
Bibliothek des technischen Wissens

# Fachwissen Netzwerktechnik

## Modelle · Geräte · Protokolle

Bernhard Hauser

**2. Auflage**

VERLAG EUROPA-LEHRMITTEL · Nourney, Vollmer GmbH & Co. KG
Düsselberger Straße 23 · 42781 Haan-Gruiten

**Europa-Nr.: 54012**

Autor:
Hauser, Bernhard Dipl.-Ing. Bisingen

Verlagslektorat:
Alexander Barth Dipl.-Ing. Haan

Bildentwürfe: Der Autor

Bildbearbeitung:
Wissenschaftliche PublikationsTechnik Kernstock, 73230 Kirchheim/Teck
Zeichenbüro des Verlags Europa-Lehrmittel GmbH & Co. KG, Ostfildern

Fotos:
siehe Seite 244

2. Auflage 2015

Druck 5 4 3 2 1

Alle Drucke derselben Auflage sind parallel einsetzbar, da sie bis auf die Behebung von Druckfehlern untereinander unverändert sind.

ISBN 978-3-8085-5402-9

Umschlaggestaltung: Grafische Produktionen Jürgen Neumann, Rimpar und Grafik & Sound, Köln.



http://www.Europa-Lehrmittel.de

Satz: Wissenschaftliche PublikationsTechnik Kernstock, 73230 Kirchheim/Teck

Druck: Konrad Triltsch, Print und digitale Medien GmbH, 97199 Ochsenfurt-Hohestadt

# Vorwort

Die moderne Netzwerk- und Kommunikationstechnik hat Einzug in alle Lebensbereiche gehalten. Ein Alltag ohne Kommunikationsnetze ist kaum mehr denkbar. Die stetig fortschreitende Vernetzung in unserem Alltag sowie die schnelle Entwicklung der Technik sorgen dafür, dass ein solides Grundwissen in diesem Bereich immer wichtiger wird.

Dieses Fachbuch **„Fachwissen Netzwerktechnik – Modelle · Geräte · Protokolle“** wendet sich an alle Leserinnen und Leser, die die Grundlagen der zeitgemäßen Netzwerktechnik lernen und verstehen möchten. Es führt die wesentlichen Begriffe ein, stellt wichtige Zusammenhänge dar und legt somit die Basis für alle, die tiefer in die Themen einsteigen möchten.

Es eignet sich daher für **Auszubildende der IT-Berufe** wie **Fachinformatiker**, **Informatikkaufleute**, **Informationselektroniker**, für **Techniker** der Elektro- und Datentechnik sowie **Studenten technischer Fächer**, für die Kenntnisse in Netzwerkgrundlagen inzwischen unabdingbar sind.

Das Buch gliedert sich in folgende Kapitel:



Mit einer bewusst verständlich gehaltenen Sprache bietet das Buch einen leichten Zugang. Zahlreiche **Abbildungen** und **Tabellen** sowie praxisnahe **Beispiele** unterstützen die Vermittlung des Stoffes. Zahlreiche **Merksätze** tragen zum Lernerfolg bei. Am Ende der jeweiligen Kapitel kann mithilfe von **Übungsaufgaben** der eigene Kenntnisstand überprüft werden.

In der überarbeiteten **zweiten Auflage** wurden die Multiplextechniken um Codemultiplex erweitert, um den aktuellen Entwicklungen auf dem Gebiet der Mobilfunktechnik gerecht zu werden. Um noch mehr Praxisbezug herzustellen, wurde das NAT-Routing erweitert und die IP-Konfiguration ergänzt.

Wir wünschen den Leserinnen und Lesern viel Freude und Erfolg mit diesem Werk.

Ihre Meinung interessiert uns! Hinweise und Verbesserungsvorschläge werden unter lektorat@europa-lehrmittel.de dankbar entgegengenommen.

Winter 2014/2015 Autor & Verlag

# Inhaltsverzeichnis

## 2.1.7 Mischtopologien

### Bus-Bus und Bus-Stern

*__Mischtopologien__ sind möglich.*

In der Regel kommen **Mischtopologien** vor, d.h., eine oder mehrere der Grundtopologien werden miteinander kombiniert. Früher war der Bus-Bus und später der Bus-Stern weit verbreitet. Heute herrscht der *Extended Star* vor. Bustopologien sind heute in Verkabelungen sehr ungebräuchlich, aber in Altinstallationen noch anzutreffen.

*__Backbone:__ Rückgrat*

Reine Busverkabelungen sind sehr veraltet. Mit dem Aufkommen der Twisted-Pair-Verkabelungen kam auch die Sterntopologie auf. Häufig wurde im **Backbone**-Bereich wegen längerer Kabelstrecken eine Koaxialleitung als Busleitung benutzt, und daran waren Sternverkabelungen angeschlossen, die die Stockwerke und Räume erschlossen.

### Erweiterter Stern

*__Erweiterter Stern:__ die Standard-Topologie in Netzen*

Der **Erweiterte Stern**, engl. *extended star*, ist die heute vorherrschende Topologie im LAN. Anstelle eines Rechners oder eines Endgerätes wird ein weiterer Sternkoppler angeschlossen (Bild 2.6).

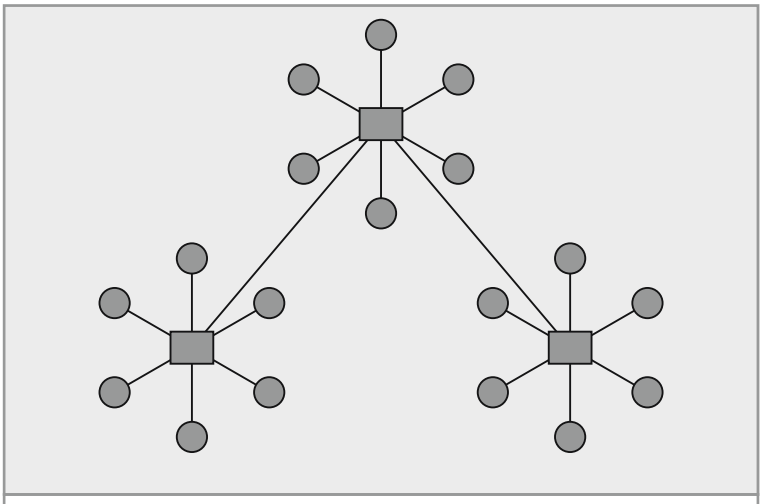


**Bild 2.6: Erweiterter Stern**

*__Baumtopologie__ ist in Wirklichkeit ein erweiterter Stern!*

Gelegentlich hört und liest man auch von der **Baumtopologie**. Diese ist nichts anderes als ein *extended star*. Eine Baum-Verkabelung gibt es nicht, auch wenn sie in Lehrbüchern gelegentlich beschrieben wird.

### Stern-Zell-Topologie

*Typisches Funknetz: Stern-Verkabelung mit Funkzellen.*

Die Kombination aus drahtgebundener Sterntopologie und drahtloser Zelltopologie wird eingesetzt bei WLANs, DECT-Telefonie und Mobilfunknetzen (Bild 2.7).

### Sonstige Mischtopologien

Beliebige andere Kombinationen von Grundtopologien wie Stern-Ring, Ring-Bus usw. sind möglich und sicher auch in einer vorhandenen

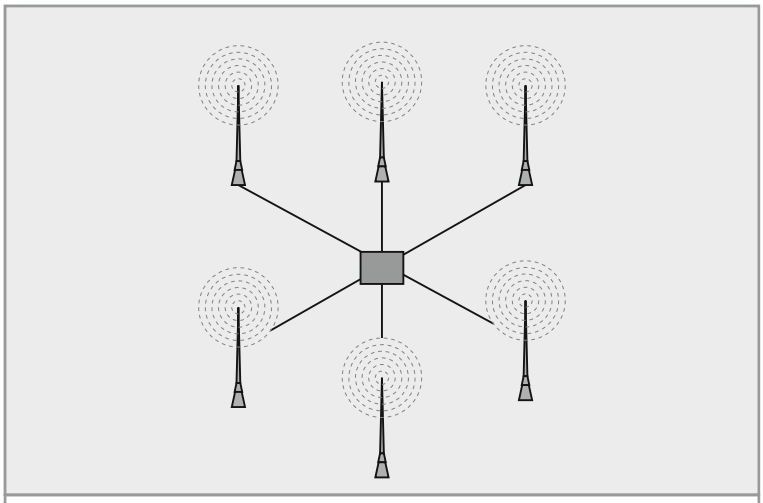


**Bild 2.7: Stern-Zell-Netz**

Installation zu finden. Komplexe Strukturen aus Bus-Ring-Stern-Masche-Zelle sind ebenso möglich.

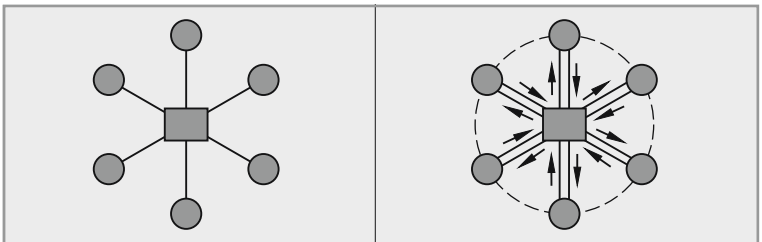
### Logische und physikalische Topologien

***Logische Topologie:*** *Wie ist der Datenfluss?*

***Physikalische Topologie:*** *Wie ist die Leitungsführung?*

Bei der Beschreibung der Topologie muss man zwischen der **logischen** und der **physikalischen Topologie** unterscheiden. Unter der logischen Topologie versteht man den Weg, den die Datenpakete nehmen. Die physikalische Topologie ist die Leitung, die Hardware. Eine Verkabelung kann durchaus anders aussehen, als sie funktioniert; man muss sich eine Verkabelung und Verschaltung schon genauer ansehen, um zu verstehen, um welche Art von logischer Topologie es sich handelt.

**Beispiel 2.1:**
In Bild 2.8, links, wird ein Netzwerk sternförmig verkabelt. Im Sternmittelpunkt befindet sich ein Sternkoppler, der alle Leitungen miteinander verbindet. Wenn alle Leitungen miteinander verbunden sind, hat man einen Bus, ein *shared media* – ein geteiltes Medium. Es handelt sich hierbei also um eine physikalische Sternverkabelung (da die Leitungen sternförmig verschaltet sind) und um eine logische Busverkabelung (da alle Leitungen parallel geschaltet sind).



(a) Physikalischer Stern – Hub als Sternkoppler – Logischer Bus

(b) Physikalischer Stern – Logischer Ring

**Bild 2.8: Logische und physikalische Topologie**

**Beispiel 2.2:**
In Bild 2.8 rechts wird ein Ringnetzwerk so verkabelt, dass die Sende- und Empfangsleitungen jeder Station in einem Kabel zusammengefasst werden. Über einen Sternkoppler werden diese Leitungen sternförmig zusammengeschaltet, wobei weiterhin die Stationen hintereinander geschaltet werden. Es handelt sich hierbei also um einen logischen Ring und um eine physikalische Sternverkabelung.

## 2.2 Zugriffsverfahren

Am Anfang war die Busverkabelung – ein *shared media*, ein gemeinsam genutztes Medium. Wie leicht einzusehen ist, kann auf einer Busleitung immer nur eine Station senden, die anderen müssen ruhig sein und dürfen nicht zur gleichen Zeit senden. Sobald zwei oder mehrere Stationen gleichzeitig senden, überlagern sich deren Signale auf der Leitung, sodass ein fehlerfreier Empfang der Daten nicht mehr gewährleistet ist. (Wenn in einem Klassenzimmer mehrere Lehrer gleichzeitig reden, versteht kein Schüler mehr, was gesagt wird.)

Es muss also ein Verfahren zum Einsatz kommen, welches den Zugriff auf das gemeinsame Medium regelt, sodass immer nur eine Station sendet.

*Es muss geregelt werden, wer wann das Medium benutzen darf.*

Man kann die Rede- bzw. Sendeerlaubnis von einer Zentralstelle aus steuern, so wie beispielsweise der Bundestagspräsident den Abgeordneten das Wort erteilt. Man kann auch Regeln erlassen, wer wann senden darf (man denke hier nur an das beliebte Managerspiel: Man sitzt im Stuhlkreis und wirft sich einen Gummiball zu; wer den Ball hat, der darf reden).

Im LAN haben sich 3 Verfahren durchgesetzt:

- CSMA/CD
- CSMA/CA und
- Token Passing

### 2.2.1 CSMA/CD

***CSMA/CD** ist Standard in leitungsgebundenen Netzen.*

Das **CSMA/CD**-Verfahren ist das Zugriffsverfahren bei leitungsgeführten Ethernet-Netzwerken. Das Verfahren ist ganz simpel und deshalb auch sehr effektiv. Die Abkürzung steht für *Carrier Sense Multiple Access / Collision Detection*, was soviel bedeutet wie: Trägererkennung auf einem Medium mit Mehrfachzugriff und Kollisionserkennung.

CSMA/CD funktioniert wie eine Schulklasse (funktionieren sollte). Derjenige, der etwas sagen möchte, redet nicht einfach darauf los. Er hört erst eine Weile in den Raum (*carrier sense*) und bleibt ruhig, solange noch geredet wird. Prinzipiell kann jeder reden (*multiple access*). Erst wenn er sich sicher ist, dass kein anderer redet, kann er selbst anfangen zu reden. Wenn er redet, hört er weiterhin in den Raum, um sicher zu stellen, dass er der einzige ist, der redet. Stellt er fest, dass ein anderer dazwischen redet, unterbricht er sofort seine Rede, da sie durch das Zwischengerede des anderen von den restlichen Zuhörern nicht mehr korrekt empfangen werden konnte (*collision detection*).

*Abbrechen der Übertragung bei Kollision, Zufalls-Wartezeit abwarten und erneut versuchen.*

Soweit ist alles logisch und einfach geregelt. Der Clou an dem Verfahren setzt aber dann ein, wenn eine Kollision auftritt, wenn also mehrere

Schüler gleichzeitig reden bzw. mehrere Stationen gleichzeitig senden. Als Reaktion auf die Kollision wird nicht nur die Sendung unterbrochen, es wird sogar ein Warnsignal gesendet, das Jam-Signal. Vergleichbar wäre dies etwa mit dem Pfeifen mit einer Trillerpfeife, sobald eine Kollision auftritt. Spätestens jetzt hört auch der Störer auf zu reden. Nun beginnt eine Wartezeit und die unterbrochene Station darf nicht sofort wieder anfangen zu senden. Damit die beiden Redner oder die beiden Stationen nicht wieder gleichzeitig anfangen zu senden, läuft bei jeder Station eine andere Wartezeit. Die Wartezeit wird durch einen Zufallsgenerator festgelegt. Nach Ablauf der Wartezeit beginnt die ganze Prozedur von vorne, d. h. Hören, ob das Medium frei ist und so weiter (siehe Bild 2.9).

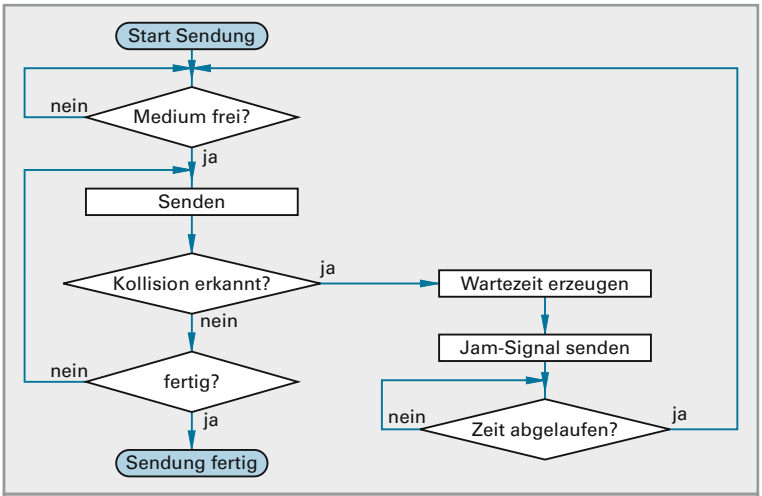



**Bild 2.9: Prinzipieller Ablauf des CSMA/CD-Verfahrens**

## 2.2.2 CSMA/CA

*__CSMA/CA__: Standard in Funknetzen*

Ein anderes Zugriffsverfahren ist das **CSMA/CA**-Verfahren. Diese Abkürzung steht für *Carrier Sense Multiple Access / Collision Avoidance*, also Kollisionsverhinderung anstelle der Kollisionserkennung. Dieses Verfahren ist deutlich komplizierter als das CD-Verfahren und verursacht zusätzlichen Netzwerkverkehr. Dieses Verfahren muss eingesetzt werden, wenn das Erkennen von Kollisionen nicht möglich ist. Bei Funknetzen kann die Sendestation nicht erkennen, ob eine andere Station gleichzeitig sendet. Hier kommt das CA-Verfahren zum Einsatz. Kollisionen können hier nicht vollständig verhindert werden, aber die Anzahl der Kollisionen kann reduziert werden. Vor jeder Übertragung prüft die sendewillige Station, ob das Medium frei ist (*listen before talk*). Dazu hört diese Station für eine gewisse Zeit das Medium ab. Die Dauer des Abhörens entspricht der IFS-Zeit (*interframe-spacing-Zeit*), der Zeit zwischen zwei Datenpakenten (eine Art Sicherheitsabstand zwischen den Paketen). Ist das Medium nach dieser Zeit immer noch frei, so ist die Wahrscheinlichkeit, dass es tatsächlich frei ist, ziemlich groß und die Übertragung kann beginnen.

*„listen before talk“: erst hören, dann reden*

Ist das Medium aber besetzt, so stellt die Station die Übertragung für eine bestimmte Wartezeit zurück.

*„Hidden-Station-Problem“: zwei Stationen sehen sich nicht, wenn die Entfernung zu groß ist.*

Folgendes Problem wird damit aber nicht gelöst (Bild 2.10): Zwei Stationen in derselben Zelle liegen beide nahe genug am Accesspoint, um mit ihm zu kommunizieren. Sie liegen aber zu weit auseinander, als dass die eine Station bemerken kann, wann die andere sendet. Deshalb kommt hier noch ein weiterer Mechanismus ins Spiel. Die sendewillige Station schickt, nachdem sie das Medium als nicht belegt überprüft hat, eine Sendeanfrage an den Empfänger, also den Accesspoint. Dieser beantwortet die Sendeanfrage (*Request to Send*, RTS) mit einer Sendefreigabe (*Clear to Send*, CTS), wenn diese senden darf. Klappt dieser RTS-CTS-Austausch problemlos, so kann die Sendestation nach Ablauf einer weiteren Wartezeit mit der eigentlichen Sendung beginnen. Klappt dieser RTS-CTS-Austausch nicht, so beginnt das Verfahren nach einer zufälligen Wartezeit wieder ganz von vorne.

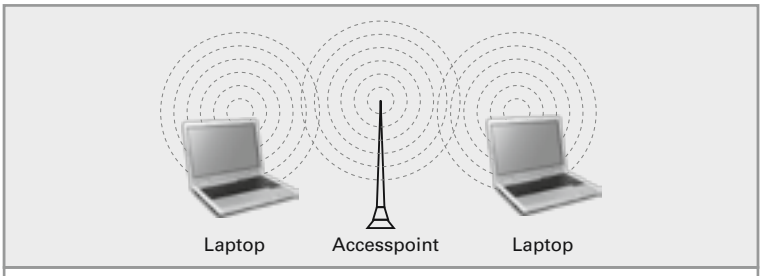



**Bild 2.10: Laptops und Accesspoint**

### 2.2.3 Token Passing

*Nur wer den Token hat, darf senden.*

Das englische Wort *Token* bedeutet auf Deutsch soviel wie Pfand. Token-Ring ist der bekannteste Vertreter dieser Technologie, wenngleich nicht mehr sehr gebräuchlich. Der Token-Bus gehört der Vergangenheit an. Das Verfahren besticht durch seine Einfachheit. Ein Token ist nichts anderes als ein elektronisches Telegrammformular. Es kreist im Ringnetzwerk und wird von Station zu Station weitergeschickt. Es darf zur selben Zeit nur einen Token geben. Wenn eine Station senden will, dann muss sie warten, bis der (leere) Token bei ihr vorbeikommt. Dann füllt sie ihn mit Daten. Sie trägt wie auf einem Telgrammformular die Empfänger- und die Absenderadresse sowie die zu übertragenden Nutzdaten ein. Dieser Token kreist nun genau ein Mal im Netz, bis er wieder beim Absender ankommt. Dieser löscht dann die Inhalte aus dem Formular und schickt das leere Formular weiter. Wenn keine Station senden möchte, dann kreist der Token leer im Netzwerk.

## 2.3 UGV – Universelle Gebäudeverkabelung

### 2.3.1 Strukturierte Verkabelung

*Eine klare Struktur dient dem Verständnis.*

Universelle Gebäudeverkabelung wird oft auch als *„strukturierte diensteneutrale Verkabelung“* bezeichnet. Um ein Netzwerk professionell und auch kostengünstig über viele Jahre betreiben zu können, ist eine klare

Struktur der Netzwerkverkabelung absolut notwendig. Diensteneutral bedeutet in Bezug auf Netzwerkverkabelung, dass die Verkabelung unabhängig von dem Dienst ist, der die Leitungswege benutzt. Über die bisher übliche Telefonverkabelung kann man nur Dienste mit geringer Bandbreite benutzen, wie eben Telefon und Fax. Eine zukunftsfähige Verkabelung muss aber alle heutigen Dienste wie Computernetzwerk, Video und eben auch Telefon bedienen können. Statt einer separaten Verkabelung für jeden gewünschten Dienst wird in einer strukturierten, diensteneutralen Verkabelung nur eine Verkabelung realisiert, auf welcher dann die unterschiedlichsten Geräte angeschlossen werden.

*Unterschiedliche Dienste auf einer Verkabelung.*

Selbstverständlich ist eine gute Netzwerkleitung teurer als eine Telefonleitung. Betrachtet man aber die Gesamtkosten (*Total Cost of Ownership* TCO), so ist eine einheitliche Verkabelung jedoch deutlich billiger als zwei getrennte Verkabelungen.

Die Normen EN 50173-1 bzw. ISO/IEC 11801 regeln den Aufbau einer Kommunikationsverkabelung. Die Gesamtverkabelung wird in drei Bereiche eingeteilt:

- Primärbereich
- Sekundärbereich
- Tertiärbereich

***Primärbereich:*** *Standort-Verkabelung*

Der erste Bereich, die **Primärverkabelung** eines Firmennetzwerkes, ist die Standortverkabelung. Im Primärbereich werden von einem Standortverteiler aus die einzelnen Gebäude auf einem Firmengelände miteinander angeschlossen. Diese Verkabelung wird oft auch *Backbone* (Rückgrat) bezeichnet. Ausgehend von einem Standortverteiler werden alle Gebäude sternförmig angeschlossen (Bild 2.11).

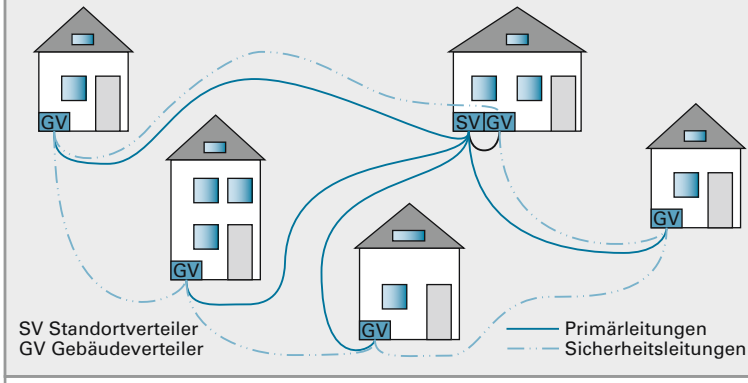



**Bild 2.11: Primärverkabelung, Standortverkabelung**

***Sekundärbereich:*** *Gebäude-Verkabelung*

Der zweite Bereich, die **Sekundärverkabelung** eines LANs, ist die Gebäudeverteilung. Im Sekundärbereich werden von einem Gebäudeverteiler aus die einzelnen Stockwerke angeschlossen. Diese Verkabelung nennt man oft auch Vertikal-Verkabelung und die Leitungen nennt man Steigleitungen, da die Leitungen von unten nach oben verlaufen (Bild 2.12).

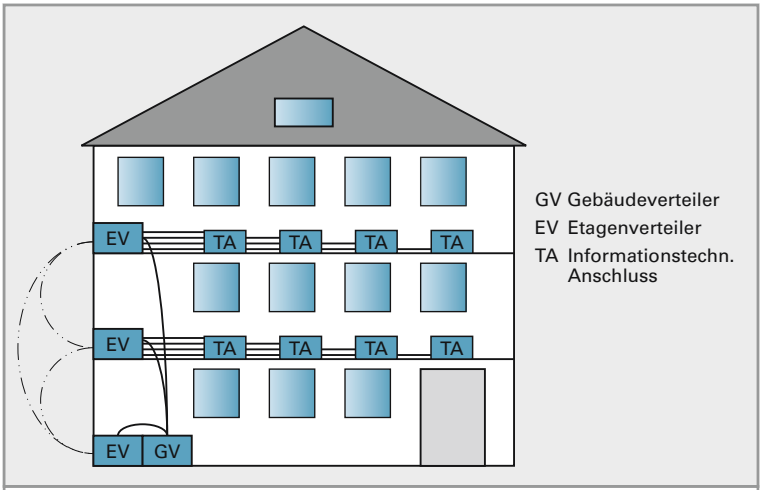



**Bild 2.12: Sekundär- und Tertiärverkabelung im Gebäude und auf der Etage**

***Tertiärbereich:*** *Etagen-Verkabelung*

Der dritte Bereich, die **Tertiärverkabelung** eines LANs, ist die Etagenverteilung. Im Tertiärbereich werden von einem Etagenverteiler aus die Steckdosen in den Büros usw. angeschlossen. Diese Dosen nennt man TAs (TA: Technischer Anschluss). Diese Verkabelung nennt man oft auch Horizontal-Verkabelung, bei der die Leitungen auf einer Ebene, dem Stockwerk, verlegt werden.

*Jede Verkabelungsebene ist eine Sterntopologie. Zusammen ergibt sie einen erweiterten Stern.*

Die übliche Topologie ist der Stern. Ausgehend vom Standortverteiler werden sternförmig die Gebäudeverteiler angefahren. Vom Gebäudeverteiler aus werden die Etagenverteiler eines jeden Gebäudes wieder sternförmig angefahren. Von jedem Etagenverteiler aus werden nun die TAs wiederum sternförmig angeschlossen (Bild 2.13).

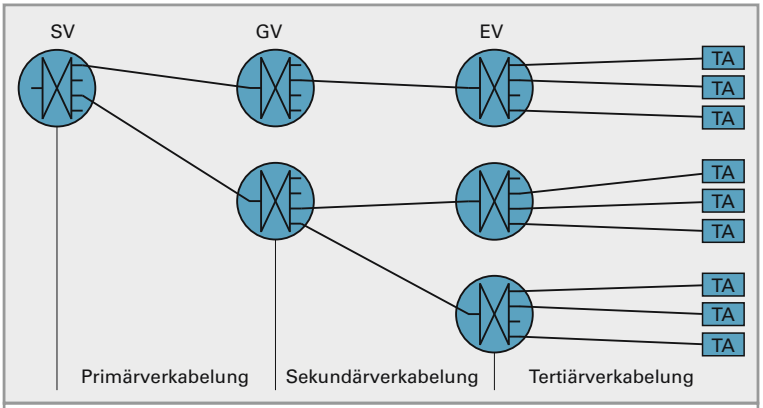



**Bild 2.13: Strukturierte Verkabelung – Erweiterter Stern**

Die Gesamttopologie ist also ein Erweiterter Stern. Es ergibt sich bei dieser Verkabelung folgendes Problem:

*Querverbindungen dienen der Ausfallsicherheit.*

Wird eine Leitung im Primärbereich, beispielsweise durch Kabelbruch unbrauchbar, dann ist ein ganzes Gebäude vom restlichen Firmennetzwerk isoliert.

Die Lösung ist sehr einfach: Man verbindet die Gebäude nach Möglichkeit auch mit ihren Nachbarn durch Reserveleitungen. Diese Leitungen sind im Regelfall unbenutzt. Im Fehlerfall können sie aber aktiviert werden, sodass das isolierte Gebäude über einen Umweg wieder mit dem restlichen LAN verbunden wird. Die daraus resultierende Topologie ist dann eine unvollständige Masche. Wie dies aber genau gemacht wird, wird im Kapitel über Switches beim Spanning-Tree-Verfahren erläutert. Hier dazu nur soviel: Es funktioniert automatisch, ohne dass Leitungen im Fehlerfall von Hand umgesteckt werden müssen.

*Die Querverbindungen werden von den Switches bei Bedarf automatisch aktiviert.*

Innerhalb eines Gebäudes hat man dasselbe Problem und auch hier dieselbe Lösung. Die Etagenverteiler werden ebenfalls miteinander verbunden.

*Querverbindungen bilden Maschen.*

Bei kleineren Netzen wird natürlich nur ein Teilbereich der Verkabelung realisiert, abhängig von den Bedürfnissen. In einer Arztpraxis mit mehreren Zimmern auf einem Stockwerk wird natürlich nur ein Etagenverteiler und die Tertiärverkabelung realisiert. Eine Firma mit einem mehrstöckigen Gebäude wird einen Gebäudeverteiler, die Sekundärverkabelung, die Etagenverteiler und die Tertiärverkabelung bekommen.

Wichtig ist, dass die Verkabelung des Netzwerkes, egal wie groß das Netzwerk auch ist, von Anfang an sauber dokumentiert wird. Die Lage der Verteiler, der Verlauf der Leitungswege und die Lage der TAs müssen in Plänen (am besten den Architektenplänen) eingetragen werden. Erweiterungen und Änderungen an der Verkabelung müssen immer sofort in den Plänen nachgetragen werden, damit immer aktuelle Unterlagen vorhanden sind.

Welche Leitungen in welchem Bereich verwendet werden, hängt von den Anforderungen des Netzwerkbereibers und von den örtlichen Gegebenheiten ab. Als Richtwert kann man sagen, dass die Primärverkabelung in Lichtwellenleitern (Glasfasern) ausgeführt wird. Oft kommen hier Singlemode-Fasern zum Einsatz. Die Sekundärverkabelung wird in der Regel auch in Lichtwellenleitern ausgeführt. Hier wird meist Multimodefaser eingesetzt. Der Endbereich, die Tertiärverkabelung, wird in Kupferleitungen ausgeführt. Hier können Leitungen der Kategorie 6, 7 oder 8 oder auch Wireless-LAN eingesetzt werden.

*Der Einsatzbereich entscheidet, welche Leitungen eingesetzt werden.*

*Die Kategorie beschreibt die Leistungsfähigkeit der Leitung.*

**Bild 2.14: Verteilerschrank**

### Beschriftung von TAs und Verteilerschränken

Um das Ziel der strukturierten Verkabelung zu erreichen, muss die gesamte Verkabelung dokumentiert werden. Dazu dienen Lagepläne vom Architekten, in die Verteiler, Dosen und die Leitungsführung eingezeichnet werden.

*Dokumentation und Beschriftung ist notwendig und hilfreich.*

Pläne allein reichen aber nicht aus. Die Komponenten müssen

gut sichtbar beschriftet werden. Dazu verwendet man gut haftende Aufkleber.

Jeder Verteilerschrank wird eindeutig gekennzeichnet, beispielsweise mit SV für Standortverteiler, GV1, GV2, usw. für Gebäudeverteiler, EV1, EV2, usw. für die Etagenverteiler.

Jedes Steckfeld in den Verteilern wird ebenfalls gekennzeichnet. Hier werden am einfachsten die Steckfelder von oben nach unten durchnummeriert. Die einzelnen Steckplätze sind in der Regel auf dem Steckfeld nummeriert.

Die TAs werden ebenfalls gekennzeichnet. Sie tragen die Nummer der Buchse im Etagenverteiler, auf der ihre Leitung endet.

**Beispiel**: Der TA mit der Bezeichnung EV2.5.12 ist mit der Buchse 12 des 5. Patchfeldes im Etagenverteiler 2 verbunden.

### Die Cisco-Einteilung

*Die Firma **Cisco** ist ein großer Pionier auf dem Gebiet der Netzwerktechnik.*

**Cisco** teilt eine Firmenverkabelung ebenso in drei Bereiche ein:

- Core layer
- Distribution Layer
- Access Layer

Im Core-Layer befinden sich sehr leistungsstarke Switches oder Router. Sie kommen üblicherweise im Primärbereich zum Einsatz.

Im Distribution-Layer werden Switches mit guter Leistungsfähigkeit eingesetzt – also üblicherweise im Sekundär-Bereich.

Als Access-Layer wird die Tertiärverteilung bezeichnet. Hier werden Endgeräte mit typischerweise 100 Mbps oder 1 Gbps angeschlossen.

## 2.3.2 Netzklassen und -kategorien

*Die Klasse spezifiziert die Gesamtverkabelung.*

Die Leistungsfähigkeit einer Netzwerkverkabelung mit symmetrischen Kupferleitungen wird in Netzwerk-Anwendungs-Klassen A bis F eingeteilt (Tabelle 2.1). Dabei werden ausschließlich die passiven Netzkomponenten bewertet.

**Tabelle 2.1: Netzanwendungsklassen**

| Klasse | Frequenzbereich | Anwendungen |
|---|---|---|
| A | ≤ 100 kHz | niederfrequente Anwendungen (z. B. Telefon, Fax) |
| B | ≤ 1 MHz | Anwendungen mit niedriger Bitrate (z. B. ISDN) |
| C | ≤ 16 MHz | Anwendungen mit hoher Bitrate (z. B. Ethernet) |
| D | ≤ 100 MHz | Anwendungen mit sehr hoher Bitrate (z. B. Fast-Ethernet oder Gigabit-Ethernet) |
| E | ≤ 250 MHz | Anwendungen mit sehr hoher Bitrate (z. B. Fast-Ethernet, Gigabit-Ethernet oder 10-Gigabit-Ethernet, Kabelfernsehen) |
| $E_A$ | ≤ 500 MHz | Anwendungen mit sehr hoher Bitrate (z. B. Fast-Ethernet, Gigabit-Ethernet oder 10-Gigabit-Ethernet, Kabelfernsehen) |
| F | ≤ 600 MHz | reserviert für künftige Anwendungen |
| $F_A$ | ≤ 1000 MHz | reserviert für künftige Anwendungen |

Eine höhere Klasse einer Verkabelungsstrecke beinhaltet auch die Anforderungen an die darunter liegenden Klassen – sie sind also abwärtskompatibel. Bei den Steckern und Buchsen ist dies jedoch ab Klasse F nicht mehr gegeben, wohl aber für die Verkabelung.

Tabelle 2.2 zeigt eine Übersicht mit den wichtigsten nationalen und internationalen Normen für strukturierte Verkabelungen.

**Tabelle 2.2: Übersicht wichtiger Normen im Verkabelungsbereich – Normen für strukturierte Verkabelungen**

| Netzwerkklasse | D | E | $E_A$ | F | $F_A$ |
|---|---|---|---|---|---|
| Bandbreite | 100 MHz | 250 MHz | 500 MHz | 600 MHz | 1000 MHz |
| USA-Normen | TIA/EIA 568 B.2-1:2002 CAT5e | TIA/EIA 568 B.2-1:2002 CAT6 | TIA/EIA 155 CAT6 Mitigaton | | |
| | | | TIA/EIA 568 B.2-1:2002 CAT6A (augmented CAT6) | | |
| Internationale Normen | ISO/IEC 11801 Ed.2:2002 CAT5/Klasse D | ISO/IEC 11801 Ed.2:2002 CAT6/Klasse E | ISO/IEC 11801:2002 Amd.1:2008 Channel Class $E_A$ | ISO/IEC 11801 Ed.2:2002 CAT7 / Klasse F | ISO/IEC 11801:2002 Amd.1:2008 Channel Class $F_A$ |
| | | | ISO/IEC 11801:2002 Amd.2:draft – Link Class $E_A$, CAT6A | | ISO/IEC 11801 Ed.2:2002 Amd.2:draft – Link Class $F_A$, CAT7A |
| | | | ISO/IEC TR> 24750 CAT6 / Class E Mitigaton | | |
| EU-Normen | | EN 50173-1...5:2007 CAT6 / Class E | EN 50173-1 Beiblatt 1:2008 Class $E_A$-Channel | EN 50173:2007 CAT7/ Class F | EN 50173-1 Beiblatt 1:2008 Class $F_A$-Channel |
| | | | prTR50173-99-1^CAT6 Mitigaton für 10G Base-T | | |

### Leitungskategorien

***Kategorien** spezifizieren einzelne Leitungen, Stecker, Dosen.*

Aufgrund der in einer Verkabelung verwendeten Leitung und Komponenten kann die Netzwerkanwendungsklasse festgelegt werden (Tabelle 2.3). Die endgültige Einteilung in eine Klasse kann aber nur über einen messtechnischen Nachweis erfolgen. D.h., jede Verkabelungsanlage muss, auch bei sorgfältigster Planung und Installation, vor der Übergabe an den Kunden vermessen werden! Die Messprotokolle sind dem Betreiber der Kabelanlage zu übergeben. Anhand dieser Protokolle kann später entschieden werden, ob eine neue Anwendung auf der bestehenden Anlage betrieben werden kann oder nicht.

**Tabelle 2.3: Leitungs-Kategorien**

| Kategorie | Frequenzbereich | Anwendung | geeignet für Klasse |
|---|---|---|---|
| 3 | ≦ 16 MHz | Telefon, Token-Ring, Ethernet | C |
| 5 | ≦ 100 MHz | Fast Ethernet, Gigabit-Ethernet | D |
| 6 | ≦ 250 MHz | Gigabit-Ethernet, 10-Gigabit-Ethernet | D, E |
| $6_A$ | ≦ 625 MHz | Gigabit-Ethernet, 10-Gigabit-Ethernet | D, E, $E_A$ |
| $6_E$ | ≦ 500 MHz | Gigabit-Ethernet, 10-Gigabit-Ethernet | D, E, $E_A$ |
| 7 | ≦ 600 MHz | 10-Gigabit-Ethernet, Kabelfernsehanlagen | D, E, $E_A$, F |
| $7_A$ | ≦ 1000 MHz | 10-Gigabit-Ethernet, Kabelfernsehanlagen | D, E, $E_A$, F, $F_A$ |

## 2.3.3 Abnahmemessung

*Jede Installation muss durchgemessen und abgenommen werden.*

Nach Fertigstellen einer Verkabelung muss diese durchgemessen werden. Das sorgfältige Aussuchen der verwendeten Komponenten ist Grundvoraussetzung, um eine bestimmte Netzwerkklasse zu erreichen.

**Beispiel 5.1:**
An einem PC ist ein Browserfenster geöffnet und es wird eine Domain-Adresse ins Adressfeld eingegeben. Dann startet der PC zuerst die Namensauflösung, um die IP-Adresse der Domäne zu erfragen. Diese Anfrage schickt er mit seinem Absender-Port 53 (für DNS) an den DNS-Server aus seiner Netzwerkkonfiguration. Als Ziel-Port wird auch der Port 53 angegeben, weil auf diesem Server vielleicht noch andere Anwendungen laufen. Dadurch wird der DNS-Dienst auf diesem Server adressiert.

Der DNS-Server schickt nun die angefragte IP-Adresse an den PC zurück und adressiert wiederum den dortigen DNS-Port.

Dann startet der PC seine eigentliche Anfrage. Er adressiert die Anfrage an den Ziel-Server und schickt dabei die Portnummer des angefragten Dienstes mit, hier also Port 80 für HTTP. Der Absenderport ist ebenfalls HTTP.

Auf einem Unix-Rechner ist diese Liste in der Datei `/etc/services` definiert.

Unter Betriebssystemen der Windows-NT-Linie findet sich diese unter: `\%\system32\drivers\etc\services`

Es folgt eine Liste der wichtigsten Portnummern:

**Tabelle 5.1: Einige wichtige Port-Nummern-Belegungen**

| Portnummer | Bezeichnung | Bemerkung |
|---|---|---|
| 20 | ftp-data | Datenkanal bei FTP |
| 21 | ftp-ctrl | Steuerkanal für FTP |
| 22 | ssh | Secure Shell<br>(wie Telnet – aber verschlüsselt) |
| 23 | Telnet | Terminalemulation |
| 25 | SMTP | E-Mail-Versand |
| 53 | DNS | Namensauflösung in IP-Adressen |
| 67 | DHCP | automatische IP-Adressvergabe an Clients |
| 80 | HTTP | Webserver |
| 110 | POP3 | PostOfficeProtocol, E-Mail-Verkehr |
| 123 | NTP | Network Time Protocol,<br>Zeitsynchronistation |
| 143 | IMAP | E-Mail-Verkehr |
| 443 | HTTPS | Webserver, verschlüsselt |
| 1521 | Oracle | Zugriff auf Oracle-Datenbanken |
| 1723 | VPN | Virtuelle private Netzwerke |
| 3306 | MySQL | Zugriff auf MySQL-Datenbanken |
| 3389 | RDP | Windows Remotedesktopzugriff, Windows Terminal Services |
| 5190 | ICQ | Instant-Messaging-Programm ICQ |
| 5432 | PostgreSQL | Zugriff auf PostgreSQL-Datenbanken |
| 6667 | IRC | Chatserver |

## 5.2 IP-Adressen – Network-Layer

IP-Adressen erlauben die Strukturierung des Adressraumes. Sie adressieren die Rechner auf Netzwerkebene (OSI Layer 3). Eine IP-Adresse besteht aus 4 Bytes, die durch Punkte getrennt sind:

**Beispiel 5.2:**
Die Darstellung erfolgt in dezimaler Schreibweise:
**w.x.y.z**
Beispiel: 134.103.220.250

***IP-Adressen***
*⇒ Netzwerk-Layer*

Jede Stelle kann daher Werte von 0 bis 255 annehmen. Jeder Knoten im Internet (Rechner, Server, Router usw.) ist durch eine eindeutige **IP-Adresse** identifiziert. Eigentlich müsste man nur die IP-Adressen der Internetsites eingeben, die man besuchen möchte. Zum einfacheren Merken der Rechneradressen verwendet man allerdings „sprechende Namen" wie beispielsweise ard.de oder cnn.com.

## 5.3 MAC-Adressen – Network-Access-Layer

Auf Layer 2 werden Hardware-Adressen verwendet. Jedes Netzwerkinterface hat eine eindeutige Kennung. Beim Ethernet ist diese Adresse die MAC-Adresse. MAC steht dabei für **M**edia-**A**ccess-**C**ontrol.

| | |
|---|---|
| L7 | Application |
| L6 | Presentation |
| L5 | Session |
| L4 | Transport |
| L3 | Network |
| L2 | Data Link |
| L1 | Physical |

Die MAC-Adresse ist 6 Byte groß und gliedert sich in 2 Bereiche:

| 3 Byte | 3 Byte |
|---|---|
| Vendor-ID | Serial No. |

Vendor-ID ist die 3 Byte große Herstellerkennung. Die folgenden 3 Bytes sind herstellerinterne Type- und Seriennummern.

Die Schreibweise ist hexadezimal in der Form: **xx-xx-xx-xx-xx-xx.**

Der herstellerintene Teil der MAC-ID beinhaltet meist die Typ-Kennung der Karte und die Seriennummer. Große Kartenhersteller verwenden auch mehrere Vendor-IDs.

***MAC-Adressen***
*⇒ Datalink-Layer*
*⇒ adressiert eine Netzwerkkarte*

Normalerweise sind die **MAC-Adressen** fest in die Netzwerkkarten eingebrannt und können nicht verändert werden. Bei einigen wenigen Karten lässt sich im Nachhinein dennoch die MAC-ID verändern. Allerdings lässt sich die MAC-Adresse bei fast jedem Betriebssystem sehr leicht verändern, sodass mit wenig Aufwand jedem Gerät eine beliebige MAC-Adresse gegeben werden kann.

Es existieren noch wichtige Spezialadressen, die wichtigste ist die Broadcast-Adresse. Die **Broadcast-Adresse** kann nur als Ziel-Adresse verwendet werden. Dabei sind alle 48 Bits auf High eingestellt.

***MAC-Broadcast:***
*ff-ff-ff-ff-ff-ff*

Sie lautet: **ff-ff-ff-ff-ff-ff**, alle Bits sind high.

Mit dieser Adresse werden alle Netzwerkinterfaces eines Netzes adressiert. Dies ist z. B. der Fall, wenn die Adresse eines bestimmten Rechners herausgefunden werden muss (siehe Kapitel 6.7).

***MAC-Multicast:***
*01-00-5e-ff-ff-ff*

Weitere Spezialadressen sind die **Multicast-Adressen**. Mit diesen Adressen wird jeweils eine Gruppe von Rechnern angesprochen. Eine

geläufige Multicast-Adresse lautet: **01-00-5e-xx-xx-xx**. Statt x wird die Gruppenadresse eingetragen.

Es gibt noch weitere Spezialadressen. Beispielsweise werden mit der Adresse 00-00-5E-00-01-xx sogenannte virtuelle Router angesprochen, wobei xx die Nummer des virtuellen Routers ist. Diese Technik wird bei Hochverfügbarkeits-Netzen eingesetzt. Dabei werden mehrere physikalische Router zu einem logischen, virtuellen Router zusammengeschlossen.

Hier eine kurze, unvollständige Liste von Adresskennungen:

**Tabelle 5.2: Einige MAC-Adresskennungen**

| Adresskennung | Hersteller/Funktion |
|---|---|
| 00-00-AA-xx-xx-xx | XEROX |
| 00-AA-00-xx-xx-xx | Intel |
| 02-60-8C-xx-xx-xx | 3COM |
| 00-50-8B-xx-xx-xx | Compaq |
| 00-00-5A-xx-xx-xx | Schneider & Koch |
| 00-00-0C-xx-xx-xx | Cisco |
| 01-00-5E-00-00-00<br>⋮<br>01-00-5E-FF-FF-FF | Multicast |
| 00-00-5E-00-01-xx | Virtuelle Router |
| 33-33-FF-xx-xx-xx | IPv6 Multicast |
| FF-FF-FF-FF-FF-FF | Broadcast |

## 5.4 IP-Adressklassen

Der gesamte IP-Adressbereich wurde ursprünglich in Klassen eingeteilt. Damit waren 3 Größen von Netzwerken definiert: Class A für sehr große Netzwerke (bis zu 224 Rechner), Class B für große Netzwerke (bis zu 216 Rechner) und Class C für kleine Netzwerke (mit bis zu 255 Rechnern).

Diese Einteilung wurde mit der Verknappung der IP-Adressen in den 90er Jahren bereits aufgehoben. Es soll hier zum besseren Verständnis dennoch erklärt werden.

### 5.4.1 Class A

*__Class A__ für sehr große Netze*

**Class A** zeichnet sich dadurch aus, dass das erste Bit (das höchstwertigste Bit) NULL ist. Dies wurde per Definition beim Entwickeln des Adresssystems so festgelegt.

Es ergibt sich folgendes Schema in binärer Schreibweise:
**0**nnn'nnnn.xxxx'xxxx.xxxx'xxxx.xxxx'xxxx

n steht hier für Netz-Bits. Die Bits mit x stehen für die Rechneradressen in jedem Netz.

Daraus ergibt sich ein Adressbereich von

- **0**000'0000.xxxx'xxxx.xxxx'xxxx.xxxx'xxxx
  ⇒ erste Netzadresse: 0.0.0.0 (in dezimaler Notation)

bis

- **0**111'1111.xxxx'xxxx.xxxx'xxxx.xxxx'xxxx
  ⇒ letzte Netzadresse: 127.0.0.0 (in dezimaler Notation)

In Klasse A sind also maximal 127 Netzadressen möglich. In jedem dieser Netze sind $2^{24}$ = 16 Mi Rechneradressen möglich.

*Mi: Mega Binary ist ein Binär-Präfix ⇒ 1.048.576*

Per Definition entspricht das erste **Oktett** der Netzadresse. Die restlichen 3 Oktette bilden die Host-Adressen.

*Ein **Oktett** ist eine Folge von 8 Bit.*

**Beispiel 5.3:**
Der 100. Rechner im 100. Class A Netz ist:
0110'0100.0000'0000.0000'0000.0110'0100 ⇒ 100.0.0.100

## 5.4.2 Class B

Die Adressbits der **Class B** beginnen mit der Bitfolge 10.

***Class B** für große Netze*

Es ergibt sich dadurch folgendes Schema in binärer Schreibweise:
**10**nn'nnnn.nnnn'nnnn.xxxx'xxxx.xxxx'xxxx

- **10**00'0000.0000'0000.xxxx'xxxx.xxxx'xxxx
  ⇒ erste Netzadresse: 128.0.0.0
- **10**11'1111.1111'1111.xxxx'xxxx.xxxx'xxxx
  ⇒ letzte Netzadresse: 191.255.0.0

Damit sind in Klasse B maximal $2^{14}$ Netzadressen möglich. In jedem dieser Netze sind $2^{16}$ = 64 Ki Rechneradressen möglich.

*Ki: Kilo Binary ist ein Binär-Präfix ⇒ 1024*

Per Definition bilden die ersten zwei Oktette die Netzadresse. Die restlichen 2 Oktette bilden die Host-Adressen.

### 5.4.3 Class C

*__Class C__ für kleine Netze*

**Class C** beginnt mit der Bitfolge 110.

Daraus ergibt sich dieses binäre Adressschema:
**110**n'nnnn.nnnn'nnnn.nnnn'nnnn.xxxx'xxxx

- **110**0'0000.0000'0000.0000'0000.xxxx'xxxx
  ⇒ erste Netzadresse: 192.0.0.0
- **110**1'1111.1111'1111.1111'1111.xxxx'xxxx
  ⇒ letzte Netzadresse: 223.255.255.0

Klasse C umfasst somit eine große Anzahl von Netzen, die relativ wenig Rechneradressen enthalten. Es sind also maximal $2^{21}$ = 2 Mi Netzadressen möglich.

In jedem dieser Netze sind $2^8$ = 256 Rechneradressen möglich.

Per Definition bilden hier die ersten drei Oktette die Netzadresse. Das restliche 4. Oktett bildet die Host-Adressen.

*__Class D__ für Multicast – Internet-TV, Web-radio, usw.*

### 5.4.4 Class D

Für die Klasse D gilt folgender Bereich:
**1110**'xxxx.xxxx'xxxx.xxxx'xxxx.xxxx'xxxx

- **1110**'0000.0000'0000.0000'0000.0000'0000
  ⇒ erste Netzadresse: 224.0.0.0
- **1110**'1111.1111'1111.1111'1111.1111'1111
  ⇒ letzte Netzadresse: 239.255.255.255

*__Class E__ nur für Forschungszwecke*

### 5.4.5 Class E

Die Klasse E umfasst schließlich diesen Bereich:
**1111**'xxxx.xxxx'xxxx.xxxx'xxxx.xxxx'xxxx

- **1111**'0000.0000'0000.0000'0000.0000'0000
  ⇒ erste Netzadresse: 240.0.0.0
- **1111**'1111.1111'1111.1111'1111.1111'1111
  ⇒ letzte Netzadresse: 255.255.255.255

Die Klassen A, B und C werden als Unicast-Adressen verwendet. Dies sind die „normalen" IP-Adressen im Netz.

Klasse D-Adressen sind Multicast-Adressen. Sie werden beispielsweise für Webradio und IP-Fernsehen verwendet.

*__IETF:__ Internet Engineering Task Force, die sich mit der Entwicklung des Internet befasst*

Klasse E-Adressen sind für Forschungszwecke der **IETF** vorbehalten und werden im Alltag nicht eingesetzt.

Bild 5.2 zeigt die prozentuale Aufteilung der Klassen:

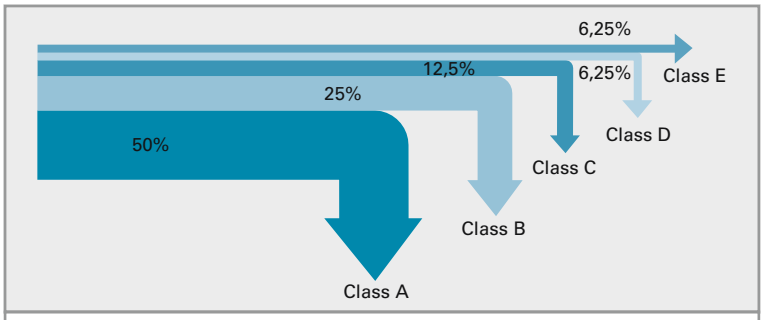



**Bild 5.2: Aufteilung der IP-Adressen in Klassen**

## 5.5 Aufteilen der IP in Netz- und Hostanteil

### 5.5.1 Subnetzmaske

Per Definition haben die Netze der 3 verwendeten Adressklassen eine bestimmte Größe. Diese wird zusätzlich durch die Subnetzmaske (oder Subnetmask) angegeben.

Zu jeder IP-Adresse gehört eine Subnetmask!

*Zu einer IP-Adresse gehört immer eine Subnetz-Maske.*

Die Subnetmask gibt an, wie viele Bits der IP-Adresse die Netzadresse und wie viele die Rechneradresse angeben.

#### Analogie zum Telefon

Beim Telefon verhält es sich ähnlich. Eine vollständige Telefonnummer besteht auch immer aus Telefon-Vorwahl (für das Ortsnetz) und der Anschlussnummer. Die Grenze zwischen Netz und Anschluss wird nicht explizit mitangegeben.

Der Telefonnummer 030123456789 sieht man an, dass 030 die Vorwahl für Berlin ist. 123456789 ist demnach die Anschlussnummer innerhalb von Berlin. Dass die Vorwahl nur 030 ist, weiß man aus Erfahrung. Die Netznummer ist (ohne die führende Null) nur 2-stellig. Es handelt sich also um ein großes Ortsnetz. Der Nummer 073867890123 sieht man schon nicht so einfach an, wo die Grenze zwischen Netznummer und Anschlussnummer ist. Dieses Ortsnetz ist relativ klein. Deshalb ist die Vorwahl 4-stellig: (0)7386.

Die althergebrachte Subnetzmaske wird ebenso in Dezimalschreibweise geschrieben wie die IP-Adressen. In binärer Schreibweise betrachtet, stehen Einsen an den Stellen, die zur Netzadresse gehören. Nullen stehen an den Stellen, die die Host-Adresse darstellen. Schreibt man IP-Adresse und Subnetzmaske binär untereinander, sieht man auf einen Blick, was zur Netzadresse bzw. zur Hostadresse gehört.

Dies ergibt folgende **Standard-Subnetzmasken**:

**Class A:**

**1111'1111**.0000'0000.0000'0000.0000'0000

⇒ Subnetmask: 255.0.0.0

**Class B:**

**1111'1111.1111'1111**.0000'0000.0000'0000

⇒ Subnetmask: 255.255.0.0

**Class C:**

**1111'1111.1111'1111.1111'1111**.0000'0000

⇒ Subnetmask: 255.255.255.0

### 5.5.2 CIDR-Notation

So wie bisher beschrieben, war das Internet-Protokoll ursprünglich gedacht. Man konnte nur ganze Netze miteinander verbinden. Man nennt dies *classful routing*.

Um Netze LAN-intern zu strukturieren, kann man große Netze in kleine Sub-Netze aufteilen. Dabei werden von links nach rechts Einsen in die Subnetzmaske geschoben. Diese Schreibweise ist etwas umständlich und sieht – trotz der Einfachheit – kompliziert aus.

*Die Anzahl der Netz-Bits wird hinter die IP-Adresse geschrieben.*

Ende der 80er Jahre erkannte man, dass die IP-Adressen rar werden, und dass große Netze nicht handhabbar sind. 1993 wurden die Klassen aufgehoben und das **Classless InterDomain Routing CIDR** eingeführt.

Die Subnetmaske wurde durch das Präfix ersetzt. Das Präfix (es ist eigentlich ein Postfix, weil es hinten angehängt wird) ist eine Zahl, die angibt, wie viele Bits der IP-Adresse zum Netzanteil gehören.

Die CIDR-Schreibweise lautet:

**w.x.y.z/n**, wobei n die Anzahl der Netzbits darstellt.

Beispiel: Anstatt der IP 10.1.2.3 mit der Subnetzmaske 255.255.0.0 schreibt man 10.1.2.3/16, weil in der Subnetzmaske 16 Einsen stehen. Der Rechner steht also in Netz 10.1.0.0 und hat die Host-Nummer 0.0.2.3.

Bei Windows-Rechnern wird meist die alte Dezimalschreibweise verwendet. Bei anderen Betriebssystemen kann man meistens beide Schreibweisen verwenden.

Inhaber der Class-A-Netze gaben beim Einführen von CIDR Teile ihres unbenutzen Adressbereiches wieder zurück, damit andere Firmen diese IP-Adressen verwenden konnten. So gibt es heute Class-B und Class-C-Netze, und natürlich ebenso größere und kleinere Netze, die ursprünglich Class-A-Netze waren. Man kann also heute nicht mehr von der IP-Adresse einer Firma über die Klasse dieser Adresse auf die Größe der Firma schließen.

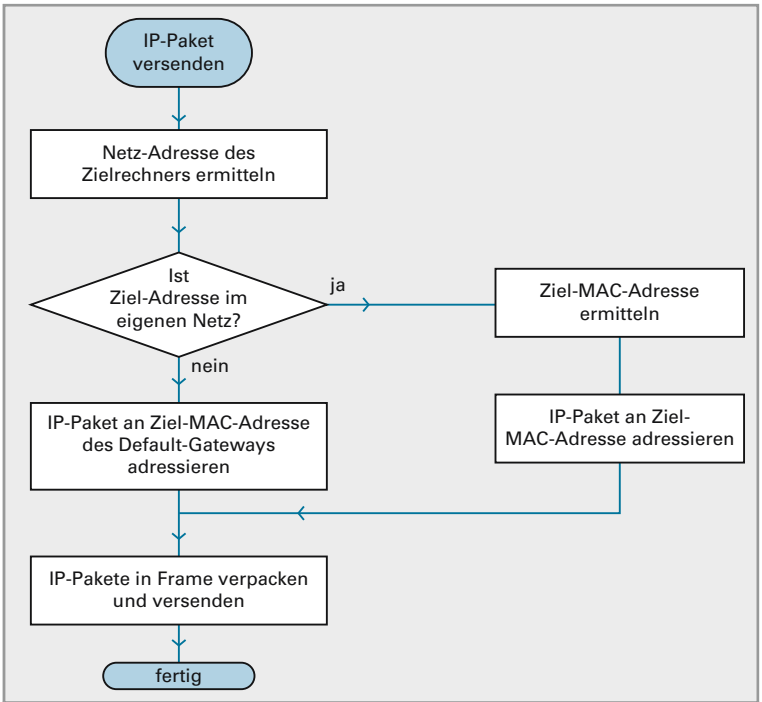



**Bild 7.12: Ermitteln der physikalischen Adresse**

### IP-Netz- und IP-Rechneradressen

So wie die Telefonnummer in einen Netz- und einen Anschlussteil aufgetrennt wird, so verhält es sich auch bei IP-Adressen. Im Gegensatz zu den Telefonnummern gibt es hier eine klare Angabe, wie viele Stellen der Adresse das Netzwerk und wie viele den Rechner adressieren. Hierzu sind 2 Verfahren gebräuchlich. Das bisherige Verfahren nutzt zusätzlich zur IP-Adresse die Subnetzmaske. Das neuere Verfahren gibt mit der IP-Adresse die Anzahl der Netz-Bits an (CIDR-Schreibweise).

**Herkömmliches Verfahren** – IP-Adresse mit Subnetzmaske:

Schreibweise IP: w.x.y.z und SN: s.t.u.v

Beides wird in dezimaler Schreibweise angegeben. Jede Stelle umfasst ein Oktett (≙ 8 Bit). Die Subnetzmaske wird von links nach rechts mit Einsen aufgefüllt. Die Stellen, an denen eine 1 steht, gehören zum Netzanteil, der Rest steht für die Rechneradresse.

Um nun die Netzadresse zu berechnen, gibt es mehrere Verfahren:

1. Man schreibt IP-Adresse und Subnetzmaske binär untereinander und bildet bitweise eine logische UND-Verknüpfung. Das Ergebnis ist der Netzanteil der IP-Adresse.
2. Man schreibt IP-Adresse und Subnetzmaske binär auf und zählt die Einsen der Subnetzmaske. Dieselbe Anzahl von Bits werden von links nach rechts von der IP-Adresse abgezählt. Diese Bits entsprechen dem Netzanteil. Die restlichen Bits der IP-Adresse ergeben den Hostanteil.

**Beispiel 7.4:**

| | Binär | Dezimal |
|---|---|---|
| IP | 0000’1010.0000’0001.0000’0001.0000’0111 | 10.1.1.7 |
| SN | 1111’1111.1111’1111.0000’0000.0000’0000 | 255.255.0.0 |
| UND | 0000’1010.0000’0001.0000’0000.0000’0000 | 10.1.0.0 |

Man erkennt, dass die ersten 16 SN-Bits 1 sind. Somit gehören die ersten 16 Bit der IP-Adresse zum Netzanteil, der Rest zum Hostanteil.
Es ergeben sich also die Netzadresse 10.1.0.0 und die Hostadresse 0.0.1.7.

### CIDR-Schreibweise

Die CIDR-Schreibweise ist eine IP-Adresse mit Angabe der Netzbit-Anzahl: w.x.y.z/n; dabei gibt die Zahl n hinter dem Schrägstrich die Anzahl der Netzbits an.

**Beispiel 7.5:**
10.1.17.1/20 bedeutet, dass die ersten 20 Bits der IP-Adresse die Netzwerkadresse ergeben. Bitweise betrachtet ergibt sich:
IP = 0000’1010.0000’0001.0001’0001.0000’0001.
Betrachtet man als erstes nur die ersten 20 Bits, so erhält man als Netz-Adresse:
Net-ID = 0000’1010.0000’0001.0001’0000.0000’0000 = 10.1.16.0

Betrachtet man die bisher unbeachteten Bits 21 bis 32, so erhält man die Hostadresse:
Host-ID: 0000’0000.0000’0000.0000’0001.0000’0001 = 0.0.1.1

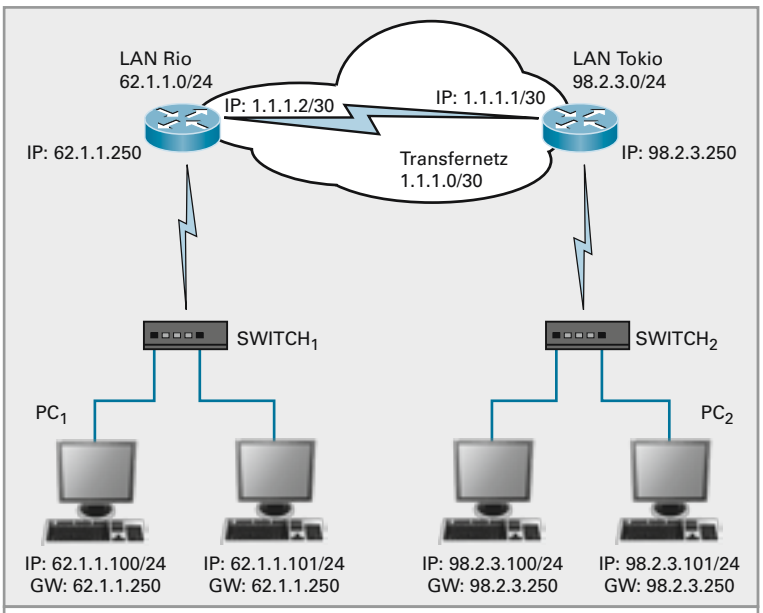



**Bild 7.13: Routingbeispiel mit 2 Netzen**

**Beispiel 7.6: Routing (Bild 7.13)**

Darstellung des Datentransportes über zwei Router: $PC_1$ mit der IP 62.1.1.100 schickt ein Datenpaket (OSI-Layer 3) an den Rechner $PC_2$ mit der IP 98.2.3.101. Das IP-Paket wird vom ersten PC mit seiner Absender-IP-Adresse und mit der Ziel-IP-Adresse des 2. Rechners versehen.

Der sendende PC reicht nun das Paket zum weiteren Versenden an die Schicht 2 weiter. Hier werden Frames erstellt und Netzwerkkarten adressiert. Bevor der Rechner nun die physikalische MAC-Adresse des Empfängers einsetzen kann, muss er prüfen, ob sich der Zielrechner im selben Netz befindet wie er. Dadurch muss er wissen, in welchem Netz er sich selbst befindet. Dies weiß der PC durch seine Netzwerkeinstellungen.

Aus der IP-Adresse 62.1.1.100 und 24 Bits Netzanteil (aus der Angabe „/24“) errechnet der PC das Netz mit der Nummer 62.1.1.0.

$PC_2$ liegt somit nicht im eigenen Netz. Das Paket muss also über den Router zugestellt werden. Dazu wird das Paket an den Router Rio mit der IP 62.1.1.250 adressiert. Der PC muss jetzt die MAC-Adresse des Interfaces mit dieser IP-Adresse ermitteln. Dies geschieht mithilfe des ARP. Wenn der PC die MAC-Adresse des Routerinterfaces hat, kann er das Originalpaket, weiterhin mit der Ziel-IP-Adresse von $PC_2$, an den Router schicken. Der Frame, in den das IP-Paket eingepackt wird, wird an den Router adressiert.

$PC_1$ verschickt den Datenframe, den als nächstes beim $Switch_1$ ankommt. $Switch_1$ liest die Ziel-MAC-Adresse aus dem Frame aus und vergleicht diese Adresse mit den Adressen aus seiner Switching-Tabelle. Er kennt die MAC-Adresse des Routers und leitet den Frame sofort unverändert an diesen Anschluss weiter, an dem der Router Rio angeschlossen ist.

Der Router Rio empfängt nun den Frame und packt ihn aus. Aus dem enthaltenen IP-Paket liest er die Zieladresse aus, also die IP-Adresse von $PC_2$. Der Router Rio kennt den Weg ins Zielnetz, in dem sich $PC_2$ befindet. Er weiß aus seiner Routing-Tabelle, dass er das Paket an den Router Tokio schicken muss. Er verpackt das IP-Paket wieder in einen Frame und adressiert diesen Frame an die MAC-Adresse des Routers Tokio.

Router Tokio packt den Frame aus und erhält das IP-Paket. Er liest die Ziel-IP-Adresse aus und sieht, dass sich der Zielrechner ein einem Netz befindet, welches bei ihm angeschlossen ist. Er kann also den Zielrechner direkt erreichen. Er verpackt dann das IP-Paket in einen Frame, welches direkt an den $PC_2$ adressiert wird.

Der $Switch_2$ leitet den Frame sofort unverändert zum Ziel-PC.

Der Ziel-PC empfängt den Frame. Er vergleicht die empfangene Ziel-MAC-Adresse mit seiner eigenen MAC-Adresse. Da die Adressen übereinstimmen, liest er alle Daten von der Netzwerkleitung in seinen Pufferspeicher ein und übergibt den empfangenen Frame dem Betriebssystem.

Die Tabelle 7.6 zeigt, wie sich die Adressen während der Übermittlung der Daten verändern. Man sieht, dass die IP-Adressen im Datenpaket (Layer 3) unverändert bleiben. Man sieht, dass die Adressen der unteren Schicht (Layer 2) immer verändert werden.

**Tabelle 7.6: Adressen während des Transportes**

| Strecke | Quell-IP | Ziel-IP | Quell-MAC | Ziel-MAC |
|---|---|---|---|---|
| $PC_1$ – $Switch_1$ | $PC_1$ | $PC_2$ | $PC_1$ | R-Rio |
| $Switch_1$ – R-Rio | $PC_1$ | $PC_2$ | $PC_1$ | R-Rio |
| R-Rio – R-Tokio | $PC_1$ | $PC_2$ | R-Rio | R-Tokio |
| R-Tokio – $Switch_2$ | $PC_1$ | $PC_2$ | R-Tokio | $PC_2$ |
| $Switch_2$ – $PC_2$ | $PC_1$ | $PC_2$ | R-Tokio | $PC_2$ |

### 7.2.7 Default Gateway

*Der **Gateway** führt nach außen.*

Ein **Gateway** (oder auf deutsch: Torweg) war im Mittelalter ein Weg, der aus einer Stadt oder einer Burg hinaus führte. Diese Wege aus dem geschützten Bereich der Mauern waren durch ein Tor geschützt und wurden streng bewacht (Bild 7.14).

**Bild 7.14: Gateway**

In einem Netzwerk braucht man ebenso einen „Ausweg" aus dem eigenen Netz. Ein jeder PC in einem Netzwerk kann Daten an alle Rechner seines Netzes schicken. Hat er Daten an Rechner zu verschicken, die sich nicht in seinem Netz befinden, so schickt er diese Daten an den Gateway.

Router haben ihre Routingtabellen. Ihnen sind die Netze bekannt, die sie direkt erreichen und die direkt an ihnen angeschlossen sind. Netze hinter anderen Routern kennen die Router auch, da sie sich gegenseitig mitteilen, welche Netze sie erreichen können.

Da natürlich auch Router nicht alle Netze kennen können, haben sie für die ihnen unbekannten Netze einen Default Gateway.

### 7.2.8 NAT/PAT – Network Address Translation / Port Address Translation

Würde man eine Anzahl von Rechnern in einem LAN über einen normalen Router ans Internet anschließen, so bräuchte jeder einzelne Rechner eine eigene, einmalige IP-Adresse aus dem öffentlichen Adressraum. Alle Rechner müssten dann ein Class-A, Class-B oder Class-C Netz bilden, oder zumindest ein Subnetz eines solchen öffentlichen Netzes. Dadurch könnte zwar jeder Rechner mit dem gesamten Internet kommunizieren, wäre aber auch vom gesamten Internet erreichbar und angreifbar.

Die WiGig (*Wireless Gigabit Alliance*) arbeitet mit der Wi-Fi-Alliance zusammen. Daher ist zu erwarten, dass der neue Standard kompatibel mit den bisherigen WLAN-Standards sein wird. Dieser Standard bringt Gigabit-Geschwindigkeit auch ins WLAN. Datenübertragungsraten von über einem Gigabit pro Sekunde sind damit machbar. Die maximale Bruttodatenrate wird bei 7 Gbps liegen. Die Trägerfrequenz beträgt 60 GHz.

Auch bei Funk gilt: Je höher die Frequenz, desto größer die Dämpfung! Bei gleicher Sendeleistung ist die Reichweite im 5 GHz-Bereich geringer als im 2,5 GHz-Bereich. Die geringste Reichweite erreicht deshalb man mit dem neusten 60 GHz-WLAN.

### 8.10.2 WLAN-Betriebsarten

Es gibt 3 Betriebsarten für WLANs:

- Ad-Hoc-Mode
- Infrastructure-Mode
- Wireless-Distribution-System WDS

#### Ad-hoc-Mode

***Ad hoc:*** *sofort, jeder Rechner bildet eine Funkzelle.*

Der **Ad-hoc**-Mode ist für das schnelle und unkomplizierte Aufbauen von Sofortverbindungen zwischen mehreren Rechnern. Keine Station ist dabei privilegiert, alle Stationen sind gleichberechtigt.

Dazu muss jeder Rechner, der Mitglied eines solchen Ad-hoc-Netzes werden möchte, die Kennung des Netzes haben. Diese Kennung ist die SSID, die „Service Set Identifier". Jeder Rechner mit derselben SSID gehört zu diesem Netzwerk.

#### Infrastructure-Mode

***Infrastructure-Mode:*** *ein oder mehrere Accesspoints zur Kommunikation.*

Im **Infrastructure-Mode** steht ein WLAN-Accesspoint in der Mitte des Funknetzes. Jeder Rechner muss sich mit diesem Accesspoint verbinden, wenn er in dieses Netzwerk möchte. Der Accesspoint sendet regelmäßig eine Kennung aus, im Normalfall zweimal pro Sekunde. Diese Kennung, man nennt sie Beacon, enthält die SSID des Funknetzes, die Datenübertragungsrate und die Art der Verschlüsselung.

*WLANs immer mit Passwort oder -satz versehen!*

Wenn sich ein Rechner mit einem Accesspoint (AP) verbindet, dann muss er sich am AP authentifizieren. Es empfiehlt sich, am AP ein möglichst kompliziertes Passwort zu hinterlegen, welches dann am PC oder Laptop eingegeben werden muss. Am besten sind hier Passsätze, da sie leichter als Passwörter zu merken und somit schwerer zu knacken sind.

Aus Gründen des Abhörens muss die Datenübertragung verschlüsselt erfolgen. Ursprünglich wollte man mit einem Verschlüsselungsverfahren dieselbe Abhör-Sicherheit herstellen wie bei verkabelten Netzen. Das hierzu entwickelte Protokoll WEP (*Wired Equivalent Privacy*) hält aber nicht, was es verspricht. Heute gilt das WPA2-Verschlüsselungsverfahren als sicher. Da Funkwellen von jedem, der sich im Bereich der Funkzelle aufhält, empfangen werden können, ist hier allergrößte Vorsicht geboten.

*WLANs immer verschlüsseln!*

Die Rechtsprechung ist hier eindeutig: Wer ein WLAN nicht sichert und verschlüsselt, ist haftbar, wenn andere das WLAN missbrauchen! Da ein WLAN normalerweise immer seine Kennung mit dem Beacon aussendet, wird es einem potenziellen Angreifer leicht gemacht, das Netzwerk seines Opfers ausfindig zu machen. Hier hilft das Abschalten der SSID im Beacon. Man kann und darf den Beacon nicht verhindern, aber man kann den Beacon ohne SSID aussenden. Man sieht dann nur ein WLAN, sieht aber keinen Namen dazu.

*Bei WLANs immer das Aussenden der SSID abschalten!*

*Nur so viele Verbindungen erlauben wie nötig!*

Eine weitere Möglichkeit, um ein WLAN sicherer zu machen, ist das Beschränken der Anzahl der angemeldeten Rechner am AP. Wenn man nur mit einem einzigen Rechner auf sein WLAN zugreift, dann muss man nicht 100 Verbindungen zulassen. Weiterhin kann man die MAC-Adresse der Rechner angeben, die zugelassen werden. Rechner mit anderen MAC-Adressen werden abgewiesen. Natürlich können MAC-Adressen auch gefälscht werden. Deshalb ist dieser MAC-Filter nur eine weitere Hürde, die man einbaut.

*Nur bekannte MAC-Adressen zulassen!*

***Wardriving** oder **Warwalking** ist das Suchen nach ungeschützten WLANs.*

Ein beliebtes Gesellschaftsspiel ist **Wardriving** oder auch **Warwalking**. Dabei fährt man mit dem Auto oder man geht zu Fuß durch die Straßen und hält Ausschau nach offenen WLANs, die man eventuell für den Internetzugang nutzen kann.

### Wireless Distribution System WDS

Beim WDS wird eine Funkzelle über einen oder mehrere weitere APs vergrößert. Nur ein AP braucht Anschluss an die LAN-Verkabelung. Die weiteren APs arbeiten als Funk-Repeater und reichen das LAN-Signal weiter. Dadurch lassen sich große Funk-Netzbereiche realisieren. Mobile Stationen können sich durch dieses Funknetz bewegen und werden von einem AP zum nächsten übergeben. Man nennt dies *Roaming*.

## 8.11 Übungen Übertragungstechnik

### Übungsaufgabe Nr. 1

Eine Leitung hat folgende Werte laut Datenblatt:

$R' = 300\,\Omega/100\,\text{m}$

Wie groß ist der Leitungswiderstand bei 75 Metern Leitungslänge?

### Übungsaufgabe Nr. 2

Weshalb ist das Übertragungsverhalten einer Leitung frequenzabhängig?

### Übungsaufgabe Nr. 3

Eine Netzwerkleitung hat eine Dämpfung $a$ von 3 dB. Die Übersprechdämpfung $a_{NEXT}$ zu einem Nachbarpaar beträgt 70 dB. Wie groß ist der Störabstand der beiden Signale (Bild 8.62)?

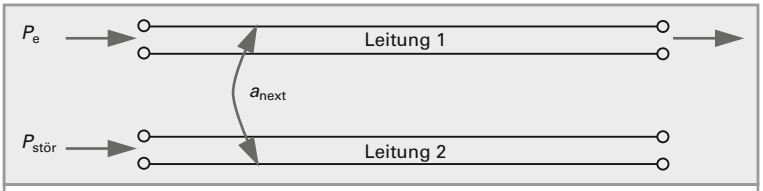



**Bild 8.62: Übersprechen**

### Übungsaufgabe Nr. 4

Eine Datenleitung hat einen Dämpfungsbelag von 5 dB pro km. Die Übersprechdämpfung beträgt 60 dB. Der tolerierbare Störabstand beträgt 40 dB.

Wie lang darf die Leitung maximal sein?

### Übungsaufgabe Nr. 5

Eine Datenleitung die mit 1 Volt gespeist wird, ist mit 100 Ω abgeschlossen. Am Leitungsende wird eine Störspannung von 0,01 V gemessen.

Wie groß ist der Störabstand in dB?

### Übungsaufgabe Nr. 6

Ein WLAN-Accesspoint der Norm 802.11a hat 1 Watt Sendeleistung.

Welchem absoluten Pegel entspricht dies?

### Übungsaufgabe Nr. 7

Ein Lichtstrahl fällt unter einem Winkel von 50 Grad auf eine Glasplatte mit einem Brechungsindex von 1,4.

Wie groß ist der Winkel im Glas?

### Übungsaufgabe Nr. 8

Welche Dämpfung hat eine Glasfaserstrecke von 600 m Länge bei Betrieb mit einem Laser mit 850 nm Wellenlänge? Benutzen Sie dazu das Bild 8.48.

### Übungsaufgabe Nr. 9

Eine Glasfaser hat eine Kern-Brechzahl von 1,481 und eine numerische Apertur von 0,2. Wie groß ist die Brechzahl des Mantelglases?

### Übungsaufgabe Nr. 10

Welcher Frequenzbereich wird bei DSL-Übertragungen benutzt und in wie viele Übertragungskanäle wird dieser Bereich eingeteilt?

### Übungsaufgabe Nr. 11

Warum ist die Anzahl der Upload-Kanäle geringer als die Anzahl der Download-Kanäle?

### Übungsaufgabe Nr. 12

Mit welchem Verfahren wird geregelt, welche Station senden darf und welche nicht?

# 9 Anhang

## 9.1 Normen und Normungsgremien

Es gibt weltweit mehrere, zum Teil konkurrierende Gremien, die sich mit der Normung befassen. Hier wird nur ein ganz kleiner Einblick in die Vielzahl von Normen und Gremien gegeben.

### 9.1.1 IEEE

**Die LAN-Standards**

Das Institute of Electrical and Electronics Engineers, kurz IEEE, ist der weltweit größte technische Berufsverband mit Niederlassungen in über 150 Ländern. Das IEEE veröffentlicht Standards auf vielen technischen Gebieten.

Im Februar 1980 wurde mit ihr eine Kommission gegründet, die sich mit Standards in dem neu aufkommenden Gebiet der lokalen Netze befassen sollte. Nach dem Gründungszeitpunkt erhielt diese Kommission die Bezeichnung 802.

Innerhalb dieser Kommission wurden verschiedene Arbeitsgruppen eingerichtet, die sich mit Teilbereichen der LANs zu befassen hatten. Diese Arbeitsgruppen veröffentlichten im Laufe der Zeit viele Standards. Manche Gruppen sind nicht mehr aktiv, da der technologische Fortschritt sie überflüssig machte. Andere sind dagegen sehr aktiv, wenn es um neue Entwicklungen und Trends geht, wie beispielsweise das 100 Gigabit-Ethernet oder Funknetze.

Die Gruppe der 802-Standards legt alles fest, was die unteren Schichten (Datalink und Physical-Layer bei OSI, bzw. NetworkAccess bei TCP/IP) betrifft. Tabelle 9.1 zeigt einen Auszug aus den wichtigsten 802-Standards.

### 9.1.2 ISO, Internationale Organisation für Normung

Die Internationale Organisation für Normung – kurz ISO[1] – ist die internationale Vereinigung von Normungsorganisationen und erarbeitet internationale Normen in allen Bereichen mit Ausnahme der Elektrik und der Elektronik, für die die Internationale elektrotechnische Kommission (IEC) zuständig ist, und mit Ausnahme der Telekommunikation, für die

1 von Gr.: *isos*; zu Dt. „gleich“, engl. *International Organization for Standardization*

die Internationale Fernmeldeunion (ITU) zuständig ist. Gemeinsam bilden diese drei Organisationen die WSC (World Standards Cooperation).

- ISO 216 – Papierformate
- ISO 1000 – SI-Einheiten
- ISO 3103 – Zubereitung von Tee (kein Witz!)
- ISO 8859 – Zeichensätze, die ASCII als Untermenge beinhalten (z. B. ISO 8859-1, ISO 8859-2)
- ISO 9899 – Die Programmiersprache C
- ISO/IEC 10164 – Informationstechnik; Kommunikation Offener Systeme; Systemmanagement
- ISO/IEC 10165 – Informationstechnik; Kommunikation Offener Systeme; Managementdienste; Strukturierung der Managementinformation (OSI Managementmodell)

**Tabelle 9.1: Auszug aus den wichtigsten 802-Standards**

| Arbeitsgruppe | Untergruppe | Bezeichnung |
|---|---|---|
| 802.1 | | High Level Interface (Internetworking) |
| | **802.1D** | Spanning Tree Protocol |
| | **802.1Q** | Virtual Bridged LANs, VLANs |
| | 802.1w | Rapid Spannig Tree Protocol |
| 802.2 | | Logical Link Control |
| **802.3** | | Ethernet CSMA/CD |
| | 802.3a | 10Base-2 Ethernet über Koaxialleitungen |
| | 802.3i | 10Base-T Ethernet über Twisted-Pair |
| | 802.3j | 10Base-F Ethernet über Glasfaser |
| | 802.3u | 100Base-T, Fast Ethernet |
| | 802.3z | 1000Base-F, Gigabit Ethernet über Glasfaser |
| | 802.3ab | 1000Base-T, Gigabit Ethernet über UTP |
| | 802.3ad | Link Aggregation |
| | 802.3ae | 10 Gigabit Ethernet, 10GE |
| | 802.3an | 10 Gigabit Ethernet über TP, 10GBase- T |
| | 802.3ba | 40 Gigabit Ethernet und 100 Gigabit Ethernet |
| | 802.3af | Power over Ethernet, PoE |
| 802.4 | | Token-Passing-Bus |
| 802.5 | | Token-Passing-Ring |
| 802.6 | | Metropolitan Area Networks |
| 802.9 | | Integrated Voice and Data Networks |
| **802.11** | | Wireless LAN |
| | 802.11a | WLAN mit 54 Mbps auf 5 GHz-Träger |
| | 802.11b | WLAN mit 11 Mbps auf 2,4 GHz-Träger |
| | 802.11g | WLAN mit 54 Mbps auf 2,4 GHz-Träger |
| | 802.11n | WLAN mit 600 Mbps auf 2,4 GHz und 5 GHz-Träger |
| | 802.11ad | Gigabit-WLAN mit bis zu 7 Gbps auf 60 GHz-Träger |
| **802.14** | | Cable Television (CATV, Kabelfernsehen) |
| 802.15 | | Wireless PAN (Personal Area Network) |
| | 802.15.1 | Bluetooth |