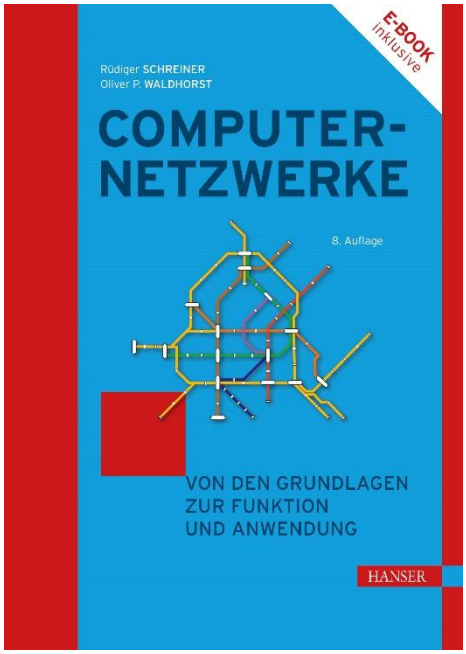
HANSER



Leseprobe

zu

Computernetzwerke

von Rüdiger Schreiner und Oliver P. Waldhorst

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

Weitere Informationen und Bestellungen unter
https://www.hanser-kundencenter.de/fachbuch/artikel/9783446474154
sowie im Buchhandel

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

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.

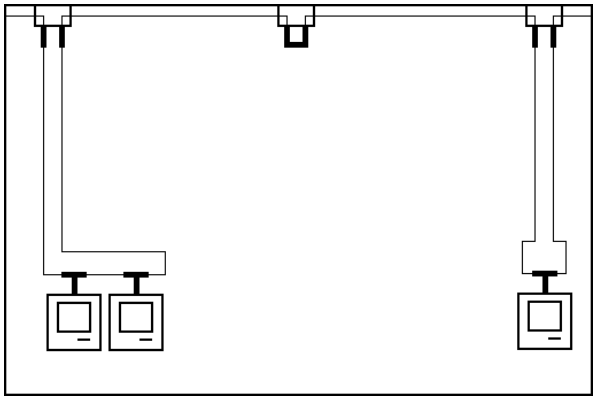


Bild 2.2 Beispiel eines Büros: Das Thin-Wire-Kabel wird an die Geräte herangeführt und der Strang als eine Kette von angeschlossenen Geräten konfiguriert. Anschlussdosen, die nicht benutzt sind, werden überbrückt.

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.

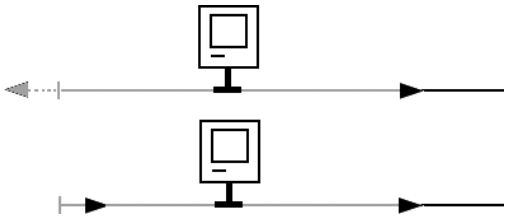


Bild 2.3 Das gesendete Signal läuft an dem Medium entlang. Erreicht es sein Ende, wird es reflektiert (links unten), läuft im Medium zurück und zerstört sich und alle anderen Signale durch Überlagerung. Wird das Signal am Ende des Mediums bewusst vernichtet, erscheint das Medium der sendenden Station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

Dazu kommt, dass um jeden Leiter, durch den Strom fließt, ein Magnetfeld entsteht. Eine richtige Verdrillung der Adernpaare sorgt auch dafür, dass die entstehenden Magnetfelder entgegengesetzt gerichtet sind und sich gegenseitig auslöschen oder zumindest gegenseitig abschwächen. Die Kabel haben einen Wellenwiderstand von 100 Ω. Die Gesamtlänge eines Segmentes darf 100 Meter betragen, für die Kaskadierung mit Verstärkern gilt dasselbe wie bei der Koaxialverkabelung.

2.3.1 Kabeltypen Twisted Pair

Gängige Übertragungsgeschwindigkeiten sind heute 1000 Mbit/s. Über Twisted-Pair-Kabel sind jedoch auch Geschwindigkeiten von 10 Gbit/s, 25 Gbit/s und 40 Gbit/s möglich. Diese werden häufig in Rechenzentren eingesetzt, dann in der Regel mit kürzeren Segmenten.

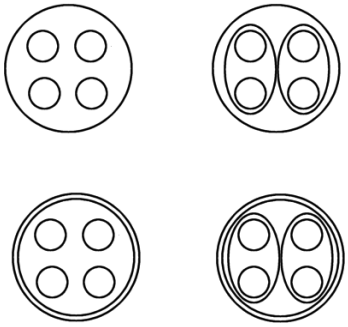


Bild 2.4 Übliche Kabeltypen im Netzwerk. Das gängigste Kabel ist UTP, Unshielded Twisted Pair (links oben). Zur weiteren Abschirmung gibt es die Varianten STP, Shielded Twisted Pair (rechts oben), und S/UTP, Shielded/Unshielded Twisted Pair (links unten). Einmal sind hier die Adernpaare selbst geschirmt, zum anderen wird das gesamte Bündel geschirmt. Die höchste Qualität hat S/STP, Shielded/Shielded Twisted Pair (rechts unten). Hier sind sowohl die Adernpaare einzeln als auch das gesamte Kabel nochmals geschirmt. S/STP ist einzusetzen, wenn hohe Störfelder erwartet oder die Längenrestriktionen erreicht werden. Nachteil ist ein wesentlich dickeres Kabel mit kritischeren Biegeradien. Abgebildet sind jeweils schematisch die vier Adernpaare.

Wie beim Koaxialkabel bestimmt der physikalische Aufbau den Wellenwiderstand. Knicke und Deformationen der Kabel müssen daher auch hier peinlich vermieden werden. Ebenfalls muss darauf geachtet werden, dass zu fest gezogene Kabelbinder das Kabel nicht quetschen, damit seine Geometrie verändern und so seine Eigenschaften erheblich beeinflussen.

Kritiker könnten nun anmerken, dass die Stecker widersprüchlich sind. Einerseits sprechen wir davon, dass die Kabel sehr empfindlich sind und schon Verformungen zu Qualitätsverlusten führen können. Andererseits benutzt man eine Steckertype, in der eben diese Geometrie völlig aufgehoben wird und alle Adern parallel in den Stecker ausgeführt werden. Diese Frage ist berechtigt, aber für eine sichere und handhabbare Verbindung müssen wir Qualitätsverluste in Kauf nehmen. Es sollten daher so wenig als möglich Verbindungsstellen im Netzwerk sein. Vier sind es in der Regel immer, zwei am Arbeitsplatz, beim Anschluss des Rechners an die Wanddose, und zwei am Verteiler/Switch (siehe unten). Gute Kabel verfügen über Stecker mit einer Metallhülle, die äußere Störeinflüsse abschirmt.

Bild 2.5 Hier sehen Sie ein aufgeschnittenes Kabel des Typs S/UTP. Deutlich sieht man die einzelnen in sich verdrillten Adernpaare. Um die Adernpaare liegt ein Mantel aus Metallgeflecht zur Abschirmung. Dies ist zwar teurer als Metallfolie, macht das Kabel aber beweglicher.

2.3.2 Verlegung der universellen Gebäudeverkabelung und Geräteverbindungen

Die Endgeräte werden nicht mehr in einer Kette, sondern in Form einer Sternverkabelung an einen Verteiler angeschlossen. Verteiler sind Geräte mit mehreren Netzwerkanschlüssen (im Fachjargon Ports). Diese wurden zunächst als sogenannte Hubs realisiert, die die an einem Netzanschluss eingehenden Signale an alle anderen Netzanschlüsse weiterleiten. Auf allen Kabelsträngen, die an einen Hub angeschlossen sind, liegen somit die gleichen Signale an.

In der Regel handelt es sich bei Verteilern heute aber um Switches, deren Funktionsweise im Rahmen der Behandlung von Layer II detailliert beschrieben wird. An Switches werden die Endgeräte direkt angeschlossen, T-Stücke und Endwiderstände sind nicht mehr nötig, der Bus wird im Switch terminiert. Der Nachteil ist ein wesentlich höherer Bedarf an Kabeln. Der Vorteil ist, dass bei einem Unterbruch eines Kabels nur das betroffene Endgerät vom Netzwerk isoliert ist und nicht alle, wie bei der Koaxialverkabelung.

Die Kommunikation erfolgt über definierte Drähte. Die Sendeleitung eines Gerätes muss daher auf die Empfangsleitung seines Partners aufgeschaltet werden und umgekehrt. Die Switches müssen daher eine andere Pinbelegung der Stecker/Dosen besitzen als die Netzwerkadapter.

Werden zwei Switches bzw. zwei Endgeräte direkt miteinander verbunden, muss unter Umständen ein spezielles Kabel eingesetzt werden, das diese Leitungen richtig zusammenfügt, Senden und Empfangen werden hier überkreuzt, daher kommt der Name Crossover-Kabel (Pins 1 und 2 auf Pin 3 und 6 des RJ-45-Steckers). Vorsicht ist auch hier bei Gigabit-Ethernet und höheren Geschwindigkeiten geboten. Bei diesen werden alle Adern genutzt, man benötigt hier spezielle Crossover-Kabel. Diese werden als „doppelt gekreuzt“ bezeichnet.

Aus den genannten Gründen müssen Switches über einen Eingang verfügen, der in der Pinbelegung entweder schaltbar oder fest gekreuzt ist, den sogenannten Uplink-Port. Er sorgt dafür, dass nur eine Sorte Kabel verwendet werden muss und das Crossover-Kabel überflüssig wird. Zur Vereinfachung und Fehlervermeidung besitzen heutige Switches Anschlüsse, die selbstständig erkennen, ob andere Netzwerkgeräte oder Netzwerkadapter angeschlossen sind, und die Pinbelegung automatisch richtig umschalten.

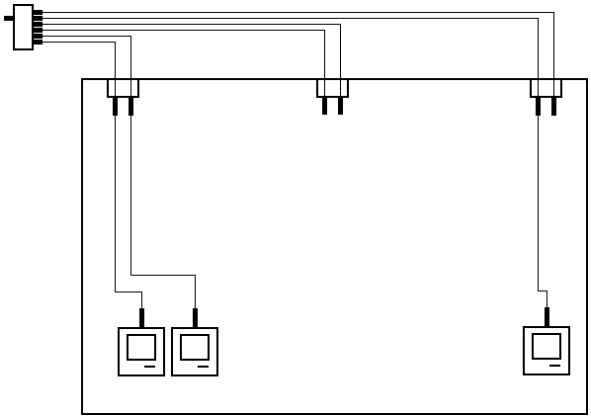


Bild 2.6 Eine Verkabelung nach UGV: Die Rechner werden direkt an einen Switch angeschlossen. Unbenutzte Dosen müssen nicht überbrückt werden, der Switch erkennt, ob ein Gerät angeschlossen ist oder nicht. Der Bus wird im Switch terminiert. Die Kabel werden an jede Dose herangeführt, die Endgeräte sind also „autonom“ angeschlossen. Wird ein Kabel beschädigt, ist nur ein Endgerät betroffen, nicht alle.

Diese Technologie nennt man „MDI-Autosensing“, und sie setzt sich langsam überall durch. Sie hat große Vorteile, denn es ist nur noch eine Sorte Kabel ist notwendig. Dies hat aber auch Nachteile, da hier Switches, an denen zwei Ports miteinander verbunden werden, einen Link (d. h. eine Verbindung) haben. Im Layer II werden wir kennenlernen, dass das katastrophale Auswirkungen haben kann. Ohne MDI-Autosensing passiert nichts, wenn wir oder unsere Anwender, zum Beispiel durch Verbinden zweier Anschlussdosen im Büro, aus Versehen zwei Ports mit einem Anschlusskabel verbinden, es funktioniert einfach nicht. Bei Ports mit MDI-Autosensing gibt es immer einen Link.

Nach dem Verständnis der Hersteller wird vom Switch ausgegangen. Alles, was an ihn angeschlossen wird, gilt im Prinzip als Endgerät, also auch zum Beispiel Router (siehe Layer III). Bei Verbindungen von Endgeräten zu Verteilern sind die Pinbelegungen bereits richtig vorbereitet, man benötigt kein Crossover-Kabel. Die Crossover-Kabel sollten daher gut gekennzeichnet werden, um Verwechslungen von vornherein auszuschließen.

■ 2.4 Glasfaser

Mit der Entwicklung der Glasfasertechnik wurde es möglich, wesentlich weitere Strecken zu überbrücken. Vor allem in der vertikalen Verkabelung von Gebäuden und zwischen ihnen war es wichtig, die Längenbeschränkungen zu umgehen. Da Glasfasern eine immer größere Rolle in der EDV spielen, wird hier besonders auf das Thema eingegangen.

Je nach Faser- und Sender-/Detektortyp können heute bis zu 10 – 120 km ohne Verstärker überbrückt werden, mit Verstärkern über 1000 km. Glasfasern sind äußerst leistungsfähig, die Übertragungskapazität wächst von Jahr zu Jahr. In Tests erreicht man bereits Übertragungsraten von mehr als einem Petabit/s (dies entspricht 1000 Terabit/s!).

Zur Verbindung von Endgeräten verwendet man üblicherweise 1000 Mbit/s. Im Backbone sind 100 Gbit/s und an einigen Stellen bereits bis zu 400 Gbit/s zu finden. Glasfasern sind sehr empfindlich bei Biegung und mechanischer Belastung. Ihre Vorteile neben der größeren einsetzbaren Länge sind die Abhörsicherheit (keine elektromagnetische Emission) und keinerlei Empfindlichkeit auf elektromagnetische Störeinflüsse. Ein weiterer großer Vorteil der Glasfasern ist die galvanische Trennung (Potenzialtrennung). Wird ein Gerät im Netzwerk durch Überspannungen oder Blitzschlag etc. zerstört oder beschädigt, wird dies, im Gegensatz zur Kupferverkabelung, nicht an andere Geräte weitergeleitet.

2.4.1 Exkurs in die Physik – Glasfasertypen, Lichtwellenleiter, Effekte

Heute sind standardmäßig drei Typen von Glasfasern im Einsatz. Es sind Multimode-Fasern mit Kerndurchmessern von 62,5 µm (die amerikanische Norm) und 50 µm (die europäische Norm) sowie Single- oder Monomode-Fasern mit 9 µm Kerndurchmesser. Es gibt unzählige Typen verschiedenster Aufbauarten. Sie alle hier zu beschreiben, wäre zu umfangreich. Daher ist zu beachten, dass hier nur die gängigsten beschrieben sind und es noch viele andere gibt, sowohl im physikalischen Aufbau als auch in der Funktion. Um die Namensgebung und die Funktion zu verstehen, müssen wir einen kleinen Exkurs in die Physik der Lichtwellenleiter wagen.

2.4.2 Lichtleitung in der Faser

Ein Lichtwellenleiter besteht aus einem Kern, der Licht leitet (meist aus Silizium-Germanium-Oxid, einem Glastyp, Kunststoffe sind bereits ebenfalls im Einsatz). Um den Kern liegt eine Kunststoffhülle. Die Faser selbst ist so dünn, dass sie nur unter einer starken Lupe sichtbar ist. Um die Hülle liegt ein Gelmantel, der erlaubt, dass sich der Kern geringfügig bewegen kann. Dies ist wichtig, da sonst der Biegeradius enorm wäre. Außen liegt dann eine Schutzhülle aus festem Kunststoff, die vor mechanischer Belastung schützt. Diese Schutzhülle gibt es in den verschiedensten Ausführungen, von relativ dünn bis hin zu sehr festen Mänteln bei erwarteter mechanischer Belastung. Bei Fasern, die in der Natur oder in Kanälen verlegt werden, kann aussen herum auch, wie bei Kupferkabeln, ein Nagetierschutz angebracht sein. Hier muss der Typ der Lichtwellenleiter nach dem Bedarf ausgesucht werden.

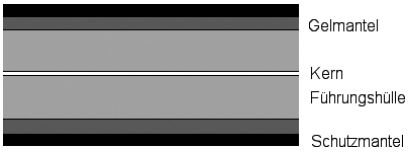


Bild 2.7 Der schematische Aufbau eines Lichtwellenleiters: Der Kern besteht aus dem das Licht leitenden Material. Er ist sehr dünn, mit dem bloßen Auge fast nicht zu sehen. Er wird von einer Kunststoffhülle gestützt. Diese ist von einem Gelmantel (oft aber auch ein Fadengeflecht) umgeben, der erlaubt, dass sich der Kern bewegen kann. Ganz außen ist eine Schutzhülle aus Kunststoff, die vor mechanischer Belastung schützt.

Interessant ist hier eigentlich nur der Faserkern, der das Licht leitet. Ein Lichtstrahl bewegt sich durch Totalreflexion im Lichtleiter fort. Trifft ein Lichtstrahl auf eine Grenzfläche zwischen zwei Materialien mit unterschiedlichem Brechungsindex, wird er gebrochen. Jeder hat das schon einmal selbst gesehen, der einen Stock ins Wasser steckt und von oben betrachtet. Es sieht so aus, als ob er an der Wasseroberfläche geknickt wäre. Wird der Einfallswinkel nun immer kleiner, erfolgt ab einem Grenzwinkel keine Brechung mehr, sondern Reflexion. Der Winkel, in dem eingestrahlt werden muss, damit es zur Reflexion kommt, heißt bei der Glasfaser die numerische Apertur.

Das Licht muss also in einem Winkel in die Faser eingeführt (in der Fachsprache sagt man eingekoppelt) werden, der eine Totalreflexion ermöglicht. Alles andere Licht wird weggebrochen und ist für uns und unsere Datenübertragung nutzlos.

Glas kennen wir als zerbrechliches Medium. Eine Faser ist aber derart dünn, dass sie ohne Bruch gebogen werden kann. Die meisten haben schon einmal die „Wunderlampen“ gesehen, die aus einem großen Büschel aus Glasfasern bestehen, das von einer Seite her beleuchtet wird. Schaltet man sie ein, sieht man winzige Lichtpünktchen an den Spitzen der Fasern.

Diese Fasern bewegen sich schon im kleinsten Luftzug und brechen auch bei der Biegebewegung in einem gewissen Rahmen nicht. Glasfasern haben natürlich trotz ihrer großen Biegefähigkeit einen definierten Bruchpunkt.

Wer eine Glasfaser knickt oder den Biegeradius überschreitet, zerstört diese sofort. Insbesondere sind Glasfasern auf Zug nicht belastbar. Sie sind spröde und reißen leicht. Dies wird durch die Zugstabilität der Hülle aufgefangen. Sie stellt die Zugentlastung dar, die diese Kräfte aufnimmt.

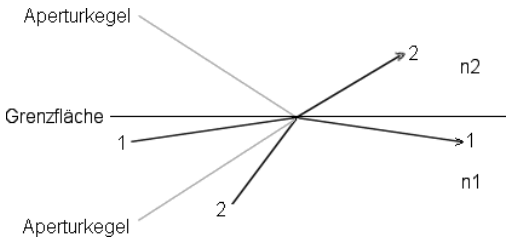


Bild 2.8 Trifft ein Lichtstrahl auf eine Grenze zwischen zwei Medien mit unterschiedlichem Brechungsindex, wird er gebrochen, sprich abgelenkt. Trifft er aber unter einem bestimmten Winkel auf, wird er reflektiert. Strahl 2 wird außerhalb der Apertur eingestrahlt und damit gebrochen. Strahl 1 liegt innerhalb der Apertur, daher wird er an der Grenzfläche reflektiert.

2.4.3 Die Stufenindexfaser

Um diese Grenzfläche zu realisieren, die zur Reflexion des Lichtes führt, ist der Faserkern aus zwei Schichten aufgebaut, dem Innenkern und dem Mantel. Diese beiden besitzen unterschiedliche Brechungsindices n.

Wird der Lichtstrahl innerhalb der Apertur in den Leiter eingekoppelt, bewegt er sich in diesem durch Totalreflexion vorwärts.

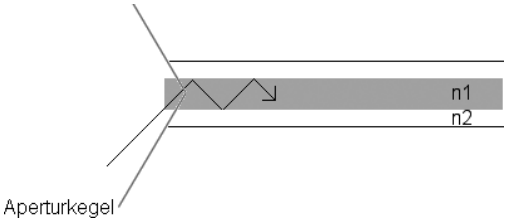


Bild 2.9 Der Kern besitzt eine höhere Brechzahl n als der Mantel. Daher bewegt sich ein Lichtstrahl, der innerhalb des Aperturkegels eingekoppelt wird, durch Totalreflexion im Lichtwellenleiter fort. Eine solche Glasfaser nennt man Stufenindexfaser, da hier der Brechungsindex im Kernleiter in einer Stufe verändert wird und im Mantel wie auch dem Kern selbst konstant ist.

2.4.4 Längenbeschränkung und Grenzen/Dispersion

Die Datenübertragung über eine Glasfaser besitzt eine beschränkte Längenausdehnung, in der eine Datenübertragung möglich ist. Viele Effekte stören die Signalübermittlung. Zuallererst ist dies die Dämpfung im Lichtleiter. Die eingestrahlte Intensität an Licht fällt exponentiell zur Länge des Lichtleiters ab. Grund dafür ist die Absorption des Lichts und die Streuung. Die Faser ist nie völlig homogen. An kleinsten Unregelmäßigkeiten in Dichte und Brechungsindex kommt es zur Streuung. Die Lichtteilchen werden abgelenkt, fallen aus der Apertur und laufen damit nicht mehr den Leiter entlang. Diesen Effekt nennt man Rayleigh-Streuung.

Weiter ist die Glasfaser nicht völlig „durchsichtig“. Ein kleiner Teil des Lichtes wird von den Atomen absorbiert. Extrem störend sind OH-Gruppen, Bausteine des Wassers. Daher sind Lichtwellenleiter und Anschlussdosen stets mit einer Schutzkappe versehen, damit keine Luftfeuchtigkeit eindringen kann. Diese sind auch extrem wichtig, um das Eindringen von Staub zu vermeiden, der die Grenzflächen der Fasern zerkratzt und natürlich nicht „durchsichtig“ ist.

Das eingekoppelte Licht muss definierte Wellenlängen haben, die nicht in dem Bereich liegen, in dem die Materie des Leiters absorbiert. Es kann also nicht einfach mit irgendeiner Lichtquelle gearbeitet werden. Die Wellenlängenbereiche, in denen eine Übertragung möglich ist, nennt man optische Fenster. Im Alltag sehen wir das, wenn wir ultraviolettes Licht benutzen müssen. Hier muss Quarzglas eingesetzt werden, da normales Fensterglas für UV-Strahlung undurchsichtig ist.

Verluste entstehen auch durch eine starke Krümmung des Leiters, der gerade Weg der Reflexionen wird gestört. Es ist daher extrem wichtig, beim Verlegen auf die Biegeradien zu achten.

Der nächste Komplex an Verlust kommt durch eine Verfälschung des Signals zustande. Um diese zu verstehen, muss wieder ein kleiner Exkurs in die Physik herhalten.

Eine Lichtquelle emittiert in der Regel, wenn sie aufleuchtet, nicht nur einen Wellenzug, sondern viele. Aufgrund der Tatsache, dass Licht Wellencharakter hat, können nicht alle Lichtstrahlen aller eingestrahlten Winkel transportiert werden. (Für Interessierte: nur Wellenzüge einer fixen Phasenbeziehung. Sie interferieren konstruktiv, bei den anderen kommt es zur Auslöschung.)

Diese Eigenwellen, die transportiert werden, nennt man Moden. Je nach dem Kerndurchmesser und Brechungsindex können das Tausende bis einige Millionen sein. Da die Moden winkelabhängig sind, unterscheiden sie sich durch ihre Laufrichtung in Bezug zur optischen Achse des Mediums.

Dies hat Konsequenzen für die Datenübertragung.

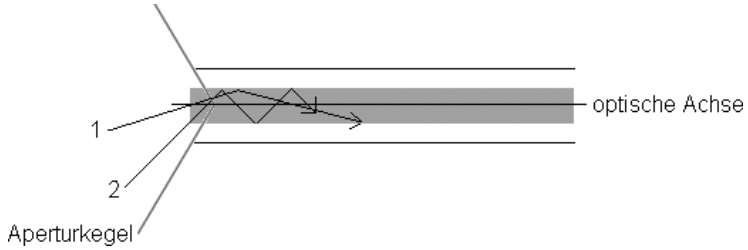


Bild 2.10 Schematisches Beispiel zweier lauffähiger Moden innerhalb eines Lichtwellenleiters: Sie bewegen sich beide im Leiter, sie sind innerhalb der Apertur eingekoppelt worden. Sie treten aber in unterschiedlichen Winkeln ein und werden in diesen reflektiert.

Je kleiner der Winkel zwischen der optischen Achse und dem Lichtstrahl ist, desto kürzer ist der Weg des Lichtes im Leiter. Die Ausbreitungsgeschwindigkeit aller Moden ist dieselbe, sie ist vom Brechungsindex des Leiters abhängig. Der Brechungsindex ist nichts anderes als der Quotient aus der Lichtgeschwindigkeit im Vakuum geteilt durch die Lichtgeschwindigkeit im untersuchten Medium. Da Licht im Vakuum in der Regel immer schneller ist als in irgendeinem anderen Medium, ist der Brechungsindex stets größer als eins.

Der Weg durch den Leiter aber ist für beide Moden sehr unterschiedlich, je nach dem Winkel zur optischen Achse.

Ein an der Grenze der Apertur eingekoppelter Lichtstrahl muss im Zickzack einen erheblich längeren Weg zurücklegen als ein fast zentral eingekoppelter, der nur einen sehr geringen Winkel zur optischen Achse hat. Daher kommen die Moden zu unterschiedlichen Zeiten am Empfänger an. Hier kommt es zu einer Beeinflussung des Gesamtsignals.

Dieser Effekt führt zu einer Signalverbreiterung. Ab einer gewissen Länge fließen die Signale ineinander und können nicht mehr korrekt aufgelöst werden. Hier ist die Längenbeschränkung erreicht.

Diese Art der Signalverfälschung bezeichnet man als die Modendispersion. Sie tritt immer in Erscheinung, wenn Lichtwellenzüge in verschiedenen Winkeln eingekoppelt werden. Diese Modendispersion ist einer der größten Störfaktoren bei der Glasfaserübertragung. Sie ist hauptsächlich für die Längenbeschränkungen der Datenübertragung über Glasfasern verantwortlich.

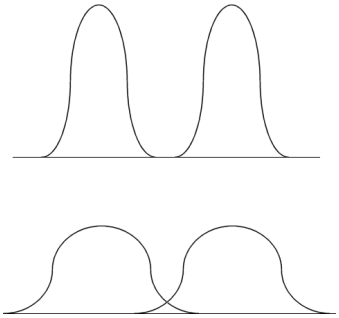


Bild 2.11 Zwei Signale am Anfang (oben) und am Ende (unten) des Lichtleiters. Durch die verschiedenen Wege der Moden werden die Signale „verwischt“, also verbreitert. Am Anfang noch klar getrennt, laufen sie nun im Laufe des Weges ineinander. Sind sie so weit überlappt, dass sie nicht mehr aufgelöst werden können, ist die Längenbeschränkung gegeben.

Da Lichtwellenleiter europäischer Norm mit einem Kerndurchmesser von 50 µm erheblich weniger Moden zulassen als die der amerikanischen Norm mit 62,5 µm, sind mit ersteren größere Längen zu überbrücken. Bei Gigabit-Übertragungen wird dies deutlich, bei Fasern mit 62,5 µm liegt die Längenbeschränkung bei 275 m, bei 50 µm bei 550 m.

2.4.5 Die Gradientenindexfaser

Die Längenbeschränkung durch die Modendispersion konnte erheblich durch neue Herstellungsverfahren verbessert werden. Die Stufenindexfaser ist schon für Gebäudeverbindungen an der Grenze. Um die Laufzeitunterschiede der Moden zu minimieren, wurde der Faserkern durch Dotieren (einbauen) von Fremdatomen verändert. Er besitzt nun nicht mehr einen konstanten Brechungsindex, sondern dieser wird von innen nach außen immer kleiner. Der Mantel hat nach wie vor einen konstanten Brechungsindex.

Eine Mode, die in die Außenbereiche des Kerns kommt, bewegt sich damit zunehmend durch ein Medium mit geringerem Brechungsindex. Die Ausbreitungsgeschwindigkeit einer Mode ist von diesem Brechungsindex abhängig. Moden im Zentrum des Kernes bewegen sich also langsamer als Moden im Außenbereich. Dadurch wird die oben beschriebene Dispersion korrigiert, sprich die Laufzeitunterschiede werden nivelliert und die Signalverbreiterung erheblich zurückgedrängt.

Die Wellenzüge, die mit einem Winkel eingekoppelt werden, der bedingt, dass sie sich mehr im Zickzack durch den Kern bewegen, halten sich häufiger im Außenbereich des Kerns auf (sie bewegen sich schraubenförmig durch den Leiter), dort bewegen sie sich schneller. Wellenzüge, die fast nur im Zentrum des Kerns laufen, haben einen kürzeren Weg, bewegen sich aber langsamer. Glasfasern mit einem Kerndurchmesser 50 µm oder 62,5 µm nennt man aufgrund dieser Vorgänge auch Multimode-Fasern, da in jedem Signal unzählige Moden zum Transport der Daten eingesetzt werden.

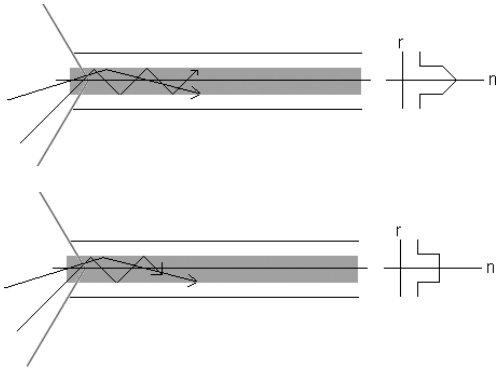


Bild 2.12 Bei der Gradientenindexfaser (oben) nimmt der Brechungsindex n des Kerns nach außen kontinuierlich ab. Der Mantel hat einen festen Brechungsindex. Bei der Stufenindexfaser haben Mantel und Kern feste Brechungsindices. In einem Medium mit geringerem Brechungsindex bewegt sich das Licht schneller vorwärts. Moden, die sich daher öfter im Außenbereich des Kerns aufhalten, laufen schneller als solche, die flacher zur optischen Achse verlaufen. Die Geschwindigkeitsunterschiede werden dadurch verringert und die Signalverbreiterung zurückgedrängt. Somit können wesentlich größere Entfernungen realisiert werden, bevor die Signale unbrauchbar werden.

2.4.6 Qualitäten und Längenbeschränkung

Die Qualitäten der Fasern zeigen sich stark in der Längenbeschränkung. Nach diesen Qualitäten werden sie in drei Klassen eingeteilt, dem OM-Standard. Er wird durch spezielle Messungen ermittelt, und die Fasern werden dadurch klassifiziert. Dies ist eminent wichtig bei der Neuplanung oder einer Migrationsplanung der Verkabelung. Mögliche Längenbeschränkungen sollen am Beispiel des Übergangs von 1 Gbit/s auf 10 Gbit/s aufgezeigt werden. Bei einer Übertragung mit 1 Gbit/s schaffen Fasern nach OM 2,50 µm eine Distanz von 550 m, bei einer Qualität von OM3 aber 900 m. Bei 10 Gbit/s sind es bei OM2 ca. 80 m, bei OM3 300 m. Mit den alten OM1-Kabeln ist leider nichts mehr zu gewinnen. Bereits nach ca. 30 m ist es vorbei mit 10 Gbit.

Der Kostenunterschied zwischen OM2- und OM3-Fasern ist nicht mehr groß. OM2 wird immer noch standardmäßig angeboten. Hier sollte man zur Zukunftssicherheit bei Neuverkabelungen den Standard OM3 vorziehen.

Wer noch OM2-Kabel hat (sie sind noch breit im Einsatz), kann sich behelfen, selbst wenn er etwas über die Grenzen kommt. Einige Hersteller bieten spezielle Patchkabel an, die die Dispersion durch eine spezielle Fertigung stark korrigieren. Diese Kabel nennt man „Mode-Conditioning-Kabel“. Sie sind zwar teuer, aber auf jeden Fall günstiger als eine Neuverkabelung.

2.4.7 Die Mono- oder Singlemode-Faser

Noch besser lässt sich die Modendispersion unterdrücken, wenn sie nicht mehr auftritt. Welche und wie viele Moden erlaubt sind, hängt von der Wellenlänge, dem Brechungsindex und dem Kerndurchmesser der Glasfaser ab. Wird der Durchmesser unter 10 µm gewählt, ist nur noch eine einzige Mode erlaubt. Die Modendispersion tritt nicht mehr auf. Daher nennt man Glasfasern dieses Typus Mono- oder Singlemode-Fasern. Sie können weitaus größere Strecken überbrücken, sind aber auch erheblich teurer und schwerer zu verlegen.

Daher haben Fasern mit 50 µm oder 62,5 µm durchaus ihre Berechtigung – es muss nicht immer Kaviar sein.

Im Bereich der vertikalen Gebäudeverbindungen, „Glasfaser bis zum Arbeitsplatz“ und Strecken innerhalb der Längenrestriktionen ist die Multimode-Faser absolut tauglich und breit im Einsatz. Auch sind hier die Interfaces wesentlich günstiger.

Die Modendispersion ist der größte Störfaktor. Es gibt noch andere Arten der Dispersion, die vor allem im Weitbereich relevant werden (Polarisationsdispersion, chromatische Dispersion, etc.). Ebenso gibt es noch weitere Mechanismen, die das Signal im Kabel dämpfen. Hierzu sei jedoch auf weiterführende Literatur verwiesen, sie sind meist nur mit gutem physikalischen Hintergrund zu verstehen.

2.4.8 Verlegung und Handhabung

Glasfasern werden in der Regel fest verlegt. An Koppelstellen werden sie gespleißt, das heißt, fest verschweißt. Dies ist nur mit speziellen Geräten möglich. An den Anschlussstellen werden Anschlussdosen gesetzt, an die mit Glasfaserkabeln angekoppelt werden kann.

Auch bei der Glasfaser gilt, dass Verbindungen von Gerät zu Gerät anders sind als Verbindungen von Gerät zu Endgerät. Auch hier muss die Sendeleitung des Gerätes auf die Empfangsleitung des Endgerätes gesteckt werden. Glasfaserverbindungen haben in der Regel zwei Fasern, Senden und Empfangen. Werden zwei Endgeräte oder zwei Netzwerkgeräte miteinander verbunden, müssen die Fasern gekreuzt werden.

Die Güte der Steckverbindung bestimmt, wie viel Dämpfung durch eine solche auftritt. In der Regel gilt wie bei der Kupferverkabelung, dass so wenig als möglich lösbare Verbindungen im Einsatz sein sollten. Im Gegensatz zu gespleißten Verbindungen, die heute fast keine Dämpfungen mehr verursachen, sind Steckverbindungen immer mit einer Dämpfung des Signals und Reflexionen behaftet. Dies wird klar, wenn man zum Fenster hinaussieht: Ein schwaches Spiegelbild ist zu sehen. An einer glatten Glasfläche werden ca. 5 – 8 % des auftreffenden Lichtes direkt reflektiert. Dieses geht für das Signal verloren. Darüber hinaus kommt es zu Störungen, da dieses Licht im Leiter zurückläuft.

Die besten Steckertypen sind deshalb heute schräg (8°) angeschliffen. Dadurch wird das reflektierte Licht in den Mantel gestreut und stört die Vorgänge im Kern nicht mehr. Weiter wird heute dafür gesorgt, dass mit einem leichten Federdruck beide Faserenden in der Verbindung aufeinandergepresst werden. Besteht kein Luftspalt in der Steckverbindung, tritt weit weniger Streuung an Luft auf. Inzwischen gibt es sehr viele Typen von Steckverbindungen. Für sie sei auf weiterführende Literatur verwiesen. Die gängigsten sind am Ende des Buches abgebildet. Jeder Steckertyp hat seine Vor- und Nachteile, verschiedene Dämpfungen und Güteklassen. Je nach dem Einsatz, dem Fasertyp, der Länge und der Geschwindigkeit muss abgewägt werden, welche Typen eingesetzt werden müssen. Hier müssen erhebliche Kostenunterschiede mit den Anforderungen abgewägt werden. Durchgesetzt hat sich bei fast allen Steckertypen eine zylindrische Führung. Bei Schrägschliff muss der Stecker zwangsgeführt werden, um ein Verdrehen zu vermeiden. Die Faserkerne werden in eine zylindrische Hülle eingeklebt, die Ferrule. Diese wird nun in eine Führung aus Keramik eingeschoben.

Bild 2.13 Schematischer Aufbau einer Steckverbindung von Glasfasern: Die Ferrulen mit den beiden Faserkernen werden in einem Führungsrohr zentriert. Kleine Federn sorgen dafür, dass die Stirnflächen aneinandergepresst werden.

Viele Steckertypen wurden entwickelt und sind im Einsatz. Das Problem bei allen Steckverbindungen ist die Dämpfung des Signals an der Kontaktfläche durch Reflexion und Streuung (mehr dazu siehe Kapitel 12, „Steckertypen“). Generell unterschieden werden die Stecker nach zwei Kriterien. Einmal werden die Faserenden durch Federn oder den Aufbau der Stecker fest aufeinandergepresst (Physical Contact), oder es verbleibt ein winziger Luftspalt. Erstere sind natürlich von der Qualität her wesentlich besser.

2.4.9 Laser sind gefährlich

Nicht alle Laser, die zur Übertragung eingesetzt werden, sind im sichtbaren Bereich des Lichtes. Gerade Fernverbindungen werden mit Lasern bedient, die außerhalb des für uns sichtbaren Spektrums sind. Daher sind sie aber nicht weniger gefährlich. In eine Faser oder einen Anschluss sollte man daher nie hineinschauen. Ernste Beschädigungen der Augen können die Folge sein. Die Leistungen sind zwar gering, im Bereich von Milliwatt, aber die Bündelung auf 50 µm oder sogar 9 µm ergibt umgerechnet auf einen Quadratmeter immense Werte. Neueste Weitverkehrssysteme, die mit vielen Lasern gleichzeitig arbeiten, sind so leistungsfähig, dass Verbrennungen der Haut auftreten, wenn man sich dem Lichtstrahl exponiert. Die Laser sind so stark, dass der Lichtstrahl die Kabelhülle zerstört und austritt, wenn der Biegeradius unterschritten wird.

2.4.10 High-Speed-Verfahren

Mit den neuesten Technologien lassen sich ungeheure Übertragungsraten erzielen. Da diese Verfahren immer mehr eingesetzt werden, sollen sie kurz erläutert werden.

Arbeitet man nicht mit einem Laser, wie üblich, sondern gleichzeitig mit mehreren Lasern verschiedener Frequenzen, lassen sich vielfache Datenströme simultan über eine Faser übertragen. Am Empfänger müssen diese einzelnen „Farben“ wieder durch Filter oder wellenlängenempfindliche Detektoren getrennt werden. Dieses Verfahren nennt man WDM, Wavelength Division Multiplexing.

Zwei Varianten dieses Verfahrens sind im Weitverkehrsbereich im Einsatz, das CWDM, Coarse Wavelength Division Multiplexing, benutzt Laser, die Wellenlängen benutzen, die einen Wellenlängenabstand von ca. 20 Nanometern haben. Hier lassen sich Datenraten von ca. 2,5 Gigabit (pro „Farbe“/Laser) erzielen. Mit diesen Interfaces lassen sich Strecken von bis zu 60 – 70 Kilometern ohne Verstärker erreichen.

Eine viel teurere Variante, die sehr viel teurere und in der Handhabung kompliziertere Laser verwendet, ist das DWDM, das Dense Wavelength Division Multiplexing. Hier beträgt der Abstand der Wellenlängen nur ca. einen Nanometer. Dafür lassen sich heute mit dieser Technologie Daten mit ca. 40 Gbit/s übertragen. Es sind Strecken von bis zu 1000 Kilometern möglich.

Mit den neuesten Geräten ist es möglich, Verstärker zu bauen, die das Signal direkt optisch verstärken. Es muss nicht erst decodiert und auf Kupferleitungen umgesetzt werden. Diese Verfahren sind aber noch derart teuer, dass sie nur in Weitverkehrsverbindungen eingesetzt werden.

■ 2.5 Die Gesamtverkabelung

Auf Layer I sind noch etliche andere Medien im Einsatz, alle aufzuführen wäre zu umfangreich. Bislang haben wir Verkabelungen im LAN-Bereich (Local Area Network, meist begrenzt auf Gebäude) betrachtet. Im Bereich MAN (Metropolitan Area Network, ein Mittelding zwischen lokal und weit, zum Beispiel Verbindung von Gebäuden über Straßen hinweg etc.) und WAN (Wide Area Network, bis weltweit) sind andere Übertragungsmechanismen im Einsatz, von Satellitenübertragung bis Seefunk, Richtfunk und Richtlaser. Die Glasfaser in den verschiedensten Typen und Ausführungen ist in allen drei Bereichen im Einsatz.

2.5.1 Gebäude/Büro

Wie oben betrachtet, wird heute eine sternförmige Verkabelung eingesetzt, das heißt, alle Anschlussdosen an den Arbeitsplätzen werden von Kabeln erschlossen, die an einer zentralen Stelle zusammengeführt werden, zum Beispiel Stockwerk für Stockwerk. Dies gilt für die UGV genauso wie für Umgebungen mit Glasfaser bis hin zum Arbeitsplatz. Dies kann ein Stockwerks- oder bei kleineren Umgebungen auch ein Gebäudeverteiler sein. Dort ist ein Switch eingebaut, der den Kontakt entweder zum Haus/-Firmennetzwerk oder zu einer WAN-Verbindung herstellt.

Soll nun ein Netzwerkgerät (Drucker, PC etc.) ans Netzwerk angeschlossen werden, muss mithilfe zweier kurzer Verbindungskabel, sogenannter Patch-Kabel, eine Verbindung zwischen der Netzwerkkarte und der Anschlussdose und zwischen dem Switch und dem Kabelende im Verteilerraum gesteckt werden.

Bei der Installation des Netzwerkes ist es üblich, dass alle Kabel von allen Anschlussdosen her in einen Netzwerkschrank (Rack) geführt und dort fest mit Anschlussdosen versehen werden. Eine deutliche Beschriftung ist eine Selbstverständlichkeit, da in einem Gebäudeverteiler Hunderte von Anschlüssen enden können!

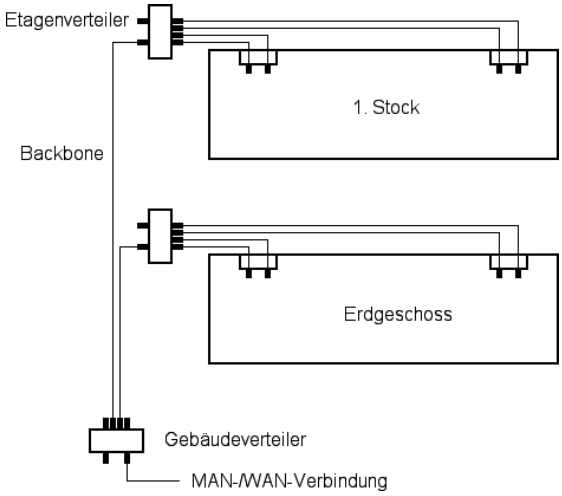


Bild 2.14 Der heute übliche Aufbau einer Gebäudeverkabelung: Zentral im Gebäude ist ein Gebäudeverteiler installiert, von dem aus die Unterverteiler (zum Beispiel Etagenverteiler) erschlossen sind. Diese erschließen die einzelnen Wanddosen in einem Rangierpanel. In der Regel sind heute die vertikalen Verbindungen Glasfasern, die horizontalen UGV.

Ein solches Array von Anschlussdosen in einem Rack (Kommunikationsschrank) nennt man ein Rangierpanel. Es ist die Aufgabe des Netzwerkbetreuers, hier die nötigen Verbindungen vorzunehmen, zu dokumentieren und unbenutzte Anschlüsse wieder zurückzunehmen. Hierbei muss größte Sorgfalt angewendet werden. Eine UGV versorgt auch andere Dienste über dieselbe Verkabelung! Wer versehentlich einen ISDN-Anschluss (mit ca. 100 Volt Spannung!) auf ein Netzwerkgerät steckt, kann einen enormen Schaden verursachen! (Normalerweise wird dies durch verschiedene Pinbelegungen der Dienste verhindert. Aber wie oben ausgeführt, lassen sich über ein Kabel mit speziellen Anschlussdosen zwei Verbindungen über ein Kabel realisieren. Hier sind alle Pins belegt.)

Die Netzwerkleitungen, welche die Verbindung zwischen den Stockwerken und den Netzwerkgeräten vornehmen und an die normalerweise keine Endgeräte angeschlossen werden, nennt man das Backbone (Rückgrat) eines Netzwerkes. Meist wird es mit Glasfasern realisiert, schon aufgrund der Längenrestriktionen. Hier wird in der Regel Gigabit-Ethernet eingesetzt. Da in letzter Zeit die Preise gefallen sind, wird bei Neuausrüstungen und Ersatz der Backbone-Geräte immer mehr 10 Gbit/s oder mehr eingesetzt. Der Backbone sollte natürlich die höchste Performance haben.

2.5.2 Geschwindigkeit

Gigabit Ethernet hat sich gegenüber UGV durchgesetzt (die meisten PCs und Server haben bereits Gigabit-Ethernet-Karten onboard), daher muss auf die Qualität der Verkabelung geachtet werden. Insbesondere bei älteren Verkabelungen oder niedrigerer Qualität kann es hier zu hohen Fehlerraten kommen. Das Beste ist, eine bestehende Verkabelung vermessen zu lassen, dies erledigt jeder zertifizierte Elektriker.

In der Regel sollte man heute Switches einsetzen, die mindestens Gigabit-Uplinks zum Anschluss an den Backbone haben. Für Endkunden, die große Datentransferraten haben, lohnt es sich, überall Gigabit-Ports zu verwenden: Selbst wenn es nicht mit Gigabit geht, so

doch mit besserer Performance als mit 100 Mbit. Für „normale Büroarbeitsplätze“, Drucker, Scanner, etc. aber können die weitaus günstigeren Switches mit Gigabit-Uplink und Fast-Ethernet-Ports eingesetzt werden oder bestehende, noch funktionierende Geräte mit Fast Ethernet weiter genutzt werden.

Vorsicht ist auch geboten, wenn Geräte der billigen Preisklasse angeboten werden. Was für ein Datendurchsatz ein Switch bietet, hängt nicht nur von der Fähigkeit seiner Ports ab. Ein 48-Port Gigabit-Switch, der zu kleine Pufferspeicher hat und ein Backplane von 10 Gbit/s, ist völlig überbucht. Sind hier genug Geräte angeschlossen, ist ihre Performance geringer als bei einem Fast-Ethernet-Gerät, das aber kapazitativ ausreichend ausgerüstet ist.

Zum Backbone sollte aus Sicherheitsgründen niemand als der Administrator Zugang haben. Genauso sollten die Anschlüsse nur von eingewiesenem Personal verwaltet werden. Wie wir unten sehen werden, kann eine einzige falsche Verbindung im Netzwerk enormen Schaden anrichten.

Die Länge der Patchkabel sollte so kurz als möglich gewählt werden. Manchmal müssen aber, zum Beispiel in großen Büros oder bei einer ungünstigen Lage der Anschlussdosen in den Räumen, längere eingesetzt werden. Hier muss auf die Längenrestriktionen geachtet werden. Selbstverständlich müssen die Patchkabel hier mit eingerechnet werden. Ein guter Planer bezieht genug Reserve für die Patchkabel bei der Konzeption einer Gesamtverkabelung ein.

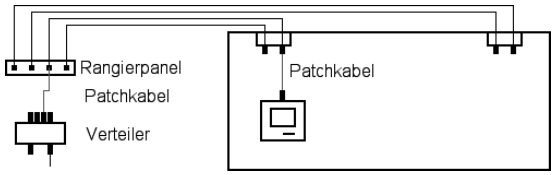


Bild 2.15 Alle Anschlussdosen werden fest verkabelt und in einem Rangierpanel zusammengeführt. Wird nun eine Dose in einem Raum in Betrieb genommen, verbindet der Netzwerker die Wanddose und die Netzwerkkarte des Rechners mit einem kurzen Kabel. Ebenso stellt er mit einem solchen die Verbindung zwischen dem Verteiler und dem Rangierpanel her. Das Endgerät ist nun mit dem Netzwerk verbunden. Diese kleinen Kabel, die diese Verbindungen herstellen, nennt man Patchkabel.

Eines muss dabei bedacht werden: Kabel, die zur festen Verlegung hergestellt sind, sind meist besser abgeschirmt als Patchkabel. Dies hat den Grund, dass man die Patchkabel büroseitig gerne flexibler und nicht so steif haben möchte. Patchkabel haben daher eine höhere Dämpfung. Die möglichen 100 m Distanz bei 100 Mbit/s lassen sich daher mit einem Patchkabel nicht erreichen.

2.5.3 Miniswitches

Oft sind nicht genug Anschlussdosen in einem Raum vorhanden. Einerseits wächst die Zahl der Endgeräte (PCs, Drucker etc.) ständig, und die Verkabelungen sind oft schon älter, andererseits ist es auch sinnlos, bei Neuverkabelungen einfach Unmengen von Dosen zu planen.

Sind in einem Raum nicht genug Anschlussdosen vorhanden, können einzelne Dosen mit Miniswitches (Büroswitch) vervielfacht werden. Dabei muss peinlich darauf geachtet werden, dass keine Loops entstehen (siehe Layer II).

2.5.4 Fiber-to-the-Desk

Vor einigen Jahren war die standardmäßige Qualität der liegenden Verkabelung noch nicht so hoch, wie es heute möglich ist. Ebenso waren die Switches und Interfaces für Glasfaser nicht bereit oder sehr teuer. Daher sah man die Glasfaser als die Zukunft an. Zur Zukunftssicherung gab es den Trend, auch die Arbeitsplätze mit Glasfaser zu erschließen, damals in der Regel mit 100 Mbit/s. Dieser Trend hat sich nicht durchgesetzt. Heute ist als Hauptvorteil der Glasfaser in diesem Bereich nur noch die enorm höhere Längenkapazität geblieben. Die Gesamtverkabelung ist nun in der Lage, auch ohne Glasfaser Gigabit zu bieten. Die Kosten für die Anschlüsse per Glasfaser sind erheblich teurer. Ebenfalls muss für jedes Gerät eine Netzwerkkarte angeschafft und eingebaut werden. Für Geräte wie Drucker, Faxe, etc. muss mit Mediumkonvertern gearbeitet werden, hier lassen sich in der Regel gar keine anderen Netzwerkkarten einbauen. Netzwerkkarten mit Glasfaseranschluss setzen sich hauptsächlich im Server-Bereich durch, weshalb bei einer Neuerschließung von Glasfaser in Büroräumen abzuraten ist. Sollten die Längen in einem Gebäude zu groß sein, kann mit Switches gearbeitet werden, die einen Glasfaser-Uplink haben. Im Büro/Raum sollte dann mit Kupferpatchkabeln gearbeitet werden.

■ 2.6 Kabeltypen/Dateneinspeisung/Entnahme

2.6.1 Kabeltypen

Bevor wir das Thema Layer I beenden können, müssen wir noch die Spezifikationen der Kabeltypen und die Fachterminologie betrachten. Die Bezeichnungen der Kabel verraten dem Fachmann sofort, um was für eine Ausführung es sich handelt, sie sind eindeutig bezeichnet. Um diese Bezeichnungen zu verstehen, müssen wir wieder einen kleinen Exkurs in die Physik wagen.

Über ein Medium lassen sich die Daten in Form elektrischer Signale in verschiedenen Mechanismen und Codierungen übertragen. Der Computer kennt intern nur zwei Zustände, ja und nein. Deshalb erfolgt der Austausch von Daten in der Regel binär, Zustand null oder eins, Signal oder nicht.

Die Daten werden also codiert und als Folge von Nullen und Einsen, Signal oder nicht, auf die Zeit bezogen, ins Medium eingespeist.

Hierfür gibt es zwei Methoden:

Eine definierte Frequenz wird benutzt. Sollen mehrere Dienste gleichzeitig Daten über das Medium senden, müssen diese zeitlich gemultiplext werden.

Wird einem Dienst dabei eine gewisse Anzahl von Takten pro Sekunde fest zur Verfügung gestellt, kann er mit einer virtuellen Teilfrequenz pro Sekunde kommunizieren. Man sagt, er bekommt „Bandbreite“ zugewiesen. Die Gesamtbandbreite teilen sich alle Dienste. Je mehr Dienste also gleichzeitig senden, desto weniger Übertragungskapazität stehen dem Einzelnen zur Verfügung.

Ein zeitliches Multiplexing erfordert eine definierte Taktrate und eine Synchronisation zwischen Sender und Empfänger. Am Empfänger müssen die Daten wieder demultiplext, sprich zerlegt, und sinnvoll wieder zusammengefügt werden.

Bild 2.16 Zwei Dienste senden gleichzeitig Informationen über ein Medium. Sie müssen dies abwechselnd tun (hier schematisch, schwarze und graue Segmente, die über ein Medium gesendet werden). Am Empfänger wird das Signal wieder aufgelöst und verteilt. Beide Dienste sehen davon nichts, sie haben aber nur die halbe Bandbreite zur Verfügung.

Die andere Methode ist, dass mehrere Frequenzen gleichzeitig eingesetzt werden. Diese sind in klar trennbaren Abständen angeordnet. Der Empfänger setzt nun einen Filter, sodass er nur die gewünschte Frequenz empfängt und decodiert. Somit lassen sich über ein Medium mehrere Datenströme übertragen. Im Bereich des Fernsehens ist diese Technologie im Einsatz. Hier werden die Programmkanäle auf verschiedene Frequenzen aufmoduliert und können so gleichzeitig über ein Medium verschickt werden.

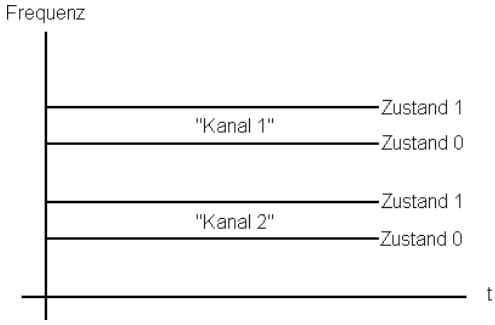


Bild 2.17 Mehrere Frequenzen werden gleichzeitig eingesetzt. So entstehen im Verlauf der Zeit die Frequenzbänder oder „Kanäle“.

So entstehen im Verlauf der Zeit sogenannte Frequenzbänder. Die erste Art dieser Signalisation nennt man die Basisbandübertragung, die zweite die Breitbandübertragung. Im Bereich Netzwerke ist die Basisbandübertragung heute der Standard. Im Bereich Rundfunk und Fernsehen via Kabelanschluss dominiert die Breitbandübertragung mit verschiedenen Frequenzbändern für die „Programmkanäle“ (über Koaxialkabel mit einem Wellenwiderstand von 75 Ohm). Für die Vernetzung von Computern wird die Breitbandübertragung für Internetanschlüsse über die Breitbandkabel der Fernsehanbieter verwendet. Beide Techniken haben Vor- und Nachteile. Diese zu diskutieren würde jedoch den Rahmen des Buches überschreiten.

Jetzt aber haben wir (endlich!) alles, um die verschiedenen Fachbezeichnungen der Kabeltypen verstehen zu können. Die Bezeichnungen sind klar strukturiert aufgebaut. Die erste

Zahl gibt die Übertragungsrate in Mbit/s an, gefolgt vom Typ der Übertragung. Anschließend kommt eine Information zur maximalen Ausdehnung des Mediums oder zu dem Typ. Diese Bezeichnungen sind sehr wichtig, da zur liegenden Verkabelung die richtigen Patchkabel gewählt werden müssen. Wer eine Verkabelung nach STP hat, aber UTP-Patchkabel einsetzt, beeinträchtigt die Vorteile und Qualität der hochwertigeren installierten Verkabelung.

In der Regel wird heute in der Gebäudeverkabelung die Basisbandübertragung eingesetzt, auf die wir uns hier beschränken. Früher waren beide parallel im Einsatz. In der Regel ist der Endkunde auch beim Breitbandkabel-Internetanschluss nicht davon betroffen. Das Signal wird in der Regel sofort direkt am Fernsehanschluss abgekoppelt, decodiert und über ein spezielles Anschlussgerät, das Kabelmodem, als „normaler“ Ethernet-Anschluss zur Verfügung gestellt. Hier sind wir wieder bei der Basisbandübertragung. Die OnBoard-Anschlüsse der heute gekauften Geräte können so direkt angeschlossen werden.

Die Bezeichnungen der Verkabelungstypen sind wie folgt aufgebaut:

- Die Zahl am Anfang gibt die Nenndatenrate an, z. B. 10, 100, 10 G. Der Zusatz G steht für Gbit/s. Wird kein Buchstabe angegeben, ist die Einheit Mbit/s.
- Es folgt die Art der Übertragung. Base- steht für Basisband, Broad- für Breitbandübertragung. In der Gebäudeverkabelung findet man in der Regel Base-.
- Als Nächstes wird das Medium angegeben. Hier steht z. B. T für Twisted Pair, S für kurze Wellenlängen mit Multimode-Glasfaser, L oder E/Z für lange bzw. sehr lange Wellenlängen in der Regel mit Singlemode-Glasfaser. Historisch stehen 2 und 5 für Koaxialkabel mit 180 m bzw. 500 m Reichweite.
- Optional folgt noch die verwendete Kodierung, z. B. X, R. Auf diese wird hier nicht näher eingegangen.
- Ebenfalls optional steht am Ende die Anzahl der Leitungen pro Verbindung, z. B. 2, 4, 10.

Hier einige Beispiele für gängige Verkabelungstypen:

10Base-5	10 Mbit/s, 500 m (Yellow Cable)
10Base-2	10 Mbit/s, 180 m (Thin-Wire)
10Base-T	10 Mbit/s, Twisted Pair
10Base-FL	10 Mbit/s, Glasfaser, Single- oder Multimode
100Base-TX	100 Mbit/s, Twisted Pair
100Base-FX	100 Mbit/s, Glaserfaser, Single- oder Multimode
1000Base-TX	1000 Mbit/s Twisted Pair
1000Base-LX	1000 Mbit/s, Glaserfaser, Single- oder Multimode
1000Base-SX	1000 Mbit/s, Glaserfaser, Multimode
10GBase-T	10 Gbit/s, Twisted Pair
10GBase-SR	10 Gbit/s, Glaserfaser, Multimode
10GBase-LR	10 Gbit/s, Glaserfaser, Singlemode

Wie immer, gibt es bei den Glasfasern noch viel mehr Implementationen, vor allem um auf die vielfältigen Arten der bestehenden Verkabelungen eingehen zu können. Bei Einsatz oder Migration zu 10 Gbit/s sollten der Hersteller der Geräte ebenso gefragt werde wie Spezialisten in der Verkabelung.

Auf Layer I des Netzwerkes gibt es noch viele andere Übertragungsverfahren, von Richtfunk, Wireless-Funknetzen, freiem Richtlaser bis hin zur Satellitenübertragung. Diese alle zu beschreiben würde den Rahmen des Buches sprengen. Am Ende des Buches wird jedoch noch auf Wireless LAN eingegangen. Als flexible Erweiterung des kabelgebundenen Netzzugangs nicht nur in Privathaushalten, sondern auch in Bürogebäuden sowie öffentlichen Gebäuden und Plätzen setzt sich diese Technik immer mehr durch. Für das Verständnis eines Netzwerkes und die Konfiguration ist es aber unerheblich, ob ein Rechner mit einem Patchkabel oder per Funk angeschlossen ist, daher wird dies nicht hier, sondern in einem gesonderten Kapitel besprochen.

2.6.2 Kabelkategorien

Innerhalb der UGV wird die Qualität der Kabel in Abschirmung und Fertigung in verschiedenen Kabelkategorien beschrieben. Diese Kategorien bestimmen, mit welchen Geschwindigkeiten und Längen gearbeitet werden kann.

- **Kategorie 1:** Billige Telefonverkabelung (sogenannter Klingeldraht). Die Adern sind parallel. Die Kabel eignen sich maximal für analoges Telefon und sollten nicht mehr eingesetzt werden.
- **Kategorie 2:** Etwas bessere Qualität als Kategorie 1. Tauglich für Telefon, ISDN.
- **Kategorie 3:** Tauglich für Telefon, ISDN und 10 Mbit/s Ethernet (10Base-TX).

  Kategorie 3 war lange Zeit die Standardverkabelung für UGV. Sie wurde dann aber rasch von Kategorie 5 verdrängt, die höhere Geschwindigkeiten zulässt.
- **Kategorie 4:** Bessere Abschirmung und Fertigung. Geeignet für Telefon, ISDN und 10 Mbit/s Ethernet (10Base-TX) sowie Token Ring.
- **Kategorie 5/5e:** Diese Kategorie ist für Frequenzen bis 100 MHz geprüft. Geeignet für Fast Ethernet (100Base-TX). Eingeschränkt tauglich, je nach Qualität und Verlegung für Gigabit Ethernet (1000Base-TX) und sehr eingeschränkt für 10G Ethernet (10GBase-T).
- **Kategorie 6:** Gut geschirmte Kabel. Geprüft bis 250 MHz. Sie sind für 1000Base-TX zertifiziert, ebenso für 10GBase-T.
- **Kategorien 7 und 7 A:** Hochgeschirmte Kabel, im Minimum S/STP. Zertifiziert bis 600 MHz bzw. 1000 MHz. Sie sind für 1000Base-TX zertifiziert, ebenso für 10GBase-T.
- **Kategorien 8, 8.1 und 8.2:** Hochgeschirmte Kabel. Die unterschiedlichen Typen beziehen sich auf Aufbau und Komponenten. Es wird eine Eignung für Bandbreiten von bis zu 2000 MHz erwartet. Anwendungen sind beispielsweise 25GBase-T und 40GBase-T.

Die Kategorien sind immer abwärtskompatibel, auf Kategorie 7 lässt sich natürlich auch Telefon, ISDN oder Fast Ethernet übertragen.

Die unteren Kategorien gibt es je nach Hersteller und Fertigungstechniken in vielen Ausführungen (UTP/STP/S-UTP etc.). Entscheidend für die Kategorie sind die Leistungsdaten und Spezifikationen.

2.7 Transceiver

Jedes Endgerät muss mithilfe eines Netzwerkadapters (Netzwerkkarte) angeschlossen werden. Je nach dem Zugriffsverfahren (siehe unten) und dem Typ des Mediums muss dieser den geeigneten Anschluss bieten (BNC, RJ-45, Glasfaser etc.). Der direkte Zugriff auf das Medium selbst wird durch ein spezielles Gerät vorgenommen, das sich Transceiver (TRANSmitter/reCEIVER, Sender und Empfänger) nennt. In den meisten Netzwerkadaptern ist es fest eingebaut und tritt nach außen nicht sofort ersichtlich in Erscheinung. Der Transceiver wandelt die Daten, die das Netzwerkgerät oder Endgerät versenden oder empfangen will, in eine Form um, die der Implementierung des Layers I seines Netzwerkes entspricht, ist also für die korrekte Signalisation zuständig.

Dasselbe gilt analog für die Entnahme von Daten aus dem Netzwerk. Jedes Netzwerkgerät muss über dieses Gerät angeschlossen werden. Auch die Ports eines Switches beinhalten Transceiver. Ein Mediumkonverter, der zum Beispiel Segmente mit ThinWire und UGV verbindet, ist also im Prinzip nichts anderes als ein Gerät mit zwei Transceivern und einem Minibus, der beide verbindet.

Die Netzwerkadapter sind in den verschiedensten Typen erhältlich, die es ermöglichen, an jeden beliebigen Typ Medium (Layer I) anzuschließen. Oftmals sind auch Typen erhältlich, die mehrere verschiedene Anschlüsse anbieten (sogenannte Combo-Adapter), also intern mehrere Transceiver eingebaut haben. Ebenso gibt es auch Netzwerkadapter mit Anschlüssen für externe Transceiver. Mit solchen Karten und einem geeigneten Transceiver kann an fast jeden beliebigen Typ ein Medium auf Layer I angekoppelt werden.

- Im Bereich 10-Mbit/s-Netze nennt man diese „nativen“ Anschlüsse für Transceiver AUI-Ports (Attachment Units Interface).
- Im Bereich 100 Mbit/s und 1000 Mbit/s nennen sie sich MII und GMII (Media Independent Interface/Gigabit Media Independent Interface).
- Bei 10Gbit/s nennen sie sich 10G-MII (10 Gigabit-Media Independent Interface) oder XGMII.

Zur Unterscheidung nennt man „normale“ Anschlüsse, wie man sie zum Beispiel an Switches oder Netzwerkadaptern findet, die also interne Transceiver besitzen und nur den endgültigen Anschluss nach außen führen, MDI (Media Dependent Interface) oder MDI-X (Uplink-Port, Media Dependent Interface-Crossover).

Heute ist es nicht mehr üblich, mit nativen Schnittstellen und externen Transceivern zu arbeiten, außer bei Netzwerkkomponenten. Früher waren die Netzwerkkarten und Transceiver wesentlich teurer. Heute werden die meisten Endgeräte mit bereits fest eingebauten Netzwerkanschlüssen geliefert (Ethernet-on-Board).

In der Regel rüstet man ein Endgerät mit Netzwerkadaptern aus, die bereits den richtigen Transceiver fest eingebaut haben und nach außen nur das MDI ausführen (in den meisten Fällen RJ-45).

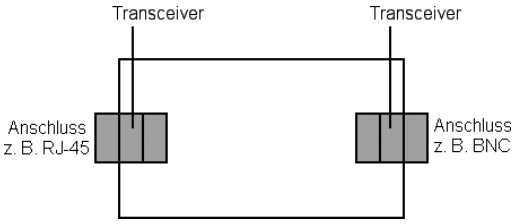


Bild 2.18 Ein Mediumkonverter ist im Prinzip nichts anderes als ein Minibus mit zwei fest eingebauten Transceivern, die Signalisation wird geändert.

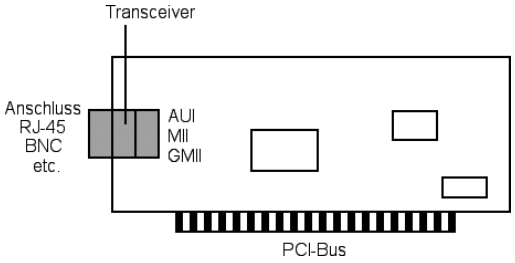


Bild 2.19 Der schematische Aufbau einer Netzwerkkarte: Einerseits kommuniziert sie mit dem Mainboard (PCI-Bus), andererseits führt sie Anschlüsse für den Kontakt zum Netzwerk aus. Hier die übliche Variante. Das AUI/MII/GMII ist bereits auf der Karte fest mit einem Transceiver versehen. Nur der Anschluss wird ausgeführt.

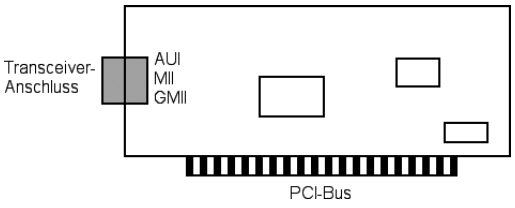


Bild 2.20 Eine Netzwerkkarte ohne integrierten Transceiver: Hier wird das AUI/MII/GMII nach außen ausgeführt. Zum Anschluss an das Netzwerk muss ein externer Transceiver verwendet werden. Der Vorteil ist in Mischumgebungen, dass mit dem dementsprechenden Transceiver an verschiedene Layer I-Typen angeschlossen werden kann.

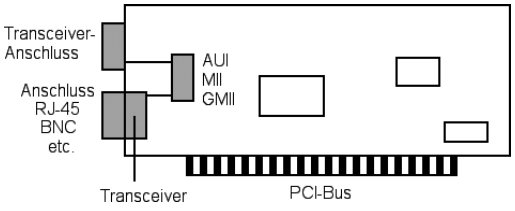


Bild 2.21 Ein Combo-Adapter: Er führt über einen Transceiver fest einen Anschluss aus; andererseits aber auch das AUI/MII/GMII. Der Vorteil ist, dass bei einem Wechsel des Layers I mit einem Transceiver immer noch verbunden werden kann. Es ist nicht möglich, beide Anschlüsse gleichzeitig zu nutzen.

■ 2.8 Zugriffsverfahren

Wird ein Netzwerk auf der Basis von Thin-Wire aufgebaut, teilen sich alle Endgeräte das Medium. Dies bedeutet, dass immer nur ein Gerät senden kann. Der Netzwerkadapter muss also vor einer Sendung „lauschen“, ob das Medium frei ist. Erst wenn kein anderer sendet, kann er beginnen, Daten ins Medium einzuspeisen. Die Signale breiten sich im Medium aus und werden am Ende des Busses bewusst vernichtet. „Lauscht“ nun ein zweiter Rech-

ner zu einem Zeitpunkt, an dem das Signal noch nicht bis zu ihm das Medium belegt hat, „denkt“ er, dass das Medium frei wäre, und beginnt ebenfalls zu senden. Treffen sich die Signale, kommt es zu einer Kollision, und die Signale überlagern sich und werden dadurch unbrauchbar.

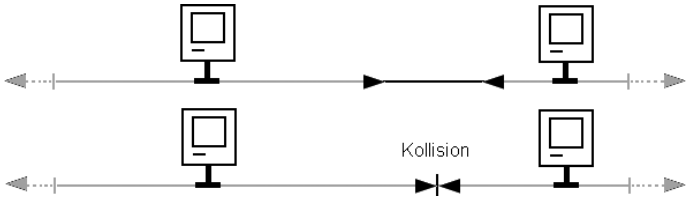


Bild 2.22 Der linke Rechner sendet. Ist das Signal noch nicht über das gesamte Medium ausgebreitet, kann ein zweiter Rechner (hier der rechte) dies nicht sehen und „denkt“, das Medium ist frei. Er beginnt also ebenfalls zu senden (oben). Treffen sich die Signale, vernichten sie sich gegenseitig, es kommt zu einer Kollision im Medium (unten).

Daher muss ein Rechner, der sendet, die doppelte Laufzeit des Signals auf der Länge des Stranges warten, bis er sich sicher sein kann, dass es keine Kollision gegeben hat. Sendet der Rechner am anderen Ende gerade dann, wenn das Signal des ersten angekommen ist, dauert es nochmals die gesamte Laufzeit, bis der erste die Kollision sehen kann.

Bild 2.23 Sind zwei Rechner genau an den Enden eines Stranges angeschlossen, wird der Parameter der doppelten Laufzeit ersichtlich. Sendet der Rechner rechts, kurz bevor das Signal des Rechners links bei ihm eintrifft, kommt es zur Kollision. Diese bemerkt der linke Sender aber erst nach der gesamten neuerlichen Laufzeit, da die Kollision über das gesamte Medium erst zu ihm zurückkommen muss.

2.8.1 CSMA/CD

Die Netzwerkadapter haben einen Sensor, der eine solche Kollision am Signalpegel entdecken kann. Der der Kollision am nächsten liegende Adapter bemerkt diese als erster und reagiert darauf, indem er ein spezielles Signal generiert, welches das gesamte Medium belegt und allen Adaptern mitteilt, dass es zu einer Kollision gekommen ist (Jam-Block). Alle wissen nun, dass im Moment nicht gesendet werden darf, und die beiden Stationen, welche die Kollision verursacht haben, wissen, dass ihre Signale zerstört sind und nochmals gesendet werden müssen.

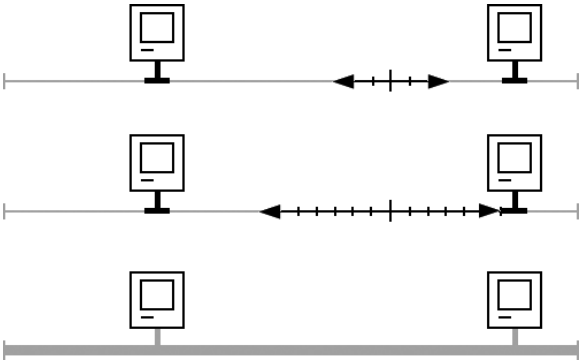


Bild 2.24 Die Kollision breitet sich im Medium aus (oben). Erreicht sie den nächsten Netzwerkadapter, wird sie von ihm entdeckt (hier vom Adapter des rechten Rechners, Mitte). Jeder Netzwerkadapter besitzt einen Sensor dafür. Er generiert nun ein Jam-Signal, welches das gesamte Medium belegt und allen mitteilt, dass eine Kollision passiert ist und im Moment niemand senden darf (unten).

Um eine sofortige neue Kollision nach einem Jam-Block zu vermeiden, beginnt auf jedem Adapter nach der Kollision (dem Ende des Jam-Signals) ein Timer anzulaufen. Diese Zeit muss der Rechner warten, bevor er wieder senden darf. Hierzu gibt es verschiedene Verfahren. Manche Hersteller setzen randomisierte Timer ein, andere wiederum bemühen die Hardwareadressen als Berechnungsgrundlage der Wartezeit.

Jeder Adapter hat eine weltweit eindeutige, in der Hardware verankerte Adresse, die sogenannte MAC-Adresse (Media Access Control Address). Sie wird unten im Layer II ausführlich besprochen. Die Dauer des Timers wird hier aus der MAC-Adresse berechnet. Da alle Stationen in einem LAN-Segment verschiedene Adressen haben müssen, ist sichergestellt, dass nach einer Kollision nicht sofort wieder zwei Stationen gleichzeitig zu senden beginnen. Dies verhindert eine sofortige neue Kollision nach dem Ende des Jam-Blocks.

Die Implementierung der Regeln, die zur Teilung eines Mediums für viele Rechner definiert werden, nennt man das Zugriffsverfahren. Das hier beschriebene ist CSMA/CD (Carrier Sense Multiple Access/Collision Detection). „Carrier Sense Multiple Access“ bedeutet, viele Rechner teilen sich ein Medium (Multiple Access), sie prüfen vor einer Sendung, ob das Medium frei ist (Carrier Sense). Ist es zu einer Kollision gekommen, kann dies erkannt und darauf reagiert werden (Collision Detection).

Der klassische Standard Ethernet beschreibt ein Netzwerk mit 10 Mbit/s auf der Basis einer Thin-Wire-Verkabelung mit CSMA/CD als Zugriffsverfahren.

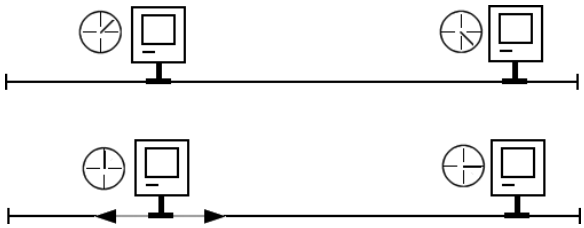


Bild 2.25 Nach dem Jam-Signal läuft auf jedem Adapter ein Timer an (oben). Der Rechner, dessen Timer zuerst wieder abgelaufen ist, darf erneut senden. So wird eine sofortige neue Kollision vermieden. Die Dauer des Timers wird nach verschiedenen Verfahren berechnet, sei es aus der Hardwareadresse (MAC-Adresse) des Adapters oder randomisiert etc. Es muss lediglich sichergestellt werden, dass nach einer Kollision nicht zwei Rechner gleichzeitig zu senden beginnen. Da in einem LAN-Segment nie zweimal dieselbe MAC-Adresse vorhanden sein darf (siehe unten), sind nach dieser Methode definitiv alle Timer-Zeiten unterschiedlich.

Ein defekter Collision-Detection-Sensor oder eine fehlerhafte Carrier Sense kann zu erheblichen Störungen im Netzwerk führen, die zum Teil schwer zu diagnostizieren sind. Prüft ein Rechner nicht mehr korrekt, ob das Medium frei ist, beziehungsweise kann er Kollisionen nicht mehr erkennen, so kann er das gesamte Layer I-Segment lahmlegen, da er einfach sendet und damit unter Umständen ständig die Daten der anderen – und natürlich seine eigenen – korrumpiert.

2.8.2 Andere Verfahren – kollisionsfreie Verfahren

CSMA/CD wurde immer wieder als Auslaufmodell angesehen. Durch die konstant wachsende Anzahl an Endgeräten im Netzwerk nahm die Zahl der Kollisionen ebenfalls ständig zu. Wie unten beschrieben wird, fand man immer wieder neue Lösungen, dies zu umgehen, CSMA/CD ist heute noch der Standard.

Viele haben versucht, andere Zugriffsverfahren zu entwickeln. Die wichtigsten sehen wir uns in der Übersicht an. An dieser Stelle noch eine wichtige Anmerkung. Im gesamten Zusammenhang der Zugriffsverfahren beschreiben wir die Kommunikation von Rechnern oder Netzwerkadaptern. Selbstverständlich betrifft das Gesagte alle Netzwerkgeräte. Alle haben ein Interface (Netzwerkkarte) im Netzwerk. Es gilt also alles nicht nur für PCs und Server, sondern genauso für Router, Switches, Netzwerkdrucker etc.

Einige Hersteller haben versucht, Zugriffsverfahren zu entwickeln, die darauf basieren, keine Kollisionen hinzunehmen und zu korrigieren, sondern von vornherein zu vermeiden. Durchgesetzt hat sich keines. CSMA/CD ist heute noch der Standard. Heute werden Kollisionen durch Geräte auf Layer II des Netzwerkes zurückgedrängt oder vermieden.

Eine Variante von CSMA/CD ist CSMA/CA. Das CA am Ende steht für Kollisionsvermeidung (Collision Avoidance). Hierbei sendet ein Adapter (Netzwerkkarte), der eine Übertragung starten möchte, ein Request-to-Send-Signal (RTS) auf das Medium, wenn dieses frei ist. Wenn es keine Kollision mit einem anderen RTS-Signal gibt, wird das RTS-Signal vom designierten Empfänger der Übertragung empfangen. Dieser wiederum antwortet mit einem Clear-to-Send-Signal (CTS), das alle anderen Adapter empfangen, sodass sie wissen, dass sie nicht senden dürfen. Ohne diese erfolgreiche „Anmeldung“ darf nicht gesendet werden. Wie wir in Kapitel 8 sehen werden, ist dieses Zugriffsverfahren im Wireless LAN (Funknetz) realisiert. Im kabelgebundenen Netzwerk hat es sich noch nicht durchgesetzt.

Token Ring ist ein inzwischen historisches Verfahren, das sehr verbreitet im Einsatz war. Die Geschwindigkeit (16 Mbit/s beziehungsweise 4 Mbit/s) ist heute zu langsam geworden. Beim Token Ring wird das Netzwerk in Form eines Ringes verlegt. Ein Rechner im Ring ist der Token Master. Er verwaltet und kontrolliert ein Bitmuster, das Token. Dieses wird von Gerät zu Gerät weitergereicht. Ist das Token „leer“, darf es der momentane Besitzer entnehmen. Er sendet nun Daten zum Empfänger. Der Empfänger quittiert dem Sender den Empfang der Daten, und der Sender reicht daraufhin das Token wieder weiter. Geht das Token verloren, wird es vom Master neu generiert.

Token Bus ist im Prinzip dasselbe Verfahren wie Token Ring, nur dass hier nicht im Ring gearbeitet wird, sondern wieder auf Thin-Wire oder UGV. Hierbei wird das Token auf dem Bus weitergereicht. Erreicht es das Ende des Busses, wird es wieder zum Anfang zurückgereicht. Damit wird virtuell die Ringstruktur im Hintergrund wiederhergestellt. Alle Features des Token Rings sind so auf einer Busstruktur realisierbar. Token Bus wird aufgrund

derselben Restriktionen, die bei Token Ring auftreten, heute nicht mehr eingesetzt. Die Verfahren sind zu langsam und zu kompliziert geworden.

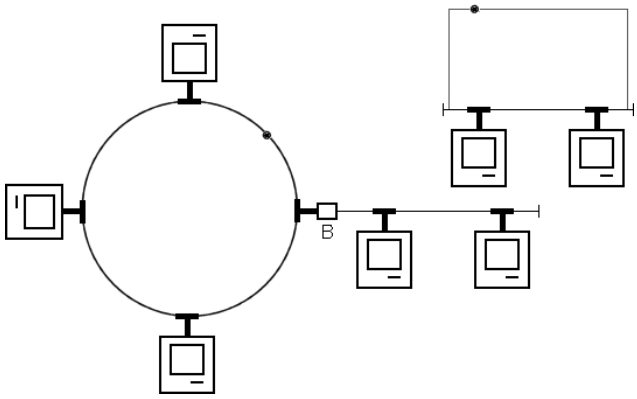


Bild 2.26 Links: Token Ring. Ein Token kreist im Ring. Nur der jeweilige Besitzer des Tokens darf senden. Ist seine Transaktion abgeschlossen, reicht er das Token wieder weiter. Rechts oben kleines Bild: Das Token wird auf einem Bus weitergereicht. Kommt es ans Ende, wird es zum Anfang zurückgereicht und wieder gesendet. Virtuell entsteht so wieder die Ringstruktur. Beide Verfahren bieten einen kollisionsfreien Zugriff auf das Medium.

Es wurden noch viele andere Verfahren entwickelt, zum Teil auch sehr proprietär. An vielen Stellen können in (in sich) geschlossenen und isolierten Umgebungen die Vorteile einer mangelnden Kompatibilität mit anderen überwiegen. Als Beispiel kann zum Beispiel die Vernetzung von Rechnern zum Aufbau eines Hochgeschwindigkeitsclusters dienen. Hier können die Längenbeschränkungen erheblich verkürzt werden. Da sind in der Regel die Geschwindigkeit und die Latenzzeiten das Wichtigste. Für den Datenaustausch nach außen kann wieder Ethernet eingesetzt werden. Für diese Verfahren möchten wir Interessierte auf die weiterführende Literatur verwiesen. CSMA/CD ist heute der Standard und fast überall im Einsatz.

■ 2.9 Zum Weiterlesen

Die zweite Organisation, die viele für die Welt der Computernetze relevante Standards herausgibt, ist das Institute of Electrical and Electronics Engineers (IEEE). Sie standardisiert vor allem Technologien der Schicht II. So basieren weite Teile dieses Kapitels auf der Ethernet-Standardfamilie IEEE 802.3, über die die Website [Healey2023] einen guten Überblick gibt.

Literatur

[Healey2023] Healey, Adam: IEEE 802.3 Ethernet Working Group. 2023. Zugegriffen 18. 07. 2023. *https://www.ieee802.org/3/*.

Index

G

H

I

R

S

X

Z