des zweiten PCs mit dem Betriebssystem Windows ME:
- Öffnen Sie dazu das Netzwerk-Fenster durch Doppelklicken auf das Desktop-Symbol **Netzwerk**.



**Bearbeitungsschritte (Fortsetzung):**



- Öffnen Sie die Ansicht für **Gesamtes Netzwerk** und in dem neuen Fenster die Arbeitsgruppe **Area51** jeweils durch Doppelklick.



- Jetzt sehen Sie auch von diesem PC aus (PC02) das Netzwerk mit der Arbeitsgruppe **Area51** und den beiden bislang eingerichteten **PC01** und **PC02**.

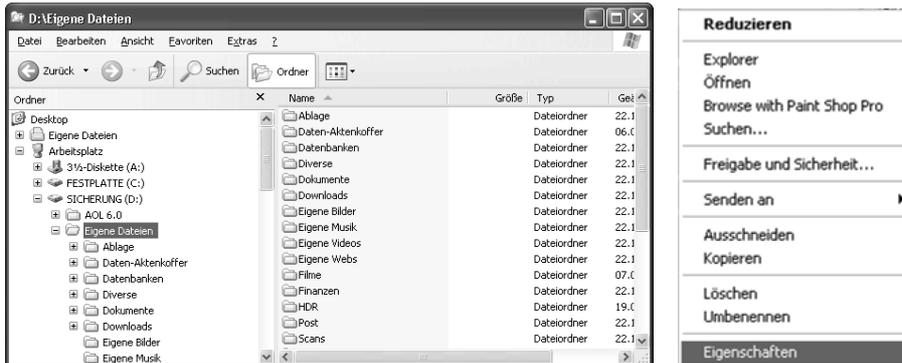
Um diese Netzwerkverbindung (z. B. zu einem Datenaustausch der beiden PCs) nutzen zu können, fehlt jetzt allerdings noch die Freigabe der Daten, die auf dem jeweils anderen PC (oder bei mehreren Netzwerk-Computern auf allen anderen PCs) sichtbar sein sollen. Dazu gibt es verschiedene Möglichkeiten, die hier zunächst an einem Beispiel angesprochen werden sollen:

### Bearbeitungsschritte:

- Öffnen Sie auf dem PC01 den **Windows-Explorer**, indem Sie mit der **rechten** Maustaste auf die Schaltfläche **Start** und dann auf den Menüpunkt **Explorer** klicken.



- oder indem Sie alternativ dazu über **Start**, **Alle Programme** und **Zubehör** auf den **Windows-Explorer** klicken.



- Wählen Sie den Ordner, der für die anderen PCs im Netzwerk sichtbar (freigegeben) werden soll (in diesem Beispiel ist dies der Ordner **Eigene Dateien**), klicken Sie an dieser Stelle auf die rechte Maustaste und wählen Sie den Menüpunkt **Eigenschaften**. Wählen Sie die Registerkarte **Freigabe**.

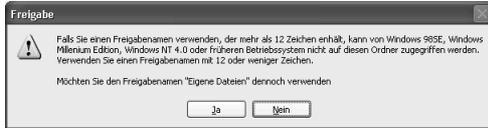


(c) by Jens Rieger

- aktivieren Sie unter dem Feld **Netzwerkfreigabe und -sicherheit** das Kontrollfeld **Diesen Ordner im Netzwerk freigeben** und deaktivieren Sie das Kontrollfeld **Netzwerkbenutzer dürfen Dateien verändern**. Klicken Sie auf die Schaltfläche **OK**.

**Bearbeitungsschritte (Fortsetzung):**

- Die darauf erscheinende Meldung macht deutlich, dass Sie keine Freigabenamen verwenden sollten, die länger als 12 Zeichen sind!



- Klicken Sie auf die Schaltfläche **Nein**, ändern Sie den Freigabennamen z. B. auf **My Docs** und bestätigen dann diesen Vorgang mit **OK**.
- Beim erneuten Aufrufen des Windows-Explorers erkennen Sie nun eine Hand unter dem Ordner Eigene Dateien, dadurch wird die Freigabe eines Ordners angezeigt.

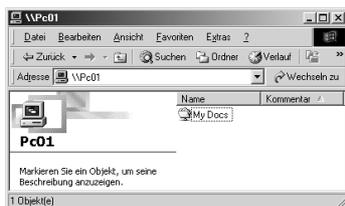


Sie können diesen freigegebenen Ordner jetzt auf allen PCs im Netzwerk sehen und z. B. Daten von dort kopieren. Wichtig ist dabei, dass auch alle Unterordner sichtbar werden, übergeordnete Ordner von einem anderen PC aus jedoch nicht aufgerufen werden können.

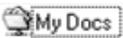
Zur Überprüfung der Freigabe führen Sie die folgenden Bearbeitungsschritte vom PC02 aus durch:

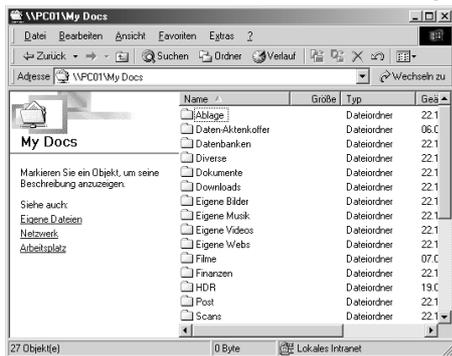
**Bearbeitungsschritte:**

- Öffnen Sie (analog zum letzten Bearbeitungsschritt am PC01) an dem **PC02** die Ansicht für das **Gesamte Netzwerk** und in dem neuen Fenster die Arbeitsgruppe **Area51** jeweils durch Doppelklick.
- Führen Sie dann einen Doppelklick auf das Symbol für den **PC01** aus und Sie erkennen den mit dem Freigabennamen **My Docs** versehenen Ordner **Eigene Dateien** auf dem entfernten **PC01**.



© by Jens Rieger

- Durch das Doppelklicken auf das Symbol **My Docs**  , das einen vernetzten Ordner darstellt, sehen Sie die Dateien bzw. Ordner unterhalb von **Eigene Dateien** auf dem **PC01** und können sich so beliebig weit in diesem Verzeichnisabschnitt „bewegen“.

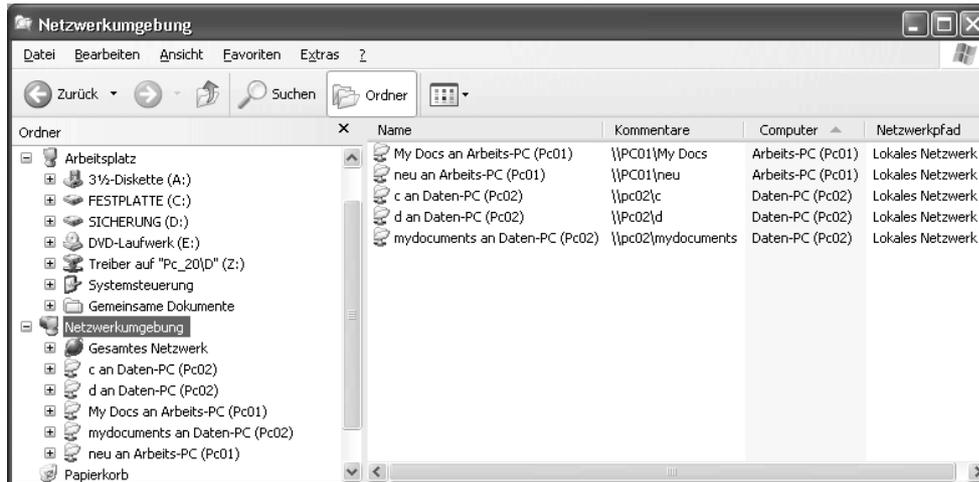


Überlegen Sie demnach vor einer Freigabe genau, ob Sie wirklich alle Daten im entsprechenden Ordner mit allen Unterverzeichnissen freigeben wollen, oder ob das Kopieren in ein Verzeichnis (z. B. an ein Ende einer Verzeichnisstruktur) sinnvoller bzw. sicherer ist.

Da nach einiger Zeit unter Umständen nicht mehr jeder freigegebene Ordner im Gedächtnis geblieben ist und auch nicht immer alle Verzeichnisse im Windows-Explorer geöffnet sind, so dass Freigaben evtl. verdeckt bleiben, kann es durchaus sinnvoll sein, sich einen aktuellen Überblick zu verschaffen und zu kontrollieren, welche Ordner eines PCs bereits freigegeben sind.

### Bearbeitungsschritte:

- Rufen Sie den Windows-Explorer (z. B. mit der rechten Maustaste auf **Start**) auf und klicken Sie auf das +-Zeichen vor der **Netzwerkumgebung**.



- Jetzt werden alle aktuellen Freigaben angezeigt und Sie können diese z. B. durch einen Klick auf die Spaltenüberschrift **Computer** in der Form sortieren lassen, dass die Zuordnung zu dem eigenen oder anderen PCs leicht möglich ist.

Sie haben jetzt ein Peer-to-Peer-Netzwerk aufgebaut und können dies unter Berücksichtigung der genannten Besonderheiten durch weitere PCs erweitern, indem Sie diese an den Hub bzw. den Switch anschließen und die oben genannten Bearbeitungsschritte auf allen zu vernetzenden PCs durchführen.

Für den privaten Gebrauch, bei dem in der Regel nur wenige PCs verschiedener Grundausstattungen miteinander vernetzt werden sollen, ist dieser noch nicht sehr hohe Arbeitsaufwand durchaus gerechtfertigt. Sollen jedoch mehr PCs zu einem Netzwerk zusammengeschlossen werden und sind diese im Idealfall auch noch mit der gleichen Hardware bestückt, so lassen sich z. B. durch das Kopieren von bestimmten Konfigurationen bzw. durch das Erzeugen von so genannten **Images** wesentliche Arbeitserleichterungen und Zeitersparnisse erzielen. Dabei handelt es sich um ein Abbild entweder einer Partition oder einer gesamten Festplatte, das auf einem Datenträger (z. B. einer Festplatte oder evtl. mehreren CDs) abgelegt werden kann und bei Bedarf unter relativ geringem Zeitaufwand wieder zurückzuspielen ist. Das Erzeugen dieser Images lässt sich mit der heutigen Software sehr leicht durchführen und kann bei neueren Versionen mittels einer verständlichen Windows-Oberfläche bereits im laufenden Betrieb gestartet werden.

### 13.3 Einrichtung eines zentralen Internetzuganges

Ein großer Vorteil eines Netzwerkes besteht nun z. B. darin, mit einem einzelnen Internetzugang auch anderen PCs im Netzwerk diesen Dienst zur Verfügung zu stellen. Das heißt, alle im Netz befindlichen PCs nutzen diesen zentralen Internetzugang, ohne dass für die Clients eine eigene Internetverbindung eingerichtet werden muss.

Vorausgesetzt wird an dieser Stelle, dass Sie an einem PC bereits über einen Internetzugang verfügen. Ist dies nicht der Fall, so gibt es verschiedene Möglichkeiten, diese Verbindung über die Telefonleitung einzurichten. Entweder erfolgt dies z. B. über ein analoges Modem oder bei einem ISDN-Anschluss über eine ISDN-Karte, die wie die Netzwerkkarte in den PC eingebaut wird.

Der PC mit dem Internetzugang kann wie in unserem Beispiel mit dem Betriebssystem Windows ME ausgestattet sein, denn häufig sind die Internetserver nicht die neuesten bzw. leistungsstärksten PCs, da an sie unter Umständen nicht besonders hohe Anforderungen gestellt werden müssen. Allerdings muss dieser PC ein Teilnehmer des (wie z. B. oben beschrieben) eingerichteten Netzwerkes sein und erhält in unserem Beispiel die später wichtige IP-Adresse **192.168.0.1**.

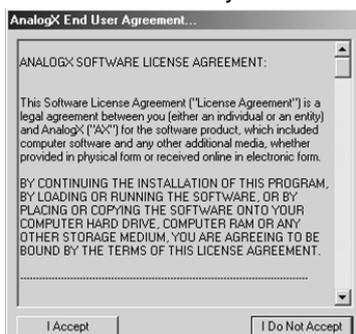
Windows bietet z. B. mit dem Betriebssystem Windows 98 SE die Möglichkeit, eine Internetfreigabe zu installieren (falls nicht bereits geschehen). Dieser PC kann dann als Internetserver bzw. Gateway für alle anderen im Netzwerk befindlichen PCs dienen. Allerdings müssen dazu eine Reihe von Einstellungen vorgenommen werden und es kann bei der Nutzung verschiedener Betriebssysteme in der Kombination mit bestimmten Internet-Providern durchaus zu Verbindungsproblemen kommen, sodass wir hier einen für den Privatanwender gut geeigneten, recht einfachen und problemlosen Weg darstellen wollen.

Dazu wird auf dem „**Internetzugangsrechner**“ ein sogenannter **Proxy** (Stellvertreter) eingerichtet, der sich als kleines Softwarepaket (mit weniger als 300 Kbyte) darum kümmert, die über das Netzwerk an ihn adressierten Clients mit dem Internet zu verbinden. Grundsätzlich kann dieses auch häufig als Internetserver bezeichnete Programm als Datenpuffer dienen, um Informationen zwischenzulagern und bei Bedarf wieder abzurufen.

Dieser hier benötigte Proxy braucht nur sehr klein zu sein, um die gewünschte Funktionalität zu erfüllen. Es gibt verschiedene Proxy-Lösungen, als Beispiel ist hier der für private Nutzung (beachten Sie dabei die Lizenzbestimmungen!) im Internet frei erhältliche Proxy der Fa. AnalogX gewählt worden, den Sie entweder über [www.analogx.com](http://www.analogx.com) oder direkt zum Download über <http://www.analogx.com/contents/download/network/proxy.htm> erreichen.

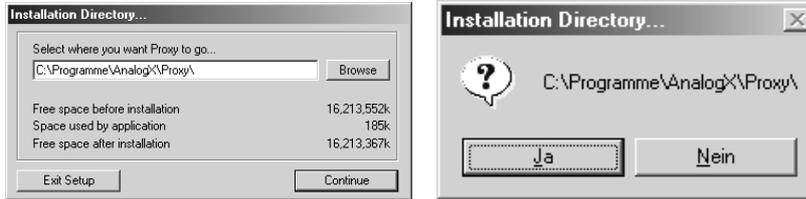
#### Bearbeitungsschritte:

- Laden Sie den Proxy aus dem Internet und starten Sie die ausführbare Datei.



### Bearbeitungsschritte (Fortsetzung):

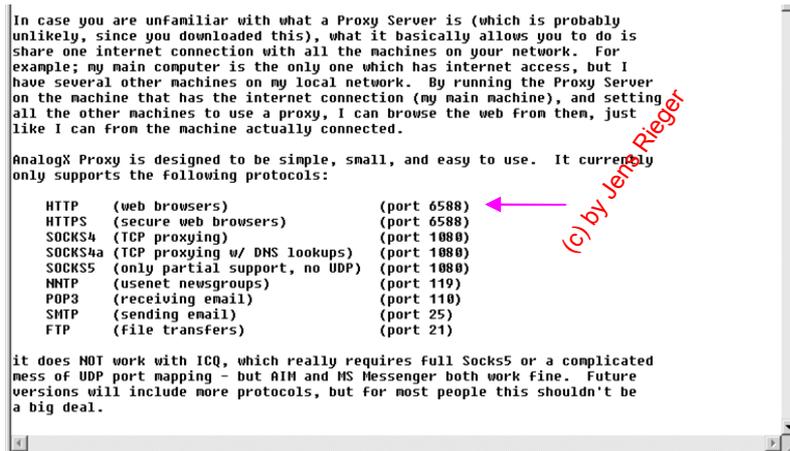
- Lesen Sie die Lizenzbestimmungen und klicken Sie dann zur Annahme dieser auf die Schaltfläche **I Accept**.
- Wählen Sie den Installationspfad bzw. übernehmen Sie die entsprechende Vorgabe, klicken Sie dann auf die Schaltfläche **Continue** und bestätigen Sie die darauf folgende Kontrollfrage mit **Ja**.



- Die Frage nach der Registrierung beantworten Sie mit **Nein** (da diese auch zu einem späteren Zeitpunkt vorgenommen werden kann).



- Es öffnet sich automatisch der Texteditor und Sie haben nun die Möglichkeit, sich mit den Besonderheiten dieses Proxyserver vertraut zu machen. Die z. B. für die Nutzung eines **web browsers** (z. B. **MS Internet Explorer**) wichtige Einstellung, die wir in den nächsten Schritten verwenden werden, lässt sich dieser Textdatei entnehmen.



- Schließen Sie den Texteditor und klicken Sie bei der nachfolgenden Meldung, dass der Proxy erfolgreich installiert wurde, auf die Schaltfläche **OK**.



Die Installation des Internetserver ist damit abgeschlossen, dieser Vorgang muss **nicht** auf den Clients im Netzwerk durchgeführt werden, allerdings benötigen diese noch die Information, dass es im Netzwerk einen Proxy gibt, der sich um den Internetzugang kümmert, und wo sich dieser befindet.

**Bearbeitungsschritte:**

- Rufen Sie den **MS Internet-Explorer** auf, indem Sie diesen auf dem Desktop doppelt anklicken



oder über **Start** und die Direktauswahl oder über **Start – Alle Programme** und dann **Internet Explorer** auswählen



- Noch konnte keine Internetverbindung aufgebaut werden bzw. der Aufruf einer Webseite erfolgen. Dauert der Vorgang des Suchens zu lange, so brechen Sie diesen durch Drücken der Escape-Taste ab.
- Wählen Sie den Menüpunkt **Extras – Internetoptionen** und dort das Registerblatt **Verbindungen**.



- Klicken Sie unter **LAN-Einstellungen** auf die Schaltfläche **Einstellungen**.

### Bearbeitungsschritte (Fortsetzung):

- Achten Sie darauf, dass das Kontrollkästchen für die **Automatische Suche der Einstellungen** nicht aktiviert ist.



- Aktivieren Sie unter **Proxyserver** das Kontrollkästchen und tragen Sie die **IP-Adresse** Ihres Internetserver (**192.168.0.1**) und die in diesem Fall gültige **Port-Adresse 6588** ein. Bestätigen Sie die Eingaben in diesem und im übergeordneten Fenster jeweils mit **OK**.
- Besteht zu diesem Zeitpunkt eine Verbindung des Internetserver zum Internet und ist der Proxyserver (als Dienst) aktiv, so kann im Internet-Explorer mit einem Klick auf die Schaltfläche **Aktualisieren**  bereits das Internet genutzt werden.

