Cisco Systems

Übersetzung: Christian Alkemper
Deutsche Bearbeitung: Ernst Schawohl

Cisco Networking Academy Program
1. und 2. Semester

Cisco Press

Markt+Technik Verlag

Kapitel 3

Netzwerkmedien

Die Funktion der Bitübertragungsschicht besteht darin, Daten gemäß den elektrischen, Funkwellen- oder Lichtspezifikationen zwischen Absender und Empfänger zu übertragen. Wenn Daten ein Gebäude erreichen, werden sie in Form von Niederspannungssignalen über Leitungen in Wänden, Böden, Decken und Kabelkanälen an Workstations, Server und Netzwerkgeräte weitergeleitet. Daten – also etwa Texte, Bilder, Audio- und Videodaten – werden mit hoher Geschwindigkeit über diese Leitungen übertragen und durch elektrische Impulse im Kupferdraht oder durch Lichtimpulse in Glasfaserkabeln repräsentiert.

In diesem Kapitel werden Sie Grundlagen der Elektrotechnik kennen lernen, die für das Verständnis der Vorgänge in der Bitübertragungsschicht des OSI-Modells unentbehrlich sind. Ferner werden wir die verschiedenen Formen der Netzwerkmedien behandeln, die in der Bitübertragungsschicht eingesetzt werden: geschirmte und ungeschirmte TP-Kabel, Koaxialkabel, Glasfaserkabel sowie drahtlose Medien.

Beachten Sie bitte die diesem Kapitel zugeordneten interaktiven Medienaufgaben, Videos und Photo-Zooms auf der beiliegenden CD-ROM. Sinn dieser Zusatzinformationen ist die Ergänzung des Materials und die Vertiefung des Stoffes, der in diesem Kapitel vorgestellt wird.

3.1 Kupfermedien

Kupfer ist das meistverwendete Medium zur Signalverkabelung. Kupferdrähte sind Bestandteile eines Kabels, in dem Signale von einem Absendercomputer zu einem Empfängercomputer übermittelt werden. Kupfer weist eine Anzahl wichtiger Eigenschaften auf, die es für die elektrische Verkabelung sehr geeignet machen:

– **Leitfähigkeit.** Kupfer ist für seine Fähigkeit, den elektrischen Strom gut zu leiten, wohl am besten bekannt. Es ist aber auch ein sehr guter Wärmeleiter. Diese Eigenschaft nutzt man etwa bei der Herstellung von Kochtöpfen, Heizkörpern und Kühlschränken.

- **Korrosionsfestigkeit.** Kupfer rostet nicht und ist weitgehend unempfindlich gegen Korrosion. Kupfer oxidiert wesentlich langsamer als andere Metalle.
- **Dehnbarkeit.** Kupfer ist extrem dehnbar, d. h., es kann zu sehr dünnen Drähten gezogen werden, ohne zu brechen. So kann etwa ein Kupferstab mit einem Durchmesser von 1 cm erwärmt, gerollt und dann für Kupferlitze zu einem Draht gezogen werden, der dünner ist als ein menschliches Haar.
- **Formbarkeit.** Reines Kupfer ist extrem formbar. Es bricht nicht, wenn es in ungewöhnliche Formen gehämmert, geprägt, geschmiedet oder gedreht wird. Kupfer kann sowohl kalt als auch warm bearbeitet werden.
- **Belastbarkeit.** Kaltgewalztes Kupfer hat eine Zugfestigkeit von 3.500 bis 4.900 kp/cm^2. Es behält seine Stärke und Belastbarkeit bis zu einer Temperatur von über 200°C.

In diesem Abschnitt wollen wir uns auf zwei Kupferkabeltypen konzentrieren, die in Netzwerken zum Einsatz kommen:

- **TP-Kabel.** TP-Kabel (vom engl. *Twisted Pair*, dt. »paarweise verdrillt«) enthalten ein oder mehrere Paare verdrillter Kupferdrähte. Die meisten Daten- und Sprachnetzwerke verwenden die TP-Verkabelung.
- **Koaxialkabel.** Koaxialkabel verfügen über einen in der Mitte gelegenen, aus festem Kupfer oder Kupfergeflecht bestehenden Leiter. Früher waren Koaxialkabel erste Wahl für LANs, aber heute werden sie praktisch nur noch für Videoverbindungen, Hochgeschwindigkeitsleitungen (T3 oder E3) und Kabelfernsehen benutzt.

3.1.1 Elektrische Größen

Wie bei vielen anderen physikalischen Vorgängen müssen Sie auch bei der Elektrizität in der Lage sein, sie zu messen – andernfalls können Sie sie nicht optimal nutzen. Elektrische Größen lassen sich auf viele unterschiedliche Arten messen; in diesem Abschnitt allerdings wollen wir uns auf die Grundeinheiten Spannung, Strom, Widerstand und Impedanz konzentrieren.

Spannung

Da Elektronen und Protonen ungleichnamige Ladungen tragen, ziehen sie einander mit einer Kraft an – ähnlich wie die Anziehungskraft der beiden unterschiedlichen Pole zweier Magneten. Wenn die Ladungen getrennt werden, erzeugt diese Trennung eine Anziehungskraft zwischen den Ladungen. Diese Kraft ist die Spannung. Sie wirkt anziehend bei ungleichnamigen Ladungen und stößt gleichnamige Ladungen ab. Dieser Prozess findet etwa

in einer Batterie statt, wo chemische Reaktionen eine Freisetzung von Elektronen am negativen Pol der Batterie auslösen; die Elektronen wandern dann durch den externen Stromkreis – und nicht durch die Batterie selbst – zum entgegengesetzten positiven Pol. Die Trennung der Ladungen erzeugt die Spannung. Spannung kann außerdem durch Reibung (statische Elektrizität), durch Magnetismus (Stromgenerator) und durch Sonnenenergie erzeugt werden.

Die Spannung wird durch den Buchstaben *U* symbolisiert, die Maßeinheit ist Volt (und wird mit dem Buchstaben V abgekürzt). Es gibt zwei Arten der Spannung:

– **Gleichspannung.** Eine Batterie ist ein Beispiel für eine Gleichspannungsquelle. Die Bewegung der Elektronen in einem Gleichstromkreis erfolgt immer in der gleichen Richtung: vom Minuspol zum Pluspol. Häufig trifft man auf die Abkürzung DC, die vom engl. *Direct-Current Voltage* stammt.

– **Wechselspannung.** In einem Wechselstromkreis wechseln der Plus- und der Minuspol der Spannungsquelle regelmäßig die positive und negative Polung. Dieser ständige Wechsel führt auch zu einer stetigen Änderung der Bewegungsrichtung der Elektronen. Auch hier gibt es eine Abkürzung: AC (vom engl. *Alternating-Current Voltage*).

Lab

Siehe auch CNAP und [1]»Safe Handling and Use of a Multimeter« und »Voltage Measurements«.

Impedanz und Wellenwiderstand

In Leitern wandern Elektronen sehr leicht, weswegen man hier zur Elektronenbewegung nicht viel Spannung benötigt. In Isolatoren hingegen sind die Elektronen fest an ihre Kreisbahnen gebunden, sodass eine Bewegung hier wesentlich schwieriger ist. Dies führt zu einem höheren Widerstand; hierunter versteht man die Eigenschaft eines Materials, der Elektronenbewegung zu widerstehen. Leiter hingegen haben einen sehr niedrigen Widerstand.

Der Widerstand wird durch den Buchstaben *R* repräsentiert. Die Maßeinheit ist das Ohm, das aufgrund der akustischen Ähnlichkeit durch den griechischen Buchstaben Omega (Ω) dargestellt wird.

Der Begriff »Widerstand« wird meistens für Gleichstromkreise verwendet. Geht es hingegen um den Widerstand in einem Wechselstromkreis, so spricht man von der Impedanz, die durch den Buchstaben Z repräsentiert wird. Auch

hier ist die Grundeinheit das Ohm, angegeben durch Ω. Weiterhin bezeichnet Z auch den Wellenwiderstand eines Kabels. Diese wichtige Eigenschaft eines Netzwerkkabels wird ebenfalls in Ohm (Ω) gemessen und tritt erst bei Wechselspannungen höherer Frequenzen auf.

Der Begriff der »Dämpfung« ist in Zusammenhang mit Netzwerken ebenfalls wichtig: Hierunter versteht man den Widerstand gegen den Elektronenfluss. Die Dämpfung ist Ursache dafür, dass ein Signal, das durch einen Leiter fließt, immer schwächer wird.

Lab

Siehe auch CNAP und [1]»Resistance Measurements«.

Strom

Elektrischer Strom ist der Fluss der Ladungen, der entsteht, wenn Elektronen sich bewegen. Wenn eine Spannung (elektrischer Druck) angelegt wird und ein Weg für den Strom existiert, dann bewegen sich die Elektronen vom negativen Pol (der sie abstößt) entlang dieses Weges zum positiven Pol (der sie anzieht).

Strom wird mit dem Buchstaben *I* bezeichnet. Die Maßeinheit des Stroms ist Ampere (A). Ein Ampere ist definiert als die Anzahl der Ladungen, die pro Sekunde einen Punkt im Stromweg passieren. Man kann sich dies als Menge des Elektronenverkehrs vorstellen, der einen Stromkreis durchfließt; je mehr Elektronen einen Punkt in einem Stromkreis passieren, desto höher ist der Strom.

Auf Gleichspannung basierender Strom fließt immer in die gleiche Richtung, nämlich vom negativen zum positiven Pol. Strom, der auf Wechselspannung beruht, fließt zunächst in eine Richtung, ändert dann die Flussrichtung, kehrt danach wieder zur ursprünglichen Richtung zurück usw.

Leistung

Wenn man sich den Strom (bzw. die Stromstärke) als Menge der fließenden Elektronen veranschaulicht, dann entspricht die Spannung der Geschwindigkeit des Elektronenstroms. Die Kombination aus Stromstärke (Menge der Elektronen an einem gegebenen Punkt) und Spannung (Druck oder Geschwindigkeit der Elektronen) bezeichnet man als elektrische Leistung. Die Grundeinheit der von der Elektrizität erbrachten Leistung (oder »Arbeit«) ist das Watt (W). Die Leistung ist das Produkt aus Spannung und Strom ($W = U \times I$).

Elektrische Geräte wie Glühlampen, Motoren und Computernetzteile werden anhand ihrer Wattzahl kategorisiert, d. h. auf der Basis der Leistung, die sie verbrauchen oder erzeugen. Die eigentliche Arbeit in einem Stromkreis verrichtet der Strom. So hat etwa statische Elektrizität eine sehr hohe Spannung – so hoch, dass sie eine Lücke von einigen Zentimetern Breite überspringen kann. Die Stromstärke hingegen ist sehr niedrig, d. h., man bekommt von statischer Elektrizität zwar einen leichten elektrischen Schlag, aber sie ist nicht wirklich gefährlich. Umgekehrt arbeitet der Anlasser eines Automotors mit einer niedrigen Spannung von 12 V, aber er benötigt sehr viel Strom, um die Kraft zu erzeugen, mit welcher der Motor gestartet wird. Ein Blitzschlag weist sehr hohe Werte für Spannung *und* Stromstärke auf; er kann so sehr schwere Schäden verursachen.

Stromkreise

Strom fließt nur in geschlossenen Stromkreisen. Diese müssen aus leitfähigem Material bestehen und Spannungsquellen aufweisen, denn erst Spannung verursacht den Stromfluss, während Widerstand und Impedanz ihm entgegenwirken. Strom besteht aus Elektronen, die von den negativen Polen weg in Richtung der positiven Pole fließen. Mit dieser Erkenntnis kann man den Stromfluss auch steuern.

Die Elektrizität des 230-V-Stromnetzes fließt in Richtung der elektrischen Masse bzw. Erde, sofern ein Pfad vorhanden ist. Der Strom fließt dabei immer entlang dem Pfad des geringsten Widerstandes. Dies gilt auch, wenn dieser Pfad des geringsten Widerstandes der menschliche Körper ist. Bei 230-V-Netzsteckdosen dienen die am Rand gelegenen Schutzkontakte als Erdungs- bzw. Masseanschlüsse. Sie bilden einen sehr niederohmigen Strompfad, über den die Elektronen in die Erde fließen können. Das ist neben verschiedenen Techniken zur Abschaltung der Spannung eine Schutzmaßnahme für den Menschen, denn der Widerstand des menschlichen Körpers ist größer als der direkte Erdwiderstand. Als Masse bezeichnet man normalerweise einen Spannungspegel von 0 Volt in einer elektronischen Schaltung, der auch oft zur Schirmung der Schaltung bzw. des Kabels genutzt wird.

Elektronen bewegen sich am besten durch leitende Materialien. Zwar weist auch trockene Luft halbwegs gute Leiteigenschaften auf (wie jeder weiß, der schon einmal einen Funkenüberschlag durch statische Elektrizität gespürt hat), aber bei niedrigen Spannungen können Elektronen den Abstand zwischen einem Batteriepol und einem nahe gelegenen, aber nicht direkt angeschlossenen Kupferdraht nicht überwinden. Strom – oder Elektronenbewegung – tritt nur in *geschlossenen* Stromkreisen auf.

Spannung, Strom und Widerstand stehen in einer bestimmten Beziehung zueinander, die sich im so genannten Ohm´schen Gesetz äußert:

$$U = I \times R$$

Dies bedeutet, dass die Spannung das Produkt des Stroms multipliziert mit dem Widerstand ist. Benannt ist das Gesetz nach dem Wissenschaftler, der diese Zusammenhänge untersucht hat.

LAB

Siehe auch CNAP und [1] »Series Circuits«.

Es gibt zwei Arten des Stromflusses, nämlich Wechselstrom (engl. *Alternating Current*, AC) und Gleichstrom (*Direct Current*, DC). Stromleitungen übertragen Elektrizität in Form von Wechselstrom, da dieser besser über große Entfernungen übertragen werden kann. Gleichstrom wird hingegen bei Batterien oder Taschenlampen eingesetzt und betreibt auch Mikrochips auf der Hauptplatine eines Computers, wo nur kurze Stromstrecken zurückzulegen sind.

Bei elektrischen Systemen erfolgt der Fluss unabhängig vom verwendeten Strom (Gleich- oder Wechselstrom) immer von einer negativ zu einer positiv geladenen Quelle. Allerdings muss, damit ein kontrollierter Elektronenfluss stattfinden kann, ein vollständiger Stromkreis vorhanden sein. Zur Erinnerung: Elektrischer Strom nimmt den Weg des geringsten Widerstands.

3.1.2 Kabel- und Anschlussstandards

Standards (oder Spezifikationen) sind Sätze von Regeln oder Prozeduren, die weit verbreitet sind und als generell akzeptierte Verfahren gelten. So stellen etwa die Standards des OSI-Referenzmodells sicher, dass Netzwerkgeräte in der ganzen Welt miteinander kompatibel sind und zusammenarbeiten können. Es gibt auch viele von den im Folgenden aufgeführten amerikanischen Institutionen veröffentlichte Verkabelungsspezifikationen, die Interoperabilität, Sicherheit und Leistungsfähigkeit gewährleisten sollen.

Das IEEE (Institute of Electrical and Electronic Engineers, Institut der Elektro- und Elektronikingenieure) veröffentlicht die Verkabelungsstandards für LANs. IEEE 802.3 etwa ist ein Standard für Ethernet-Netzwerke, IEEE 802.5 der Token-Ring-Netzwerkstandard. Eine weitere Einrichtung sind die UL (Underwriters Laboratories, unabhängiges Institut für Produktsicherheitstests in den USA), die in erster Linie sicherheitsrelevante Standards veröffentlichen.

TIA (Telecommunications Industry Association, Verband der Telekommunikationsindustrie) und EIA (Electronic Industries Alliance, Verband der Elektroindustrie) geben gemeinsam Spezifikationen heraus, die häufig als TIA/EIA-Standards bezeichnet werden. Die folgende Liste beschreibt einige dieser Standards:

- **TIA/EIA-568-B.** Ein Verkabelungsstandard für Telekommunikationsnetze in Wirtschaftsgebäuden.
- **TIA/EIA-569-B.** Dieser ehemals unter der Bezeichnung »TIA/EIA-568-A« bekannte Standard beschreibt Telekommunikationsleitungen und -räume in Wirtschaftsgebäuden.
- **TIA/EIA-570-A.** Standard für die Telekommunikationsverkabelung in Privat- und kleinen Wirtschaftsgebäuden.
- **TIA/EIA-606.** Administrationsstandard für die Telekommunikationsinfrastruktur in Wirtschaftsgebäuden.
- **TIA/EIA-607.** Standard für die Erdungs- und Masseanforderungen von Telekommunikationsnetzen in Wirtschaftsgebäuden.

Die im Laufe der Zeit von dieser Organisation herausgegebenen Spezifikationen haben bedeutenden Einfluss auf die Netzwerkstandards gehabt. Sie beschreiben Standards für Horizontal- und Backbone-Verkabelung, Verteiler- und Geräteräume, Arbeitsbereiche und Anbindungseinrichtungen. Es sind die TIA/EIA-Standards, die Planung und Installation von LAN-Geräten in einer Weise ermöglichen, die es dem Netzdesigner erlaubt, Geräte frei auszuwählen und trotzdem ein betriebsfähiges LAN entwerfen zu können.

Der Standard TIA/EIA-568-B enthält Spezifikationen zur Horizontalverkabelung, d. h. für Kabel, die von einer Anschlussdose in einem Arbeitsbereich zu einem Verteilerraum verlaufen. In Europa definiert die Norm EN 50173 technische Kennwerte der strukturierten Verkabelung.

Es gibt acht der bereits erwähnten Kabelkategorien (CAT1 bis CAT8), von denen bisher allerdings nur CAT3, CAT4, CAT5(e) und CAT6 dem Standard TIA/EIA-568-B angehören. Die derzeit meistinstallierten Kabel sind CAT5e-Kabel. Zu den neuen Kategorien gehören CAT7- und CAT8-Kabel; die Standards für CAT8-Kabel befinden sich noch in der Entwicklung. Diese neuen Standards bieten im Vergleich zu CAT5e Verbesserungen und genügend Reserve für künftige Übertragungsverfahren und werden sich nach und nach durchsetzen.

Der Standard TIA/EIA-568-B sieht an jeder Anschlussdose zwei Kabel vor:

- Telefonkabel für Sprache
- Netzwerkkabel für Daten

Beim Telefonkabel muss es sich um ein zweipaariges UTP-Kabel mit passenden Anschlusssteckern handeln. Beim Netzwerkkabel hat man die Auswahl unter den folgenden Kabeltypen (auch hier ist auf korrekte Terminierung zu achten):

– vierpaariges UTP-Kabel (100 Ω) für Ethernet-LANs
– Glasfaserkabel (62,5/125 µm) für Ethernet-LANs
– Koaxialkabel (wird bei Neuinstallationen nicht mehr eingesetzt und aller Voraussicht nach bei der nächsten Revision des Standards aus dieser Liste gestrichen werden)
– zweipaariges STP-Kabel (150 Ω) für Token-Ring-LANs (nur noch sehr selten im Einsatz)

Neben diesen Anschlüssen kann ferner ein RG-6-Koaxialkabel (75 Ω) für einen TV-Anschluss eingesetzt werden, auch wenn dies im Standard nicht vorgesehen ist.

Der Standard gibt für UTP-Kabel außerdem die maximale Länge aller Kabelstrecken von der Anschlussdose zum Verteilerraum an. Für die Verbindung von der Workstation zur Anschlussdose ist ein Patchkabel (Anschlusskabel) mit einer Länge von 3 Metern vorgesehen. Die Distanz zwischen der Anschlussdose und dem Verteilerfeld im Verteilerraum darf durch ein höchstens 90 Meter langes Kabel überbrückt werden, und vom Verteilerfeld bis zum Stockwerkverteiler im Verteilerraum darf noch einmal ein 6 Meter langes Kabel verlaufen. Dieser Standard stellt sicher, dass die gesamte Kabelstrecke eine Länge von 100 Metern nicht überschreitet.

Weitere Beispiele für Ethernet-Spezifikationen, die sich auf das verwendete Kabel beziehen, sind 10/100/1000BaseT, 10Base5 oder 10Base2:

– 10/100/1000BaseT bezieht sich auf die Übertragungsrate von 10 bis 1000 Mbit/s. Es handelt sich um eine digitale Basisbandsignalisierung. Das *T* steht für *Twisted Pair* (dt. *verdrillte Aderpaare*).
– 10Base5 arbeitet ebenfalls mit einer Rate von 10 Mbit/s und der Basisbandsignalisierung. Die *5* bezeichnet die Fähigkeit des Kabels, das Signal etwa 500 Meter weit zu übertragen, bevor es aufgrund der Signaldämpfung so schwach wird, dass der Empfänger es nicht mehr einwandfrei erkennen kann. 10Base5 wird häufig auch als Thicknet bezeichnet; tatsächlich aber ist 10Base5 ein Netzwerktyp, während Thicknet das darin verwendete Kabel benennt.
– Auch 10Base2 arbeitet mit einer Rate von 10 Mbit/s und Basisbandsignalisierung. Die *2* bezeichnet die Fähigkeit des Kabels, das Signal knapp 200 Meter weit zu übertragen, bevor es aufgrund der Signaldämpfung so

schwach wird, dass der Empfänger es nicht mehr einwandfrei erkennen kann. 10Base2 wird häufig auch als Thinnet bezeichnet; tatsächlich aber ist 10Base2 ein Netzwerktyp, während Thinnet das darin verwendete Kabel benennt.

3.1.3 Koaxialkabel

Koaxialkabel (Abbildung 3.1) besteht aus den folgenden vier Komponenten:

- Kupferleiter
- Kunststoffisolierung
- geflochtene Kupferschirmung
- Kabelmantel

In der Mitte des Kabels befindet sich ein fester Kupferleiter, der von einer Schicht flexiblen Isoliermaterials umgeben ist. Um diese gewickelt ist ein Kupfergeflecht oder eine Metallfolie, die bzw. das als zweiter Leiter und außerdem als Schirmung für den inneren Leiter agiert; mit diesem Schirm werden externe Störeinflüsse vermindert. Umgeben ist der Schirm vom Kabelmantel. Für Koaxialkabel wird ein BNC-Steckverbinder verwendet (British Naval Connector oder Bayonet Neill Concelman).

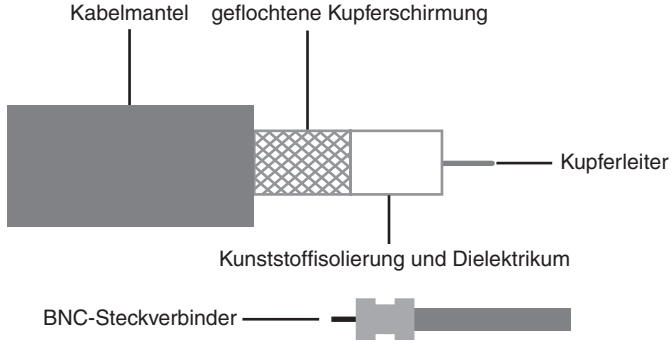


Abbildung 3.1: Koaxialkabel

In der ersten Hälfte der Neunzigerjahre war Koaxialkabel ein beliebtes LAN-Medium, denn es bot mehrere Vorzüge. Die Strecke, nach der eine Signalregenerierung erfolgen muss, ist weitaus größer als bei STP- und UTP-Kabeln, man benötigt also weniger Repeater. Zwar ist es teurer als UTP-Kabel, aber preiswerter als Glasfaserkabel. Die Technologie ist bereits bekannt, da Koaxialkabel seit vielen Jahren in der Datenkommunikation eingesetzt wird, z. B. zur Anbindung an Fernsehkabelnetze und für schnelle Internetzugänge. Beim Kabelfernsehen etwa werden häufig RG-59-Kabel

verwendet, deren Innenleiter einen AWG[1]-Durchmesser von 20 haben. RG-6 wird für die TV-Leitung von der Straße zum einzelnen Haushalt benutzt, weil es besser geschirmt ist und der Innenleiter einen AWG-Wert von 18 hat, und die Verteilung der Signale in die verschiedenen Wohnbereiche erfolgt mithilfe eines RG-11-Kabels mit noch besserer Schirmung und einem Innenleiter mit dem AWG-Wert 14.

Bei Kabeln sind die Abmessungen sehr wichtig. Mit steigendem Kabeldurchmesser vergrößern sich auch die Probleme beim Umgang mit einem Kabel. Immerhin müssen Kabel durch Kabelrohre und -kanäle gezogen werden, deren Größe beschränkt ist.

Koaxialkabel gibt es in einer Vielzahl von Größen. Der größte Durchmesser wurde früher als Kabel für Ethernet-Backbones spezifiziert, denn ein solches Kabel wies eine größere Übertragungsreichweite und bessere Störunterdrückungseigenschaften auf als andere Kabeltypen. Dieses Kabel war das so genannte Thicknet-Kabel (Abbildung 3.2). Wie der Name schon sagt, kann dieses Kabel aufgrund seines Durchmessers und der sich daraus ergebenden hohen physikalischen Steifheit die Installation erheblich erschweren. Thicknet-Kabel werden heute praktisch nicht mehr eingesetzt.

Abbildung 3.2: Koaxialkabel (Thicknet)

Später verwendete man Koaxialkabel mit einem Außendurchmesser von etwa 5 mm in Ethernet-Netzwerken. Diese Kabelsorte wird auch – im Gegensatz zum Thicknet – als Thinnet-Kabel bezeichnet (Abbildung 3.3). Thinnet war nützlich für Installationen, in denen das Kabel um viele Ecken und Winkel verlegt werden musste. Da es leichter zu installieren war, war die Installation auch billiger (deshalb und wegen des niedrigen Kabelpreises wurde diese Kabelsorte auch »Cheapernet« genannt).

Zwar arbeiten einige wenige Netzwerke mit Bustopologie noch heute mit Koaxialkabel, aber mittlerweile werden weder der Medientyp noch die Topologie vom IEEE als Standard für Ethernet-Netzwerke empfohlen. Praktisch alle neuen LANs basieren auf einer erweiterten Sterntopologie und medienseitig auf einer Kombination aus TP- und Glasfaserkabel.

1. AWG (American Wire Gauge) ist ein amerikanisches Maß für den Durchmesser eines Leiters, abgeleitet von der Anzahl der Ziehvorgänge bei der Herstellung des Kupferdrahtes. Informationen hierzu erhalten Sie im weiteren Verlauf des Kapitels.

Abbildung 3.3: Koaxialkabel (Thinnet)

Abschließend eine kurze Zusammenfassung der Merkmale von Koaxialkabeln:

- **Geschwindigkeit und Durchsatz:** 10 Mbit/s
- **Durchschnittskosten pro Knoten:** preiswert
- **Abmessungen von Medien und Steckverbindern:** mittelgroß
- **maximale Kabellänge:** mittlere Länge (500 Meter)

Exkurs: Das AWG-System

Der Durchmesser von Kabeldrähten oder -leitern wird normalerweise mithilfe des AWG-Systems angegeben. Das logarithmisch aufgebaute AWG-System (American Wire Gauge, amerikanisches Drahtmaß) ist ein in den USA gültiger Standard zur Messung des Durchmessers von Kabeln (und zwar hauptsächlich Kupfer- und Aluminiumkabeln). Normale Wohnhausverkabelungen haben einen AWG-Wert von 12 oder 14, während die in den meisten Telefonanschlussleitungen (von der Fernsprechzentrale zu einem Haus oder einem Bereich mehrerer Häuser) verwendeten Kabel die AWG-Werte zwischen 19 und 26 haben. Neuere Kabel haben Werte von AWG 22 bis AWG 26, wobei der Durchmesser 24 am gängigsten ist. Je niedriger die AWG-Zahl, desto dicker ist der Draht. Dickere Drähte weisen einen geringeren Widerstand auf, können höhere Ströme übertragen und haben bessere HF-Eigenschaften, was sich in einer höheren Signalqualität insbesondere über große Entfernungen niederschlägt. Ein Draht mit dem AWG-Wert 24 hat einen Durchmesser von 0,51 mm, AWG 22 hat einen Durchmesser von 0,64 mm.

3.1.4 TP-Kabel

Unter dem Begriff TP-Kabel versteht man einen Kabeltyp, der für Telefon und die meisten modernen Ethernet-Netzwerke verwendet wird. Ein Leiterpaar bildet einen Schaltkreis, der Daten übertragen kann. Die Paare sind verdrillt, um sie gegen Übersprechen – Störsignale, die durch das Vorhandensein benachbarter Leitungen entstehen – zu schützen.

Es gibt zwei Gründe für die Verdrillung der Paare. Zunächst einmal erzeugt eine Spannung, die einen Leiter durchläuft, ein Magnetfeld um diesen Leiter herum. Dieses Feld kann sich störend auf Signale in benachbarten Leitern auswirken. Um dieses Problem zu beseitigen, übertragen die Leiterpaare die Signale in jeweils entgegengesetzter Richtung, sodass die Magnetfelder ebenfalls in entgegengesetzten Richtungen wirken und so einander aufheben. Dieser Vorgang heißt auch Störunterdrückungseffekt. Die Verdrillung der Leiterpaare verschränkt die beiden Leiter miteinander und unterstützt auf diese Weise den Störunterdrückungseffekt innerhalb des Kabels.

Der zweite Grund besteht darin, dass Netzwerkdaten mithilfe der beiden Leiter eines Paares übertragen werden. Jeder Leiter enthält eine Kopie der Daten, und die beiden Kopien sind Spiegelbilder voneinander. Diese Signale heißen auch differenzielle Signale. Sind die beiden Leiter verdrillt, dann entstehen Störsignale, die in einem Leiter vorhanden sind, auch im anderen. Wenn die Daten dann empfangen werden, wird eine der Kopien invertiert, dann werden die beiden Signale miteinander verglichen. Auf diese Weise kann der Empfänger Störsignale ausfiltern, da die invertierten Störungen einander auslöschen.

Es gibt zwei grundlegende Varianten der TP-Kabel: STP und UTP. Die folgenden Abschnitte beschreiben diese Kabeltypen genauer.

STP-Kabel

Das STP-Kabel (vom engl. *Shielded Twisted Pair*, dt. »geschirmtes, paarweise verdrilltes Kabel«, oft auch als PiMF für »Paare in Metallfolie« oder S-STP-Kabel bezeichnet) enthält in der Regel vier Paare aus dünnen, von farblich gekennzeichneten Kunststoffisolierungen umgebenen Kupferleitern, die verdrillt sind. Jedes Leiterpaar ist einzeln in Metallfolie eingewickelt, und die vier Leiterpaare werden dann noch einmal gemeinsam in Metallfolie oder -geflecht verpackt. Dieses gesamte Flechtwerk ist von einem Kunststoffmantel umgeben. Abbildung 3.4 zeigt ein STP-Kabel.

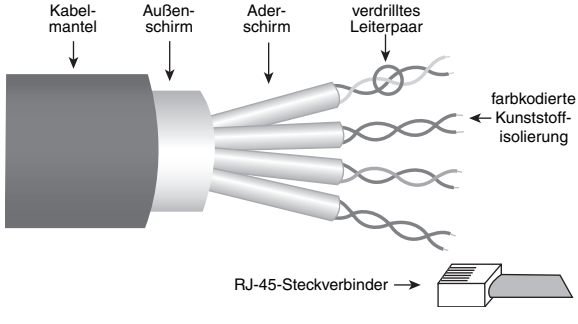


Abbildung 3.4: S-STP-Kabel

Der Wellenwiderstand beträgt für STP-Ethernet-Kabel 100 bis 120 Ω und für STP-Kabel mit zwei Aderpaaren zur Verwendung in Token-Ring-Netzwerken 150 Ω. Der Steckverbinder, der an STP-Kabeln für Ethernet zum Einsatz kommt, ist ein geschirmter RJ45-Stecker.

Das ScTP-Kabel (vom engl. *Screened Twisted Pair*, auch »FTP-Kabel« vom engl. *Foil Twisted Pair* oder »S-UTP-Kabel« genannt) ist eine Hybridform aus geschirmtem und ungeschirmtem Kabel. Es handelt sich hierbei im Wesentlichen um ein UTP-Kabel, bei dem eine Folienschicht um alle vier Leiterpaare gewickelt ist (Abbildung 3.5). Die Schirmung verringert sowohl bei STP- als auch bei ScTP-Kabeln unerwünschte elektrische Störeinstrahlungen. Diese Störunterdrückung stellt einen wesentlichen Vorteil der STP-Kabel gegenüber ungeschirmten Kabeln dar.

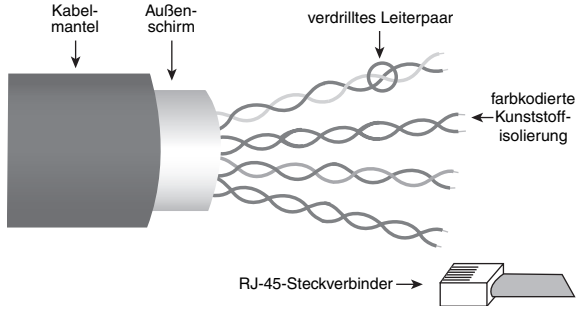


Abbildung 3.5: ScTP-Kabel

Ein Nachteil geschirmter Kabel besteht darin, dass sie schwieriger zu installieren sind als ungeschirmte Kabel, weil die Schirmung geerdet werden muss. Wenn STP- und ScTP-Kabel unsachgemäß installiert werden, sind sie sehr anfällig für Störeinstrahlungsprobleme, weil eine ungeerdete Schirmung wie eine Antenne wirkt und unerwünschte Signale auffängt. Ohne Repeater ist die Reichweite von STP- und ScTP-Kabel erheblich geringer als die von Koaxial- und Glasfaserkabel. Isolierung und Schirmung vergrößern die Abmessungen und das Gewicht der Kabel erheblich und steigern zudem die Kosten. Doch trotz dieser Nachteile werden STP-Kupferkabel insbesondere in Europa überwiegend als Netzwerkmedien eingesetzt.

Abschließend eine kurze Zusammenfassung der Merkmale von STP-Kabeln:

- **Geschwindigkeit und Durchsatz:** 10 … 10.000 Mbit/s
- **Durchschnittskosten pro Knoten:** mäßig teuer
- **Abmessungen von Medien und Steckverbindern:** mittelgroß bis groß
- **maximale Kabellänge:** kurz (≤ 100 Meter)

Exkurs: Kabelbezeichnungen

Neben den hier genannten Kabelbezeichnungen für Twisted-Pair-Kabel gibt es mitunter mehrere (und zum Teil verwirrende) Herstellerbezeichnungen für ein und dieselbe Kabelsorte (wie hier z. B. ScTP, FTP und S-UTP). Zur Vereinheitlichung schlägt die 2. Ausgabe der Norm ISO/IEC 11801 hier folgende Kennzeichnung vor:

x x / y T P

Dabei kann *x x* (Gesamtschirm) folgende Werte annehmen:

- S (Geflechtschirm)
- F (Folienschirm)
- SF (Schirm aus Geflecht und Folie)

Zudem kann *y* (Einzelschirm) die Werte *U* (ungeschirmt) und *F* (Folienschirm) annehmen.

UTP-Kabel

UTP-Kabel (vom engl. *Unshielded Twisted Pair*, dt. »ungeschirmtes, paarweise verdrilltes Kabel«) ist ein in Nordamerika weit verbreitetes Netzwerkmedium. Es enthält vier Paare aus dünnen, von farblich gekennzeichneten Kunststoffisolierungen umgebenen Kupferleitern, die verdrillt sind (Abbildung 3.6). Die Leiterpaare sind von einem Kunststoffmantel umgeben. Der Steckverbinder, der an UTP-Kabeln zum Einsatz kommt, ist ein RJ45-Stecker (Registered Jack 45, Abbildung 3.7).

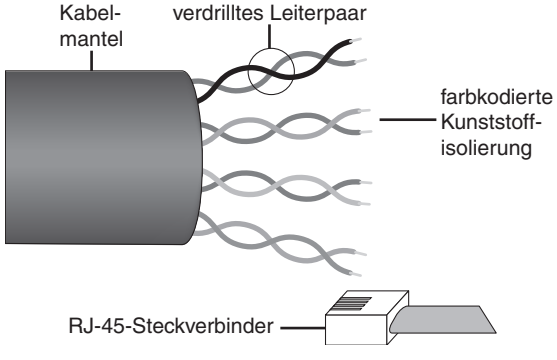


Abbildung 3.6: UTP-Kabel

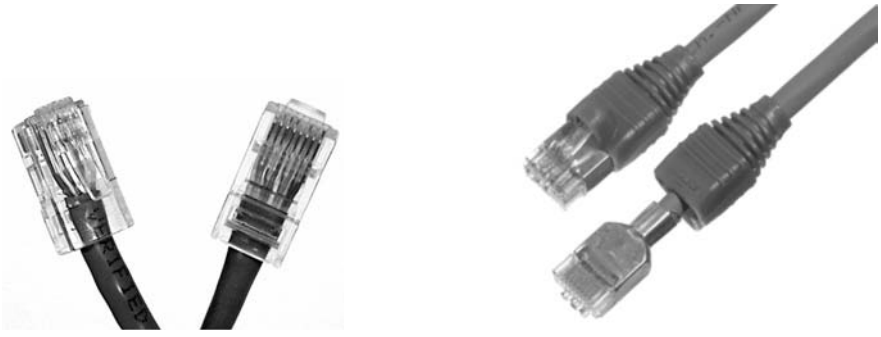


Abbildung 3.7: RJ45-Steckverbinder ungeschirmt (links) und geschirmt (rechts) (Quelle rechts: Tyco Electronics AMP)

UTP-Kabel weisen eine Reihe von Vorteilen auf: Sie haben einen geringen Durchmesser und müssen nicht geerdet werden, d. h., sie sind der am leichtesten zu installierende Kabeltyp. Der geringe Umfang bietet einen weiteren Vorteil, da mehr UTP-Kabel an einem gegebenen Ort installiert sein können als andere Kupfermedien. Ferner sind UTP-Kabel das preiswerteste Medium, und der Steckverbinder ist leicht zu montieren. Unterstützt werden nicht ganz so hohe Datenraten wie bei STP-Kupfermedien.

Der wesentliche Nachteil von UTP-Kabel ist seine im Vergleich zu anderen Netzwerkmedien ausgeprägte Anfälligkeit gegenüber elektrischen Störsignalen und Interferenzen. Da keine Schirmung vorhanden ist, basiert die Störsignalunterdrückung ausschließlich auf dem Störunterdrückungseffekt und der Nutzung differenzieller Signale. Ein weiterer Mangel besteht wie bei STP-Kabeln darin, dass die maximal zulässige Kabellänge geringer ist als bei Koaxial- und Glasfaserkabel.

Hier eine kurze Zusammenfassung der Merkmale von UTP-Kabeln:

– **Geschwindigkeit und Durchsatz:** 10 … 1.000 Mbit/s
– **Durchschnittskosten pro Knoten:** sehr preiswert
– **Abmessungen von Medien und Steckverbindern:** klein
– **maximale Kabellänge:** kurz (≤ 100 Meter)

Man unterscheidet verschiedene Kategorien von TP-Kabeln:

– **Kategorie 1 (CAT1).** Wird für die Telefonkommunikation eingesetzt. Für die Datenübertragung ungeeignet.
– **Kategorie 2 (CAT2).** Geeignet für die Datenübertragung bis 4 Mbit/s.
– **Kategorie 3 (CAT3).** Wird in Nordamerika für 10BaseT-Ethernet-Netzwerken eingesetzt. Geeignet für die Datenübertragung bis 10 Mbit/s.

- **Kategorie 4 (CAT4).** Wird in Token-Ring-Netzwerken eingesetzt. Geeignet für die Datenübertragung bis 16 Mbit/s.
- **Kategorie 5 (CAT5).** Geeignet für die Datenübertragung bis 100 Mbit/s. Wird in Fast-Ethernet-Netzwerken eingesetzt.
- **Kategorie 5e (CAT5e).** Geeignet für die Datenübertragung bis 1.000 Mbit/s. Wird in Gigabit-Ethernet-Netzwerken eingesetzt.
- **Kategorie 6 (CAT6).** Die CAT6-Spezifikation wurde 2003 veröffentlicht und kann mit UTP- und STP-Kabeln für Installation und Betrieb benutzt werden. Wird in Gigabit-Ethernet-Netzwerken eingesetzt.
- **Kategorie 7 (CAT7).** Die CAT7-Spezifikation wurde 2004 verabschiedet und erreicht 600 MHz. Diese Spezifikation wird zurzeit nur von doppelt geschirmten Kabeln erfüllt, die für das zukünftige 10GBaseT eingesetzt werden können.
- **Kategorie 8 (CAT8).** Die CAT8-Spezifikation existiert noch nicht als Norm. Die Kabel übertragen Signale bis zu 1.500 MHz. Diese „Spezifikation" wird zurzeit nur von doppelt geschirmten Kabeln erfüllt. Die Kabel sind besonders geeignet für das zukünftige 10GBaseT und können auch für Videoübertragung (CATV) eingesetzt werden.

In der Regel bestehen CAT5-Kabel und höher aus vier Paaren eines massiven oder mehrfasrigen Kupferleiters mit dem AWG-Wert 24. In älteren Installationen werden CAT3-Kabel für die Sprachkommunikation und CAT5-Kabel für die Datenübertragung eingesetzt, in neueren Implementierungen werden CAT5e-Kabel gleichermaßen für Sprache und Daten verwendet. Zwar sind diese Kabel etwas teurer, amortisieren sich aber auf lange Sicht.

Beachten Sie die folgenden Aspekte beim Vergleich zwischen UTP- und STP-Kabeln:

- Die Bandbreite beider Typen ist normalerweise für LAN-typische Entfernungen ausreichend.
- Es handelt sich hierbei um die preiswertesten Medien für die Datenkommunikation. Dabei ist UTP noch preiswerter als STP.
- Da in den USA im Gegensatz zu Europa in den meisten Gebäuden bereits UTP-Kabel verlegt sind, wurden viele Übertragungsstandards so verfasst, dass sie diese Kabel benutzen, um eine kostspielige Neuverlegung alternativer Kabeltypen zu vermeiden. Man muss sicherstellen, dass die Kategorie der vorhandenen Kabel zur Unterstützung der gewünschten Technologie ausreicht; so kann beispielsweise ein Gebäude, in dem CAT3-Kabel vorhanden sind, in dieser Form Fast Ethernet nicht unterstützen, weil diese Technologie mindestens CAT5 benötigt.

Lab

Siehe auch CNAP und [1] »Communications Circuits«, »Fluke 620 Basic Cable Testing«, » Straight-Through Cable Construction«, »Rollover Cable Construction«, »Crossover Cable Construction«, »UTP Cable Purchase«.

3.2 Optische Medien

Glasfaser ist das heute meistverwendete Medium für längere Point-to-Point-Verbindungen mit hoher Bandbreite, wie sie in LAN-Backbones und in WANs benötigt werden. Für den Einsatz von Glasfasern sprechen viele Gründe: Glasfaserkabel werden in Netzwerke eingesetzt, weil

- sie nicht empfindlich sind für Blitzschlag, elektromagnetische und Hochfrequenzstörungen und diese Störungen auch nicht verursachen,
- sie eine wesentlich größere Bandbreitenkapazität aufweisen als andere Medien,
- sie erheblich größere Reichweiten und eine exzellente Signalqualität bieten, da nur eine sehr geringe Signaldämpfung auftritt,
- sie sicherer als andere Medien sind (es ist schwierig, an einem Glasfaserkabel einen Abgriff anzubringen, und solche Abgriffe werden in der Regel auch schnell entdeckt),
- derzeitige Sender- und Empfängerkomponenten für Glasfaser ohne weiteres durch modernere und schnellere Technologien ersetzt werden können, sobald diese verfügbar sind, d. h., es lassen sich höhere Übertragungsgeschwindigkeiten über vorhandene Glasfaserverbindungen erzielen, ohne die Kabel austauschen zu müssen,
- Glasfaser gerade bei langen Kabelwegen ihre Kostenvorteile ausspielen können,
- als Rohmaterial für die Fasern Sand dient – ein Rohstoff, der im Übermaß vorhanden ist,
- Erdungsprobleme anders als bei der Signalübertragung auf der Basis von geschirmten Leitungen nicht auftreten,
- Glasfaserkabel ein geringes Gewicht haben und leicht zu installieren sind,
- Glasfaserkabel gegenüber Umwelteinflüssen (z. B. Wasser) robuster sind als Kupferkabel,
- sich Glasfaserkabelwege praktisch beliebig verlängern lassen.

Aus diesen Gründen werden Glasfaserverbindungen häufig verwendet, wenn sehr große Datenmenge über lange Strecken – d. h. Strecken von mehr als 100 Metern – übertragen werden müssen.

In diesem Abschnitt werden wir die Grundlagen des Glasfaserkabels erläutern. Sie werden erfahren, wie die Fasern Licht über große Distanzen hinweg übertragen. Ferner werden Sie lernen, welche Arten von Kabeln verwendet werden, wie Glasfaserkabel installiert werden, welche Arten von Steckern und Geräten in Verbindung mit Glasfaserkabeln zum Einsatz kommen und wie die Funktionsfähigkeit der Kabel geprüft werden kann.

3.2.1 Das elektromagnetische Spektrum

Beim in Glasfasernetzwerken verwendeten Licht handelt es sich um einen Typ mit elektromagnetischer Energie. Wenn eine elektrische Ladung sich vorwärts und rückwärts bewegt oder beschleunigt wird, dann wird eine elektromagnetische Energie erzeugt. Diese Energie kann in Form von Wellen durch ein Vakuum, durch die Luft und durch einige Materialien – z. B. Glas – übertragen werden. Eine wesentliche Eigenschaft einer Energiewelle ist die Wellenlänge (Abbildung 3.8).

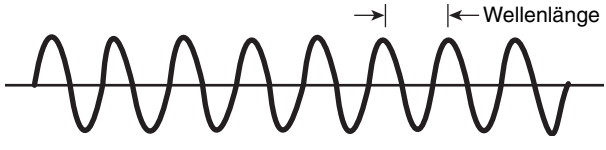


Abbildung 3.8: Wellenlänge

Dem Menschen erscheinen Funkwellen, Mikrowellen, Radarwellen, sichtbares Licht, Röntgenstrahlen und Gammastrahlen als völlig unterschiedliche Dinge, aber sie alle sind Ausprägungen der elektromagnetischen Energie. Wenn man all diese Arten elektromagnetischer Wellen in Bezug auf ihre Wellenlänge absteigend sortiert, dann entsteht eine Skala, die als elektromagnetisches Spektrum bezeichnet wird.

Die Wellenlänge einer elektromagnetischen Welle ist dadurch definiert, wie häufig die elektrische Ladung, welche die Welle erzeugt, sich rückwärts und vorwärts bewegt. Bewegt sich die Ladung beispielsweise eher langsam rückwärts und vorwärts, dann wird eine lange Welle erzeugt. Man kann die Bewegung der elektrischen Ladung mit der Bewegung vergleichen, die man mit einem Stock in einem stehenden Gewässer erzeugt: Wenn Sie den Stock langsam nach links und rechts bewegen, dann entstehen Wellen auf dem Wasser, deren Kämme weit auseinander liegen. Bewegt man den Stock hingegen schneller, dann liegen auch die Wellenkämme näher aneinander – die Wellenlänge ist kürzer.

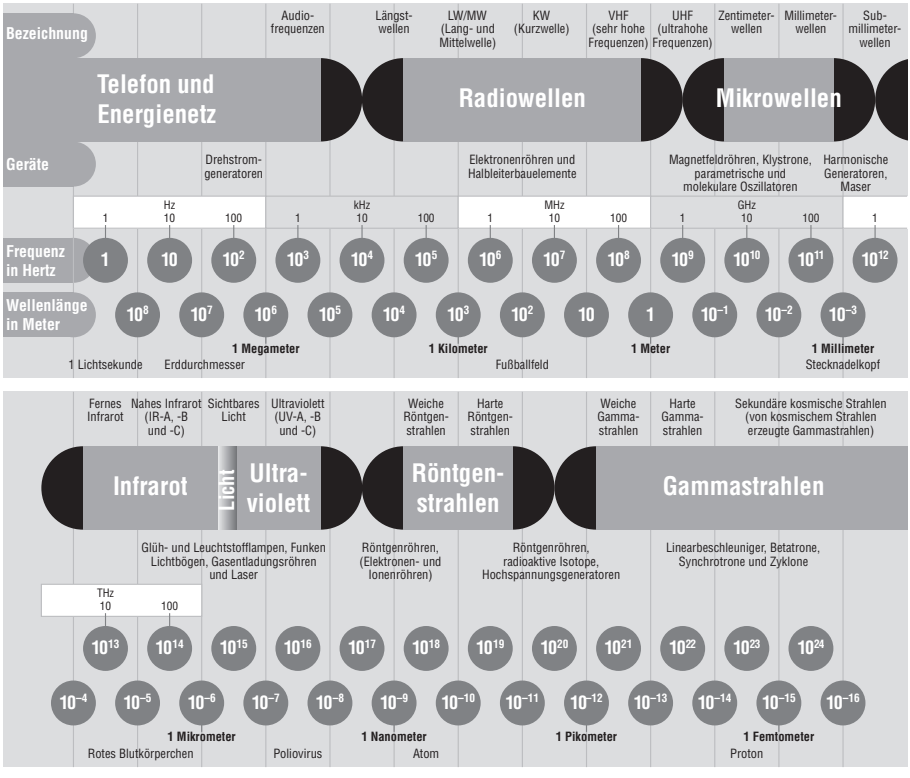


Abbildung 3.9: Das elektromagnetische Spektrum

Da alle elektromagnetischen Wellen auf die gleiche Weise erzeugt werden, weisen sie auch eine Menge Gemeinsamkeiten auf. So werden sie im Vakuum alle mit der gleichen Geschwindigkeit übertragen, nämlich der Lichtgeschwindigkeit (300.000 km/s).

Das menschliche Auge erkennt elektromagnetische Energie nur dann, wenn sie eine Wellenlänge zwischen 800 und 400 nm aufweist[1]. Man nennt elektromagnetische Energie in diesem Bereich »sichtbares Licht«. Dabei erscheinen uns Wellen mit einer Länge von etwa 700 nm als die Farbe Rot, während die kürzeren Wellen mit einer Länge von 400 nm als violett erkannt werden. Dieser Abschnitt des elektromagnetischen Spektrums enthält die Farben des Regenbogens.

Zur Übertragung von Daten über eine Glasfaser werden meist Wellenlängen verwendet, die für das menschliche Auge nicht sichtbar sind. Das entsprechende Licht hat eine Länge, die ein wenig länger ist als rot, weswegen man von Infrarotlicht spricht. Mit Infrarotlicht arbeiten z. B. auch die Fernbedie-

1. 1 nm (Nanometer) = 0,000000001 m, also ein Milliardstel Meter.

nungen von Fernsehgeräten. Die gängigen Wellenlängen des für die Glasfaserübertragung verwendeten Lichts sind die folgenden:

- 850 nm
- 1310 nm
- 1550 nm

Diese Wellenlängen wurden gewählt, weil ihre Übertragungseigenschaften in der Glasfaser besser sind als die anderer Wellenlängen.

3.2.2 Das Strahlenmodell

Wenn elektromagnetische Wellen – also z. B. Lichtwellen – von einer Quelle ausgesandt werden, breiten sie sich geradlinig aus. Die geraden Linien, die in der Lichtquelle ihren Ursprung nehmen, heißen Strahlen. Strahlen sind schmale Lichtstreifen, wie man sie etwa von Lasern her kennt. Im Vakuum des luftleeren Raums pflanzt sich das Licht geradlinig mit einer Geschwindigkeit von 300.000 km/s fort. Die Fortpflanzung in anderen Materialien – Luft, Wasser oder Glas – erfolgt jedoch mit anderen, geringeren Geschwindigkeiten.

Wenn ein Lichtstrahl – in der Optik redet man vom *einfallenden* Strahl – auf die Grenze zwischen zwei unterschiedlichen Materialen (etwa Luft und Glass) trifft, dann wird ein Teil der Lichtenergie im Strahl zurückgeworfen. Dies ist beispielsweise der Grund, warum man sich in einem Spiegel sehen kann. Das zurückgeworfene Licht ist der *reflektierte* Strahl.

Die Lichtenenergie im einfallenden Strahl, die nicht reflektiert wird, tritt in das Glas ein. Dabei wird der eintretende Strahl in der Regel in einem bestimmten Winkel gebogen. Dieser Strahl heißt nun *gebrochener* Strahl. Wie stark der einfallende Strahl gebrochen wird, hängt von zwei Faktoren ab:

- dem Winkel, in dem der einfallende Strahl auf die Oberfläche des Glases auftrifft,
- den unterschiedlichen Geschwindigkeiten, mit denen sich das Licht in den beiden betroffenen Medien (hier: Luft und Glas) fortpflanzt.

Die Brechung des Lichts an der Grenzfläche der beiden Medien ist der Grund dafür, dass das Licht sich auch dann in einem Glasfaserkabel weiterbewegt, wenn dieses um eine Ecke verlegt ist.

Wie viele Lichtstrahlen im Glas gebrochen werden, hängt von der optischen Dichte des Glases ab. Der Begriff der optischen Dichte beschreibt, wie stark ein Lichtstrahl verlangsamt wird, wenn er ein Medium durchquert. Je größer

die optische Dichte eines Materials, desto stärker werden die Lichtstrahlen abgebremst. Das Verhältnis zwischen der Geschwindigkeit eines Lichts in einem Material und der Lichtgeschwindigkeit in einem Vakuum wird als Brechungsindex n des Materials bezeichnet und wie folgt ausgedrückt:

$$n = \frac{\text{Geschwindigkeit des Lichts im Vakuum}}{\text{Geschwindigkeit des Lichts im Material}}$$

Insofern ist das Maß der optischen Dichte eines Materials für seinen Brechungsindex verantwortlich. Ein Material mit einem hohen Brechungsindex hat eine größere optische Dichte – und bremst die Lichtenergie mithin stärker – als ein Material mit einem niedrigen Brechungsindex. Tabelle 3.1 zeigt die Brechungsindizes von Luft, Glas, Diamant und Wasser.

Tabelle 3.1: Brechungsindex n verschiedener Medien

Medium	Brechungsindex
Luft	1,000
Glas	1,523
Diamant	2,419
Wasser	1,333

Bei einem Medium wie Glas lässt sich der Brechungsindex (also die optische Dichte) erhöhen, indem man ihm bestimmte Chemikalien beifügt. Umgekehrt kann man den Wert *n* auch verringern, indem man das Glas äußerst rein macht.

In den nächsten beiden Abschnitten werden Sie mehr zu den Themen Reflexion und Brechung erfahren. Sie benötigen dieses Wissen, um Aufbau und Funktionsweise von Glasfaserkabeln verstehen zu können.

3.2.3 Reflexion

Wenn das Licht sich in einem Medium wie Luft fortpflanzt und dann auf ein anderes Medium wie etwa Glas trifft, dann wird es teils reflektiert, teils gelangt es in bzw. durch das zweite Medium hindurch (Abbildung 3.10). Wie viel Licht genau reflektiert wird bzw. durch das Medium gelangt, wird von dem Winkel bestimmt, in dem es auf die Oberfläche trifft. Der Winkel zwischen dem einfallenden Strahl und einer gedachten Linie, die senkrecht zur Oberfläche steht, heißt Einfallswinkel. Wenn der Einfallswinkel einen bestimmten Punkt – den so genannten kritischen Winkel – erreicht, dann wird das gesamte Licht in das ursprüngliche Medium reflektiert (Abbildung 3.11).

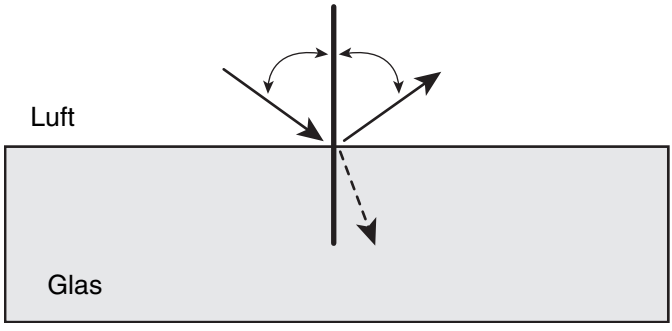


Abbildung 3.10: Reflexion

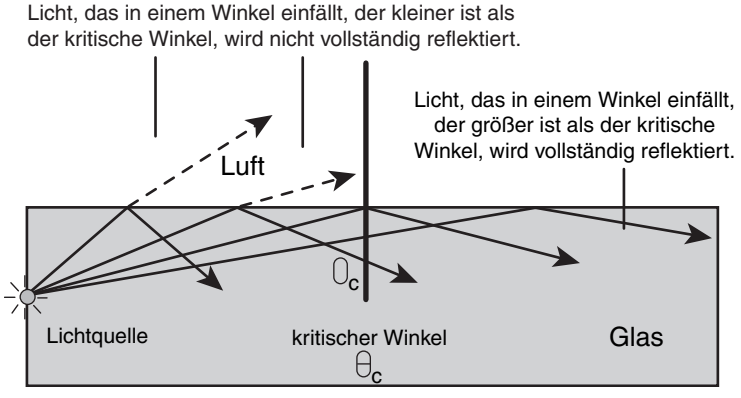


Abbildung 3.11: Kritischer Winkel

Die Bezugslinie wird als die Senkrechte (Lot) bezeichnet. Sie ist kein Lichtstrahl, sondern vielmehr ein Hilfsmittel, das eine Winkelmessung ermöglicht. Der Winkel zwischen der Senkrechten und dem reflektierten Strahl ist der Ausfallswinkel oder Reflexionswinkel. Das Reflexionsgesetz besagt, dass der Ausfallswinkel eines Lichtstrahls mit dem Einfallswinkel identisch ist, d. h., der Winkel, in dem ein Lichtstrahl auf eine reflektierende Oberfläche auftrifft, stimmt mit dem Winkel überein, in dem der Strahl von der Oberfläche zurückgeworfen wird.

3.2.4 Brechung

Wenn das Licht auf die Grenzfläche zweier transparenter Materialien trifft (z. B. Luft und Glas), dann wird es geteilt: Ein Teil des Lichts wird wieder in das erste Medium – die Luft – zurückgeworfen, wobei der Reflexionswinkel dem Einfallswinkel entspricht. Die verbleibende Lichtenergie durchquert die Grenzfläche und tritt in das zweite Medium ein: das Glas.

Wenn der einfallende Strahl in einem Winkel von exakt 90° auf die Glasoberfläche auftrifft, dann tritt er geradlinig in das Glas ein, d. h., er wird nicht gebrochen. Beträgt der Einfallswinkel jedoch nicht exakt 90°, dann wird die Richtung des in das Glas eintretenden Strahls geändert. Dies bezeichnet man als Brechung des Strahls. Wie stark der Strahl gebrochen wird, hängt vom Brechungsindex der beiden transparenten Materialien ab. Wenn der Strahl aus einem Medium mit niedrigem Brechungsindex in ein anderes mit einem höheren Brechungsindex eintritt, dann wird er in Richtung der Senkrechten gebrochen; tritt er hingegen aus einem Medium mit höherem Brechungsindex in eines mit niedrigerem Brechungsindex ein, dann wird er von der Senkrechten weggebrochen. Abbildung 3.12 zeigt ein Beispiel für die Brechung.

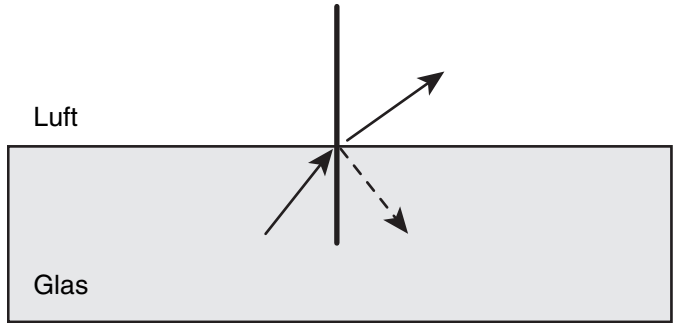


Abbildung 3.12: Brechung

Betrachten Sie etwa einmal einen Lichtstrahl, der in einem Winkel ungleich 90° auf die Grenzfläche zwischen Glas und Diamant trifft (Abbildung 3.13). Das Glas hat einen Brechungsindex von etwa 1,523, der Diamant hingegen einen Brechungsindex von ca. 2,419. Aus diesem Grund wird der Strahl, der in den Diamanten eintritt, zur Normalen hin gebrochen. Wenn dieser Lichtstrahl in einem Winkel ungleich 90° auf die Grenzfläche zwischen dem Diamanten und der Luft trifft, wird er von der Senkrechten weggebrochen. Der Grund hierfür besteht darin, dass Luft einen kleineren Brechungsindex (etwa 1,000) hat als der Diamant.

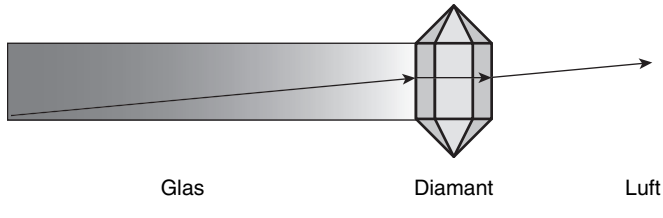


Abbildung 3.13: Brechung (Beispiel)

3.2.5 Interne Totalreflexion

Ein Lichtstrahl, der ein- und ausgeschaltet wird, um Daten als Nullen und Einsen über eine Glasfaser zu übertragen, muss innerhalb der Faser bleiben, bis er sein Ziel erreicht. Der Strahl darf nicht in das Material gebrochen werden, das die Glasfaser umgibt, denn solche Brechungen würden zu einem teilweisen Verlust der Lichtenergie führen. Es muss ein Aufbau für die Glasfaser gefunden werden, bei dem die Außenfläche der Faser als Spiegel für den Lichtstrahl wirkt, der sich in der Glasfaser fortbewegt. In einem geeigneten Wellenleiter wird ein Lichtstrahl, der an der Seite der Glasfaser auszutreten versucht, in einem Winkel in die Faser reflektiert, der ihn in Richtung des Ziels schickt (Abbildung 3.14).

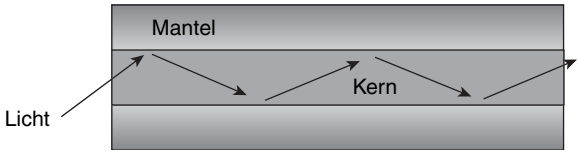


Abbildung 3.14: Interne Totalreflexion

Die Reflexions- und Brechungsgesetze sagen uns, wie eine Faser auszusehen hat, die Lichtwellen bei minimalem Energieverlust übertragen kann. Damit Lichtstrahlen in einer Glasfaser wieder in die Faser reflektiert werden, ohne dass Energieverluste durch Brechung auftreten, müssen zwei Bedingungen erfüllt sein:

– Der Kern (d. h. die Innenseite) der Glasfaser muss einen höheren Brechungsindex aufweisen als das den Kern umgebende Material, das so genannte Mantelglas.

– Der Einfallswinkel des Lichtstrahls muss größer sein als der kritische Winkel von Kern und Mantel.

Werden diese beiden Bedingungen erfüllt, dann wird das gesamte in die Glasfaser einfallende Licht zurück in die Faser reflektiert. Diese Bedingung heißt auch interne Totalreflexion und ist die Konstruktionsgrundlage für Glasfaserkabel. Die interne Totalreflexion sorgt dafür, dass die Lichtstrahlen in der Glasfaser von der Grenzfläche zwischen Kern und Mantel reflektiert werden und ihren Weg zum entfernten Ende der Faser fortsetzen. Das Licht folgt gewissermaßen einem Zickzackpfad durch den Glasfaserkern.

Eine Glasfaser, welche die erste Bedingung erfüllt – also über einen Kern mit einem Brechungsindex verfügt, der höher ist als der des Mantels –, lässt sich relativ leicht anfertigen. Auch der Einfallswinkel der Lichtstrahlen, die in den Kern gelangen, lässt sich durch Beschränkung zweier Faktoren steuern:

– **Die numerische Apertur der Glasfaser.** Die numerische Apertur des Kerns ist der Winkelbereich, in dem in die Glasfaser einfallende Strahlen intern vollständig reflektiert werden (Abbildung 3.15).
– **Die Moden.** Moden sind Pfade, auf denen sich ein Lichtstrahl in der Glasfaser fortbewegt.

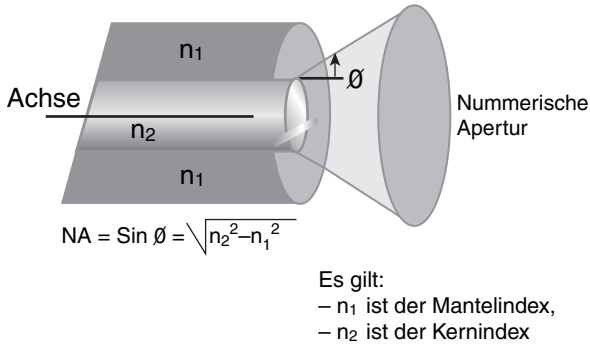


Abbildung 3.15: numerische Apertur

Wenn diese beiden Faktoren entsprechend gestaltet sind, lässt sich eine Glasfaser mit interner Totalreflexion erstellen, d. h. ein Lichtwellenpfad, der für die Datenkommunikation geeignet ist (Abbildung 3.16).

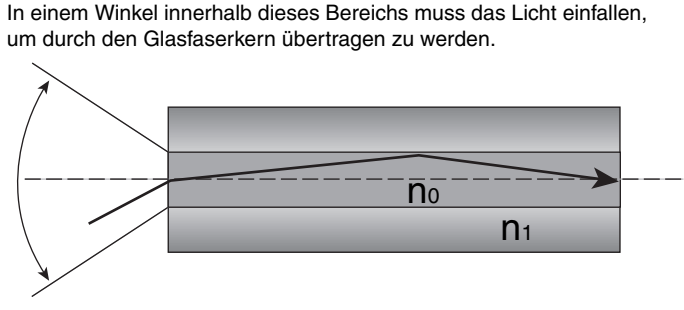


Abbildung 3.16: Lichtwellenpfad

3.2.6 Glasfaserkabel

Das Glasfaserkabel ist ein Netzwerkmedium, in dem über dünne Glasadern Daten in Form von moduliertem Licht übertragen werden. Signale, die Datenbits repräsentieren, werden in Lichtstrahlen umgewandelt. Es soll an dieser Stelle gesagt werden, dass Elektrizität zwar an den Endgeräten benötigt wird, um die Lichtsignale zu erzeugen bzw. zu erkennen, dass aber – anders als bei kupferbasierten Medien – in den Kabeln selbst keine Elektri-

zität vorhanden ist. Glasfaserkabel sind vielmehr hervorragende Isolatoren und kupferbasierten Medien in vielerlei Hinsicht überlegen.

Jedes Glasfaserkabel, das in der Netzwerktechnik eingesetzt wird, besteht aus zwei Glasfasern mit jeweils separatem Mantel. Eine Faser überträgt die gesendeten Daten von Gerät A zu Gerät B, die andere von Gerät B zu Gerät A. Es existiert also eine Datenfaser in jede Richtung – ähnlich etwa wie baulich getrennte Fahrbahnen in gegenläufigen Richtungen. Diese Anordnung realisiert eine Vollduplexleitung. Ähnlich wie TP-Kabel getrennte Leitungspaare zum Senden und Empfangen verwenden, bieten Glasfaserverbindungen jeweils eine Faser für den Empfang und eine zum Senden von Daten (Abbildung 3.17). Normalerweise befinden sich die beiden Fasern bis zu dem Punkt in einem gemeinsamen Kabelmantel, an dem die Stecker befestigt sind.

Abbildung 3.17: Duplexglasfaser

An diesem Punkt werden die beiden Kabel getrennt. Eine Verdrillung oder Schirmung wird nicht benötigt, denn da das Licht innerhalb der Faser nicht abgestrahlt werden kann, entstehen im Glasfaserkabel auch keine Übersprechprobleme. In der Regel werden mehrere Faserpaare in ein und demselben Kabel untergebracht, d. h., es verläuft nur ein einziges Kabel zwischen Verteilerraum, Stockwerken oder Gebäuden. Ein Kabel kann zwei, vier, acht, zwölf, 24, 48 oder mehr getrennte Fasern enthalten. Im Gegensatz dazu muss beim Einsatz von TP-Kabeln für jede Verbindung ein Kabel verlegt werden (ausgenommen hiervon ist die Doppelnutzung, da für 10BaseT und 100BaseT nur zwei der vier Aderpaare benötigt werden). Glasfasern haben zudem einen wesentlich höheren Datendurchsatz und können die Daten über größere Entfernungen übertragen, als es mit Kupfer möglich ist.

Wie Abbildung 3.18 und Abbildung 3.19 zeigen, besteht ein typisches Glasfaserkabel aus fünf Komponenten:

- Kern
- Mantelglas
- Puffermaterial
- Verstärkungsmaterial
- Außenmantel

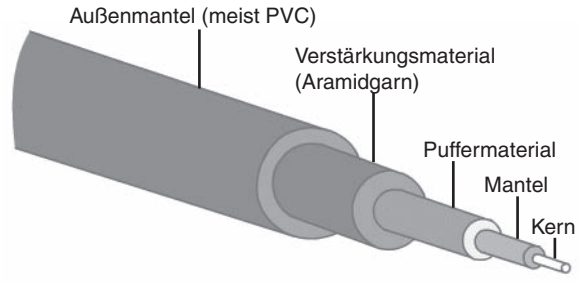


Abbildung 3.18: Aufbau eines Glasfaserkabels

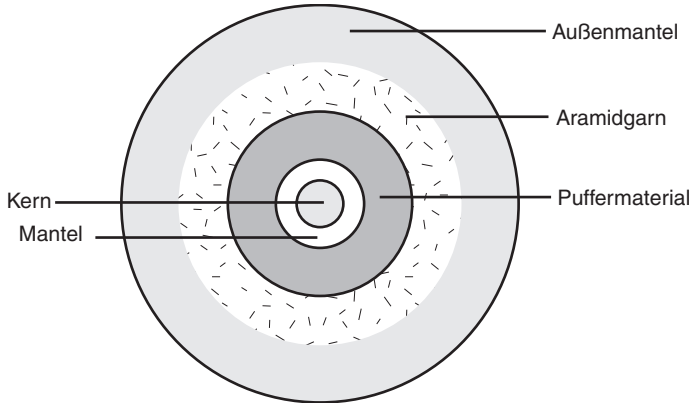


Abbildung 3.19: Querschnitt durch ein Glasfaserkabel

Der Kern ist das Lichtübertragungselement in der Mitte des Glasfaserkabels, d. h., das gesamte Licht bewegt sich in diesem Kern fort. Der Kern ist in der Regel aus Glas gemacht, das aus einer Mischung von Kieselerde (Siliziumdioxid) und anderen Elementen besteht. Um den Kern herum befindet sich das Mantelglas, das ebenfalls aus Kieselerde besteht, aber einen geringeren Brechungsindex hat als der Kern. Lichtstrahlen, die durch den Glasfaserkern wandern, werden an der Grenzfläche von Kern und Mantel reflektiert, d. h., das Licht wird im Kern gehalten, während es sich in der Glasfaser fortpflanzt.

Um die Schirmung herum ist ein Puffermaterial angelegt, das Beschädigungen der Innenkomponenten verhindern soll. Hierbei handelt es sich meist um Kunststoff.

Das Verstärkungsmaterial umgibt das Puffermaterial und soll verhindern, dass es bei der Verlegung zu stark gedehnt wird. Hier findet in erster Linie Kevlar Verwendung, ein Material, das auch zur Fertigung kugelsicherer Westen benutzt wird. Das letzte Element – der Außenmantel – umgibt das

Kabel und schützt die Glasfaser vor Abnutzung und vor Lösungs-, Reinigungs- und anderen aggressiven Mitteln. Die Zusammensetzung des Außenmantels hängt vom Einsatzzweck des Kabels ab.

Das Licht, das zur Datenübertragung gedacht ist, kann nicht in einem beliebigen Winkel in den Kern des Glasfaserkabels eintreten; dieser Winkel muss sich vielmehr innerhalb der numerischen Apertur der Glasfaser befinden. Ähnlich gilt, dass, wenn die Lichtstrahlen einmal in den Kern eingetreten sind, es nur eine begrenzte Anzahl an Pfaden gibt, in denen sich der Strahl durch die Faser fortpflanzen kann. Diese optischen Pfade heißen Moden. Wenn der Durchmesser eines Glasfaserkerns groß genug ist, sodass viele Pfade existieren, dann spricht man von einer Multimode-Glasfaser (»Mehrmodenglasfaser«). Singlemode-Glasfasern (»Einmodenglasfaser«) hingegen haben einen wesentlich kleineren Kern, der dem Licht nur einen einzigen optischen Pfad in der Glasfaser bietet. Abbildung 3.20 zeigt die Unterschiede zwischen Multimode- und Singlemode-Fasern.

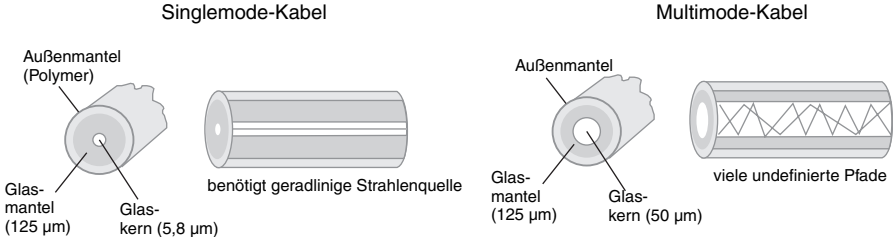


Abbildung 3.20: Singlemode versus Multimode

Tabelle 3.2 vergleicht die Eigenschaften von Singlemode- und Multimode-Glasfasern.

Tabelle 3.2: Eigenschaften von Singlemode- und Multimode-Glasfasern

	Singlemode-Glasfaser	**Multimode-Glasfaser**
Kern	kleiner Kern (≤ 10 µm)	größerer Kern als bei der Singlemode-Faser (≤50 bzw. 62,5 µm)
Dispersion	geringe Dispersion	größere Dispersion (d. h. auch Verluste in der Signalqualität)
Reichweiten	geeignet für sehr lange Strecken (≤ 100 km)	geeignet für kürzere Strecken (≤ 2 km)
Lichtquelle, Einsatzzweck	verwendet Laser als Lichtquelle, wird oft in Campus-Backbones zur Überbrückung von Strecken von mehreren tausend Metern und/oder sehr hohe Datenraten benutzt	verwendet LED als Lichtquelle, wird oft in LANs zur Überbrückung von Strecken von mehreren hundert Metern innerhalb eines Campus-Netzwerks benutzt

In den nächsten beiden Abschnitten werden wir die beiden Glasfasertypen genauer kennen lernen.

Multimode-Glasfaser

Multimode-Glasfasern bieten mehrere Moden (optische Pfade), in denen sich das Licht im Glasfaserkern ausbreiten kann (wohingegen Singlemode-Fasern nur eine Mode enthalten). Je nach Eintrittswinkel kann das Licht in den Moden während der Übertragung unterschiedliche Strecken zurücklegen, d. h., sie treffen am Ziel (der Empfängerseite des Kabels) zu leicht unterschiedlichen Zeitpunkten ein. Dieses Phänomen bezeichnet man als modale Dispersion. Multimode-Glasfaser basiert auf einem Glastyp namens Gradientenfaser, der zur Außenkante des Kerns hin einen niedrigeren Brechungsindex aufweist. Die Gradientenfaser sorgt dafür, dass das Licht umso langsamer wird, je weiter innen es im Kern übertragen wird, während Lichtstrahlen, die sich durch die äußeren Kernbereiche fortpflanzen, schneller sind. Hierdurch wird sichergestellt, dass alle Lichtmoden das Ende des Kabels weitgehend gleichzeitig erreichen. Man verwendet eine solche Struktur, weil ein Lichtstrahl, der direkt in der Mitte des Kerns übertragen wird, eine weniger weite Entfernung zurücklegen muss als ein anderer Strahl, der in der Glasfaser vielfach reflektiert wird. Alle Strahlen sollen zur selben Zeit am Ende der Faser eintreffen; nur dann erkennt der Empfänger einen starken Lichtblitz statt eines längeren Lichtimpulses mit geringer Helligkeit.

Ein standardgemäßes Multimode-Glasfaserkabel – der häufigste in LANs eingesetzte Glasfaserkabeltyp – basiert auf einer Glasfaser, die einen Kern mit 62,5 oder 50 µm[1] und eine Schirmung mit 125 µm Durchmesser aufweist (deswegen bezeichnet man diese Kabel auch als 62,5/125-µm- bzw. 50/125-µm-Kabel). Da der Durchmesser der Schirmung wesentlich größer ist als die Wellenlänge des zu übertragenden Lichts, wird dieses bei der Bewegung innerhalb des Kerns oft reflektiert. In Nordamerika setzt man in der Regel einen Kern-/Manteldurchmesser von 62,5/125 µm ein. In Europa dagegen ist die 50/125-µm-Variante mit einem bessere Bandbreitenlängenprodukt verbreiteter, was sich bei Gigabit- und 10-Gigabit-Netzwerken in deutlich größeren Kabellängen auswirkt.

Als Lichtquellen kommen bei Multimode-Fasern normalerweise Infrarot-LEDs oder VCSELs (Vertical Cavity Surface Emitting Laser, oberflächenemittierende Halbleiterlaser) zum Einsatz. LEDs sind in der Herstellung etwas preiswerter und aus sicherheitstechnischer Sicht einfacher in der Handhabung, allerdings ist die Reichweite nicht so hoch wie bei den Lasern. Glasfaserkabel vom Typ 62,5/125 µm können Entfernungen von bis zu

1. 1 µm (Mikrometer) ist ein Millionstel Meter.

2.000 Metern überbrücken. Derartige Kabel werden vorzugsweise in LANs (und dort auch für die Backbone-Verkabelung) eingesetzt.

Singlemode-Glasfaser

ACHTUNG

Beachten Sie, dass das Laserlicht, das in Verbindung mit Singlemode-Glasfasern benutzt wird, eine größere Wellenlänge hat, die in den Bereich des nichtsichtbaren Lichts fällt. Das Licht ist so stark, dass es schwerwiegende Augenschäden hervorrufen kann. Sehen Sie niemals in das Ende eines Glasfaserkabels, dessen anderes Ende an ein Gerät angeschlossen ist. Blicken Sie auch niemals in den Sendeport einer Netzwerkkarte, eines Switchs oder eines Routers (es gibt dort sowieso nichts zu sehen). Denken Sie immer daran, die entsprechenden Schutzkappen auf die Enden der Glasfaserkabel bzw. in die jeweiligen Ports der Switches und Router zu setzen. Hier ist allergrößte Vorsicht geboten!

Singlemode-Glasfasern enthalten nur eine Mode zur Ausbreitung des Lichts im Kern. Hier ist der Kerndurchmesser wesentlich geringer als bei Multimode-Fasern: nur etwa 8 bis 10 µm. Die gängigsten Kabel haben einen Durchmesser von 9 µm. Die Angabe »*9/125*« auf dem Außenmantel eines Singlemode-Kabels besagt, dass der Kern einen Durchmesser von 9 µm und der Mantel einen Durchmesser von 125 µm hat.

Der Kerndurchmesser einer Singlemode-Faser lässt dem Licht nur sehr wenig Raum zur Dispersion. Ferner wird als Lichtquelle ein stark fokussierter Infrarotlaser verwendet. Der von ihm erzeugte Lichtstrahl tritt in einem Winkel von 90° in den Kern ein. Aufgrund dieser Tatsache werden die zur Datenübermittlung verwendeten Lichtstrahlen geradlinig durch die Mitte des Kerns übertragen (Abbildung 3.21). Dieses Verhalten erhöht sowohl die Übertragungsgeschwindigkeit als auch die maximale Übertragungsstrecke beträchtlich.

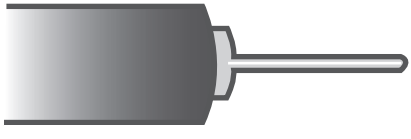


Abbildung 3.21: Singlemode-Glasfaser

Aufgrund ihres Aufbaus bietet die Singlemode-Faser höhere Datenraten (d. h. eine höhere Bandbreite) und größere Reichweiten als die Multimode-Faser. Singlemode-Kabel können LAN-Daten über bis zu 100 Kilometer übertragen, während die maximale Streckendistanz bei Multimode-Kabeln nur etwa 2.000 Meter beträgt. Allerdings sind Laser und Singlemode-Fasern wesentlich teurer als LEDs und Multimode-Kabel. Aufgrund dieser Eigenschaften werden Singlemode-Kabel häufig in WANs eingesetzt oder verwendet, um verschiedene Standorte miteinander zu vernetzen.

Abbildung 3.22 zeigt die Größenverhältnisse für beide Glasfaserkabeltypen als Querschnitt. Der wesentlich kleinere und edlere Faserkern im Singlemode-Kabel ist zwar in der Herstellung teurer, aber Grundlage für die im Vergleich zur Multimode-Faser höhere Bandbreite und die größeren Reichweiten.

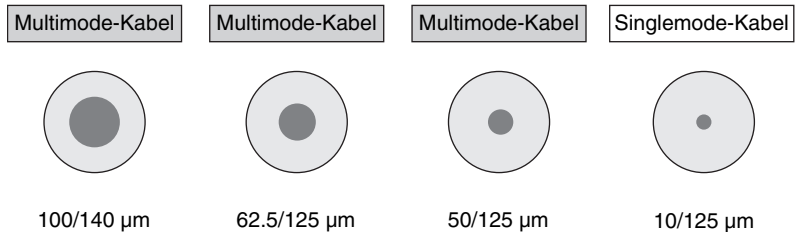


Abbildung 3.22: Singlemode- und Multimode-Fasern

Die folgende Übersicht fasst die Eigenschaften von Glasfaserkabeln zusammen:

- **Geschwindigkeit und Durchsatz:** Mehr als 10 Gbit/s.
- **Durchschnittskosten pro Knoten:** hoch
- **Abmessungen von Medien und Steckverbindern:** gering
- **maximale Kabellänge:** 100 km bei Singlemode-Kabeln, 2 km bei Multimode-Kabeln

Exkurs: Bauformen von Glasfaserkabeln

Wie Abbildung 3.23 zeigt, unterscheidet man zwei Ausführungen von Glasfaserkabeln:

- Hohlader (mit Sonderform Bündelader)
- Vollader (auch als »Festader« bezeichnet)
- Kompaktader

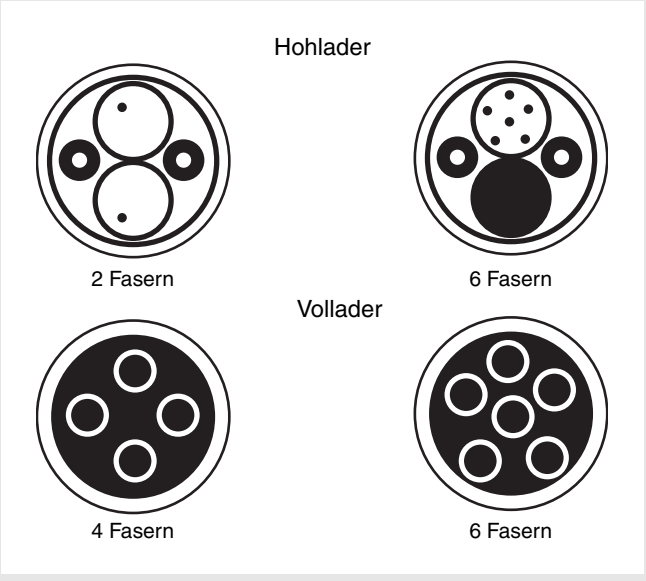


Abbildung 3.23: Hohlader- und Volladerkabel

Bei Volladerkabeln hat das flexible Puffermaterial, das den Mantel umgibt, direkten Kontakt mit diesem Mantel. Die Vollader hat dadurch einen kleineren zulässigen Biegeradius als die Hohlader. Bei der Hohlader ist der Innendurchmesser erheblich größer als der Faserdurchmesser, wodurch diese Faser zum Teil auch von den auf das Kabel wirkenden Kräften entkoppelt wird. Die Kompaktader ist ein Kompromiss zwischen Vollader und Hohlader. Der wesentliche praktische Unterschied zwischen den Ausführungen besteht in der Anwendung: Bündeladern werden in erster Linie für Außeninstallationen eingesetzt, während Volladern im Gebäudeinnern verwendet werden. Die meisten in LANs verwendeten Glasfaserkabel sind Multimode-Volladerkabel.

3.2.7 Weitere optische Komponenten

Die meisten Daten in einem LAN werden als elektrische Signale übertragen. Glasfaserverbindungen hingegen verwenden zur Datenübertragung Licht. Es werden also Bauelemente benötigt, um die Elektrizität in Licht und am Ende der Verbindung zurück in Elektrizität zu konvertieren. Für dieses Szenario benötigen wir also zwei Komponenten: einen Transmitter und einen Receiver.

Neben Transmittern und Receivern werden in diesem Abschnitt auch verschiedene Formate von Steckern für Glasfaserkabel und andere Geräte beschrieben, die in der optischen Netzwerktechnologie eingesetzt werden.

Transmitter

Der Transmitter erhält die zu übertragenden Daten in Form elektrischer Signale von Switches oder Routern. Er wandelt diese Signale dann in äquivalente Lichtimpulse um. Für die Codierung und Übertragung der Daten über das Kabel kommen zwei Lichtquellen zum Einsatz:

- **LEDs.** Eine LED (Light-Emitting Diode, Leuchtdiode) erzeugt Infrarotlicht mit einer Wellenlänge von 850 oder 1.310 nm und kommt in Multimode-Fasern etwa in LANs zum Einsatz. Zur Fokussierung des Infrarotlichts am Ende der Faser werden Linsen eingesetzt. LEDs sind aus sicherheitstechnischer Sicht weitgehend unbedenklich.
- **Laser.** Ein Laser ist eine Lichtquelle, die einen dünnen Strahl intensiven Infrarotlichts mit eine Wellenlänge von 1.310 oder 1.550 nm erzeugt. Laser werden mit Singlemode-Fasern eingesetzt, die zur Überbrückung längerer Strecken in WANs oder Campus-Backbones benötigt werden. Im Umgang mit Lasern ist größte Sorgfalt walten zu lassen, um Augenverletzungen zu vermeiden.

Beide Lichtquellen können sehr schnell aktiviert bzw. deaktiviert werden, d. h., Nullen und Einsen können mit hoher Datenrate gesendet werden.

Receiver

Am anderen Ende des Glasfaserkabels befindet sich der Receiver. Er funktioniert prinzipiell wie die Fotozelle eines solarbetriebenen Taschenrechners. Wenn das Licht auf den Receiver auftrifft, wird Elektrizität erzeugt. Erste Aufgabe des Receivers ist es, Lichtimpulse zu erkennen, die ihn aus der Glasfaser kommend erreichen. Wird ein solcher Impuls erkannt, dann konvertiert der Receiver ihn zurück in das elektrische Signal, das am entgegengesetzten Ende des Kabels in den Transmitter eingespeist wurde. Nun steht das Signal wieder in Form von Spannungsänderungen zur Verfügung und kann über Kupferleitungen in jedes beliebige Empfängergerät übertragen werden: Computer, Switches oder Router.

Die Halbleitergeräte, die normalerweise als Receiver für Glasfaserverbindungen verwendet werden, heißen PIN-Fotodioden (*p-intrinsic-n*-Dioden). PIN-Fotodioden sind so konstruiert, dass sie nur dann reagieren, wenn Licht mit einer bestimmten Wellenlänge auf sie fällt – nämlich der Wellenlänge des Lichts, das beim Transmitter am anderen Ende des Glasfaserkabels eingespeist wurde (850, 1.310 oder 1.550 nm). Wenn ein Lichtimpuls der passenden Wellenlänge auf die PIN-Fotodiode fällt, erzeugt diese sehr schnell eine elektrische Spannung. Trifft kein Licht auf die Diode, wird die Spannungserzeugung sofort eingestellt. Dieser Vorgang erzeugt die Spannungsänderungen, die in Kupferleitungen die Nullen und Einsen repräsentieren.

Steckverbinder

Steckverbinder sind an den Enden der Glasfaser befestigt, um die Kabel mit den Transmitter- und Receiveranschlüssen zu verbinden. Die gängigsten Steckertypen, die bei Multimode-Kabel zum Einsatz kommen, sind SC-Stecker (Subscriber Connector, Abbildung 3.24), bei Singlemode-Kabeln verwendet man meist ST-Stecker (Straight Tip, Abbildung 3.25). Bei diesen beiden Steckverbindertypen gibt es jeweils einen Stecker für jede Faser. Neuere Stecker fassen die Sende- und Empfangsfasern aus Gründen der Platzersparnis in einem modularen Stecker zusammen, der von den Abmessungen her dem RJ45-Stecker ähnelt.

Abbildung 3.24: SC-Stecker

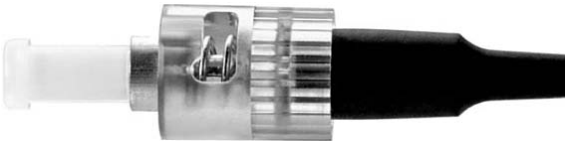


Abbildung 3.25: ST-Stecker

Optische Verstärker und Glasfaserverteilerfelder

Neben Transmittern, Receivern, Steckern und Glasfasern, die für den Betrieb eines optischen Netzwerks notwendig sind, findet man hin und wieder auch andere Geräte in einem Glasfasernetz.

Optische Verstärker gehören von der Funktion her zu den Repeatern, denn sie empfangen abgeschwächte Lichtimpulse und geben diese in ursprünglicher Form, Stärke und Taktung wieder aus. Das so wiederhergestellte Signal kann dann seine Reise zum Empfänger am entfernten Ende des Glasfaserkabels fortsetzen.

Glasfaserverteilerfelder (Abbildung 3.26) ähneln den Verteilerfeldern, die in kupferbasierten Netzwerken eingesetzt werden. Diese Verteilerfelder erhöhen die Flexibilität eines optischen Netzwerks, denn sie ermöglichen ein schnelles Ändern vorhandener Verbindungen zwischen Geräten wie Switches oder Routern über die vorhandenen Glasfaserstrecken (Kabelverbindungen).

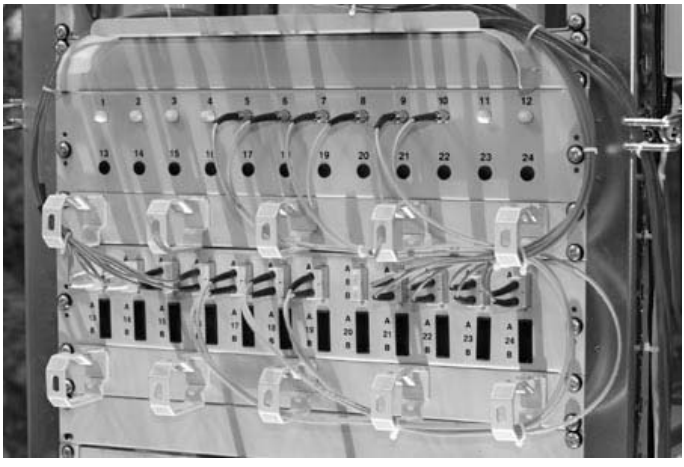


Abbildung 3.26: Glasfaserverteilerfeld

3.2.8 Signale und Störungen bei Glasfasern

Externe Störungsquellen, die Probleme in Zusammenhang mit kupferbasierten Medien verursachen können, haben auf Glasfaserkabel keinen Einfluss. Ursache hierfür ist, dass externes Licht ausschließlich am Transmitter-seitigen Kabelende in die Glasfaser eindringen kann. Die Mantelung ist von einem Puffer und einem Außenmantel umgeben, die verhindern, dass Licht in das Kabel eindringen oder es verlassen kann.

Hinzu kommt, dass die Übertragung von Licht in einem Kabel keine Interferenzen erzeugt, welche die Übertragung in einer anderen Faser stören, d. h., es gibt bei Glasfasern anders als bei Kupfermedien kein Übersprechen. Die Qualität von Glasfaserverbindungen ist tatsächlich so gut, dass neuere Standards für Gigabit- und 10-Gigabit-Ethernet Übertragungsentfernungen vorsehen, die weit höher liegen als die zwei Kilometer umfassende Reichweite des ursprünglichen Ethernet (mehr zu Ethernet erfahren Sie in Kapitel 7, »Ethernet-Technologien«, und Kapitel 8, »Ethernet-Switching«). Die Glasfasertechnologie erlaubt die Verwendung des Ethernet-Protokolls in MANs (Metropolitan-Area Networks, Stadtbereichsnetze) und WANs.

Glasfaserkabel sind zwar das beste aller Übertragungsmedien, wenn es darum geht, große Datenmengen über lange Strecken zu übertragen. Wenn das Licht sich in der Faser fortbewegt, geht immer ein wenig Lichtenergie verloren. Je weiter das Licht übertragen wird, desto mehr verliert es an Stärke. Diese Dämpfung des Signals wird von mehreren Faktoren verursacht, die durch die Natur der Glasfaser selbst gegeben sind. Der wichtigste

Faktor ist die Streuung. Die Lichtstreuung in einer Glasfaser hat ihre Ursache in einer mikroskopisch kleinen Inhomogenität (Verformung) in der Faser, die einen Teil der Lichtenergie reflektiert und streut (Abbildung 3.27).

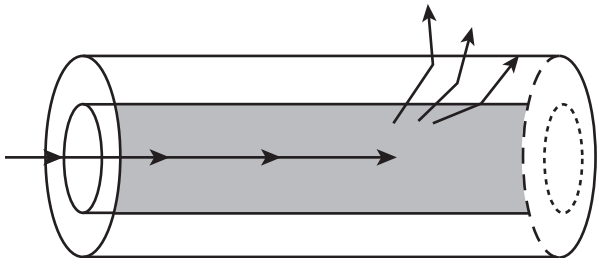


Abbildung 3.27: Streuung

Ein weiterer Grund für einen Verlust an Lichtenergie ist die Absorption. Wenn ein Lichtstrahl auf bestimmte chemische Unreinheiten in der Faser trifft, dann absorbieren diese einen Teil der Lichtenergie. Diese Lichtenergie wird in eine kleine Menge Wärmeenergie umgewandelt. Absorption macht das Lichtsignal etwas dunkler.

Auch Fertigungsfehler oder raue Stellen an der Grenzfläche zwischen Kern und Schirmung können die Lichtdämpfung fördern. Energie des Lichts geht teilweise infolge einer nicht einwandfreien internen Totalreflexion an rauen Stellen verloren. Winzig kleine Durchmesser- oder Symmetrieungenauigkeiten in der Faser verringern die interne Totalreflexion, weswegen ein Teil der Lichtenergie vom Mantel absorbiert wird.

Auch die Dispersion eines Lichtimpulses begrenzt die Reichweite einer Faser. Unter der Dispersion versteht man hier das Spreizen eines Impulses während der Übertragung, wie es in Abbildung 3.28 dargestellt ist.

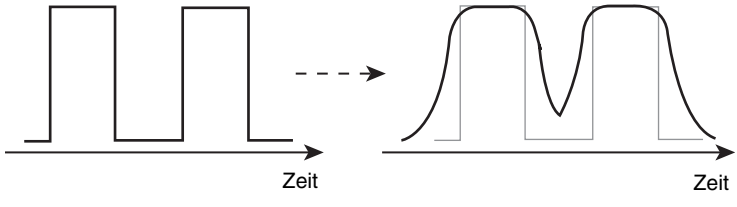


Abbildung 3.28: Dispersion

Multimode-Gradientenfaser ist so aufgebaut, dass sie unterschiedliche Entfernungen ausgleicht, die der Lichtstrahl in den verschiedenen Modi innerhalb des Kerns zurücklegt. Bei Singlemode-Fasern tritt dieses Problem naturgemäß nicht auf. Die chromatische Dispersion jedoch ist ein Phänomen, das bei Multimode- und Singlemode-Fasern gleichermaßen auftritt. Es gibt näm-

lich einige Wellenlängen, bei denen das Licht sich mit einer etwas anderen Geschwindigkeit im Glas ausbreitet als bei anderen Wellenlängen. Diese Abweichung führt zur chromatischen Dispersion. Dies ist auch der Grund, warum ein Prisma die Lichtwellenlängen trennen kann.

Im Idealfall sendet die LED bzw. der Laser nur Licht mit ein und derselben Frequenz aus; dann tritt chromatische Dispersion nicht auf. Leider aber erzeugen Laser und insbesondere LEDs meist einen ganzen Bereich von Wellenlängen, d. h., die chromatische Dispersion begrenzt die Entfernung, über die Daten in einem Glasfaserkabel übertragen werden können. Wenn Sie ein Signal über eine zu große Strecke senden wollen, kommt von dem hellen Lichtimpuls, den Sie gesendet haben, auf der Receiverseite nur noch ein schwaches, gespreiztes und ungetaktetes Signal an, und der Receiver kann zwischen Nullen und Einsen nicht mehr unterscheiden.

3.2.9 Glasfaserkabel installieren, betreiben und testen

Ein Hauptgrund für übermäßige Dämpfung in Glasfaserkabeln ist die unsachgemäße Installation. Wenn die Faser zu sehr gedehnt oder zu stark gebogen wird, treten winzige Risse im Kern auf, die zu einer Streuung des Lichts führen. Wird das Kabel zu eng um die Ecke gelegt, dann kann sich der Einfallswinkel des Lichtstrahls auf die Grenzfläche zwischen Kern und Schirmung so ändern, dass er unterhalb des kritischen Winkels für die interne Totalreflexion liegt. Dies führt dazu, dass das Licht sich teilweise am Mantel bricht und verloren geht.

Man unterscheidet zwei Arten des Verbiegens:

- **Makrokrümmung.** Eine Makrokrümmung ist eine Verformung, die man sehen kann. Wenn man ein Glasfaserkabel verbiegt, dann kann dies dazu führen, dass einige Lichtstrahlen den kritischen Winkel überschreiten, d. h., das Licht »versickert« im Mantel. Von dort aus gelangt es nur schwer zurück in den Kern, umso leichter allerdings in das Puffermaterial (Abbildung 3.29).
- **Mikrokrümmung.** Eine Mikrokrümmung hat die gleichen Folgen wie eine Makrokrümmung: Sie führt dazu, dass das Licht den kritischen Winkel überschreitet und aus dem Kern gelangt. Mikrokrümmungen sind allerdings mikroskopisch klein und für das bloße Auge nicht sichtbar.

  Eine Mikrokrümmung kann auch durch extreme Temperaturschwankungen im installierten Kabel entstehen, wenn die verschiedenen Materialien in der Kabelstruktur sich in unterschiedlichem Maße ausbreiten bzw. zusammenziehen. Hierdurch kann die Glasfaser gepresst oder gedehnt werden, was wiederum eine Mikrokrümmung zur Folge hat.

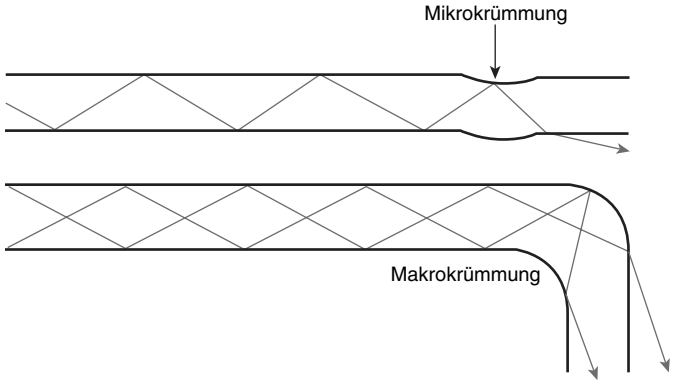


Abbildung 3.29: Makro- und Mikrokrümmung

Um zu verhindern, dass Glasfasern zu stark gebogen werden, können die Kabel durch ein Installationsrohr oder einen Kabelkanal verlegt werden. Ein Installationsrohr ist wesentlich robuster als das Glasfaserkabel und kann nicht so stark durchgebogen werden, dass das in ihm liegende Glasfaserkabel überbogen wird. Das Führungsrohr schützt also das Glasfaserkabel, erleichtert die Verlegung und stellt sicher, dass der Biegeradius des Kabels nicht zu klein wird.

Wenn die Glasfaser verlegt ist, müssen ihre Enden mit speziellen Werkzeugen (so genannten Cleavern) geschnitten und akkurat poliert werden, damit sichergestellt ist, dass sie glatt sind. Abbildung 3.30 zeigt, welche Probleme in Verbindung mit unsachgemäß behandelten Glasfaserenden auftreten können, und Abbildung 3.31 stellt geeignete Poliertechniken für die Glasfaserenden dar.

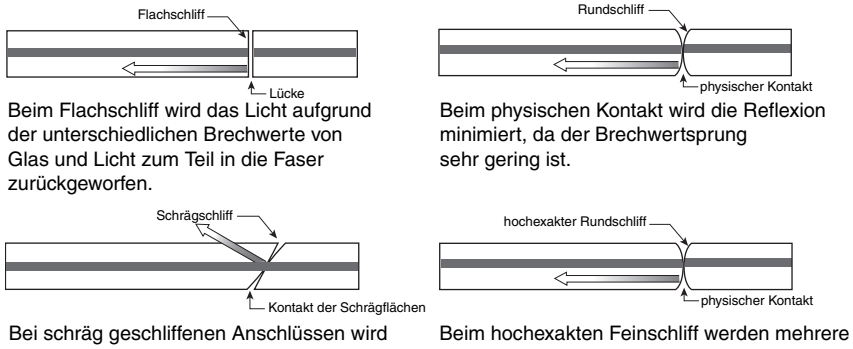


Abbildung 3.30: Abschlussformen von Glasfaserenden

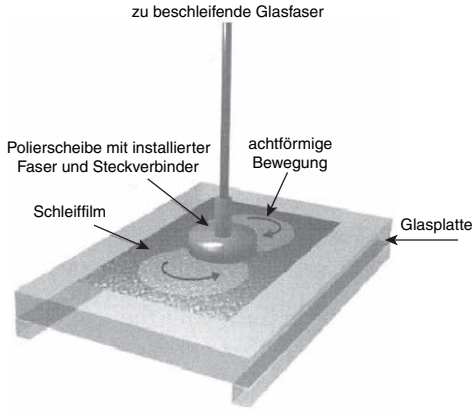


Abbildung 3.31: Poliertechnik für das Glasfaserende

Man verwendet ein Mikroskop oder ein Testinstrument mit eingebauter Vergrößerungsfunktion, um zu überprüfen, ob das Ende der Glasfaser korrekt poliert und geformt ist. Dann wird der Stecker vorsichtig am Kabelende befestigt. Faktoren wie unsachgemäß befestigte Stecker, schlechte Verbindungen oder das Aneinanderfügen zweier Kabel mit unterschiedlichen Kerndurchmessern führen zu einer drastischen Verringerung der Lichtstärke des übertragenen Strahls. Abbildung 3.32 zeigt die Folgen des Aneinanderfügens einer 62,5-µm-Glasfaser an eine 50-µm-Glasfaser.

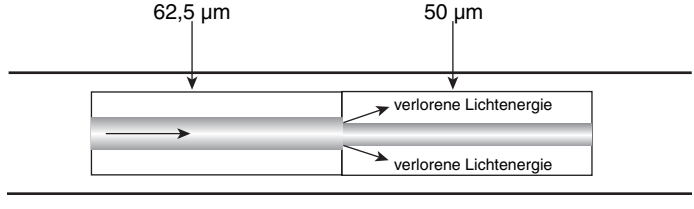


Abbildung 3.32: Aneinanderfügen ungleicher Glasfasertypen

Wenn die Glasfaserkabel und die Steckverbinder einmal installiert sind, muss auf peinliche Sauberkeit an den Kabelenden und den Steckern geachtet werden. Die Kabelenden sollten immer mit den zugehörigen Schutzkappen versehen werden. Werden diese Kappen vor dem Anschluss des Kabels an den Port eines Switchs oder Routers abgenommen, dann müssen die Kabelenden gereinigt werde. Verwenden Sie zu diesem Zweck fusselfreies Reinigungstuch für Kameralinsen, das zuvor mit reinem Isopropylalkohol angefeuchtet wurde. Auch sollten die Glasfaseranschlüsse an Switch und Router, wenn sie nicht in Verwendung sind, mit den Schutzkappen geschlossen und vor Herstellung einer Verbindung ebenfalls mit Reinigungstuch und

Isopropylalkohol gereinigt werden. Verschmutzte Kabelenden können den Betrag des Lichts, der beim Empfänger ankommt, erheblich reduzieren.

All diese Faktoren – Streuung, Absorption, Dispersion, unsachgemäße Installation und verschmutzte Kabelenden – führen zu einer Verringerung der Lichtsignalstärke und werden deswegen als Störeinflüsse bei optischen Verbindungen betrachtet. Bevor Sie ein Glasfaserkabel einsetzen, müssen Sie es testen, um sicherzustellen, dass das Licht tatsächlich mit ausreichender Stärke beim Empfänger ankommt und die Nullen und Einsen so korrekt erkannt werden.

Wenn eine Glasfaserverbindung geplant wird, muss die Größe der tolerablen Signaldämpfung berechnet werden. Diese Toleranz bezeichnet man als Dämpfungsbudget (auch OLB, vom engl. *Optical Loss Budget*). Man kann dies mit dem finanziellen Budget vergleichen, das Ihnen monatlich zur Verfügung steht: Wenn alle Ausgaben (in diesem Fall: Dämpfungen) abgezogen sind, muss immer noch genügend Geld übrig sein, damit Sie über den Monat kommen.

Die Einheit, in weclher der Signalleistungsverlust gemessen wird, ist das Dezibel (dB). Hiermit wird der Leistungsprozentsatz des gesendeten Lichts ausgedrückt, der tatsächlich beim Empfänger ankommt.

Glasfaserkabel vor dem Einsatz zu testen und zu messen ist extrem wichtig. Die Testergebnisse müssen zudem schriftlich festgehalten und archiviert werden. Für die Prüfung kommen mehrere spezielle Testgeräte zum Einsatz, deren zwei wichtigste das Messgerät für optische Verluste im Glasfaserkabel und der Glasfaserkabeltester (OTDR, vom engl. *Optical Time Domain Reflectometer*) sind. Diese beiden Messgeräte erlauben eine Prüfung der Glasfaserkabel, um sicherzustellen, dass das Kabel den entsprechenden TIA/EIA-Standards entspricht. Ferner können Sie hiermit auch überprüfen, ob die optischen Leistungsverluste nicht unter das Dämpfungsbudget fallen. OTDRs bieten häufig detaillierte Diagnoseinformationen über eine Glasfaserverbindung und können auch zur Fehlersuche herangezogen werden.

Lab

Siehe auch CNAP und [1] »Fiber Optic Purchase«.

3.3 Funknetze

Die verschiedenen Netzwerktechnologien, die wir weiter oben in diesem Kapitel erläutert haben, basieren durchweg auf physischer Konnektivität. Die Vorteile sind Geschwindigkeit, Zuverlässigkeit und – in einem gewissen

Maße – Komfort. Die Netzwerkanbindung erlaubt eine erhöhte Produktivität, denn sie ermöglicht die gemeinsame Nutzung von Druckern, Servern und Software. Allerdings setzen vernetzte Systeme voraus, dass die Workstations ortsfest bleiben, d. h., nur innerhalb der Medienreichweite (z. B. innerhalb eines Gebäudes) den Standort wechseln können.

Die Erfindung drahtloser Technologien beseitigte diese Beschränkungen und machte die Welt der Computer erst richtig mobil. Zwar bieten Funktechnologien derzeit weder die hohen Übertragungsraten noch die Sicherheit und die Betriebszuverlässigkeit kabelbasierter Netzwerke, aber diese Nachteile werden durch die gewonnene Flexibilität oft aufgewogen.

Wenn es um die Installation eines Netzwerks in einer vorhandenen Einrichtung geht, steht die Funktechnologie meist ganz oben auf der Wunschliste der Administratoren. Ein einfaches Funknetz kann nach Einschalten der Workstations innerhalb von Minuten betriebsbereit sein. Die Anbindung an das Internet erfolgt über eine Kabelverbindung (Router, Kabelmodem oder DSL-Modem) und einen Access-Point, der als Hub für die Funknetzknoten agiert. In einem Heimnetzwerk oder einem kleinen Firmennetz können diese Komponenten in einem einzigen Gerät zusammengefasst sein.

3.3.1 Drahtlose Kommunikation

Drahtlose Signale (Funksignale) sind elektromagnetische Wellen, die sich im Vakuum des Weltraums und in Medien wie etwa der Luft in unserer Atmosphäre ausbreiten. Aus diesem Grund werden für Funksignale keine Kabelmedien benötigt, weswegen die drahtlose Kommunikation in den letzten Jahren ein vielseitiges Mittel zum Aufbau eines Netzwerks wurde. Drahtlose Übertragungen können durch Verwendung von Hochfrequenzsignalen große Entfernungen überbrücken. Jedes Signal verwendet eine andere Frequenz, d. h., die Signale bleiben separat.

Drahtlose Technologien gibt es bereits seit vielen Jahren: Satellitenfernsehen, UKW- und MW-Radio, Mobiltelefone, Fernsteuerungseinrichtungen, Radarsysteme, Alarmanlagen, Wetterstationen, schnurlose Telefone und Scannerkassen sind Bestandteil des täglichen Lebens. Funktechnologien spielen heutzutage eine wesentliche Rolle in Wirtschaft und Gesellschaft.

Drahtlose Datenkommunikation

Das Funkspektrum ist der Teil des elektromagnetischen Spektrums, der zur Übertragung von Sprache, Video und Daten verwendet wird. Es liegt im Frequenzbereich zwischen 3 kHz und 300 GHz. In diesem Abschnitt wollen wir uns auf den Teil des Funkspektrums konzentrieren, den die drahtlose Datenübertragung benutzt.

Wie Abbildung 3.33 zeigt, gibt es eine ganze Reihe drahtloser Datenkommunikationstechnologien. All diese Technologien haben ihre Vor- und Nachteile:

- **Infrarotübertragung.** Sehr hohe Datenraten und niedrige Kosten, aber sehr geringe Reichweiten.
- **Schmalbandübertragung.** Niedrige Datenraten und mäßige Kosten bei begrenzter Reichweite. Es wird eine Lizenz benötigt.
- **Bandspreizung (Spread-Spectrum-Technologie).** Gemäßigte Kosten, hohe Datenraten. Auf Campusreichweite beschränkt. Cisco Aironet basiert auf der Bandspreizung.
- **Breitband-PCS (Personal Communications Service).** Niedrige Datenrate, überschaubare Kosten. Die Reichweite kann eine Stadt abdecken. (Ausnahme: Sprint-PCS-Systeme bieten internationale Reichweiten.)
- **Übertragung von Paketdaten (zellulare Daten und CDPD-Daten[1]).** Niedrige Datenraten, hohe Paketgebühren, nationale Reichweiten.
- **Satellitenkommunikation.** Niedrige Datenraten, hohe Kosten, nationale und internationale Reichweiten.

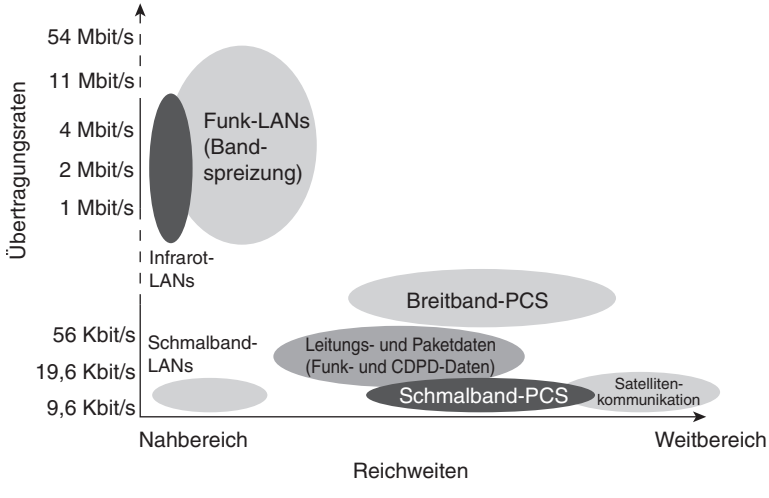


Abbildung 3.33: Drahtlose Datennetze

1. CDPD (Cellular Digital Packet Data) ist ein Verfahren zur gesicherten drahtlosen Datenkommunikation über analoge zellulare Sprachnetze.

Funksignale

Wenn ein Signal in einem Datenformat übertragen wird, müssen die folgenden drei Parameter in Betracht gezogen werden:

- **Geschwindigkeit.** Welche Datenrate kann erreicht werden?
- **Reichweite.** Wie weit dürfen die Stationen von WLANs (Wireless LANs, Funk-LANs) auseinander liegen, damit die maximale Datenrate erreicht wird?
- **Kapazität.** Wie viele Benutzer können im Netzwerk vorhanden sein, ohne dass die Datenrate beeinträchtigt wird?

All diese Parameter beziehen sich auf die Fähigkeit, über eine möglichst große Distanz ein möglichst deutliches Signal empfangen zu können. Eine Anhebung der Datenmenge setzt die Verwendung weiterer Frequenzspektren oder aber eine andere Methode der Kodierung der Daten im Funksignal voraus.

Der Wirkungsgrad der Funkübertragung wird durch die folgenden drei Faktoren beeinflusst (Abbildung 3.34):

- **Verwendeter Modulationstyp.** Komplexere Modulationsmethoden ermöglichen einen größeren Durchsatz.
- **Entfernung.** Je weiter das Signal übertragen werden muss, desto schwächer wird es.
- **Störeinflüsse.** Elektrische Störsignale und Hindernisse beeinträchtigen das Funksignal.

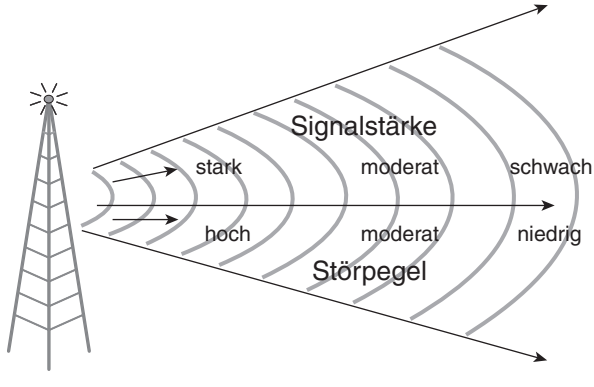


Abbildung 3.34: Faktoren, welche die Reichweite der Funkübertragung beeinträchtigen

Wir werden diese Faktoren in den folgenden Abschnitten näher untersuchen.

Modulation

Der Begriff Modulation beschreibt den Vorgang, bei dem die Amplitude, Frequenz oder Phase einer Funk- oder Lichtwelle geändert werden, um Informationen zu übertragen. Die Merkmale der Trägerwelle werden kontinuierlich von einer anderen Wellenform geändert: durch den Modulator. Die Modulation integriert also zum Zweck der Datenübertragung in einem Netzwerk ein Datensignal (Text, Sprache usw.) in einen Träger.

Nachfolgend aufgelistet sind die gängigsten Methoden zur Modulation (Abbildung 3.35):

- **AM (Amplitudenmodulation).** Die Amplitude (Auslenkung) einer Welle wird verändert.
- **FM (Frequenzmodulation).** Die Frequenz einer Welle wird verändert.
- **PM (Phasenmodulation).** Die Phase (Polarität) einer Welle wird verändert.

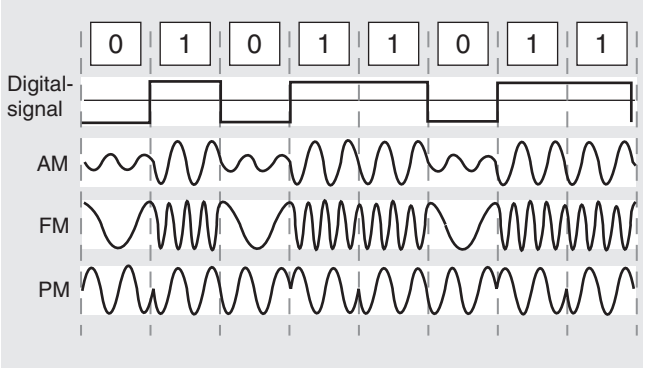


Abbildung 3.35: Modulation

Wirkung der Entfernung auf ein Signal

Wenn ein Empfänger sich zunehmend von einem Sender wegbewegt, wird das Signal immer schwächer, und der Unterschied zwischen Signal und Störungen wird immer geringer. Schließlich kann das Signal nicht mehr vom Störsignal unterschieden werden: Die Kommunikation reißt ab. Der Umfang der Kompression (d. h. die Modulationsmethode), mit der das Signal gesendet wird, bestimmt, wie stark das Signal sein muss, um es aus dem Störpegel »heraushören« zu können. Je komplexer das Modulationssystem und je höher die Datenraten, desto größer ist auch die Anfälligkeit gegen Störungen. In einem solchen Fall muss die Entfernung verringert werden.

Anmerkung

Um fehlerfrei empfangen zu können, müssen komplexe Modulationsmethoden ein optimales Verhältnis des Signals zu den Störpegeln aufweisen (d. h. ein möglichst großes Signal bei möglichst kleinem Störsignal; man bezeichnet dies auch als Störabstand). Wenn Störungen in einem Kanal vorhanden sind, wird die Leitungsgeschwindigkeit verringert. Bandbreite, Störsignal, erreichbare Datenrate und Entfernung hängen also direkt miteinander zusammen (Theorem von Claude Shannon).

Wirkung der Störungen auf ein Signal

Elektronische Störsignale und Hindernisse wirken sich negativ auf den Wirkungsgrad der Funkübertragung aus. Eine exakte maximale Übertragungsentfernung für WLAN-Produkte kann nicht angegeben werden, ohne das Produkt direkt am gewünschten Standort zu testen. Beispielsweise können Mauern, wenn sich in ihnen Metallarmierungen befinden (z. B. Stahlbetonwände), die Reichweite von Funksignalen erheblich verringern.

Funkfrequenzbänder

Die meisten Funkfrequenzbänder werden durch staatliche Einrichtungen lizenziert. In den Vereinigten Staaten ist etwa die FCC (Federal Communications Commission) dafür zuständig, in Deutschland sichert die Regulierungsbehörde für Telekommunikation und Post (Reg TP) eine effiziente und störungsfreie Nutzung von Frequenzen. Um über diese Frequenzen senden zu können, benötigen Sie eine kostenpflichtige Lizenz.

Unlizenzierte Frequenzbänder sind leichter zu benutzen und kosten mittel- und langfristig weniger, weil hierfür keine Lizenzgebühren zu entrichten sind. Es existieren drei unlizenzierte Bänder (Abbildung 3.36):

- **900 MHz.** Dieses Band ist für Funktelefone und schnurlose Telefone vorgesehen.
- **2,4 GHz.** Der IEEE-Standard 802.11b – der meistverbreitete Funkstandard – arbeitet im unlizenzierten 2,4-GHz-Band und liefert eine Datenrate von maximal 11 Mbit/s. Die Weiterentwicklung 802.11g erreicht in diesem Frequenzband eine Datenrate von 54 Mbit/s.
- **5 GHz.** Dieses Frequenzband wurde von der FCC kürzlich für die unlizenzierte Nutzung durch schnelle Datenkommunikationseinrichtungen freigegeben. Cisco setzt diese Frequenz bei neuen Produkten ein, z. B. den Geräten der Serie Cisco Aironet 1200, die sowohl das 2,4-GHz-Band nach 802.11b als auch das 5-GHz-Band nach 802.11a unterstützen. Der Standard 802.11a liefert eine Datenrate von maximal 54 Mbit/s, konnte

sich aber wegen der Inkompatibilität zu den verbreiteten Standards 802.11b und 802.11g bisher nicht durchsetzen.

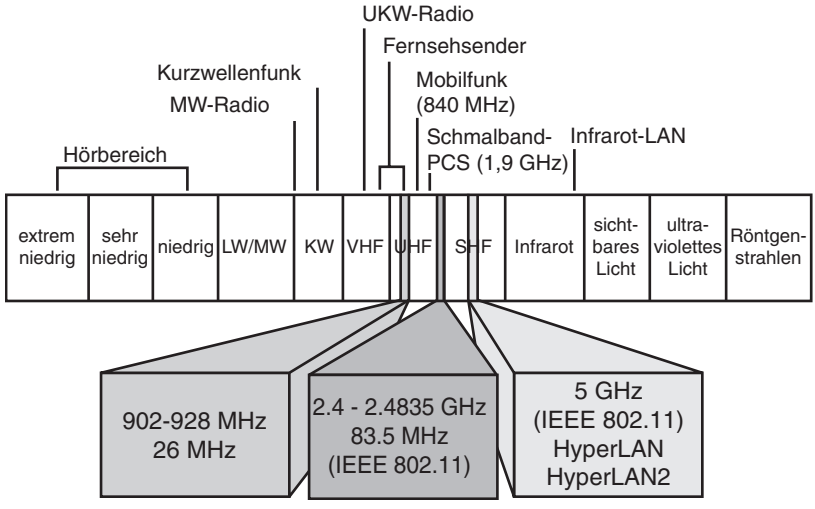


Abbildung 3.36: Unlizenzierte Frequenzbänder

Zwischen der Frequenz und der Datenmenge, die gesendet werden kann, besteht eine Beziehung. Das Konzept ähnelt dem einer Rohrleitung: Je größer die Bandbreite, desto mehr Frequenzen stehen zur Verfügung. Je breiter das Spektrum, desto höher die Rate der zu übertragenden Daten. Der Umfang des verfügbaren Spektrums bestimmt also die Datenrate.

Da im 900-MHz-Band Funktelefone und andere Endverbraucherprodukte arbeiten, ist dieses Frequenzband überfüllt, und Benutzer haben häufig Probleme mit Störungen oder keinen Netzzugriff. Der Vorteil des Bandes besteht darin, dass es (bei gleicher Antenne) eine größere Reichweite bietet als das 2,4-GHz-Band. Der Nachteil des 900-MHz-Bandes besteht in der geringen Datenrate von maximal 1 Mbit/s, bedingt durch den beschränkten Frequenzbereich.

Das 2,4-GHz-Band ist wesentlich breiter als das 900-MHz-Band und erlaubt so höhere Datenraten bei einer Reichweite von ca. 300 m (mit speziellen Antennen auch über 40 Kilometer). Die Geräte der Cisco Aironet 1100 und 1200 Wireless LAN-Serie haben einen Durchsatz von 11 bzw. 54 Mbit/s im 2,4-GH-Band.

Cisco hat auch die 5-GHz-Technologie implementiert und bietet für diesen weitgehend ungestörten Frequenzbereich Produkte an, da die größere Bandbreite einen höheren Datendurchsatz erlaubt. Der Cisco Aironet 5-GHz-WLAN-Adapter (54 Mbit/s) ist ein IEEE 802.11a-kompatibler CardBus-Adapter, der in den Bändern UNII-1 und UNII-2 operiert. Der Clientadapter

ergänzt den 802.11a-Access-Point der Aironet 1200-Serie. Der Nachteil des 5-GHz-Bandes allerdings ist seine eingeschränkte Reichweite: Innerhalb eines Gebäudes liegt sie bei gerade einmal 30 Metern, außerhalb bei über 70 Metern. Diese geringere Reichweite resultiert aus den ungünstigeren Ausbreitungsbedingungen bei 5 GHz. Außerdem dürfen diese Geräte in Europa nur mit einer Sendeleistung von 30 Milliwatt eingesetzt werden. So will man in diesem Frequenzband Störungen von Flugsicherung und Militär vermeiden.

Bandspreizung

So wie Ihr Autoradio mit UKW- und MW-Bändern arbeitet, verwenden auch andere Empfänger bestimmte Bänder, Frequenzen und Modulationstypen. Die Bandspreizung (auch bekannt unter der englischen Bezeichnung *Spread Spectrum*) ist eine Modulationsmethode, die in den Vierzigerjahren des vergangenen Jahrhunderts entwickelt wurde und ein Übertragungssignal über ein breites Band von Funkfrequenzen »ausbreitet«. Dieser Ansatz opfert Bandbreite, um einen guten Störabstand zu erhalten. Er ist für die Datenkommunikation ideal, weil er recht unempfindlich gegen Funkstörungen ist und verhältnismäßig wenige Interferenzen erzeugt.

Wie Abbildung 3.37 zeigt, ist die Bandspreizung ein System, bei dem das übertragene Signal über eine Frequenz verteilt wird, die wesentlich breiter ist als die zur Übermittlung des Signals benötigte Mindestbandbreite. Dieser Vorgehensweise liegt die Annahme zugrunde, dass in Kanälen mit Schmalbandinterferenzen eine Erhöhung der Bandbreite für das Übertragungssignal die Wahrscheinlichkeit erhöht, dass die empfangenen Informationen fehlerfrei sind.

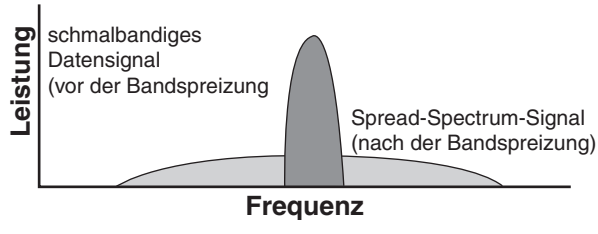


Abbildung 3.37: Bandspreizung

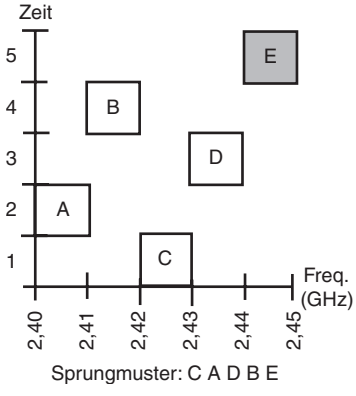
Anmerkung

Schmalbandige Interferenzen treten auf, wenn zwei Signale über die gleiche Frequenz innerhalb eines geografischen Bereichs gesendet werden. Der Begriff *Band* bezeichnet eine Gruppe von Frequenzen, d. h., ein Schmalband ist ein relativ kleiner Frequenzbereich. Schmalbandstörungen können bestimmte Kanäle oder Bandspreizungskomponenten beeinträchtigen.

FHSS und DSSS

Will man unlizenzierte Funkbänder verwenden, dann muss man die Bandspreizung einsetzen. FHSS und DSSS sind zwei Bandspreizungsmethoden, welche die Funkwellenenergie über das verfügbare Band verteilen. Als Modulationsmethoden haben sowohl FHSS (Frequency-Hopping Spread Spectrum, Frequenzsprungverfahren) und DSSS (Direct-Sequence Spread Spectrum, direkte Bandspreizung) ihre Vor- und Nachteile.

Bei der FHSS-Technologie springen die Übertragungen in einem Zufallsmuster von einer Frequenz zu einer anderen. Abbildung 3.38 zeigt ein Beispiel, in dem die Übertragung von C (2,42 GHz) über A (2,40 GHz), D (2,43 GHz) und B (2,41 GHz) zu E (2,44 GHz) springt. Diese Vorgehensweise ermöglicht ein »Umspringen« der Schmalbandinterferenzen, was ein deutliches Signal und eine höhere Übertragungszuverlässigkeit zur Folge hat. Allerdings ist die FHSS-Technologie recht langsam, und der Empfänger muss das gleiche Zufallsmuster zur Dekodierung benutzen.



Zeit	Frequenz (GHz)
1	2,42
2	2,40
3	2,43
4	2,41
5	2,44

Abbildung 3.38: FHSS-Technologie

Die DSSS-Technologie (Abbildung 3.39) ist zuverlässiger, weil jedes Bit (1 oder 0) durch eine Zeichenkette dargestellt wird, die man als Chipping-Sequenz bezeichnet. Sogar dann, wenn vierzig Prozent der Zeichenkette verloren gehen, lässt sich die ursprüngliche Übertragung wiederherstellen. Die DSSS-Technologie bietet damit einen hohen Datendurchsatz und größere Reichweiten.

Aufgrund der Beschränkung auf eine Datenrate von 2 Mbit/s empfiehlt sich FHSS nur für sehr spezielle Anwendungen, z. B. bestimmte Typen von Wasserfahrzeugen. Bei allen anderen drahtlosen LAN-Anwendungen ist DSSS sicher die bessere Wahl. Die 2003 veröffentlichte Weiterentwicklung des IEEE 802.11b zum Standard IEEE 802.11g bietet eine dem Ethernet ähnliche Datenrate von 54 Mbit/s über DSSS.

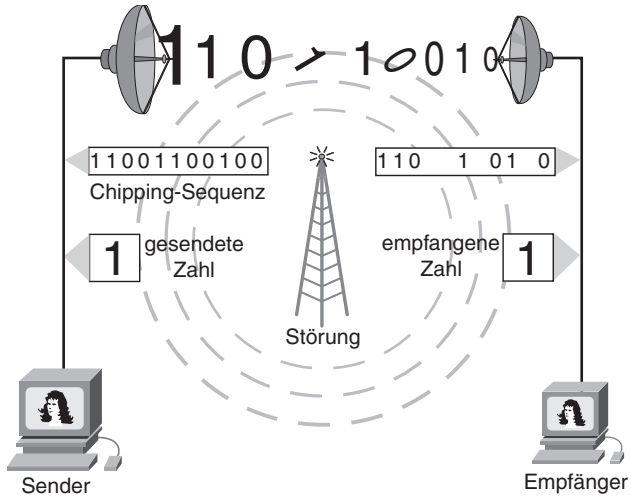


Abbildung 3.39: DSSS-Technologie

3.3.2 WLAN-Standards

Kenntnisse zu den Vorschriften und Standards, die für drahtlose Technologien gelten, sind dabei hilfreich sicherzustellen, dass eingerichtete Netzwerke interoperabel und miteinander kompatibel sind. Das IEEE, das wir bereits von den kabelbasierten Netzwerken her kennen, ist auch Herausgeber der wichtigsten Standards für Funknetze. Diese Standards wurden auf der Basis der Vorschriften entwickelt, die von der FCC formuliert wurden.

Die verwendeten Technologien innerhalb des ersten IEEE 802.11-Standards sind DSSS und FHSS. Beide Verfahren konnten in Funknetzeinrichtungen mit einer Rate zwischen 1 und 2 Mbit/s arbeiten. Der nächste genehmigte Standard war IEEE 802.11b, der die Übertragungskapazität auf 11 Mbit/s erhöhte.

IEEE 802.11b bezieht sich auf DSSS-Systeme, die mit Übertragungsraten von 1, 2, 5,5 oder 11 Mbit/s arbeiten. Alle 802.11b-Systeme sind dahingehend abwärtskompatibel, dass sie auch den ursprünglichen 802.11-Standard für DSSS-Systeme unterstützen, die nur mit 1 oder 2 Mbit/s übertragen. Diese Abwärtskompatibilität war wichtig, weil sie eine Aktualisierung des Funknetzes ermöglicht, ohne Netzwerkkarten oder Access-Points austauschen zu müssen.

IEEE 802.11b-Geräte erzielen den höheren Datendurchsatz durch Verwendung einer von 802.11 unterschiedlichen Kodiermethode, welche die Übertragung von mehr Daten innerhalb des gleichen Zeitraums unterstützt. Allerdings bieten die 802.11b-kompatiblen Geräte keinen Durchsatz von

10 Mbit/s, wie man ihn vom kabelgestützten Ethernet gewohnt ist, sondern arbeiten prinzipbedingt mit Nettoraten zwischen 2 und 5 Mbit/s.

Der Standard 802.11a bezieht sich auf WLAN-Geräte, die im 5-GHz-Übertragungsband arbeiten. Die Nutzung dieses Bandes verhindert eine Interoperabilität mit 802.11b-Geräten, da diese im 2,4-GHz-Band operieren. 802.11a unterstützt einen Datendurchsatz von 54 Mbit/s und erreicht dank einer proprietären Technologie namens Ratenverdopplung sogar 108 Mbit/s. In realen Netzwerken liegt die Standardrate allerdings eher zwischen 20 und 26 Mbit/s.

802.11g unterstützt dank der OFDM-Modulationstechnologie (Othogonal Frequency Division Multiplexing) den gleichen Durchsatz wie 802.11a, bietet aber Abwärtskompatibilität mit 802.11b-Geräten. Cisco hat einen Access-Point entwickelt, der 802.11b- und 802.11a-Geräten die Koexistenz im gleichen WLAN ermöglicht. Dieser Access-Point realisiert Gateway-Dienste, die eine Kommunikation zwischen diesen eigentlich inkompatiblen Geräten ermöglicht.

Weitere Erhöhungen der Übertragungsgeschwindigkeit auf 100 Mbit/s mittels neuer Modulierungs- und Kodierungsverfahren und Verbesserungen des MAC-Protokolls verspricht der künftige Standard 802.11n. Bei diesem Standard wird die Übertragungsrate auch erstmalig oberhalb der MAC-Schnittstelle gemessen und ist damit im Gegensatz zu den Angaben der früheren Normen eine Nettoübertragungsrate.

3.3.3 Funknetzeinrichtungen und Funknetztopologien

Bereits zwei Geräte – nämlich zwei PCs mit Funknetzkarten – können ein Funknetzwerk bilden. Abbildung 3.40 zeigt eine interne Funknetzkarte, Abbildung 3.41 eine externe Karte für den Anschluss an den USB-Port. Ein solches Ad-hoc-Netzwerk kann aus zwei oder mehr Notebooks bestehen und entspricht einem kabelbasierten Peer-to-Peer-Netzwerk: Beide Geräte arbeiten in dieser Umgebung gleichermaßen als Server und als Client. Zwar wird auf diese Weise eine Verbindung hergestellt, aber die Sicherheit ist ebenso niedrig wie der Durchsatz. Auch die Kompatibilität kann hier zum Problem werden, weil Netzwerkkarten unterschiedlicher Hersteller oftmals nicht kompatibel miteinander sind.

Häufiger jedoch wird ein Access-Point (Abbildung 3.42) installiert, der dann als zentraler Hub für den WLAN-Infrastrukturmodus agiert. Der Access-Point ist fest an das verkabelte LAN angeschlossen und bietet so Konnektivität zum lokalen Netzwerk und zum Internet. Access-Points sind mit einer oder zwei Antennen ausgerüstet und stellen drahtlose Verbindungen in einem räumlich beschränkten Bereich her, der als Zelle bezeichnet wird.

Abbildung 3.40: Interne Funknetzkarte

Abbildung 3.41: Externe Funknetzkarte (USB-Variante)

Abbildung 3.42: Access-Point

Abhängig vom strukturellen Aufbau des Standorts, an dem der Access-Point installiert wird, sowie von der Größe und dem Gewinn der Antenne kann die Zelle einige Meter bis 40 Kilometer groß sein. Am verbreitetsten sind Zellen mit einem Erfassungsbereich von 100 bis 150 Metern. Um größere Bereiche versorgen zu können, installiert man mehrere Access-Points, deren Reichweiten sich überdecken und auf diese Weise das so genannte Roaming, d. h., das nahtlose Wechseln zwischen den Zellen erlauben (Abbildung 3.43). Das Roaming ähnelt den Diensten, die in Mobilfunknetzen verwendet werden. Die Überlagerung mehrerer Access-Point-Bereiche ist wichtig für die Bewegung der Geräte innerhalb des WLAN. Zwar ist der Umfang der Bereichsüberdeckung in den IEEE-Standards nicht definiert, aber ein Wert von 20 bis 30 Prozent ist wünschenswert, um das Wechseln zwischen den Zellen zu ermöglichen: Auf diese Weise kann die Verbindung zum Access-Point gewechselt werden, ohne dass hierfür Dienste unterbrochen werden müssen.

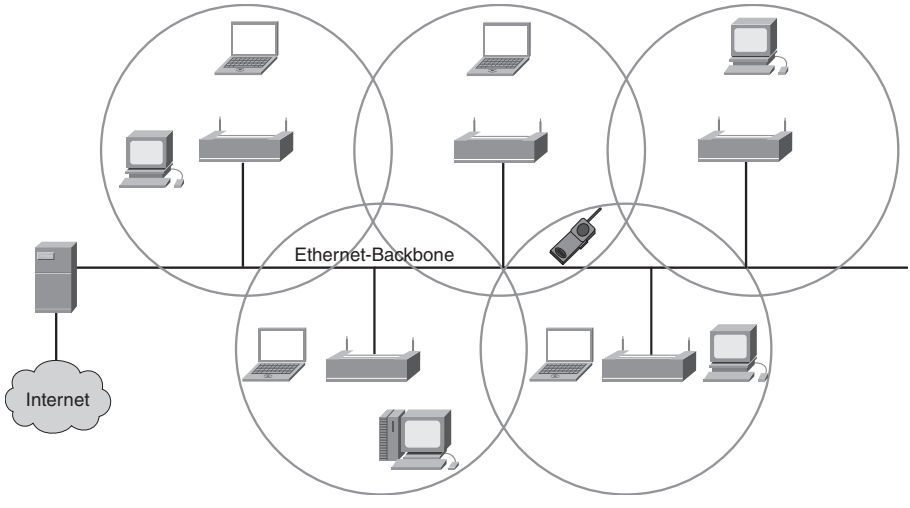


Abbildung 3.43: Roaming

Wenn ein Client innerhalb des WLAN aktiviert wird, fängt er an, nach einem kompatiblen Gerät zu suchen, mit dem er eine Verbindung herstellen kann. Dieser Vorgang wird als Scanning bezeichnet und kann aktiver oder passiver Natur sein:

– Beim aktiven Scanning wird eine Suchanforderung vom WLAN-Knoten, der einem Netzwerk beitreten will, quasi »ins Blaue hinein« gesendet. Diese Anforderung enthält die SSID (Service Set Identifier, Dienstsatzkennung) des erwünschten Netzwerks. Wird ein Access-Point mit der gleichen SSID gefunden, dann antwortet dieser, und die Authentifizierungs- und Verbindungsschritte werden abgeschlossen.

– Passiv scannende Knoten hingegen suchen nach speziellen Management-Frames – den Beacons –, die von Access-Points im Infrastrukturmodus oder Peer-Knoten im Ad-hoc-Modus gesendet werden. Empfängt ein Knoten einen Beacon, der die SSID des Netzwerks enthält, dem er beitreten möchte, dann versucht er diesen Beitritt. Das passive Scanning ist ein kontinuierlicher Vorgang, bei dem die Knoten Assoziationen mit Access-Points je nach Signalstärke jederzeit herstellen und trennen können.

3.3.4 Kommunikation in WLANs

Wenn ein Knoten eine Verbindung zum WLAN hergestellt hat, sendet er – wie bei jedem 802.3-Netzwerk auch – Frames. Allerdings verwenden WLANs keine Frames entsprechend dem 802.3-Standard, weswegen der auch häufig verwendete Begriff *Funk-Ethernet* irreführend ist. Es gibt drei Arten von Frames, nämlich Steuer-, Management- und Daten-Frames. Nachfolgend sind alle Frames aufgelistet, die den einzelnen Frame-Typen zugeordnet sind:

– Management-Frames
  – Assoziationsanforderungs-Frame
  – Assoziationsantwort-Frame
  – Suchanforderungs-Frame
  – Suchantwort-Frame
  – Beacon-Frame
  – Authentifizierungs-Frame
– Steuer-Frames
  – RTS-Frame (Request to Send)
  – CTS-Frame (Clear to Send)
  – Bestätigungs-Frame
– Daten-Frames

Nur der Daten-Frame ähnelt den 802.3-Frames. Die Nutzlast von WLAN- und 802.3-Frames beträgt 1.500 Bytes; ein Ethernet-Frame kann insgesamt nicht länger als 1.518 Bytes sein. Ein WLAN-Frame kann hingegen 2.346 Bytes lang sein, er wird allerdings in der Größe meist auf 1.518 Bytes beschränkt, da er häufig in ein drahtgebundenes Ethernet-Netzwerk übertragen werden soll.

Da Funkwellen ein gemeinsames Medium sind, können ebenso wie bei drahtgebundenen Medien auch hier Kollisionen auftreten. Der wesentliche Unterschied besteht darin, dass in Funknetzen keine Möglichkeit vorhanden

ist, dem Absenderknoten mitzuteilen, dass eine Kollision stattgefunden hat. Aufgrund dieser Tatsache verwenden WLANs die CSMA/CA-Technologie (Carrier Sense Multiple Access with Collision Avoidance), die der in Ethernet-Netzwerken verwendeten CSMA/CD-Methode ähnelt, die in Kapitel 6, »Grundlagen zum Ethernet«, eingehend erklärt werden wird.

Wenn ein Absenderknoten einen Frame sendet, schickt der Empfänger eine Positivbestätigung (ACK) zurück, wodurch logischerweise 50 Prozent der verfügbaren Bandbreite belegt werden. Diese Vorgehensweise sorgt in Verbindung mit dem CSMA/CA-Protokoll dafür, dass der tatsächliche Datendurchsatz sich in einem 802.11b-Netzwerk, das nominell mit 11 Mbit/s arbeitet, auf maximal 5 bis 5,5 Mbit/s beschränkt.

Die Leistungsfähigkeit des Netzwerks wird aber auch durch die Signalstärke und die Verschlechterung der Signalqualität aufgrund von Entfernungen und Interferenzen beschränkt. Wenn das Signal schwächer wird, kann die ARS-Funktion (Adaptive Rate Selection, automatische Anpassung der Übertragungsrate) aufgerufen werden, um die Übertragungsrate der sendenden Station von 11 Mbit/s über 5,5 und 2 Mbit/s bis hinab auf 1 Mbit/s zu senken (Abbildung 3.44).

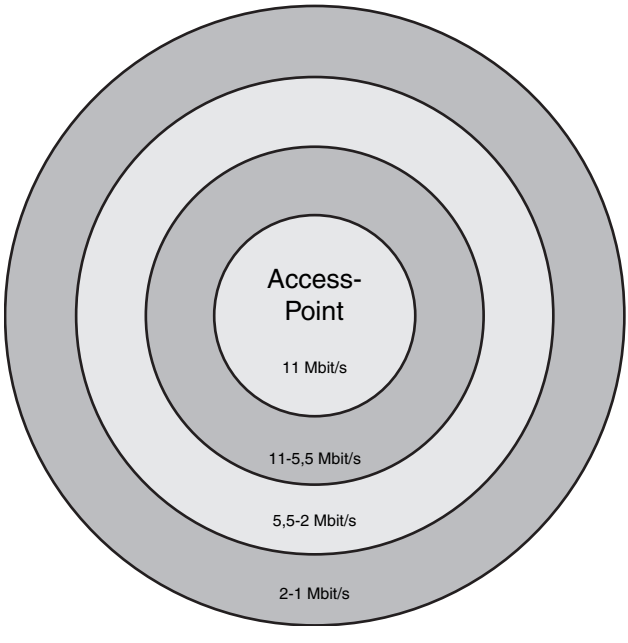


Abbildung 3.44: ARS (Adaptive Rate Selection)

3.3.5 Authentifizierung und Assoziation

Die WLAN-Authentifizierung findet in Schicht 2 statt und besteht eigentlich in der Authentifizierung des Gerätes und nicht der des Benutzers – dies ist ein wichtiger Aspekt, der bei Administration und Fehlersuche im WLAN ebenso zu berücksichtigen ist wie bei sicherheitstechnischen Betrachtungen.

Die Authentifizierung kann ein direkter Prozess sein, wie es etwa bei einem neuen Access-Point oder einer neuen Netzwerkkarte der Fall ist, auf dem bzw. der die Standardeinstellungen konfiguriert sind. Der Client sendet einen Authentifizierungsanforderungs-Frame an den Access-Point, und dieser Frame wird dann vom Access-Point angenommen oder abgelehnt. Der Client wird in jedem Fall über einen Authentifizierungsantwort-Frame vom Ergebnis in Kenntnis gesetzt. Der Access-Point kann aber auch so konfiguriert sein, dass er die Authentifizierungsaufgaben einem Authentifizierungsserver übergibt, der einen etwas umfangreicheren Überprüfungsvorgang durchführt.

Die Assoziation (oder auch »Zuordnung«), die nach der Authentifizierung durchgeführt wird, ist der Betriebszustand, in dem ein Client die Dienste des Access-Points für den Datenversand in Anspruch nehmen darf.

Authentifizierungs- und Assoziationstypen

Man unterscheidet die folgenden Typen der Authentifizierung und Assoziation:

- **Nicht authentifiziert, nicht assoziiert.** Der Knoten ist vom Netzwerk getrennt und keinem Access-Point zugeordnet.
- **Authentifiziert, nicht assoziiert.** Der Knoten ist im Netzwerk authentifiziert, aber noch nicht mit einem Access-Point verbunden.
- **Authentifiziert und assoziiert.** Der Knoten ist mit dem Netzwerk verbunden und kann Daten über den Access-Point senden und empfangen.

Authentifizierungsmethoden

IEEE 802.11 listet zwei Authentifizierungsprozesse auf:

- **Open System (offenes System).** Dieser Vorgang ist ein offener Verbindungsstandard, bei dem nur die SSID übereinstimmen muss. Er kann in einer sicheren wie auch in einer nicht sicheren Umgebung eingesetzt werden; allerdings ist die Möglichkeit gegeben, dass ein systemnah arbeitender Netzwerk-Sniffer die SSID relativ schnell ermitteln kann.

– **Shared Key (gemeinsamer Schlüssel).** Dieser Vorgang setzt den Einsatz von WEP (Wired-Equivalent Privacy, Datenschutz wie in leitungsbasierten Netzen) voraus. WEP ist ein recht einfacher Algorithmus, der 64-Bit- und 128-Bit-Schlüssel verwendet. Am Access-Point wird zunächst ein kodierter Schlüssel kodiert; Knoten, die über den Access-Point auf das Netzwerk zugreifen wollen, müssen über einen eigenen, zu diesem Schlüssel passenden Schlüssel verfügen. Statisch zugewiesene WEP-Schlüssel bieten zwar ein höheres Maß an Sicherheit als ein offenes System, aber keinen definitiven Schutz vor Angriffen.

Es gibt mittlerweile eine zunehmende Anzahl von Sicherheitslösungen und Technologien, welche die Anfälligkeit von WLANs für unautorisierten Zugriff zu beseitigen versuchen.

3.3.6 Funkwellen- und Mikrowellenspektren

Funkwellen werden durch Variation elektrischer Ströme in der Antenne des Senders erzeugt und dann von der Antenne in gerader Richtung abgestrahlt. Allerdings schwächen sich Funkwellen nach dem Abstrahlen von der Antenne zunehmend ab. In einem WLAN hat ein Funksignal, das in einem Abstand von zehn Metern von der Sendeantenne gemessen wird, nur mehr ein Tausendstel der ursprünglichen Stärke.

Wie Licht können auch Funkwellen von manchen Materialien absorbiert werden, während andere sie reflektieren. Wenn die Wellen von einem Material (z. B. Luft) in ein anderes (etwa Mauern) überwechseln, werden sie gebrochen. Außerdem werden Funkwellen von Wassertröpfchen in der Luft gestreut und absorbiert.

Die Eignungsprüfung eines Ortes für die Installation eines WLAN nennt man Standortaufnahme.

Da Funksignale auf dem Weg vom Sender immer schwächer werden, muss der Empfänger ebenfalls mit einer Antenne ausgestattet sein. Treffen die Funkwellen auf die Antenne eines Empfängers, werden in ihr schwache elektrische Ströme erzeugt, die den Strömen entsprechen, welche die Funkwellen in der Sendeantenne erzeugt haben. Der Empfänger verstärkt diese Signale.

Beim Sender werden die elektrischen Datensignale von einem Computer bzw. aus einem LAN nicht direkt in die Sendeantenne eingespeist. Stattdessen wird mit diesen Signalen ein anderes, sehr starkes Signal – die Trägerwelle – moduliert. Dieses Trägersignal wird dann beim Empfänger wieder demoduliert: Der Empfänger wertet die Phasenänderungen des Trägersignals aus und stellt auf dieser Basis das ursprüngliche elektrische Datensignal wieder her.

3.3.7 Nutz- und Störsignale im WLAN

In einem Ethernet-Netzwerk ist die Diagnose von möglichen Störeinflüssen meist verhältnismäßig leicht. Bei der Funktechnologie müssen Sie hingegen mehrere unterschiedliche Störungsformen in Betracht ziehen:

– **Schmalbandstörungen.** Dies ist das Gegenteil der Bandspreizung. Wie der Name bereits sagt, betreffen schmalbandige Störungen nicht das gesamte Frequenzspektrum des Funksignals. Eine mögliche Lösung für ein solches Problem besteht im Wechseln des vom Access-Point verwendeten Kanals. Tatsächlich aber ist die Ursachenfindung bei solchen Störungen eine zeit- und kostenaufwändige Angelegenheit. Um die Herkunft zu ermitteln, benötigt man einen Spektralanalysator, bei denen bereits die preiswertesten Modelle zwischen 3.000 und 4.000 EUR liegen. Mögliche Verursacher schmalbandiger Störungen sind CB- und Amateurfunkgeräte.

– **Allbandstörungen.** Allbandstörungen betreffen den gesamten Spektralbereich. Die Bluetooth-Technologien etwa springen viele Male pro Sekunde im gesamten 2,4-GHz-Band hin und her und können so in einem 802.11b-Netzwerk erhebliche Störungen verursachen. Deswegen trifft man an bestimmten Einrichtungen, in denen Funknetze zum Einsatz kommen, häufig auf Schilder, die Benutzer auffordern, vor dem Eintritt alle Bluetooth-Geräte abzuschalten. Ein in Heim- und Unternehmensumgebungen häufig übersehenes Gerät, das Störungen verursachen kann, ist der ganz normale Mikrowellenherd. Austretende Mikrowellen eines solchen Herdes in das Funkspektrum können bereits bei einer Leistung von nur 1 Watt erhebliche Behinderungen im WLAN verursachen, da es selbst nur eine maximale Sendeleistung von 100 mW benutzen darf. Auch schnurlose Telefone, die im 2,4-GHz-Spektrum arbeiten, können die Leistung im Funknetz beeinträchtigen.

– **Das Wetter.** Im Allgemeinen werden Funksignale auch durch die extremsten Wetterbedingungen nicht beeinträchtigt. Eine Ausnahme bilden hier Nebel oder eine sehr hohe Luftfeuchtigkeit. Manchmal kann auch Blitzschlag die Atmosphäre aufladen und so den Pfad eines Übertragungssignals ändern.

Erste und offensichtlichste Ursache eines Signalproblems können die sendende Station oder der Antennentyp sein. Eine leistungsstärkere Station sendet das Signal über eine größere Strecke, und eine Parabolantenne fokussiert das Signal und erhöht so den Übertragungsbereich.

In SOHO-Umgebungen (Heimbereich und Kleinunternehmen) verwenden Access-Points meist zwei omnidirektionale Antennen (Abbildung 3.45), die

das Signal in alle Richtungen übertragen und dadurch eine geringere Reichweite haben.

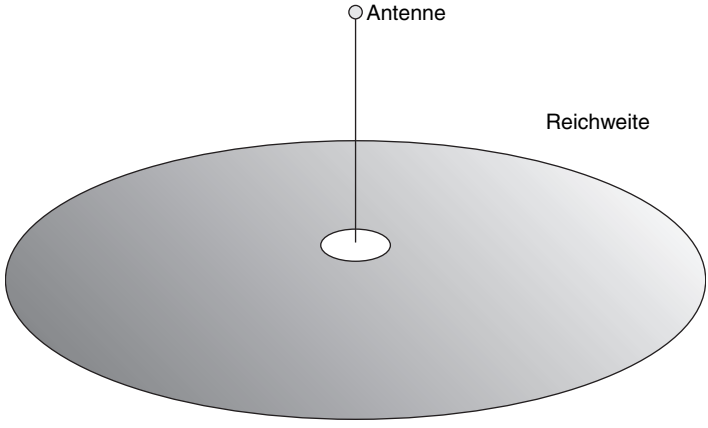


Abbildung 3.45: Omnidirektionale Antenne

3.3.8 Sicherheit im WLAN

Das exponentielle Wachstum der Netzwerke – und hier auch und gerade der Funktechnologien – hat die Sicherheitsrisiken erhöht. Die Optimierung der Sicherheit hat aber auch zur Folge, dass man mehr Zeit mit der Verwaltung des Systems verbringt.

Die erste Sicherheitsmaßnahme in einem WLAN besteht darin, die Funkfrequenzwellen selbst zu schützen. Access-Points strahlen die Funkwellen über einen großen Bereich ab, der nicht nur auf das Gebäude beschränkt ist. Weil »Lauscher« unbemerkt auf diese Wellen zugreifen können, ist hier ein Sicherheitsproblem gegeben. Die Funkwellen von WLAN-Bridges hingegen sind in einem kleinen Winkel fokussiert; um auf diese Wellen zugreifen zu können, muss der Lauscher in den Strahlenpfad gelangen und die Kommunikation abfangen. Aufgrund dessen benötigen Access-Points in der Regel mehr sicherheitstechnische Maßnahmen als WLAN-Bridges.

WEP

WEP (Wired-Equivalent Privacy) ist eine Sicherheitsmethode, die im 802.11-Standard definiert ist und die Übertragung von Daten zwischen WLAN-Access-Points und Netzwerkkarten schützen soll. Der Standard IEEE 802.11b sieht 40-Bit-Schlüssel für die Verschlüsselung vor, aber viele Anbieter – darunter auch Cisco – unterstützen ebenfalls den optionalen 128-Bit-Standard.

Die wesentlichen Ziele von WEP sind die folgenden:

– Blockierung des Netzwerkzugriffs für unautorisierte Benutzer, die nicht über den passenden WEP-Schlüssel verfügen

– Unmöglichkeit der Entschlüsselung abgefangenen WLAN-Datenverkehrs ohne Besitz des passenden WEP-Schlüssels

WEP verwendet die von Ron Rivest entwickelte RC4-Kodierung zur Verschlüsselung[1]. Der RC4-Verschlüsselungsalgorithmus ist eine symmetrische Bitstromchiffre, die Schlüssel variabler Länge unterstützt. Eine symmetrische Chiffre verwendet für Ver- und Entschlüsselung den gleichen Schlüssel. Dieser Schlüssel ist die einzige Information, die von den beiden beteiligten Endpunkten gemeinsam verwendet werden muss.

Sehr schnell haben Verschlüsselungsexperten Sicherheitslücken bei den Authentifizierungs- und WEP-Verschlüsselungssystemen des IEEE 802.11-WLAN-Standards entdeckt. Aus diesem Grund ist davon abzuraten, WEP als einzigen Sicherheitsmechanismus im WLAN einzusetzen; vielmehr sollte WEP durch andere fortgeschrittene Sicherheitsmaßnahmen ergänzt bzw. ersetzt werden, wie z. B. WPA, EAP-TLS, LEAP, IPSec, VPN oder Firewall.

VPN, WPA, EAP und LEAP

In der letzten Zeit wurde eine Reihe neuer Sicherheitslösungen und -protokolle entwickelt, z. B. VPNs (Virtuelles Privates Netzwerk), WPA (WiFi Protected Access) und EAP (Extensible Authentication Protocol). Bei Verwendung von EAP führt ein Access-Point die Authentifizierung des Clients nicht selbst durch, sondern übergibt diese Aufgabe an einen Sicherheitsserver, der speziell für diesen Zweck eingerichtet wurde. Mithilfe eines integrierten VPN-Servers erstellt die VPN-Technologie einen Tunnel, der auf ein vorhandenes Protokoll (z. B. IP) aufsetzt. Dieser Tunnel stellt eine Schicht-3-Verbindung her (im Gegensatz zur Verbindung zwischen Access-Point und sendendem Knoten, bei der es sich um eine Schicht-2-Verbindung handelt).

Hier eine kurze Beschreibung von WPA, EAP und LEAP (Lightweight Extensible Authentication Protocol):

– **WPA (WiFi Protected Access).** WPA mit TKIP (Temporal Key Integrity Protocol) ist eine Zwischenlösung des WiFi-Konsortiums und bietet wesentliche Verbesserungen gegenüber WEP. Das TKIP-Protokoll eliminiert zwei der Hauptprobleme von WEP: den statischen Schlüssel und die unzureichende Integritätssicherung.

1. Ron Rivest ist Mitarbeiter der bekannten Sicherheitsfirma RSA Security. RC steht übrigens für »Ron's Code«.

- **EAP-MD5-Challenge.** EAP ist der älteste WLAN-Authentifizierungstyp und ähnelt stark dem CHAP-Passwortschutz (Challenge Handshake Authentication Protocol) in drahtgebundenen Netzwerken. EAP ermöglicht WLAN-Clients, die unterschiedliche Authentifizierungstypen unterstützen, mit verschiedenen Back-End-Servern wie etwa einem RADIUS-Server (Remote Authentication Dial-In User Service) zu kommunizieren.
- **LEAP-Protokoll.** Mit diesem Protokoll hat Cisco eine Variante des EAP-Protokolls entwickelt, die auf gegenseitiger Authentifizierung basiert. Gegenseitige Authentifizierung bedeutet, dass sowohl der Benutzer als auch der Access-Point, an dem der Benutzer sich anzumelden versucht, authentifiziert werden müssen, bevor ein Zugriff aufs Unternehmensnetzwerk möglich ist. Die gegenseitige Authentifizierung schützt Unternehmen vor der unautorisierten Implementierung von Access-Points, die als potenzielle Hintertüren in das Unternehmensnetzwerk verwendet werden können.

  LEAP ist der bei Access-Points von Cisco meistverwendete Authentifizierungstyp, denn das Protokoll ermöglicht einen sicheren Austausch von Anmeldeinformationen, verschlüsselt die Daten mit dynamischen WEP-Schlüsseln und unterstützt die gegenseitige Authentifizierung.

Zu den Sicherheitsmerkmalen von VPNs gehören die folgenden:

- **Benutzerauthentifizierung.** Nur autorisierten Benutzern werden Verbindung sowie Versand und Empfang von Daten über das Funknetz ermöglicht.
- **Verschlüsselung.** VPNs benutzen Verschlüsselung und schützen die Daten auf diese Weise besser vor Angreifern.
- **Datenauthentifizierung.** Sie stellt die Integrität der Daten sicher, weil sowohl die Absender- als auch die Zielgeräte authentifiziert werden.

Oftmals ist die Reichweite von WLANs größer als der Bereich, in dem sie benutzt werden sollen, und ohne Implementierung von Sicherheitsmaßnahmen können Angreifer mit wenig Mühe in das Netzwerk eindringen. Wird ein WLAN nicht durch ein VPN gesichert, dann wird jeder Datenverkehr eines Funknetzteilnehmers sofort akzeptiert und weitergeleitet. Die VPN-Technologie sichert ein WLAN gegen unautorisierte Teilnehmer von außen ab, und ihre Implementierung ist für den Netzwerkadministrator weitgehend unproblematisch.

3.4 Zusammenfassung

In diesem Kapitel werden die folgenden Sachverhalte erläutert:

- Elektrostatische Entladung kann bei empfindlichen Elektronikgeräten schwerwiegende Probleme verursachen.
- Unter der Dämpfung versteht man den Widerstand gegen den Elektronenfluss. Die Dämpfung ist Ursache dafür, dass ein elektrisches Signal, das über einen Leiter transportiert wird, immer schwächer wird.
- Strom fließt in geschlossenen Stromkreisen. Diese müssen aus leitfähigem Material bestehen und Spannungsquellen aufweisen.
- Ein Multimeter misst Spannung, Strom, Widerstand und andere elektrische Größen, die sich numerisch ausdrücken lassen.
- In der Netzwerktechnik kommen drei Arten von Kupferkabel zum Einsatz: Straight-Through-Kabel, Crossover-Kabel und Rollover-Kabel.
- Koaxialkabel besteht aus einem hohlen zylindrischen Außenleiter, der einen einzelnen inneren Leiter umgibt.
- UTP-Kabel ist ein ungeschirmtes Medium mit vier Leiterpaaren, das in Nordamerika bei einer Vielzahl von Netzwerken eingesetzt wird.
- STP-Kabel kombinieren die Methoden der Schirmung, des Störunterdrückungseffekts und der Leiterverdrillung (wird auch als PiMF-Kabel bezeichnet).
- Ein Glasfaserkabel ist ein gutes Übertragungsmedium, wenn es fachgerecht installiert, getestet und gewartet wurde.
- Lichtenergie – eine Form elektromagnetischer Energiewellen – wird verwendet, um große Datenmengen sicher über relative große Entfernungen zu übertragen.
- Das in einer Glasfaser übertragene Lichtsignal wird von einem Transmitter erzeugt, der ein elektrisches Signal in ein Lichtsignal konvertiert.
- Ein Receiver wandelt Licht, das am beim Empfänger eintrifft, wieder in das ursprüngliche elektrische Signal um.
- Glasfasern werden paarweise verwendet, um die Vollduplexkommunikation zu ermöglichen.
- Lichtstrahlen gehorchen auf ihrem Weg durch Glasfaser den Gesetzen der Reflexion und Brechung. Aus diesem Grund können Fasern mit der Eigenschaft der internen Totalreflexion hergestellt werden. Die interne

Totalreflexion sorgt dafür, dass das Licht auch dann innerhalb der Faser bleibt, wenn diese nicht völlig gerade ist.

- Die Dämpfung eines Lichtsignals wird bei langen Kabeln insbesondere dann zum Problem, wenn das Kabel mehrfach über Verteilerfelder oder Spleißverbindungen geführt wird.
- Kabel und Steckverbinder müssen fachgerecht installiert und mithilfe hochwertiger optischer Prüfgeräte vor Inbetriebnahme vollständig getestet werden. Auch danach sind mithilfe dieser Geräte regelmäßig Tests durchzuführen, um festzustellen, ob sich die Leitungsqualität auf irgendeine Weise verschlechtert hat.
- Schützen Sie immer Ihre Augen, wenn Sie mit starken Lichtquellen wie etwa Lasern umgehen.
- Detaillierte Kenntnisse der Regeln und Standards der WLAN-Technologie sind erforderlich, um Netzwerke einzurichten, die interoperabel sind.
- Kompatibilitätsprobleme mit WLAN-Netzwerkkarten lassen sich durch Installation eines Access-Points lösen, der als zentraler Hub im WLAN agiert.
- In der Funkkommunikation werden drei Arten von Frames eingesetzt, nämlich Steuer-, Management- und Daten-Frames.
- In WLANs kommt die CSMA/CA-Technologie (Carrier Sense Multiple Access/Collision Avoidance) zum Einsatz.
- Bei der WLAN-Authentifizierung wird nicht der Benutzer, sondern das Gerät authentifiziert.
- Zu den wichtigsten Standards für Funknetze gehören IEEE 802.11, IEEE 802.11a, IEEE 802.11b und IEEE 802.11g.
- Zu den im WLAN eingesetzten Geräten gehören PCMCIA-Netzwerkkarten für Laptops, externe USB-Funknetzkarten und Access-Points.

3.5 Lernzielkontrolle

Beantworten Sie die folgenden Fragen, um Ihren Kenntnisstand bezüglich der in diesem Kapitel beschriebenen Themen und Konzepte zu überprüfen. Die Antworten finden Sie in Anhang A, »Antworten zu den Lernzielkontrollen«.

1. Welche der folgenden Aussagen zur Elektrizität ist nicht zutreffend?

   a) Ungleichnamige Ladungen reagieren aufeinander mit einer Kraft, die eine gegenseitige Anziehung verursacht.

   b) Gleichnamige Ladungen reagieren aufeinander mit einer Kraft, die eine gegenseitige Abstoßung verursacht.

   c) Sowohl bei ungleichnamigen als auch bei gleichnamigen Ladungen gilt, dass die Kraft umso größer wird, je näher die Ladungen aufeinander zu bewegt werden.

   d) Keine der genannten.

2. Ordnen Sie die korrekten Maßeinheiten zu:

1. Spannung	A. Ohm
2. Strom	B. Ampere
3. Widerstand	C. Volt

   a) 1-C, 2-B, 3-A

   b) 1-B, 2-C, 3-A

   c) 1-A, 2-C, 3-B

   d) 1-C, 2-B, 3-A

3. Elektronen fließen in Schleifen. Welche Eigenschaft haben diese Schleifen, und wie heißen sie?

   a) offene Schleifen namens »Spannungen«

   b) geschlossene Schleifen namens »Spannungen«

   c) offene Schleifen namens »Stromkreise«

   d) geschlossene Schleifen namens »Stromkreise«

4. Wie lang darf ein STP-Kabel maximal sein?

   a) 100 Fuß

   b) 150 Fuß

   c) 10 Meter

   d) 100 Meter

5. Aus wie vielen Leiterpaaren besteht ein UTP-Kabel?

   a) 2

   b) 4

c) 6

d) 8

6. Wie heißt der für TP-Kabel verwendete Steckverbinder?

a) STP

b) BNC

c) RJ45

d) RJ-69

7. Welchen Vorteil hat ein Koaxialkabel gegenüber STP oder UTP?

a) Es kann Datenraten von 10 bis 100 Mbit/s erzielen.

b) Es ist kostengünstig.

c) Es kann ohne Signalregeneration längere Strecken überwinden.

d) Keinen der genannten.

8. Was ist der Zweck der Verdrillung von Leitern in einem TP-Kabel?

a) Das Kabel ist dünner.

b) Das Kabel ist preisgünstiger.

c) Störprobleme werden vermindert.

d) Die Verdrillung ermöglicht die Integration von sechs Leiterpaaren in einem Raum, in dem normalerweise nur vier Paare Platz fänden.

9. Worin besteht die Bedeutung der EIA/TIA-Standards? Wählen Sie alle zutreffenden Antworten!

a) Sie sind ein Rahmen für die Implementierung des OSI-Referenzmodells.

b) Sie beinhalten Richtlinien, die durch die Hersteller von Netzwerkkarten beachtet werden müssen, um größtmögliche Kompatibilität zu gewährleisten.

c) Sie formulieren die Minimalanforderungen für Netzwerkmedien, damit auch Produkte unterschiedlicher Hersteller im Netzwerk gemeinsam eingesetzt werden können .

d) Keines der genannten.

10. Welcher Typ von Glasfaserkabel kann mehrere von einer LED generierte Lichtströme transportieren?
    a) Multimode-Glasfaserkabel
    b) Multichannel-Glasfaserkabel
    c) Multiphase-Glasfaserkabel
    d) Keiner der genannten.
11. Welches ist einer der Vorteile des Einsatzes von Glasfaserkabel in Netzwerken?
    a) Glasfaserkabel ist preisgünstig.
    b) Glasfaserkabel ist leicht zu installieren.
    c) Glasfaserkabel ist ein Industriestandard und in jedem Elektronikgeschäft erhältlich.
    d) Mit Glasfaserkabel lassen sich höhere Datenraten erzielen als mit Koaxial- oder TP-Kabeln.

Wenn Sie dieses Kapitel gelesen haben, sollten Sie in der Lage sein, die folgenden Fragen zu beantworten:

- Welche Unterschiede bestehen zwischen Sinus- und Rechteckschwingungen?
- Wie ändern sich Analogsignale in Bezug auf die Zeit und die Frequenz?
- Welche zwei grundlegenden Arten von Kupferkabeln gibt es für den Netzwerkeinsatz?
- Wie übertragen Glasfaserkabel Datensignale?
- Was versteht man unter dem Begriff der Dämpfung?
- Welche Störquellen gibt es bei Kupfermedien?
- Welche drei Arten von Übersprechen gibt es?
- Welches sind die zehn wichtigsten Parameter, die in den TIA/EIA-Standards in Bezug auf Kabeltests beschrieben werden?

Zusätzlich zu diesen Kernthemen stellt dieses Kapitel die folgenden für Netzwerktechniker wichtigen Themen vor:

- Exponenten und Logarithmen
- Dezibel
- Signalverlauf in Bezug auf Zeit und Frequenz
- Störungen in Bezug auf Zeit und Frequenz
- Einheiten analoger und digitaler Bandbreite
- zeitbasierte Parameter
- Testmöglichkeiten bei Glasfasern
- der CAT6-Standard