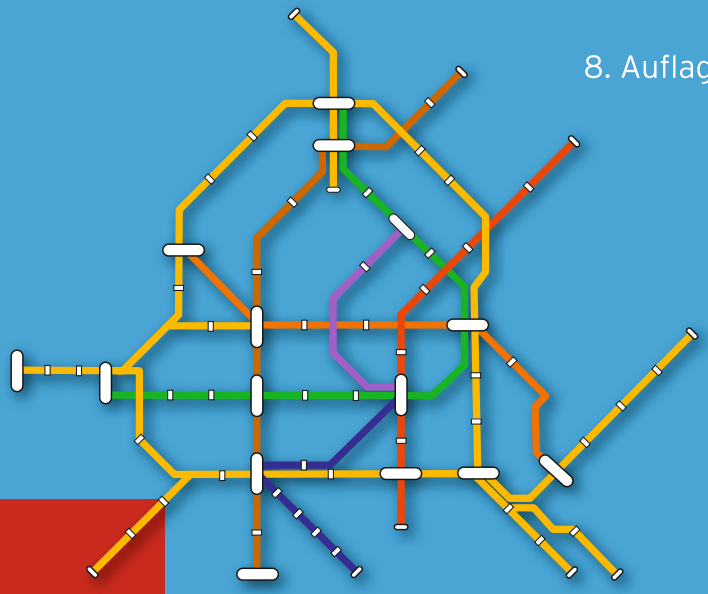
Rüdiger **SCHREINER**
Oliver P. **WALDHORST**

COMPUTER-NETZWERKE



8. Auflage

VON DEN GRUNDLAGEN ZUR FUNKTION UND ANWENDUNG

HANSER

Schreiner/Waldhorst

Computernetzwerke

Rüdiger Schreiner
Oliver P. Waldhorst

Computernetzwerke

Von den Grundlagen zur Funktion und Anwendung

8., aktualisierte Auflage

HANSER

Die Autoren:
Rüdiger Schreiner, Schopfheim
Prof. Dr. Oliver P. Waldhorst, Offenburg

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Lektorat: Sylvia Hasselbach
Copy editing: Sandra Gottmann, Wasserburg
Umschlagdesign: Marc Müller-Bremer, www.rebranding.de, München
Umschlagrealisation: Max Kostopoulos
Satz: Eberl & Koesel Studio, Kempten
Druck und Bindung: Hubert & Co. GmbH & Co. KG BuchPartner, Göttingen
Printed in Germany

Print-ISBN 978-3-446-47415-4
E-Book-ISBN 978-3-446-47472-7
E-Pub-ISBN 978-3-446-48004-9

Inhalt

Vorwort

Noch ein Buch über Netzwerke? In jeder Buchhandlung gibt es sie bereits meterweise. Aber dieses Buch unterscheidet sich von den anderen und hat eine besondere Geschichte. Der beste Aspekt daran ist, dass es nicht geplant war. Beruflich arbeite ich sehr viel mit Computerbetreuern zusammen, in allen Schattierungen der Ausbildung und des Wissensstandes, von Hilfsassistenten ohne Computererfahrung bis hin zu professionell ausgebildeten Fachkräften.

Wenn diese Probleme haben, die sie nicht lösen können oder Beratung brauchen, wenden sie sich an mich. Und dies in einer völlig inhomogenen Umgebung, mit Windows, Linux, MacIntosh, Sun, etc. Die Fluktuation ist sehr groß, in großen Teilen der Umgebung muss das Rad ständig neu erfunden werden.

Im Laufe der Jahre fiel mir auf, dass immer wieder dieselben Fragen, immer wieder Verständnisprobleme an denselben Stellen auftreten. Weshalb? Netzwerke sind heute eine unglaublich komplexe Angelegenheit. Aber wie der Computer selbst, finden sie immer mehr Einzug auch in Privathaushalte. Längst ist die Zeit vorbei, in der es zu Hause nur wenige Rechner gab. Längst sind wir so weit, dass viele Haushalte mehrere Computer besitzen und untereinander Daten austauschen und ans Internet wollen. Viele Spiele sind netzwerkfähig geworden, Drucker, Faxgeräte und Scanner werden gemeinsam genutzt. Oft ist es kein Problem, ein paar Rechner zusammenzuhängen und ein kleines Netzwerk zum Laufen zu bekommen. Aber wenn es Probleme gibt, sind die meisten verloren.

Ebenso ist in kleineren und mittleren Unternehmen (oft durch die Aufgabentrennung in großen Unternehmen ebenso) das IT-Personal meist auf die Betreuung der Rechner und Server ausgerichtet. Das Netzwerk wird meist eingekauft und als Black-Box betrieben. Netzwerke sind oft ein „Buch mit sieben Siegeln“ und eine Infrastruktur, die wie das Telefon behandelt wird. Jeder verlässt sich darauf, aber wenn es nicht funktioniert, ist die Katastrophe da. Oft wird „gebastelt“, bis es irgendwie funktioniert, ohne darüber nachzudenken, dass es noch viel besser sein könnte, performanter und stabiler und nicht nur einfach funktionieren kann.

Im Bereich Netzwerk gibt es eine unheimliche Grauzone des Halbwissens. Ähnliches sieht man bei den Betriebssystemen. CD rein, Setup angeklickt, 15mal „OK“ gedrückt und der Rechner läuft – solange, bis es Probleme gibt.

Viele sind sehr interessiert am Thema Netzwerk. Der Einstieg aber ist schwer, das Thema ist keine Wochenendsache und meist fehlen die Ansprechpartner. Beklagt wird von den meisten, dass es auf dem Markt entweder Bücher gibt, die nur sehr oberflächlich sind, oder aber sofort auf einen Level gehen, in dem der Einsteiger verloren ist. Weiter sind sehr viele

Bücher zu einem hochspeziellen Thema geschrieben worden und erlauben so nur den Einstieg in kleine Teilbereiche. Oft ist die Sicht der Lehrbücher herstellerbezogen. Linux-Netzwerke, Windows-Netzwerke, meist Nebenkapitel in Büchern über die Betriebssysteme selbst. Oder es sind Bücher von Herstellern der Netzwerkgeräte, die detailliert das Featureset und die Konfiguration beschreiben.

Sicher sind diese Bücher sehr gut – aber nicht für einen Einstieg geeignet. Sie behandeln speziell die Konfigurationen und Möglichkeiten ihrer Geräte und Umgebungen – und nicht der Standards. Auch sind sie nicht für einen Heimanwender geeignet, der mehr verstehen will, und ebenso nicht für eine Firmenleitung oder IT-Abteilung kleiner und mittlerer Umgebungen, die strategisch entscheiden müssen, welchen Weg sie im Bereich Netz gehen wollen.

Dieselbe Erfahrung musste ich selbst machen, als ich erstmalig mit dem Thema Netzwerke konfrontiert wurde. Es gibt viele gute Kurse und Ausbildungen, meist von den Herstellern der Geräte. Eine Privatperson oder kleine Firma kann aber nicht tausende Euro bezahlen, aus einfachem Interesse. Immer wieder erkläre ich dasselbe neu. Und oft hörte ich: „Kannst Du mir nicht ein Buch empfehlen, das wirklich einen Einstieg erlaubt? Das soviel Grundwissen vermittelt, dass man versteht, wie das alles funktioniert, aber auf einer für jedermann verständlichen Basis? Ohne aber nur oberflächlich zu sein? Das ein breites Spektrum des „Wie“ bietet, verstehen lässt und den „Aha-Effekt“ auslöst?“

Ein Bekannter, der gutes Computer-, aber kein Netzwerk-Know-how hatte, bat mich, ihn ins Thema Netzwerke einzuweisen. Wir trafen uns eine Weile regelmäßig und ich überlegte mir, wie ich ihn an das Thema heranbringen kann. Aus diesen Notizen, „Schmierzetteln“ und Zeichnungen stellte ich eine kleine Fibel zusammen. Weiter fand ich Interesse in einem Computer-Verein, baute die Unterlagen aus und hielt den ersten „Netzwerkkurs“. Die Resonanz war enorm. Nie hätte ich gedacht, dass so viele Interesse haben. Vom Schüler, der seine PCs zum Spielen vernetzen will, über den KMU-Besitzer, der Entscheidungsgrundlagen sucht, bis zum IT-Spezialist, der über den Tellerrand schauen wollte, war alles vertreten.

Die Teilnehmer brachten mich auf die Idee, aus den Unterlagen ein Buch zu machen. Dies ist die Geschichte dieses Buches. Das Ziel ist, dem Leser zu ermöglichen, Netzwerke wirklich zu verstehen, egal ob in großen Umgebungen oder zu Hause. Das Ziel ist, soviel Knowhow zu erarbeiten, dass der Interessierte versteht, wie es funktioniert und aufbauen kann, und der Einsteiger, der in Richtung Netz gehen will, das Handwerkszeug bekommt, um tiefer einzusteigen und sich an die „dicken Wälzer“ zu wagen. Gezeigt wird, wie es wirklich funktioniert, wie es strukturiert ist und welche großen Stolperfallen es gibt. Genauso soll der Leser in der Terminologie firm werden.

Ein interessierter Einsteiger will nicht 200 Seiten Kommandozeile eines Routers lesen, sondern verstehen, was ein Router wirklich ist. Ist es sein Job oder Interesse, soll er dann nach der Lektüre dieses Buches in der Lage sein, die Erklärungen dieser Kommandozeile sofort zu verstehen. Das Hauptziel dieses Buches sind die Grundlagen und ihr Verständnis. Wer die Grundlagen verstanden hat, dem fügt sich alles wie ein Puzzle zusammen. Leider wird darauf in der Literatur zu wenig eingegangen. Diese Lücke will das Buch schließen. Ein gutes Fundament, Verständnis und „wirklich verstehen“ ist der Leitfaden. Am Ende soll der Leser qualitativ, aber nicht oberflächlich, alle Informationen und Zusammenhänge kennen, wird arbeitsfähig sein, in der Terminologie firm und bereit für den nächsten Schritt. Die Grundlagen werden mit Absicht ziemlich tief behandelt, denn ein Verstehen der Basis ist

immer Voraussetzung für ein fundiertes Wissen. Dies ist in jedem komplexen Thema so. Daher gibt es einige Exkurse in die Physik und Mathematik. Das hört sich abschreckend an, sie sind aber, so hoffe ich, für jeden verständlich gehalten.

Das Buch wurde bewusst als ein Buch zum Lesen geschrieben. Trockene Theorie, die manchen bekannt ist, manchen nicht, habe ich als Exkurse an das Ende des Buches ausgelagert, um den Fluss nicht zu stören. Wer diese Grundlagen nicht hat, ist gebeten, sich die Mühe zu machen, diese Exkurse zur richtigen Zeit zu lesen; es wird im Text jeweils darauf verwiesen. Ich rate dazu, das Buch nicht einfach wie einen Roman zu lesen, sondern sehr bewusst und kapitelweise. Es stecken viele Informationen in sehr kompakter Form darin. Man ist leicht versucht, es in einem Zug zu lesen, doch wird dabei eine Menge untergehen. Ein Repetitorium und Fallbeispiele geben am Ende die Möglichkeit, mit dem Erlernten umzugehen.

Zum Schluss möchte ich nicht versäumen, einigen Personen zu danken, die einen großen Anteil am Entstehen der Unterlagen beziehungsweise des Buches hatten: Herrn Prof. Dr. F. Rösel für die Chancen und die Möglichkeit der Weiterbildungen; Herrn Dr. H. Schwedes für die Korrekturlesung und die wertvollen Anregungen; der Linux Usergroup Lörrach e. V. für das tolle Feedback; Herrn H. Volz für die akribische fachliche Korrekturlesung und seine Anmerkungen; Herrn Dr. P. Zimak für die stets offene Türe und die vielen beantworteten Fragen in den letzten Jahren; und nicht zuletzt ganz besonders meiner Familie für die gestohlene Zeit.

Das Buch ist aus den Erfahrungen in Jahren der Praxis entstanden – es ist ein Buch der Praxis und ein dynamisches Buch, das aus ständigem Feedback gewachsen ist. In diesem Sinne wünsche ich Ihnen möglichst großen Gewinn und viel Spaß bei seiner Lektüre. Eines haben mir die bislang abgehaltenen Netzwerkkurse und Diskussionen gezeigt: Ein so trockenes Thema wie Netzwerke kann auch Spaß machen! Interessant ist es allemal.

Lörrach, im Oktober 2005
Rüdiger Schreiner

Vorwort zur achten Auflage

„Computernetzwerke“ von Rüdiger Schreiner – ein Buch, das Generationen von Auszubildenden und Studierenden einen einfachen Einstieg in die Welt der Netzwerke ermöglicht hat und daher durchaus als Standardwerk bezeichnet werden darf. Umso mehr fühle ich mich geehrt, dass man mir das Vertrauen geschenkt hat, das Buch für die achte Auflage zu aktualisieren.

Seit der ersten Auflage sind fast 18 Jahre vergangen. Im Zeitalter der Computernetzwerke sind das Jahrhunderte! Kaum ein Gebiet ist einem so schnellen Wandel unterworfen. Und so ist es in der Geschichte des Buches nicht selten vorgekommen, dass Technologien und Trends, die in einer Auflage als „die Zukunft“ angekündigt wurden, beim Erscheinen der nächsten Auflage bereits Standard oder gar veraltet waren.

Ein Überblick über die historische Entwicklung der Computernetze mit allen jemals relevanten Technologien hat sicherlich seinen eigenen Wert. In einer zu großen Häufung werden Ausführungen zu historischen Technologien aber schnell als Ballast empfunden – gerade in einem Buch, das in die Materie einführen soll. Aus diesem Grund habe ich mich von manchen Themen getrennt.

Bei der Aktualisierung anderer Themen habe ich darauf geachtet, die für eine Einführung in die Materie wesentlichen Aspekte hervorzuheben. Damit erfüllt das Buch weiterhin seinen Zweck, einen niederschwelligen Einstieg in die Thematik zu bieten. Spezialliteratur zu einzelnen Themen findet sich an anderer Stelle. Auf diese wird in den zentralen Kapiteln des Buches verwiesen.

Den Lesern der Vorauflagen danke ich für ihre Hinweise und Korrekturen. Allen Lesern der 8. Auflage wünsche ich viel Freude bei der Lektüre und würde mich natürlich über erneutes Feedback freuen.

Offenburg, im Juli 2023
Oliver P. Waldhorst

1 Zur Geschichte der Netzwerke

1.1 Netzwerke – der Beginn

In der Anfangszeit der Datenverarbeitung standen zentrale Rechner im Mittelpunkt, die von wenigen Spezialisten betrieben werden konnten. In Firmen, Institutionen und Universitäten wurden die Daten auf- und vorbereitet und dann zentral im Großrechner verarbeitet. Meist waren die Systeme und Programme proprietär, der Weg der Daten war denkbar umständlich. Die meisten Daten mussten in Form von Papier oder mobilen Datenträgern zur Zentraleinheit gebracht, eingegeben und die Ergebnisse nach der Verarbeitung ebenso wieder abgeholt werden.

Die Programme zur Verarbeitung der Daten wurden meist selbst geschrieben und auf Lochkarten, Lochstreifen, etc. eincodiert und jeweils vor der Verarbeitung der Datensätze in das System eingelesen.

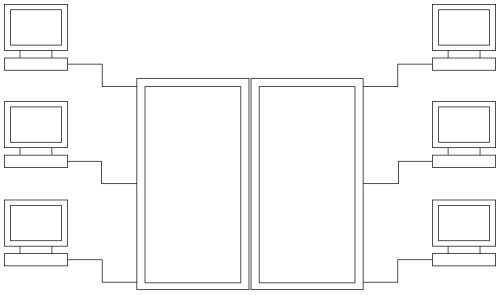


Bild 1.1 Ein Terminalsystem: An einer großen Zentraleinheit, welche die gesamte „Intelligenz“ beherbergte, waren Terminals ohne eigene Intelligenz angeschlossen. Somit hatte jeder Zugriff auf die vom Großrechner gebotenen Ressourcen.

Eine erste Abhilfe brachten Terminalsysteme. Hier wurden Terminals (im Prinzip nur ein Monitor und eine Tastatur) ohne eigene Intelligenz an Großrechner angeschlossen und boten so einen Zugriff auf die Ressourcen bis hin zum Arbeitsplatz an (zum Beispiel IBM, Digital und Siemens).

Mit der beginnenden Entwicklung der Personal Computer (PC) kam die eigene Verarbeitungskapazität bis an den Arbeitsplatz heran.

Vor allem aus Kostengründen wurde sofort die Frage nach einer gemeinsamen Nutzung von Ressourcen laut (ein Laserdrucker kostete 1985 noch über DM 20 000). Auch war es relativ umständlich, die Daten auf einem PC zu erzeugen und dann per Diskette oder als Ausdruck weiterzugeben.

Dazu kommt noch, dass nun Dinge wie die Datensicherung, die Benutzerverwaltung und die Systempflege auf jedem Rechner einzeln durchgeführt werden mussten, was einen sehr großen Aufwand an Administration darstellte. Was früher zentral am Großrechner administriert wurde, musste nun an jedem Arbeitsplatz einzeln bewältigt werden. Die Lösung war die Vernetzung. Sie bot Datenaustausch und -sicherung, Ressourcenteilung, zentralisierte Userverwaltung und -authentifizierung in einem an.

Mit der zunehmenden Kommunikationsfähigkeit und Leistungskapazität der PCs wurde ein Ende der zentralen Großrechner vorausgesagt. Heute ist jedoch der gängige Zustand eine Koexistenz beider. Im Netzwerk untereinander erreichbar bieten Großrechner enorme Rechenkapazitäten, Fileserver zentrale Datenhaltung und -sicherung sowie Printserver, Faxserver etc. eine gemeinsame Ressourcennutzung an. Die Arbeitsplatzstationen als Ersatz der „dummen“ Terminals bieten dabei aber genug „Intelligenz“ für die täglichen Anwendungen vor Ort ohne Belastung des Zentralsystems an.

Das frühere Sternsystem, Zentraleinheit und sternförmig angeschlossene Datenterminals und das Peer-to-Peer-Netzwerk, ein vermaschter Netzwerkverbund von gleichwertigen Stationen, sind in heutigen Client-Server-Umgebungen zusammengeflossen.

In vielen Fällen tendiert man heute wieder dazu, Dienste auf Servern zu konsolidieren. Die Leistungsfähigkeit der Server ist enorm gestiegen, Terminalsysteme sind heute fast für alle Betriebssysteme erhältlich.

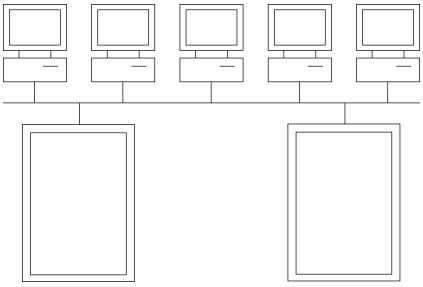


Bild 1.2 Ein heterogenes Netzwerk: Hier sind Clients und Server miteinander vernetzt. Die Server bieten spezielle Dienste an, die von allen genutzt werden können.

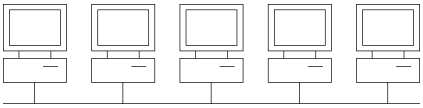


Bild 1.3 Ein Peer-to-Peer-Netzwerk. Gleichwertige Stationen sind untereinander vernetzt.

Im Laufe der Jahre wurden immer mehr dieser isolierten Netzwerke (Intranets) an das weltweite Internet angeschlossen. Ein Austausch von Daten ist daher weltweit möglich. Mehr zum Thema Internet folgt weiter unten.

1.2 Definition eines Netzwerkes

Was ist denn nun ein Netzwerk? Der Begriff Netzwerk umfasst nicht nur die Welt der Computer. Das weltweite Telefonnetz, das ISDN, der Verbund der Bankautomaten etc. sind ebenfalls Informationsnetzwerke.

Generell lässt sich daher definieren:

> *Ein Netzwerk ist eine Infrastruktur, die Datenendgeräten die Kommunikation, den Datenaustausch und die Nutzung gemeinsamer Ressourcen transparent ermöglicht.*

Transparent bedeutet, der Endbenutzer muss sich nicht darum kümmern, mithilfe welcher Verfahren, Geräte und Medien die Informationen transportiert werden.

Hier in diesem Buch wollen wir uns mit Computernetzwerken beschäftigen, obwohl durchaus Überschneidungen auftreten, zum Beispiel bei PPP (Point to Point Protocol, siehe unten), dem Netzwerkzugang über den Telefonanschluss und ein Modem. Hier benutzt das Computernetzwerk die Infrastruktur des Telefonienetzwerkes zur Datenübertragung.

Was muss beachtet werden, um eine bestehende Netzwerkinfrastruktur ausnutzen zu können? Welche verschiedenen Geräte und Medien sind im Einsatz, und was muss dabei berücksichtigt werden? Die Technik, die Geräte, die Verkabelung und die Softwareparameter, die im alltäglichen Gebrauch verwendet werden, stehen im Vordergrund dieser Einführung. Ebenso die Terminologie. Es gilt, in den gängigen Fachbegriffen firm zu werden. Das Ziel ist es, einen Einstieg in die Materie Netzwerk zu bekommen, der es ermöglicht, je nach Interesse, in die vielen verschiedenen Facetten des Themas tiefer einzusteigen. Die Frage „Wie funktioniert es?“ steht im Vordergrund, ebenso und vor allem auch das Verstehen der Grundlagen.

Im Laufe der Jahre wurden nun viele Typen von Netzwerken entwickelt, meist isoliert und herstellerabhängig. Mit der Einführung der (welt-)weiten Verbindungen mussten Standards ausgearbeitet werden, die entweder eine weltweite Konvergenz herbeiführten oder eine Übersetzung der Verfahren ermöglichten. Dies gilt für den physikalischen Aufbau (Netzwerkgeräte, Verkabelung etc.) genauso wie für die Datenformate.

1.3 Das OSI-Modell

1984 entwickelte die ISO (International Standardization Organisation) ein umfassendes Modell für die Kommunikation unter Computern, das OSI-Referenzmodell (Open Systems Interconnection). In diesem wird die Kommunikation zwischen Rechnern in sieben in sich abgeschlossene Schichten aufgeteilt. Jede Schicht kann somit einzeln weiterentwickelt werden, ohne die gesamte Kommunikation zu beeinflussen.

Tabelle 1.1 Das OSI-Modell in der Übersicht: Jede Zeile beschreibt einen Layer des Modells.

Layer VII	Anwendungsschicht	(Application)
Layer VI	Darstellungsschicht	(Presentation)
Layer V	Kommunikationsschicht	(Session)
Layer IV	Transportschicht	(Transport)
Layer III	Vermittlungsschicht	(Network)
Layer II	Sicherungsschicht	(Data Link)
Layer I	Physikalische Schicht	(Physical)

Für den Netzwerker sind die Schichten eins bis vier essenziell. Sie regeln die Datenübertragung an sich, die Schichten fünf bis sieben sind anwendungsbezogen. Pro Schicht sind viele verschiedene Standards implementiert.

Wichtig ist im OSI-Modell, dass die Kommunikation zwischen Rechnern und zwischen den Schichten geregelt ist. Ob PC 1 nun eine andere Implementierung von Layer I benutzt als PC 2, muss für die anderen Schichten bedeutungslos sein. Genauso muss es egal sein, ob die Maschinen Unix, Mac OS, Windows oder ein anderes Betriebssystem benutzen.

1.4 Übersicht über das OSI-Modell

Zu Beginn ein kleiner Vorgriff. Der Leitfaden für den Einstieg in das Netzwerk wird das OSI-Modell sein, Layer für Layer. Daher ein kurzer Überblick. Einige Parameter sind sicher bekannt. Wie sie zusammenhängen, werden wir Schritt für Schritt erarbeiten.

Das OSI-Modell ist sehr wichtig. Im Umfeld der Netzwerker ist es eine Arbeitsschablone. Netzwerker reden von „Layer II-Problemen“, „Layer III-Grenzen“ etc. Man sollte daher auf jeden Fall in diesem Modell firm sein. Aber genauso muss man immer bedenken, dass das OSI-Modell ist, was sein Name besagt – ein Modell. Es ist nirgends genau implementiert, es gibt etliche Abweichungen und Ausnahmen.

Es hilft uns aber, die Zusammenhänge zu verstehen, und wir begehen keinen Fehler, zuerst einmal anzunehmen, alles würde OSI-konform verlaufen.

1.4.1 Layer I – die physikalische Schicht (Physical)

Hier sind, wie schon der Name sagt, die physikalischen Parameter definiert. Dazu gehören die Kabeltypen, die Anschlüsse, die Streckenlängen, die elektrischen Eckdaten wie Spannungen, Frequenzen etc. Getrennt wird hier in drei Bereiche:

- Der Nahbereich (LAN, Lokal Area Network, meist in einem Gebäude),
- mittlere Entfernungen (MAN, Metropolitan Area Network, meist Gebäudeverbindungen) und
- die Fernverbindungen (WAN, Wide Area Network, Fernstrecken bis weltweit).

Beispiele für die Standards im Layer I sind zum Beispiel verschiedene Übertragungsmedien wie Kupferkabel, Glasfaser, Richtfunk, Signalform und Frequenzen im Medium.

1.4.2 Layer II – die Sicherungsschicht (Data Link)

Die Sicherungsschicht ist für eine zuverlässige Übertragung der Daten zuständig. Sie regelt die Flusssteuerung, regelt den Zugriff, verhindert eine Überlastung des Empfängers und ist für die physikalische Adressierung innerhalb eines Netzsegmentes (siehe unten) auf dieser Schicht verantwortlich. Hier ist die erste Fehlererkennung implementiert. Die Topologie eines Netzwerkes ist stark von dieser Schicht abhängig, sie definiert die Art und Weise, wie die Rechner und Netzwerkgeräte miteinander verbunden sind.

Ein Beispiel im Layer II sind Hardwareadressen.

1.4.3 Layer III – die Vermittlungsschicht (Network)

In Schicht drei des OSI-Modells wird die logische Adressierung (segmentübergreifend bis weltweit) der Geräte definiert. Die Routing-Protokolle dieser Schicht ermöglichen die Wegfindung in großen (bis weltweiten) Netzwerken und redundante Wege ohne Konflikte. Routing-Protokolle sorgen ebenfalls dafür, dass die Ressourcen in vermaschten Netzen mit vielen redundanten Wegen bei dem Ausfall einer Verbindung weiterhin benutzt werden können.

Quality of Service (QoS), Routing und das IP-Protokoll sind Beispiele im Layer III.

1.4.4 Layer IV – die Transportschicht (Transport Layer)

Die Transportschicht beschreibt Mechanismen für den Datentransport zwischen Anwendungen und Prozessen auf verschiedenen Endgeräten. Die Schicht vier regelt das Datenmultiplexing und die Flusskontrolle, das heißt, mehrere Anwendungen höherer Protokolle können gleichzeitig Daten über eine Netzwerkverbindung transportieren. In der Transportschicht sind verbindungslose und verbindungsorientierte Dienste implementiert. Der Begriff Verbindung bezieht sich dabei auf eine logische Verbindung zwischen zwei Anwendungen bzw. Prozessen. Verbindungsorientierte Dienste können einen zuverlässigen Datenaustausch durchführen. Der Sender und der Empfänger kontrollieren ihre Möglichkeiten der Kommunikation (Aufbau einer logischen Verbindung), die Daten werden erst nach dieser Prüfung versandt. Eine weitgehende Fehlerkontrolle prüft die Daten und for-

dert entweder verlorene oder korrumpierte Daten zur erneuten Übersendung an. Am Ende der Kommunikation wird die Verbindung gezielt und kontrolliert wieder abgebaut. Verbindungslose Dienste verzichten auf den Verbindungsaufbau und -abbau sowie auf die Wiederholung der Übertragung verlorener oder korrumpierter Pakete. In der Regel führen sie dennoch eine Fehlerkontrolle durch. Dabei werden fehlerhafte Daten nicht erneut angefordert, sondern stillschweigend verworfen und nicht an höhere Schichten weitergegeben. Im Layer IV wird nach definierten Anwendungen unterschieden. Hier beginnt die Kommunikation zwischen dem Netzwerk und der Anwendung.

Beispiele im Layer IV sind etwa das TCP- oder das UDP-Protokoll.

1.4.5 Layer V – die Kommunikations-/Sitzungsschicht (Session)

Die Kommunikationsschicht ist hauptsächlich eine „Serviceschicht“ für die bidirektionale Kommunikation von Anwendungen in verschiedenen Endgeräten. Sitzungen und Datenströme werden angefordert, aufgebaut, kontrolliert und koordiniert. Meist bedienen sich die Services der Schicht V dabei der Dienstangebote der Schicht IV.

Ein Beispiel im Layer V ist unter anderem das SMB-Protokoll zum Drucken und zum Verbinden mit Windows-Freigaben.

1.4.6 Layer VI – die Darstellungsschicht (Presentation)

Die Darstellungsschicht sorgt dafür, dass die Daten so bearbeitet werden, dass sie optimal ausgetauscht und verarbeitet werden können. Hierfür gibt es etliche standardisierte Kodierungs-, Konvertierungs- und Kompressionsverfahren, zum Beispiel für Verschlüsselungsroutinen, Zeichendarstellungen, Video- und Audioübertragungen.

Beispiele im Layer VI sind Standards wie MPEG, TIFF, GIF und ASCII.

1.4.7 Layer VII – die Anwendungsschicht (Application)

Die Anwendungsschicht interagiert direkt mit der Software (Anwendung), die eine Netzwerkübertragung anfordert. Sie ermittelt, ob die Möglichkeit einer Verbindung besteht, und identifiziert und sucht Ressourcen.

Beispiele im Layer VII sind verteilt arbeitende Server-Client-Lösungen sowie Kontroll- und User-Interfaces.

1.5 Übertragungswege im OSI-Modell

Das OSI-Modell selbst bietet natürlich keine Möglichkeit, Daten auszutauschen, sondern liefert die Rahmenbedingungen, mit denen ein Datenaustausch unter den verschiedensten Systemen reglementiert wird. Die Datenübertragung wird von den Implementierungen der Regeln durch die Hersteller innerhalb der Schichten mittels Protokollen vorgenommen.

Ein Protokoll ist also nichts anderes als eine Aufstellung von definierten Regeln zur Kommunikation. Dabei kommuniziert eine Schicht virtuell mit derselben Schicht (Anwendung/Protokoll) auf dem Kommunikationspartner. Der wirkliche Weg der Daten ist von oben durch die Schichten bis nach unten auf Layer I, dann die Übertragung über das Medium und beim Empfänger wieder vertikal nach oben.

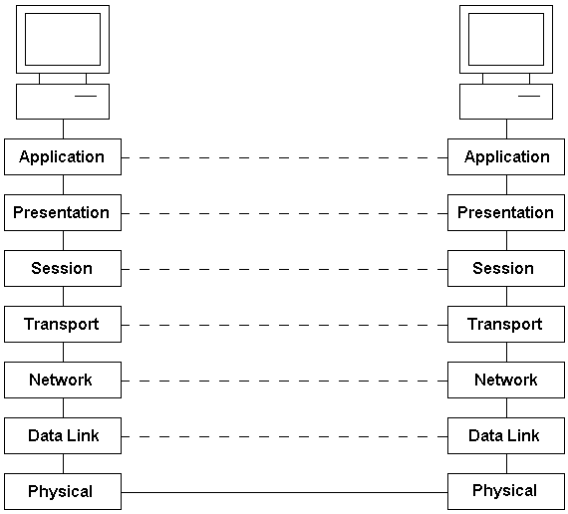


Bild 1.4 Die virtuelle (gestrichelt) und die echte Kommunikation: Jede Schicht kommuniziert scheinbar mit derselben auf dem Partner. In Wirklichkeit aber verläuft die Kommunikation vertikal durch alle Schichten nach unten, die Daten werden über die physikalischen Medien versendet und nehmen ihren Weg dann wieder vertikal bis zum Ziel.

Der große Vorteil ist, sofern sich die Hersteller an die Standards und Schichtung halten, dass jeder, der einen Dolmetscher für seine eigene Art der Implementierung eines Layers anbietet, mit allen anderen kommunikationsfähig bleibt.

So ist es möglich, dass Apple-Computer, Intel-basierte Computer unter Windows oder Linux, Unix-Computer unter Solaris, DEC-Unix etc. untereinander kommunizieren, Daten austauschen und gemeinsame Ressourcen anbieten und nutzen können.

Jede Schicht verpackt das Datenpaket, das sie von einer höheren zur Weiterverarbeitung bekommt, in ein eigenes „Kuvert“ und reicht es eine Schicht weiter.

Beim Empfänger läuft es genau andersherum. Jede Schicht entfernt ihr Kuvert und reicht das Paket nach oben weiter. Schicht vier zum Beispiel ist dabei absolut uninteressiert daran, was vorher für eine Verpackung um das Paket war und über welches Medium es transportiert wurde. Sie interessiert es auch nicht, was als Inhalt im Paket ist, lediglich das „Kuvert Schicht vier“ ist für sie von Bedeutung. So wird deutlich, wie die Interkommunikation unter den verschiedensten Plattformen und Systemen möglich wird. Sind die Protokolle korrekt implementiert, steht der Kommunikation nichts mehr im Wege.

Sind zwei völlig inkompatible Netze zu verbinden, muss ein Gerät dazwischengeschaltet werden, das eine Übersetzung vornimmt, bis zu der Schicht, die wieder gleich implementiert ist. Ein Beispiel auf Layer I ist ein Medienkonverter, der z. B. ein Kupfer- mit einem Glasfasernetz verbindet. Ein Beispiel auf Layer II ist ein Access Point, der ein WLAN-Netz mit Ethernet verbindet.

Ab dieser Übersetzung ist der Weg wieder völlig gleich. Die höheren Schichten bekommen von dieser Übersetzung nichts mit (ebenso der Anwender/User). Aber nochmals sei betont, das OSI-Modell ist ein Modell und so gut wie nirgends absolut starr implementiert. Es ist unser Leitfaden und eine Vorgabe für die Hersteller.

Als Beispiel kann der Brief verschiedener Bittsteller an den Präsidenten der Vereinigten Staaten gelten. Einmal kommt er von einer einsamen Insel, einmal aus einer Großstadt. Der Großstädter schreibt seinen Brief und wirft ihn frankiert in den nächsten Postkasten. Die Post befördert ihn über diverse Sortier- und Verteilerstellen per Bahn, LKW oder Flugzeug nach Washington und liefert ihn aus. Die Antwort des Präsidenten nimmt denselben Weg in die andere Richtung.

Der Inselbewohner geht dann zum örtlichen Telegrafenamt, von wo aus die Nachricht per Morsezeichen und Funk an die Küste übermittelt wird. Dort wird sie niedergeschrieben und per Fax nach Amerika geschickt. Der Kontaktmann des Volkes bringt das Fax zum Dolmetscher, der es übersetzt und danach als Brief weiterschickt. Auch hier nimmt die Antwort denselben Weg zurück.

Weder der Präsident noch die beiden Absender haben eine Ahnung vom Transport. Der Präsident bekommt zwei Briefe. Vom unterschiedlichen Weg, den der Inhalt genommen hat, muss er dabei nichts wissen. Ebenso ist es den Absendern egal, ob der eine morst und der andere schreibt. Beide Nachrichten finden ihren Weg hin und zurück, trotz der unterschiedlichen Wege. Der Inselbewohner sendet Morsesignale und erhält auf diese Weise auch die Antwort. Er braucht von allem anderen nichts zu wissen, virtuell hat ihm der Präsident per Morsezeichen geantwortet.

Der andere Bittsteller versendet einen Brief – und bekommt einen solchen zurück. Er hat keine Kenntnis davon, dass ein anderer Bittsteller Morsezeichen verwendet hat.

Beide haben aber ihr Ziel erreicht, sie haben kommuniziert. Sie könnten dies auch untereinander tun, auf dieselbe Art und Weise, ohne zu bemerken, dass sie lokal andere Methoden benutzen. Dies ist nicht das Ziel eines weltweiten Netzwerkes. Ziel ist, dass jeder mit jedem kommunizieren kann und sich keine Gedanken machen muss, wie seine Daten transportiert werden.

1.6 Allgemeine Bemerkungen

Was ist nun wichtig zu wissen, um einen Betrieb aufrechtzuerhalten? Was muss man über die Implementierung der Hersteller in den Schichten wissen, um einen Betrieb zu garantieren?

Die Layer I bis IV sind sehr netzwerkbezogen, die Layer V bis VII darstellungs- und anwendungsbezogen.

Im Verlauf dieser Einführung werden wir die Layer I bis IV schrittweise und realitätsbezogen kennenlernen. Die Layer V bis VII überlassen wir den Anwendern und Anwendungsentwicklern!

Dementsprechend ist der Hauptteil dieses Buches (Kapitel 2 bis 13) den Layern I bis IV gewidmet. Diese werden in den Kapiteln 2 bis 5 aufeinander aufbauend behandelt. Kapitel 6 geht auf neue Aspekte in diesen Layern ein, die sich aus dem immer stärker werdenden Trend zur Virtualisierung von Hardware ergeben.

Die Kapitel 7 bis 9 behandeln den Zugang zum Netzwerk und dem Internet. Kapitel 7 befasst sich mit dem Netzwerkzugang von entfernten Standorten aus über Virtual Private Networks (VPN), während es in Kapitel 8 um den lokalen drahtlosen Zugang über Wireless LAN geht. Verschiedene Szenarien für die Anbindung eines Netzwerks an das Internet werden in Kapitel 9 vorgestellt.

Einer der wichtigsten Technologiewechsel im Internet ist die Umstellung des Layer III von IPv4 auf IPv6. Während Kapitel 4 hauptsächlich auf IPv4 basiert, wird IPv6 in Kapitel 10 behandelt.

Netzwerkspeicher sind ein wichtiger Bestandteil heutiger Netzwerkumgebungen. Obwohl diese teilweise auf Layer VII Protokollen basieren, werden sie im Hauptteil des Buches in Kapitel 11 beschrieben.

Ein Repetitorium mit Wiederholungsfragen sowie praktischen Übungen schließen den Hauptteil des Buches in Kapitel 12 bzw. 13 ab.

Im Anhang finden sich in Kapitel 14 vertiefende Exkurse, die bewusst aus dem Hauptteil ausgelagert wurden. Darüber hinaus enthält Kapitel 15 Beispiele für die Netzwerkplanung in verschiedenen Szenarien unter Verwendung von Bausteinen aus dem Hauptteil. Eine Übersicht über gängige Steckertypen findet sich in Kapitel 16. Kapitel 17 gibt praktische Hinweise zur Fehleranalyse. Der Anhang schließt mit einem Abkürzungsverzeichnis und dem Stichwortverzeichnis.

Wir werden sehen, dass sich die verschiedenen Implementierungen der Layer und die Protokolle nicht absolut genau an das OSI-Modell halten. Es ist auch kein starres Gesetz, sondern ein Kommunikationsmodell. Leichte Abweichungen, die sich die Hersteller erlauben, sind ohne Bedeutung, solange sie irgendwann wieder an der Grenze der Schichten korrigiert werden. Ab dieser Schicht ist wieder eine native (OSI-konforme) Kommunikation möglich. Die Protokolle, die auf den verschiedenen Schichten angesiedelt sind, sind nichts Anderes als festgelegte Regeln, nach denen verfahren werden muss. Benutzen alle dieselben Protokolle oder gibt es Protokollübersetzer, steht dem Datenaustausch nichts mehr im Wege.

Das OSI-Modell ist ein essenzielles Werkzeug im Netzwerkbereich. Jeder, der in diesem Gebiet tätig ist, sollte die Layer und ihre Bedeutung genau kennen. Nochmals sei betont, das OSI-Modell ist ein Modell. Wir werden es als festes Modell betrachten und mit ihm arbeiten. Aber wir müssen immer im Hinterkopf behalten, dass es nirgends so implementiert ist, wie wir hier annehmen. Trotzdem begehen wir keinen Fehler, wenn wir uns an ihm orientieren.

1.7 Zum Weiterlesen

In der Welt der Computernetzwerke ist vieles standardisiert, das bedeutet, dass in offiziell verabschiedeten Dokumenten festgelegt ist, wie die Dinge funktionieren. Dies ist dringend notwendig, da wir in der Regel Geräte verschiedener Hersteller über das Netzwerk miteinander verbinden und alles reibungslos funktionieren soll. Wir werden im Laufe des Buches immer wieder auf Standards verweisen, in denen der interessierte Leser weitere Details finden kann. Es ist immer lohnenswert, einen Blick hineinzuwerfen.

Es gibt zahlreiche Organisationen, die sich mit der Standardisierung befassen. Die erste Organisation, die in diesem Buch genannt wurde, ist die Internationale Organisation für Normung (ISO). Interessierten Lesern empfehlen wir einen Blick in den offiziellen Standard [ISO1994], der das ISO/OSI-Modell detailliert beschreibt.

Literatur

[ISO1994] International Organization for Standardization (ISO): ISO/IEC 7498-1:1994 – Information Technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. International Organization for Standardization, 1994. Zugegriffen am 18.07.2023. *https://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip*

2 Layer I des OSI-Modells

2.1 Die Medien

Auf der untersten Ebene des OSI-Modells ist definiert, was „über den Draht“ kommt. Die Bedeutung wird oft unterschätzt. Jedoch sind wir in der Regel in kleinen bis mittleren Umgebungen hauptsächlich mit Layer I und II eines Netzwerkes konfrontiert.

Im Layer I sind die physikalischen Parameter definiert, der Aufbau der Netzwerkkabel, die elektrischen Eckdaten, die Spannungen, die Frequenzen etc.

Der Layer I beinhaltet vor allem das Sichtbare eines Netzwerkes. Ca. 80 % aller Fehler, Ausfälle und Störungen entstehen durch Schäden an der Verkabelung und durch defekte Netzwerkgeräte! Besonders mit der Verkabelung wird in der Regel sehr nachlässig umgegangen. Wie wir sehen werden, ist dies mit einem hohen Risiko verbunden. Die Empfindlichkeit der Kabel wird meistens unterschätzt. Die Korrekturmechanismen höherer Layer sind in der Regel sehr gut, defekte Daten werden nachgefordert, sodass der Benutzer einer maladen Verkabelung in erster Linie nichts bemerkt, außer dass die Performance durch hohe Fehlerraten eingeschränkt ist.

Wir werden uns hier mit den gängigsten Typen der Verkabelung beschäftigen, sollten aber immer im Hintergrund bedenken, dass es noch viele andere Typen gibt. Wir wollen uns nun der Reihe nach genau ansehen, was es für Medien gibt, ihre Charakteristika und ihre Spezifikationen näher kennenlernen. Darüber hinaus wollen wir genau betrachten, wie die Daten im Medium übertragen werden.

Darüber hinaus beschäftigen wir uns schwerpunktmäßig mit der weitverbreiteten Ethernet-Technologie [Healey2023]. Ursprünglich mit einer Datenrate von wenigen Mbit/s gestartet, können heute Datenraten von mehreren Hundert Gbit/s erreicht werden.

Ethernet mit 100 Mbit/s Datenrate wird „Fast Ethernet“ genannt, mit 1000 Mbit/s Gigabit Ethernet, mit 10 Gbit/s 10 Gigabit Ethernet.

2.2 Historische Verkabelung: Thin-Wire (Koaxialkabel)

Am Anfang stand (bei Ethernet) das Thin-Wire-(dünner Draht) oder Koaxialkabel. Es besteht aus einem Kupferaderkern, der mit einer Kunststoffschicht ummantelt ist. Um diese liegt eine leitfähige Folie bzw. ein Metall-Flechtmantel (aus Gründen der Abschirmung, das Prinzip eines Faraday'schen Käfigs). Den Außenmantel bildet wiederum eine feste Kunststoffschicht. Die Kabel sind sehr robust und durch ihren Aufbau ausgezeichnet gegen elektromagnetische Störungen abgeschirmt.

Bild 2.1 Aufbau eines Standard-Koaxialkabels

Bei der Koaxialverkabelung wird ein Strang gelegt. Er darf aufgrund der Physik der Übertragung nicht weiter verzweigt werden. Die Computer werden mithilfe von T-Stücken und BNC-Steckern (Bayonet Navy Connectory) angeschlossen. Ein Bild dazu ist in Kapitel 16, „Steckertypen", zu finden.

Aufgrund der elektrischen Vorgaben darf der Weg zwischen dem T-Stück und der Netzwerkkarte beim klassischen Thin-Wire-Netz niemals verlängert werden. Das Kabel muss also an jeden Arbeitsplatz herangeführt werden. Sind Wanddosen montiert, müssen diese bei der Nichtbenutzung überbrückt werden, anderenfalls müssen die im Raum angeschlossenen Geräte in eine Schleife integriert werden.

Die maximale Länge eines Stranges darf 180 m betragen. Weitere Ausdehnungen sind möglich, wenn Verstärker (Repeater) eingesetzt werden. Maximal können fünf Segmente mit vier Verstärkern gekoppelt werden, was eine Gesamtlänge von 900 m ergibt. Auch wenn dies möglich ist, sollte so verkabelt werden, dass keine so langen Segmente benötigt werden.

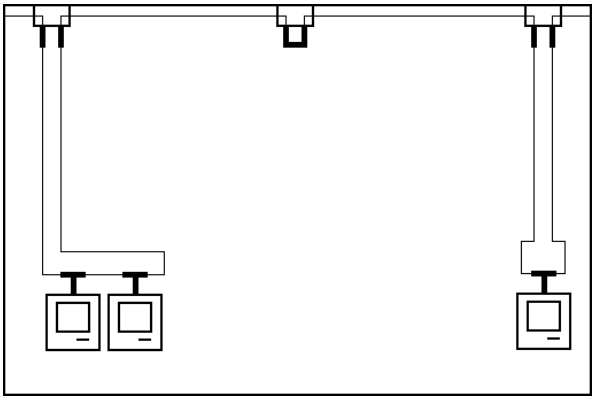


Bild 2.2 Beispiel eines Büros: Das Thin-Wire-Kabel wird an die Geräte herangeführt und der Strang als eine Kette von angeschlossenen Geräten konfiguriert. Anschlussdosen, die nicht benutzt sind, werden überbrückt.

Wichtig bei dieser (eigentlich jeder!) Verkabelung ist, dass der Biegeradius der Kabel eingehalten wird. Zu stark verbogene oder geknickte Kabel führen zu Brüchen in der Ader oder der Schirmungsfolie, mit gravierenden Auswirkungen auf die Leistung bis hin zum Netzausfall. Wie wir noch sehen werden, ist der physikalische Aufbau der Kabel entscheidend mit der Funktion verbunden. Knicke und Schäden bewirken eine immense Beeinflussung der Funktion.

An den beiden Enden eines Stranges muss auf die letzten T-Stücke ein Endwiderstand (Terminator, 50 Ohm) aufgesetzt werden. Ohne diese ist ein Datenverkehr unmöglich. Sie unterbinden Fehler, die hardwaremäßig vorgegeben sind.

Zum Verständnis werfen wir einen kurzen Blick in die Physik. Sendet eine Netzwerkkarte ein Signal ins Medium, breitet sich dieses in beide Richtungen aus. Trifft das Signal auf eine Barriere, sprich einen stark erhöhten Widerstand, wird es reflektiert und läuft zurück. Dabei zerstört es sich selbst und andere Signale durch Überlagerung. Am Ende des Stranges (unendlicher Widerstand am Ende des Kabels) muss das Signal folglich bewusst vernichtet werden. Dies erledigt ein Widerstand, der exakt denselben Widerstand wie das Medium besitzt. Er sorgt dafür, dass das Medium für den Sender in beide Richtungen unendlich lang erscheint, sodass keinerlei Reflexionen auftreten.

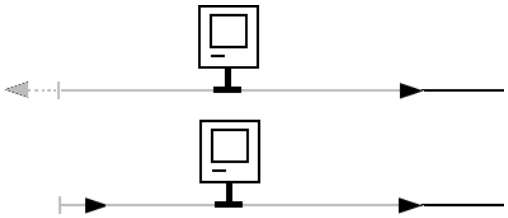


Bild 2.3 Das gesendete Signal läuft an dem Medium entlang. Erreicht es sein Ende, wird es reflektiert (links unten), läuft im Medium zurück und zerstört sich und alle anderen Signale durch Überlagerung. Wird das Signal am Ende des Mediums bewusst vernichtet, erscheint das Medium der sendenden Station unendlich lang (oben). Reflexionen treten nicht auf.

Das im Netzwerkbereich verwendete Koaxialkabel (Thin Wire) hat einen Wellenwiderstand von 50 Ω. Daher werden Endwiderstände mit diesem Wert eingesetzt. Der Wellenwiderstand ist deutlich zu unterscheiden vom ohmschen Widerstand des Kupferleiters selbst, der gegen null geht. Der Wellenwiderstand ergibt sich aus der Tatsache, dass zur Übertragung hochfrequente elektrische Signale verwendet werden. Für diese gelten andere Regeln als für Gleichstrom, z. B. ist eine Spule für Gleichstrom kein Hindernis, für hochfrequente Signale aber ein großer Widerstand. Für Interessierte sei an dieser Stelle auf weiterführende Literatur zur Elektrotechnik verwiesen.

Starke Verformungen des Kabels beeinflussen lokal den Wellenwiderstand und führen zu Reflexionen, die das Netzwerk außer Betrieb setzen können. Wichtig ist die Dielektrizitätskonstante, d. h. direkt der physikalische Aufbau, das Material und die Geometrie des Mediums. Eine Verformung oder ein Knicken des Kabels ist daher zu vermeiden, da der physikalische Aufbau beeinträchtigt wird.

Anmerkung: Ein Datenübertragungssystem, das aus einem durchgehenden Medium besteht, das von mehreren Kommunikationsgeräten gemeinsam genutzt wird, wird als Bussystem bezeichnet. Jedes Bussystem muss aus den oben genannten Gründen terminiert werden. Zum Beispiel muss am Ende einer SCSI-Kette ein Terminator verwendet werden.

Der große Nachteil der Koaxialverkabelung ist zum einen die Beschränkung auf eine maximale Übertragungsrate von 10 Mbit/s. Theoretisch sind bis zu 50 Mbit/s möglich, aber der Standard, das klassische Ethernet, liegt per Definition bei 10 Mbit/s. Zum anderen ist das Ausfallrisiko hoch: Wird der Strang unterbrochen, beschädigt oder ein Terminatorwiderstand entfernt, ist der gesamte Strang wertlos. Niemand kann mehr kommunizieren, auch nicht über intakte Bereiche des Kabels hinweg. Ein Vorteil ist die hervorragende Abschirmung (Faraday'scher Käfig).

Aufgrund der eingeschränkten Übertragungsgeschwindigkeit und der Gefahr eines Totalausfalls der Netzwerkverbindung im Fehlerfall wird Thin Wire heute bei Neuverkabelungen nur noch sehr selten eingesetzt. Lediglich in Bereichen mit hohen elektromagnetischen Störfeldern kann eine Koaxialverkabelung heute noch sinnvoll sein. Aber auch hier werden zunehmend Glasfasern eingesetzt.

2.3 Die universelle Gebäudeverkabelung (UGV)

Aufgrund dieser Nachteile entwickelte man eine andere Art der Verkabelung, wie sie heute bei Netzwerken gängig im Einsatz ist, die UGV, die universelle Gebäudeverkabelung.

Der Standard sind heute achtaderige Kabel, die je nach Qualität und Abschirmung verschiedenen Kategorien angehören. Durchgesetzt hat sich als Verbindung der sogenannte Western-Modularstecker. Er ist in Kapitel 12, „Steckertypen", am Ende des Buches abgebildet. Vier der Adern des Kabels sind vom Netzwerk im Gebrauch. Es ist also möglich, mit speziell verkabelten Anschlussdosen zwei volle Geräteanschlüsse über ein Kabel zu erschließen. Dies gilt jedoch nur bis 100 Mbit/s (Fast Ethernet). Bei Gigabit oder 10 Gbit Ethernet wird heute mit allen acht Adern gearbeitet (4 × 250 Mbit/s bzw. 4 × 2,5 Gbit/s im Channel). Hier ist nur eine Dose pro Kabel möglich.

Wieso eine UGV? Es ist unflexibel, das Netzwerk, die Telefonie etc. getrennt zu verkabeln, daher setzt man heute, wenn möglich, nur noch eine Sorte der Verkabelung ein, die dem höchsten Qualitätsstandard genügt.

Zwar ist zum Beispiel eine klassische zweiadrige Telefonverkabelung erheblich billiger als eine hochwertige Netzwerkverkabelung, aber diese ist in der Lage, alle Services zu übertragen, und die Flexibilität in Zukunft ist gewährleistet. Es ist möglich, alle Signale, von ISDN über Wechselsprechanlagen bis zur Haustürklingel, über diese Kabel zu führen und später frei zu variieren, welcher Dienst und welches Gerät wo angeschlossen wird.

Die Anordnung der acht Adern des Kabels ist wohldefiniert. Je immer zwei sind in ineinander verdrillten Zweierpärchen angeordnet. Diese vier Pärchen wiederum sind in sich nochmals verdrillt im Kabel angeordnet, daher der Name Twisted Pair. So wird dafür gesorgt, dass die Strecken, in denen die Adern im Kabel parallel nebeneinander verlaufen, minimiert sind und dadurch Störeinflüsse von Ader zu Ader durch elektromagnetische Abstrahlungen und Signalübertritte minimiert werden. Diese Signalübertritte nennt man im Fachjargon „Nahnebensprechen" oder NEXT (Near End Crosstalk).