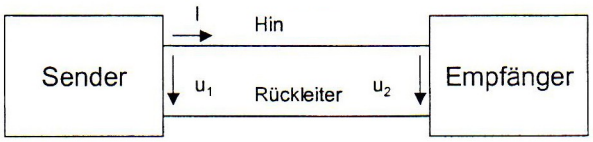
Zur Verbindung von Systemen in Netzwerken (PC, Server, Router, …) sind **Übertragungsstrecken** notwendig. Übertragungsstrecken mit ihren Systemen bestehen grundsätzlich aus:

- einem **Sender**
- einem **Empfänger**
- einem **Medium**, das Sender und Empfänger verbindet

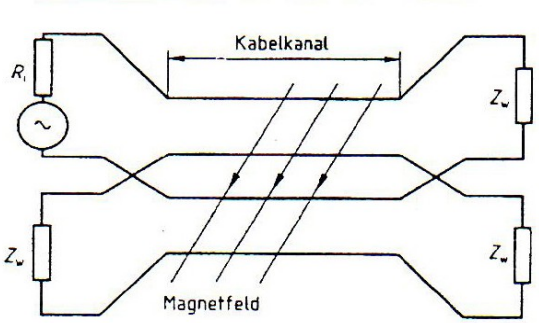
Zweidrahtleitungen

Im folgenden einfachen Beispiel sind Sender und Empfänger durch eine einfache Zweidrahtleitung verbunden. Da ein Stromkreis bekanntlich immer geschlossen sein muss, dient ein Leiter als Hinleiter, der andere als Rückleiter zum Sender.
Alternativ könnte auch auf den Rückleiter verzichtet werden. Er kann auch über die gemeinsame Erdung von Sender und Empfänger gebildet werden (Eindraht-Leitung). Die war früher bei den Telegraphenleitungen der Fall



Ein grundsätzliches Problem von Übertragungswegen, die mit Zweidrahtleitungen aufgebaut sind, ist die **gegenseitige störende Beeinflussung mehrerer Leitungen in einem Kabel untereinander**. Entsprechend den vorher erwähnten magnetischen und elektrischen Feldern, die um jede stromdurchflossene Leitung entstehen, können diese Felder in benachbarten Leitungen **Störspannungen** verursachen. Das Schlagwort dazu lautet EMV = Elektromagnetische Verträglichkeit, was bedeutet, dass das System einerseits störfest ist (passiv) als auch selbst keine Störungen verursacht (aktiv).

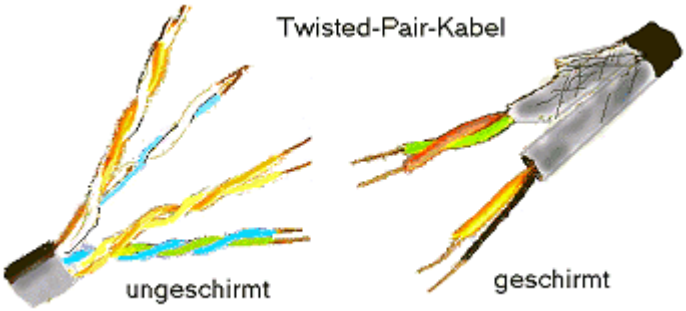
In der Nachrichten- / Datenübertragung werden grundsätzlich Wechselspannungssignale übertragen. Durch die vom Wechselstrom verursachten Magnetfelder können daher Induktionsspannungen in benachbarten Leitungen und somit auch Störungen entstehen.



Hochwertige Leitungen für Datennetzwerke minimieren die Störungen innerhalb des Kabels durch Verdrillung (gegen Magnetfelder) und/oder Schirmungen (gegen elektrische Felder).

Twisted-Pair (TP)

Twisted-Pair (´verdrilltes Paar´) ist ein vieradriges, paarweise verdrilltes Kupferkabel, bei dem zwischen Sender und Empfänger für jede Übertragungs-richtung zwei Kupferadern genutzt werden.

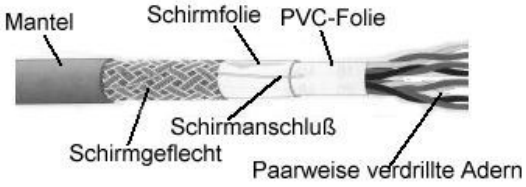


Die maximale Leitungslänge wird durch die Dämpfung des Datensignals begrenzt und hängt unter anderem davon ab, ob die Adernpaare einzeln abgeschirmt sind. Bei Datenraten bis 10GBit/S kann ein Twisted-Pair-Kabel neuer Bauart **bis zu 100 m lang** sein. Das Kabel verbindet, wenn kein Switch dazwischen geschaltet ist, genau zwei Stationen miteinander.

Kabelklasse (Categorie, CAT)

Sie bestimmt den Frequenzbereich und damit die mögliche Datenrate, die übertragen werden kann: A - 100 kHz, B - 1 MHz, C - 16 MHz, D - 100 MHz, E - 300 MHz, F - 600 MHz)

- CAT-1 für Alarmsysteme und analoge Sprachübertragung
- CAT-2 für Sprache und RS232-Schnittstellen
- CAT-3 bis 16 MHz
- CAT-4 bis 20 MHz
- CAT-5/5e bis 100 MHz (e=enhanced, verbessert) = 1GBit/s
- CAT-6 bis 250 Mhz = 1GBit/s, 6e bis 10GBit/s
- CAT-7 bis 1 GHz = 10GBit/s (aktueller Typ)
- CAT-8 bis 2GHz = 40GBit/s (aktueller Typ)



Schirmungs-Typen von Kabeln:

- UTP (Unshielded Twisted Pair, nicht abgeschirmte verdrillte Leitungen) gehörten früher typischerweise der Kategorie 3 an. Inzwischen gibt es sie auch als CAT-5-Kabel. UTP-Kabel haben im industriellen Bereich oder in der Datentechnik mit hohen Datenraten nichts verloren.
- S/UTP (Screened/Unshielded Twisted Pair) haben einen Gesamtschirm aus einem Kupfergeflecht zur Reduktion der äußeren Störeinflüsse.
- S/STP (Screened/Shielded Twisted Pair) besitzen eine Abschirmung für jedes Kabelpaar sowie eine Gesamtschirmung. Hierdurch kann eine optimale Störleistungsunterdrückung erreicht werden. Auch das Übersprechen zwischen den einzelnen Adernpaaren kann so wirksam unterdrückt werden.
- ITP (Industrial Twisted Pair) ist die industrielle Variante von S/STP. Während typische Netzwerkadern jedoch vier Adernpaare besitzen, beschränkt sich ITP auf zwei Paare.

Der Leiterdurchmesser der Adern beträgt bei CAT 7 z.B. 0,53mm.
Bei Neuinstallation wird heute zutage Cat-7-Kabel und als letzter Standard auch bereits Cat-8 verwendet, womit man auf längere Zeit zukunftssicher ist. **Bis 100MBit/s werden dabei zwei, ab 1GBit/s alle 4 Paare zur Übertragung verwendet.**

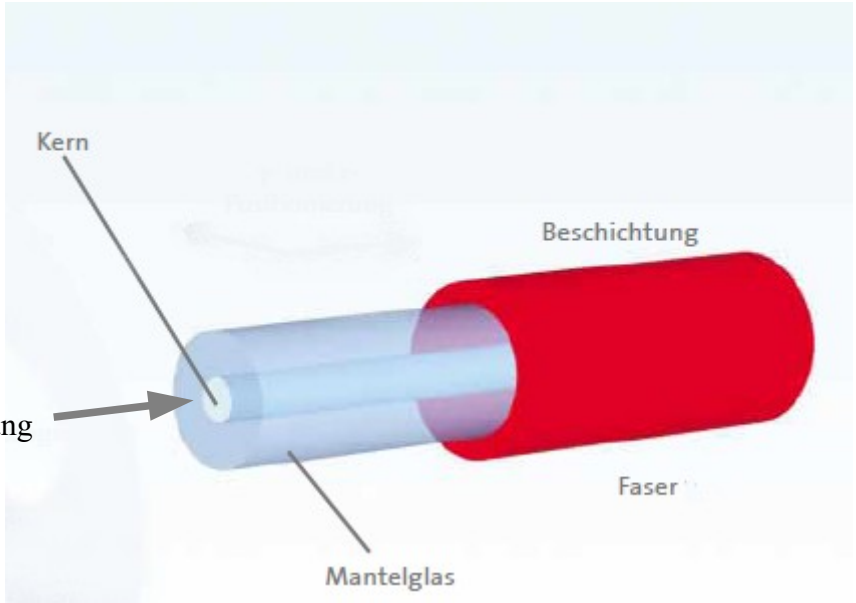
Lichtwellenleiter

Schon seit längerer Zeit werden Netzwerkleitungen teilweise als Lichtwellenleiter verlegt. Lichtwellenleiter bieten gegenüber dem Kupferkabel entscheidende Vorteile:

- Lichtwellenleiter können beliebig mit anderen Versorgungsleitungen parallel verlegt werden. Es gibt keine elektromagnetischen Störeinflüsse.
- Wegen der optischen Übertragung gibt es keine Störstrahlungen oder Kontaktprobleme. Auch Ausgleichsströme, die über den Kabelschirm fließen können, wenn das Netzwerkkabel zwei Orte (z.B. Stockwerke) mit unterschiedlichem Erdpotential verbindet, können nicht auftreten („Masseprobleme“).
- Verluste des Signals bei steigender Leitungslänge, wie bei Kupferkabeln, treten im Bereich der Gebäudeinstallation und der relativ geringen Längen nicht auf.
- In neuester Technologie können die Übertragungsraten durch mehrere Trägerwellen mit unterschiedlichen Wellenlängen (´Laserfarben´) noch weiter bis in den Bereich von TBit/s gesteigert werden. (sogenanntes Wellenlängen-Multiplex, eng.: Wave-Division-Multiplexing, WDM)
- Für den Übergang von TP zu LWL sind die bereits bekannten *Medienkonverter* nötig, die die Signale von elektrisch zu optisch und umgekehrt wandeln.

Bei allen Vorteilen: Lichtwellenleiter sind bei üblichen Verkabelungslängen in Gebäuden teurer als Kupferleitungen. Dies betrifft nicht nur die Materialkosten, sondern auch den Aufwand für die Installation und die Einbindung in das Netz, wofür Spezialwerkzeuge notwendig sind.

Wie arbeitet nun der LWL? Das Licht wird frontal in den LWL eingekoppelt. Durch Reflexion an den Randschichten wird es im Inneren des LWL gehalten und läuft so durch den Leiter. Deshalb konstruiert man den Lichtwellenleiter als „optische Röhre“.



Die angebotenen LWL-Typen unterscheiden die sich im Herstellungsaufwand und damit im Preis. Ein technisches Unterscheidungsmerkmal ist der Weg des Lichts durch die Leiter. Bei den billigeren Fasertypen kann das Licht auf verschiedenen Wegen durch den Leiter laufen, was die Impulse „verwäscht“ (dehnt) und damit die Leistungsfähigkeit (Datenrate) und Reichweite beschränkt. Die teuerste Faser, der so genannte *Momomode-LWL*, leitet das Licht nur „geradlinig“ durch den Leiter. Der Kerndurchmesser ist so klein, dass sich das Licht fast nur entlang der Längsachse ausbreiten kann. Mit diesen Fasern sind die größten Übertragungsraten und Reichweiten zu erzielen. Daher kommen sie auch in kontinentalen und ozeanischen Fernnetzen zum Einsatz.

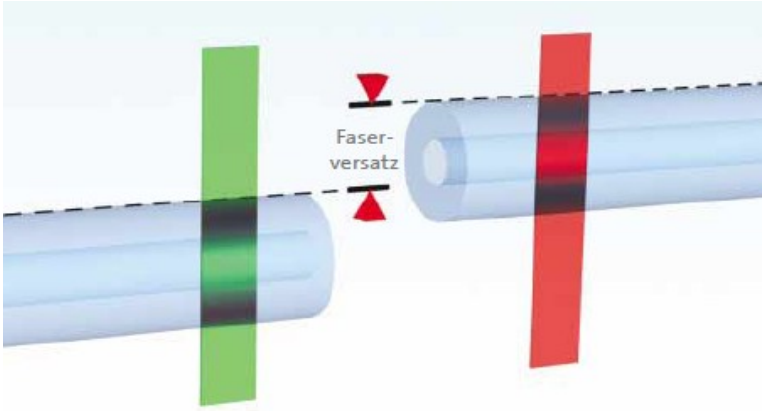
Sende-Elemente

Als Sender für die LWL-Übertragung stehen *Leuchtdioden* (LEDs) und *Laserdioden* (LD) zur Verfügung. dabei werden LEDs am besten im Bereich von 850/860 nm (Lichtwellenlänge in Nanometer) eingesetzt und LDs im Bereich von 1300nm, da dort die Dämpfung für die jeweiligen Lichtwellenlängen ein Minimum hat.

LWL-Verbindungen

Die optischen Sender und Empfänger (meist Laserdioden) müssen genau auf die Faser abgestimmt sein, um die maximale Energie ein- und auskoppeln zu können. Beim Verlegen von LWL ist der Übergang von einem Leiterstück auf ein anderes, das sogenannte „*Spleißen*“, technisch anspruchsvoll. Im Gegensatz zum elektrischen Leiter, bei dem eine Klemm- oder Lötverbindung genügt, müssen die Glasfasern genau in der optischen Achse plan miteinander verschweißt werden.

Da es hier zahlreiche Fehlermöglichkeiten gibt, leitet man zum Prüfen der Verbindung sichtbares Licht in die Faser und prüft die Fläche auf Verunreinigungen oder Kratzer. Zum Reinigen der Kontaktfläche verwendet man reinen Alkohol.



Faser mit Schmutz und Ausbrüchen

Bedingt durch den Bedarf an immer höheren Bandbreiten rückt die LWL-Technologie aus dem Fernnetz ("Backbone") immer weiter in die Fläche vor.
Die Abstufungen haben dabei folgende Bezeichnungen

- **FTTC**: fiber to the **curb**
  Die Glasfaser hat den ersten Abschnitt des bisherigen Kupfer-Ortsnetzes, die Hauptkabel (HK) ersetzt und endet nun im Kabelverzweiger (KVz). Das sind die „grauen Kästen“ am Straßenrand.

- **FTTB**: fiber to the **building**
  Die Glasfaser hat das komplette Ortsnetz-Kupferkabel ersetzt und wurde in das Gebäude eingeführt. Sie endet in der Hauseinführung. Von dort werden die Datenströme dann intern weiter verteilt - meist über vorhandene Kupferleitungen. Dies ist oftmals die Situation in Wohnblöcken / Häusern mit mehreren Wohneinheiten. Bei Änderung des Gebäudeanschlusses von Kupfer auf Glas muss an den Wohnungsanschlüssen somit nichts geändert werden.

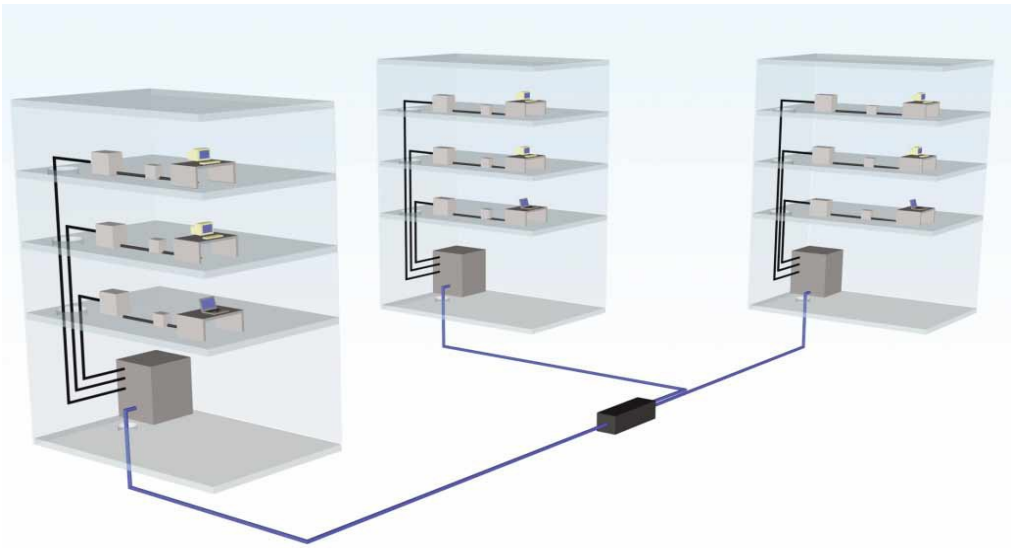
- **FTTH**: fiber to the **home**
  Als Fortführung von FTTB sind hier bereits die einzelnen Wohnungen mit LWL angeschlossen. Nur die Endgeräte sind noch über Kupfer-LAN-Kabel oder W-LAN angeschlossen.
  Aktuell dringt die Glasfaser verstärkt auch in den Privaten Bereich vor - je nach Stand des Netzausbaus. Als lokale Netzbetreiber treten hier verschiedene Anbieter auf. Am Beispiel der Telekom hier eine kurze Übersicht zur Anschlusstechnik bzw. den nötigen Anschlussvoraussetzungen im Haus.
  Im Unterschied zur direkten Anschlussleitung der "alten" Kupferleitung an den Router benötigt man für den Betrieb am GF-Anschluss einen Medienkonverter (mit entsprechender Stromversorgung), der die Wandlung optisch-elektrisch und umgekehrt vornimmt. Damit ergibt sich eine ähnliche Situation wie früher am ISDN-Anschluss, für den ebenfalls ein vor die Endgeräte geschaltetes Netzabschlussgerät zur Codewandlung/Leitungsanpassung nötig war.

- **FTTD**: fiber to the **desk**
  Der LWL-Anschluss wird bis zum "Schreibtisch" weiter geführt. Dies dürfte in den allermeisten Fällen nicht notwendig sein, da sich über aktuelle Kupfer.Netzwerkleitungen bequem auch 10GBit/s übertragen lassen. Dies ist deutlich mehr, als der private LWL-Anschluss überhaupt liefert.

Ein etwas in die Jahre gekommenes Video der Deutsche Bundespost zeigt die Herstellung und Eigenschaften der LWL sehr gut:

Verkabelungsstruktur in Gebäuden

Gebäudeverkabelungen werden heute zutage in so genannter *strukturierter Verkabelung* aufgebaut. Dies bedeutet, ausgehend von einem zentralen Verteilpunkt, eine **sternförmige** Verkabelung der Stockwerke mit LWL. Verbindungen zwischen Gebäuden werden **Punkt-zu-Punkt** ausgeführt, bei mehr als zwei Gebäuden wird ebenfalls sternförmig verkabelt.
Bei besonders hohen Anforderungen an die Verbindungssicherheit wird ein **zweiter unabhängiger Weg** eingerichtet.



Das folgende Bild zeigt einen mittelgroßen Verteiler für LWL mit aktiven und passiven Komponenten.

Bildquellen: ekukabelundsysteme.de

Drahtlose Netzwerklösungen (Funk-LAN, W-LAN)

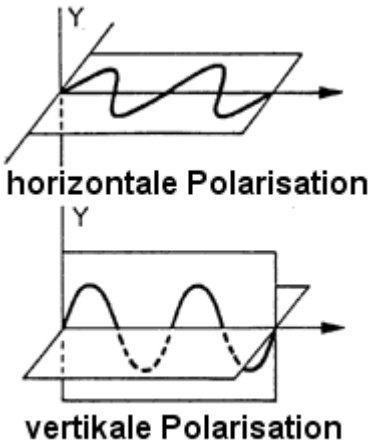
WLAN können heute in nahezu allen Branchen und Umgebungen zur Erweiterung oder Verbindung von lokalen Netzen eingesetzt werden. Ein typischer Einsatzbereich für die W-LAN-Technologie ist der Netzzugang für mobile Nutzer (Notebooks, Smartphones) oder die Vernetzung von LANs verschiedener Gebäude per Funk.

Grundlagen

Wireless LAN ist eine Funktechnik im 2,4-GHz- oder 5-GHz-Bereich zur Herstellung von Netzwerkverbindungen. Im praktischen Gebrauch ersetzt die Funkverbindung das Netzwerkkabel. Für das Betriebssystem und die Programme sieht es so aus, als wäre der Rechner über ein Netzwerkkabel angeschlossen.

Eigenschaften einer W-LAN-Verbindung:

- Alle Teilnehmer teilen sich den Kanal und erkennen nicht immer, dass eine andere Station gleichzeitig funkt. Sämtliche Sender „streiten“ sich um die maximal verfügbare Bandbreite (Übertragungsrate).
- Alle Teilnehmer in der Reichweite des Senders müssen gegenseitig „Rücksicht“ nehmen. Die Größe des Bereiches, in dem Kollisionen bei gleichzeitigem Senden auftreten können, hängt von der Reichweite der Sender ab. Auch daher muss diese begrenzt werden.
- Beispiel für funktechnische Besonderheiten und Probleme:
  - ✗ **Reflexion, Überlagerungen:** Das Funksignal gelangt auf verschiedenen Wegen zum Empfänger (direkt und über Reflexion). Im Extremfall kommt es zur Verdopplung bzw. totalen gegenseitigen Auslöschung der Signale. Es entstehen so im Raum verteilt örtliche Minima und Maxima der Empfangsfeldstärke („Funklöcher“).
  - ✗ **Unterschiediche Polarisation:** Je nach mechanischer Ausrichtung der Antenne sind die Wellen horizontal oder vertikal polarisiert (Polarisation= Schwingungsebene des elektrischen Feldes der elektromagnetischen Welle). Die Empfangsfeldstärke ist immer dann maximal, wenn die Antennen beider Stationen **gleich ausgerichtet** sind. Die Polarisation kann sich bei Reflexionen aber drehen und damit Signalschwund verursachen, wenn die Polarisationsebenen von Sender und Empfänger nicht mehr übereinstimmen.



Datenraten:
Beispiele von Standards und die Bruttobitraten (was ist nochmal brutto ? ;-) sind z.B.:

- 802.11a: 11 MBit/s im 2,4GHz-Band
- 802.11g: 54 MBit/s im 2,4GHz-Band
- 802.11n mit 540 Mbit/s im 2,5 bzw. 5GHz-Band

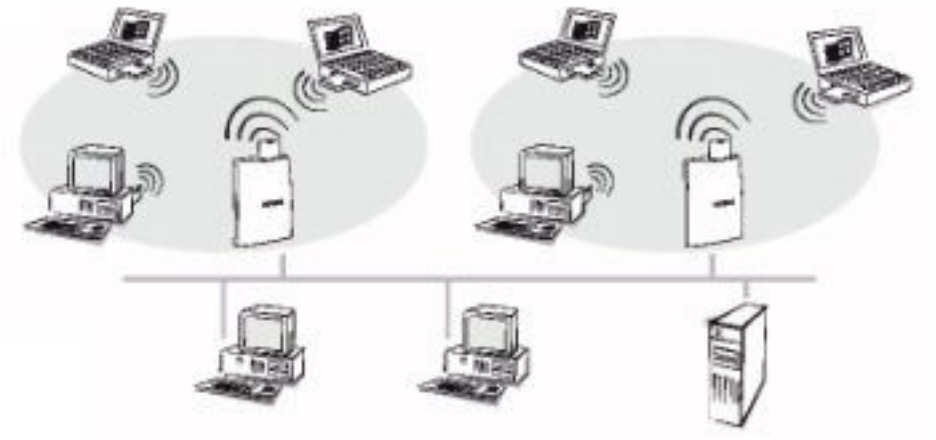
Tatsächliche Nettodatenraten (Nettobitrate = Bitrate, die dem Nutzer tatsächlich zur Verfügung steht): Bei einer größeren Anzahl von Nutzern stehen letztendlich für jede Endstelle nur ein Bruchteil der Bandbreite zur Verfügung, oftmals unter 10%.

Mit dem Begriff *Diversity* wird in der Funktechnik der Einsatz von zwei Antennen zur Empfangsoptimierung bezeichnet. Der Empfang lässt sich - vor allem in Innenräumen mit ihren Überlagerungsmustern (*Interferenz*) von direktem und reflektierten Signalen - deutlich verbessern, wenn man zwei Antennen verwendet. Diese haben idealerweise einen Abstand von mehr als einer halben Wellenlänge voneinander. Die Idee dahinter: Wenn die eine Antenne aufgrund eines lokalen Empfangsminimums schlechten Empfang hat, ist die Wahrscheinlichkeit groß, dass die andere Antenne in einem Maximum „sitzt“. Der Chipsatz, also die interne Steuerung, wählt ständig die Antenne mit dem besseren Empfang aus. Diversity bringt eine Empfangsverbesserung, um ungefähr 3dB (doppelte Empfangsleistung).
Beide Antennen sollten zudem am besten mit einem Winkel von 90 Grad zueinander ausgerichtet werden. Das liegt daran, dass nicht nur die Signalstärke eine Rolle spielt, sondern auch die erwähnte Polarisation. Durch Reflexionen wird die Polarisation – wie bereits beschrieben - gedreht.
Daher richtet man in Innenräumen die Diversity-Antennen senkrecht zueinander aus, so dass jeweils eine Antenne eine Polarisationsrichtung abdeckt.
Jede W-LAN-Erweiterungssteckkarte besitzt bereits zwei Antennen und betreibt damit Diversity Dass zwei so dicht nebeneinander angeordneten Antennen (bei Kartenformat) natürlich nicht optimal sind, sollte klar sein. Wesentlich besser ist da schon die häufig bei Access-Points zu findende Bauweise mit zwei schwenkbaren Antennen.

-

Integration in das LAN

W-LAN können unkompliziert als Ergänzung zum drahtgebundenen Netz betrieben werden.
Ein Wireless Access Point (Zugangspunkt) koordiniert dabei die einzelnen Stationen. Da W-LAN die „selbe Sprache“, also das selbe Protokoll (TCP/IP) wie das Kabel-LAN verwendet, kann über einen W-LAN-Zugangspunkt mit Netzwerk-Anschluss leicht eine Verbindung zu kabelgebundenen Netzen hergestellt werden. Eine Netzwerkkarte „merkt“ also gar nicht, ob sie mit einer anderen Netzwerkkarte über Kabel oder (über einen Access Point) mit einer W-LAN-Karte kommuniziert.



W-LAN-Netzwerk mit Access-Point

7. Sicherheitsaspekte

Wie alle Funktechnologien ist auch W-LAN besonders anfällig für Sicherheitsverletzungen.
Dies gilt um so mehr, als dass es sich um ein gemeinsam genutztes Medium handelt, sich also mehrere Nutzer eine Funkzelle teilen. Bekannt ist dieses Prinzip etwa vom Mobilfunk.
Doch während sich das Handy beim Einloggen über seine ID auf der SIM-Karte identifiziert und der Netzbetreiber dafür sorgt, dass der eingewählte Telefonanschluss geschützt ist, muss sich der W-LAN-Nutzer selbst um die Sicherheit kümmern.
Hinzu kommt: Grundsätzlich lässt sich die Reichweite der Signale nicht einfach auf den Gebäudebereich beschränken. Ein Hacker könnte sich also, z.B. mit dem Auto, auf den Parkplatz stellen und von dort aus versuchen, in das Netzwerk einzudringen.

Schlagworte für die Sicherheit im W-LAN sind:

- Verschlüsselung (derzeit bester Standard ist WAP)
- Beschränkung des Zugangs über die Abfrage der Hardware (MAC-) Adressen.
  Damit kann nicht jeder oder jedes Gerät in das Netz.
- Zugangspasswörter

Es ist völlig klar, dass es sich beim Thema Sicherheit von Netzwerken immer um ein Wettrennen zwischen den Angreifern und den Verteidigern handelt. Der Aufwand, Angriffe zu erkennen und abzuwehren, ist inzwischen immens angewachsen. Der materielle und zeitliche Aufwand ist dabei enorm. Dennoch gelingt es, vor allem staatlichen „feindlichen“ Stellen immer wieder, selbst in die Kernbereiche der Netzwerke einzudringen. Selbst Microsoft war /ist 2024 davon in hohem Maße betroffen.

Aufgaben, Fragen:

1. Beschreibe den grundsätzlichen Aufbau einer Übertragungsstrecke.
2. Nenne ein Hauptproblem von Übertragungswegen, die mit Zweidrahtleitungen aufgebaut sind.
3. Erkläre, warum und wie ein Leiter in einem benachbarten Leiter eine Störspannung erzeugen kann.
4. Erkläre den Begriff EMV.
5. Nenne Maßnahmen zur Verminderung der ´Störenden Beeinflussung´.
6. Nenne Einsatzbereiche von symmetrischen Leitungen.
7. Erläutere den grundsätzlichen Aufbau eines Twisted-Pair-Kabels (TP) und erkläre den Unterschied zwischen einem S/UTP und S/STP-Kabel.
8. Nenne die maximale Länge eines TP-Segmentes bei CAT 7/8-Verkabelung
9. Nenne jeweils die Adernanzahl, die bei symmetrischen Kuper-Netzwerkkabeln bei 100MBit/s und 1GBit/s benutzt wird.
10. Erstelle eine kurze tabellarische Gegenüberstellung der Vor- und Nachteile von LWL gegenüber Kupferkabeln.+
11. Beschreibe die grundsätzliche Funktion eines LWL und den prinzipiellen Aufbau. Erkläre dabei auch, weshalb das Licht nicht nach außen verloren geht.
12. Erkläre, warum das Verbinden von Leiterstücken (´Spleißen´) bei LWL viel schwieriger ist, als bei Kupferkabeln.
13. Erkläre die Begriffe: FTTH, FTTD.
14. Erkläre den Begriff *Strukturierte Verkabelung*.
15. Erkläre die Funktion eines *Medienkonverters* und weshalb er eingesetzt wird.
16. Erkläre den Begriff WLAN.
17. Nenne Nachteile von WLAN Funknetze gegenüber kabelgebundenen Netzen.
18. Nenne Vorteile von WLAN-Lösungen
19. Erkläre einem Nutzer, der sich über langsame Verbindungsgeschwindigkeiten im Netz beklagt den Grund dafür. Kläre ihn darüber auf, welchen Datendurchsatz er realistisch erwarten kann.
20. Erkläre, warum bereits wenige cm neben einem Empfangsmaximum ein Minimum liegen kann.
21. Erkläre die Begriffe *Polarisation* und *Diversity*
22. Worin liegt das grundsätzliche Sicherheitsrisiko im WLAN?
23. Nenne Maßnahmen zu Erhöhung der Sicherheit im WLAN.