

Berufskolleg für Gestaltung und Technik



In Kooperation mit dem HERDT-Verlag stellen wir Ihnen eine PDF inkl. Zusatzmedien für Ihre persönliche Weiterbildung zur Verfügung. In Verbindung mit dem Programm HERDT|Campus ALL YOU CAN READ stehen diese PDFs nur Lehrkräften und Schüler*innen der oben genannten Lehranstalt zur Verfügung. Eine Nutzung oder Weitergabe für andere Zwecke ist ausdrücklich verboten und unterliegt dem Urheberrecht. Jeglicher Verstoß kann zivil- und strafrechtliche Konsequenzen nach sich ziehen.

Netzwerke

Netzwerktechnik

Karsten Bratvogel, Siegmund Dehn

(Stand 2019)

1. Ausgabe, Januar 2020

ISBN 978-3-86249-929-8

NWTK_2019



Impressum

Matchcode: NWTK_2019

Autoren: Karsten Bratvogel, Siegmund Dehn

Produziert im HERDT-Digitaldruck

1. Ausgabe, Januar 2020

HERDT-Verlag für Bildungsmedien GmbH
Am Kümmerling 21-25
55294 Bodenheim
Internet: www.herdt.com
E-Mail: info@herdt.com

© HERDT-Verlag für Bildungsmedien GmbH, Bodenheim

Alle Rechte vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotokopie, Mikrofilm oder einem anderen Verfahren) ohne schriftliche Genehmigung des Verlags reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Dieses Buch wurde mit großer Sorgfalt erstellt und geprüft. Trotzdem können Fehler nicht vollkommen ausgeschlossen werden. Verlag, Herausgeber und Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Wenn nicht explizit an anderer Stelle des Werkes aufgeführt, liegen die Copyrights an allen Screenshots beim HERDT-Verlag. Sollte es trotz intensiver Recherche nicht gelungen sein, alle weiteren Rechteinhaber der verwendeten Quellen und Abbildungen zu finden, bitten wir um kurze Nachricht an die Redaktion.

Die in diesem Buch und in den abgebildeten bzw. zum Download angebotenen Dateien genannten Personen und Organisationen, Adress- und Telekommunikationsangaben, Bankverbindungen etc. sind frei erfunden. Eventuelle Übereinstimmungen oder Ähnlichkeiten sind unbeabsichtigt und rein zufällig.

Die Bildungsmedien des HERDT-Verlags enthalten Verweise auf Webseiten Dritter. Diese Webseiten unterliegen der Haftung der jeweiligen Betreiber, wir haben keinerlei Einfluss auf die Gestaltung und die Inhalte dieser Webseiten. Bei der Bucherstellung haben wir die fremden Inhalte daraufhin überprüft, ob etwaige Rechtsverstöße bestehen. Zu diesem Zeitpunkt waren keine Rechtsverstöße ersichtlich. Wir werden bei Kenntnis von Rechtsverstößen jedoch umgehend die entsprechenden Internetadressen aus dem Buch entfernen.

Die in den Bildungsmedien des HERDT-Verlags vorhandenen Internetadressen, Screenshots, Bezeichnungen bzw. Beschreibungen und Funktionen waren zum Zeitpunkt der Erstellung der jeweiligen Produkte aktuell und gültig. Sollten Sie die Webseiten nicht mehr unter den angegebenen Adressen finden, sind diese eventuell inzwischen komplett aus dem Internet genommen worden oder unter einer neuen Adresse zu finden. Sollten im vorliegenden Produkt vorhandene Screenshots, Bezeichnungen bzw. Beschreibungen und Funktionen nicht mehr der beschriebenen Software entsprechen, hat der Hersteller der jeweiligen Software nach Drucklegung Änderungen vorgenommen oder vorhandene Funktionen geändert oder entfernt.

Bevor Sie beginnen ...	4	7 Installationsrichtlinien für die Verkabelung	105
1.1 Grundlagen der Netzwerktechnik	6	7.1 EN 50173 und weitere Standards	105
1.2 Übertragungsrichtung	7	7.2 Struktur nach ISO/IEC 11801	107
1.3 Struktur von Kommunikationsnetzen	8	7.3 Richtlinien für Kupferkabel	109
1.4 Übertragungsmedien für Verbindungen	10	7.4 Besonderheiten für LWL-Kabel	112
1.5 Integration verschiedener Dienste	12	7.5 Kennzeichnung und Beschriftung	112
1.6 Übertragungstechniken	12		
1.7 Grundlagen der Signalübertragung	13		
1.8 Leistungstheorie	14		
1.9 Übung	20		
2 Medien für die Datenübertragung	21	8 Planung und Dokumentation von Netzwerken	113
2.1 Kabel mit metallischen Leitern	21	8.1 Planung eines Netzwerks	113
2.2 Kabel mit nicht metallischen Leitern	27	8.2 Anforderungen an die Infrastruktur	115
2.3 Kabellose Systeme	40	8.3 Ausstattung der Arbeitsplätze	118
2.4 Übung	48	8.4 Überspannungsschutz	118
3 Erweiterung von Netzwerken	49	8.5 Bauliche Maßnahmen	120
3.1 Die Aufgabe von aktiven Komponenten	49	8.6 Dokumentation	120
3.2 Einteilung aktiver Komponenten nach dem ISO/OSI-Modell	49		
3.3 Koppelemente	50		
3.4 Übung	63		
4 Unterbringung und Absicherung von Netzwerkelementen	64	9 Lokale Netzwerke (LAN)	126
4.1 Passive Geräte für Netzwerke	64	9.1 Wireless LAN (WLAN)	126
4.2 Server- und Netzwerkschränke	65	9.2 WLAN-Sicherheitsaspekte	127
4.3 Schrank-Kontroll-Systeme	67	9.3 Übung: Wireless-System planen	130
4.4 Verbinder und Anschlusskabel	69	9.4 WLAN als drahtloser Internetzugang	133
4.5 Patchpanel und Datendosen	71	9.5 Übung: Switch einrichten	135
5 Kabelverlegung	75	9.6 Fehleranalyse bei Switchen	138
5.1 Stecker und Anschlusstechnik	75	9.7 IP-Routing verstehen und einrichten	140
5.2 Installationsbeispiel: AMJ-S-Modul (Cat 6A) konfektionieren	76	9.8 Routing-Befehle und Routing-Tabelle	147
5.3 Übungsszenario: RJ-45-Stecker auf ein TP-Patchkabel (UTP/STP) montieren	79	9.9 IP-Hardware-Router einrichten	149
5.4 Montagebeispiel: TP-Kabel an Cat 6A-Datendose anschließen	80	9.10 IPv6	152
5.5 Lichtwellenleiter verlegen	82	9.11 IPv6-Routing	154
5.6 Anwendungsbeispiel: LightCrimp Plus	83	9.12 Fehlersuche in kabelgebundenen Netzwerken	158
6 Qualitätssicherung	86	10 Weitverkehrsnetze (WAN)	162
6.1 Messgeräte für die Kupfertechnik	86	10.1 Übertragungstechniken in Weitverkehrsnetzwerken	162
6.2 Oszilloskop	87	10.2 VoIP mit SIP-Trunk	166
6.3 LAN-Messgeräte	88	10.3 DSL (Digital Subscriber Line)	167
6.4 Testparameter für TP-Verkabelungen	91	10.4 UMTS	170
6.5 Abnahmemessung für Kupferkabel durchführen	93	10.5 LTE	172
6.6 Messgeräte für Glasfasern	97	10.6 WiMAX	172
6.7 Optische Rückstremessung (OTDR)	98	10.7 Weitere Übertragungsprotokolle	173
6.8 Dämpfungsmessung	100	10.8 Szenario: Internetzugang einrichten	174
6.9 Übungsszenario: Dämpfungsmessung durchführen	103		
6.10 Übung	104		
		11 Weitere Entwicklungen	181
		11.1 Ethernet-Technologie	181
		11.2 PoE – Power over Ethernet	184
		11.3 Gigabit-Spezifikation	185
		11.4 Gigabit Interface Converter (GBIC)	188
		11.5 Konfigurationsbeispiele	189
		11.6 2,5- und 5-Gigabit-Ethernet	190
		11.7 10-Gigabit-Ethernet	190
		11.8 25- und 40-Gigabit	192
		11.9 Anforderungen an industrielle Gerätschaften	192
		11.10 Neue Mobilfunkstandards	193
		11.11 Weitere Technologien	194
		Bildquellenverzeichnis	196
		Stichwortverzeichnis	197

Bevor Sie beginnen ...

HERDT BuchPlus - unser Konzept:

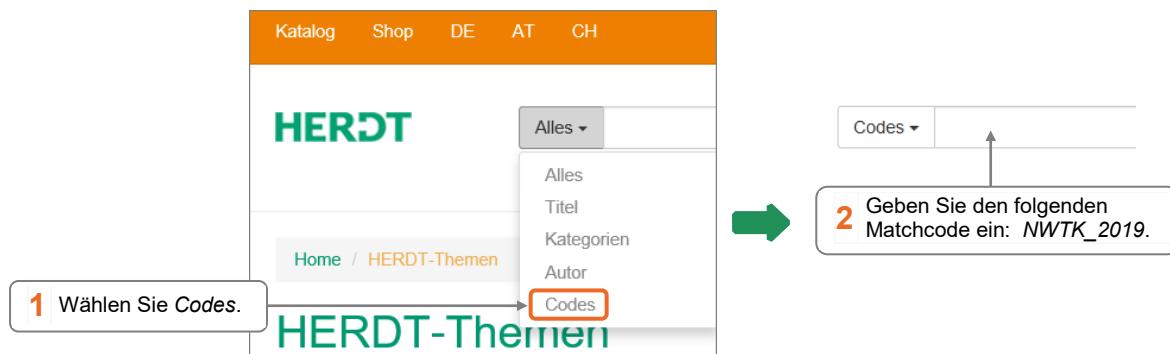
Problemlos einsteigen - Effizient lernen - Zielgerichtet nachschlagen

(weitere Infos unter www.herdt.com/BuchPlus)

Nutzen Sie dabei unsere maßgeschneiderten, im Internet frei verfügbaren Medien:



- Rufen Sie im Browser die Internetadresse www.herdt.com auf.



Voraussetzungen und Ziele

Zielgruppe

- ✓ IT-Systemelektroniker/-in
- ✓ Fachinformatiker/-in (Systemintegration)
- ✓ Systemadministratoren
- ✓ Netzwerktechniker

Empfohlene Vorkenntnisse

- ✓ Grundlagenkenntnisse Netzwerke sowie Kenntnisse in der Netzwerkverwaltung mit einem Netzwerkbetriebssystem, die z. B. denen entsprechen, die im HERDT-Buch *Netzwerke – Grundlagen* vermittelt werden

Lernziele

Dieses Buch vermittelt einen Gesamtüberblick über die Netzwerktechnik und die Vernetzung. Behandelt werden die Übertragungsmedien und Übertragungstechnologien in lokalen Netzen und Weitverkehrsnetzen sowie Netzwerkarchitekturen, Installationsrichtlinien und Installationsschemata nach ISO/IEC.

Nach dem Durcharbeiten dieses Buches kennen Sie die erforderlichen Komponenten, Kopplungselemente und Kabel zum Aufbau einer anwendungsneutralen IT-Infrastruktur. Sie können komplexe Netzstrukturen aufbauen und die Vernetzung mit Netzwerktools prüfen.

Dieses Buch kann vorbereitend und begleitend bei Vernetzungsprojekten eingesetzt werden.

Hinweise zu Soft- und Hardware

Die im Buch beschriebene Soft- und Hardware ist in großen Teilen nur als Beispiel dargestellt. Je nach Anforderung und Verfügbarkeit kann und muss der Leser andere Produkte zu Übungs- und Einsatzzwecken verwenden.

Aufbau und Konventionen

Inhaltliche Gliederung

Das Buch stellt zuerst die verschiedenen Übertragungsmedien, deren Spezifikationen und Installationsmethoden dar. Abgeschlossen wird dieser Teil mit kabelloser Übertragung (WLAN). Der zweite Teil beschäftigt sich mit aktiven und passiven Komponenten, bevor die konkrete Einrichtung von Routing-Diensten (IP und IPv6, wobei IP für IPv4 steht) beschrieben wird. Im dritten Teil werden übergeordnete Themen wie Fehlersuche, Installationsrichtlinien und Planung aufgegriffen. WAN-Technologien und aktuelle Entwicklungen bilden den letzten Teil.

Typografische Konventionen

Damit Sie bestimmte Elemente auf einen Blick erkennen und zuordnen können, werden diese im Text durch eine besondere Formatierung hervorgehoben. So werden beispielsweise Bezeichnungen für Programmelemente wie Register oder Schaltflächen immer *kursiv* geschrieben und wichtige Begriffe **fett** hervorgehoben.

- | | |
|----------------------|---|
| Kursivschrift | kennzeichnen alle vom Programm vorgegebenen Bezeichnungen für Schaltflächen, Dialogfenster, Symbolleisten etc., Menüs bzw. Menüpunkte (z. B. <i>Datei - Schließen</i>), Internetadressen und vom Benutzer angelegte Namen (z. B. Rechner-, Domänen-, Benutzernamen). |
| Courier | wird für Systembefehle sowie für Datei- und Verzeichnisnamen verwendet.
In Syntaxangaben werden Parameter <i>kursiv</i> ausgezeichnet (z. B. <code>cd Verzeichnisname</code>). Eckige Klammern [] kennzeichnen optionale Elemente. Alternative Eingaben sind durch einen senkrechten Strich getrennt. Benutzereingaben auf der Konsole werden fett hervorgehoben. |

Symbole



Hilfreiche Zusatzinformation



Praxistipp



Warnhinweis

1 Grundlagen der Netzwerk- und Elektrotechnik

In diesem Kapitel erfahren Sie

- ✓ wie die grundsätzliche Übertragung von Daten erfolgt
- ✓ welche Betriebsarten bei einer Kommunikation möglich sind
- ✓ welche Übertragungsmedien verwendet werden
- ✓ welche Übertragungsbandbreiten vorhanden sind

Voraussetzungen

- ✓ Technisches Verständnis
- ✓ Grundkenntnisse technisches Englisch

1.1 Grundlagen der Netzwerktechnik

Datenübertragung

Bei der Übertragung von Daten (Informationen: Voice, Video, Data) werden grundsätzlich ein **Sender** und ein **Empfänger** benötigt. Dabei stellt der Sender, auch **Datenquelle** (engl. data source) genannt, Informationen zur Übertragung bereit. Diese Sendeinformationen werden dann unter Angabe des Adressaten über ein Übertragungsmedium (Kabel, Lichtwellenleiter, Funkwellen oder Lichtimpulse an den Empfänger (engl. data destination), auch **Datenziel** genannt, geleitet.

Die einfachste Art des elektronischen Informationsaustausches war die analoge Telefonie. Der Sender bildet in diesem Fall das Telefon des Anrufers. Das Übertragungsmedium ist das Fernmeldenetz eines Festnetzbetreibers, und der Empfänger bildet das Telefon des angerufenen. Als Adresse des Datenziels dient in diesem Fall die Rufnummer des gewünschten Teilnehmers.

Als weiteres Beispiel der Datenübertragung sei hier die Kommunikation über ein DSL-Modem erwähnt. Die Übertragung erfolgt, wie beim Telefon, bidirektional (d. h. gleichzeitiges Senden und Empfangen der Informationen). Der Sender (PC) übermittelt z. B. über das Kabel seine Anfragen an das DSL-Modem. Das Modem setzt seinerseits die Signale in Richtung des Providers um.

Die Prozedur für die Übertragung von Daten in einem lokalen Netzwerk ist etwas komplizierter, funktioniert aber nach dem gleichen Schema. Die Datenquelle bestimmt anhand einer eindeutigen Adresse den Empfänger und sendet die Informationen, aufgeteilt in Datenframes an das Datenziel. Damit der Empfänger die erhaltenen Informationen eindeutig zuordnen kann, wird dem Datenpaket die Adresse des Senders angefügt. Je nach Art des Verbindungsprotokolls werden zusätzliche Sicherheitsinformationen im Datenframe übermittelt.

Definition Protokoll

Der Begriff **Protokoll** wird in vielen Bereichen verwendet. In der EDV beschreibt ein Protokoll den genauen Ablauf eines Kommunikationsvorganges oder eines Teilespektes. Daher kommen meist mehrere Protokolle während eines Übertragungsvorganges zum Einsatz.

Definition Netzwerk

Ein **Netzwerk** umfasst alle kommunikationstechnischen Komponenten zur Übertragung und Vermittlung von Informationen zwischen angeschlossenen Endsystemen. Der Austausch dieser Informationen und die Nutzung von Ressourcen erfolgt über entsprechende Kommunikationsverbindungen. Die **Endsysteme** (Telefon, PC, Server, Terminal ...) und die für die Verbindung notwendigen **Netzwerkknoten** (Switches, Router) können in einem **lokalen Netzwerk** (LAN) oder in einem **Weitverkehrsnetzwerk** (WAN) an unterschiedlichen Standorten liegen. Sie sind über **drahtlose** (engl. wireless) Verbindungen (WLAN, GSM, UMTS, LTE, ...) oder **drahtgebundene** (engl. wired) Verbindungen (Kabel, Lichtwellenleiter) miteinander verbunden.

Vorteile von Netzwerken sind unter anderem:

- ✓ die zentrale Datenspeicherung und der flexible Austausch von Daten (Datenverbund)
- ✓ die Nutzung von Applikationen, die nicht auf dem eigenen System vorhanden sind (Funktionsverbund)
- ✓ die gleichzeitige Lösung von Aufgaben durch mehrere Systeme (Lastverbund)
- ✓ die Redundanz von Systemen (Verfügbarkeitsverbund)

Definition Datagramme

Ein **Datagramm** ist eine in sich geschlossene unabhängige Dateneinheit. Sie wird auch als **Protocol data unit (PDU)** bezeichnet. Die darin enthaltenen Informationen werden zwischen einer Datenquelle und einem Datenziel über ein Netzwerk transportiert. Datagramme zeichnen sich durch einen geringen Protokoll-Overhead (Protokollspezifische Verwaltungsdaten) aus und enthalten im Wesentlichen nur die Empfangs- und Absenderadresse, sowie Nutzdaten.

1.2 Übertragungsrichtung

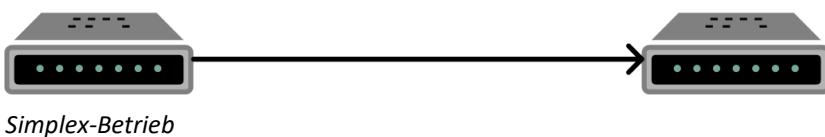
Einteilung von Übertragungsrichtungen

In Abhängigkeit der Übertragungssysteme für den logischen Informationsfluss existieren verschiedene Übertragungsarten. Bei den Übertragungseinrichtungen lassen sich folgende Konfigurationsmöglichkeiten ableiten:

- ✓ Simplex (sx)
- ✓ Halbduplex (engl. half duplex, hdx)
- ✓ Echoplex
- ✓ Duplex bzw. Vollduplex (engl. full duplex, fdx)

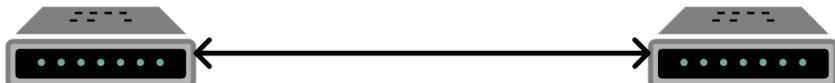
Simplex

Beim Simplex-Betrieb (engl. simplex transmission) oder auch Einwegbetrieb (unidirektional) erfolgt die Übertragung von Informationen nur in einer Richtung. Im Simplex-Betrieb ist keine Rückmeldung oder Fehlerkorrektur möglich. Beispiele für diese Betriebsart sind der Radio- und Fernsehempfang (ohne Rückkanal) oder der GPS-Dienst.



Halbduplex

Beim Halbduplex-Betrieb sind die Datenstationen in der Lage, Informationen zu senden und zu empfangen. Das Halbduplex-Verfahren erlaubt die wechselseitige Nutzung **einer** Übertragungsleitung in beiden Richtungen (bidirektional). An den Schnittstellen kann zu einem Zeitpunkt nur gesendet oder empfangen werden. Dabei werden die Informationen abwechselnd von der Datenquelle zur Datensenke übertragen und umgekehrt. Ein typisches Beispiel für den Halbduplex-Betrieb ist der Faxdienst oder Walkie-Talkie-Funkgeräte.



Halbduplex-Betrieb

Echoplex

Beim Echoplex-Betrieb werden Daten von der Empfangsstation (engl. data destination) an die Sendestation (engl. data source) zurückgespiegelt. Dadurch ist eine einfache Kontrolle der fehlerfreien Übertragung möglich. Ein eingegebenes Zeichen wird also erst dann auf dem Bildschirm dargestellt, wenn es vom Host gespiegelt worden ist. Echoplex ist eine Spezialform des Duplex-Betriebes. Telekommunikationsunternehmen nutzen dieses Verfahren um z. B. einen Leitungstest durchzuführen.



Echoplex-Betrieb

Duplex

Beim Duplex-Betrieb sind beide Datenstationen gleichberechtigt. Die Duplexübertragung wird auch als Vollduplex oder Gegenbetrieb bezeichnet. Bei Vollduplex-Verbindungen erfolgt eine permanente gleichzeitige Übertragung von Daten in beide Richtungen ohne gegenseitige Beeinflussung auf **verschiedenen** Leitungen. Der Datenaustausch im Duplex-Betrieb ist nur mit dafür geeigneten Übertragungsprotokollen möglich (z. B. Ethernet fdx, WLAN oder UMTS/LTE).



Duplex-Betrieb

1.3 Struktur von Kommunikationsnetzen

Grundlagen zur Kommunikation

Die Kommunikation zwischen Endsystemen dient vorwiegend dem wechselseitigen (seltener dem einseitigen) Austausch von Daten. Voraussetzung für eine Kommunikation sind Übertragungseinrichtungen und Übertragungswege sowie Vermittlungseinrichtungen zum Transport der Daten. Ein grundsätzlicher Bestandteil für den Austausch von Daten ist ein gemeinsames Protokoll. Ein **Kommunikationsprotokoll** definiert im informationstechnischen Sinne die Regeln der Kommunikationssprache (Syntax), deren Bedeutung (Semantik) und deren zeitliche Abfolge (Synchronisation).

Vermittlungseinrichtungen (Netzknoten)

Vermittlungseinrichtungen sind Systeme, die für einen Datenaustausch die Vermittlungsfunktionen ausführen. Sie sind für die Auswahl der geeigneten Übertragungsstrecke sowie den geregelten Auf- und Abbau von Kommunikationskanälen verantwortlich.

Der dafür erforderliche Anschluss verbindet die Vermittlungseinrichtung beim Teilnehmer mit einem Netzknoten eines Festnetz- bzw. Mobilfunkanbieters, wie z. B. der Deutschen Telekom, O2 oder Vodafone. In einer lokalen Netzinfrastruktur sind die Netzknoten Switches und/oder Router, welche die Kommunikation zwischen Endsystemen (PC bzw. Server) realisieren.

Anschlussarten

Je nach Nutzungsart wird im Telekommunikationsbereich unterschieden zwischen Wählanschlüssen, Festanschlüssen bzw. Universalanschlüssen.

Universalanschluss war die allgemeine Bezeichnung der Deutschen Telekom für einen ISDN-Anschluss. Grund dafür ist die Tatsache, dass mehrere Telekommunikationsdienstleistungen genutzt werden können. Es besteht unter anderem auch die Möglichkeit, einzelne Dienste während einer Verbindung zu wechseln. Universalanschlüsse werden als Basisanschluss oder Primärmultiplexanschluss angeboten. ISDN wird von den jeweiligen Telekommunikationsanbietern ab Ende 2020 nicht mehr genutzt.

Wählanschlüsse hingegen verbinden die Vermittlungseinrichtungen beim Teilnehmer bei Bedarf mit einem Netzknoten. Die Zusammenschaltung von zwei Wählanschlüssen wird als Wählverbindung (engl. circuit line) bezeichnet.

Festanschlüsse hingegen verbinden die Vermittlungseinrichtungen beim Teilnehmer fix mit einem Netzknoten. Die Zusammenschaltung von zwei Festanschlüssen wird als Festverbindung oder Standleitung (engl. leased line) bezeichnet.

Datenverbindungen

Damit eine Datenübertragung zwischen zwei oder mehreren Punkten möglich wird, ist es erforderlich, die entsprechenden Funktionseinheiten miteinander zu verbinden. Neben einer Verbindung auf physikalischer Ebene ist auch eine logische Verbindung (engl. logical link) erforderlich. Logische Verbindungen werden in entsprechenden Kommunikationsmodellen (ISO/OSI-Schichtenmodell) definiert. Physikalische Verbindungen können permanent oder temporär sein. Über physikalische Verbindungen können Daten zusammen mit anderen Nachrichten quasi zeitgleich mittels eines Multiplexverfahrens (lat. Vielfach/zahlreich) übertragen werden. Logische Verbindungen hingegen sind eindeutig und exklusiv zugewiesen.



Grundsätzliche Kommunikationsstruktur zwischen Übertragungseinrichtungen
(z. B. Router mit physikalischer DSL-Verbindung)

1.4 Übertragungsmedien für Verbindungen

Leitergebundene (kabellose) Systeme

Bei den **kabellosen** (engl. wireless) Systemen werden die Informationen über elektromagnetische Wellen übertragen. Beispiele hierfür sind Funktechniken (z. B. WLAN, Bluetooth, Richtfunk, GSM, UMTS, LTE) oder der Datenaustausch mithilfe von Licht, das im Frequenzbereich Infrarot (IR) bis Ultraviolett liegt. Beispiele sind die IR-Maus-/Tastatur oder Li-Fi (engl. light fidelity).

Leitergebundene (kabelgebundene) Systeme

Kabelgebundene (engl. wired) Systeme werden wiederum in metallische und nichtmetallische Leiter unterteilt. Zu den metallischen Leitern gehören u. a. Fernmeldeleitungen, Steuerleitungen und auch Datenkabel aus Kupfer. Um die Signalbeeinflussung zwischen den Leitungspaaren zu minimieren, werden diese verdrillt. Man bezeichnet dies auch als **Twisted-Pair-Kabel**. Glasfaserkabel oder auch Lichtwellenleiter gehören zu den Übertragungsmedien mit nichtmetallischen Leitern.



Es gibt auch sogenannte Hybridkabel, in denen Glasfaserleitungen und Kupferleitungen gemeinsam geführt werden. Diese Kabel werden in der Praxis jedoch seltener eingesetzt.

Einteilung von Medien

Normalerweise liegen Daten in Form von modulierten elektrischen Schwingungen oder als optische Impulse vor. Damit diese Daten den jeweiligen Adressaten erreichen, ist ein entsprechendes Übertragungsmedium notwendig. Das Übertragungsmedium ist abhängig von der gewählten Signalform. Grundsätzlich können alle Materialien und Stoffe verwendet werden, die für die jeweilige Signalform geeignet sind. Typische Medien sind:

- ✓ Kupferkabel
- ✓ Lichtwellenleiter
- ✓ Elektromagnetische Wellen

Kupferkabel

Die Übertragung von elektrischen Signalen auf Kupferkabeln ist stark von den physikalischen und geometrischen Eigenschaften dieser Kabel abhängig. Grundsätzlich gilt: Je niedriger die Signaldämpfung (Abschwächung des Signals im Vergleich Eingangs- und Ausgangssignal) ist, desto größer ist die Übertragungsreichweite. Ein weiterer wichtiger Faktor bei der Ausbreitung elektrischer Signale auf Kupferkabeln ist die Signalfrequenz (Häufigkeit der periodischen Wiederholungen einer Schwingung) und die damit resultierende Bandbreite. Auch hier gilt die umgekehrt proportionale Verbindung zwischen der Frequenzhöhe und der Reichweite.

Aufgrund der hohen Verfügbarkeit des Rohstoffes und der guten elektrischen Eigenschaften von Kupfer werden Kupferkabel in der Übertragungstechnik sehr häufig verwendet, in der Form von Koaxialkabeln oder als verdrillte Zweidraht- und Mehrdraht-Leitungen (engl. Twisted Pair).

Lichtwellenleiter

Für die Übertragung von Informationen über Lichtwellenleiter (LWL) werden die anliegenden elektrischen Daten in Lichtimpulse umgewandelt. Für die so genannte Signalwandlung – elektrisch nach optisch bzw. optisch nach elektrisch – werden Halbleiter- bzw. Laserdioden als Sender verwendet. In Abhängigkeit vom elektrischen Ansteuersignal (Information) gibt der Sender eine mehr oder weniger große optische Leistung ab. Auf der Empfängerseite sorgen z. B. Fototransistoren für die Generierung von elektrischen Signalen auf Basis der empfangenen Lichtimpulse.

Der Begriff **LWL** ist in der DIN 47002 und VDE 0888 genormt und besagt, dass es sich um ein Medium handelt, in dem moduliertes Licht übertragen wird. Der LWL kann aus Quarzglas (SiO_2) oder Polymer bestehen. Lichtwellenleiter aus Glas (Glasfaserkabel) zeichnen sich unter anderem durch extrem hohe Übertragungsraten aus. Die derzeitige Übertragungstechnik auf Lichtwellenleitern basiert auf einer Intensitätsmodulation bei einer Wellenlänge.

Durch das Wellenlängenmultiplex-Verfahren (WDM) ist die deutliche Anhebung der Übertragungskapazität einer LWL-Verbindung möglich. Grundlage bei diesem Verfahren ist die Modulation (Übertragung mehrerer Nutzsignale auf voneinander unabhängigen Trägersignalen), die je nach Anzahl der verwendeten Lichtwellenlängen, bei diesem Verfahren die Übertragungskapazität erheblich steigert.

Elektromagnetische Wellen

Elektromagnetischen Wellen können uneingeschränkt sowohl über die Atmosphäre als auch im Vakuum übertragen werden. Typische Übertragungsverfahren für den Austausch von Daten sind:

- ✓ Infrarot (IrDA)
- ✓ Wireless LAN (WLAN)
- ✓ Mobilfunk (UMTS, LTE)
- ✓ Global Positioning System (GPS)
- ✓ DECT (Telefon)
- ✓ Funktechnik (Richtfunk, Rundfunk)
- ✓ DVB-T2/S2/C2 (Fernsehen)
- ✓ DAB (Rundfunk)

Die Übertragung von Daten im Vakuum erfolgt außerhalb der Erdatmosphäre. Zur Nachrichtenübertragung werden als Netzwerkknoten Satelliten eingesetzt. Elektromagnetische Wellen werden im Vakuum als Transversalwellen bezeichnet. Diese werden für die verschiedensten Nutzanwendungen wie Forschung, Nachrichtenübertragung und zur Erdbeobachtung verwendet. Je nach Einsatzgebiet unterscheiden sich die einzelnen Satelliten in ihrer Konstruktion, Flughöhe und Flugbahn.

Der Datenaustausch findet im GHz-Bereich statt und eröffnet Frequenzbereiche mit äußerst großer Übertragungskapazität. Nachteil beim Austausch von Daten via Satelliten sind die langen Verzögerungszeiten. Grund dafür sind die langen Übertragungswege zwischen der Bodenstation und dem Satelliten. Bei geostationären Satelliten beträgt die Signallaufzeit etwa 320 ms bis 350 ms pro Verbindung.

Resultierende Topologien

Bedingt durch die Verlegung von Kabeln, ergibt sich eine Struktur der Verkabelung, die auch als physikalische Topologie bezeichnet wird. Dienste, die Daten über diese Kabelwege austauschen, können eine eigene Funktions-Topologie bilden, die sogenannte logische Topologie. Gebräuchlich sind:

- ✓ Ring-Topologie
- ✓ Stern-Topologie
- ✓ Bus-Topologie
- ✓ Baum-Topologie
- ✓ Maschen-Topologie
- ✓ Hybride Formen

Vgl. [https://de.wikipedia.org/wiki/Topologie_\(Rechnernetz\)](https://de.wikipedia.org/wiki/Topologie_(Rechnernetz))

Gemeinsam mit den Netzwerkkomponenten, die entweder passiv (ohne Aufbereitung von elektrischen Signalen z. B. Netzwerkdose, Patchpanel) oder aktiv (z. B. Netzwerkswitch mit Signalaufbereitung) sein können, weisen die Netzwerke eine physikalische Ausbreitung auf, die entweder ein genau definiertes, vom Anwender selbst administriertes Areal (LAN – **Local Area Network**) umfasst, sich über das Gebiet einer Stadt (MAN – **Metropolitan Area Network**) erstreckt oder große Distanzen in Form eines Weitverkehrsnetzes (WAN – **Wide Area Network**) überbrückt. Je nach Betrachtungspunkt sind auch die Begriffe GAN (**Global Area Network**) und UAN (**Universal Area Network**) in Gebrauch.

1.5 Integration verschiedener Dienste

Definition von Diensten

Fernmeldedienste und Datendienste sind die Oberbegriffe für eine Vielzahl von Möglichkeiten zum Austausch von Informationen mittels Dienstprotokollen. Die historische Trennung dieser beiden Gruppen von Diensten existiert heute nicht mehr. Grundsätzlich werden Daten, Sprache und Video zwischen Sender und Empfänger direkt oder über Vermittlungstechnik ausgetauscht. Technisch wird dies über das gleiche Übertragungsmedium und unterschiedliche Dienstprotokolle realisiert. Dienste im Sinne des Datenaustausches sind z. B.:

- ✓ Analoger Telefonie-Dienst
- ✓ ISDN-Dienst
- ✓ Voice over IP (VoIP)
- ✓ Fax-Dienst
- ✓ DSL-Dienst
- ✓ Ethernet (Fast-Ethernet, Gigabit-Ethernet, ..)
- ✓ Datenübertragung per Modem
- ✓ Streaming-Dienst für Video

Der große Vorteil einer Integration verschiedener Dienste in einem System besteht darin, dass nicht für jeden Kommunikationskanal eine eigenständige Netzwerkinfrastruktur aufgebaut werden muss. Bereits bestehende Übertragungswege können zum Austausch der Daten benutzt werden.

1.6 Übertragungstechniken

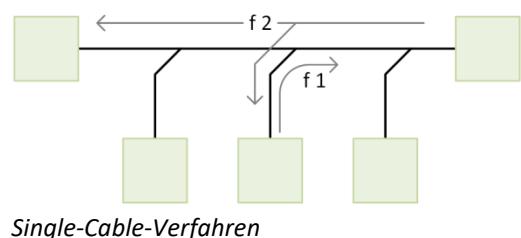
Breitbandtechnik

Bei der Breitbandtechnik erfolgt die Signalübertragung in einzelnen Frequenzkanälen. Zu diesem Zweck werden die Datensignale auf eine Trägerfrequenz moduliert. Das resultierende Datensignal wird anschließend als analoges Signal übertragen. Die Datenstationen müssen über entsprechende Modems (Modulator/Demodulator) verfügen, um die Verarbeitung der Signale bewerkstelligen zu können. Das eingesetzte Verfahren bei der Breitbandtechnik wird als Frequenzmultiplextechnik (Frequency Division Multiplex, FDM) bezeichnet. Die Bandbreite bei dieser Technik liegt zwischen 400 MHz bis zu 1 GHz. Die Ausbreitung des Signals erfolgt richtungsorientiert (unidirektional). Bei der Breitbandtechnik kommen zwei Konzepte zur Anwendung:

- ✓ Mid-Split-Verfahren (engl. Single Cable System)
- ✓ Dualkabel-Verfahren (engl. Dual Cable System)

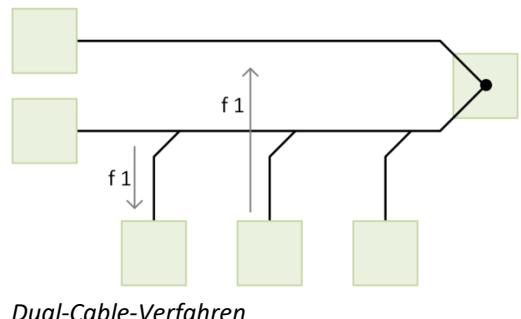
Single-Cable-Verfahren

Beim Single-Cable-Verfahren senden alle Stationen in einem Sendekanal mit der Frequenz f_1 zur Kopfstation (Headend). Die von der Kopfstation empfangenen Signale werden verstärkt und nach einer Frequenzumsetzung auf den Empfangskanal mit der Frequenz f_2 versendet. Alle Datenstationen empfangen dann die Signale mit der Frequenz f_2 .



Dual-Cable-Verfahren

Das Dual-Cable-Verfahren erfordert zwei separate Kabel, die passiv an einer Stelle gekoppelt sind (passiver Headend). Die Datenstationen können nach diesem Verfahren mit gleicher Frequenz senden und empfangen.



Breitband-LAN

Breitbandnetze dieser Bauart wurden auch als lokale Netze eingesetzt. Sie haben aber keine Marktbedeutung mehr. In einem entsprechenden Standard (IEEE 802.10Broad-36) wird für den Einsatz ein 75-Ohm-Breitband-Koaxialkabel vorgeschlagen. Diese Art von Koaxialkabel wird auch für das Kabelfernsehen verwendet.

Breitband-ISDN

Bei Breitband-ISDN (B-ISDN) sind Übertragungsgeschwindigkeiten von mehr als 2 MBit/s bis zu 150 MBit/s möglich. Das B-ISDN wird vor allem bei der Übertragung von schnellen und bandbreitenintensiven Anwendungen wie beispielsweise Videokonferenzen verwendet.

Topologie von Breitbandnetzen

Breitbandnetze werden meistens in einer Baum-Topologie aufgebaut. Den Fußpunkt eines Breitbandsystems bildet die sogenannte Head-End-Station. Von ihr ausgehend kann ein verzweigtes und hierarchisch organisiertes Kabelsystem aufgebaut werden. Das Kabelsystem kann aus einem oder mehreren Hauptsträngen (engl. Trunk), Ästen (engl. Feeder) und Zweigen (engl. Drop Lines) bestehen. Die Endpunkte (engl. Outlet) der Zweige bilden die Anschlusspunkte für die Benutzergeräte.

Neben einer systematisch strukturierten Topologie wie der Baum- oder der Stern-Topologie sind zudem noch beliebige Strukturen denkbar. Da auf einem physikalischen Breitbandsystem mehrere logisch voneinander unabhängige Netze in getrennten Kanälen implementiert werden können, ist die parallele Existenz unterschiedlicher Zugangsverfahren auf demselben Medium möglich.

Basisbandtechnik

Basisbandsysteme sind Systeme, die ohne eine Trägerfrequenz arbeiten. Die Übertragung der Daten erfolgt mit nichtmodulierten Signalen. Das Frequenzspektrum des Sendesignals und die von ihm beanspruchte Bandbreite sind direkt abhängig von der Übertragungsgeschwindigkeit. Die digitalen Signale werden dabei direkt in Form von Impulsen in das Übertragungsmedium eingespeist. Basisband-Systeme stellen nur einen Übertragungskanal zur Verfügung, der logisch auf die verschiedenen Bedürfnisse zugeschnitten ist. Grund dafür ist, dass die ausgetauschten Daten die gesamte Bandbreite oder einen Teil der Bandbreite eines Kabels verwenden und der andere Teil somit nicht mehr für weitere Dienste nutzbar ist.

1.7 Grundlagen der Signalübertragung

Eigenschaften und Kenngrößen der Signalübertragung

Die Qualität einer Signalübertragung z. B. über Kupferkabel ist von vielen Faktoren abhängig. Das Zusammenspiel dieser Faktoren bestimmt die Übertragungseigenschaften von Kupferkabeln wie beispielsweise die Übertragungsgeschwindigkeit, Reichweite und Bandbreite. Im Folgenden soll das Zusammenwirken von Leiterwiderstand, spezifischem Widerstand, Wellenwiderstand und elektrischer Leitfähigkeit näher erläutert werden.

Die physikalischen Kenngrößen, die maßgeblich zur Beeinträchtigung der Übertragungseigenschaften beitragen, sind im Wesentlichen folgende:

- ✓ der Leiterwiderstand und die spezifische Leitfähigkeit des leitenden Materials
- ✓ der Wellenwiderstand
- ✓ die Dämpfung in Abhängigkeit von der Frequenz
- ✓ der Kopplungswiderstand
- ✓ die Rückflussdämpfung

Leiterwiderstand

Der **Leiterwiderstand** wird durch die Qualität des verwendeten Kupfers und den Leiterquerschnitt bestimmt. Der Qualitätsstandard für Kupferkabel wurde international festgelegt. Bezüglich des Leiterquerschnitts haben sich einige Standard-Durchmesser herausgebildet. Bei den am häufigsten eingesetzten Leiterdurchmessern von 0,5 mm und 0,6 mm beträgt der maximal zulässige Leiterwiderstand 175 Ohm/km bzw. 130 Ohm/km. Der Leiterwiderstand ist längenabhängig. Er steigt linear mit der Kabellänge. Er ist ein wichtiger Parameter für die Leitungsdämpfung, weil er maßgeblich die Reichweite der Übertragung bestimmt. Anstelle des Leiterwiderstandes wird in Spezifikationen der Schleifenwiderstand angegeben. Dabei handelt es sich um eine Leiterschleife bestehend aus Hin- und Rückleiter von einem Kilometer. Die Formel für die Berechnung des elektrischen Widerstands lautet:

$$R = \frac{l}{\gamma \cdot A} \quad R: \text{Leiterwiderstand}, A: \text{Leiterquerschnitt}, l: \text{Leiterlänge}, \gamma: \text{Leitfähigkeit}$$

Spezifischer elektrischer Widerstand

Der **spezifische Widerstand eines Leiters** ist gleich seinem Widerstand bei 1 m Länge, 1 mm² Querschnitt und einer Temperatur von 20°C. Er stellt den Kehrwert der elektrischen Leitfähigkeit γ dar.

Beispielsweise beträgt der spezifische Widerstand von Kupfer $\rho = 0,0178 \frac{\Omega \cdot \text{mm}^2}{\text{m}}$.

Elektrische Leitfähigkeit

Die Zahl und Beweglichkeit von freien Ladungsträgern bestimmt die Eignung von verschiedenen Stoffen zur Stromleitung. Die **elektrische Leitfähigkeit fester Körper** hat bei Raumtemperatur eine Variationsbreite von 24 Zehnerpotenzen. Das führt zur Einteilung in drei elektrische Stoffklassen:

Metalle

In Metallen ist die Zahl der freien Ladungsträger sehr groß (je Atom ein freies Elektron). Ihre Beweglichkeit ist eingeschränkt, die elektrische Leitfähigkeit hoch. Die Leitfähigkeit guter Leiter liegt bei 10⁶ Siemens/cm.

Isolatoren

In Isolatoren ist die Zahl der freien Ladungsträger gleich null. Die elektrische Leitfähigkeit ist deshalb auch verschwindend gering. Die Leitfähigkeit bei guten Isolatoren liegt bei 10⁻¹⁸ Siemens/cm.

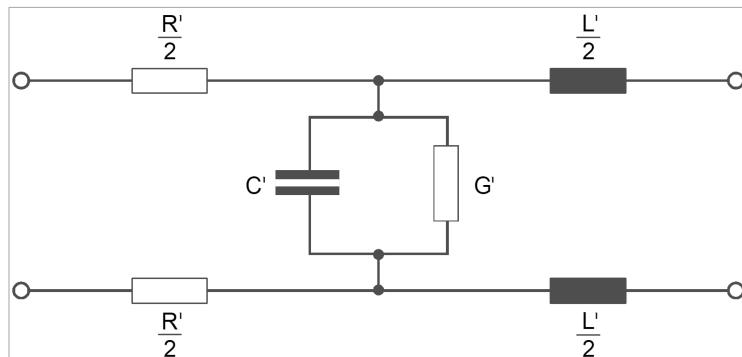
Halbleiter

Die elektrische Leitfähigkeit der Halbleiter liegt zwischen der von Metallen und Isolatoren. Sie ist stark abhängig von Druck, Temperatur und Belichtung.

1.8 Leitungstheorie

Ersatzschaltbild einer Kupferleitung

Leitungsgleichungen können mithilfe von Ersatzschaltungen abgeleitet werden. Jede Leitung hat einen **ohmschen Widerstand R'**, eine **Induktivität L'**, eine **Ableitung G'** und eine **Kapazität C'**. In der Theorie wird vorausgesetzt, dass sich diese Eigenschaften gleichmäßig über die Leitungslängen verteilen. Sie sind proportional zur Leitungslänge. Als „homogen“ bezeichnet man eine Leitung, die über die gesamte Länge eine gleiche Beschaffenheit bezüglich Abschirmung, Isolierung und Verdrillung der Leiterpaare aufweist.

*Ersatzschaltbild für Leitungen*

Die vier Leitungskonstanten werden in der Praxis auf 1 km Leitungslänge bezogen. Sie werden auch bezeichnet als:

- ✓ Widerstandsbelag R'
- ✓ Ableitungsbelag G'
- ✓ Induktivitätsbelag L'
- ✓ Kapazitätsbelag C'

Aus diesen Leitungsparametern lassen sich dann die Übertragungsparameter Wellenwiderstand Z_L und Dämpfung a als Funktion der Frequenz f ableiten.

Widerstandsbelag R'

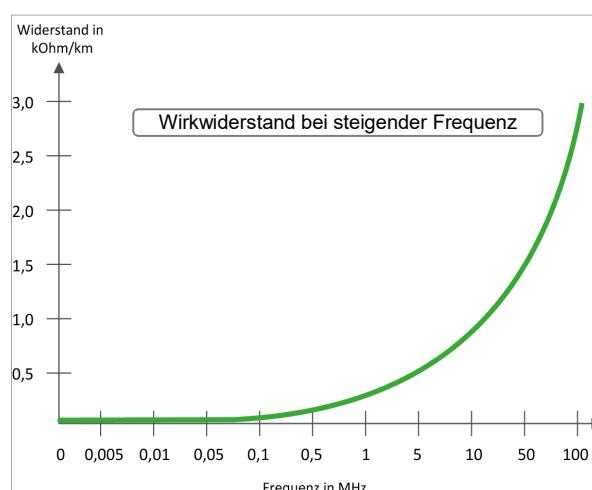
Der **Schleifenwiderstand eines Adernpaars** setzt sich aus dem Gleichstromwiderstand beider Leitungen des Adernpaars zusammen. Die Berechnung des Wechselstromverhaltens eines Kabels ist jedoch wesentlich komplexer.

Die Wechselstromwirkung im Innern des Leiters erzeugt einen Strom, der durch die Induktion des eigenen Magnetfeldes entsteht. Dieser Strom ist dem Betriebsstrom entgegengerichtet und verdrängt diesen mit zunehmender Frequenz nach außen an die Oberfläche des Leiters. Durch diesen Effekt (Skineffekt) wird nur noch eine dünne Schicht des Leiters als wirksamer Leiterquerschnitt genutzt. Die Eindringtiefen sind von Frequenz und Material abhängig. Der Leiterdurchmesser hat auf die Eindringtiefe keinen Einfluss. So hat Kupfer je nach Frequenz folgende Eindringtiefen (siehe Tabelle rechts).

Frequenz	u in μm
1 MHz	66,7
100 MHz	6,7
10 GHz	0,667

Weiterhin haben die Wirbelstromverluste einen Einfluss auf den Wechselstromwiderstand R' . Sie entstehen bei symmetrischen Leitungen durch den Skineffekt (nur bei Kabeln mit metallischer Abschirmung) und die Näheinwirkung von benachbarten Leitern. All diese Faktoren bewirken, dass die Berechnung des Wechselstromwiderstandes sehr aufwendig ist. Im Bild erkennen Sie den typischen Wirkwiderstandsverlauf eines Datenkabels der Kategorie 5 mit 0,6 mm Drahtstärke.

Der Widerstandsbelag wird in $\frac{\Omega}{\text{km}}$ angegeben.



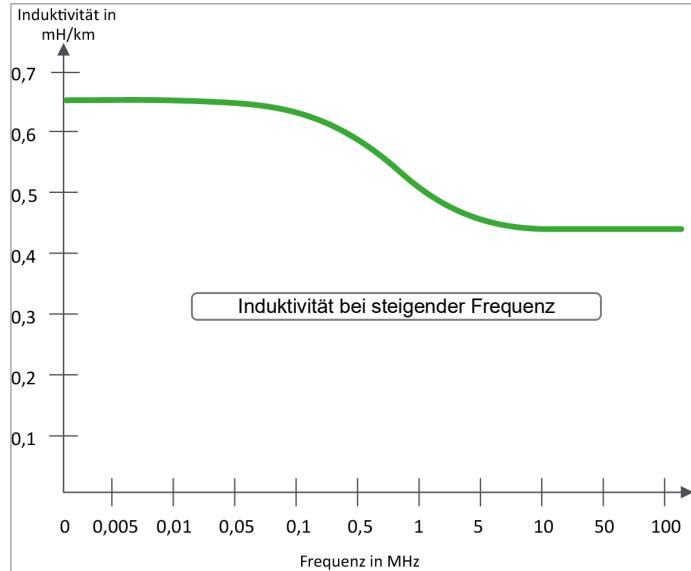
Induktivitätsbelag L'

Der **Induktivitätsbelag** setzt sich aus der äußeren Induktivität ($L'a$) und der inneren Induktivität ($L'i$) zusammen. Die äußere Induktivität ist im Gegensatz zur inneren Induktivität frequenzunabhängig. Bei geschirmten Leitungen wirken zusätzlich die frequenzabhängige Hulleninduktivität ($L'h$) und bei mehrpaarigen Kabeln die durch den Nähoeffekt erzeugte Induktivität ($L'n$).

Sowohl die magnetischen Eigenschaften als auch die Leitungsgeometrie bestimmen die äußere Induktivität. Bei der Verwendung von nicht ferromagnetischen Materialien ist die äußere Induktivität unabhängig von der Größe des Leitungsstromes. Die Magnetfelder der Leiter bestimmen die innere Induktivität. Sie nimmt mit zunehmender Frequenz ab.

Der frequenzabhängige Anteil des Induktivitätsbelages ist sehr gering. Er kann deshalb als frequenzunabhängig bezeichnet werden. Als Richtwert für Kabel gilt:

$$L' = 0,3 \text{ bis } 1 \frac{\text{mH}}{\text{km}}$$



Ableitungsbelag G'

Der **Ableitungsbelag** (G') gibt die Isolationsverluste an. Diese setzen sich aus dielektrischen Verlusten und Koronaverlusten in der Isolierung zwischen den Leitern zusammen. Statt des frequenzabhängigen Ableitungsbelages wird auch der Verlustfaktor $\tan \delta$ angegeben. Die Größe des Verlustfaktors wird von Frequenz, Temperatur und der Isolierung bestimmt. Um sehr gute Hochfrequenzeigenschaften erreichen zu können, müssen Isoliermaterialien mit sehr kleinen Verlustfaktoren verwendet werden.

Kapazitätsbelag C'

Der **Kapazitätsbelag** (auch Betriebskapazität genannt) hängt von der Anordnung der Leiter und der Art des Isoliermaterials ab. Die Kapazität einer Leitung nimmt zu, wenn ...

- ✓ der Abstand der Leiter kleiner wird,
- ✓ die Leiteroberfläche größer wird,
- ✓ die relative Dielektrizitätskonstante groß ist,
- ✓ der Feuchtigkeitsgehalt steigt.

Zur Bestimmung der Betriebskapazität müssen auch verschiedene Teilkapazitäten berücksichtigt werden. Diese werden durch Nachbarleiter und durch die Abschirmung des Kabels erzeugt.

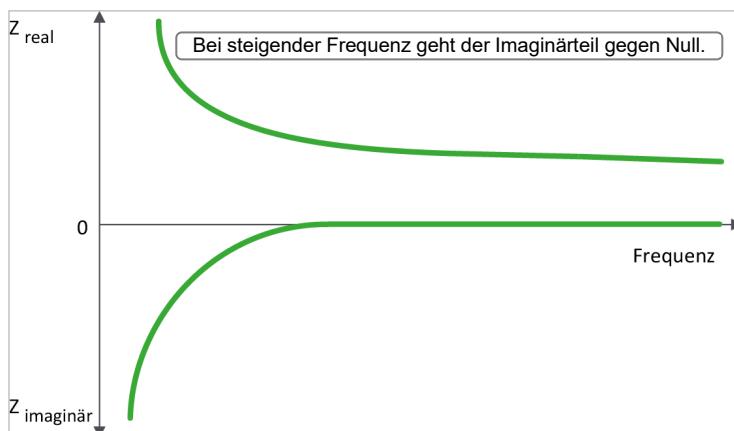
Die **Kapazität** zeichnet die Qualität eines Kabels aus. Je kleiner die Betriebskapazität einer Leitung ist, umso kleiner wird die Dämpfung und desto hochwertiger die Übertragungsleitung. Sie wird in pF/m oder nF/km angegeben. Der Richtwert für TP-Kabel (100 Ohm) liegt bei < 50 pF/m.

Wellenwiderstand

Der **Wellenwiderstand** Z_L setzt sich aus Widerstandsbelag, Kapazitätsbelag, Ableitungsbelag und Induktivitätsbelag zusammen. Er ist eine wichtige Kenngröße in einem Übertragungskreis. Der Wellenwiderstand, auch Wellenimpedanz genannt, ist unabhängig von der Leitungslänge. Er ist in der Regel jedoch in geringem Maße frequenzabhängig (Dispersion). Auch müssen alle Komponenten einer Verbindung (Kabel, Stecker, Buchsen etc.) den gleichen Wellenwiderstand aufweisen, sonst erzeugen diese Reflexionen.

Die Berechnungsformel lautet: $Z_L = \sqrt{\frac{R' + j\omega L'}{G' + j\omega C'}}$

Dieser Parameter besteht aus einem Realteil Z_r und einem Imaginärteil Z_i und wird dargestellt als $Z_L = Z_r + Z_i$. Der Wellenwiderstand Z_L ist das Verhältnis der Wellenspannungen zu den Wellenströmen. Er ist ein Kriterium für die Anpassung der Leitung. Wird eine Leitung an beiden Enden mit ihrem eigenen Wellenwiderstand abgeschlossen, wird eine ankommende Schwingung am Ende nicht reflektiert. Der Imaginärteil des Wellenwiderstandes geht bei Frequenzen ab 2 MHz gegen null. Es wird sich dem Wert Z_0 (Nennwellenwiderstand) genähert.

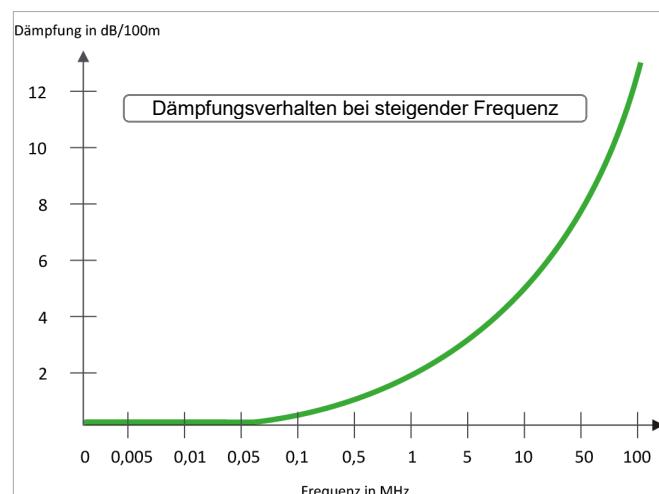


Dieser Wert ist nicht von der Frequenz abhängig und wird als **Impedanz** bezeichnet. Für die Impedanz gilt die nebenstehende Annäherungsformel:

$$Z_0 = \sqrt{\frac{L'}{C'}}$$

Leitungsdämpfung

Jede Übertragungsleitung ist mit Dämpfung behaftet. Ursachen dafür sind die beschränkte Leitfähigkeit der Leiter und die dielektrischen Verluste. Die Amplitude eines Signals längs einer Leitung nimmt somit ab. Der Verlauf der Dämpfung einer qualitativ hochwertigen Datenleitung ist aus dem Beispiel eines Datenkabels der Kategorie 5 ersichtlich. Zusätzlich zur Leitungsdämpfung entsteht eine Fehlerdämpfung. Sie wird durch die Rückflussdämpfung hervorgerufen. Diese Fehlerdämpfung kann das Übertragungsverhalten einer Leitung sehr negativ beeinflussen.



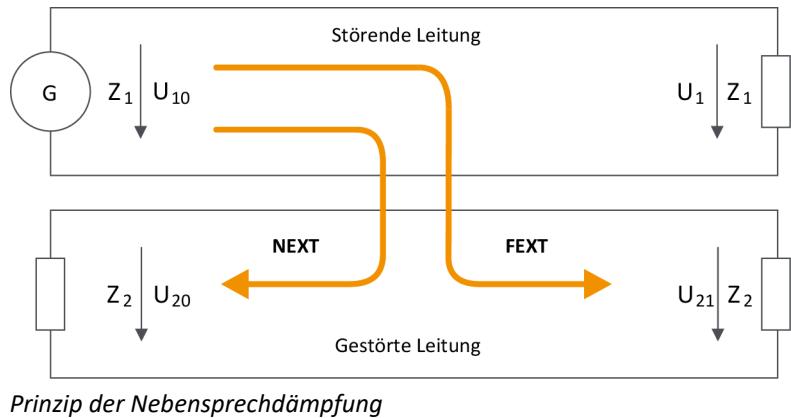
Nahnebensprechdämpfung (NEXT)

Nebensprechen ist der ungewollte Übertritt elektrischer Signale von einem Nachrichtenweg auf einen andern. Es entsteht bei symmetrischen Leitungen durch die Strominduktion in benachbarte Adern, da jede Ader ein elektromagnetisches Feld bildet. Dieses Störsignal kann an beiden Enden der gestörten Leitungen gemessen werden. Die am nahen Ende auftretende Störung wird Nahnebensprechen NEXT (engl. near end crosstalk) genannt, diejenige am entfernten Ende Fernnebensprechen FEXT (engl. far end crosstalk).

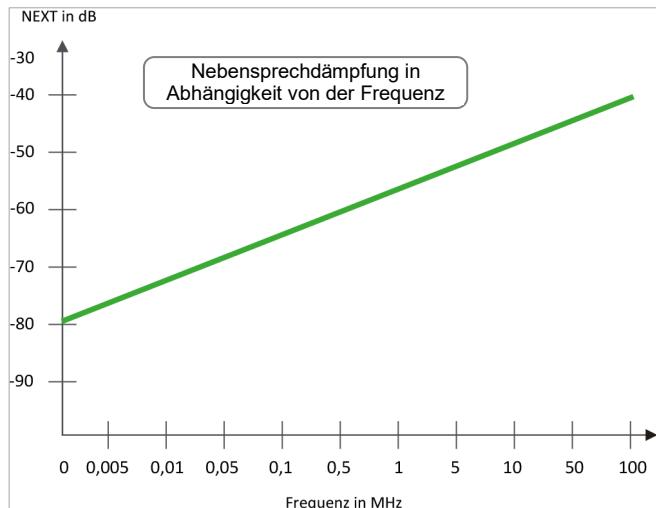
Bei der Verwendung von zweipaarigen Kabeln werden über ein Paar die Daten gesendet und über das andere Paar die Daten empfangen. Hier ist besonders auf das NEXT zu achten. Wenn mehrere Paare und somit auch mehrere Informationsdienste im gleichen Kabel benutzt werden sollen, ist zusätzlich auf das FEXT zu achten.

Die Nebensprechdämpfung (a_N) wird in dB angegeben und lässt sich nur ungenau berechnen. Sie wird in der Regel durch Messungen ermittelt. Das Nebensprechen kann reduziert werden, indem die Adernpaare der Kabel gegeneinander verdrillt (twisted pair) werden.

$$a_N = 20 \log \frac{U_1}{U_2} + 10 \log \frac{Z_2}{Z_1}$$



Vor allem im Kommunikationsbereich ist eine hohe Nebensprechdämpfung von großer Wichtigkeit. Sie verhindert das Übertreten von Informationen auf benachbarte Adern. Die Nebensprechdämpfung ist frequenzabhängig. Bei einer Länge von 450 m liegen die NEXT-Werte bei 100 MHz für paarverseilte Kabel bei 40 dB und für paargeschirmte Kabel bei über 70 dB. FEXT-Werte liegen höher, da hier die Leitungsdämpfung mit einfließt. Dieser Wert hängt von der Leitungslänge ab.



Kopplungswiderstand

Schirme können aufgrund ihrer Beschaffenheit sehr unterschiedliche Eigenschaften aufweisen. Deshalb wurde in den zuständigen Normungsgremien der **Kopplungswiderstand** (auch Transferimpedanz oder Schirmkoppelimpedanz genannt) für Kabel festgelegt. Der Kopplungswiderstand ist ein Maß für die Güte der Schirmung. Er wird als das Verhältnis der Spannung längs des Schirms des gestörten Systems zu dem Strom des störenden Systems definiert. Die Grenzwerte dürfen 50 mΩ/m bei 1 MHz und 100 mΩ/m bei 10 MHz nicht überschreiten. Die Größe und der Frequenzgang des Kopplungswiderstandes werden vom Aufbau der Schirmung bestimmt. Bei Gleichstrom und tiefen Frequenzen ist der Kopplungswiderstand gleich dem Gleichstromwiderstand der Schirmung. Bei steigenden Frequenzen verhält er sich völlig unterschiedlich. Die Schirmdämpfung für geschirmte symmetrische Kabel kann deshalb nur durch Messungen bestimmt werden. Es gibt mehrere unterschiedliche Messmethoden, die sich in dem zu messenden Frequenzbereich unterscheiden.

Isolationswiderstand

Der **Isolationswiderstand** ergibt sich aus der Qualität des verwendeten Isoliermaterials zwischen zwei Leitern oder zwischen einem Leiter und der Schirmung. Entscheidend dabei ist das verwendete **Isolationsmaterial** und nicht die Stärke der Isolation. Der Isolationswiderstand ist längenabhängig und wird in $\Omega \cdot m$ bzw. $G\Omega \cdot km$ angegeben. Der Idealwert liegt bei $1G\Omega \cdot km$. Durch die Längenabhängigkeit sinkt der Isolationswiderstand mit der Länge einer Strecke.

Rückflussdämpfung

Die **Rückflussdämpfung** ist das Maß der reflektierten Signale im Verhältnis zum gesendeten Nutzsignal. Reflektierte Signale werden durch Variationen in der Struktur der Kabel erzeugt. Die Rückflussdämpfung ist ein sehr guter Gradmesser für die Qualität eines Kupferkabels. Liegt diese z. B. über 25 dB, weist das Kabel eine gute Qualität auf. Bei installierten Kabeln kann sich die Rückflussdämpfung durch Fehlanpassung der Stecksysteme und durch metallische Objekte im näheren Umfeld ungeschirmter Kabel negativ auswirken. Die elektromagnetischen Felder um die Kabel werden durch diese Nachbarobjekte abgeleitet. Die so erzeugten Abweichungen im Übertragungsverhalten führen vermehrt zu Reflexionen. Bei geschirmten Kabeln haben solche Objekte keinen Einfluss, weil die elektromagnetischen Felder über den Schirm abgeleitet werden.

PSNEXT (Powersum NEXT)

Die **Powersum NEXT** beinhaltet die Summe aller Störsignale, die in ein Leiterpaar eingekoppelt werden. Je mehr Adernpaare in einem symmetrischen Kabel verwendet werden, desto wichtiger ist der PSNEXT-Wert. Wird nur ein zweipaariges Kabel eingesetzt, ist das PSNEXT gleich dem NEXT. Die Unterschiede werden bei steigender Leiterpaarzahl immer größer, da die Störsignale von mehreren Leiterpaaren in ein Leiterpaar eingekoppelt werden.

Signalausbreitungsgeschwindigkeit

Innerhalb von Kabeln breiten sich Signale mit unterschiedlichen Geschwindigkeiten aus. Dies ist sowohl für metallische Leiter als auch für optische Übertragungsmedien der Fall. Die **Ausbreitungsgeschwindigkeit** hängt vom Übertragungsmedium ab und ist kleiner als die Lichtgeschwindigkeit. Die Verringerung der Geschwindigkeit wird durch den Verkürzungsfaktor hervorgerufen. Der **Verkürzungsfaktor** für Koaxialkabel beträgt 0,77, für verdrillte Kabel 0,6 und für LWL-Kabel 0,67. Das bedeutet, dass die Signalausbreitungsgeschwindigkeit z. B. in Koaxialkabeln 77 % der Lichtgeschwindigkeit beträgt. Bei Lichtwellenleitern wird die Ausbreitungsgeschwindigkeit für verschiedene Wellenlängen als Gruppengeschwindigkeit bezeichnet.

Laufzeit

Die **Laufzeit** drückt die Zeit aus, die ein Signal benötigt, um von einem Punkt eines Übertragungsmediums zu einem anderen zu kommen. Sie hängt vom verwendeten Übertragungsmedium ab und entspricht der Lichtgeschwindigkeit (bei Satellitenübertragung) oder etwas weniger (bei der Übertragung in Kupferkabeln). Sie ist im Wesentlichen von der Übertragungseigenschaft des Mediums bzw. bei Lichtwellenleitern von der Brechung abhängig. Nach dem Ethernet-Standard beträgt die maximale Signallaufzeit auf dem Kabel in einem 1 Gbit/s-Netzwerk 0,26 µs, bei einem 10 Gbit/s-Netzwerk 0,026 µs.

Signalverzögerung

Unter **Verzögerungs- oder Wartezeit** wird die Zeitspanne verstanden, die ein Signal später beim Empfänger eintrifft, als es beim Sender abgeschickt wurde. Gerade bei Echtzeitanwendungen ist die Verzögerungszeit von besonderer Bedeutung. Bei der Übertragung von Sprachdiensten sind die Verzögerungszeit und das Echo ein besonderes Merkmal für die Qualität der Übertragung. Für das klassische Telefonnetz wurden die Ende-zu-Ende-Laufzeiten im nationalen Bereich auf 25 ms vorgeschrieben. Im internationalen Bereich beträgt diese Laufzeit 100 ms. In paketorientierten Netzen (z. B. Sprachübertragung über Internet, Voice over IP) kommt es bei der Sprachübertragung generell zu umsetzungs- und netzspezifischen Verzögerungen. Bei der Übertragung von grafischen Informationen in Echtzeit liegt der akzeptable Wert bei 30 ms. Im Weitverkehrsbereich sollte die Verzögerungszeit 100 ms nicht überschreiten (dies hängt jedoch stark von der Kommunikation der Provider im Netzverbund ab), im LAN muss sie unter 10 ms liegen.

Signalverformung

Bei elektrischen Signalen werden durch Dämpfung des Kabels die Flanken der Rechtecksignale „verschliffen“. Die Verformung der Signale wird umso größer, je weiter der Sender vom Empfänger entfernt ist. Die Signalverformung darf jedoch maximal nur so groß sein, dass die einzelnen Signalimpulse noch eindeutig vom Empfänger interpretiert werden können. Solche Verformungen können z. B. mithilfe von Regeneratoren (Repeatern) ausgeglichen werden.



Signalverformung (vereinfachte Darstellung)

1.9 Übung

Fragen zur Netzwerkkommunikation

Übungsdatei: --

Ergebnisdatei: uebung01.pdf

1. Welche allgemeinen Voraussetzungen sind für die Kommunikation in Netzen erforderlich?

2 Medien für die Datenübertragung

In diesem Kapitel erfahren Sie

- ✓ welche Medien für Datenübertragungen nutzbar sind
- ✓ wie sich die Medien voneinander unterscheiden
- ✓ welche Eigenschaften unterschiedliche Medien besitzen

2.1 Kabel mit metallischen Leitern

Im Wesentlichen werden Übertragungsmedien mit metallischen Leitern in drei Bauformen eingeteilt:

- ✓ Koaxialkabel
- ✓ Symmetrische Kabel
- ✓ Unsymmetrische Kabel

Bei unsymmetrischen Kabeln sind die Adern längs verseilt (Verdrillen von Drähten). Das Einsatzgebiet solcher Kabel beschränkt sich auf die Bereiche Steuer- und Regeltechnik sowie auf den Maschinenbau. Im Bereich der Datentechnik kommt diese Art von Kabel nicht zum Einsatz. Unsymmetrisch aufgebaute Kabel sind nur für Übertragungsfrequenzen im Bereich von einigen Megahertz (MHz) geeignet. In der Datentechnik werden jedoch wesentlich höhere Übertragungsfrequenzen gefordert.

Koaxialkabel sind eine Sonderbauform der unsymmetrischen Kabel. Je nach Wellenwiderstand werden diese Kabel für unterschiedliche Anwendungen genutzt, z. B. für den Multimediacbereich bzw. Kabelprovider und erlauben Übertragungsfrequenzen im Gigahertz-Bereich (GHz).



Aufbau von Kupferkabeln

Die wichtigsten Merkmale von elektrischen Leitern zur Datenübertragung sind die mechanischen und elektrischen Eigenschaften, wie:

- ✓ Leiterkonstruktion
- ✓ Ummantelung
- ✓ Isolationsmaterialien der Kabel
- ✓ Verseilung der Adern
- ✓ Abschirmung
- ✓ Übertragungsverhalten (z. B. Dämpfung, Laufzeit)

Leiterkonstruktion

Kabel mit metallischen Leitern sind aus einer oder mehreren Adern aufgebaut. Diese Adern können ihrerseits wiederum aus vielen feindrähtigen Leitern (Litze) oder aus einem massiven Leiter bestimmten Querschnitts bestehen (Kompaktader). In technischen Dokumentationen wird oft mit der Bezeichnung AWG (American Wire Gauge) gearbeitet. Sie gibt den Durchmesser bzw. Querschnitt eines Drahtes codiert wieder. So hat ein Kabel mit der Bezeichnung AWG24 einen Durchmesser von 0,511 mm und bei AWG26 sind es 0,405 mm.

Der Einsatz der jeweiligen Leiterart ist abhängig von den gestellten Anforderungen. So sind massive Leiter für festverlegte Kabel besser geeignet als feindrähtige Kabel. Massive Leiter haben den Nachteil, dass sie aufgrund ihrer Eigenschaften weniger biegsam und starrer sind. Sie haben jedoch bessere elektrische Eigenschaften (aufgrund ihres größeren Querschnittes) als feindrähtige Kabel. Letztere sind wiederum besser als Patchkabel (engl. to patch – zusammenschalten) oder Anschlusskabel für PCs bzw. Peripheriegeräte geeignet, da sie flexibler und somit leichter zu handhaben sind.



Übertragungsmedien mit metallischen Leitern können aus unterschiedlichen Materialien bestehen. Am häufigsten wird Kupfer als elektrischer Leiter verwendet. Andere Rohstoffe könnten ebenfalls Verwendung finden, sind aber meistens aufgrund ihrer Rohstoffpreise oder Verarbeitung nur bedingt im Einsatz.

Material	Leitfähigkeit	Löteigenschaften	Biegeeigenschaften	Kosten
Kupfer	Sehr gut	Gut	Sehr gut	Gering
Kupfer verzинnt	Sehr gut	Sehr gut	Gut	Gering
Kupfer versilbert	Sehr gut	Sehr gut	Gut	Sehr hoch
Kupfer vernickelt	Gut	Ausreichend	Befriedigend	Mittel
Nickel	Befriedigend	Nicht möglich	Ausreichend	Hoch
Aluminium	Gut	Schlecht	Sehr gut	Gering

Ummantelung

Neben den mechanischen und elektrischen Eigenschaften von Leitern ist der **Kabelmantel** ein wichtiges Merkmal bei den leitergebundenen Medien. Der Kabelmantel schützt den Leiter vor äußerer Beanspruchungen wie Zug, Druck und Torsion. Aber auch gegen Feuchtigkeit, chemische Einwirkungen und Flammeinwirkung bietet der Mantel Schutz. Bei der Auswahl des geeigneten Mantels spielt auch der Einsatzort eine wichtige Rolle. Für In-Haus-Verkabelungen gelten andere Maßstäbe als für eine Verlegung im Außenbereich.

Eine besondere Stellung nehmen industrielle Anwendungsbereiche ein, da in diesem Bereich mitunter extremere Umweltbedingungen für das Kabel vorliegen. Das Material für den Außenmantel sollte in so einem Umfeld vorher mit dem Kabelhersteller abgestimmt werden.

Im Außenbereich sollten Kabel immer mit einem Nagetierschutz und einer Längs- und Querwasserdichtigkeit geschützt werden.

Typische Isolier- und Mantelwerkstoffe nach DIN VDE 0292 (Auszug)

Werkstoff	Abkürzung	DIN/VDE-Bezeichnung
Ethylen-Propylen-Kautschuk	EPR	B
Ethylen-Vinylacetat-Copolymer	EVA	G
Natur- u./o. Synthetischer Kautschuk	NR u./o. SR	R
Polyethylen vernetzt	PE	Z
Polyurethan	PUR	Q
Polyvinylchlorid kältebeständig	PVC	V3
Polyvinylchlorid ölbeständig	öPVC	V5
Polyvinylchlorid vernetzt	xPVC	V4
Polyvinylchlorid wärmebeständig	PVC	V2
Silikonkautschuk	SiR	S
Textilbeflechtung mit flammwidriger Masse	PE	T2

Für den Einsatz von Datenkabeln in Ihrem Unternehmen werden Sie flammwidrige und halogenfreie Kabel verwenden. Die im internationalen Sprachgebrauch üblichen Bezeichnungen für **halogenfreie, flammwidrige Werkstoffe** (engl. Compounds) sind:

- ✓ Flame Retardant = FR
- ✓ Non Corrosive = NC
- ✓ Low Smoke Zero Halogene = LS0H

Flammwidrige Isolations- und Mantelmischungen erlöschen bei Entzündung selbst. Besonders in Büroumgebungen ist ein Einsatz solcher Kabel zwingend erforderlich. Eine sternförmige Struktur kann aufgrund ihrer „dicken“ Kabelstränge an entsprechenden Stellen die Brandlast (Wärme durch Verbrennung) erhöhen. Gerade PVC entwickelt beim Verbrennen hochgiftige Gase, die zusammen mit Wasser aggressive und zerstörende Säuren bilden.

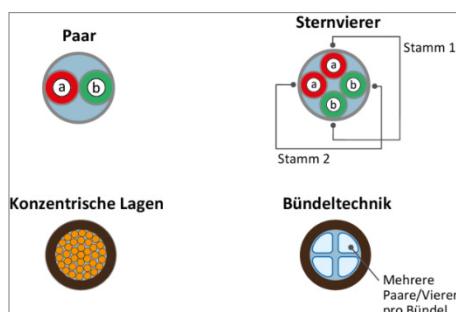
Prüfen Sie deshalb vor dem Verlegen Ihrer Datenkabel, ob diese halogenfrei sind. Angaben hierzu finden Sie in den Datenblättern der jeweiligen Hersteller oder direkt auf dem Kabel, z. B. S/STP 4x2xAWG24 4P *H*.



Ein weiterer Vorteil halogenfreier, flammwidriger Mischungen ist die Tatsache, dass bei ihrer Verbrennung keine Dioxine entstehen.

Verseilung und Bündelung

Eine **Verseilung** ist das gegenseitige Verdrillen (engl. twisted pair) von isolierten Adern. Um eine gegenseitige Störung der Adern bei symmetrischen Kabeln zu vermeiden, werden diese nach einem bestimmten Schema miteinander verseilt. Typischerweise werden jeweils zwei oder vier Adern zu einem Paar bzw. Vierer verseilt. Bei einer Verseilung werden die Adern in konzentrische Lagen oder Bündel angeordnet. Je nach Ausführung wird zwischen **Lagenverseilung** oder **Bündelverseilung** unterschieden.



Verseilarten; links unten: Lagenverseilung, daneben: Bündelverseilung

Die Anzahl der Verdrillungen pro Meter (Schlaglänge) ist eine konstruktive Maßnahme zur Unterdrückung des Übersprechens bei symmetrischen Kabeln. Einige Kabelhersteller benutzen auch eigene Verseiltechniken zur Störungsunterdrückung.

Abschirmung

Zum Schutz vor störenden Einflüssen auf die signalführenden Adern sind Leitungen für die Datenübertragung geschirmt. Eine Schirmung reduziert zudem die Abstrahlung von elektromagnetischen Wellen. Bei der Schirmung wird zwischen Folien- und Geflechtschirm unterschieden. Eine Kombination aus beiden ist ebenfalls möglich. Die Anzahl der Kabelelemente, welche eine gemeinsame Schirmung benutzen, wird wie folgt eingeteilt:

- | | |
|---------------------------------|---------------------------------|
| ✓ Ader in Metall-Folie (AiMF) | ✓ Vierer in Metall-Folie (ViMF) |
| ✓ Paar in Metall-Folie (PiMF) | ✓ Bündel in Metall-Folie (BiMF) |
| ✓ Dreier in Metall-Folie (DiMF) | |

Als Material für die Folienschirmung werden alukaschierte bzw. aluminiumbedampfte Polyesterfolien eingesetzt. Ein Geflechtschirm besteht aus einem Kupfergeflecht.

Übertragungsverhalten

Damit eine optimale Datenübertragung stattfinden kann, werden an die elektrischen Leiter unterschiedliche Anforderungen gestellt. Neben den Standardwerten, wie Leiterquerschnitt, Leitfähigkeit bzw. Widerstand, tragen auch Parameter, wie Isolationswiderstand und Wellenwiderstand, zur Leitungsqualität bei.



Der Wellenwiderstand ist eine Größe, die sich aus Leiterwiderstand, Isolationswiderstand, Betriebskapazität und Betriebsinduktivität zusammensetzt. Bei einer Fehlanpassung der Leitung an den Wellenwiderstand kann es zu Reflexionen kommen. Er ist **unabhängig** von der Leiterlänge.

Die Einkopplung von Signalen von einem Leiter auf den anderen wirkt sich negativ auf das Übertragungsverhalten aus. Dieses Übersprechen (oder Nebensprechen) von Signalen ist frequenzabhängig. Durch eine mechanische Veränderung des Verseilaufbaus verändern sich die Eigenschaften der Kabel. Hohe mechanische Beanspruchungen bei der Installation erhöhen daher das Nebensprechen. Durch zu hohe Zug- und Druckkräfte bei der Installation wird der Leiterquerschnitt verändert (Kaltfließen). Das Resultat ist ein zu hoher Dämpfungswert.

Für die Verwendung von Kupferkabeln zur Datenübertragung gelten folgende Anforderungen:

- ✓ geringe Dämpfung
- ✓ hohe Übertragungsfrequenz
- ✓ große Reichweiten
- ✓ geringes Übersprechen

Sternvierer-Kabel (twisted quad)

Bei einem **Sternvierer-Kabel** handelt es sich um ein verbessertes Telefonkabel, bei dem vier isolierte Adern miteinander verseilt sind. Haupteinsatzgebiet solcher Kabel ist die Telefonie. Besonderes Merkmal dieser Kabel ist die Konstruktion. Sternvierer-Kabel sind so stabil verseilt, dass auch nach einer hohen Beanspruchung beim Verlegen die Adern nicht verschoben werden. Der Sternvierer gehört zur Gruppe der Twisted-Pair-Kabel. Gängige Varianten der Sternvierer-Kabel sind:

- ✓ J-YY 2 x 2 x 0.6 = zwei Doppeladern
- ✓ J-YY 4 x 2 x 0.6 = vier Doppeladern
- ✓ J-YY 6 x 2 x 0.6 = sechs Doppeladern
- ✓ J-YY 10 x 2 x 0.6 = zehn Doppeladern
- ✓ J-YY 20 x 2 x 0.6 = zwanzig Doppeladern
- ✓ J-YY 50 x 2 x 0.6 = fünfzig Doppeladern
- ✓ J-YY 100 x 2 x 0.6 = hundert Doppeladern

Sternvierer-Kabel gibt es für den Innen- und Außenbereich. Außenkabel werden hauptsächlich als 200 x, 500 x oder 1000 x 2 x 0.6 in Form von Verbindungskabeln zur Vermittlungsstelle verlegt. Sternvierer-Kabel verfügen über den großen Vorteil, dass die Abmessungen geringer sind als bei Twisted-Pair-Kabeln. Dies ist gerade bei kleinen und verwinkelten Kabelführungen von großem Vorteil.

Koaxialkabel

Koaxialkabel stellten zum Anfang der Ethernet-Ära die gängigste Netzwerkverkabelung dar. Die Hauptgründe dafür waren zum einen die einfache Installation und zum anderen die geringe Anfälligkeit gegen Störstrahlungen. Koaxialkabel erforderten eine Bus-Topologie und ermöglichen nur einen Halbduplexbetrieb, wobei die maximale Übertragungsrate weniger als 10 Mbit/s betrug.

Koaxialkabel werden im Bereich Netzwerktechnik ausschließlich bei Bus- oder Stern-Topologien eingesetzt. Im Vergleich zu einer Twisted-Pair- oder Glasfaserkabelung ist eine Lösung mit Koaxialkabeln sehr kostengünstig. Im Netzwerkbereich wird dieser Kabeltyp nur punktuell eingesetzt, bei Kabelprovidern ist er für die Verbindung zum Endkunden Standard.



Koaxialkabel sind eine Sonderbauform der unsymmetrischen Kabel. Je nach Wellenwiderstand werden diese Kabel für unterschiedliche Anwendungen genutzt, z. B. für den Multimediacomplex bzw. Kabelprovider. Sie erlauben Übertragungsfrequenzen im Gigahertz-Bereich (GHz).

Twisted-Pair-Kabel (TP)

Die wichtigste Form der symmetrischen Kupferkabel ist das **Twisted-Pair-Kabel**. In der Netzwerktechnik wird überwiegend diese Bauform verwendet. Durch den verseltenen Aufbau von paarweise isolierten Adern werden günstige Eigenschaften für das Übertragungsverhalten erzielt. Zudem minimiert die paarweise Verdrillung (engl. twisted pair) der Adernpaare ein Einkoppeln durch Störungen von außen und die Beeinflussung zwischen den Adernpaaren. TP-Kabel gibt es in verschiedenen Ausführungen:

- ✓ als ungeschirmtes (engl. unshielded) TP-Kabel = U/UTP, früher nur „UTP“ genannt
- ✓ als geschirmtes (engl. shielded) TP-Kabel = früher oft nur als „STP“ bezeichnet

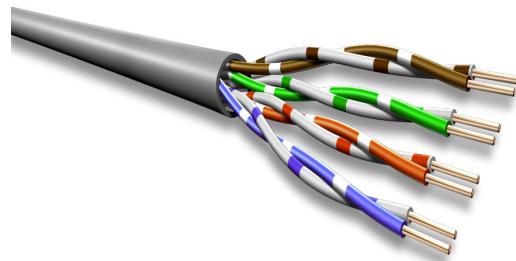
und in Kombination nach ISO/IEC 11801:

- ✓ als Twisted-Pair-Kabel mit einem Gesamtschirm (Folie F, Schirmgeflecht S oder Schirmgeflecht und Folie SF) = F/UTP, S/UTP, SF/UTP
- ✓ als Twisted-Pair-Kabel mit Gesamtschirm und einem Elementschirm für die Adernpaare = S/FTP, S/SFTP

Aufgrund ihrer elektrischen Eigenschaften werden im Datenkommunikationsbereich ausschließlich Twisted-Pair-Kabel eingesetzt. Das TP-Kabel wurde für die breitbandige Übertragung von Sprach-, Video- und Dateninformationen konzipiert. Es sind Übertragungsraten bis zu 10 Gbit/s und mehr erreichbar. Die Standardausführung von TP-Kabeln ist vierpaarig. Einpaarige TP-Kabel werden auch als Twinax-Kabel bezeichnet.

Unshielded Twisted-Pair-Kabel (UTP)

Unshielded (ungeschirmt) bedeutet, dass die einzelnen verdrillten Adernpaare keine Paarschirmung besitzen. Durch diese Art der Konstruktion sind UTP-Kabel sehr anfällig für Störungen von außen, so z. B. durch Übersprechen von Signalen benachbarter Paare oder durch Transienten (hochfrequente Störimpulse) von Schaltanlagen. Sind UTP-Kabel in einer industriellen Umgebung verlegt, können Maschinen durch hohe Schaltströme und -spannungen Störimpulse einkoppeln.



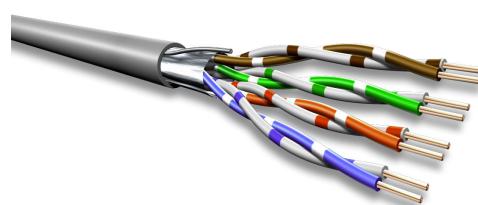
UTP-Kabel

Dies wirkt sich nachteilig auf die Datenübertragung aus. In Datennetzen werden UTP-Kabel hauptsächlich für Datenübertragungsraten bis 1 Gbit/s eingesetzt, obwohl sie bis 10 Gbit/s spezifiziert sind.

UTP-Kabel werden nach DIN EN 50173 in Deutschland nicht empfohlen, weshalb sie hier auch seltener eingesetzt werden. Der Grund sind die Vorgaben zur elektromagnetischen Verträglichkeit (EMV). Dagegen sind UTP-Kabel weltweit die meistverwendeten Kabel für lokale Netzwerke. Vorteilhaft sind die einfachere Kabelverlegung und Anschlusstechnik sowie der Wegfall der Schirmung (Potentialausgleich).

Shielded Twisted-Pair-Kabel (STP)

Shielded (geschirmt) bedeutet, dass die verdrillten Adernpaare über eine Paarschirmung verfügen. Diese Art von Kabel ist unempfindlicher gegen Störstrahlung von außen. Durch den Folienschirm werden die Adernpaare vor Einwirkungen von benachbarten Leitungen geschützt. Auch die eigene Abstrahlung wird durch diese Schirmung reduziert. Das Übertragungsverhalten von STP-Kabeln gegenüber UTP-Kabeln ist wesentlich besser. Dadurch lassen sich höhere Datenraten bei gleicher Distanz übertragen.



STP-Kabel

Durch einen zusätzlichen Gesamtschirm aus Kupfergeflecht lassen sich sowohl innere als auch äußere Stör-einwirkungen auf das Gesamtsystem weiter mindern. Gerade im Hinblick auf die EMV (elektromagnetische Verträglichkeit) ist diese Bauform sinnvoll. Die F/UTP- bzw. S/FTP-Kabel finden hauptsächlich in der strukturierten Gebäudeverkabelung Anwendung. Für höchste Anforderungen finden F/SFTP-Kabel Anwendung. STP-Kabel werden grundsätzlich bei Verkabelungen und Erweiterungen von Netzwerken im Inhouse-Bereich eingesetzt. Dieser Kabeltyp wird überwiegend im Bereich der Arbeitsplatz-Verkabelung (Tertiärbereich) verwendet. Gegenüber den Kabeln vom Typ UTP sind die aktuellen STP-Medien für höhere Frequenzspezifizierungen ausgelegt, was die Integration zukünftiger Datenübertragungsprotokolle auf diesem Medium vereinfacht.

Einteilung der Kategorien gemäß ISO/IEC

Da es bei den vielseitig einsetzbaren symmetrischen Kupferkabeln verschiedene Kabelarten gibt, wird eine Klassifizierung benötigt. Grundlage für eine Klassifizierung von Kupferkabeln zur Signalübertragung in der Daten-technik bilden die Normen der ISO (International Standard Organization) und IEC (International Electrotechnical Commission). Eine Norm mit der Bezeichnung **ISO/IEC DIS 11801** legt z. B. die Kabelstandards fest, für welche Zwecke Kupferkabel verwendet werden. Die europäische Norm **EN 50173** beruht auf der internationalen Norm **ISO/IEC 11801**. Die im Wesentlichen festgelegten Eigenschaften sind:

- ✓ Wellenwiderstand
- ✓ Rückflussdämpfung
- ✓ Übertragungsstreckenlänge
- ✓ Dämpfung
- ✓ Nahnebensprechdämpfung
- ✓ Dämpfungs-Nebensprechdämpfungs-Verhältnis
- ✓ Gleichstrom-Schleifenwiderstand
- ✓ Laufzeit

Um einen besseren Überblick über die verschiedenen Kabelarten zu bekommen, sind diese in unterschiedliche Kategorien eingeteilt. Diese Kategorien berücksichtigen bereits obige Standardwerte für den jeweiligen Einsatzbereich.

Kategorie	Klasse	Frequenzbereich	Anwendung
Kategorie 1	Klasse A	Bis 100 KHz	Telefonie, Modem DFÜ
Kategorie 2	Klasse B	Bis 1 MHz	ISDN, IBM-Verkabelung Typ 3
Kategorie 3	Klasse C	4 bis 16 MHz	Ethernet, Telefonie
Kategorie 4		Bis 20 MHz	Wird nicht benutzt
Kategorie 5/5e	Klasse D	Bis 100 MHz	Fast-Ethernet, ATM, Gigabit-Ethernet
Kategorie 6/6A	Klasse E/EA	Bis 250/500 MHz	10-Gigabit-Ethernet
Kategorie 7/7A	Klasse F/FA	Bis 600/1000 MHz	10-Gigabit-Ethernet
Kategorie 8.1/8.2	Klasse I/II	Bis 2 GHz	25-Gigabit-Ethernet, 40-Gigabit-Ethernet

Die Einteilung in Kategorien bezieht sich nur auf die Einzelkomponenten wie Kabel oder Anschlusstechnik. In der Einteilung nach Klassen wird der komplette Übertragungskanal berücksichtigt.

Anschlusstechnik

Die **RJ-45-Anschlusstechnik** ist in Netzwerken flächendeckend im Einsatz. Durch die Bauform wurde diese Technik ursprünglich nur bis 500 MHz (Cat6A) spezifiziert, was die maximal mögliche Datenübertragungsrate auf 10 Gbit/s einschränkte. Für höchste Übertragungsanforderungen (25-/40-Gigabit-Ethernet) wurde die Technik dann für die Kategorie 8.1 novelliert. Diese Kategorie ist rückwärtskompatibel zum RJ-45-Steckgesicht der Kategorien 6A, 6 und 5 der ISO/IEC 11801 und der EN 50173. RJ-45 ist nicht kompatibel mit der Kategorie 7 und 7A, daher wurden für den Einsatz oberhalb der Kategorie 6 neue Anschluss-Systeme entwickelt:

- ✓ **ARJ45** (spezifiziert für Kategorie 7 - Kategorie 8.2) des Herstellers Bel Fuse Inc.
- ✓ **GG45** (spezifiziert für Kategorie 7 - Kategorie 8.2) des Herstellers Nexans
- ✓ **TERA** (spezifiziert für Kategorie 7 - Kategorie 8.2) des Herstellers Siemon
- ✓ **MMCpro** (noch nicht standardisiert für Kategorie bis 8.2) des Herstellers BKS

Die Anschlussssysteme ARJ45 und GG45 sind miteinander kompatibel. GG45 ist abwärtskompatibel zum RJ-45-Steckersystem. So können RJ-45-Patchkabel in GG45- und ARJ45-Buchsensystemen (Netzwerkdosen, Patchpanels) verwendet werden. Umgekehrt ist es aber nicht möglich, den GG45-Stecker in einer RJ-45-Buchse zu verwenden. Diesen Migrationsvorzug weist das TERA-System nicht auf. Sie können diesen Nachteil allerdings über Patchkabel (RJ45-TERA) ausgleichen.

2.2 Kabel mit nicht metallischen Leitern

Der Lichtwellenleiter gehört zu den leitergebundenen Übertragungsmedien mit nicht metallischem Leiter. Je nach verwendetem Material lassen sich Lichtwellenleiter (LWL) in Glasfaser oder Kunststofffaser unterteilen. Der mechanische Aufbau und die Ausbreitung der Signale sind bei beiden Faserarten identisch.

Glasfaser

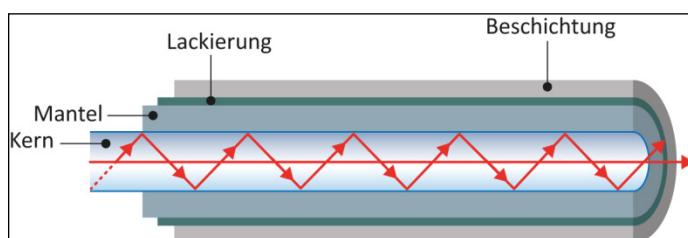
Bei einem Glasfaserkabel bestehen sowohl der Kern als auch der Mantel (engl. Cladding) aus hochreinem Quarzglas (SiO_2) mit unterschiedlichem Brechungsindex. Der Brechungsindex resultiert aus der Dotierung des Kerns (z. B. $\text{SiO}_2 + \text{GeO}_2$). Das Glasfaserkabel ist aufgrund seiner Eigenschaften besonders für die Übertragung von Signalen über längere Distanzen geeignet, z. B. für Gebäude- oder etagenübergreifende Bereiche. In der Datentechnik wird ausschließlich diese Art von Lichtwellenleiter (LWL) verwendet. Beachten Sie, dass im Allgemeinen bei einem LWL-Kabel immer von einem Glasfaserkabel die Rede ist.

Kunststoff-Faser (POF)

Eine weitere Variante des Lichtwellenleiters ist die sogenannte Polymer Optical Fiber (POF). Bei Kunststoff-Fasern wird zur Signalübertragung ein Licht leitendes PMMA (Polymethylmethacrylat) bei einer Wellenlänge von 650 nm verwendet. Kunststofffasern sind in der Investition günstiger, lassen sich einfacher verlegen und verbinden, haben aber den Nachteil, dass sie schlechtere Übertragungseigenschaften als Glasfaserkabel haben. Aufgrund ihrer höheren Dämpfungswerte (je nach POF-Typ 180 - 300 dB/km) und der direkt damit verbundenen kurzen Übertragungsstrecken (bis 70 m) sind diese Kabel nur eingeschränkt verwendbar. Ihr Einsatz erfolgt vorwiegend im Bereich der Automobilindustrie, der Medizin, im Multimediacbereich oder für Lichteffekte im Heimbereich.

Aufbau von Lichtwellenleitern

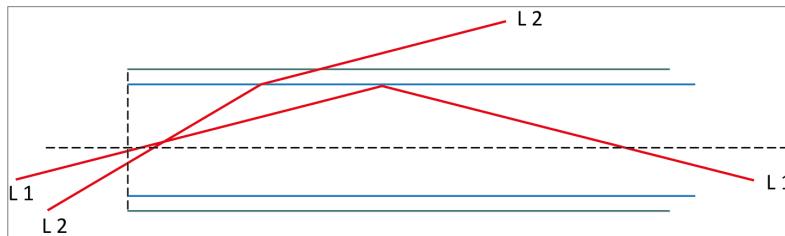
Der grundsätzliche Aufbau von Lichtwellenleitern besteht aus einem **Kern** (Core) und einem **Mantel**, dem sogenannten Cladding. Kern und Mantel dienen zur Führung des eingekoppelten Signals (Lichtimpuls). Die Beschichtung ist ein Schutz vor mechanischen Beschädigungen. Zwischen dem Cladding und dem Primary Coating befindet sich noch eine 2 bis 5 µm dicke Lackierung. Diese Lackierung dient dazu, Feuchtigkeit und somit eine Veränderung der Lichtbrechung am Mantel von der Faser fernzuhalten.



Glasfaser mit eingekoppeltem Lichtstrahl

Signalübertragung

In einem Lichtwellenleiter werden die Signale in Form von **Lichtimpulsen** übertragen. Eine Übertragung erfolgt vorwiegend nur in eine Richtung (unidirektional), weshalb für eine Übertragungsstrecke zwei Fasern notwendig sind. Es existieren auch Verfahren, die eine Übertragung in beide Richtungen (bidirektional) auf einer Faser ermöglichen. Die Ausbreitung der Signale (Lichtimpulse) im Lichtwellenleiter basiert auf dem Prinzip der Totalreflexion. Licht wird beim Übergang von einem optisch dünneren zu einem optisch dichteren Medium gebrochen. Dieser Effekt wird beim Übertragen von Lichtimpulsen auf Glasfasern genutzt.



Prinzip der Totalreflexion

Der eingekoppelte Lichtstrahl L2 wird unter einem zu großen Einfallswinkel (Akzeptanzwinkel) eingekoppelt. Er wird an der Grenzschicht von Kern zu Mantel nur gebrochen und verlässt die Faser. Für die Übertragung von Informationen ist so ein Lichtstrahl ungeeignet. Besser geeignet für die Signalübertragung ist hier der Lichtstrahl L1. Aufgrund seines günstigen Akzeptanzwinkels wird der Lichtstrahl L1 an der Grenzschicht total reflektiert und bleibt somit innerhalb des Lichtwellenleiters.



Allgemein gilt: Ein Lichtstrahl wird beim Übergang von einem optisch dünneren Medium (z. B. Luft) in ein optisch dichteres Medium (z. B. Quarzglas) zum Lot hin gebrochen. Beim Übergang von einem optisch dichteren Medium in ein optisch dünneres Medium wird der Lichtstrahl vom Lot weggebrochen.

Vorteile von Glasfaserkabeln

- ✓ Hohe Übertragungsraten
- ✓ Niedrige Signaldämpfung
- ✓ Kein Übersprechen auf benachbarte Fasern
- ✓ Keine Beeinflussung durch elektrische Störfelder von außen
- ✓ Keine Potentialverschleppung
- ✓ Großer Investitionsschutz
- ✓ Verlegung in explosionsgefährdeten Bereichen möglich
- ✓ Relative Abhörsicherheit
- ✓ Kompakte Bauform
- ✓ Kein Überspannungsschutz erforderlich

Nachteile von Glasfaserkabeln

- ✓ Aufwendiger zu verarbeiten
- ✓ Höhere Anschlusskosten im Vergleich zur Kupfertechnik
- ✓ Teure Gerätetechnik und aktive Komponenten
- ✓ Keine einheitliche Steckertechnologie
- ✓ Empfindlich gegen mechanische Belastungen
- ✓ Höhere Reparaturkosten

Dämpfung

Die Übertragungseigenschaften von Glasfaserkabeln sind sehr stark abhängig von der Dämpfung der eingekoppelten optischen Signale, der Wellenlänge und dem verwendeten Fasertyp. Die Dämpfung auf dem Glasfaserkabel sollte so niedrig wie möglich sein. Bei einer Übertragungsstrecke ist die Gesamtdämpfung eine Summe von Einzelursachen. Die wichtigsten Einzelursachen für Dämpfungsverluste bei optischen Signalen sind:

- ✓ Gesamtlänge einer Strecke
- ✓ Fehler in der Dotierung der Glasfaser
- ✓ Fehler beim Verlegen der Kabel
- ✓ schlechte Faserverbindungen (Spleiße)
- ✓ Anzahl der Spleiße auf einer Faser
- ✓ unterschiedliche Kernradien und Brechzahlprofile
- ✓ mechanische Fehler bei den Steckverbindungen
- ✓ ungenügend polierte Faseroberfläche an den Steckern
- ✓ Verunreinigung der Sende- / Empfangsoptik

Bandbreiten-Längen-Produkt

Das Bandbreiten-Längen-Produkt (Bandbreite in MHz, Länge in km) ist der entscheidende Parameter zur Bestimmung der übertragbaren Bandbreite und der Streckenlänge (bei Multimode-LWL). Das Bandbreiten-Längen-Produkt kann sowohl für metallische als auch für optische Übertragungsmedien angegeben werden. Die Angabe eines Bandbreiten-Längen-Produkts erfolgt aber vorwiegend im Zusammenhang mit einem Lichtwellenleiter.

Das Bandbreiten-Längen-Produkt ist von verschiedenen Faktoren wie Fasertyp und Wellenlänge abhängig.

Bei einem Bandbreiten-Längen-Produkt von 100 MHz x km kann die Faser 100 MHz pro Kilometer übertragen. Würde sich die Strecke auf 2000 m verdoppeln, wären nur noch 50 MHz möglich. Umgekehrt würden sich auf 500 m 200 MHz übertragen lassen.

Typische Bandbreiten-Längen-Produkte nach ISO/IEC11801 für Multimodefasern sind (gültig für OFL-Anregung mit LED):

- ✓ Optical Mode 1 (OM 1) 200/500MHz x km
- ✓ Optical Mode 2 (OM 2) 500MHz x km
- ✓ Optical Mode 3 (OM 3) 2GHz x km
- ✓ Optical Mode 4 (OM 4) 4,7GHz x km
- ✓ Optical Mode 5 (OM 5) 28GHz x km

Das Bandbreiten-Längen-Produkt wird in den Datenblättern der jeweiligen Hersteller angegeben. Beachten Sie aber bei der Auswahl der Angabe, welche Faserart bzw. welche Wellenlänge in Ihrem Unternehmen verwendet wird. Exemplarische Beispiele für die optischen Eigenschaften eines Multimode-Glasfaserkabels:

Fasertyp [µm]	50/125 µm OM 3	50/125 µm OM 4	9-10/125 µm OS2
Dämpfung [dB/km] bei 850 nm	2,5	2,5	–
Dämpfung [dB/km] bei 1300/1310 nm	0,7	0,7	0,36
Dämpfung [dB/km] bei 1550 nm	–	–	0,22
Bandbreiten-Längen-Produkt [MHz x km] (bei OFL-Anregung)	>1500	>3500	–
bei 850 nm	>900	>500	–
bei 1300 nm			

Dispersion

Dispersion nennt sich die Verbreiterung eines Lichtimpulses. Ursache für dieses Verhalten des Lichtimpulses ist der Laufzeitunterschied in einem Lichtwellenleiter. Die Laufzeitunterschiede sind von der Faserqualität, der eingesetzten optischen Sendequelle und der Streckenlänge abhängig. Es lassen sich folgende Dispersionsarten unterscheiden:

- ✓ Modendispersion
- ✓ Materialdispersion
- ✓ Profildispersion
- ✓ Wellenleiterdispersion
- ✓ Polarisationsmodendispersion (PMD)
- ✓ chromatische Dispersion (Material- u. Wellenleiterdispersion) bei Singlemode-LWL

Die Dispersion hat einen entscheidenden Einfluss auf die Übertragungsbandbreite und das damit verbundene Bandbreiten-Längen-Produkt.

Herstellung

Glasfasern werden in mehreren Schritten hergestellt. Dadurch können die mechanischen, geometrischen und optischen Eigenschaften des Lichtwellenleiters gezielt beeinflusst werden. Bei der Herstellung wird mit einer Vorform, die aus einem Kern und einem Mantelglas besteht, gearbeitet. Diese Vorform stellt eine Vergrößerung der zu fertigenden Faser dar.

Einteilung der Faserarten

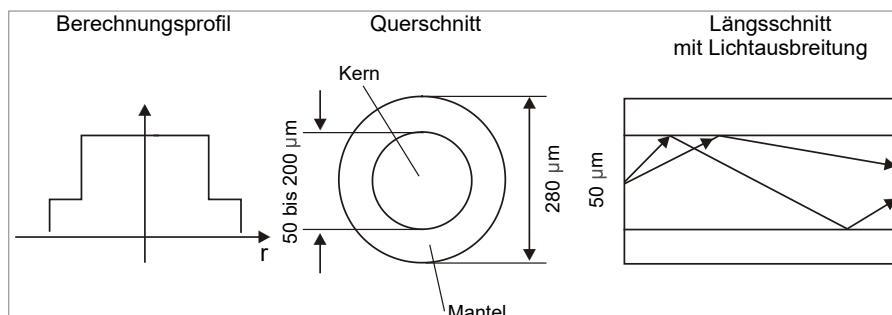
Für den Einsatz von Glasfasern in der Übertragungstechnik gibt es drei Typen von Faserprofilen, wobei nur die letzten beiden einen signifikanten Einsatz finden:

- ✓ Multimodafasern mit Stufenindex
- ✓ Multimodafasern mit Gradientenindex (OM 1 – OM 5)
- ✓ Monomodafasern (OS1 - OS2)

Multimodafasern (MM)

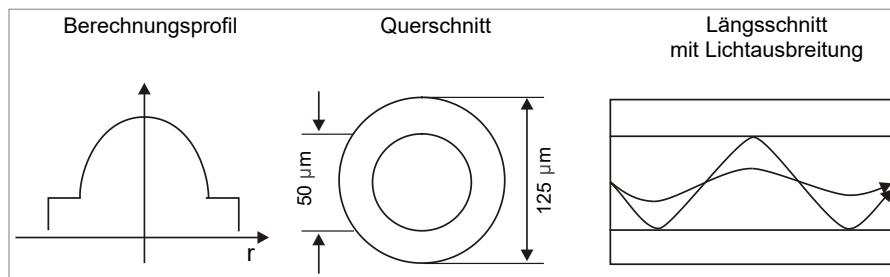
Multimodafasern können je nach Typ einen Kerndurchmesser von 50 – 400 µm und einen Manteldurchmesser von 125 – 500 µm aufweisen.

Stufenindexfasern besitzen je nach Einsatzspektrum einen Kern zwischen 125 – 500 µm Durchmesser. Der Brechungsindex ist im Kern konstant und reduziert sich stufenförmig in Richtung Mantel. Aufgrund des Stufenprofils werden die Lichtwellen an der Mantelgrenzfläche vollständig reflektiert. Wegen ihrer mechanischen Stabilität werden sie für kurze Distanzen u. a. im Steuerungs- und Multimediacbereich eingesetzt.



Brechungsprofil, Lichtausbreitung einer Multimodafaser mit Stufenindex

Die Gradientenindexfasern besitzen einen kleinen Kern ($50 \mu\text{m}$ oder $62,5 \mu\text{m}$) und haben einen Manteldurchmesser von $125 \mu\text{m}$. In Europa wird vorrangig der Typ $50/125 \mu\text{m}$ eingesetzt. Der Brechungsindex ist parabolisch vom Kern zum Mantel abfallend. Die Lichtwellen werden innerhalb ihrer Ausbreitungsrichtung gekrümmmt. Typische Einsatzgebiete sind der Telekommunikations- und Datenbereich.

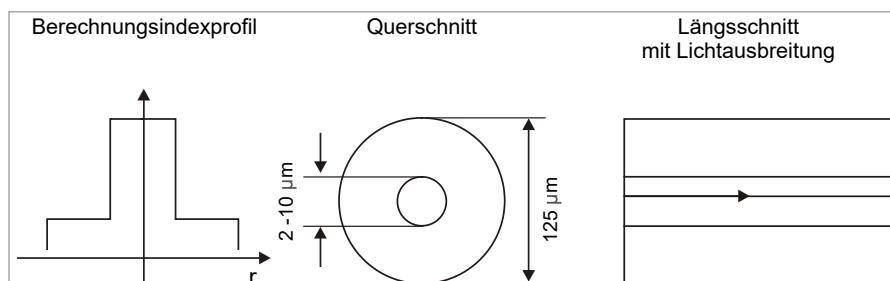


Brechungsprofil, Lichtausbreitung einer Multimodefaser mit Gradientenindex

Monomodefasern (SM)

Monomodefasern, auch Singlemodefasern genannt, haben einen Manteldurchmesser von $125 \mu\text{m}$. Der Kerndurchmesser von Standard-Singlemode-LWL beträgt $8,3 \mu\text{m}$. Sein Modenfelddurchmesser liegt beim Standard-Singlemode-LWL bei $9,2 \mu\text{m}$ (1310 nm) bzw. $10,4 \mu\text{m}$ (1550 nm). Durch diesen kleinen Kerndurchmesser wird prinzipiell nur ein Grundmode der auszubreitenden Wellenlänge zugelassen.

Mit Monomodefasern sind Bandbreiten-Längen-Produkte (in Abhängigkeit von der Dispersionstoleranz des Senders) von über $10 \text{ GHz} \times \text{km}$ möglich. Dafür sind die Kosten durch die verwendeten Lasermodule und das Medium höher. Diese Art von Kabeln wird hauptsächlich in Weitverkehrsnetzen und im Primärbereich bei der strukturierten Verkabelung eingesetzt.



Brechungsprofil, Lichtausbreitung einer Singlemodefaser mit Stufenindex

Faserspezifizierung im 10-Gigabit-Ethernet-Standard

10-Gigabit-Ethernet wird bei heutigen Anwendungen als Standard für die Übertragung von Daten in lokalen Netzwerken verwendet. Dabei spielt es keine Rolle, ob die Daten über Kupfer- oder Glasfaserleitungen übertragen werden. Lediglich die Entfernung zwischen den Endpunkten gilt als Kriterium für die Wahl des Übertragungsmediums. Bei Entfernungen größer als die für Twisted-Pair-Kabel spezifizierten einhundert Meter ist der Einsatz von Glasfaserleitungen unumgänglich.

Aufgrund der stetig wachsenden Menge an Informationen und Daten in einem Netzwerk und der Zunahme von multimedialen Inhalten, steigt auch der Bedarf an größerer Bandbreite. Mit dem 10-Gigabit-Ethernet-Standard IEEE 802.3ae wurde in der Vergangenheit eine neue Hochgeschwindigkeitstechnologie nicht nur in lokalen Netzwerken etabliert.

Gradientenindex-Profilfaser (GIF)

Um Daten in einem Netzwerk mit 10-Gigabit-Ethernet übertragen zu können, werden optimierte aktive und passive Komponenten verwendet. Das Problem bei den ersten Multimodefasern (MMF) war, dass die geforderte Segmentlänge von mindestens 300 Metern aufgrund der optischen Verluste nicht realisierbar ist. Bei ersten Tests mit Standardfasern mit einem 62,5-µm-Kern konnte man lediglich eine Linklänge von nur etwa 30 Metern realisieren. Bei einer Faser mit 50-µm-Kern wurde immerhin eine Linklänge von etwa 85 Metern erzielt.

Um die Anforderungen für den 10-Gigabit-Ethernet-Standard für Multimodeleitungen zu erfüllen und diese großflächig einzusetzen, war eine verbesserte Variante der Gradientenindex-Profilfaser erforderlich. Bei der Verbesserung handelt es sich um eine Multimodefaser, deren Brechzahlverlauf parabolisch zum Kern hin zunimmt. Der resultierende Weg der Modes ist in dieser Faser nicht geradlinig, sondern verläuft leicht wellenförmig.

Die Grundvoraussetzung für die Verwendung von Gradientenindex-Profilfasern für den 10-Gigabit-Ethernet-Standard sind zwei Optimierungen:

- ✓ Optimierung in Bezug auf Differential Mode Delay (DMD)
- ✓ Optimierung bei Verwendung von Lichtquellen bei einer Wellenlänge von 850 nm

Differential Mode Delay (DMD)

Gerade bei großen Übertragungsstrecken und hohen Bandbreiten kommt es aufgrund von Dispersion zu einer starken Veränderung der Ausgangssignale beim Empfänger. Damit diese Verluste durch unterschiedliche Laufzeiten reduziert werden, wurde die Gradientenindex-Profilfaser entwickelt. Der Parameter Differential Mode Delay ist ein Nebeneffekt, der aus der Herstellung der Multimodefaserkerne resultiert. Er entsteht gerade dann, wenn man bei einer Multimodefaser als Sendequelle einen Laser verwendet. Wird das Lasersignal in den Kern eingespeist, entstehen durch Teilanregungen des Lasers zwei oder mehr Modes, welche dann aufgrund des Profilverlaufes auf unterschiedlichen Wegen in der Faser übertragen werden. Die daraus resultierenden Laufzeitunterschiede sorgen für eine Signalverzerrung (Jitter).

Bei Sendequellen mit einer LED stellt der Differential Mode Delay kein Problem dar, da hier alle Modes verwendet werden und somit auch gleichzeitig am Empfänger eintreffen. Beim 10-Gigabit-Ethernet-Standard werden jedoch sogenannte VCSEL-Laser als Sender verwendet anstelle von LED-Lichtquellen wie beim 1-Gigabit-Standard.

Vertical-Cavity-Surface-Emitting-Laser (VCSEL)

VCSEL sind kleine Halbleiterlaser, die gerade für den Bereich hoher Übertragungsraten auf optischen Medien entwickelt wurden. Sie nutzen dabei die optischen Fenster bei 850 nm, 1300 nm und bei 1550 nm. Für den 10-Gigabit-Ethernet-Standard sind derzeit jedoch nur Laserdioden von Interesse, welche im Bereich von 850 nm (bevorzugt, da hier geringere Kosten) und 1310 nm arbeiten. Ihr großer Vorteil ist die kreisförmige Abstrahlcharakteristik und der hohe Einkopplungsgrad bereits bei kleinen Faserkernen. Bei Multimodefasern mit einem Kern von 50 µm wird mit diesen Laserdioden eine sehr hohe Einkopplung in die Faser erzielt. Der wesentliche Unterschied bei der Verwendung von VCSEL, die bei einem optischen Fenster von 850 nm arbeiten, im Vergleich zu VCSEL, die bei 1310 nm arbeiten, ist die maximale Länge der Übertragungsstrecke. Diese beruht auf dem Dispersionsminimum der Faser und der Wellenlänge. Können mit 850-nm-VCSEL maximal bis zu 500 Meter überbrückt werden, so liegt die Übertragungsdistanz bei einem optischen Fenster von 1310 nm bereits bei 10 km.

Faserklassen

Um nun entsprechende Lichtwellenleiter für den 10-Gigabit-Standard und darüber einsetzen zu können, wird ähnlich der Klassenspezifikation bei den Kupferkabeln die Qualität der Lichtwellenleiter klassifiziert. Diese ist beginnend mit der EN50173-1 normiert worden. Dabei werden die Gradientenindex-Profilfasern in fünf OM-Klassen (**optical multimode**) und die Monomodefasern in zwei OS-Klassen (**optical singlemode**) eingeteilt. Innerhalb der Klassen wird zwischen einer Einspeisung mit LED, VCSEL oder Laser als Lichtquelle unterschieden.

Die Klassen bei Gradientenindex-Multimodefasern lauten:

- ✓ OM 1; Kern-/Manteldurchmesser (50 oder 62,5)/125 µm (Multimode);
- ✓ OM 2; Kern-/Manteldurchmesser (50 oder 62,5)/125 µm (Multimode); (Fasertyp F, G, H)
- ✓ OM 3; Kern-/Manteldurchmesser 50/125 µm (Multimode); (Fasertyp I)
- ✓ OM 4; Kern-/Manteldurchmesser 50/125 µm (Multimode); (Fasertyp J)
- ✓ OM 5; Kern-/Manteldurchmesser 50/125 µm (Multimode)

Die Klassen bei Singlemodefasern lauten:

- ✓ OS 1 Kern-/Manteldurchmesser 9/125 µm (Monomode) (Fasertyp L, M)
- ✓ OS 2 Kern-/Manteldurchmesser 9/125 µm (Monomode)

Datenübertragungsrate, maximale Distanz und Sender

Anwendung	DÜ-Rate Gbit/s	Wellenlänge (nm)	Distanz (OM 1 – OM 4)	Distanz (OS 1 – OS 2)	Sendequelle
10Base-F	0,01	850	2 km (1-4)		LED
100Base-FX	0,1	1300	2 km (1-4)		LED
1000Base-SX	1	850	275 m (1) - 1,1 km (4)		VCSEL
1000Base-LX	1	1310	550 m (1-4)	2 km (1), 5 km (2)	Laser
10GBase-SR	10	850	35 m (1) - 550 m (4)		VCSEL
10GBase-LR	10	1310		2 km (1), 10 km (2)	Laser
10GBase-SR4	10	850	100 m (3-4)		VCSEL (2+2 Fasern)
40GBase-LR4	40	1310		2 km (1), 10 km (2)	VCSEL (4+4 Fasern)
100GBase-SR-10	100	850			VSEL (10+10 Fasern)
100GBase-LR4	100	1310		2 km (1), 10 km (2)	Laser (4+4 Fasern)
100GBase-ER4	100	1310		40 km (2)	Laser (4+4 Fasern)
200GBase-DR4	200	1304-1308	Draft Stand: 10/2016	500 m (2)	Laser (4 Fasern)
200GBase-FR4	200	1271-1311	Draft Stand: 10/2016	2 km (2)	Laser (4 Fasern)
200GBase-LR4	200	1295-1309	Draft Stand: 10/2016	10 km (2)	Laser (4 Fasern)
400GBase-SR16	400	840-860	100 m (4)	Draft 10/2016	Laser (16 Fasern)
400GBase-DR4	400	1304-1318	Draft Stand: 10/2016	500 m (1-2)	Laser (4 Fasern)
400GBase-FR8	400		Draft Stand: 10/2016	2 km (1-2)	Laser (8 Fasern)
400GBase-LR8	400		Draft Stand: 10/2016	10 km (1-2)	Laser (8 Fasern)

Weiterführende Informationen zu OM 5 finden Sie hier:

- ✓ <https://www.telegaertner.com/de/infostream/die-neue-faserkategorie-om5>
- ✓ <https://www.opternus.de/wissen/om-klassifizierung-der-multimodefasern>

Patchkabel, Pigtails und Leitungen

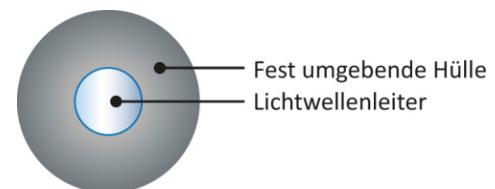
Zubehörartikel wie Patchkabel, Pigtails (vorkonfektionierter LWL-Anschluss) und Glasfaserleitungen mit Multimode-Gradientenindex der LWL-Kategorie OM 4 unterscheiden sich in ihrem äußerlichen Aufbau nicht von anderen OM-Komponenten. Wird der Einsatz von mehr als 10-Gigabit-Ethernet gefordert, sind jedoch unbedingt alle Komponenten der LWL-Kategorie OM 4 oder OM 5 zu verwenden.

Dies muss beim jeweiligen Lieferanten oder beim ausführenden Unternehmen explizit angegeben werden. Eine Mischung von OM4- und OM5-Fasern sollte aufgrund der unterschiedlichen optischen Eigenschaften der Fasern vermieden werden. Die verwendeten Pigtails müssen derselben Faserklasse entsprechen.

Faseraufbau

Festader

Festadern bestehen aus einer einzelnen Faser, welche von einer festen Hülle umgeben ist. Aufgrund ihrer Beschaffenheit sind sie flexibler als beispielsweise Hohladern. Durch den geringen Abstand zwischen der eigentlichen Faser und der umgebenden Hülle sind Festadern sehr empfindlich gegenüber mechanischen Belastungen.

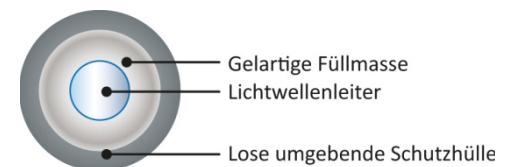


Querschnitt einer Festader

Hohlader

Die Hohlader gibt es als gefüllte und ungefüllte Variante. Eine gefüllte Hohlader besteht aus der Faser und einer sie lose umgebenden Schutzhülle. Der Zwischenraum zwischen Faser und Hülle ist mit einem wasserabweisenden Gel gefüllt. Diese Faser ist zwar von den Abmessungen etwas größer, sie besitzt dafür bessere Eigenschaften in Bezug auf mechanische Festigkeit. Bei der ungefüllten Hohlader ist der Zwischenraum zwischen Faser und Hülle ohne Füllmaterial, sie besitzt jedoch bessere Eigenschaften bei Temperaturschwankungen.

Die gefüllte Hohlader wird aufgrund ihrer guten mechanischen Eigenschaften am häufigsten eingesetzt.



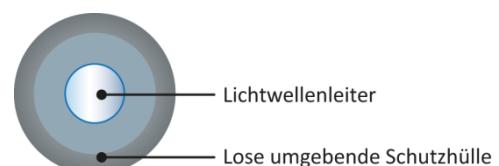
Querschnitt einer gefüllten ...



... und ungefüllten Hohlader

Kompaktader

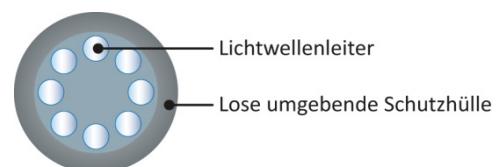
Die Kompaktader ist vom Aufbau her eine modifizierte Form der Festader. Der einzige Unterschied zur Festader ist ein geringer Abstand zwischen der Faser und dem Schutzmantel. Diese Art von Faser ist vom Aufbau vergleichsweise kompakter als eine Hohlader und hat dementsprechend verbesserte mechanische Eigenschaften gegenüber einer Festader.



Querschnitt einer Kompaktader

Bündelader

Bei der gefüllten Bündelader werden mehrere Einzelfasern durch eine gemeinsame Schutzhülle umgeben. Der Zwischenraum zwischen den Fasern und der Schutzhülle ist, wie bei der gefüllten Hohlader, mit einem wasserabweisenden Gel gefüllt. Die Faseranzahl in einer Bündelader besteht in der Regel aus zwei bis zwölf Fasern.



Querschnitt einer Bündelader

Spezifikation von Glasfaserkabeln

Für den Einsatz von Glasfaserkabeln sollten unbedingt die örtlichen Gegebenheiten geprüft werden, da es Glasfaserkabel sowohl für den Innenbereich als auch zur Verlegung im Außenbereich bzw. im Erdreich gibt. Mögliche Entscheidungskriterien sind:

- ✓ Verlegung im Erdbereich oder Außenbereich
- ✓ Einzug in Rohre und Verlegung auf Pritschen
- ✓ Verlegung in feuchten und nassen Umgebungen
- ✓ Verlegung in mechanisch ungeschützten Bereichen
- ✓ Verlegung in trockener Umgebung und In-House-Bereichen
- ✓ frei hängende Verlegung

Je nachdem, welches Umfeld sich in Ihrem Unternehmen befindet, sollten Sie gewissenhaft das eingesetzte Glasfaserkabel prüfen. In der Norm DIN VDE 0888 finden Sie eine Erklärung zum jeweiligen Kabeltyp.

Simplexkabel nach DIN VDE 0888

Position	Kabelschlüssel
1	J = Innenkabel
2	V = Vollader / H = Hohlader, ungefüllt / W = Hohlader gefüllt
3	Y = PVC-Mantel / H = Mantel aus halogenfreiem Material
4	Anzahl der Fasern
5	G = Gradientenfaser / E = Einmodenfaser
6	Kerndurchmesser in µm
7	Manteldurchmesser in µm
8	Dämpfungskoeffizient in [dB/km]
9	Wellenlänge B = 850 nm / F = 1300 nm / H = 1550 nm
10	Bandbreite [MHz x km]

Beispiel: J-VH 2G50/125

Breakoutkabel nach DIN VDE 0888

Position	Kabelschlüssel
1	AT = Außenkabel aufteilbar
2	V = Vollader / W = Hohlader, gefüllt / D = gefüllte Bündelader
3	(ZN) = nicht metallene Zugentlastungselemente
4	Mantel des Grundelements: Y = PVC-Mantel / H = Mantel aus halogenfreiem Material
5	Y = PVC-Mantel / H = Mantel aus halogenfreiem Material
6	Anzahl der Grundelemente (Fasern)
7	G = Gradientenfaser / E = Einmodenfaser
8	Kerndurchmesser in µm
9	Manteldurchmesser in µm

Position	Kabelschlüssel
10	Dämpfungskoeffizient in [dB/km]
11	Wellenlänge B = 850 nm / F = 1300 nm / H = 1550 nm
12	Bandbreite [MHz x km]
13	LG = Lagenverseilung

Beispiel: AT-V(ZN)Y 8G62,5/125

Außenkabel nach DIN VDE 0888

Position	Kabelschlüssel
1	A = Außenkabel
2	B= Bündelader, ungefüllt / D= Bündelader, gefüllt / W= Hohlader, gefüllt / H= Hohlader, ungefüllt
3	S = metallenes Element in der Kabelseele
4	F = Füllmasse zur Füllung der Verseilhohlräume in der Kabelseele
5	2Y = PE-Mantel / (L)2Y= Schichtenmantel / (ZN)2Y = PE-Mantel mit nicht metallischer Zugentlastung
6	B2Y = Bewehrung mit PE-Schutzhülle / BY = Bewehrung mit PVC-Schutzhülle
7	Anzahl der Grundelemente (Fasern)
8	G = Gradientenfaser / E = Einmodenfaser
9	Kerndurchmesser in µm
10	Manteldurchmesser in µm
11	Dämpfungskoeffizient in [dB/km]
12	Wellenlänge B = 850 nm / F = 1300 nm / H = 1550 nm
13	Bandbreite [MHz x km]
14	LG = Lagenverseilung

Beispiel: A-DQ(ZN)B2Y 24G50/125

Stecker-/Kabelfarben nach DIN EN 50173

Fasertyp	Stecker	Patchkabel	Verlegekabel
OM 1	beige	orange	orange
OM 2	beige	orange	orange
OM 3	aqua	aqua	orange
OM 4	schwarz	erikaviolett	erikaviolett
OS 1	blau	gelb	gelb
OS 2 PC*	blau	gelb	gelb
OS 2 APC*	grün	gelb	gelb

*PC, Steckerende konvex geschliffen; (PC = physical contact)

*APC, Steckerende konvex und schräg geschliffen; (APC = angled physical contact)

Anwendungsbereiche von Glasfaserkabeln

Aufgrund ihrer guten Übertragungseigenschaften werden Glasfaserkabel zum Austausch von hohen Datenmengen im Netzwerkbereich verwendet. Sie dienen als High-End-Backbone für Serverfarmen oder zur Anbindung von Firmengebäuden. Aufgrund der gesunkenen Allgemeinkosten wird Glasfaser heutzutage in speziellen Bereichen auch bis an den Arbeitsplatz verlegt (Fiber-to-the-Desk).

Einsatz von Multimodefasern

Stufenindexfasern sind wegen ihrer großen Signallaufzeitunterschiede und starken Impulsverbreiterung für kurze Distanzen (bis ca. 1 km) und einen niedrigen Frequenzbereich (bis 100 MHz) für einen praktischen Einsatz in Datennetzen nicht geeignet. Gradientenindexfasern hingegen sind für mittlere Strecken und einen hohen Frequenzbereich für bis zu 4,7 GHz u. a. für gebäudeinterne Verbindungen, Data-Center-Verkabelung, SAN-Systeme und Fiber-to-the-Home-Lösungen vorgesehen.

Einsatz von Monomodefasern

Monomodefasern sind für gebäudeübergreifende und Weitverkehrsstrecken (bis zu ca. 100 km) vorgeschrieben. Sie weisen ein Bandbreiten-Längenprodukt von mehr als 10 GHz x km auf. Experimentell ist eine Übertragung mit einer Distanz von 580 km (ohne Nutzung von aktiven Repeatern) bewiesen worden.

Lichtwellenleiterkabel für den industriellen Einsatz

Bei der Verwendung von Lichtwellenleiterkabeln für den Einsatz im industriellen und medizinischen Bereich sind zusätzliche Kriterien zu beachten. Diese Faktoren sind:

- ✓ Erweiterter Temperaturbereich
- ✓ Feuchtigkeit und Gase
- ✓ Staub und andere chemische Substanzen
- ✓ Vibrationen

Um diesen erhöhten Anforderungen gerecht zu werden, wurden die bereits bekannten Kabeltypen aus dem LAN-Umfeld um zwei zusätzliche Varianten erweitert.

- ✓ Plastic (bzw. Polymer) Optical Fiber (POF)
- ✓ Polymer Cladded Fiber (PCF)

Durch ihre besonderen Eigenschaften und bessere Robustheit gegenüber mechanischen Beanspruchungen sind diese Kabeltypen besonders gut geeignet für den Einsatz im industriellen und medizinischen Umfeld. Ein weiterer Vorteil liegt in der besseren Konfektion vor Ort. Gegenüber Glasfasertypen haben diese Kabel jedoch wesentlich höhere Dämpfungseigenschaften (Übertragungslänge max. 300 m), und sie können nicht bei hohen Temperaturen (über 80°C) zum Einsatz kommen.

Bezeichnung	10 MBit/s	100 MBit/s	Einsatzgebiet
POF	50 Meter	35 Meter	Kraftfahrzeuge, Unterhaltungselektronik, Automationstechnik, Rechnerplatten
PCF	bis zu 300 Meter		Sensorik, Medizintechnik, industrielle Datentechnik

Plastic (Polymer) Optical Fiber

Die POF-Faser ist eine reine Plastikfaser und besteht aus einem transparenten Kern aus Polymethylmethacrylat (PMMA) oder Polycarbonat (PC). Dieser Kern hat einen Durchmesser von 980 µm. Der Mantel einer POF-Faser besteht aus Polyethylen (PE) oder auch aus Polyamid (PA).

Polymer Cladded Fiber

Bei der PCF-Faser besteht der Kern aus Quarzglas (SiO_2) und hat einen Durchmesser von 50 μm bis zu 1000 μm . Der Mantel einer PCS-Faser besteht aus einem speziellen Kunststoff. Typische Abmessungen für eine Standard-Faser mit kleinem Kerndurchmesser sind 125 μm (Kern), 140 μm (Cladding) und 250 μm (Schutzmantel).

Verbindungstechnik bei Glasfaserkabelverkabelung

Ziel bei der optischen Übertragungstechnik ist es, Glasfaserkabel dauerhaft oder lösbar miteinander zu verbinden. Ist eine Verbindung dauerhaft, wird sie als optischer Spleiß bezeichnet. Wenn die Verbindung im Gegensatz dazu lösbar ist, dann wird von einer optischen Steckverbindung gesprochen. Im praktischen Einsatz werden eine einfache Handhabung sowie eine geringe und reproduzierbare Dämpfung der Verbindung gefordert. Aufgrund der Empfindlichkeit gegenüber Verschmutzungen ist die Sauberkeit lösbarer Verbindungen sehr wichtig. Die Verbindungselemente und die Faseroberfläche sollten regelmäßig sorgfältig gereinigt werden.

Vorbereitung

Zur Herstellung einer Faserverbindung sind hohe Sorgfalt und Sauberkeit gefordert. Der größte Zeitaufwand bei der Erstellung einer Faserverbindung ist für die Vorbereitung der eigentlichen Faserverbindung notwendig. Die Vorbereitung ist bei Spleiß- und Steckerverbindungen nahezu identisch. Da die Glasfaser nicht frei zugänglich ist, muss diese erst freigelegt werden. In Abhängigkeit vom Aufbau der Glasfaser müssen die äußeren Schichten entfernt werden. Ist die Glasfaser freigelegt, muss durch Anritzen und Brechen eine ebene Faserendfläche hergestellt werden. Diese ebene Endfläche ist ein Maß für die Qualität der anschließenden Verbindung. Bei Ausbrüchen, Nasen, Unebenheiten oder schlechten Schnittwinkeln sind schlechte Verbindungen vorprogrammiert.

Optische Spleiße

Nicht lösbare Verbindungen bei Glasfaserkabeln werden zur Verbindung von einzelnen Faseradern miteinander oder bei der Verbindung mit vorkonfektionierten Anschlusskabeln (Pigtails) verwendet. Es werden folgende Arten von optischen Spleißen unterschieden:

- ✓ Thermischer Spleiß
- ✓ Klebespleiß
- ✓ Mechanischer Spleiß

Spleiße sind Langzeitverbindungen und müssen eine geringe Dämpfung sowie eine stabile Verbindung besitzen.

Thermischer Spleiß

Beim thermischen Spleiß werden die Glasfaserenden mit einem Lichtbogenspleißgerät miteinander verschweißt. Durch einen Schrittmotor werden die Stirnflächen der Faserenden beim Erhitzen vorsichtig aneinander gefahren. Die beim Schmelzprozess auftretende Oberflächenspannung bewirkt einen Selbstzentrierungseffekt der Fasern, welches bei der Mantelzentrierung erforderlich ist. Aufgrund der hohen Temperaturen verschmelzen beide Faserenden zu einer Verbindung, welche nach dem Spleißvorgang noch durch einen mechanischen Zugtest geprüft wird. Nach einem erfolgreichen Verbinden der Faserenden ist es erforderlich, den Spleiß mit einem Schutz (Crimp-Spleißschutz) vor mechanischen Belastungen zu schützen.

Klebespleiß

Beim Klebespleiß wird die Faser über einer Nut, einem Röhrchen oder einer Hülse justiert und anschließend geklebt. Der Klebstoff sorgt neben einer mechanischen Festigkeit auch für eine Anpassung der Brechzahl. Typische Dämpfungswerte für Klebespleiße liegen bei 0,1 bis 0,2 dB.

Mechanischer Spleiß

Bei einem mechanischen Spleiß sorgt eine entsprechende Halterung für eine feste und langfristige Stabilität der Verbindung. Die Faserenden werden in ein V-Nut-förmiges Grundteil geführt und anschließend über Klemmstücke befestigt. Bei dieser Art von Spleiß können bei unsachgemäßer Ausführung hohe Verluste auftreten. Typische Dämpfungswerte liegen hier bei 0,2 bis 0,5 dB. Für die Verarbeitung von Monomodefasern gelten ähnliche Voraussetzungen wie für Multimodefasern, jedoch sind bei Monomodefasern die Anforderungen an die erforderlichen Gerätschaften weitaus höher.

Optische Steckverbindungen

Für den Anschluss an Glasfaserkabel werden unterschiedliche Steckverbinder eingesetzt. Einige Steckerbauformen sind der E-2000-, SC-, DIN-, LC- und der ST-Stecker. Diese werden sehr häufig in Verkabelungsstrukturen verwendet. Die Richtlinien für den Einsatz von Steckverbindern sind in der Norm EN50173 hinterlegt.

Bezeichnung	Verschluss	Verbindung	Einsatzgebiet	Fasertyp
SC	push/pull	gefedert	LAN, WAN, CATTV Messtechnik	Multi- und Monomodefaser
ST	Bajonett mit Verdrehschutz	gefedert	LAN/WAN	Multi- und Monomodefaser, POF
LC	push/pull	gefedert	LAN, WAN, Messtechnik	Multi- und Monomodefaser
E2000	push/pull	gefedert	LAN, WAN, Messtechnik	vorwiegend Monomodefaser
F3000	push/pull	gefedert	CATTV, LAN, Sensorik, Mess- u. Medizintechnik	Multi- und Monomodefaser
DIN (LSA)	Gewindemutter	geschraubt	LAN/WAN, Telecom	Multi- und Monomode
MIC	push/pull	push/pull	LAN, WAN	Multi- und Monomodefaser
MU (Mini-SC)	push/pull	gefedert	LAN	Multi- und Monomode
MTRJ	push/pull	verriegelt	LAN	Multi- und Monomode
BLINK	push/pull	verriegelt	Fiber to the Home (FTTH)	Monomode PC/APC

LC-, FC- und SC-Stecker sind aufgrund ihrer einfachen Handhabung und der reduzierten Bauform heutzutage bevorzugte Steckverbindungen.

In bestehenden Installationen finden Sie auch noch ST- und E2000-Steckverbindungen vor.

Gerade bei Patch- und Anschlusskabeln ist ein schnelles Lösen und Verbinden mit dem Port oder der Anschlussdose von Vorteil.

Der MIC-Stecker (Media Interface Connector) wurde oft bei ATM eingesetzt. Sein Einsatzgebiet ist aber eher punktuell und rückläufig.



Optische SC-Steckverbinder

2.3 Kabellose Systeme

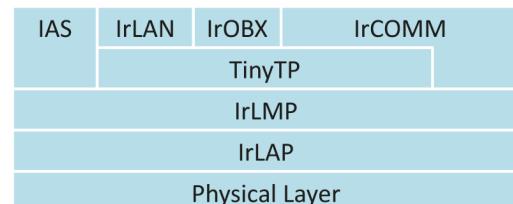
Infrarotübertragung (IrDA)

Die **Infrarotübertragung** wird zur drahtlosen Kommunikation u. a. von Notebooks, Smartphones oder Handhelds genutzt. Der IrDA-Standard entstand im Jahr 1993. Die aus über 30 Unternehmen bestehende Infrared Data Association entwarf die Standard-IR-Schnittstelle (SIR) mit der für serielle Schnittstellen üblichen Datenübertragungsrate von 115,2 kbit/s.

Mit der Ausstattung von Handys mit Infrarotschnittstellen gelang der Durchbruch für IrDA. Der IrDA-Port ermöglichte so den Austausch von Daten wie SMS, Klingeltönen und Logos zwischen den Handys. Der IrDA-Standard wurde längere Zeit nur in geringem Maße im Handy-Segment umgesetzt. Aktuell fungiert er bei Smartphones als IR-Sensorersatz für diverse Fernbedienungen. IrDA wurde danach zum FIR-Standard (Fast IR) weiterentwickelt. Er unterstützt eine Übertragungsrate von bis zu 4 Mbit/s. Die weiteren Entwicklungen waren der UFIR-Standard (Ultra Fast IR: bis zu 96Mbit/s) und der Giga-IR-Standard (Giga Infrared; bis zu 512 Mbit/s und 1 Gbit/s). Diese Standards konnten sich jedoch nicht umfassend im Netzwerkbereich durchsetzen.

Die Hardware einer **IrDA-Schnittstelle** ist wie folgt aufgebaut: Als Sender arbeitet eine Infrarotdiode mit einer Wellenlänge zwischen 850 und 900 nm. Die entsprechende Empfangsdiode ermöglicht eine theoretische Reichweite von etwa einem Meter. Als problematisch erweist sich die Tatsache, dass die Übertragung empfindlich auf äußere Einflüsse wie Umgebungslicht und reflektierende Gegenstände reagiert. Unter direkter Sonnenlichteinstrahlung beträgt die Reichweite oft nur noch 10 cm, mit Kunstlicht erreicht man bis zu einem Meter.

IrDA besitzt einen sehr umfangreichen Protokollaufbau. Das Protokoll IrLAP (Infrared Link Access Protocol) ermöglicht den Verbindungsaufbau zwischen Geräten. Wenn mehr als ein Gerät vorhanden ist, werden die Verbindungen durch das Multiplexverfahren IrLMP (Infrared Link Management Protocol) hergestellt.



IrDA-Protokollaufbau

Der Verbindungsaufbau läuft folgendermaßen ab: Die IrDA-Geräte senden alle zwei Sekunden einen Infrarotimpuls aus, um ihre Empfangsbereitschaft zu signalisieren. Das erste IrDA-Gerät, das den Impuls erhält, versucht nun, eine Verbindung aufzubauen. Nach dem Verbindungsaufbau übermitteln die Geräte mit dem IAS ihre Eigenschaften wie Gerätename, -klasse und -fähigkeit. So erkennt ein Notebook, ob das ihm gegenüberstehende Gerät auch ein Notebook ist, mit dem es Dateien austauschen kann. Für den eigentlichen Datenaustausch ist das TinyTP (Tiny Transport Protocol) verantwortlich. Es enthält eine eigene Fehlererkennung und -korrektur.

Über diesem Protokoll liegen die drei High-Level-Protokolle auf: IrLAN ermöglicht den Zugang zu lokalen Netzwerken. IrOBEX (Infrared Object Exchange Protocol) ist verantwortlich für den Austausch von Dateien, aber auch von Visitenkarten oder Kurznachrichten. Dieses Protokoll ist für Handys sehr wichtig. Das IrCOMM-Protokoll ist in der Lage, auf der Infrarotschnittstelle serielle oder parallele Schnittstellen nachzubilden. Dies ist für den mobilen Internetzugang ausschlaggebend: Das Handy simuliert ein Modem, das sich in ein Netz einwählt und Daten überträgt. Das steuernde Notebook erkennt lediglich ein Standardmodem an einem virtuellen, seriellen Anschluss. Ebenso ist über IrCOMM das kabellose Drucken mit entsprechend ausgerüsteten Druckern vom Notebook aus möglich.

DECT-Standard

DECT (Digital Enhanced Cordless Telecommunications) ist ein europäischer Standard für schnurlose Telefone und wurde vom ETSI, dem European Telecommunications Standards Institute, 2003 offiziell verabschiedet und 2005 modifiziert. Die allgemeine Zulassung des Frequenzbandes wird in Deutschland durch die Bundesnetzagentur bis Ende 2025 gewährleistet. DECT beschreibt nur die Schnittstelle zwischen dem Mobilteil und der Basisstation (engl. Gateway) und besitzt folgende Eigenschaften:

- ✓ Sprachübertragung in Form von elektromagnetischen Wellen
- ✓ flexible Zuteilung der Datenraten
- ✓ hohe Sprachqualität
- ✓ relativ gute Abhörsicherheit durch Verschlüsselung
- ✓ Identifikation des Teilnehmers
- ✓ dynamische Kanalbelegung
- ✓ mehrere Mobilteile an einer Basisstation

Damit DECT-Geräte verschiedener Hersteller miteinander kommunizieren können, wurde der GAP-Standard entwickelt. GAP steht für Generic Access Profile. DECT-Geräte, die nach diesem Standard funktionieren, können sich auch an Basisstationen anderer Hersteller anmelden.

Um untereinander kompatible DECT-Datenprodukte auf dem Markt zu etablieren, hatten sich verschiedene führende Hersteller zum DECT MultiMediaConsortium (DECT-MMC) und im DECT-Forum zusammengeschlossen. Alternativ dazu finden Sie auf den Produkten auch die Bezeichnung DECT-GAP (Generic Access Profile), welche sich nur auf die reine Kompatibilität im Telefoniebereich, ohne zusätzliche Dienstmerkmale, bezieht.



Low Radiation DECT

Mit **Low Radiation DECT** bezeichnet man DECT-Geräte, vor allem schnurlose Telefongeräte, bei denen die Dauersendeleistung reduziert wird, sobald das Mobilteil in der Basisstation ist. Ein anderer Begriff für Low Radiation ist auch DECT ECO. Befindet sich bei herkömmlichen DECT-Geräten das Mobilteil nicht in der Ladestation der Basisstation, besteht zwischen dem Mobilteil und der Basisstation eine ständige Funkverbindung. Diese wird erst unterbrochen, wenn das Mobilteil wieder in der Ladeschale der Basisstation liegt. Bei einigen Herstellern besteht sogar die Möglichkeit, die Sendeleistung der Basisstation bei mehr als nur einem angemeldeten Mobilteil auf bis zu achtzig Prozent zu reduzieren. Bei diesen Geräten ist es unter anderem auch möglich, die Sendeleistung auch dann zu reduzieren, wenn sich das Mobilteil nicht in der Basisstation befindet.

Herkömmliche DECT-Geräte werden bei mehr als nur einem angemeldeten Mobilteil zum Dauersender, da hier die Sendeleistung selbst bei aufgelegtem Mobilteil nicht abgeschaltet wird. Hinzu kommt, dass bei Geräten mit dieser Technologie die Sendeleistung im Stand-by-Betrieb vollkommen abgeschaltet wird. Dies gilt auch, wenn mehrere Mobilteile angemeldet sind. Zu beachten ist jedoch, dass durch die Reduzierung der Sendeleistung auch der Einsatzradius des Mobilteils entsprechend abnimmt. Der bis dahin überbrückbare Abstand gemäß dem DECT-Standard von Basisstation zum Mobilteil reduziert sich bis auf die Hälfte. In der Praxis heißt dies, dass der Abstand zwischen Mobilteil und Basisstation stark eingeschränkt wird.

Modulation

Die Modulation erfolgt mittels GMSK (Gaussian Minimum Shift Keying), mit der sich über die Luftschnittstelle eine Datenübertragungsgeschwindigkeit von 1152 Kbit/s pro Trägerfrequenz ergibt. Die GMSK-Modulation ist eine modifizierte Form der Frequenzumtastung (FSK). Bei dieser Art erfolgt die Modulation mittels zweier Frequenzen, die im gleichen Abstand zu einer Trägerfrequenz angeordnet sind. Die erste Frequenz repräsentiert die digitale „Eins“, die zweite entspricht der digitalen „Null“.

Sprachcodierung

Die Sprache wird mittels **ADPCM** (Adaptive Differential Pulse Code Modulation) codiert. ADPCM ist ein spezielles Verfahren zur Digitalisierung und Mehrkanalübertragung analoger Quellsignale, z. B. von Telefonsignalen. Die Verfahrensschritte sind: Abtastung, Quantisierung und Codierung. Bei einem Frequenzbereich von 50 Hz bis 7 kHz würde bei einer herkömmlichen Pulscodemodulation die Datenrate 128 Kbit/s betragen. Bei ADPCM wird ein Komprimierungsverfahren verwendet, wodurch eine Nutzdatenrate von 32 Kbit/s pro Kanal erreicht wird. Die Geschwindigkeit der parallel dazu übertragenen Signalisierungsdaten beträgt 4800 bit/s.

Kanalzugriff

Es wird das **TDMA-Verfahren** (Time Division Multiple Access) verwendet, d. h., die einzelnen Verbindungen nutzen einen Kanal jeweils mit erhöhter Datenübertragungsgeschwindigkeit, aber nur für einen Bruchteil der Zeit. Zwischen 1880 und 1900 MHz stehen 10 Trägerfrequenzen mit einem Kanalabstand von 1,728 MHz zur Verfügung, wobei jeder Träger in 24 Zeitschlüsse (Slots) eingeteilt wird. Ein Rahmen (Frame) mit 24 Slots wiederholt sich periodisch alle 10 ms. Insgesamt ergibt dies 120 Duplexkanäle.

Reichweite

Bei der Sendeleistung von 250 mW ergibt sich eine Reichweite von bis zu 50 m in Gebäuden und bis zu 300 m im Freien. Mittels Richtantennen lassen sich bis zu 5 km überbrücken. Dies ist für stationäre Systeme, insbesondere WLL (Wireless Local Loop), interessant.

Zellenstrukturen für DECT

Es können mehrere Mobilstationen an einer Basisstation (Zelle) angemeldet werden. Die Teilnehmer haben die Möglichkeit, kostenlos interne Gespräche zu führen. Gleichzeitig kann über eine nicht belegte Mobilstation auf eine Amtsleitung zugegriffen werden. Dieses Verfahren wird als Ein-Zellsystem bezeichnet.

Beim Mehr-Zellen-System sind mehrere Basisstationen über einen Controller miteinander verbunden. Der Controller ist auch für den Anschluss an andere Netze (z. B. ISDN) zuständig. Im gesamten funktechnisch abgedeckten Bereich ist eine Erreichbarkeit gewährleistet. Die Mobilstationen halten selbstständig Kontakt zur stärksten Basisstation in ihrer Reichweite.

Erweiterungen

Zur Erweiterung des Funkbereichs können sogenannte Repeater eingesetzt werden. Diese senden die empfangenen Pakete in einem anderen Zeitschlitz an die nächste Basisstation weiter. Für jedes über einen Repeater geführte Gespräch müssen somit insgesamt vier Zeitschlüsse belegt werden. Die Repeater müssen sich jeweils im Empfangsbereich der Basisstation befinden. Es können also nicht mehrere Repeater in Reihe geschaltet werden.

Kanalwahlverfahren

Die Mobilstation hat mittels **DCS** (Dynamic Channel Selection – dynamisches Kanalwahlverfahren) die Möglichkeit, aus allen zur Verfügung stehenden 120 Kanälen den nicht belegten mit der geringsten Störung auszuwählen. Dazu werden die Kanäle ständig abgehört und der empfangene Pegel für jeden Kanal gespeichert. Dies geschieht sogar während eines Gesprächs. Die Basisstation passt sich der von der Mobilstation gewählten Frequenz und dem gewählten Zeitschlitz an. Daher ist keine Frequenzplanung für die Basisstationen erforderlich.

Verbindungsaufbau

Wünscht die Mobilstation eine Verbindung zum System, baut sie mittels des Kanalwahlverfahrens DCS einen Kanal auf. Der Verbindungswunsch wird sowohl durch abgehende Anrufe als auch durch die Bereitschaft, einen eingehenden Anruf anzunehmen, ausgelöst. Eingehende Anrufe werden mittels des oben genannten Funkrufs von der Basisstation signalisiert.

Handover-Arten

Intracell-Handover ist der Wechsel auf einen anderen Kanal derselben Basisstation. Dabei wird neben dem Zeitschlitz meist auch die Frequenz gewechselt, um eine bessere Übertragungsqualität zu erreichen. Bei einem Intercell-Handover wird nicht nur der Kanal, sondern auch die Basisstation gewechselt.

Seamless Handover

Bei einem Wechsel des Kanals wird eine bestehende Verbindung nicht unterbrochen. Um dies zu erreichen, werden von einer Mobilstation kurzzeitig zwei Kanäle belegt. Die Mobilstation gibt den ersten Kanal erst dann frei, wenn die zweite Verbindung hergestellt wurde. Aber der Aufbau der zweiten Verbindung ist auch bei einem Abbruch der ersten möglich, ohne dass die logische Übertragung endet. Im Gegensatz zu den meisten anderen Systemen, z. B. GSM, wird der Handover von der Mobilstation und nicht von der Basisstation eingeleitet (MCHO – Mobile Controlled Handover). Die Mobilstation sucht dazu ständig die 11 nicht genutzten Zeitschlitz-Paare ab, um eine bessere Verbindung zur selben oder einer anderen Basisstation zu finden. Vorteil dieses Verfahrens ist ein sehr schneller und daher vom Benutzer praktisch nicht wahrnehmbarer Kanalwechsel (bei DECT dauert ein Handover 0,1 ms, bei GSM etwa 1 ms). Das Seamless-Handover-Verfahren wird auch als **Roaming** bezeichnet und findet auch bei anderen Netzwerzkzugriffsverfahren nach dem Standard IEEE 802.21 Anwendung.

Wireless LAN (WLAN)

Wireless LANs sind lokale Infrastrukturen, die ohne Kabelverbindungen arbeiten. Sie sind standardisiert nach IEEE 802.11. Sie nutzen dabei die Funkfrequenzen im ISM-Band (Industrial, Scientific and Medical Band). Besonders vorteilhaft erweisen sich drahtlose Netzwerke auf Messen, im Heimbereich oder in denkmalgeschützten Gebäuden. Meistens sind die Kosten für das Verlegen von Kabeln zwischen Server und angeschlossenen Rechnern unverhältnismäßig hoch oder es ist gar keine Kabelverlegung möglich. Hier bietet sich die Alternative an, mit z. B. 54 Mbit/s Daten übertragen zu können. Die ersten WLAN-Adapter arbeiteten nur mit etwa 2 Mbit/s, später dann mit 11 Mbit/s, aber auch das war für viele Anwendungszwecke ausreichend. Aktuelle Modelle realisieren jetzt **theoretische** Datenübertragungsraten im Bereich von 0,54–7 Gbit/s.

Die Verbindung zum Netzwerk erfolgt über sogenannte **Access-Points**, die im Gebäude installiert werden. Sie bilden die Schnittstelle zwischen bestehendem Ethernet-Netzwerk und WLAN. Die Kommunikation zwischen beiden nennt man auch AP-Modus. Daneben beherrscht ein Access-Point noch den Ad-hoc-Modus (Kommunikation von WLAN-Geräten untereinander) und mitunter den Bridge-Modus (Verbinden von zwei Funkzellen) bzw. Repeater-Modus (Erweiterung einer Funkzelle). Die Reichweite ist ein wichtiges Kriterium. Innerhalb eines Gebäudes erreicht man mit Indoor-Antennen eine Reichweite von ca. 30–100 m. Outdoor-Antennen, in Verbindung mit dem entsprechenden Access-Point, überbrücken im Freien Distanzen bis zu 20 km.

Übertragungstechnik WLAN (IEEE802.11)

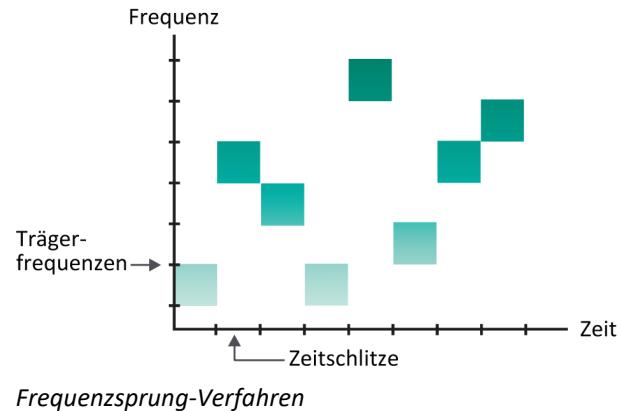
Der grundsätzliche Unterschied zum konventionellen LAN liegt darin, dass die Daten drahtlos (engl. wireless) übertragen werden. Die Anmeldung am WLAN-Netzwerk erfolgt über eine Funkzelle, die eine SSID (Service Set Identifier) besitzt. Alle über gleiche WLANs kommunizierenden Stationen müssen den gleichen Netzwerknamen (SSID) benutzen. Beim WLAN-Protokoll sollten Sie, um eine Abhörsicherheit und den Zugriffsschutz auf das Netz zu gewährleisten, grundsätzlich mit einem **aktuellen** Verschlüsselungsverfahren arbeiten.

Schmalbandübertragung

Die digitale Datenübertragung wird auf eine spezielle Trägerfrequenz aufmoduliert. Unterschiedliche Kanäle werden durch mehrere Trägerfrequenzen ermöglicht. Dieses Verfahren wird als Schmalbandübertragung bezeichnet. Störungen auf diesem Frequenzbereich wirken sich stark auf den Datentransfer aus. Die Datensicherheit ist ohne Verschlüsselung bei diesem Verfahren nicht gewährleistet, da durch Abtastung des möglichen Frequenzbereichs ein solcher Übertragungskanal gefunden (vergleichbar mit der Sendersuche in einem Radio) und dann abgehört werden kann. Gerade zu militärischen Zwecken wurde deshalb ein anderes Verfahren entwickelt. Dabei wurde die Breite des Übertragungsbandes vergrößert (Bandspreizung, Spread Spectrum Technology), um eine höhere Störfestigkeit und Abhörsicherheit zu erreichen.

Frequenzsprung-Verfahren (FHSS)

FHSS (Frequency Hopping Spread Spectrum) ist eine Modulationstechnik. Dabei vereinbaren Sender und Empfänger während des Verbindungsaufbaus eine Pseudozufallsfolge, nach der einige Male pro Sekunde (ca. 20) die Trägerfrequenz geändert wird. Dadurch gibt es praktisch keine Möglichkeit für einen unautorisierten Zuhörer, die Datenübertragung abzuhören bzw. zu manipulieren. Mehrere Kanäle sind dabei im selben Frequenzband möglich, da im Allgemeinen die Sprungfrequenz nur von einem Sender-Empfänger-Paar genutzt wird. Schmalbandige Störungen können durch den ständigen Trägerwechsel nur kurzzeitig die Übertragung beeinflussen. Werden die Daten jedoch durch eine Störung beschädigt, so muss der entsprechende Teil neu gesendet werden.



Spreizband-Verfahren (DSSS)

Bei DSSS (Direct Sequence Spread Spectrum) arbeiten Sender und Empfänger in einem festgelegten Frequenzbereich. Dabei erfolgt die Bandspreizung bereits auf Signalebene. Der Sender verschlüsselt jedes Datenbit in einer Zufallsfolge aus mindestens 10 Zuständen, den sogenannten Chips. Diese werden dann in dem festgelegten Frequenzband gesendet. Für unautorisierte Zuhörer verschwindet das Signal dadurch im Hintergrundrauschen. Der Empfänger, welcher die Verschlüsselungssequenz kennen muss, kann aus dem scheinbaren Rauschen die ursprüngliche Bitfolge restaurieren. Auch hier sind mehrere Kanäle im selben Band möglich, da eine Pseudozufallsfolge immer nur von einem Sender-Empfänger-Paar benutzt wird.

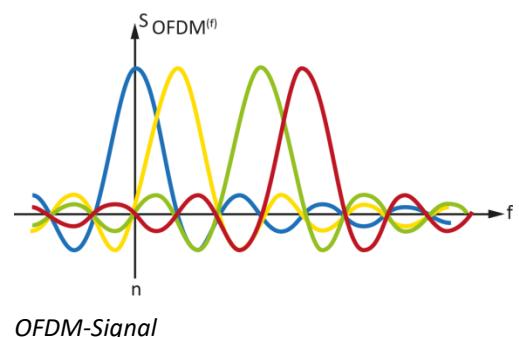
Die Spreizband-Technik ist im Gegensatz zum Frequenzsprung-Verfahren unempfindlicher gegen Interferenzen. Da bei drahtlosen Übertragungen das Signal nicht nur geradlinig vom Sender zum Empfänger gelangt, sondern auch über mehrfache Reflexionen an Wänden oder Gegenständen das Ziel erreicht, erhält der Empfänger mehrere zeitlich versetzte, abgeschwächte oder verzerrte Signale.

Dabei können sich die Signale addieren oder auch gegenseitig auslöschen. Der Empfänger muss daraus den übertragenen Wert erkennen können. Bei der Spreizband-Technik steht dafür ein breiteres Frequenz-Fenster zur Verfügung, sodass hier der Einfluss der Störungen kleiner ist. Außerdem ist eine Replikation von beschädigten Daten möglich, sodass ein erneuter Transfer unnötig ist.

Orthogonal Frequency Division Multiplexing (OFDM)

Aktuelle WLANs (IEEE802.11g/n) verwenden u. a. das **OFDM-Verfahren**, um Informationen zu codieren. OFDM ist eine Technik, bei der mehrere Trägerfrequenzen gleichzeitig benutzt werden, um ein phasen- und amplitudenmoduliertes Signal mit mehreren Bits pro Symbol zu übertragen.

Die Nutzung mehrerer Trägerfrequenzen gleichzeitig hat den Vorteil, dass auf der Empfängerseite ein Signal trotz Echos und Funkreflexionen, wie sie im täglichen Betrieb aufgrund von Reflexionen und Streuung an Wänden auftreten, empfangen werden kann.



OFDM wird mit anderen Frequenzen und Trägeranzahlen auch in anderen Gebieten der Datenübertragung benutzt (z. B. DVB-T – Digital Video Broadcasting-Treestrisch, ADSL und DAB – Digital Audio Broadcasting). Für WLANs werden 52 Trägerkanäle gleichzeitig benutzt.

Funktionalität und Standards

Alle in Europa erhältlichen Funknetze operieren in u. a. vom Normierungsgremium ETSI (European Telecommunications Standards Institute) festgelegten Frequenzbändern. Diese sind bei WLAN:

- ✓ 2,412–2,484 GHz
- ✓ UNII-1 (5,18/5,20/5,22/5,24 GHz); UNII = Unlicensed National Information Infrastructure
- ✓ UNII-2 (5,26–5,32 GHz)
- ✓ UNII-2 Extended (5,50–5,56/5,68–5,70 GHz)

Da es sich um nicht öffentliche Funkanwendungen handelt, sind diese nicht anmeldepflichtig. Die meisten Systeme halten sich auch an die im entsprechenden Standard ETS 300328 festgelegte maximale Sendeleistung von <100 mW, die gesundheitlichen Beeinträchtigungen vorbeugen soll.

WLAN-Betriebsarten

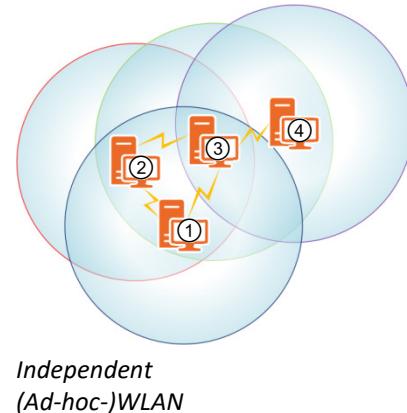
Grundsätzlich kann bei WLANs zwischen drei Konfigurationsmöglichkeiten unterschieden werden, mit denen der Datenaustausch organisiert wird:

- ✓ Independent (Ad-hoc)-WLAN
- ✓ Infrastructure WLAN
- ✓ Wireless Distribution System

Independent (unabhängige) WLANs

arbeiten im Peer-to-Peer-Betrieb. Jeder Rechner mit einer WLAN-Karte ist in diesem Netzwerk gleichberechtigt und hat die Möglichkeit, Daten zu den jeweils anderen Rechnern zu senden. Ein einzelner Rechner kann WLAN-Verbindungen zu den Partnern herstellen, die er „sieht“, d. h., in deren Funkreichweite er sich befindet. Verlässt ein Rechner diesen Bereich, kann er nicht mehr erreicht werden.

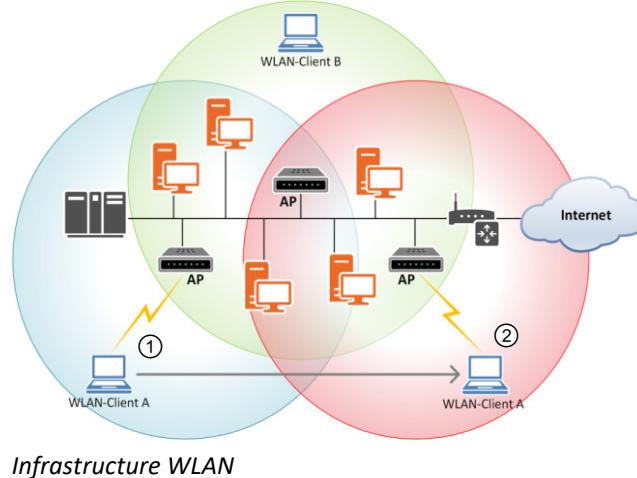
Die Abbildung rechts zeigt eine Situation, in der vier Rechner über Independent WLAN vernetzt wurden. Die Rechner ①, ② und ③ stehen nahe genug zusammen, um sich alle gegenseitig in Reichweite zu haben. Rechner ④ ist jedoch so weit entfernt, dass er nur noch zu einem der drei anderen Rechner eine Verbindung herstellen kann (Rechner ③).



Independent WLANs haben den Vorteil, wenig oder keine Konfiguration zu benötigen. Der Nachteil ist, dass ohne weiteren Aufwand kein Zugriff auf freigegebene Ressourcen möglich ist, die nicht auf WLAN-Rechnern liegen.

Infrastructure WLANs verfügen über eine weitere Komponente. Zusätzlich zu den WLAN-Karten in den Rechnern bilden Access-Points (AP) das Rückgrat des WLAN. Analog zu Mobilfunknetzen baut ein Access-Point eine Funkzelle um sich herum auf.

Verbindungen der WLAN-Clients laufen über den Access-Point. Der Access-Point selbst besitzt zusätzlich ein kabelgebundenes Ethernet-Netzwerkinterface, mit dem er an das vorhandene LAN angeschlossen werden kann. Ein Access-Point realisiert eine Layer2-Verbindung (Bridge) zwischen den Protokollen IEEE802.3 (Ethernet) und IEEE802.11 (WLAN).



Über den Access-Point sind die WLAN-Clients somit in der Lage, auf freigegebene Ressourcen im gesamten Netzwerk zuzugreifen. In der Abbildung oberhalb sind in einem LAN drei Access-Points installiert, die im gleichen Funknetzwerk (SSID) arbeiten, aber verschiedene Funk-Kanäle nutzen. Die in deren Reichweite befindlichen Clients A und B haben Zugriff auf alle Netzwerkressourcen. Über die Roaming-Funktion kann sich ein Client wie A auch von einer Funkzelle in die andere bewegen ① und behält die logische Verbindung zum Netzwerk bei. Die Funkverbindung besteht aber nun zum neuen Access-Point ②. Die Installation von mehreren Access-Points bzw. WLAN-Repeatern an unterschiedlichen Standorten innerhalb eines großen Bereichs kann die Funkausleuchtung optimieren und stellt für die WLAN-Clients die Möglichkeit dar, sich nicht nur innerhalb der Funkzelle eines Access-Points zu bewegen, sondern sich während des mobilen Einsatzes von einer Funkzelle zur nächsten zu bewegen (Roaming). Dabei hat der WLAN-Client aus logischer Sicht jederzeit Zugriff zum kompletten LAN.

Bei **Wireless Distribution System (WDS)** werden mehrere WLAN-Access-Points oder WLAN-Bridges zu einem Funknetzwerk zusammengefasst. Damit erreicht man eine größere Abdeckung als mit nur einem Zugangspunkt. Für die Access-Points und Bridges müssen nur noch entsprechende Stromanschlüsse bzw. PoE (Power over Ethernet) vorhanden sein.

Werden die Access-Points nur direkt verbunden und dürfen sich an diesen keine weiteren Clients anmelden, spricht man vom **Bridging-Modus**. Ist auch die Anmeldung von Clients möglich, bezeichnet man das als **Repeating-Modus**. Alle WDS-Access-Points sollten auf dem gleichen Kanal arbeiten sowie dieselbe SSID und denselben WLAN-Schlüssel verwenden. Zudem müssen jedem Access-Point die WLAN-MAC-Adressen des anderen Access-Points bekannt sein. Sollen mehrere Access-Points zu einem WDS zusammengeschaltet werden, sollte darauf geachtet werden, dass sie nach Möglichkeit vom gleichen Hersteller stammen. Ansonsten kann es bei den neuesten WLAN-Standards (IEEE802.11ac/ad) ggf. zu Inkompatibilitäten führen.

Roaming

In größeren Netzwerkumgebungen können mehrere Access-Points so angeordnet werden, dass mobile Einheiten nahtlos von einem Einzugsbereich eines Access-Points in einen anderen Bereich wandern können, ohne dass eine Unterbrechung der Netzverbindung auftritt.

Power Management

Mobile Clients (Laptops, PDAs etc.) sind auf eine hohe Leistung der verwendeten Stromquelle angewiesen. Da eine Funkübertragung grundsätzlich relativ große Energiemengen benötigt, besitzen Wireless-LAN-Lösungen meist ein Power Management. Dieses ist in der Lage, den WLAN-Adapter abzuschalten, wenn keine Daten übertragen werden.

SSID

Die **SSID** (Service Set Identifier) ist ein eindeutiger Name eines Funknetzes (Funkzelle). Er wird im Access-Point eingetragen und ist frei wählbar. Alle WLAN-Clients, die sich an diesem Access-Point anmelden wollen, müssen diese SSID nutzen. Werden mehrere Access-Points mit der gleichen SSID genutzt, nennt man diese ESSID (Extended SSID). Dadurch wird der räumliche Bereich der Funkzellen erweitert und der mobile Nutzer kann ohne Unterbrechung der Kommunikation zwischen den einzelnen Funkzellen wechseln (Roaming).

Bluetooth

Die erste Spezifikation von Bluetooth wurde im Mai 1998 von der Bluetooth-SIG (Special Interest Group) vorgestellt. Die Bluetooth-SIG wurde von der Firma Ericsson gegründet und bestand zu Beginn aus den Firmen IBM, Intel, Nokia und Toshiba. Im Juli 1999 stellte dann dieses Konsortium den Bluetooth-Standard in der Version 1.0 vor, und weitere Firmen kamen zur Bluetooth-SIG: Microsoft, 3COM, Lucent und Motorola. Die Absicht in der Entwicklung von Bluetooth bestand darin, eine kabellose Funkverbindung zu schaffen, die energieeffizient arbeitet und trotzdem hohe Übertragungsraten ermöglicht.

Der große Vorteil von Bluetooth gegenüber dem IrDA besteht darin, dass die Endgeräte **ohne Sichtkontakt** miteinander kommunizieren und dabei je nach Übertragungsprotokoll eine Bruttodatenübertragungsrate von 700 Kbit/s bis zu 20 Mbit/s erreichen können. Die maximale Reichweite ist abhängig von der Sendeleistung und beträgt ca. 100 Meter (bei 100mW), 10 Meter (bei 2,5 mW) und 1 m (bei 1 mW Sendeleistung). Die Funkfrequenz liegt im 2,4-GHz-Bereich, der weltweit lizenzfrei und somit gebührenfrei ist. Da diese Frequenzen auch vom WLAN-Protokoll genutzt werden, kann es hier zu gegenseitigen Störungen kommen, sofern sich die Funkkanäle überlagern. Bluetooth wurde im Standard IEEE 802.15 WPAN (Wireless Personal Area Network) spezifiziert.

Frequenzsprung-Verfahren (FHSS)

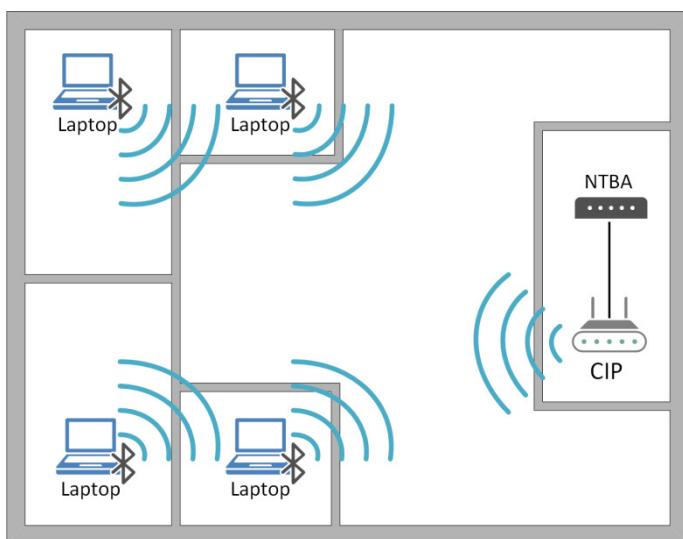
Der Frequenzbereich für Bluetooth liegt zwischen 2,402 GHz und 2,480 GHz. Innerhalb dieses Frequenzbereichs arbeitet das Frequenzsprung-Verfahren in 79 Schritten zu je 1 MHz Abstand. In einer Sekunde erfolgen 1600 Frequenzwechsel. In einem Piconet (Mini-Netzwerk aus Bluetooth-Geräten) können maximal 8 Bluetooth-Endgeräte miteinander kommunizieren. Sobald zwei oder mehrere Bluetooth-Endgeräte im Betrieb sind, identifizieren sie sich anhand einer 48 Bit langen, einmaligen Seriennummer. Das erste in einem Piconet aktivierte Endgerät wird automatisch zum Master und übernimmt die Steuerung des Frequenzsprung-Verfahrens.

Einsatzgebiete

Bluetooth findet aufgrund des effizienten Energiemanagements und der hohen Übertragungsrate vor allem im mobilen Bereich seinen Platz. Handys, Organizer, PDAs, Notebooks etc. werden mittlerweile meist standardmäßig mit der Bluetooth-Technologie ausgestattet.

Eines der ersten Bluetooth-Geräte war eine portable Freisprecheinrichtung der Firma Ericsson. Die Freisprecheinrichtung wog etwa 20 Gramm. Bei einer Reichweite von etwa 10 Metern konnte das Handy in einer Tasche, einem Aktenkoffer oder mitunter sogar im Nachbarzimmer liegen.

Ein weiteres Highlight ist das CIP (Common ISDN Access Profile), das ISDN über Bluetooth ermöglicht. In diesem CIP stehen den Bluetooth-Endgeräten alle ISDN-Leistungsmerkmale im B- und D-Kanal zur Verfügung. Als Zentrale arbeitet ein ISDN-Access-Point, der mit dem ISDN-NTBA verbunden wird. Dieser versorgt die aktiven Bluetooth-Endgeräte in einem Umkreis bis zu 100 Metern mit den ISDN-Leistungsmerkmalen.



Common ISDN Access Profile (CIP)

Entwicklungen

Derzeit wird an der Reduzierung des Stromverbrauches, an der Optimierung des Verschlüsselungsstandards und darauf aufbauenden Chipsätzen gearbeitet. Der letzte Standard (Bluetooth 4.0 + EDR) beschreibt auch eine Optimierung im Verbindungsaufbau sowie der zu überbrückenden Distanzen.

Bluetooth findet in unterschiedlichsten Bereichen Anwendung:

- ✓ kabellose Musikübertragung zwischen Stereoanlage und Lautsprecher
- ✓ Überwachung von Kühlschrank, Heizung und Alarmanlage durch eine Bluetooth-Schaltzentrale
- ✓ ein Bluetooth-Lesestift, mit dem Textseiten eingescannt und später in einem Textverarbeitungsprogramm bearbeitet werden können
- ✓ Bluetooth-Headset
- ✓ Übertragung von Fotos zwischen Digitalkamera und Smartphone bzw. Digitalkamera und PC

2.4 Übung

Fragen zu Medien für die Datenübertragung

Übungsdatei: --

Ergebnisdatei: uebung02.pdf

1. Welche Farbe weisen Multimode- bzw. Singlemode-Patchkabel auf?
2. Wo werden hauptsächlich Multimode- bzw. Monomodekabel eingesetzt?
3. Sie sind verantwortlich für das Einsatzkonzept eines neuen Verkabelungssystems auf Kupferbasis. Welche Entscheidung würden Sie bei einem maximalen Investitionsschutz (beste technische Parameter) für das Stecker- und Kabelsystem treffen?

3 Erweiterung von Netzwerken

In diesem Kapitel erfahren Sie

- ✓ welche aktiven Komponenten verfügbar sind
- ✓ welche Komponenten für Ihr Unternehmen sinnvoll sind
- ✓ welche Geräte wo eingesetzt werden können

Voraussetzungen

- ✓ Wissen über das ISO/OSI-Referenz-Modell
- ✓ Wissen über Netzwerk-Topologien

3.1 Die Aufgabe von aktiven Komponenten

Aktive Komponenten dienen dazu, Endsysteme (z. B. PCs, Server und Mobilfunkgeräte) mit der physikalischen Infrastruktur (Twisted Pair, LWL oder Funk) des Netzwerkes zu verbinden. Außerdem koppeln sie unterschiedliche Übertragungsmedien, Protokolle und Übertragungsgeschwindigkeiten miteinander. Durch den gezielten Einsatz von bestimmten aktiven Komponenten kann in einem Netzwerk der Datendurchsatz gesteigert werden.

3.2 Einteilung aktiver Komponenten nach dem ISO/OSI-Modell

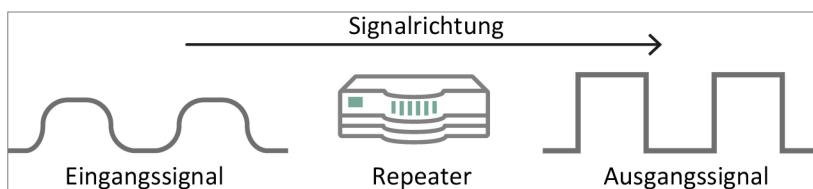
In Anlehnung an das ISO/OSI-Modell werden aktive Komponenten auch den jeweiligen Schichten des OSI Modells zugewiesen. Die folgende Tabelle zeigt, welcher Schicht die Geräte, dem allgemeinen Verständnis nach, zugeordnet sind. Es gibt jedoch auch Ausnahmen (z. B. Buffered Repeater):

OSI-Schicht	Komponente	Merkmale
4–7	Gateway, Server, PC, Proxy, VoIP-Telefon, Application Level Firewall	Komplettes Datenpaket wird umgeformt
3	Router, Layer-3-Switch (Multilayer-Switch), Packet-Firewall	Verbindung von Netzwerken über IPv4 bzw. IPv6
2	Bridge, Switch, Access-Point, Netzwerkkarte	Verbindet Endsysteme mit Netzwerk-komponenten
1	Hub, Repeater, Medienkonverter	Signalregenerierung, Signalumwandlung

3.3 Koppelemente

Repeater

Da elektrische Signale aufgrund der Übertragungseigenschaften von Leitern in ihrer Intensität abgeschwächt werden, ist es oftmals erforderlich, diese Signale aufzubereiten (regenerieren). Mithilfe von Repeatern ist es möglich, das ursprüngliche Übertragungssignal vollständig wiederherzustellen. Dabei empfängt ein **Repeater** das **Sendesignal**, bereitet dieses auf und leitet das Signal an den Empfänger weiter. Ein Repeater arbeitet vollkommen protokolltransparent auf der physikalischen Schicht und wird nur zur Überwindung von Längenrestriktionen einzelner Kabelsegmente eingesetzt. Er findet heutzutage primär Anwendung im Weitverkehrsbereich (WAN), wurde jedoch früher auch im LAN zur Kopplung von Kabelsegmenten auf Basis von Koaxialkabeln verwendet. Auch findet sich dort der WLAN Repeater, der die Ausdehnung eines Wireless LAN vergrößert.



Signalregenerierung durch einen Repeater

Die Regenerierungseigenschaften von Repeatern ermöglichen es, dass fehlerbehaftete Bitströme nicht auf das andere physikalische Segment weitergeleitet werden. Somit werden Signalfehler auf ein Netzsegment begrenzt.

Sonderformen

Es gibt verschiedene Sonderformen von Repeatern:

- ✓ Remote Repeater
- ✓ Multiport Repeater (Hub)
- ✓ Optische Repeater
- ✓ Buffered Repeater

Remote Repeater

Bei Remote Repeatern werden zwei Repeatern per Glasfaserkabel miteinander verbunden, um eine größere Distanz bei Kabeln zu überbrücken.

Multiport Repeater

Multiport Repeater besitzen mehrere Ausgänge. Dadurch ist es möglich, mehrere Segmente miteinander zu verbinden. Sie wurden in der Folge auch als **Hub** bezeichnet.

Optische Repeater

Optische Repeatern werden dazu verwendet, auftretende Dämpfungsverluste bei optischen Signalen auszugleichen. Bei sehr langen Strecken, besonders bei Monomodefasern, wird das Signal in gewissen Abständen von einem optischen Repeater regeneriert und verstärkt.

Optische Repeatern erfüllen prinzipiell die gleiche Funktion wie herkömmliche Repeatern. Einziger Unterschied ist, dass optische Repeatern nur in Netzwerken mit Glasfaserstrecken eingesetzt werden. Wesentlicher Unterschied zu den herkömmlichen Repeatern ist, dass optische Repeatern die Lichtsignale empfangen, diese in elektrische Signale umwandeln und anschließend wieder als optische Signale an den Empfänger weiterleiten. Ein Beispiel hierfür ist das Transatlantikkabel, wo jeweils im Abstand von 66 km ein optischer Repeater installiert wurde.

Buffered Repeater

Ein Buffered Repeater arbeitet auf der zweiten Schicht des OSI-Modells. Im Gegensatz zu den Standard Repeatern empfängt ein Buffered Repeater nur vollständige Datenframes. Buffered Repeater arbeiten nach dem Store-and-forward-Prinzip. Dabei werden die empfangenen Signale im Repeater zwischengespeichert, bevor sie über das Netzwerk an den Empfänger weitergeleitet werden.

Einsatzgebiete von Repeatern

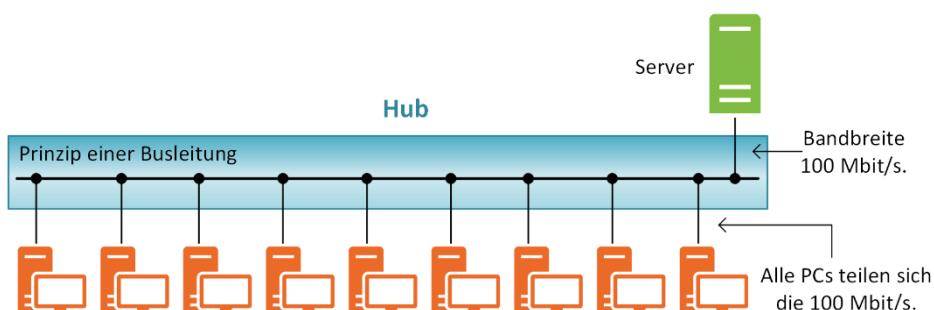
Repeaters sind vor allem da notwendig, wo es um die Ausdehnung der Übertragungsstrecken geht. Sie dienen zur Verlängerung von Glasfaserstrecken, zur Ausdehnung eines Twisted-Pair-Segments oder zur Aufbereitung von Signalen, wenn diese ansonsten aufgrund schlechter Leitungsqualitäten am Empfänger nicht mehr decodiert werden könnten.

Hub

Ein **Hub** wird häufig auch als **Kabelkonzentrator** oder **Sternverteiler** bezeichnet, da er als zentrale Stelle in einem sternförmigen Netzwerk verwendet wird. Jeder Datentransport im Netzwerk wird an alle Ports weitergeleitet. Hubs sind intern vom Grundprinzip ähnlich einer Bus-Topologie aufgebaut. Die gesamte Bandbreite wird unter den angeschlossenen Teilnehmern aufgeteilt.

Bei einem 100-Mbit-Netzwerk mit 10 Teilnehmern erhält jeder Teilnehmer eine theoretische Bandbreite von 10 Mbit, bei 20 Teilnehmern am gleichen Segment sind dies 5 Mbit pro Teilnehmer. Laufende Kollisionen der Bitströme sind daher unvermeidbar. Die Folge sind lange Wartezeiten beim Datenaustausch innerhalb des Netzwerks.

Ein Hub mit allen angeschlossenen PCs bildet somit eine Kollisionsdomäne. „Eine Kollisionsdomäne umfasst alle Netzwerkgeräte, die um den Zugriff auf ein gemeinsames Übertragungsmedium konkurrieren.“ (<https://de.wikipedia.org/wiki/Kollisionsdomäne>). Die Verwendung eines Hubs zur Kopplung von Netzen erweitert die Kollisionsdomäne um die Anzahl der angeschlossenen Netzwerkgeräte im gekoppelten Segment.



Funktionsprinzip eines Shared Ethernet

Hubs finden in modernen lokalen Netzwerken keine Anwendung mehr. Das liegt sowohl an der gemeinsamen Nutzung der verfügbaren Bandbreite als auch an der Performance dieser Komponenten.

Bridge

Die **Bridge** verbindet lokale Netzwerksegmente miteinander. Sie verfügt im einfachsten Fall nur über zwei Ports. Im Gegensatz zu einem Switch kann man mit ihr keine virtuellen LANs (VLANs) bilden und den Netzwerkverkehr auch nicht priorisieren. Dies liegt daran, weil die Bridge auf der Schicht 2 des OSI-Modells arbeitet und das Protokoll IEEE 802.1D nutzt, welches das Weiterleiten der Frames in andere Segmente anhand deren Ziel-MAC-Adresse definiert.

Durch die Einordnung auf der Schicht 2 ist eine Bridge für höhere Protokollsichten transparent. Das bedeutet, dass sämtliche Protokolle, die auf Schicht 2 aufsetzen, von der Bridge unbearbeitet weitergeleitet werden. Im Unterschied zum Repeater oder Hub kann eine Bridge unterschiedliche Übertragungsraten und unterschiedliche Zugriffsverfahren zwischen den Ports umsetzen. Eine Sonderform ist der **Access-Point**, welcher das Zugriffsverfahren IEEE 802.3 (Ethernet) in das Zugriffsverfahren IEEE 802.11 (WLAN) oder umgekehrt umsetzt.

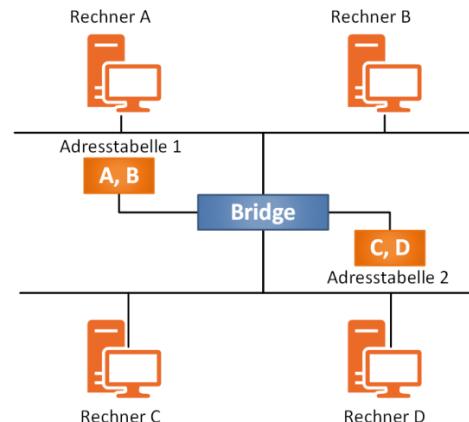


Eine Bridge kann keine Datenframes in Form von Broadcast oder Multicast auf ein Segment begrenzen, d. h., alle Stationen, die an einer Bridge angeschlossen sind, bilden ebenso wie beim Hub eine Broadcastdomäne.

Learning Bridge

Jede Bridge ist eine „Learning Bridge“, welche im Verlauf der Kommunikationsvorgänge, ihre Adressstabellen automatisch aufbaut und verwaltet. Sie lernt dabei die MAC-Adressen der angeschlossenen Netzwerkkarten, an ihren Ports, durch einfaches Mitlesen der Absenderadressen (Quell- oder Source-Adresse) aller ankommenden Frames kennen. Mit diesen Adressstabellen trägt eine Bridge auch dazu bei, den Netzverkehr zwischen den einzelnen Segmenten zu reduzieren.

Da die Bridge „weiß“, welche Station mit welcher MAC-Adresse in welchem Segment liegt, leitet sie den lokalen Verkehr innerhalb eines Segments nicht weiter. Die anderen Daten dagegen werden gezielt in das andere Segment geschickt. Letztendlich trägt eine Bridge damit zur Entlastung des Gesamtnetzes bei.

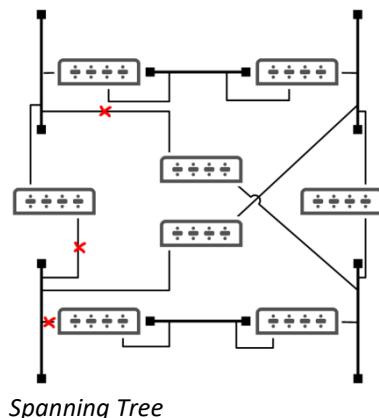


Spanning-Tree-Algorithmus

Bei Bridges wird sehr häufig das Spanning-Tree-Protokoll (STP) angewendet. **Spanning Tree** ist ein Verfahren zur Schleifenunterdrückung in Netzwerken, die mit Bridges gekoppelt sind.

Wenn in einem Gesamtnetz mehrere Bridges eingesetzt werden, können zwischen Sender und Empfänger mehrere mögliche Verbindungswege entstehen. Dies kann beabsichtigt sein, um redundante Verbindungen für den Fall des Ausfalls einer Bridge zu schaffen.

Wenn es aber mehrere Wege zwischen Sender und Empfänger gibt, passiert es, dass Frames wie in einer Schleife (Loop) immer wieder von einer Bridge zur nächsten weitergereicht werden. Dieses n-malige Weiterreichen führt dazu, dass das Netz durch Überlastung zum Stillstand kommt.



Spanning Tree legt in einem Netz immer einen eindeutigen Weg zwischen Sender und Empfänger über Bridges fest und blockiert redundante Verbindungen. Dadurch sind die MAC-Adressen-Tabellen auf jeder Bridge immer eindeutig und es können keine Loops mehr entstehen. Fällt die aktive Verbindung zwischen den Bridges aus, so schaltet Spanning Tree eine blockierte Leitung frei. Dieses Protokoll findet auch bei Switchen Anwendung. Neben dem Protokoll Spanning Tree (IEEE 802.1d) gibt es die Standard-Versionen Rapid Spanning Tree (IEEE 802.1w) und Multiple Spanning Tree (IEEE 802.1s). In Rechenzentren kommen u. a. verstärkt die Verfahren SPB (Shortest Path Bridging) nach IEEE 802.1aq bzw. TRILL (Transparent Interconnection of Lots of Links) zum Einsatz. Beide Verfahren nutzen, im Gegensatz zum klassischen Spanning Tree, alle möglichen Verbindungen zwischen Sender und Empfänger.

Switch

Ein Switch (engl. für „Schalter“) ist die Weiterentwicklung der Bridge und arbeitet in der Regel ebenfalls auf der Schicht 2 des OSI-Modells. Ein Switch besitzt die Funktionalität einer Bridge. Der Unterschied zur Bridge besteht darin, dass einerseits ein Switch entschieden mehr Ports als eine Bridge besitzt und extrem schnell zwischen den vorhandenen Ports schalten („switchen“) kann. Das realisiert er durch eine Non-Blocking-Architektur seiner Backplane. Andererseits hat der Switch zusätzliche Funktionen, wie z. B. Protokolle zur Bildung von VLANs, zur Priorisierung des Layer-2-Verkehrs (Class of Service, CoS) und zur Sicherheit der angeschlossenen Stationen (u. a. MAC-Filter, IEEE 802.1X).

Damit ein Switch schnell zwischen den Ports vermitteln kann, muss er intern (auf seiner Backplane) mit sehr hoher Geschwindigkeit arbeiten. Je nach Gerät werden hier mittlerweile Geschwindigkeiten von 40 Gbit/s oder mehr erreicht, womit problemlos mehrere Ports, die z. B. mit 100 Mbit/s, 1 Gbit/s oder 10 Gbit/s arbeiten, gleichzeitig bedient werden können.

Switching-Technologie und Mikrosegmentierung

Die Mikrosegmentierung stellt bei der Switching-Technologie den Ansatz dar, dem steigenden Bandbreitenbedarf gerecht zu werden. Ein Switch teilt das gesamte Netz in kleine Segmente auf, oder anders gesagt, jeder einzelne Port stellt ein einzelnes, eigenes Netzwerksegment dar. Dies führt zu einer sogenannten „Mikrosegmentierung“, bei der jedes Gerät an einen eigenen dedizierten Switch-Port angeschlossen ist und je für sich alleine ein eigenes Netzwerksegment bildet und so die volle Bandbreite blockadefrei nutzen kann.



Gigabit-Micro-Switch für Kabelkanaleinbau

Quelle: Microsens

Die konsequente Weiterentwicklung dieses Ansatzes führte zu dezentralen Netzwerken, in denen Micro-Switches in der Nähe der Arbeitsplätze installiert werden. Bevorzugte Einbauorte sind im Kabelkanal, in Installationssäulen, in Bodentanks, in Steckdosenleisten oder im Mobiliar. Da in einem Micro-Switch vier Switch-Ports auf einen Uplink-Port kommen, müssen in den Gebäuden deutlich weniger Leitungen zu den Arbeitsplätzen verlegt werden, was zu geringeren Brandlasten durch die Kabel führt. Werden Glasfasern für die Uplink-Ports der Micro-Switches verwendet, sind sehr viel größere Leitungslängen möglich (550 m statt 100 m), sodass in vielen Fällen nur noch ein zentraler Verteilerraum für das gesamte Gebäude benötigt wird.

Kriterien für die Neuanschaffung

Wenn Sie sich einen Switch anschaffen, sollten Sie auf die folgenden Faktoren achten:

- ✓ Anzahl der benötigten Ports
- ✓ mechanische Ausführung: Standalone Variante (Desktop Switch), professionelle Variante zur Integration in Kabelkanälen bzw. Bodentanks (Micro-Switch), robuste Ausführung (Industrial-Switch) oder für den Einbau in zentralen Verteilern (19"-Switch)
- ✓ konfigurierbar (managebar) oder nicht managebar
- ✓ ggf. Notwendigkeit des Anschlusses von Verbrauchern (wie IP-Telefone) über die Datenleitung (Power over Ethernet)
- ✓ Standalone Switch oder kaskadierbarer Switch (stackable)
- ✓ fester oder modularer Aufbau und Redundanz der Netzteile
- ✓ Dual-Speed- (10/100 Mbit/s) oder Triple-Speed (10/100/1000 Mbit/s) Switch

- ✓ benötigte Bandbreite der Uplink-Ports und Port Aggregation
- ✓ reine Layer-2/3- oder auch Applikations-Funktionalität, z. B. DHCP
- ✓ Investitionsschutz bis Auslauf der Geräteproduktion EOL (End of life)
- ✓ Port Security, d. h. Kontrolle des Zugriffs anhand der am Port anliegenden MAC-Adresse
- ✓ Übernahme zusätzlicher Funktionen wie beispielsweise der Steuerung der Gebäudetechnik im Smart Building/Smart Home durch Mini-Programme (Applications, kurz: Apps)

Managebare Switche

Managebare Switche ermöglichen die Konfiguration des Gerätes dediziert nach den Netzanforderungen. Hierzu existieren mehrere Möglichkeiten:

- ✓ Der Switch verfügt über einen seriellen Port. Dann können Sie mittels eines entsprechenden Kabels über eine Applikation, z. B. PuTTY, eine Initialkonfiguration durchführen.
- ✓ Das Gerät verfügt über eine Default-IP-Adresse. Hier haben Sie die Möglichkeit, den Switch remote z. B. über Telnet oder SSH zu konfigurieren.
- ✓ Der Switch verfügt über einen integrierten Webserver (http oder https). Zum Managen über die grafische Benutzeroberfläche nutzen Sie einfach Ihren Webbrowser und geben dort die Default-IP-Adresse des Switches an.



Managebare Switche sollten grundsätzlich in Netzwerken eingesetzt werden, in denen auch andere manageable Geräte (Server, NAS, SAN) Verwendung finden.

Nicht managebare Switche

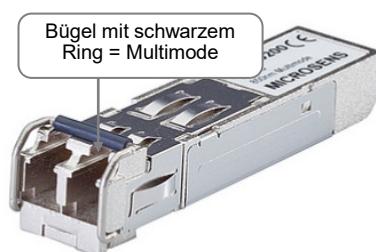
Nicht managebare Switche sind in ihrer Anschaffung kostengünstig. Sie sind primär für kleinere Büros oder Geschäftsstellen geeignet.

Uplink-Port (Highspeed Port)

Bei den meisten Switchen besteht die Möglichkeit, mittels eines modularen Steckplatzes ein Highspeed-Modul einzusetzen. Mit einem LWL-Backbone zwischen den Switchen lassen sich Geschwindigkeit und Entfernung deutlich steigern. Passende Gigabit- oder 10-Gigabit-Module kommen hier zum Einsatz. Für noch höhere Anforderungen können auch Module für 40 oder 100 Gbit/s gewählt werden.

Moderne Switches verfügen über bereits integrierte modulare Uplink-Ports für den Einsatz von steckbaren Transceivern. Das am weitesten verbreitete Format stellen SFPs (Small Form-Factor Pluggable, umgangssprachlich als Mini-GBIC bezeichnet) und SFP+ Transceiver (Enhanced Small Form-Factor Pluggable) dar. Über SFPs werden üblicherweise Gigabit-Ethernet-Glasfaser-Strecken verbunden. Die maximale Distanz hängt von der Art der Glasfaser und den optischen Parametern der verwendeten Lasertechnologie ab. Bei Multimodefasern liegt die max. Distanz bei 500 m (50/125 µm, 850 nm, 1000Base-SX). Bei Verwendung von Monomodefasern sind folgende Distanzen möglich: 10 km (9/125 µm, 1310nm, 1000Base-LX), 40 km (1310 nm, 1000Base-EX), 80 km (1550 nm, 1000Base-ZX) und 120 km (1550 nm, 1000Base-EZX).

Als Weiterentwicklung der SFPs unterstützen SFP+ Transceiver Datenraten bis zu 10 Gbit/s. Mit den wichtigsten SFP+ Varianten können folgende Distanzen überbrückt werden: Multimode 300 m (OM3) bzw. 400m (OM4) (50/125 µm, 850nm, 10GBase-SR); Monomode 10 km (9/125 µm, 1310 nm, 10GBase-LR), 40 km (1550 nm, 10GBase-ER), 80 km (1550 nm, 10GBase-ZR).



SFP Transceiver für 1-Gbit-Ethernet

Mit QSFP+ Transceivern können 40 Gbit/s Uplinks (4×10 Gbit/s) realisiert werden, optional mit QSFP28 bis zu 100 Gbit/s (4×25 Gbit/s). Im Bereich hochperformanter Anbindung setzt sich der CFP-Transceiver als weiteres Format zunehmend durch. Damit werden Geschwindigkeiten von 100 Gbit/s (10×10 Gbit/s oder 4×25 Gbit/s) übertragen.

Mit zunehmender Miniaturisierung konnten die mechanischen Abmessungen halbiert (CFP2) oder gar auf ein Viertel der ursprünglichen CFP-Größe gebracht werden (CFP4). Die Farbe des Verriegelungsbügels von SFP-Transceiver gibt auch im gesteckten Zustand Aufschluss, ob es sich um eine Multimode- oder Monomode-Variante handelt. Verfügt der Bügel über einen schwarzen Ring (so wie in der vorherigen Abbildung), handelt es sich um eine Multimode-Version (SX). Ein blauer (LX) bzw. grüner Ring (ZX) weist auf den Anschluss von Monomode-Kabeln hin. Auch weitere Farben (violett, orange usw.) sind verfügbar, hier handelt es sich um spezielle xWDM-Transceiver.

Analog gibt auch die Farbe des LWL-Steckverbinder einen Hinweis darauf, ob es sich um eine Multimode- oder Monomode-Variante handelt. Ein beigegebener Steckverbinder ist ein Multimodestecker (50/125 bzw. 62,5/125) und somit mit einem SFP zu verbinden.

Der SFP besitzt einen schwarz markierten Bügel. Ein blauer Steckverbinder ist ein Monomodestecker (9/125) mit einem sogenannten Gradschliff (PC, Physical Contact) und somit bei allen blau bzw. grün markierten SFP-Transceivern zu verwenden. Ein grüner Steckverbinder ist ebenfalls ein Monomodesteckverbinder, allerdings mit einer schrägen Stirnfläche (9° Schrägschliff, APC = Angled Physical Contact) und deshalb nur beim Übergang Stecker zu Stecker zu verwenden.

Stecker mit Schrägschliff sind nicht für den Anschluss aktiver Transceiver geeignet.



Verwendung der Farbcodierung von steckbaren Glasfasertransceivern und Glasfasersteckern:

- ✓ Schwarzer Bügel = Multimode; Anschluss eines beigefarbenen Steckverbinder
- ✓ Bunter Bügel = Monomode; nutzt einen blauen Steckverbinder mit Gradschliff (PC)

Port Aggregation (IEEE 802.1AX)

Mit dieser Eigenschaft ist es Switchen möglich, mehrere physikalische Ports zu einem logischen Kanal zu bündeln. Dadurch kann zum Beispiel der Datendurchsatz bei einer Backbone-Anbindung zwischen den Geräten gesteigert werden. Die Möglichkeiten der Port Aggregation werden überwiegend für den Einsatz von **Switch-zu-Switch**-Verbindungen oder für eine Hochgeschwindigkeitsverbindung **Server-zu-Switch** verwendet. Seitens der Hersteller können aktuell bis zu 8 Ports bzw. bis zu 2 Uplink-Ports für Port Aggregation zusammengefasst werden. Das dabei genutzte **Link Aggregation Control Protocol** (LACP) ermöglicht eine dynamische Bündelung der einzelnen Links. Mit LACP wird eine Lastverteilung auf die einzelnen Links vorgenommen werden, was auch die Ausfallsicherheit der gesamten Verbindung erhöht. Fällt eine einzelne Verbindung aus, kann die Datenmenge der intakten Verbindungen bis zu ihren maximalen Datenraten erhöht werden.

VLAN-Fähigkeit (IEEE 802.1Q)

Ein VLAN ist eine in sich geschlossene logische Gruppe innerhalb eines physikalischen Netzwerkes. Diese logischen Gruppen bilden sozusagen ein eigenständiges Netzwerk im Netzwerk. Alle Frames werden nur innerhalb dieses logischen Segmentes versendet. Auch Broadcastframes, die sonst über alle Ports eines Switches weitergeleitet werden, verbleiben nun im VLAN. Ein VLAN kann sowohl über einen Switch als auch über mehrere Switch gebildet werden.

Switches für den industriellen Einsatz

Moderne Switches verfügen mittlerweile über eine enorme Rechenleistung, sodass sie neben dem reinen Datentransfer vermehrt zusätzliche Aufgaben übernehmen. Damit können sie zu intelligenten Steuerzentralen in modernen Gebäuden werden. Applikationen, kurz Apps, werden als Mini-Programme auf den Switchen installiert, ohne dass in die Switch-Firmware eingegriffen werden muss. Apps ermöglichen weitreichende Funktionalitäten wie beispielsweise die Steuerung von Beleuchtung, Beschattung, Heizung und Klimatisierung im Raum. Über die Kopplung mit Präsenzmeldern und einem elektronischen Kalender können alle relevanten Anlagen der technischen Gebäudeausrüstung anwesenheits- und zeitabhängig gesteuert werden. Das Konzept des Smart Buildings basiert darauf.

Anforderungen

In der rauen Umgebung von Gewerbebetrieben und Industriegebäuden kommen sogenannte „ruggedized Switches“ zum Einsatz. Sie können auf Hutschienen montiert und platzsparend in kleinen Wandverteilern oder einem dafür vorgesehenen Feld des Elektroverteilers untergebracht werden. Bei modularen Ausführungen können einzelne Module bedarfsabhängig aneinandergereiht werden.



Industrieswitch mit Erweiterungsmodul

Besonderheiten der Industrieswitches

Um den Anforderungen im Produktionsbereich gerecht zu werden, müssen die verwendeten Ethernet-Komponenten erweiterte Voraussetzungen erfüllen. Hierzu zählen:

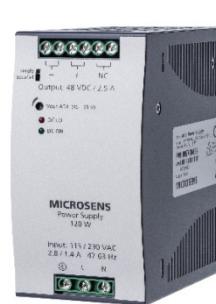
- ✓ Robustere technische Ausführung, möglichst lüfterlos
- ✓ Möglichkeit der Befestigung auf Tragschienen (Hutschiene), mit 48VDC
- ✓ Redundante Spannungsversorgung für Power over Ethernet (PoE)
- ✓ Erhöhter Schutz gegen elektromagnetische Störungen
- ✓ Erweiterter Temperaturbereich (0–60°C Standard bzw. -40–75°C Erweitert)
- ✓ Besserer Schutz gegen Feuchtigkeit (bis 95% rel. Luftfeuchte)
- ✓ Besonderer Schutz gegen Eindringen von Staub und gegen Spritzwasser
- ✓ Schutz gegen Schmierstoffe und Öle
- ✓ Vibrationsfestigkeit beim Einsatz an Maschinen
- ✓ Höhere Ausfallsicherheit durch die Nutzung von physikalischen Ringstrukturen
- ✓ Höchste Zuverlässigkeit im Betrieb (Mean Time Between Failures - MTBF)
- ✓ Zusätzliche I/O-Anschlüsse (z. B. für Störungsmeldungen)
- ✓ Flexible Firmware-Architektur für optimale Softwareerweiterung



*Profi Line Modular Basis-Switch
Hersteller: Microsens*



Erweiterungsmodul



Spannungsversorgung 48 VDC für PoE/PoE+

Die Ethernet-Infrastruktur wird durch den offenen PROFINET (*Process Field Network*) standardkonform spezifiziert. Durch die teilweise extremen Bedingungen in der Fertigung werden auch höhere Anforderungen an die Datenverkabelung und die Anschlusspunkte gestellt. Die Qualität der übertragenen Daten muss über den gesamten Transportweg gesichert werden und Störungen an den Anschlusspunkten sind entsprechend zu minimieren. Diese Störungen treten gerade an den Steckern der Anschlussdosen und Buchsen der verwendeten Komponenten auf.

Um dies zu vermeiden, haben Hersteller eine eigene Produktlinie für den Einsatz im industriellen Bereich entwickelt. Sie verfügt über stabile und geschützte Gehäuse und entspricht dem IP-44-Standard (International Protection) oder höher.

Router

Ein **Router** ist ein Gerät, das getrennte Netzwerke koppeln oder Netzwerke in Subnetze trennen kann. Diese Kopplung kann eine Verbindung zwischen zwei oder mehr lokalen Netzen oder die Verbindung zwischen LAN und WAN bzw. WAN und WAN sein. Er arbeitet auf der Schicht 3 des OSI-Referenzmodells mit den Protokollen IP und IPv6. Die wesentliche Funktion ist die „Vermittlung“, oder anders gesagt, die Kenntnis der verschiedenen Netze und der Wege zu diesen Netzen. Im Gegensatz zu einem Switch, der nur Interfaces mit gleichen Übertragungsprotokollen besitzt, kann ein Router unterschiedliche Interfaces (z.B. ISDN, ATM, PPP, HDLC, WLAN) aufweisen.

Im Wesentlichen werden folgende Routertypen unterschieden:

- ✓ Einzelprotokoll-Router
- ✓ Multiprotokoll-Router

Einzelprotokoll-Router

Das wichtigste Merkmal bei Einzelprotokoll-Routern ist, dass sie für eine Verbindung zwischen zwei Netzwerken lediglich ein einzelnes Netzwerk-Protokoll verwenden können. In den meisten Fällen werden Einzelprotokoll-Router dazu verwendet, Netzwerke untereinander (LAN-LAN-Verbindung) oder Netzwerke in einem Weltverkehrsnetz (WAN-WAN-Verbindung) zu verbinden.

Multiprotokoll-Router (MPR)

Multiprotokoll-Router sind in der Lage, Netzwerke über unterschiedliche Protokolle zu verbinden. Werden in einem Netzwerk beispielsweise Protokolle wie TCP/IP und TCP/IPv6 verwendet, dann existiert für jedes dieser Protokolle ein eigener Protokoll-Stack im Router. Über diese Protokoll-Stacks, die in einem Router implementiert sind, werden verschiedene logische Netzwerke jeweils untereinander verbunden. In der Praxis werden fast ausschließlich Multiprotokoll-Router genutzt.

Folgende Kriterien sollten Sie beachten, wenn Sie für Ihr Unternehmen einen Router einsetzen wollen:

- ✓ Ist der Router 19"-einbaufähig oder kann der Router auf einen Fachboden gestellt werden?
- ✓ Für welche Netzwerkprotokolle soll der Router geeignet sein?
- ✓ Sollen Zweigstellen an das Unternehmensnetzwerk angebunden werden?
- ✓ Ist eine spätere Erweiterung des Unternehmensnetzwerkes erforderlich (modulare Router)?
- ✓ Sollen die Verbindungen gesichert aufgebaut werden (VPN)?
- ✓ Ist eine integrierte Firewall-Funktionalität vorgesehen?

Je nach Leistung und Performance lassen sich Router auch noch in verschiedene Klassen einteilen:

- ✓ Höchstleistungsrouter
- ✓ Enterprise-Router
- ✓ SoHo-Router
- ✓ Gigabit-Router
- ✓ Access-Router

Während Höchstleistungsrouter, Gigabit-Router und Enterprise-Router nur in großen und hoch performanten Netzwerken eingesetzt werden, sind Access-Router und SoHo-Router (Small Office/HomeOffice) für Netzwerke mittlerer Größe konzipiert. Mit SoHo-Routern werden meist Internetzugänge oder die Anbindung von Zweigstellen realisiert. Access-Router dienen als zentrale Schaltstelle in einer Hauptverwaltung, über welche dann die Zweigstellen miteinander verbunden sind. Diese Arten von Routern sind modular aufgebaut und können je nach Bedarf mit den entsprechenden Modulen bestückt sein (seriell, ISDN, S₂M, xDSL, Gigabit-Ethernet).

Multilayer Switch (MLS)

Ein **Multilayer Switch** (auch als Layer3 oder L3-Switch bezeichnet) ist eine Netzwerkkomponente, die neben dem Switching (Layer 2) auch das Routing (Layer 3) beherrscht. Es gibt jedoch Unterschiede zu einem klassischen Router. Während ein Router über verschiedene Interfacemodule verfügt, besitzt der MLS nur Portmodule eines Typs (z. B. Fast-Ethernet, Gigabit-Ethernet, ...). Des Weiteren nutzt ein Router LAN- und WAN-Protokolle, während ein MLS vorrangig nur LAN-Protokolle verwendet.

Gateway

Bei einem **Gateway** handelt es sich um ein System, bei dem verschiedene Netze miteinander verbunden werden oder an andere Netze durch Protokollumsetzung angeschlossen sind. Zu diesem Zweck werden Daten von einem Gateway neu gepackt, damit sie den Anforderungen des Zielsystems entsprechen. Ein Gateway kann dementsprechend auch als eine Art Protokollkonverter verstanden werden.

Ein Gateway arbeitet gemäß dem OSI-Schichtenmodell auf der Anwendungsschicht (Schicht 7). Das Gerät versteht die umzusetzenden Protokolle vollständig und ist in den angrenzenden Netzwerken ein adressierbarer Netzknoten. Bei der Umsetzung der entsprechenden Netzwerkprotokolle werden alle Informationen des Datenpaketes wie beispielsweise Ziel- und Quelladresse an das jeweilige Format des remote (engl. abgelegen) befindlichen Netzwerkes angepasst. Neben der reinen inhaltlichen Anpassung von Datenpaketen erfolgen auch die Umsetzung der Flusskontrolle und die Anpassung an die Übertragungsgeschwindigkeit im anderen Netzwerk. Der einzige Nachteil bei der Verwendung eines Gateways ist, dass dieses System nur ein Applikationsprotokoll umsetzen kann. In einem heterogenen Netzwerk mit einer Vielzahl an Protokollen ist aus diesem Grund eine entsprechende Anzahl an Gateways erforderlich. Damit erhöht sich, in einem großen Netzwerk, auch der administrative Aufwand.

Da die Funktion von Gateways auf eine spezielle Applikation zugeschnitten ist, werden Gateways häufig nach dem Namen ihrer Aufgabe bezeichnet. Beispielsweise versteht man unter einem http-Gateway einen Proxy, der als Vermittler auf der einen Seite http-Anfragen entgegennimmt, um dann über seine eigene Adresse eine http-Verbindung zur anderen Seite herzustellen. Dabei ist der Proxy in der Lage, die Kommunikation auf Applikations-ebene selbst zu führen und zu beeinflussen.

Medienkonverter

Medienkonverter verbinden zwei **unterschiedliche** physikalische Medien miteinander. Es können beispielsweise Twisted Pair mit Twisted Pair oder Glasfaser verbunden werden. Ein Medienkonverter hat zwei medienabhängige Interfaces für die Standardkabel, die in lokalen Netzwerken verwendet werden. Medienkonverter werden dazu eingesetzt, Längenrestriktionen der Medien zu überbrücken. Sie können z. B. einen Medienkonverter (Twisted Pair nach Glasfaser) verwenden, wenn Sie in Ihrem Unternehmen eine abgesetzte Arbeitsstation an Ihr Netzwerk anbinden möchten.



Medienkonverter mit RJ-45- und LWL-Verbindung

Medienkonverter wandeln elektrische Signale von einem Medientyp in entsprechende Signale des anderen Medientyps um. Hierfür besitzen Medienkonverter die entsprechenden Interface-Bausteine, welche für die Kabelgeometrie benötigt werden. Im Falle einer Umsetzung von beispielsweise Kupfer auf Glasfaser werden beim Sender elektrische Signale in optische Signale umgewandelt und auf der Empfängerseite optische Signale wieder in elektrische Signale transformiert. Medienkonverter sind protokolltransparent und arbeiten auf der physikalischen Schicht (Bitübertragungsschicht) des OSI-Referenzmodells.

Beim Einsatz von Medienkonvertern sollten Sie folgendes beachten:

- ✓ Die Umsetzung ist hauptsächlich zwischen zwei verschiedenen Medien gedacht (Twisted Pair nach LWL oder umgekehrt). Es gibt aber auch Modelle für die Umsetzung von LWL-Multimode- nach LWL-Singlemodefasern.
- ✓ Medienkonverter haben fest eingestellte Übertragungsrichtungen (Halbduplex oder Vollduplex).
- ✓ Bei Medienkonvertern ist das Steckerinterface für Glasfasern (LC, SC, ST ...) vorab zu bestimmen.
- ✓ Verschiedene Medienkonverter haben auch einen Auto-Crossing-Port auf der Twisted-Pair-Seite.

Varianten

Medienkonverter unterscheiden sich hauptsächlich in den Netzarten und Protokollen, die sie unterstützen:

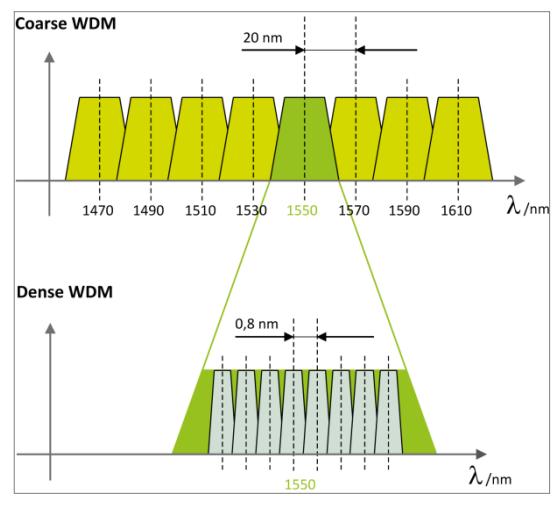
- | | |
|--|---|
| <ul style="list-style-type: none"> ✓ Ethernet, Fast-Ethernet, Gigabit-Ethernet, 10-Gigabit-Ethernet ✓ Serielle Protokolle wie RS-232, RS-422, RS-485 | <ul style="list-style-type: none"> ✓ G.703 ✓ Videosignale |
|--|---|

Optische Multiplexer

Damit die Übertragungskapazitäten bestehender optischer Netze noch effizienter genutzt werden können, werden sogenannte optische Multiplexer eingesetzt. Bei optischen Multiplexern wird die Information auf unterschiedlichen Wellenlängen übertragen (Wavelength Division Multiplexing). Zu diesem Zweck werden Komponenten verwendet, welche eine oder mehrere Wellenlängen gezielt aus dem Datenstrom trennen oder hinzufügen können. Diese Komponenten sind auch bekannt unter dem Namen Add/Drop Multiplexer. Optische Multiplexer arbeiten auf der Schicht 1 des ISO/OSI-Modells und übertragen die Daten protokolltransparent.

CWDM – Coarse Wavelength Division Multiplexing (ITU G.694.2)

Bei diesem Verfahren ist der Abstand der einzelnen Wellenlängen zu dem jeweiligen Nachbarkanal um ein Vielfaches größer. Die Übertragung erfolgt in 18 genormten Kanälen mit Wellenlängen zwischen 1.271 nm und 1.611 nm für Singlemodefasern. Die einzelnen Kanäle haben einen Kanalabstand von 20 nm zueinander. Auf jedem der einzelnen Kanäle erfolgt eine Übertragung bis zu 2,5 Gbit/s. Somit lassen sich beispielsweise mit einem 8-Kanalsystem Bandbreiten bis zu 20 Gbit/s erreichen.



DWDM – Dense Wavelength Division Multiplexing (ITU G.694.1)

Bei einem DWDM-System sind im Gegensatz zu einem CWDM die Kanalabstände nur 0,2 nm, 0,4 nm oder 0,8 nm. Dies hat zwar den Vorteil, dass sich die Anzahl der übertragbaren Bandbreite wesentlich erhöht, jedoch werden bei so einem System höhere Anforderungen an die erforderlichen elektrischen und optischen Bauelemente gestellt. Besonders der Sende-Laser ist bei diesen Systemen ein kritischer Faktor. Der Gewinn der Bandbreite spiegelt sich aber in den Anschaffungskosten solcher Systeme wieder. Im Vergleich zu einem CWDM-System sind DWDM-Systeme bis um ein Fünffaches teurer.

Topologie

Optische Multiplexer werden in folgenden Topologien verwendet:

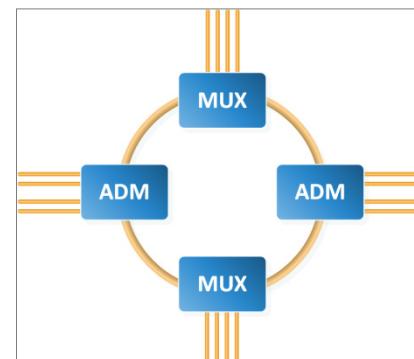
- ✓ Punkt-zu-Punkt-Topologie
- ✓ Ring-Topologie
- ✓ Linear-Add-Drop-Topologie

Punkt-zu-Punkt-Topologie

Die Punkt-zu-Punkt-Topologie ist der Standardanwendungsfall für den Einsatz optischer Multiplexer. Hierbei werden die Datenkanäle parallel zwischen den Standorten übertragen. An jedem Standort werden entsprechende Multiplexer sowie Demultiplexer eingesetzt, damit die Kanäle optisch zusammengeführt bzw. wieder getrennt werden.

Ring-Topologie

Die Ring-Topologie findet gerade im Telekom-Bereich ihren Einsatz, da aufgrund der Ringstruktur eine hohe Ausfallsicherheit gewährleistet ist. Im Falle einer Unterbrechung des Rings kann die Übertragung zwischen den restlichen Knoten weiterhin aufrechterhalten bleiben. Damit die einzelnen Knoten im Ring erreicht werden, ist es erforderlich, alle Knoten mit Add-Drop-Multiplexern auszustatten.



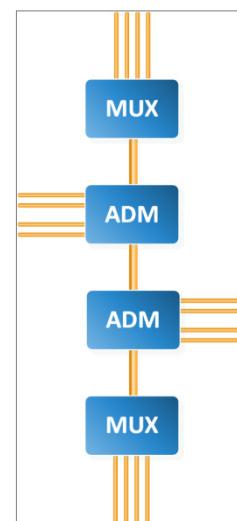
Ring-Topologie

Lineare Add-Drop-Topologie

Bei der Linear-Add-Drop-Topologie handelt es sich im Wesentlichen um eine erweiterte Punkt-zu-Punkt-Topologie. Hierbei werden zwischen den jeweiligen Endknoten noch weitere, zusätzliche Add-Drop-Multiplexer eingefügt. An den Endpunkten werden, wie bei der Punkt-zu-Punkt-Topologie, Multiplexer und Demultiplexer verwendet.

Einsatzbereiche

Aufgrund der attraktiven Anschaffungskosten sind optische Multiplexer mit CWDM-Technologie gerade auch für private Netzwerke mittlerer Größe eine echte Alternative. Aber auch wenn es darum geht, kosteneffiziente Lösungen mit hohen Bandbreiten zur Standortanbindung zu realisieren, können solche optischen Punkt-zu-Punkt-Verbindungen eine Lösung bieten.



Lineare Add-Drop-Topologie

Netzwerkkarten

Network interface card (NIC) sind Einsteckkarten für Bussysteme, wie sie beispielsweise in PCs verwendet werden. Netzwerkadapterkarten bilden die physikalische Schnittstelle zu einem Netzwerk. Zum Anschluss an das jeweilige physikalische Übertragungsmedium besitzen die Netzwerkkarten entsprechende Buchsen. Bei Ethernet-Netzwerkkarten sind u. a. folgende Anschlüsse verfügbar:

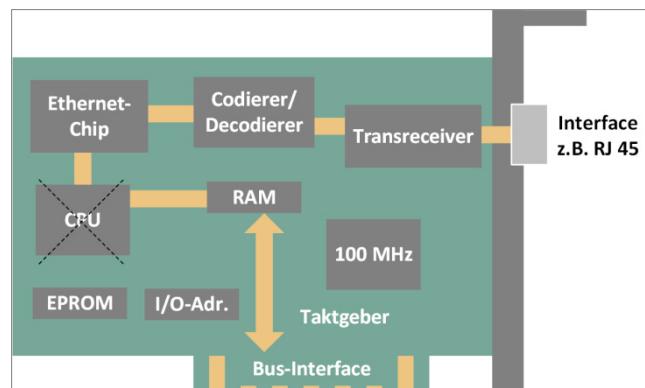
- ✓ RJ-45-Buchse
- ✓ Antennenanschluss für ein Wireless-Netzwerk
- ✓ SC/LC/MTRJ-Anschluss für Glasfaser (100BaseFX oder 1000Base-SX/LX/LH, ...)
- ✓ SFP/SFP+-Anschluss
- ✓ GG45/ARJ45-Konector
- ✓ TERA-Buchse



NIC mit RJ-45- bzw. Antennenanschluss;
Quelle: D-Link

Funktionseinheiten von Netzwerkkarten

Mithilfe von Netzwerkkarten (Network Interface Card, NIC) sind Computer in der Lage, über das entsprechende Medium mit anderen Systemen in einem Netzwerk zu kommunizieren. Sie bilden die Schnittstelle zwischen einem Endsystem und dem Übertragungsmedium (Kupfer, Glasfaser, Funk). Aktuelle Mainboards haben die NIC als Chip integriert.



Funktionsgruppen einer NIC

Leistungsmerkmale von Netzwerkkarten

Im Enduserbereich werden vorrangig folgende Leistungsmerkmale genutzt:

- ✓ Dual-Speed (10/100 Mbit/s) oder Triple-Speed (10/100/1000 Mbit/s) mit RJ-45-Anschluss
- ✓ Auto MDI-I/MDI-X (die Fähigkeit, ein angeschlossenes Kabel als Cross-over-Kabel oder Patchkabel zu erkennen und den Port automatisch darauf einzustellen)
- ✓ VLAN Tagging

Im Serverbereich kommen zusätzliche nachfolgende Merkmale zum Einsatz:

- ✓ 10 Gbit/s über TP-Kabel (Cat 6/7/8) oder LWL
- ✓ 40 Gbit/s, vorwiegend über LWL (Multimode oder Singlemode)
- ✓ 100 Gbit/s, primär über LWL (Multimode oder Singlemode)
- ✓ Dual-Port- bzw. Quad-Port-Netzwerkkarten (Erhöhung der Bandbreite durch Bündelung der Ports)

Betriebsart Promiscuous Mode

Grundsätzlich werden von Netzwerkkarten neben Broadcast- und Multicastadressen nur Datenframes akzeptiert, welche an die entsprechende Hardwareadresse (MAC-Adresse) der Karte adressiert sind. Die empfangenen Datenframes werden dann über das physikalische Interface an die nächsthöhere Schicht weitergeleitet. Manche Netzwerkkarten sind jedoch auch in der Lage, alle anliegenden Datenframes auf einem Netzwerk zu lesen und an die darüber liegenden Schichten weiterzuleiten. Diese Betriebsart wird „Promiscuous Mode“ genannt. Der Promiscuous Mode wird überwiegend von der Netzwerkanalyse-Software und anderen Überwachungstools für die Protokollierung der Datenpakete im Netzwerk benutzt.

Auto Negotiation

Die automatische Verhandlung der Übertragungsgeschwindigkeit (engl. auto negotiation) ist im Standard IEEE 802.3 für Ethernet definiert. Dieser Vorgang spielt sich beim Verbindungsaufbau in wenigen Millisekunden ab. Bei der Auto Negotiation handeln zwei Geräte in einem Netzwerk automatisch die beste mögliche Übertragungsgeschwindigkeit aus. Die Reihenfolge bei einer automatischen Geschwindigkeitsauswahl bei einer Triple-Speed-Netzwerkkarte ist wie folgt:

- | | | |
|--------------------------|-------------------------|-----------------------|
| ✓ 1000BASE-TX Vollduplex | ✓ 100BASE-TX Vollduplex | ✓ 10BASE-T Vollduplex |
| ✓ 1000BASE-TX Halbduplex | ✓ 100BASE-TX Halbduplex | ✓ 10BASE-T Halbduplex |

Gigabit-Ethernet für Kupfer

Der große Vorteil von Gigabit-Ethernet gegenüber Kupferkabeln ist, dass es bei älteren strukturierten Verkabelungen der Kategorie 5 verwendet werden kann. Bei den verlegten Kupferkabeln ist jedoch darauf zu achten, dass eine Übertragung beim 1000Base-T Standard über alle vier Adernpaare erfolgt. Die Gigabit-Ethernet-Karten sind abwärtskompatibel zu den Fast-Ethernet-Karten mit 10/100 Mbit/s und unterstützen Auto Negotiation.

Die Datenrate von 1 Gbit/s wird durch die gleichzeitige Übertragung von je 250 Mbit/s je Adernpaar erzielt. Bei vier Adernpaaren ergibt dies in der Summe 1 Gbit/s. Hierbei erfolgt die Übertragung, ähnlich wie bei 100 Mbit/s, bei einer Frequenz von 125 MHz. Es wird jedoch anders als bei 100 Mbit/s ein besseres Codierungs- und Decodierungsverfahren verwendet. Im Vergleich zu 100 Mbit/s – hier wird ein 1-Bit-Symbol bei 125 MHz übertragen (=125 Mbit/s) – werden bei 1 Gbit/s je 2 Bits bei 125 MHz (250 Mbit/s) übertragen. Aufgrund des verwendeten Codierungsverfahrens bei 100 Mbit (4B5B-Code) ergeben sich bei einer Frequenz von 125 MHz 100 Mbit/s als Datenrate.

Alternative Netzwerkkarte

Gigabit Bridging Einbau-Konverter

Als Alternative zum Einbau einer Glasfasernetzwerkkarte ermöglicht ein Gigabit- Bridging-Einbau-Konverter einen einfachen und schnellen Anschluss von PCs, Industrie PCs und Thin Clients an Glasfasernetze.

Der Einbau-Konverter wird direkt in einem PCI-Erweiterungsslot montiert und über ein kurzes Twisted Pair-Kabel mit dem vorhandenen On-Board-Netzwerkanschluss des Rechners verbunden.



PC-interner Gigabit-Ethernet Bridging Konverter

Im Gegensatz zum Einbau von Netzwerkkarten müssen dazu weder Treiber installiert noch Softwaresysteme neu konfiguriert werden. Die Montage erfolgt rein mechanisch. Diese „sanfte“ Migration auf Glasfaser bis zum Endgerät spart insbesondere bei der Umrüstung großer Netze viel Zeit.

3.4 Übung

Fragen zu Komponenten

Übungsdatei: --

Ergebnisdatei: uebung03.pdf

1. Ordnen Sie die Komponenten den Schichten des OSI-Referenzmodells zu:

Komponente	OSI-Schicht				
	Layer 1	Layer 2	Layer 3	Layer 4-7	
Medienkonverter					
Hub					
Bridge					
Access-Point					
Multilayerswitch					
Router					
Firewall (Paketfilter)					
VoIP-Telefon					
Server					
Tablet-PC					
Netzwerkkarte					
LWL-Kabel					
RJ-45-Stecker					

4 Unterbringung und Absicherung von Netzwerkelementen

In diesem Kapitel erfahren Sie

- ✓ welche passiven Komponenten verfügbar sind
- ✓ welche Komponenten für Ihr Unternehmen sinnvoll sind
- ✓ welche passiven Geräte Sie verwenden können

Voraussetzungen

- ✓ Technisches Verständnis
- ✓ Wissen über Netzwerk-Topologien

4.1 Passive Geräte für Netzwerke

Computernetzwerke bestehen grundsätzlich aus passiven und aktiven Komponenten. **Passive Komponenten** sind Geräte, die keine eigene Stromversorgung besitzen und nicht unmittelbar mit dem Datenverkehr eines Netzwerks zu tun haben. Sie stellen lediglich eine Voraussetzung für den Datenverkehr dar. Vergleichsweise ist eine Straße mit einer Kreuzung die passive Komponente. Die Ampel übernimmt die Rolle der aktiven Komponente. Die Straße ist die Voraussetzung, damit der Verkehr „fließen“ kann. Die Ampel „regelt“ den Verkehr.

Passive Komponenten:

- | | |
|--------------|------------------|
| ✓ Datenkabel | ✓ Schränke |
| ✓ Datendosen | ✓ Anschlusskabel |
| ✓ Patchpanel | |

Aktive Komponenten hingegen regeln unmittelbar den Datentransport zwischen den Endgeräten und besitzen, sofern sie nicht über PoE (Power over Ethernet) versorgt werden, eine eigene Stromversorgung. Sie steuern/ modifizieren den Datentransfer zwischen den verschiedenen Segmenten eines lokalen oder Weitverkehrsnetzes. Mit aktiven Komponenten werden Netzwerke strukturiert, der Verkehr reglementiert und die Wege optimiert.

Aktive Komponenten:

- | | |
|-----------------------------|----------------------------|
| ✓ Computer, Server | ✓ Switche, Access-Points |
| ✓ Storagesysteme (SAN, NAS) | ✓ Netzwerkkarten |
| ✓ Gateways, Proxies | ✓ Medienkonverter/Repeater |
| ✓ Router, Multilayerswitche | ✓ Firewall |

4.2 Server- und Netzwerkschränke

Server- und Netzwerkschränke sind der Grundstein zur Aufnahme von passiven und aktiven Komponenten. Patchpanel, Router, Switch und Server werden in Server- und Netzwerkschränken nicht nur vor äußeren Einflüssen wie Verschmutzung geschützt, sondern auch vor unbefugtem Zugriff. Sie erhalten Server- und Netzwerkschränke in den verschiedensten Ausführungen. Grundsätzlich wird zwischen Wandschrank und Standschrank unterschieden. Es gibt Serverschränke, aktive Netzwerkschränke und passive Netzwerkschränke. Diese Ausführungen gibt es mit unterschiedlichen Abmessungen in Höhe, Breite und Tiefe. Bereits bei der Planung eines Netzwerks sollte die Auswahl des richtigen Server- und Netzwerkschranks erfolgen. Die Abmessungen der Komponenten, welche darin untergebracht werden, sollten bereits zu diesem Zeitpunkt bekannt sein. Berücksichtigen Sie auch zusätzliche Reserven für eventuelle spätere Erweiterungen.



*Knürr DCM®
Serverschrank*



*Knürr Miracel®
Netzwerkschrank*



*Knürr ConAct®
Wandgehäuse*

Server- und Netzwerkschränke gibt es in unterschiedlichen Abmessungen:

- ✓ Serverschränke haben meist eine Tiefe von 1000 bis 1200 mm, eine Breite von 600 bis 800 mm und eine Höhe von 2000 oder 2200 mm.
- ✓ Aktive Netzwerkschränke haben meist eine Tiefe von 1000 bis 1200 mm, eine Breite von 800 mm und eine Höhe von 2000 oder 2200 mm.
- ✓ Passive Netzwerkschränke haben meist eine Tiefe von 800 bis 1000, eine Breite von 800 mm und eine Höhe von 2000 oder 2200 mm. Bei passiven Netzwerkschränken wird oft ein Sockel mit meist 100 oder 200 mm Höhe verwendet.

Wandschränke bzw. Wandgehäuse werden hauptsächlich als passive Netzwerkschränke verwendet und haben kleinere Abmessungen.

Im Inneren des Schranks befinden sich zwei oder vier Profilschienen zur Aufnahme der 19"-Komponenten. 19 Zoll (19") stellt eine genormte (IEC 297 und DIN 41494) Einbaubreite von 482,6 mm dar. In Serverschränken und aktiven Netzwerkschränken werden immer vier Stück 19"-Profilschienen benötigt (zwei vorne und zwei hinten) und in passiven Netzwerkschränken reichen oft auch zwei 19"-Profilschienen vorne. Die Höhe der aktiven und passiven 19"-Komponenten wird in sogenannten Höheneinheiten (HE) angegeben. 1 HE entspricht einer Höhe von 44,45 mm. Die Höheneinheiten liegen bei Schränken zwischen 24 und 47 HE und bei Wandgehäusen zwischen 9 und 24 HE. Die Profilschienen eines 2000 mm hohen Schranks haben zum Beispiel 41 oder 42 HE.

Aufbau eines Schrankgrundgerüsts

Ein Server- oder Netzwerkschrank besteht meist aus einem Grundgestell, 19"-Profil-schienen, Seitenteilen, einer Front- und Rücktür, einem Deckel und in einigen Fällen einem Boden.

Serverschränke und aktive Netzwerkschränke haben zur **Kühlung** der aktiven Komponenten meist perforierte Front- und Rücktüren. Passive Netzwerkschränke sind meist mit einer Glastür vorne und einer Blechtür hinten ausgestattet. Werden in passiven Netzwerkschränken aktive Komponenten eingebaut, so werden diese meist mit Dachlüftern oder einem Schrankklimagerät gekühlt.



Schrankgrundgestell

Die Datenkabel können wahlweise durch das Dach oder den Bodenbereich (häufig aus dem Doppelboden) in den Server- oder Netzwerkschrank eingeführt werden. Bei der **Verkabelung** eines Schranks sollte darauf geachtet werden, dass die Datenkabel genügend „Reserve“ für eventuelle spätere Änderungen enthalten. Diese Reserve lässt sich im Sockel oder im Doppelboden eines Schrankes verstauen. Gerade bei Glasfaserkabeln ist eine korrekte Verlegung erforderlich, denn der minimale Biegeradius darf keinesfalls unterschritten werden. Des Weiteren kann in den Schrank eine Beleuchtung eingebaut werden, die sich automatisch beim Öffnen einschaltet.

Zubehör für Server- und Netzwerkschränke

- ✓ Fachboden fest oder ausziehbar und Schubfächer
- ✓ Einschub- und Teleskopschienen
- ✓ Blindplatten in verschiedenen Größen (1 HE, 2 HE etc.)
- ✓ Kabelführungsplatten
- ✓ Kabelrangierbügel nach Bedarf
- ✓ ggf. Kabdurchführungsplatten, falls Kabel zur Front des Schranks geführt werden müssen
- ✓ Lüftereinheiten/Klimagerät
- ✓ Stromverteilungsleisten
- ✓ Schranküberwachungssysteme
- ✓ Beleuchtung
- ✓ Tastaturschublade
- ✓ u. A.



Kabelführungsplatte



Lüftereinheit



Kabelmanagement

4.3 Schrank-Kontroll-Systeme

Überwachung von Schränken

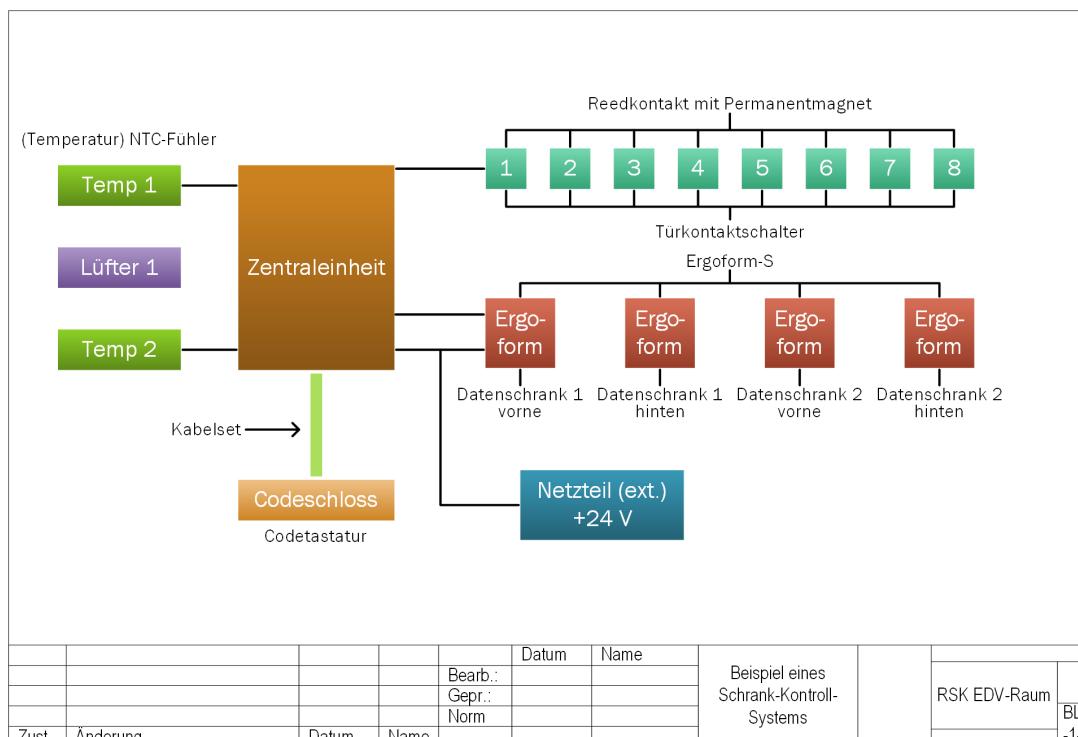
Die Überwachung von Schränken und Rechenzentren ist essentiell für einen störungsfreien Betrieb und wird durch verschiedene Systeme gewährleistet. Als besonders kritische Parameter in Rechenzentren gelten die **Temperatur** und der **Energieverbrauch**.

In den letzten Jahren haben sich die Monitoringfunktionen von Servern und Netzwerkswitchen erheblich verbessert. Darüber hinaus liefern intelligente Stromverteilungssysteme Informationen über Spannung, Strom, die zu entwärmende Verlustleistung sowie häufig auch Umweltparameter.

Je nach Anwendungsfall werden zusätzliche Informationen benötigt:

- ✓ Temperatur
- ✓ Rauch, auch neben einem immer zu installierenden professionellen Feuermeldesystem
- ✓ Feuchtigkeit
- ✓ Erschütterungen
- ✓ Zugang
- ✓ Bewegung

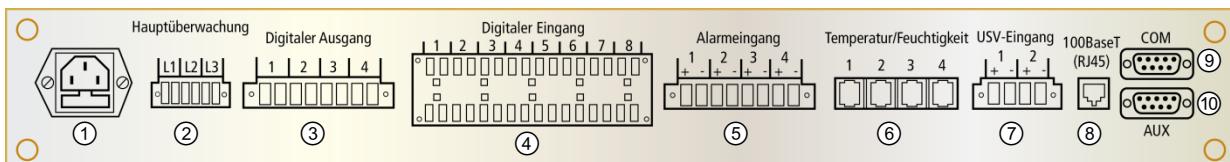
Diese Umgebungsvariablen werden über eine entsprechende Schnittstelle an eine Überwachungseinheit weitergeleitet und ausgewertet. Je nach Ereignis werden die zugehörigen Funktionen oder Alarmierungen ausgelöst. Aktuelle Überwachungssysteme ermöglichen zudem eine Anpassung der Funktionalität hinsichtlich Alarmierung und wichtiger Alarmkonsolidierung.



Anschlussbeispiel eines Schrank-Kontroll-Systems

Zentraleinheit

Die Basis eines Schrank-Kontroll-Systems ist eine mikroprozessorgesteuerte Überwachungseinheit. Diese Zentraleinheit wird in einem 19"-Metallgehäuse im dafür vorgesehenen Daten- oder Serverschrank montiert. Bei Schränken mit Glastür kann der Betriebsstatus des Überwachungssystems über den Zustand von LEDs oder über ein LC-Display abgelesen werden. Die Grundeinheit verfügt über eine entsprechende Anzahl von Eingängen. An diese werden dann die entsprechenden Sensoren und die zu überwachenden Geräte angeschlossen.



Rückansicht einer Zentraleinheit

- ① Netzzschluss für Versorgungsspannung (50/60 Hz)
- ② Steckerleiste zur Überwachung der drei Phasen
- ③ Vier digitale Schaltausgänge (potentialfrei)
- ④ Digitale Eingänge (potentialfrei) und 12 V DC-Ausgänge zur Spannungsversorgung für externe Sensorik
- ⑤ Vier Alarmlinien (z. B. Rauchmelder, Erschütterungssensor)
- ⑥ Vier Anschlüsse für Temperatur- und Feuchtigkeitssensor oder kombinierten Feuchtigkeits-/Temperatursensor
- ⑦ Steckerleiste (4-polig) für zwei Eingänge USV (Unterbrechungslose Stromversorgung)
- ⑧ 100BaseT-Ethernet
- ⑨ Serielle Schnittstelle (SUB-D 9-polig) für die Konfiguration
- ⑩ Überwachung externer Geräte (z. B. USV oder Klimaanlage)

Netzwerkanschluss über RJ-45

Der ungeschirmte/geschirmte RJ-45-Eingang ist für den Anschluss der Zentraleinheit an ein Netzwerk konzipiert. Über diesen Netzwerkanschluss ist es möglich, mithilfe von gängigen Netzwerkprotokollen auf IP/IPv6-Basis von einem Managementserver bzw. Kontroll-PC über das Netzwerk auf die Zentraleinheit zuzugreifen. Als mögliche Protokolle kommen infrage:

- | | |
|--------------|--|
| ✓ Telnet/SSH | ✓ http/https |
| ✓ SNMP | ✓ ggf. proprietäre Gebäudemanagementprotokolle |

Da über ein Netzwerk mittels SNMP auf die Zentraleinheit zugegriffen werden kann, ist eine einfache Integration der Zentraleinheit in Netzwerkmanagementplattformen möglich. Somit besteht die Möglichkeit, alle Betriebszustände des Schrankes zentral zu überwachen und entsprechende Meldungen über das Managementsystem auszuwerten.

Grafische Benutzeroberflächen

Neben SNMP besteht auch die Möglichkeit, über eine grafische Benutzeroberfläche auf ein Schrank-Kontroll-System zuzugreifen. Dafür benötigen Sie nur einen Browser (beispielsweise IE, Firefox, Chrome). Über die Eingabe der IP-Adresse bzw. des Namens wird eine Verbindung zur Zentraleinheit aufgebaut. Mithilfe einer grafischen Oberfläche werden entsprechende Alarmierungen der im Netzwerk befindlichen Kontroll-Systeme unter Angabe von Uhrzeit, Datum, Adresse und Namen dokumentiert. Es können die Funktionen aller angeschlossenen Sensoren ausgewertet und verschiedene Informationen grafisch dargestellt werden. Die wesentlichen Funktionen solcher grafischen Tools sind:

- ✓ Die Temperaturwerte können grafisch angezeigt werden
- ✓ Alle analogen Eingabewerte können unterschiedlich grafisch animiert werden
- ✓ Es können alle Sollwerte direkt verändert werden
- ✓ Entsprechende Textwerte können beliebig verändert werden

Einige Systeme bieten die lokale Speicherung von Messwerten und -verläufen an. Angesichts der immer leistungsfähigeren Managementsoftware-Tools wird diese Funktion zunehmend auf die Managementserver ausgelagert. Die Bedienung der grafischen Benutzeroberflächen ist herstellerabhängig.

Updatefähige Systemsoftware

Änderungen der Systemsoftware, welche vom Hersteller eines Schrank-Kontroll-Systems gemacht werden, können jederzeit in die Zentraleinheit eingespielt werden. Dies erfolgt entweder über die serielle Schnittstelle oder über das Netzwerk. Das Installieren neuer Systemsoftware kann auch im laufenden Betrieb der Zentraleinheit erfolgen.

Zutrittskontrolle

Für die meisten Schrank-Systeme gibt es elektronische Schließsysteme. Diese Sicherheitsgriffe haben die Aufgabe, den Daten- oder Serverschrank vor unbefugtem Öffnen zu schützen. Dies ist in vielen Fällen erforderlich, da die einzelnen Hersteller von Daten- und Serverschränken der Standardausführung keine Sicherheitsschlösser beilegen. Es werden vielmehr gängige und universell einsetzbare Schlosser verwendet, deren Schlüssel den Nachteil haben, dass sie meist nicht nur beim eigenen Daten- oder Serverschrank passen.

Schließsysteme werden in unterschiedlicher Ausprägung angeboten, teils als Zubehör zu einer Überwachungseinheit, in vielen Fällen als separate Schließanlage oder auch mit einer direkten Anbindung an bestehende Gebäudeschließsysteme. Als Identifikationsschnittstelle eignen sich u. a. RFID-Kartensysteme oder schlicht ein potentialfreier Kontakt zur Anbindung weiterer ID-Technologien.

Typischerweise werden Schließstatus und/oder Türstatus an ein Schrank-Kontroll-System für eine Rückmeldung verbunden. Somit ist es möglich, einen Status über den Zustand der Schranktür, offen oder geschlossen, zu erhalten.

Sensoren für die Überwachung

Damit das Umfeld eines Daten- und Serverschrankes überwacht werden kann, sind entsprechende Sensoren zur Messung der Umgebungsvariablen zu verwenden. Für jede Variable sind geeignete Sensoren erhältlich. Im Wesentlichen gibt es folgende Sensoren:

- | | | |
|-----------------------|--------------------|--------------------|
| ✓ Temperatursensor | ✓ Rauchmelder | ✓ Vibrationssensor |
| ✓ Feuchtigkeitssensor | ✓ Türkontaktsensor | ✓ Bewegungsmelder |

4.4 Verbinder und Anschlusskabel

Einsatzbereich von Patchkabeln

Patchkabel dienen zum Anschluss von aktiven Komponenten an passive Komponenten, zum Beispiel für den Anschluss einer Netzwerkkarte an eine Datendose. Grundsätzlich wird zwischen Kupfer- und LWL-Patchkabel unterschieden. Da diese ggf. einer mechanischen Beanspruchung unterliegen, sollte immer für ausreichenden Ersatz gesorgt werden.

TP-Patchkabel (Twisted Pair)

Patchkabel unterscheiden sich in ihren Eigenschaften kaum von fest verlegten Kabeln, sie sind allerdings in ihrem mechanischen Aufbau flexibler. Das ergibt sich aus einem geringeren Adernquerschnitt (0,42–0,48 mm) und dem elastischeren Kabelmantel. Sie sind im Datenbereich für die Kategorien 5 bis 8 genormt.

An beiden Enden des Patchkabels befindet sich bis 10-Gbit-Ethernet ein 8-poliger RJ-45-Stecker, der je nach Kabel und Kategorie geschirmt oder ungeschirmt sein kann. Als Knickschutz werden die Stecker jeweils mit einer Knickschutztülle versehen. Je nach Hersteller liegt die Lebensdauer bei etwa 750 Steckzyklen.



*Patchkabel,
CAT 6 ungeschirmt*

Kupferpatchkabel gibt es in verschiedenen Standardlängen:

- | | |
|---------|---------|
| ✓ 0,5 m | ✓ 5,0 m |
| ✓ 1,0 m | ✓ 7,5 m |
| ✓ 2,0 m | ✓ 10 m |
| ✓ 3,0 m | ✓ u. a. |

Einige Hersteller bieten Sonderlängen wie z. B. 15 m oder 20 m an. Die Länge eines Patchkabels sollte aber aufgrund der schlechteren Übertragungseigenschaft im Gegensatz zu den fest verlegten Datenkabeln 10 m nicht überschreiten.

Um in einem Netzwerkschrank ein unnötiges „Kabelchaos“ zu vermeiden, sollte die Länge der Patchkabel nicht zu groß gewählt werden, allerdings sollten sie mindestens so lang sein, dass der Patch problemlos verfolgt werden kann.

Auch bietet es sich an, die Übersichtlichkeit zu verbessern, indem farbige Patchkabel für bestimmte Bereiche oder Dienste verwendet werden. Standardmäßig sind beispielsweise folgende Farben erhältlich:

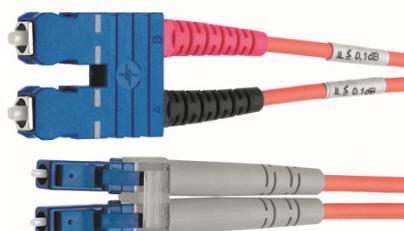
- | | | | | |
|--------|--------|--------|-------|--------|
| ✓ Grau | ✓ Gelb | ✓ Grün | ✓ Rot | ✓ Blau |
|--------|--------|--------|-------|--------|

Neben den hauptsächlich verwendeten Patchkabeln mit RJ-45 finden mitunter auch ARJ45-, GG45-, TERA-Steckerformen Anwendung.

LWL-Patchkabel

Besonders wichtig bei der Auswahl der LWL-Patchkabel ist der passende Fasertyp. Er muss dem Fasertyp des fest verlegten LWL-Kabels entsprechen. Die Steckerauswahl der LWL-Patchkabel richtet sich nach den eingesetzten aktiven (z. B. Medienkonverter) und passiven (z. B. Patchpanel) Komponenten. LWL-Patchkabel sind zur besseren Verlegung wesentlich flexibler und dadurch auch etwas empfindlicher.

Gerade deshalb sollten Sie hier auf einen sorgfältigen Umgang und besonders auf den Biegeradius achten. Die Stecker der LWL-Patchkabel sind mit Schutzkappen versehen. Diese sollten erst kurz vor dem Steckvorgang abgenommen werden, um eine unnötige Verunreinigung der Stirnfläche des Steckers zu vermeiden. Die Lebensdauer bei LC- bzw. SC-Steckern liegt bei etwa 1000 Steckzyklen.



LWL-Patchkabel Vergleich SC- mit LC-Stecker (unten)

Im LWL-Bereich werden eine Vielzahl von Steckertypen eingesetzt. Sie unterscheiden sich im Einsatzbereich und der Bauform erheblich. Hier ein kleiner Auszug:

- ✓ ST-Stecker (engl. straight tip), veraltet
- ✓ SC-Stecker (engl. subscriber connector), Standard
- ✓ FC-Stecker (engl. fiber connector), veraltet
- ✓ MTRJ-Stecker (engl. mechanical transfer), Standard
- ✓ MPO-Stecker (engl. multipath push-on), Standard
- ✓ E2000-Stecker, Standard
- ✓ F-SMA-Stecker (engl. subscriber connector), veraltet
- ✓ LC-Stecker (engl. lucent connector), Standard
- ✓ URM-Stecker (engl. yoU aRe Modular), Standard

Zur besseren Unterscheidung der angeschlossenen Fasern (Multimode/Monomode) werden LWL-Patchkabel mit farbig abgesetzten Tüllen (beige, aqua, blau, grün oder schwarz) ausgeliefert.

Kommen in einem Schrank gemischte ST- und SC-Steckersysteme zum Einsatz, bieten verschiedene Hersteller hierfür auch Adapterkabel an.

4.5 Patchpanel und Datendosen

Patchpanel für Twisted-Pair-Kabel

Patchpanel werden sowohl für Telekommunikations- als auch für Datennetze eingesetzt. Sie bilden die Schnittstelle zwischen den fest verlegten Netzwerkkabeln und den aktiven Komponenten wie Switches, Access-Points, Routern und den Endsystemen.

Die Auswahl der Patchpanel erfolgt nach den Bedürfnissen des Netzwerks. Werden in einem 10 Gbit-Netzwerk Datenkabel der Kategorie 6A eingesetzt, muss das Patchpanel mindestens der gleichen Kategorie oder höher entsprechen.

Ungeschirmte nicht modulare Patchpanel

Diese Patchpanel entsprechen der Kategorie 3 bis 6 für ungeschirmte Verbindungen und werden für Telefonverteilungen oder Datennetze eingesetzt. Sie erfüllen die Normen ISO/IEC 11801 bzw. EN50173. Dank der hohen Packungsdichte von 24, 30 oder mehr Ports (RJ-45) auf einer Höheneinheit wird eine platzsparende Installation gewährleistet (z. B. 50- oder 100-paariges Telefonkabel auf 1 HE). Der Anschluss der Kabel, bei denen der Adern durchmesser 0,6 mm nicht überschreiten sollte, erfolgt in LSA+-Technik (Löt-, schraub- und abisolierfreie Anschlusstechnik). Für die Montage werden als Zubehör Kabelbinder, Schrauben für den 19"-Einbau sowie Erdungsmaterial benötigt. Viele Patchpanel sind zur besseren Zugänglichkeit ausziehbar.

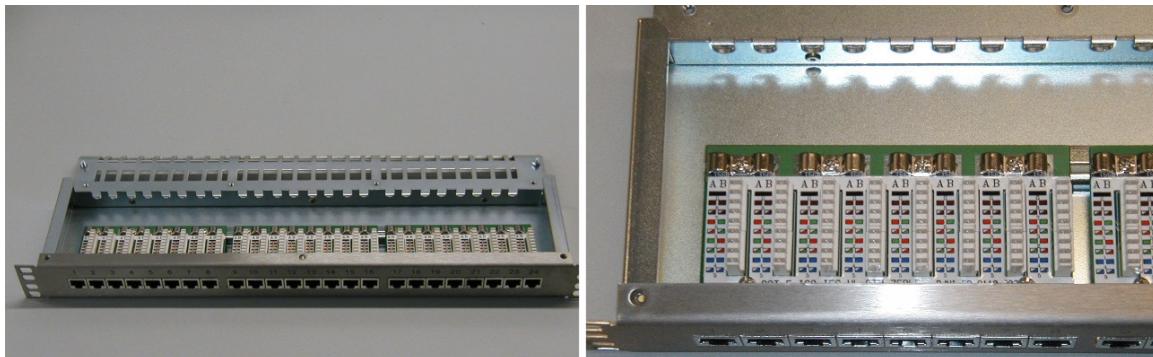


Patchpanel 28 Ports CAT 6

Geschirmte nicht modulare Patchpanel

Geschirmte Patchpanel entsprechen der Kategorie 5, 6 oder 6A (ISO/IEC 11801/EN50173). Die Auswahl der Kategorie richtet sich nach den verwendeten Datenkabeln und Datendosen. Geschirmte nicht modulare Patchpanel sind als 16- oder 24-Port-Ausführung (1 HE) erhältlich. Der Anschluss der Datenkabel erfolgt ebenfalls in LSA+-Technik, wobei für jedes Datenkabel ein eigener Schirmanschluss vorhanden ist. In jedem Fall ist die Montageanweisung des Herstellers zu beachten.

Die Ports auf der Frontseite der Patchpanels sind meist durchnummieriert oder mit Beschriftungsfeldern versehen. Für die Montage werden als Zubehör Kabelbinder, Schrauben für den 19"-Einbau sowie Erdungsmaterial benötigt. Bei diesen Patchpanels sind alle 8 Pins durchverdrahtet.



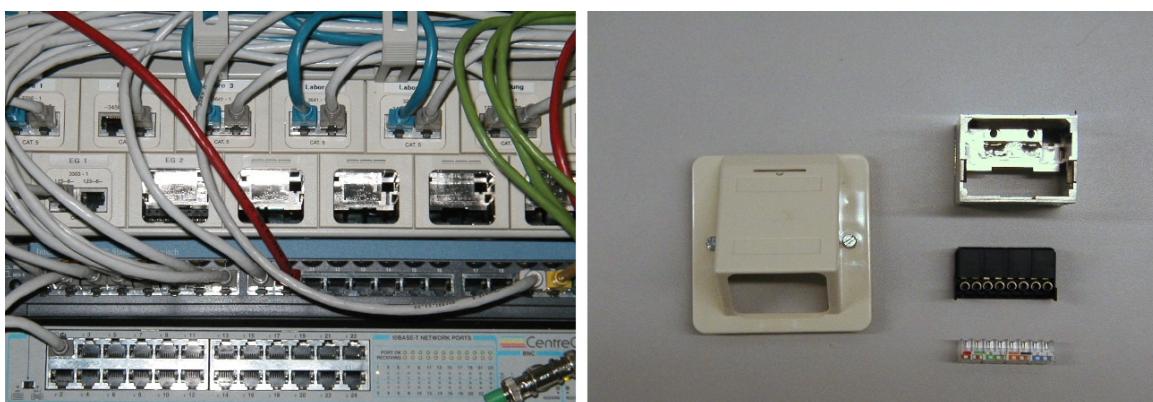
Geschirmtes nicht modulares Patchpanel mit 24 Ports, Kategorie 6

Modulare Patchpanel

Durch den Einsatz von modularen Systemen wird ein Höchstmaß an Flexibilität erreicht. Es werden alle 8 Adern fest in einem geschirmten Gehäuse mittels Crimp-Verfahren aufgelegt. Damit ist ein und dieselbe Verkabelung universell nutzbar, z. B. für:

- ✓ Anschluss analoger TK-Komponenten (1 Adernpaar wird benötigt)
- ✓ Anschluss von ISDN-Komponenten (2 Adernpaare werden benötigt)
- ✓ 10/100 Mbit-LAN (2 Adernpaare ...)
- ✓ 1 Gbit-LAN (4 Adernpaare ...)
- ✓ 10 Gbit-LAN (4 Adernpaare ...)

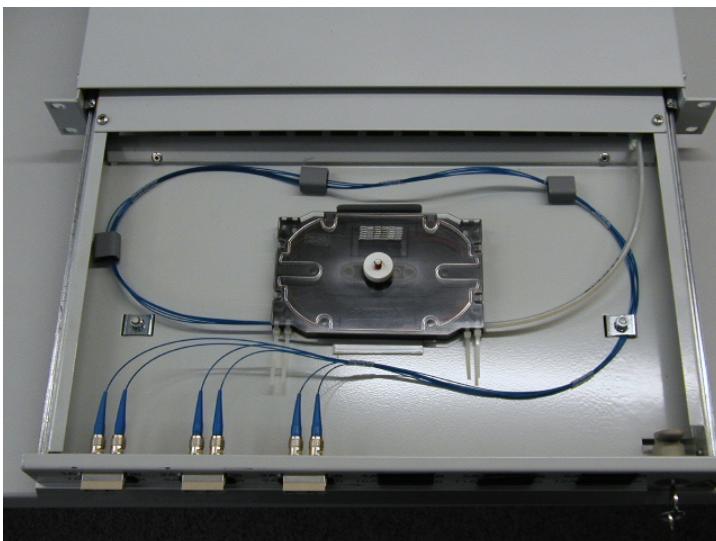
An der Frontseite des Gehäuses wird ein Einsatz mit der gewünschten Dienstkennung eingesteckt. Es ist in jedem Fall darauf zu achten, dass sowohl Patchpanel als auch Datendosen vom gleichen Hersteller eingesetzt werden. Modulare Patchpanel gibt es mit 16, 24 und 32 Einsatz-Ports (2 HE bzw. 3 HE).



Modulare Patchpanel, daneben Gehäuse und Einsatz

LWL-Patchpanel

LWL-Patchpanel eignen sich zur Aufteilung mehradriger LWL-Kabel auf Einzeladern, entweder als Verteilerrahmen oder mit geschlossenem Gehäuse zur Aufnahme von Spleißkassetten. Sie sind in Größen von 1 HE bis 4 HE erhältlich. LWL-Patchpanel mit 1 HE können 6, 12 oder 16- Duplex-Kupplungen aufnehmen, je nach Steckeranforderung (LC, SC, E2000 ...). Einige Hersteller bieten Patchpanel mit 24- Kupplungen auf 1 HE an. Die LWL-Kabel werden an der Rückseite des Panels durch eine PG16-Verschraubung eingeführt und zugentlastet. Im Inneren befinden sich Halterungen zur Aufnahme von Spleißkassetten und zur sauberen Faserführung. Je nach Ausführung bieten manche Patchpanels eine ausziehbare Schublade für einen komfortablen Zugang zur Spleißablage.



LWL-Patchpanel offen, 1 HE, 12 ST-Kupplungen, mit Spleißkassette

Wie bei den Kupfer-Patchpanels gibt es auch im LWL-Bereich modulare Systeme. Solche modularen LWL-Patchpanels haben meist 4 HE und können mit Teilfrontplatten oder 19"-Frontplatten für bis zu 96 Kupplungen bestückt werden. Durch den Einsatz von Teilfrontplatten können z. B. LC- und SC-Stecksysteme kombiniert werden.

Datendosen für Kupferverkabelung

Datendosen für Kupferverkabelung bestehen aus einem vollgeschirmten Gehäuse, in dem sich die LSA+- Anschlussleisten befinden. Das Schirmgeflecht des Datenkabels wird meist durch eine Klemmtechnik mit dem Gehäuse verbunden. Solche Datendosen müssen der Kategorie der verwendeten Datenkabel entsprechen, wie der Kategorie 5, 6 oder 7. Je nach Installationsbedarf gibt es Datendosen zur Auf- oder Unterputzmontage mit verschiedenen Abdeckungen (cremeweiß, reinweiß, grau etc.). Wahlweise haben Datendosen einen oder zwei RJ-45-Ports, die jeweils 8-polig beschaltet sind. Je nach Einsatzgebiet sollten Datendosen mit Schrägauslass verwendet werden, bei denen die Portöffnung nach unten zeigt.

Zum einen schützt dies die eingesteckten Patchkabel vor Beschädigung, zum anderen die Ports vor Verschmutzung.



Datendose CAT 6, 2-Ports mit Schrägauslass

Bei der Montage der Datendosen ist darauf zu achten, dass die Verdrillung der Adernpaare sowie die Paarschirmung so weit wie möglich an die Anschlussleiste heranzuführen ist.

Kupfer-Datendosen für den industriellen Einsatz

Um die hohen Anforderungen bei einer verschmutzungsgefährdeten und rauen industriellen Umgebung zu erfüllen, werden entsprechende Komponenten benötigt.

Gerade im Außenbereich können herkömmliche Datendosen für die Kupfertechnik gar nicht oder nur bedingt verwendet werden. Speziell für die Industrie und den Einsatz im Außenbereich gibt es entsprechende RJ-45-Stecker und RJ-45-Anschlussdosen, welche für die sichere Übertragung von Daten geeignet sind.

Die Anwendungsbereiche dieser Industrie-Datendosen liegen sowohl im Schaltschrankbereich als auch an Arbeitsplätzen, bei denen starke Verschmutzungen beim Endgeräteanschluss auftreten. Durch ihre speziellen Eigenschaften können solche Datendosen auch an Arbeitsplätzen eingesetzt werden, an denen Spritzwasser auftritt. Sowohl die Einsätze in der Anschlussdose als auch die Steckereinsätze sind metallisch voll geschirmt.



RJ-45-Datendose für den industriellen Einsatz

Datendosen für LWL-Verkabelung

Die Vorteile eines Glasfaser-Netzwerks können nur dann voll genutzt werden, wenn LWL-Kabel bis zum Arbeitsplatz verlegt sind (fiber to the desk). Netzwerkverkabelungen mit LWL-Kabeln erfordern lösbare und robuste Steckverbindungen zwischen den LWL-Kabeln und den Teilnehmeranschlusskabeln.

Die LWL-Kupplungen müssen in einer Wandauslassdose oder einem Bodentank so montiert werden, dass die Verbindungen einfach gesteckt und gelöst werden können.

Weiterhin darf die LWL-Kabelführung den zulässigen Mindestradius von 25 mm nicht unterschreiten. Auch Ablagen für Spleiße und Reservelängen sowie Zugentlastungsmöglichkeiten spielen eine große Rolle.

Die Abbildung zeigt eine LWL-Anschlussdose für Kabelkanäle. Sie besitzt Anschlussmöglichkeiten für zwei Teilnehmer, die mit LC-, SC- oder SC-Duplex-Kupplungen bestückt werden können. Im Inneren befindet sich eine Aufwickeltrommel für die Faserreserve mit einem Wickelradius von 25 mm. Zum Schutz der LWL-Patchkabel besitzt diese Anschlussdose einen Schrägauslass in einem Winkel von 20° zur Senkrechten nach unten.



LWL-Anschlussdose, up,
Schrägauslass 20°

5 Kabelverlegung

In diesem Kapitel erfahren Sie

- ✓ wie ein Twisted-Pair-Kabel konfektioniert wird
- ✓ wie eine RJ-45-Datendose angeschlossen wird
- ✓ welche Verlegevorschriften für LWL-Kabel gelten

5.1 Stecker und Anschlusstechnik

Verbindungssystem RJ-45

Als Stecksystem für Twisted-Pair-Kabel hat sich das RJ-45-Stecksystem (IEC-60603) etabliert. Hierbei handelt es sich um ein 8-poliges Miniaturstecksystem, welches unter dem Standard TSB 40 von der EIA/TIA normiert ist (ISO/IEC DIS 11801).

Das RJ-45-Stecksystem wird für universelle Verkabelungssysteme gemäß ISO/IEC der Klassen D, E verwendet. Damit ist dieses Stecksystem für Datenraten bis 10 Gbit/s spezifiziert.

Damit die Anschlussbelegungen unterschiedlicher Hersteller einheitlich sind, wurden entsprechende Standards für die Zuordnung der Kabelfarben zu den Kontaktpins festgelegt.



Verschiedene Institutionen haben hierzu Farbcodes festgelegt. Der vorzugsweise benutzte Farbcode ist der **IEC-Farocode nach EIA**, wobei in Deutschland hauptsächlich T568B nach ANSI/TIA-568 Anwendung findet.

Adernpaar	RJ-45-Kontakt	IEC-Code T568B	IEC-Code (in Anlehnung)	REA-Code	DIN-47.100- Code
Paar 1	4 und 5	blau/weiß	weiß/blau	weiß/blau	weiß/braun
Paar 2	3 und 6	weiß/grün	rot/orange	türkis/violett	grün/gelb
Paar 3	1 und 2	weiß/orange	schwarz/grün	weiß/orange	grau/rosa
Paar 4	7 und 8	weiß/braun	gelb/braun	türkis/violett	blau/rot

Verbindungssystem GG45/GP45

GG45 (Buchse) und GP45 (Stecker) sind die Namen des neuen Stecksystems, das für die Verkabelung der Kategorie 7 entwickelt wurde. Sie wurde auch als Gigagate bezeichnet. Die GG45-Buchse ist kompatibel mit dem RJ-45-Stecker. Das Verbindungssystem entspricht der Link-Klasse 7 bis zur Link-Klasse 8.2 (bis 2000 MHz). Damit sind Datenübertragungsraten von 10 Gigabit/s über eine Distanz von 100 m bzw. 40 Gigabit/s (Link-Klasse 8.2) über eine Distanz von 30 m erreichbar.



GG45-Buchse

Durch die Abwärtskompatibilität können im Anschlussbereich weiterhin RJ-45-Patchkabel verwendet werden. Dieses Stecksystem findet vereinzelt im DataCenter- und Fibre Channel-Bereich Anwendung.

Verbindungssystem ARJ45

ARJ45 wurde parallel zu GG45 entwickelt und ist in einigen Punkten mit diesem System kompatibel. Es erfüllt die elektrischen Parameter bis zur Kategorie 8.2. Das System ARJ45 ist jedoch nicht rückwärtskompatibel.

Verbindungssystem TERA

TERA wurde in der Norm EN50173 für vollständig geschirmte Steckverbindungs-systeme der Kategorien 7 und 7A und darüber standardisiert und ist nicht kompatibel mit dem RJ-45-Standard. Es wurde als Multimedia-Steckverbinder-system für Kommunikationsnetze entwickelt und wird u. a. bei CATV (Cable TV) eingesetzt. TERA ist als ein-, zwei- und vierpaarige Variante verfügbar, d. h., unterschiedlichste Dienste können über verschiedene Adernpaare (engl. cable sharing) übertragen werden. Damit bietet das Steckersystem eine extrem hohe Flexibilität, da jedes Adernpaar einzeln gepatcht werden kann. In der aktuellen Version unterstützt das TERA-System oberhalb der Kategorie 7A Übertragungsgeschwindigkeiten von > 10 Gbit/s.



TERA-Buchse Frontansicht

5.2 Installationsbeispiel: AMJ-S-Modul (Cat 6A) konfektionieren

Werkzeug und Material

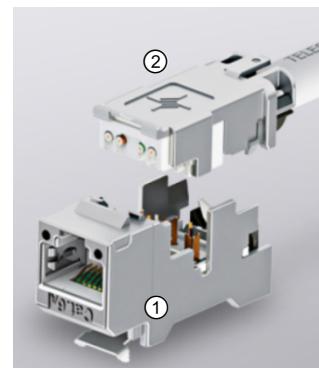
Für die Erweiterung eines bestehenden Netzwerkes werden modulare Anschlussdosen und Patchpanels verwendet. Zu diesem Zweck sollen Netzwerkkabel (Kategorie 6A) in der benötigten Länge mit Modulen konfektioniert werden. Vorteil dieser Technik ist die optimale Bauweise, das zeitsparende Konfektionieren und die geringe Fehlerquote bei der Installation.

Werkzeug

- ✓ Parallelzange für das Modul
- ✓ (Elektronik-)Seitenschneider
- ✓ Abisolierzange oder ein anderes geeignetes Werkzeug
- ✓ Schraubendreher
- ✓ Messgerät zur Verifizierung der Kabelstrecke

Material

- ✓ AMJ-S-Modul, bestehend aus Oberteil ① und Unterteil ②



AMJ-S-Modul,
Hersteller: Telegärtner

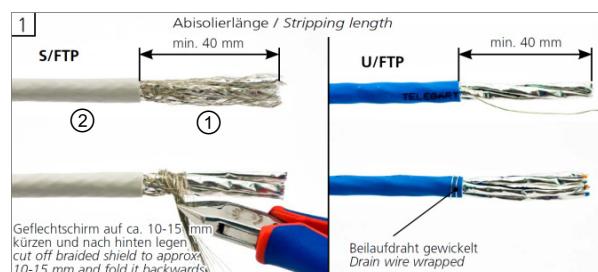
Montage des AMJ-S-Moduls

Abmanteln

- Entfernen Sie den Außenmantel ② des geschirmten bzw. ungeschirmten Twisted-Pair-Kabels mit einem Abisolierwerkzeug über eine Länge von mindestens 40 mm.

Kürzen Sie den Geflechtschirm ① auf eine Länge von ca. 15 mm und verdrehen diesen über den Außenmantel.

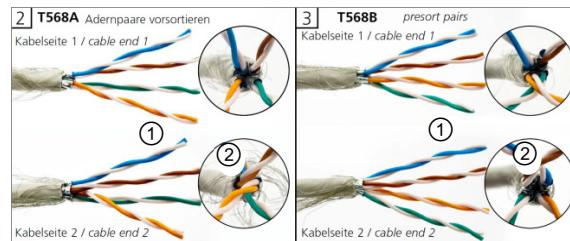
Bei diesen Arbeiten dürfen der Geflechtschirm bzw. der Beidraht und die Adern des Kabels nicht beschädigt werden.



Twisted-Pair-Kabel mit Geflechtschirm

Adern sortieren

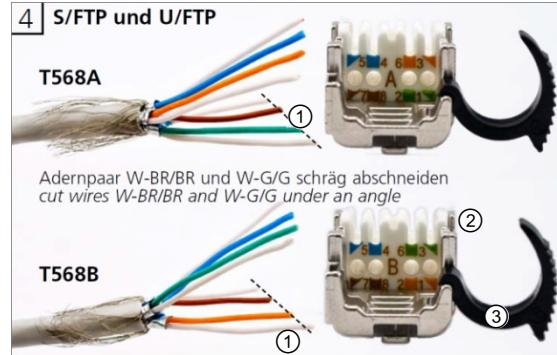
- Legen Sie die Adernpaare ① in Kreuzform ② und entfernen Sie den vorhandenen Elementschirm.
Im Anschluss müssen die vier Adernpaare entdrillt werden, wobei die jeweilige farbige Ader mittig positioniert werden muss.



Sortiertes Twisted-Pair-Kabel

Modul bestücken

- Schneiden Sie die ersten beiden Adernpaare ① mit einem Elektronik-Seitenschneider schräg an.
Dadurch erhalten Sie die Möglichkeit, die Adern leichter in das Unterteil des Moduls ② einzuführen.



- Führen Sie nun die ersten beiden Adernpaare in den unteren Teil und die anderen in den oberen Teil des Moduls ein. Danach schließen Sie die Zugentriegelung ③ des Moduls.
Die überstehenden Adern müssen Sie nun mit einem Seitenschneider am Unterteil des Moduls bündig trennen ④.



AMJ-S-Modul bestücken

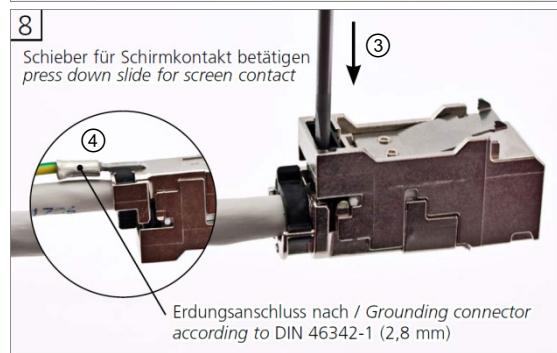
AMJ-S-Modul fertigstellen

- Verbinden Sie das fertig konfektionierte Unterteil ① mit dem Oberteil ②. Danach verpressen Sie beide Teile mit einem Zangenschlüssel oder einer Parallelzange, bis Sie ein Rastgeräusch wahrnehmen.
Nun ist die Kontaktierung zwischen beiden Modulteilen hergestellt.



- Drücken Sie mit einem Schraubendreher den Rasthebel ③.
Damit wird der Schirm mit dem Modul verbunden.

Den Abschluss bildet der Anschluss des Erdungskontaktes ④, wie er in den DIN EN 50310 und DIN 46342-1 vorgesehen ist.



Fertiges AMJ-S-Modul

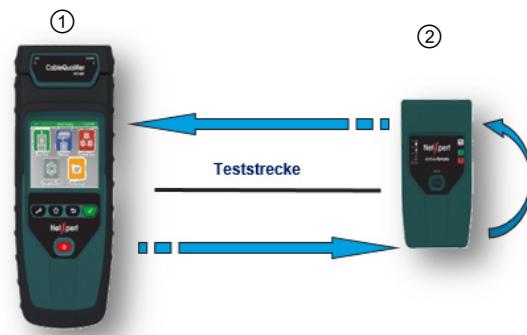
Konfektionierte Kabel überprüfen



Für alle folgenden Messungen zur Überprüfung eines Kabels darf es noch nicht an das Netzwerk angeschlossen werden.

- ▶ Schalten Sie beide Handteile, das lokale Bedienteil ① und das entfernte Handteil ② des Messgerätes ein. Wählen Sie am Bedienteil den kundenspezifischen Messbereich, beispielsweise CAT 6A STP.
- ▶ Verbinden Sie das Bedienteil mit dem einen Ende des konfektionierten Kabels und das Handteil mit dem anderen Ende.
- ▶ Drücken Sie die Autotest-Taste am Bedienteil. Warten Sie nun, bis die Messung durchgeführt wurde.
- ▶ Überprüfen Sie, ob Ihre Messung erfolgreich war.

Sofern keine Fehler angezeigt werden, sind Ihre AMJ-S-Module qualitativ korrekt angeschlossen. Sollten Sie eine Fehlermeldung erhalten, müssen Sie die Konfektionierung des AMJ-S-Moduls wiederholen.



Messgerät zum Qualifizieren von Twisted-Pair-Kabeln

Häufige Fehler

- ✓ offene Kabelenden und Unterbrechungen
- ✓ Kurzschlüsse und das Vertauschen von Adern
- ✓ Längenrestriktionen des Kabels sind überschritten oder falscher Kabeltyp (ungleiche Dämpfung)
- ✓ Überdehnung des Kabels bei der Verlegung oder nicht korrekte Terminierung (Erdung) des Kabels
- ✓ schlechte Schneidkontakteverbindungen am Modul oder defektes Modul
- ✓ Adern-Verdrillung zu weit geöffnet oder Adern-Abschirmung unzureichend
- ✓ defektes Messgerät, Messkabel oder Adapter

- ▶ Überprüfen Sie, ob eine der zuvor angegebenen Fehlerquellen zutreffend ist.
- ▶ Ermitteln Sie, auf welcher Seite der Fehler angezeigt wird, sofern ein Messfehler ausgeschlossen werden kann.
- ▶ Ersetzen Sie zunächst das AMJ-S-Modul auf der fehlerhaften Seite. Ist das Fehlerbild danach immer noch vorhanden, muss man von einem Kabelfehler ausgehen und dieses ersetzen.

5.3 Übungsszenario: RJ-45-Stecker auf ein TP-Patchkabel (UTP/STP) montieren

Im Netzwerk wurde ein Patchkabel beschädigt. Da der Schaden direkt an der PC-Anschlusseite entstand, muss der entsprechende RJ-45-Stecker ersetzt werden.

Sicherheitshinweis

- ▶ Vergewissern Sie sich vor dem Abschneiden des defekten RJ-45-Steckers, dass die Kabelverbindung zwischen dem PC und der entsprechenden Datendose getrennt wurde.

Werkzeug

- ✓ Abisolierzange oder ein anderes geeignetes Werkzeug
- ✓ Crimpzange (für verwendete Steckerform)
- ✓ Seitenschneider / Elektronik-Seitenschneider



Crimpzange

Material

- ✓ RJ-45-Steckersatz z. B. bestehend aus Kabeltülle, Aufteilungskamm und Steckerkörper
- ✓ Patchkabel als Meterware

RJ-45-Stecker existieren in unterschiedlichen Bauformen, in geschirmten und ungeschirmten Varianten, die entweder gecrimpt oder aber auch ohne Spezialwerkzeuge montiert werden können. Das jeweilige Vorgehen bei der Montage erfolgt in Abhängigkeit zum verwendeten Stecker, beinhaltet aber in jeden Fall das Absetzen des Kabelmantels, das Verbinden der Adern mit den Kontakten im Steckerkörper und dem Herstellen einer Zugentlastung für den Stecker.

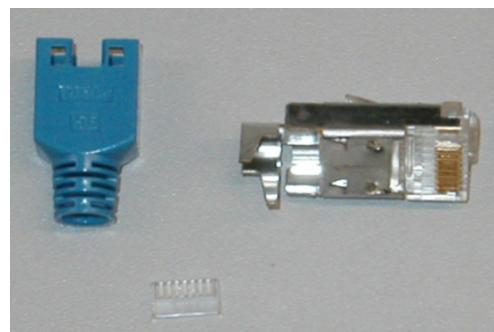
Ein Beispiel, wie dieser Typ Stecker montiert wird, finden Sie auf der nachfolgenden Seite. Eine gute Übersicht über das Crimpen von verschiedenen Stecktypen bietet auch die Webseite:

- ✓ https://www.reichelt.de/reicheltpedia/index.php5/Crimp_Anleitungen

Auch findet man z. B. auf YouTube Filme, die die fachgerechte Montage unterschiedlicher Stecker zeigen. Nachfolgend nur zwei Beispiele:

- ✓ <https://www.youtube.com/watch?v=kZOvugRdUeY>
- ✓ <https://www.youtube.com/watch?v=coXKqq6YbhA>

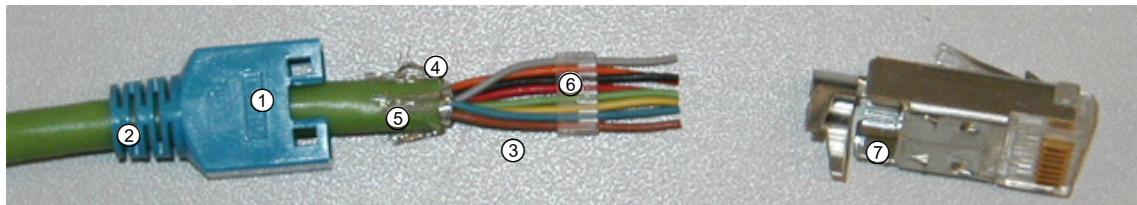
Ein Patchkabel ist flexibel, weil die einzelnen Adern als Litze aufgebaut sind, also aus einem Bündel feiner Drähte bestehen. RJ-45-Stecker können nur an diesen Kabeln angebracht werden.



RJ-45-Stecker in Einzelteilen

Arbeitsschritte zur Montage des RJ-45-Steckers auf ein Twisted-Pair-Kabel

- ▶ Stecken Sie die Kabeltülle ① über das Ende des Twisted-Pair-Kabels ②.
- ▶ Manteln Sie das Twisted-Pair-Kabel mit dem Cable-Stripper über eine Länge von 30 mm ab ③.
- Dabei darf das Innere des Kabels nicht beschädigt werden.**
- ▶ Kürzen Sie das Schirmgeflecht mit dem Cable-Stripper oder einem Seitenschneider auf ca. 7 mm ④ und streifen Sie es anschließend über den Kabelmantel ⑤ zurück. Entfernen Sie die Schirmfolie.
- ▶ Drillen Sie die Adernpaare auf und führen Sie die einzelnen Adern nach dem IEC-Farbcode (EIA/TIA-B) durch den Aufteilungskamm ⑥. Achten Sie auf eine flache und gerade Führung der einzelnen Adern.



Vorbereitetes TP-Kabel, abgemantelt mit Aufteilungskamm

- ▶ Kürzen Sie die Kabeladern auf eine Gesamtlänge von 18 mm.
- ▶ Führen Sie die Kabeladern mit dem Aufteilungskamm in den RJ-45-Stecker ⑦ so weit ein, bis diese an der Steckerfront anstehen.
- ▶ Führen Sie eine Sichtprüfung durch. Jede einzelne Ader sollte deutlich an der Steckerfront zu sehen sein.
- ▶ Crimpen Sie den RJ-45-Stecker mit der dafür vorgesehenen Crimpzange.
- ▶ Überprüfen Sie anschließend den RJ-45-Stecker auf den korrekten Sitz der einzelnen Adern sowie den Sitz des Schirmgeflechts.
- ▶ Entfernen Sie überstehende Drähte der Abschirmung mit dem Seitenschneider.
- ▶ Schieben Sie die Kabeltülle über den RJ-45-Stecker, bis diese einrastet.

5.4 Montagebeispiel: TP-Kabel an Cat 6A-Datendose anschließen

Durch eine Umbaumaßnahme in einem Büro wurden einzelne Datendosen versetzt. Die Baumaßnahmen sind abgeschlossen und die vorübergehend ausgelagerten Arbeitsplätze müssen wieder in Betrieb genommen werden. Die abgetrennten Datenkabel sind fachgerecht anzuschließen und die Datendosen auf ihre Funktion hin zu überprüfen.

LSA+-Technik

Die LSA+-Technik hat sich sowohl im Kommunikations- als auch im Netzwerkbereich weitgehend durchgesetzt und bietet eine schnelle und fehlerfreie Montage.

LSA+ bedeutet „**Lötfrei**“, „**Schraubfrei**“, „**Abisolierfrei**“. Zum Einsatz der LSA+-Technik benötigen Sie ein spezielles Anlegewerkzeug. Die einzelnen Kabeladern werden in Schneidklemmen eingelegt und mithilfe des Anlegewerkzeugs in die Schneidklemme eingedrückt und gleichzeitig abgeschnitten. Die Schneidklemme durchdringt die Isolation der angelegten Ader und stellt so den Kontakt zum Leiter her.



CAT6-RJ-45-Datendose in Einzelteilen

Die LSA+-Technik findet ihren Einsatz hauptsächlich bei:

- ✓ Datendosen
- ✓ ISDN-Dosen
- ✓ Patchpaneln
- ✓ Telefonverteilern/Telefonanlagen

Da das Anlegewerkzeug von verschiedenen Firmen hergestellt wird, ist auch die Ausführungsqualität unterschiedlich. Gerade im Bereich der Netzwerktechnik sollte ein Anlegewerkzeug von hoher Qualität und Präzision eingesetzt werden. Beispielsweise sollte der Kopf des Anlegewerkzeugs aus Metall und nicht aus Kunststoff bestehen.



LSA+ Anlegewerkzeug

Werkzeug

- | | |
|---|---|
| <ul style="list-style-type: none"> ✓ Seitenschneider/Elektronik-Seitenschneider ✓ Abisolierzange/Abmantelwerkzeug ✓ Cable-Stripper ✓ Wasserfester Stift | <ul style="list-style-type: none"> ✓ LSA+-Anlegewerkzeug ✓ Schraubendreher Kreuzschlitz klein ✓ Schraubendreher klein und mittel |
|---|---|

Material

- ✓ Cat 6-Datendose
- ✓ Kabelbinder klein (falls erforderlich)

Anschluss des Twisted-Pair-Kabels an eine Cat 6-Datendose

- Manteln Sie den Kabelmantel des Datenkabels mit dem Cable-Stripper auf eine Länge von etwa 50 mm ab.

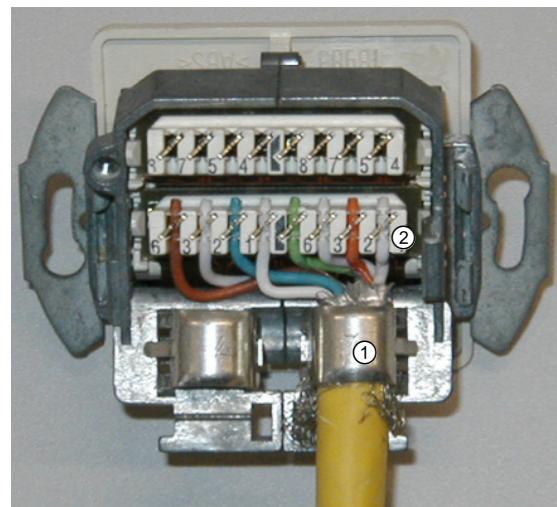
Das Innere des Datenkabels darf nicht beschädigt werden.

Kürzen Sie anschließend das Schirmgeflecht mit einem Seitenschneider auf eine Länge von etwa 10 mm.

- Streifen Sie das Schirmgeflecht über den Kabelmantel zurück.
- Entfernen Sie die Schirmfolie der einzelnen Adernpaare.

Die Verdrillung darf nicht geöffnet werden.

- Setzen Sie die in der Datendose mitgelieferte Kabelhalterungsklammer ① ein und befestigen Sie mit dieser das Kabel.



Vollständig aufgelegte Datendose

Mit der Kabelhalterungsklammer wird auch gleichzeitig der Schirm des Datenkabels mit der Datendose verbunden. Achten Sie hier auf einen korrekten und festen Sitz der Kabelhalterung. Die Kabelhalterungsklammer darf nur den Kabelmantel umfassen, nicht das Kabelinnere. Als weitere Zugentlastung verwenden Sie einen kleinen Kabelbinder (abhängig vom Hersteller der Datendose).

- ▶ Legen Sie jetzt die einzelnen Adernpaare in die beschrifteten Schneidklemmen der Datendose. Achten Sie dabei auf die Einhaltung der Farbcodes. Die Verdrillung der einzelnen Adernpaare muss so weit wie möglich beibehalten werden.
- ▶ Drücken Sie die einzelnen Adern mithilfe Ihres Anlegewerkzeugs in die dafür vorgesehenen Schneidklemmen ② der Datendose.
- ▶ Achten Sie darauf, dass dabei alle überstehenden Enden der Adern sauber abgetrennt werden.
- ▶ Führen Sie eine Sichtprüfung aller aufgelegten Einzeladern durch. Überprüfen Sie auch die Einhaltung der Farbcodes.
- ▶ Beschriften Sie das angeschlossene Datenkabel mit der zugehörigen Kabelnummer oder Portnummer mit einem wasserfesten Stift.
- ▶ Setzen Sie die Abdeckung auf die Datendose und schrauben Sie diese zu.
- ▶ Führen Sie als letzten Schritt eine Messung nach ISO/IEC zur Überprüfung der Datenstrecke aus.

5.5 Lichtwellenleiter verlegen

Die Verlegung von Lichtwellenleitern im Außen- und Innenbereich muss unter Beachtung der einschlägigen Normen, Vorschriften und anerkannten Regeln erfolgen. Ein besonders wichtiges Ziel bezogen auf Lichtwellenleiter ist es, Stauchungen oder Überdehnungen der Fasern zu vermeiden, da dadurch Sofortschäden oder Langzeitschäden entstehen können.

LWL werden im Außenbereich häufig durch Einschieben, Einziehen oder Einblasen in Kabelschutzrohren verlegt, allerdings können längere Distanzen (>200 m) nur mit der Einblasmethode erreicht werden, da die Kabel ansonsten zu stark mechanisch belastet werden. Es existieren eine Reihe weiterer Verlegestrategien für Außen- und Innenkabel, die jedoch den Rahmen des Buches sprengen würden. Daher finden Sie weitere Informationen als Links unterhalb dieses Abschnitts. Im Innenbereich verwendet man im allgemeinen Installationsrohre und -kanäle, sowie Kabelpritschen und -wannen. Hier sind die vorgegebenen Biegeradien unbedingt einzuhalten und ein Verdrehen der Kabel zu vermeiden. Ebenso wie bei Kupferkabeln findet man auch bei LWL Varianten für den Innen- und Außenbereich.

Verlegehinweise und Planungsleitfäden für die Kabelverlegung im Außen- und Innenbereich finden Sie unter den folgenden Webadressen:

- ✓ https://www.rhenania-lwl.de/pdf/verlegehinweise_rev03.pdf
- ✓ https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/breitbandausbau-verlegetechniken.pdf?__blob=publicationFile
- ✓ https://www.bmvit.gv.at/service/publikationen/telekommunikation/downloads/planungsleitfaden_outdoor_ua.pdf
- ✓ https://www.bmvit.gv.at/service/publikationen/telekommunikation/downloads/planungsleitfaden_indoor_ua.pdf

Bei den letztgenannten handelt es sich um Publikationen des österreichischen Bundesministers für Verkehr, Innovation und Technologie, die in weiten Teilen ebenfalls auf EN-Normen (**Europa-Norm**) und IEC-Standards (**International Electrotechnical Commission**) basieren.

5.6 Anwendungsbeispiel: LightCrimp Plus

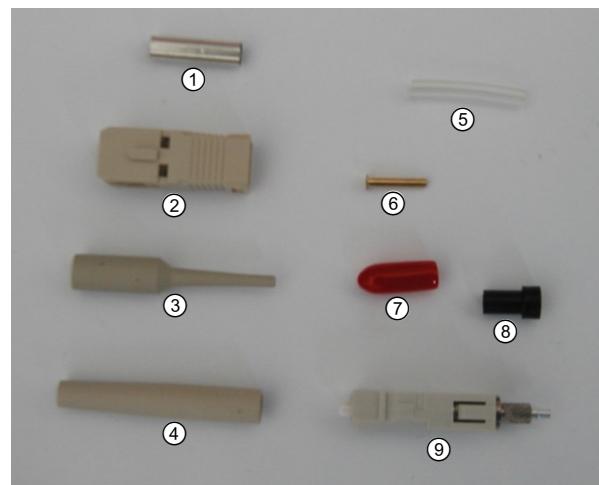
LightCrimp Plus ist die Produktbezeichnung des Herstellers AMP, für eine leicht zu handhabende LWL-Steckertechnik. Auf der Webseite von AMP heißt es:

„Konfektionieren Sie selbst Glasfaserstecker in unter 1 Minute!“ ... „die Stecker müssen nur gecrimpt werden. Durch die schnelle Montage mit wenigen Werkzeugen, eignet sich diese Technik ideal für die Außenmontage auf Baustellen oder kleinere Projekte als Alternative zum Spleißen.“

Bei dem LWL-Steckverbinder LightCrimp Plus handelt es sich um einen Lichtwellenleitersteckverbinder, bei dem bereits werkseitig eine Glasfaser in den Stecker eingeklebt ist. Dies ist eine Multimode-Glasfaser mit einem Kern durchmesser von 50 µm oder 62,5 µm. Die Endflächen der eingeklebten Glasfaser sind bereits maschinell poliert und müssen nicht nachbehandelt werden. Das andere Ende der Glasfaser ist geschnitten und liegt in dem im Stecker integrierten mechanischen Spleißelement. Bei der Verarbeitung ist das Installationskabel abzusetzen und anschließend zu reinigen. Danach wird das Installationskabel angeritzt und gebrochen. Dieses so behandelte Ende der Einzelfaser wird dann in dem im Stecker integrierten mechanischen Spleißelement auf Stoß aneinandergelagert und anschließend 2- bis 4-mal gecrimpt.

Inhalt eines LightCrimp Plus Steckerkits

- ✓ äußere Crimpföhre ①
- ✓ Steckergehäuse ②
- ✓ Knickschutz für 900 µm ③
- ✓ Knickschutz für Kabelmantel ④
- ✓ Röhrchen für Easy-Strip-Adern ⑤
- ✓ innere Crimpföhre ⑥
- ✓ Staubschutz ⑦
- ✓ Staubschutz ⑧
- ✓ Steckverbinder mit eingeklebter Faser ⑨



Bauteile eines LightCrimp Plus Steckverbinderkits

LightCrimp Plus Steckverbinder sind in erster Linie für Büroumgebungen entwickelt worden. Bei anderen Einsatzgebieten sollte ein anderes Verfahren verwendet werden.



Steckertypen für SC LightCrimp Plus

- ✓ Simplex 50/125
- ✓ Simplex für 10 Gbit/s XG 50/125
- ✓ Duplex für 10 Gbit/s XG 50/125
- ✓ Simplex 62,5/125
- ✓ Duplex 50/125

An LightCrimp Plus Steckverbinder können alle gängigen Glasfaserkabel mit Bündelader sowie Mini-Breakout- und Breakout-Kabel mit Festaderaufbau (900 µm) verarbeitet werden. Kunststoffadern dagegen können nicht verarbeitet werden.

Sauberkeit

Beim Umgang mit und der Verarbeitung von Glasfaserprodukten gilt als oberstes Gebot Sauberkeit – sowohl für das verwendete Werkzeug als auch für die eingesetzten Messgeräte. Glasfaserreste gelten als Sondermüll und müssen entsprechend entsorgt werden. Die Verwendung von entsprechenden Spezialwerkzeugen bei der Verarbeitung von Glasfasern ist zwingend erforderlich.

Werkzeug

- ✓ Microstripper ①
- ✓ Crimpzange mit Matrize (Pressform) für SC-Steckverbinder ②
- ✓ Ritz- und Brechwerkzeug ③
- ✓ Mantelstripper ④
- ✓ Kevlarschneider ⑤
- ✓ wasserfester Stift für Markierungen ⑥
- ✓ Kabelhalter ⑦



Werkzeug für Steckermontage

Sicherheitshinweise

- Tragen Sie zur Installation immer eine Schutzbrille, um Augenverletzungen zu vermeiden.
- Seien Sie vorsichtig im Umgang mit den Faserenden. In die Haut eindringende Fasern können abbrechen und Hautreizungen hervorrufen.
- Achten Sie darauf, dass alle überstehenden Faserenden sauber abgetrennt werden.
- Verwenden Sie ein verschließbares Gefäß für die Faserreste.
- Essen und trinken Sie niemals an Ihrem Arbeitsplatz.
- Das Werkzeug und der Arbeitsplatz sollen immer sauber sein.

Crimpen eines LightCrimp Plus Steckverbinder

- Öffnen Sie die Verpackung des Steckverbinderkits und prüfen Sie, ob alle erforderlichen Bauteile vorhanden sind.
- Wählen Sie den entsprechenden Knickschutz für Ihr Kabel aus und schieben Sie diesen über die Ader.
- Entfernen Sie den Staubschutz am Steckverbinder.
- Legen Sie die Ader so in die Mulde des Kabelhalters, dass das vordere Ende am Anschlag der Mulde liegt ①.
- Markieren Sie die Ader an beiden die Mulde kreuzenden Schlitten mit einem wasserfesten Stift.
- Setzen Sie die jeweilige Ader mit dem Microstripper auf eine Länge von etwa 35 mm ab ②.
- Entfernen Sie jetzt den Schutzlack, der die eigentliche Glasfaser umgibt, mit einer Absetzzange für Glasfaserkabel (Millerzange).

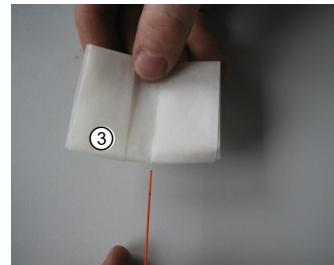


Kabelhalter

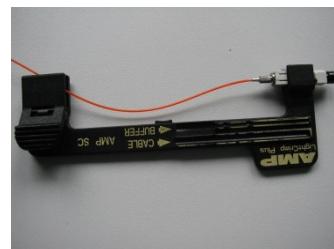


Microstripper

- ▶ Reinigen Sie die so bearbeitete Faser mit einem fusselfreien Tuch, das mit Isopropylalkohol getränkt ist ③. Achten Sie nach dem Reinigen der Faser darauf, diese nicht mehr zu berühren.
 - ▶ Überprüfen Sie, ob Ihr Brechwerkzeug für die Glasfaser sauber und ohne Rückstände von vorangegangenen Arbeiten ist. Zum Reinigen können Sie ebenfalls Isopropylalkohol verwenden.
 - ▶ Ritzen Sie die Glasfaser mit einem Abstand von etwa 8 mm und brechen Sie diese an dieser Stelle mit einem geeigneten Werkzeug (Ritz- und Brechwerkzeug).
 - ▶ Nehmen Sie den Kabelhalter mit dem vorgefertigten Steckverbinder und schieben Sie die Ader mit der gebrochenen Faser vorsichtig in den Steckverbinder. Schieben Sie das Kabel so weit in den Steckverbinder, bis die zweite Markierung auf der Ader im Stecker verschwunden ist.
 - ▶ Entlasten Sie die Ader am anderen Ende des Kabelhalters mithilfe des dafür vorgesehenen Schnellverschlusses. Sorgen Sie durch einen Bogen für eine leichte Entspannung der Installationsader.
- Dabei sollte der Bogenmittelpunkt in der Mitte des Kabelhalters sein. Durch diesen Bogen wird die Faser leicht in den Steckverbinder gedrückt.
- ▶ Nehmen Sie die geöffnete Crimpzange mit der SC-Matrize, drücken Sie diese leicht zusammen, bis es zweimal hörbar geklickt hat.
 - ▶ Legen Sie den Steckverbinder in die Zange. Achten Sie darauf, dass der weiße Keramikstift (Ferrule) des Steckverbinder in die Pfeilrichtung, die auf der Matrize angebracht ist, zeigt.
 - ▶ Drücken Sie die Crimpzange mit mäßiger Geschwindigkeit bis zum Endpunkt zu. Sie fixieren damit die Installationsfaser an der im Stecker eingeklebten Faser.
 - ▶ Öffnen Sie die Zange und legen Sie den fixierten Steckverbinder in das dafür vorgesehene Crimpnest der Zange.
 - ▶ Drücken Sie die Crimpzange erneut bis zum Endpunkt zu.
 - ▶ Lösen Sie die Zange und nehmen Sie den Steckverbinder aus der Zange.
 - ▶ Schieben Sie abschließend den Knickschutz über den Steckverbinder und schieben Sie das Gehäuse auf den Steckverbinder.
 - ▶ Sollten Sie den Steckverbinder nicht unmittelbar verwenden, stecken Sie den Staubschutz auf das vordere Ende der Ferrule.



Reinigen der Faser



Entlastung der Installationsader



Fixieren der Installationsfaser



Crimpen des Steckverbinder



Fertig gecrimpter Steckverbinder (ohne Staubschutz)

Messen der Verbindung

Je nach Einsatzgebiet als Patchkabel oder als Verbindungsstrecke sollte der gecrimpte Steckverbinder unmittelbar vor der Verwendung oder gleich nach der Konfektionierung mittels geeigneter Messgeräte auf Fehlerfreiheit geprüft werden. Durch diese Art der Steckermontage (Crimptechnik) kann es vorkommen, dass die Installationsfaser nicht bis an das entsprechende Ende der eingeklebten Faser gedrückt wird. Ist dies der Fall, entstehen Verluste durch zu hohe Dämpfung an den Übergangsstellen. Sollte die Messung der Übertragungsstrecke einen zu hohen Wert (Verlust) aufweisen oder gar keine Werte anzeigen, ist der Steckverbinder zu trennen und erneut zu konfektionieren. Der verwendete Steckverbinder ist in diesem Fall nicht mehr zu gebrauchen und muss entsorgt werden.

6 Qualitätssicherung

In diesem Kapitel erfahren Sie

- ✓ welche Messgeräte zum Messen von Kupfer- und LWL-Kabeln eingesetzt werden
- ✓ wie eine Abnahmemessung im LAN vorgenommen wird

Voraussetzungen

- ✓ Kenntnisse in Funktion und Umgang mit einem Multimeter
- ✓ Kenntnisse in Funktion und Umgang mit einem LAN-Messgerät

6.1 Messgeräte für die Kupfertechnik

Wenn eine Verkabelung durchgeführt wurde und alle angeschlossenen Geräte einwandfrei funktionieren, dann hat der Systemverwalter ein ruhiges Leben. Doch was ist zu tun, wenn Geräte nicht einwandfrei arbeiten oder sich nicht ins Netzwerk einbinden lassen? Ursachen hierfür gibt es viele, z. B. defekte Netzwerkkarten oder fehlerhafte Ports an Switch-Geräten. Das Problem kann aber auch in der Verkabelung beziehungsweise in der Verdrahtung der passiven Komponenten oder bei den Upper-Layer-Protokollen liegen. Messgeräte für Kupferverkabelungen prüfen sowohl die Kabel selbst, als auch Anschlüsse und Verbindungen auf ihre Eigenschaften. Gerade in der Datentechnik müssen physikalische Grenzwerte von Übersprechen, Impedanz, Dämpfung u. v. m. streng eingehalten werden, da es sonst zu Reflexionen und Signalverlusten kommen kann.

Einfache Kabeltester (Verifizierer)

Einfache Prüfmittel dienen zur Kontrolle der hergestellten Anschlüsse sowie zur Überprüfung der verwendeten Kabel. Mit einfachen Prüfmitteln kann festgestellt werden, ob die gewünschten Pins (z. B. an Datendose und Patchpanel) korrekt belegt und durchgeschaltet wurden. Prüfmittel können durch die Kombination von digitalen und analogen Ton-Signalisierungen praktisch jedes Kupferkabel (Telefon-, Twisted-Pair-Daten-, Koaxial- sowie Sicherheits- und Alarmverkabelungen), unabhängig von der Anwendung oder Umgebung, lokalisieren und verifizieren. Damit lassen sich Unterbrechungen und Kurzschlüsse in der Verbindung feststellen. Sie geben allerdings keinen Aufschluss über die elektrischen Eigenschaften der gesamten Verbindung und somit der Leitungsgüte.

Einsatzbereiche für die analoge Signalprüfung

Die analoge Signalprüfung eignet sich für Telefonkabel (bis Cat 3) sowie für Koaxial-, Sicherheits-/Alarm- und Lautsprecherkabel. Sie erlaubt das exakte Lokalisieren einzelner Adernpaare anhand der Signaländerung und die genaue Ortung bei der Verfolgung von Adern. Die Kabel sind für niederfrequente Übertragungen konzipiert und können daher mit einem niedrigfrequenten Ton leicht isoliert werden. Die analoge Tonprüfung sollte außerdem in Bereichen mit relativ wenigen Interferenzen von elektronischen Geräten eingesetzt werden. In Umgebungen mit starken Interferenzen ist die digitale Tonprüfung möglicherweise die bessere Wahl.



Verifizierer (Kabeltester):
CableMaster 600

Einsatzbereiche für die digitale Signalprüfung

Die digitale Signalprüfung (das Signal ist digital codiert) ist vorwiegend für Datenverkabelungen (Cat 5 – 8.2) und in aktiven Netzwerkumgebungen vorgesehen. Es arbeitet auf einer hohen Frequenz und ist daher für höherfrequente Datenmodulationen geeignet, die von der Verkabelung übertragen wird. Mittels der digitalen Signalprüfung lassen sich Kabel identifizieren, auch wenn diese an einer aktiven Komponente angeschlossen sind (z. B. Switch, um Kabelzugehörigkeit zu einem Port zu erkennen). Gleichzeitig können der Kabeldurchgang und eine Fehlererkennung (z. B. Kurzschlüsse, vertauschte Adernpaare, Unterbrechungen) durchgeführt werden.

Anwendungsbereiche für analoge und digitale Signalgeber

Der Signalgeber ist für Kupferkabel inkl. 75- oder 50-Ohm-Koaxialkabel, Zweileitersteuerung, allgemeine Steuerkabel, POTS/ISDN-Telekommunikationsleitungen sowie UTP- bzw. STP-Kabel einsetzbar. Dazu kann über die Signalschnittstelle auf allen Leitungspaaren entweder ein codiertes Datensignal oder ein analoges Tonsignal (Frequenzbereich: 500–1200 Hz) mit 4 Melodien eingespeist werden.

6.2 Oszilloskop

Grundlegendes über Oszilloskope

Bei Oszilloskopen wird die zu messende Eingangsgröße, im Allgemeinen sind dies Spannungswerte, über ihren zeitlichen Verlauf grafisch dargestellt. Dabei werden zu genau definierten Zeitpunkten die anliegenden Spannungswerte gemessen.

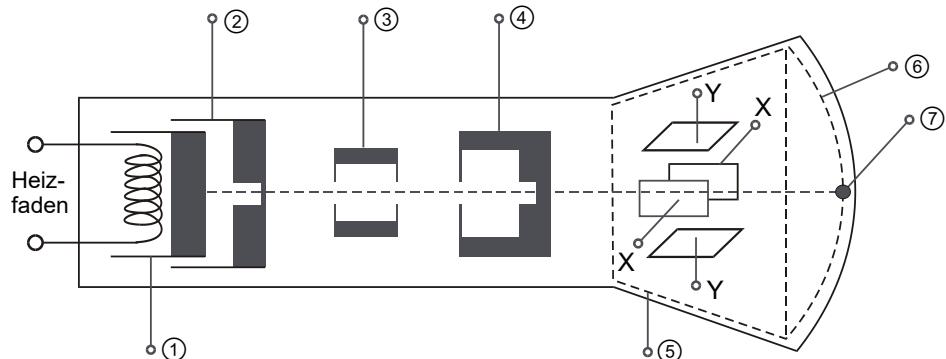
Oszilloskope eignen sich besonders, wenn Aussagen zum zeitlichen Verlauf eines Signals erforderlich sind. Hilfreich ist dies zum Beispiel, um ein Eingangs- und Ausgangssignal miteinander zu vergleichen und das Signalverhalten darzustellen.

Funktionsweise eines Oszilloskops

Für die Anzeige auf einem analogen Oszilloskop wird eine sogenannte Elektronenstrahlröhre verwendet. Die für den Elektronenstrahl erforderlichen negativen Ladungsträger werden durch einen Heizfaden in unmittelbarer Umgebung zur Kathode durch Elektronenemission erzeugt. An der Kathode liegt eine Spannung von 200 bis zu 800 Volt an. Die an der Kathode produzierten Elektronen werden durch die an der Anode anliegende Spannung (+100 V bis +200 V) in Richtung Anode beschleunigt. Da das Vakuum innerhalb der Glaskugel für die Elektronen keinen Widerstand auf ihrem Weg zur Anode darstellt, erreichen diese sehr hohe Geschwindigkeiten. Die Darstellung des Elektronenstrahls erfolgt durch eine aufgetragene Leuchtschicht auf der Bildschirmrückseite der Röhre.

Der so entstandene Elektronenstrahl kann in seiner Intensität im Wehneltzylinder beeinflusst werden. Im Wehneltzylinder wird eine Art Bremsfeld erzeugt und es können weniger Elektronen austreten und zum Leuchtschirm fliegen. Dadurch ist der am Leuchtschirm dargestellte Elektronenstrahl schwächer und der dargestellte Lichtstrahl dunkler.

Aufbau der Braunschen Röhre



- | | | |
|--------------------|----------------------------|--------------|
| ① Kathode | ④ Anode | ⑦ Brennpunkt |
| ② Wehneltzylinder | ⑤ Nachbeschleunigungsanode | |
| ③ Elektronen-Optik | ⑥ Leuchtschicht | |

X X-Platten für die Zeitmessung (horizontale Ablenkung): Der Elektronenstrahl wird durch elektrische Felder nach links oder rechts abgelenkt.

Y Y-Platten für die Spannungsmessung (vertikale Ablenkung): Der Elektronenstrahl wird durch elektrische Felder nach oben oder unten abgelenkt.

Einsatzgebiet

Oszilloskope werden zur Darstellung von periodischen bzw. einmaligen Signalen verwendet. Durch die einstellbaren Messbereiche sind Oszilloskope in der Lage, Auskunft über die Periodendauer und die Amplitude eines Signals zu geben. Beim Aufbau und der Fehlersuche in elektronischen Schaltungen sind Oszilloskope unabdingbare Messgeräte. Ein Einsatz als Messgerät in Netzwerken ist jedoch weniger empfehlenswert, da es in Netzwerken hauptsächlich auf den Inhalt von Paketen und weniger auf den Verlauf der Datensignale ankommt.

Oszilloskope können jedoch sehr gut bei der Darstellung von Signalverläufen und -verzögerungen in Netzwerken verwendet werden, wenn der Verdacht besteht, dass Signale aufgrund der Leitungs- und Übertragungsbedingungen stark verändert werden. Aktuell finden vorwiegend digitale Oszilloskope (DSO, engl. Digital Storage Oscilloscope) Anwendung, die über eine Speicherfunktionalität der erfassten Messwerte verfügen.

Es existiert eine große Anzahl von Digital-Oszilloskop-Adaptoren, die über die USB-Schnittstelle an den PC angeschlossen werden. Diese sind oft eine preisliche Alternative zu klassischen Oszilloskopen. Sie weisen gegenüber den professionellen Messmitteln jedoch eine eingeschränkte Funktionalität (besonders bei der Bandbreite) auf.

6.3 LAN-Messgeräte

LAN-Messgeräte sind leistungsfähige Kabeltester zum Testen und Messen von Twisted-Pair- und Koaxialkabeln. Sie werden für Abnahmemessungen bei einer strukturierten Verkabelung verwendet. Das Set besteht aus einem Handgerät mit Display und einem Endgerät. Das Handgerät mit Display steuert beide Geräte und führt alle Funktionen aus. Handgerät und Endgerät sind mit einem Akkusatz bestückt, damit die Messungen flexibel und ohne Störungen durch das Stromnetz durchgeführt werden können.

Je nach Hersteller arbeiten LAN-Messgeräte mit unterschiedlichen Messmethoden:

- ✓ analoge Messung
- ✓ digitale Messung

Analoge Messtechnik

Bei der analogen Methode, z. B. bei einem 1000-MHz-Tester, wird der Frequenzbereich schrittweise abgetastet (wobbeln). Im Frequenzbereich von 1 Hz bis ca. 31 MHz wird eine Schrittweite von 150 KHz verwendet. Diese erhöht sich ab ca. 32 MHz bis 100 MHz auf etwa 250 KHz. Die Schrittweite innerhalb weiterer Frequenzbereiche ist in der Tabelle dargestellt. Aus den so erhaltenen Messpunkten (Stützpunkte) wird dann das Messergebnis gemittelt.

Frequenzbereich	Schrittweite
1 MHz bis ca. 32 MHz	150 KHz
32 MHz bis 100 MHz	250 KHz
100 MHz bis 250 MHz	500 KHz
250 MHz bis 1000 MHz	1 MHz

Vektorielle Messtechnik

Bei der vektoriellen Messtechnik wird über den Betrag des Messwertes hinaus die Phaseninformation ausgewertet. Unter Phaseninformation ist der Phasenwinkel zwischen Sende- und Empfangssignal zu verstehen. Mit der vektoriellen Messtechnik erschließt sich die Möglichkeit, die Referenzebene zu verschieben, damit der örtliche Standpunkt der Messung direkt vor die RJ-45-Stecker bzw. -Buchsen gelegt werden kann.

Dies ist Voraussetzung für die sogenannte Permanent-Link-Messung. Die Permanent-Link-Definition löst in der Standardisierung (Entwurf: ISO/IEC 11801 2. Ausgabe Klasse E/F und EN50173.A1) die Basic-Link-Definition ab. Im Gegensatz zur Basic-Link-Definition darf bei der Permanent-Link-Definition der Einfluss der Anschlussleitung nicht in das Messergebnis eingehen.

Diese analoge vektorielle Messtechnik lehnt sich an das Messverfahren von hochwertigen Netzwerkanalysatoren an, welche bereits bis in den GHz-Messbereich vorgestoßen sind.

Digitale Messtechnik

Bei der digitalen Methode wird der anliegende Messwert durch eine stufenweise Bearbeitung des Messsignals ermittelt. Dieser Messwert ist eine quantisierte Abbildung der Messgröße. Dabei werden die eingehenden Signale in zeitlich fest definierten Zeitabständen abgetastet (Sampling). Zu jedem dieser Abtastpunkte wird der gemessene Wert in eine digitale Größe umgewandelt.

LAN-Messgeräte zum Qualifizieren

Diese Messgeräte sind zur Fehlersuche bei Datenverbindungen für den Servicetechniker vor Ort bestens geeignet. Mithilfe solcher Messgeräte lässt sich ein schneller Nachweis über die Qualität einer Datenstrecke erbringen. Durch die integrierten Hilfsfunktionen ist es möglich, in kürzester Zeit Kabelfehler wie Kurzschlüsse oder Kabelbrüche zu lokalisieren. Mit diesen Geräten besteht auch die Möglichkeit, die Verbindungsqualität einer Gigabit-Strecke gemäß dem IEEE-802.3 Clause-40-Standard zu prüfen. Zu diesem Zweck werden über die Verbindung Datenframes zwischen den beiden Handteilen gesendet.

Im Gegensatz zu den verifizierenden Prüfmitteln lassen sich mit diesen Kabelmessgeräten wesentlich bessere und genauere Angaben bei der Fehlersuche machen. Auch lässt sich der Nachweis der Anforderung an eine Verkabelung in der Praxis führen. Die gespeicherten Daten können über einen PC ausgelesen werden. Anhand der mitgelieferten Software oder über integrierte Austauschformate können übersichtliche Berichte gedruckt und dem Anwender als qualifizierte Dokumentation übergeben werden.



Qualifizierer: NetXpert 1400

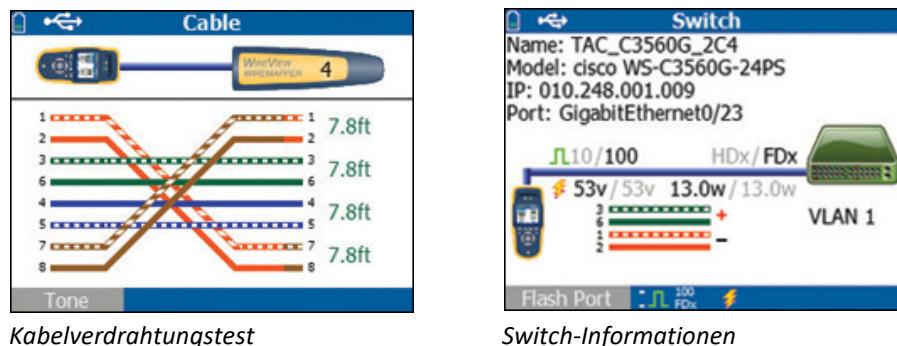
Eigenschaften von LAN-Messgeräten zum Qualifizieren von Übertragungsstrecken sind:

- ✓ Durchführen von Linktests bis mindestens Gigabit-Ethernet
- ✓ einfache Bedienbarkeit und interne Speicherung der Messergebnisse
- ✓ Echtzeit-Darstellung der Bitfehlerrate zum Auswerten bei Netzwerkfehlern
- ✓ Darstellung des Verdrahtungsplans (Wire Map) gemäß EN 50173 und EIA/TIA 568 A/B
- ✓ integrierte TDR-Messung zum schnellen Lokalisieren von Kurzschlüssen oder Drahtbruch
- ✓ Verifizierung der Verbindung zu einem Switch bzw. VLAN
- ✓ Testen des IEEE802.1X-Protokolls (optional)
- ✓ integrierter Konnektivitätstest für IP und IPv6-Endgeräte
- ✓ Unterstützung unterschiedlicher Übertragungsmedien (Kupfer und LWL)
- ✓ Testen der PoE(Power over Ethernet)-Parameter
- ✓ einfache DHCP- und DNS-Tests
- ✓ schnelle Fehlersuche vor Ort

Grafische Darstellung der Messergebnisse

Der **Verdrahtungstest** zeigt ermittelte Unterbrechungen, Kurzschlüsse, Fehlverdrahtungen und Split-Pair-Fehler bei nicht konfektionierten Kabeln mit einem WireView-Kabelabschlussstecker an.

Die dargelegten **Switch-Informationen** zeigen die Darstellung der Parameter Switch-Name und Modell, IP-Adresse, Port, Steckplatz und VLAN, Duplex-Modus und Geschwindigkeit (tatsächliche und angekündigte Geschwindigkeit), Signalstärke, Verbindungs-MDI oder -MDI/X, PoE-Spannung und -Leistungsaufnahme (tatsächlich und Grenzwerte) und grafische Darstellung der Stromversorgung der Paare an.



Firmware

Da LAN-Messgeräte mit einer eigenen Firmware ausgestattet sind, ist es immer wieder möglich, die neueste Version aufzuspielen. Diese Firmwareupdates beinhalten wichtige Entwicklungen in den Mess-Standards oder Funktionserweiterungen der Messgeräte. Software-Updates sind entweder direkt vom Hersteller des LAN-Messgerätes oder über das World Wide Web unter der entsprechenden Adresse erhältlich. Für den Upload der Software auf die Geräte steht in den Handbüchern der Messgeräte die genaue Vorgehensweise.

Verkabelungstypen

Mit LAN-Messgeräten können verschiedene zu testende Verkabelungstypen ausgewählt werden. Es ist aber auch möglich, die Prüfparameter auf Ausbreitungsgeschwindigkeit, Frequenzbereich, Anschlussbelegung und Grenzwerte an Ihre Bedürfnisse anzupassen. Bei der Auswahl eines Kabeltyps werden die betreffenden Kabelspezifikationen automatisch eingestellt.

Wählbare Verkabelungstypen sind z. B.:

- ✓ RJ-45: 10BASE-T, 100BASE-TX, 1000BASE-T und PoE (IEEE 802.3af und 802.3at)
- ✓ kundenspezifische Kabeltypen
- ✓ optional SFP-Adapter (z. B. 100Base-FX, 1000Base-LX/SX/ZX)

LAN-Messgeräte zum Zertifizieren

Die im obigen Abschnitt dargelegten Messgeräte sind mitunter kein Ersatz für die vollwertigen Messgeräte zur zertifizierten Abnahme eines Netzwerkes. Vielmehr dient diese Art von LAN-Messgeräten eher als zusätzliches Tool bei der Fehlersuche oder zur schnellen Überprüfung einer neu verlegten Kabelstrecke.



Zertifizierer: WireXpert 4500

Die Zertifizierung bildet die klassische Abnahmemessung von Netzwerken. Hierzu gehören:

- ✓ genormte Abnahmemessungen mittels Nieder- und Hochfrequenzmessungen und Nachberechnungen der elektrischen Eigenschaften der Datenstrecke
- ✓ die garantierte Einhaltung der vorgegebenen Grenzwerte einer Leistungsklasse und die Sicherstellung der problemlosen Übertragung unterschiedlichster Anwendungen; dies erfolgt durch die Beurteilung der relevanten Standards und Normen
- ✓ der Nachweis der Kompatibilität der unterschiedlichen Steckerdefinitionen auf der Installations- und Übertragungsstrecke

6.4 Testparameter für TP-Verkabelungen

Die Qualität einer Übertragungsstrecke ist von ihren elektrischen Eigenschaften abhängig wie beispielsweise Kapazität, Dämpfung, DC-Widerstand und Impedanz. Ein hoher Dämpfungswert reduziert die effektive Übertragungsbandbreite. Durch die Verwendung eines TP-Kabels mit beispielweise größerem Aderquerschnitt können die erzielten Messwerte beeinflusst werden. Es sollte auch beachtet werden, dass eine Dämpfungsangabe unmittelbar mit der Länge einer Strecke zusammenhängt.

Zu den elektrischen Parametern einer Abnahmemessung gehören:

- | | | |
|-----------------|---------------------|----------------------|
| ✓ Verdrahtung | ✓ Dämpfung | ✓ ACR-N |
| ✓ Länge | ✓ Rückflussdämpfung | ✓ ACR-F |
| ✓ DC-Widerstand | ✓ Übersprechen | ✓ Powersum-Parameter |

Verdrahtung

Bei der Verdrahtungsmessung erfolgt ein Überprüfen der Adern und, sofern vorhanden, der Abschirmung auf Durchgang. Mit diesem Test ist es möglich, Unterbrechungen, Kurzschlüsse und Verdrahtungsfehler (Vertauschungen) festzustellen. Damit eine leichtere Erkennung der Messergebnisse möglich ist, werden diese grafisch dargestellt.

Länge

Die Längenmessung wird aufgrund der Laufzeit, die ein reflektiertes Signal über die Leitungslänge benötigt, ermittelt. Dieses Verfahren wird auch Laufzeitmessung (TDR = Time Domain Reflectometry) genannt. Für ein genaues Ergebnis muss die Ausbreitungsgeschwindigkeit (NVP-Wert) des betreffenden Kabels bekannt sein.

Gleichstrom-Widerstand

Dieser Test gewährleistet eine wirksame Kontrolle der einwandfreien Funktion von Kabel und Steckerverbindern. LAN-Messgeräte überprüfen mit diesem Test, ob der Einzelwiderstand pro Paar und Gesamtwiderstand im empfohlenen Bereich liegt.

Einfügedämpfung

Der Dämpfungswert beschreibt die Abschwächung eines Signals auf einer Übertragungsstrecke. Die Dämpfung einer metallischen Leitung hängt zum einen von der Länge und dem Aderquerschnitt ab, zum anderen von der übertragenen Frequenz. Der angegebene Wert ist ein logarithmisches Verhältnis zwischen Eingangs- zu Ausgangsleistung beziehungsweise Eingangs- zu Ausgangsspannung. Ein zu hoher Dämpfungswert kann dazu führen, dass der Empfänger die übertragenen Signale falsch interpretiert oder gar nicht erkennt.

Rückflussdämpfung

Dieser Wert kennzeichnet die Güte der Impedanz einer Übertragungsstrecke. Die Rückflussdämpfung einer Kabelstrecke gibt das Verhältnis zwischen der Sendeleistung am Kabelanfang zur reflektierten Empfangsleistung am Kabelende an. Der Wert für die Rückflussdämpfung sollte möglichst hoch sein. Je geringer dieser Wert ist, desto größer ist der Anteil des zum Sender zurückreflektierten Signals.

Übersprechen

Unter Übersprechen versteht man das Einkoppeln eines Signals von einem Adernpaar auf das benachbarte Adernpaar. Da in einem Adernpaar häufig das Sendesignal, in einem anderen das Empfangssignal übertragen wird, kann es durch das Übersprechen zu Störungen beim Empfänger kommen.

Die angegebenen Werte für das Übersprechen, genauer die Übersprechdämpfung, werden in Dezibel (dB) angegeben. Bei einem hohen Wert für die Übersprechdämpfung ist das Einkoppeln auf benachbarte Adernpaare sehr gering.

ACR-N

Für die Qualität eines Übertragungskanals ist das Verhältnis von Kabeldämpfung zur Nebensprechdämpfung in Abhängigkeit von der Frequenz ausschlaggebend. Dieses Verhältnis heißt **attenuation to crosstalk ratio** (ACR). Als ACR wird das Verhältnis zwischen der Stärke des ankommenden Signals und des Rauschens auf einer Leitung bezeichnet. Das in ein Kabelpaar eingespeiste Signal reduziert sich am Kabelende um die Kabeldämpfung. Eine weitere Signalverschlechterung erfolgt durch das eingekoppelte Signal, das infolge des Nahnebensprechens entsteht. Der ACR-Wert gibt die Beziehung zwischen der Dämpfung und dem Nahnebensprechen bei einer bestimmten Frequenz an. Auf einer Übertragungsstrecke gibt es sowohl einen ACR-Wert am nahen Ende (N) als auch am fernen Ende (F). Man unterscheidet daher zwischen **ACR-N** und **ACR-F**.

ACR-F

ACR-F ist eine relative Größe, die das Verhältnis des übersprechenden Ausgangspegels zum eigentlichen Ausgangspegel definiert. Zur Berechnung der ACR-F-Werte werden die auf das zweite Leiterpaar eingestreuten Störpegel ins Verhältnis zum Ausgangspegel gesetzt. Der ACR-F -Wert hat gegenüber dem zugrunde liegenden FEXT-Wert (far end crosstalk/Fernnebensprechdämpfung) den Vorteil, dass er nicht von der Kanallänge abhängig ist, da sowohl das „ferne“ Störsignal als auch das Ausgangssignal von der Kanallänge abhängen und am gleichen Entfernungsort bestimmt werden.

Powersum-Parameter

Die Powersum-Berechnungen bilden die Leistungssumme der entsprechenden Tests. Es handelt sich dabei um die Summe aller Störsignale, die von den benachbarten Adernpaaren in ein Leiterpaar eingekoppelt werden. Dieser Wert ist besonders wichtig bei vier- und höherpaarigen symmetrischen Kabeln. Bei zweipaarigen Kabeln entspricht beispielsweise das PSNEXT (powersum NEXT) dem NEXT (near end crosstalk). Bei höheren Leiterpaarzahlen werden die Unterschiede immer größer, da die Störsignale von mehreren Leiterpaaren in ein Leiterpaar eingestreut werden. Powersum-Berechnungen werden für NEXT, ACR-N und ACR-F ausgeführt.

6.5 Abnahmemessung für Kupferkabel durchführen

Abnahmemessungen sind bei einer strukturierten Gebäudeverkabelung unbedingt erforderlich, damit eine Aussage über die Qualität der einzelnen Übertragungsstrecken getroffen werden kann. Sie sollten diese Abnahmemessung in Ihrem Unternehmen unbedingt ausführen oder von einer entsprechenden Fachfirma ausführen lassen. Bei einer zertifizierten Abnahmemessung müssen die Messgeräte jährlich kalibriert werden. Anhand solcher Kabeltests sind Sie außerdem in der Lage, Fehlerquellen bei der Verkabelung auszuschließen.

Verkabelungstyp, Topologie und Mess-Standard einstellen

Wählen Sie den zu testenden Verkabelungstyp (z. B. Twisted Pair), die Topologie (Permanent oder Channel Link) und den erforderlichen Mess-Standard aus (z. B. ISO Class F STP). Bei einer Channel Link Messung wird die Verkabelung inkl. Patchkabel gemessen, bei Permanent Link ohne Patchkabel. Durch diese Einstellungen werden die zutreffenden Messparameter und Grenzwerte automatisch eingestellt.

NVP (Nominal Velocity of Propagation)

Bei der Übertragung von Signalen auf einem Medium wie beispielsweise Kupfer ist die Laufzeit eines Signals länger, als dies bei einem Lichtstrahl im Vakuum der Fall ist. Die Nominal Velocity of Propagation (NVP) gibt das relative Verhältnis der Laufzeit auf einem Medium gegenüber der Laufzeit von Licht im Vakuum an. Die typische Ausbreitungsgeschwindigkeit eines Signals liegt auf Kupferleitungen etwa bei 60 % bis 80 % der Lichtgeschwindigkeit. Ein NVP von beispielsweise 0,78 gibt an, dass die Ausbreitungsgeschwindigkeit auf dieser Leitung 78 % der Lichtgeschwindigkeit beträgt. NVP-Werte können Sie direkt vom jeweiligen Kabelhersteller unter Angabe des Kabeltyps erfragen. Die Vorgabe des NVP-Wertes ist wichtig für eine genaue Längenmessung. Falsche NVP-Werte würden die Messwerte direkt proportional verfälschen.

Damit eine exakte Angabe des NVP-Wertes erfolgen kann, können Sie auch eine Referenzmessung erstellen. Zu diesem Zweck verwenden Sie eine feste Teillänge des TP-Kabels, welches zu messen ist. Rollen Sie mindestens 30 Meter, besser 40 Meter von der entsprechenden Trommel ab und schließen Sie an die Enden eine entsprechende Anschlussdose an. Dann wählen Sie bei Ihrem LAN-Messgerät den Menüeintrag NVP ERMITTeln und geben die entsprechende Teilstrecke in Metern an. Das Messgerät prüft anhand dieser Angaben die Signallaufzeit und gibt Ihnen am Display den passenden NVP-Wert aus.

NVP einstellen

Bei den eingestellten Mess-Standards wird jeweils ein vorgegebener Wert für den NVP verwendet. Haben Sie den genauen Wert für den NVP von Ihrem verlegten Datenkabel, so sollten Sie diesen über einen Menüeintrag auf Ihrem Messgerät entsprechend ändern.

Autotest

Die Autotest-Funktion führt einen Testlauf unter Beachtung der vorprogrammierten Grenzwerte der geltenden Verkabelungsstandards aus. Als Resultat der einzelnen Tests wird ein Gesamtergebnis mit *OK* oder *FEHLER* angezeigt. Mit der Autotest-Funktion werden beispielsweise bei einem modernen Tester folgende Messungen ausgeführt:

- | | |
|---|--|
| ✓ Verdrahtung | ✓ Rückflussdämpfung |
| ✓ DC-Schleifenwiderstand | ✓ Impedanz (optional) |
| ✓ Länge (informativ) | ✓ Laufzeit |
| ✓ Kapazität (optional) | ✓ Berechnung der Laufzeitunterschiede |
| ✓ Dämpfung | ✓ PS ACR-F (Power Sum ACR-F) |
| ✓ Dual NEXT | ✓ PS ACR-N (Power Sum ACR-N) |
| ✓ Berechnung des ACR-N
(engl. Attenuation Crosstalk Ratio) | ✓ PS NEXT (Power Sum NEXT) |
| | ✓ Berechnung des ACR-F (engl. Attenuation Crosstalk Ratio Far-end) |

Die Autotest-Funktion kann so eingestellt werden, dass die ermittelten Testergebnisse automatisch abgespeichert werden. Um einen bereits bestehenden Messwert zu überschreiben, ist auch eine manuelle Speicherung der Ergebnisse möglich.

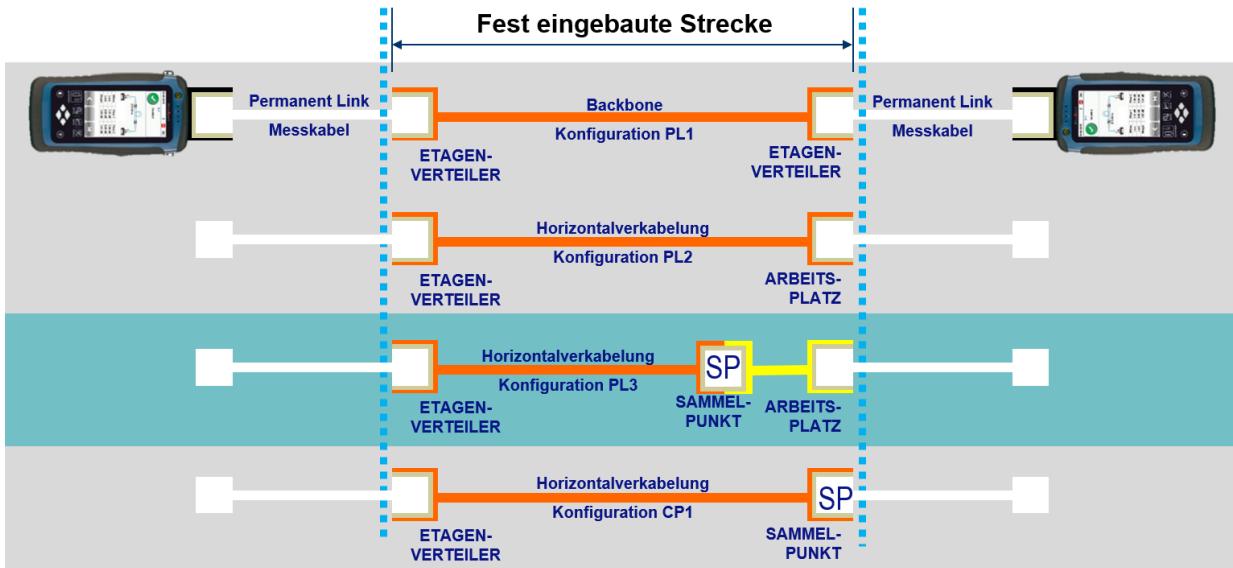
Autotest einstellen

Wählen Sie bei Ihrem Messgerät die Funktion Autotest. Der Autotest ist die einfachste und schnellste Methode zur Messung und Kontrolle Ihrer Verkabelungssysteme. Denken Sie aber daran, unbedingt einen Feld-Nullabgleich durchzuführen, bevor Sie mit der Messreihe beginnen.

Da es nicht für alle Verkabelungen erforderlich ist, die gesamten unter Autotest programmierten Testreihen auszuführen, haben Sie auch die Möglichkeit, die Testreihe für den Autotest individuell anzupassen, einzelne Testparameter abzuwählen bzw. Grenzwerte abzuändern. Bei den gängigsten Gebäudeverkabelungen ist dies aber nicht notwendig.

Permanent Link

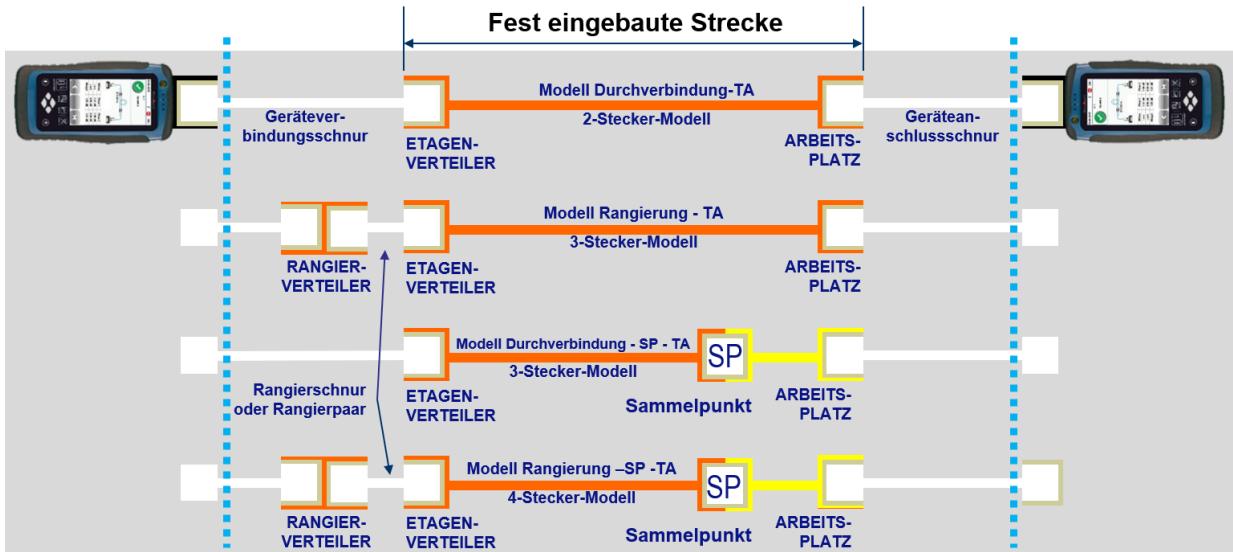
Beim Permanent-Link-Modell wird lediglich der Verkabelungsabschnitt von der Anschlussdose bis hin zum Verteilerfeld gemessen. Dieser Abschnitt besteht normalerweise aus einem installierten Etagenkabel von bis zu 90 Metern Länge (Richtwert). Einzig ein sogenannter Sammelpunkt (Consolidation Point) kann noch in der Datenstrecke quasi als Unterverteilung eingebaut sein. Gemessen wird lediglich mit einem Messgerätekabel vom Patchfeld bzw. von der Anschlussdose bis zum Messgerät.



Permanent-Link-Messung

Channel Link

Das Channel-Link-Modell berücksichtigt alle Komponenten einer Datenstrecke. Es besteht aus einem installierten Etagenkabel von bis zu 90 Metern Länge (Richtwert) und den angeschlossenen Patch- bzw. PC-Kabeln. Es können noch Rangierverteiler und Sammelpunkte (Consolidation Points) in der Datenstrecke eingebaut sein. Die Länge der Gesamtstrecke, Etagenkabel plus Geräte- und Patchkabel, sollte eine Gesamtlänge von 100 Metern nicht überschreiten.



Channel-Link-Messung

Nullabgleich

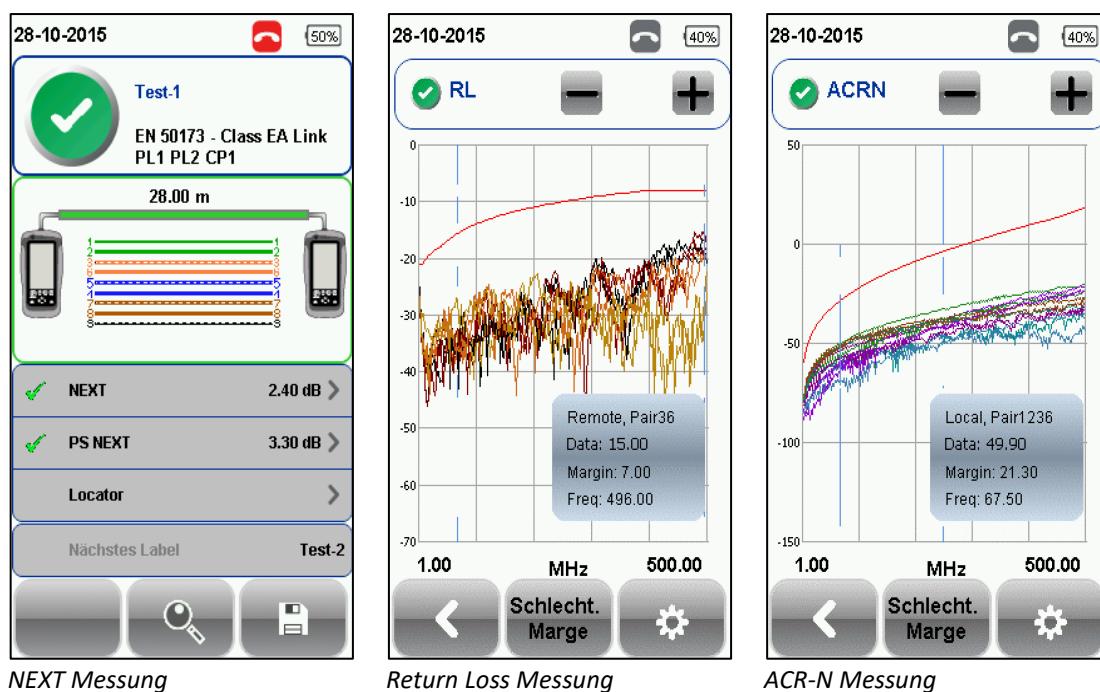
Beim Nullabgleich wird die Sende- und Empfangselektronik von Handgerät und Endgerät elektronisch synchronisiert. Zu diesem Zweck werden Handgerät und Endgerät miteinander verbunden. Anschließend wird über einen Menüeintrag im Handgerät der Nullabgleich gestartet. Bei einem erfolgreichen Abgleich kann anschließend die Messreihe erstellt werden. Bei einigen modernen Testern wird der Nullabgleich auch zur Charakterisierung der verwendeten Messkabel verwendet, um sowohl Permanent- als auch Channel-Link-Messungen mit demselben Messaufbau durchführen zu können. Damit optimale Messergebnisse erzielt werden, sollten Sie vor jeder Messreihe einen Nullabgleich durchführen. Neuere Messgeräte fordern den Benutzer bereits beim Einschalten zu einem Nullabgleich auf.

Vorbereitungen durchführen

- ▶ Wählen Sie im entsprechenden Menü des LAN-Messgerätes den zu testenden Verkabelungstyp, die Topologie und den Mess-Standard aus, zum Beispiel *ISO Class F STP Perm*. Das Messgerät übernimmt die dazugehörigen Messparameter und Grenzwerte.
- ▶ Ändern Sie den Wert für NVP so ab, dass er mit den Herstellerangaben oder Ihrer Referenzmessung übereinstimmt.
- ▶ Stellen Sie bei Ihrem Messgerät die Funktion Autotest ein.
- ▶ Führen Sie unmittelbar vor der Messung am Messort einen Nullabgleich des LAN-Messgerätes durch.

Link-Messung auswerten

Die Messung mit einem LAN-Zertifizierer kann grafisch auf dem Gerät oder mithilfe einer Auswerte-Software als professioneller Testbericht dargestellt werden.



Als Ergebnis für eine Link-Messung wurden exemplarisch NEXT, RL und ACR-N dargestellt. NEXT beschreibt die elektromagnetische Kopplung zwischen den Adernpaaren (Nebensprechen). Eine NEXT-Messung wirkt nur 30–40 m in das Kabel hinein, daher muss die Messung an beiden Kabelenden durchgeführt werden, um eine Aussage zum NEXT zu treffen. Bei Kabellängen <20m (Short Link) treten jedoch verfälschte Messergebnisse auf.

Die Rückflussdämpfung (Return Loss -RL-) zeigt das Maß für die Gleichmäßigkeit der Impedanz auf der Übertragungsstrecke und ermittelt die Signalreflektion bei Impedanzänderungen. Es dient als Kriterium für die exakte Verlegung des Kabels. Das Dämpfungs-Nahnebensprechdämpfungs-Verhältnis (Attenuation Crosstalk Ratio Near End -ACR-N-) ermittelt das Verhältnis zwischen Nutz- und Störsignal. Es wird auch als Signal-/Rauschverhältnis bezeichnet.

6.6 Messgeräte für Glasfasern

Die Ausbreitung optischer Signale auf einem Lichtwellenleiter wird überwiegend durch **Dämpfung** beeinflusst. Ursachen für die Dämpfung in einem Lichtwellenleiter sind Absorption, die physikalisch reduzierbare Rayleigh-Streuung und Strahlungsverluste von optischer Energie. Die Absorption bezieht sich auf das Glasfasermaterial, während die Streuung sowohl mit dem Glasfasermaterial als auch mit Strukturierungsgenauigkeiten im Lichtleiter zusammenhängt. Damit eine Übertragungsstrecke aus Glasfaser beurteilt werden kann, sind auch hier Messungen der Eigenschaften von Lichtwellenleitern erforderlich.

Die erzielten Resultate bei Messungen an Glasfaserstrecken sind stark von den vom Anwender getroffenen Maßnahmen abhängig. Sie sollten sehr sorgfältig und sauber mit den optischen Fasersystemen umgehen.



Die notwendigen Prüf- und Messverfahren sind u. a. in der DIN EN 61300-3-35 „Lichtwellenleiter-Verbindungs-elemente und passive Bauteile“ und der DIN EN 61280-4-1 „Prüfverfahren für Lichtwellenleiter-Kommunikations-untersysteme“ hinterlegt. Die Funktionsprüfung von Glasfaserstrecken kann generell wie folgt eingeteilt werden:

- ✓ einfache Durchgangsprüfung
- ✓ optische Rückstremessung (**optical time domain reflectometry / OTDR**)
- ✓ Dämpfungsmessung

Mitunter zur Prüfung verwendete Laserpointer und LED-Taschenlampen eignen sich grundsätzlich nicht zur Messung und lassen keine Aussage zur Funktionsfähigkeit zu. Die Prüfung von Singlemodefasern ist mit diesen Mitteln völlig unmöglich.

Geeignete Prüfmittel

Die optische Durchgängigkeit (Ende-zu-Ende-Durchgangskontrolle) der Faser wird z. B. mit einem Visible Fault Finder überprüft. Dazu wird ein Laser im Rotlichtbereich (650 nm) verwendet. Der Tester kann für Prüfungen an Multi-mode- bzw. Singlemodefasern genutzt werden. Für die verschiedenen Stecker-geometrien besitzt der Tester Adapter. Ein universeller 2,5-mm-Adapter ermöglicht die einfache Verbindung an einen SC-, ST-, FC- und FJ-Stecker. Ein 1,25-mm-Adapter wird für den Anschluss an einem LC- und MU-SFF-Stecker genutzt.



Visible Fault Finder

Reinigung

Bevor Sie mit der Messung beginnen, müssen messwertbeeinflussende Parameter ausgeschlossen werden. Vor der **Reinigung** sollte mittels eines Videomikroskops der Verschmutzungsgrad der Anschlüsse erfasst werden. Erst danach kann die Reinigung erfolgen. Dazu sollten Sie eine Reinigungskassette verwenden. In ihr finden Sie u. a. Tupfer für die 1,25mm- und 2,5mm-Anschlüsse, Reinigungswürfel bzw. Tücher und ein alkoholfreies Lösungsmittel für die Feuchtreinigung. Die Reinigung muss senkrecht zur Anschlussfläche erfolgen. Die Trockenreinigung wird mit OneClick Cleaner vorgenommen. Alle Reinigungsmaterialien müssen fusselfrei und dürfen nicht elektrostatisch aufladbar sein. Nur so kann eine optimale Feucht- und/oder Trockenreinigung der Anschlüsse erreicht werden.



Reinigungskassette

Prüfen Sie nach Abschluss der Arbeiten die Endflächen (bzw. die Anschlüsse) der Glasfaser erneut mit dem Videomikroskop, um sicherzustellen, dass alle Verunreinigungen beseitigt sind. Wenn die Flächen immer noch verunreinigt sind, wiederholen Sie den Reinigungsvorgang, bis die Flächen vollständig sauber sind.

Überprüfung der LWL-Installation mittels Videomikroskop

Eine rein optische bzw. videotechnische Überprüfung von LWL-Anschlüssen erfolgt über ein **Videomikroskop**. Es verfügt über Adapter, um alle gängigen Anschlüsse verifizieren zu können. Eine Panelsonde erlaubt auch die Begutachtung des in der Kupplung befindlichen Steckers.

Dies ist heute Standard bei der Abnahme und auch als Norm IEC 61300-3-35 hinterlegt. Die Mikroskope sind entweder Stand-Alone-Geräte bzw. mit USB-Anschluss verfügbar, um die Anzeige über das Display eines Notebooks oder Tablets vorzunehmen oder zu Dokumentationszwecken aufzuzeichnen.



OTDR5000 als Videomikroskop

Spezielle Laserquellen

Laserquellen finden ihre Anwendung bei der Installation, Wartung und Fehlersuche in faseroptischen Netzwerken. Die Laserlichtquelle zeichnet sich durch einen Laserstrahl mit 635 nm aus. Der Vorzug gegenüber anderen Geräten ist die deutlich bessere Sichtbarkeit des Lichts bei dieser Wellenlänge. Das Licht tritt aus der Faser aus, wenn der Durchgang an einer Stelle gestört ist, was beispielsweise bei Faserbrüchen oder zu starken Biegeradien der Fall ist. Ein Faserbruch kann mit diesen speziellen Laserquellen auch noch in einer Entfernung von mehr als 3 Kilometern schnell und einfach ermittelt werden. Dies ist jedoch davon abhängig, ob sich die Faser in einer Spleißbox oder in einem Mantel befindet.



Die Verwendung von **Halbleiter-Lasern** in faseroptischen Messinstrumenten wird durch verschiedene Sicherheitsnormen geregelt. Vermeiden Sie es, direkt in die Laserquelle zu schauen, da eine dauerhafte Schädigung der Netzhaut die Folge sein kann.

6.7 Optische Rückstreumessung (OTDR)

Grundlagen der optischen Rückstreumessung

Die **optische Reflektometrie** ist ein Verfahren zum Messen und Testen von Lichtwellenleitern. Mit dem Optical-Time-Domain-Reflectometry-Verfahren (OTDR) können die übertragungstechnischen Eigenschaften von Lichtwellenleitern gemessen und analysiert werden. So liefert die Rückstreumessung eine Aussage über die Dämpfung, den Dämpfungsbelag (dB/km), über Störstellen (Stecker, Spleiße), deren Dämpfung und Lage sowie über die Streckenlänge.

Bei der **OTDR-Messung** wird ein Lichtimpuls von der Quelle des OTDR-Gerätes in die Glasfaser eingespeist. Dieser eingespeiste Lichtimpuls wird innerhalb der Glasfaser rückgestreut. Besonders ausgeprägt sind die Reflexionen an Kabelbrüchen, Spleißen, LWL-Steckern und Adapters. Die an der Störstelle reflektierte Lichtleistung wird zum OTDR-Messgerät zurückreflektiert und vom Messgerät erfasst und ausgewertet. Aus der Laufzeit des ausgestreuten Lichtimpulses und seiner Reflexion kann unmittelbar auf den Fehlerort geschlossen werden. Aufgrund der Kurvendarstellung eines eingekoppelten Lichtimpulses ist es möglich, eine Aussage auf einen möglichen Fehler an der Übertragungsstrecke zu treffen. An vorhandenen Spleißstellen entstehen beispielsweise erhöhte Dämpfungen. Bei Kabelquetschungen oder fehlerhaften Verbindungen, wie dies beispielsweise bei Steckern der Fall ist, entstehen höhere Reflexionen.

Die **Pulsbreite** ist einer der Einstellparameter beim OTDR. Je nach Wahl erzielt man entweder eine hohe Auflösung eng beieinander liegender Ereignisse oder eine hohe Reichweite. Im Multimode-Bereich arbeitet man mit Pulsbreiten unter 300 ns, da die Längen selten größer als 3 km sind. Mit Singlemode-OTDRs können mit einer Pulsbreite von 10 -30 µs, abhängig von der Dynamik des OTDRs Fasern weit über 100 km, ja sogar bis 200 km gemessen werden.

Pulsbreite	Auflösung
10 µs	1 km
1 µs	100 Meter
100 ns	10 Meter
1 ns	10 cm

OTDRs sind heute Multifunktionsgeräte und häufig modular aufgebaut, was bedeutet, dass je nach Anwendung unterschiedliche Module eingesetzt werden. Nebenstehendes Bild zeigt ein modulares Gerät, geeignet für die Messung von Multimode- und Singlemodefasern.



OTDR-Messgerät

Physikalisches Prinzip der Rückstreumessung

Die **Rückstreumessung** nutzt zwei grundlegende physikalische Prinzipien:

- ✓ die Rayleighstreuung
- ✓ die Fresnelreflexionen

Die Rückstreuung des gesendeten Lichtimpulses an der atomaren Struktur der Glasfaser (SiO_2) wird **Rayleighstreuung** genannt. Dabei wird ein Teil des gestreuten Lichtes wieder in der Faser zurückgeführt und dient als Messgröße für das OTDR.

Fresnelreflexionen entstehen an Unstetigkeiten der Brechzahl entlang der Strecke. Physikalisch ist hier das amorphe Material an der gesteckten Faser völlig anders orientiert, und daher entsteht eine verhältnismäßig hohe Reflexion, die zudem noch fast vollständig in der Faser zurückgeführt wird. Im OTDR-Diagramm ist die Höhe des Peaks ein Maß für die Größe der Rückreflexion. Ein offener Stecker und somit ein Glas-Luft-Übergang generiert den größten Wert (ca. -14 dB).

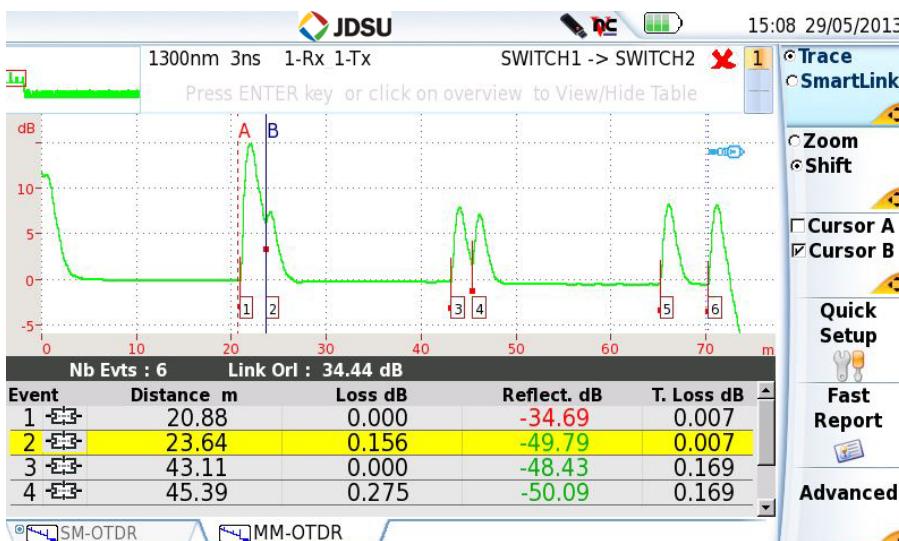
Kurvendarstellung

In der grafischen Darstellung einer OTDR-Kurve wird auf der Vertikalachse die Dämpfung in dB und in der Horizontalachse die Entfernung in Metern dargestellt. Spleißverbindungen erzeugen, ebenso wie starke Faserbiegungen, erhöhte Dämpfungswerte. Faserbiegungen sowie Spleiße werden in der OTDR-Kurve durch einen Sprung in der Grafik dargestellt.

Bei Steckern mit einem Luftspalt wird die entsprechende Lichtleistung an der Übergangsstelle stark reflektiert. Wegen dieser überhöhten Lichtleistung ist der Kurvenverlauf einer OTDR-Messung typischerweise als kurzer Spitzenwert dargestellt.

Die Faserenden einer offenen Glasfaserstrecke werden an der Übergangsstelle zum Medium Luft reflektiert. Wurde das Faserende bereits mit einem Faserbrechwerkzeug entsprechend bearbeitet, lässt sich dies durch eine kleine Spitze am Faserende bei Schrägschliffsteckern erkennen. Bei einem unbearbeiteten Faserende treten kaum Reflexionen auf. Der Übergang von Faserende in das Medium Luft wird als Rauschen dargestellt.

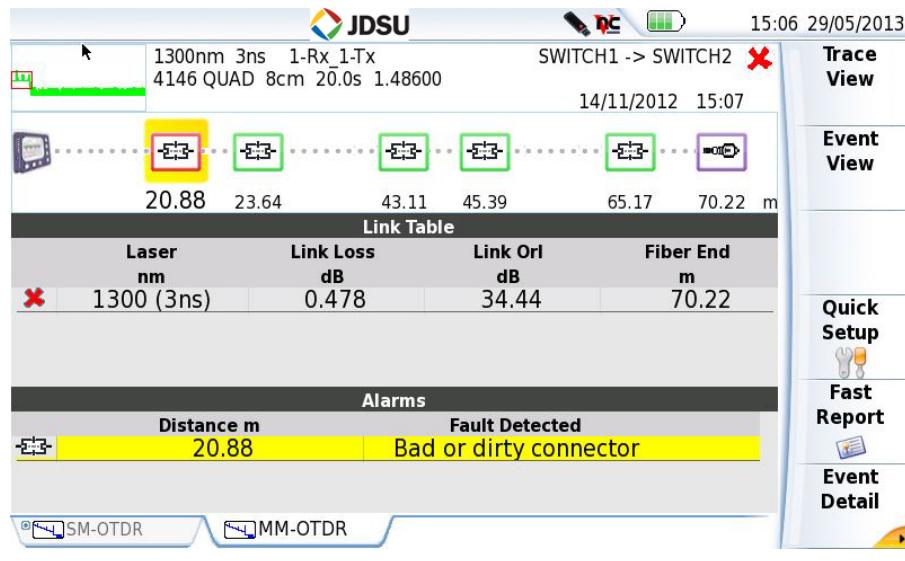
Das nachfolgende Bild zeigt ein Ergebnis bei einer sehr kurzen Multimodefaser.



Ergebnis einer OTDR-Messung an einer Multimodefaser

Die gesamte Faserlänge beträgt hierbei ca. 70 m, und es befinden sich drei Patchkabel darin. Gemessen wurde bei der Wellenlänge $\lambda=1300$ nm mit einer Pulsbreite von 3 ns. In der Tabelle werden jeweils aufgeführt die Entfernung des Ereignisses, dessen Dämpfung und Reflexionsgrad. Die Gesamtdämpfung ist beim Ereignis 6 in der Spalte T. Loss zu finden. Zur einfacheren Beurteilung des Ergebnisses wurden im Vorfeld Grenzwerte, hier nur für den Reflexionsgrad festgelegt. Steckverbindung 1 verletzt diesen Grenzwert, daher wird dieser Wert in Rot dargestellt.

Um die Abnahmemessung noch übersichtlicher zu gestalten, wird die Kurve in sogenannte Icons „übersetzt“. Deshalb kann die Glasfaser noch wesentlich schneller beurteilt werden, und es werden sogar Hinweise auf eine mögliche Fehlerursache gegeben.



Abnahmemessung mit ICON-Darstellung

Informationsgehalt der Messungen

Der Informationsgehalt der gemessenen Glasfaserstrecke sollte Folgendes beinhalten:

- ✓ die Dämpfung
- ✓ eine Lokalisierung von Störstellen durch Angabe der Entfernung
- ✓ die Ermittlung der gesamten Streckenlänge

Vorlauffaser – Nachlauffaser

Eine **Vorlauffaser** ist eine spezielle Faser, welche bei einer OTDR-Messung vor die Messstrecke geschaltet wird. Der Vorteil dieses Verfahrens liegt darin, dass der erste LWL-Stecker einer LWL-Verbindung bereits eindeutig gemessen werden kann, ohne dabei vom Anschlussstecker des OTDR-Gerätes beeinflusst zu werden. Die Vorlauffasern sollten bei Messungen von Multimodefasern etwa 100 m lang sein. Ebenso wie eine Vorlauffaser gibt es auch eine Nachlauffaser, die der Messstrecke nachgeschaltet wird, um damit eine eindeutige Messung am Faserende zu ermöglichen.

6.8 Dämpfungsmessung

Dämpfungsmessung bei Glasfaserkabeln

Bei einer **Dämpfungsmessung** werden die tatsächlichen Verluste einer Glasfaserstrecke gemessen. Die Dämpfungsmessung liefert eine Aussage über die Qualität der optischen Eigenschaften einer Glasfaserstrecke. Für die Durchführung von Dämpfungsmessungen werden spezielle Geräte eingesetzt. Faseroptische Dämpfungssets bestehen aus einem optischen Leistungsmessgerät und einer optischen Lichtquelle.

Lichtquelle

Die Sendeeinheit eines Dämpfungsmessgerätes besteht aus einer konstanten Lichtquelle und verfügt normalerweise über zwei Ausgänge (850 nm und 1300 nm) für Multimode-Fasermessungen.

Höherwertige Dämpfungsmessgeräte verfügen zusätzlich noch über Lichtquellen mit 1310 nm und 1550 nm für Monomode-Messungen.

Die gesendete Lichtleistung ist von den Umgebungsverhältnissen wie Temperatur und Luftfeuchtigkeit abhängig, welche jedoch durch die Geräte kalibriert werden können.



Optischer Sender und Empfänger

Leistungsmessgerät

Leistungsmessgeräte empfangen die von der Lichtquelle gesendete optische Leistung und vergleichen diese mit dem Wert einer Referenzmessung. Das Resultat zwischen Sendeleistung und empfangener Leistung ist die tatsächliche Dämpfung der Glasfaserstrecke in dB.

Leistungsmessgeräte sind in der Lage, die gemessenen Werte in einem Zwischenspeicher abzulegen. Je nach Ausführung können Hunderte von Messungen gespeichert werden. Das Auslesen der Werte kann mittels Software-tools über die RS-232- oder USB-Schnittstelle erfolgen.

Messkabel

LWL-Messkabel sind herkömmliche Anschlusskabel, wie beispielsweise Patchkabel. Es ist jedoch darauf zu achten, dass die verwendeten Messkabel den gleichen Kerndurchmesser (bei Multimodefaser, sowie den gleichen Modenfelddurchmesser bei Monomodefaser) wie die zu messende Strecke besitzen. Für die Durchführung von Dämpfungsmessungen sollten Sie für jeden gängigen Steckertyp und Faserdurchmesser einen Satz Kabel in Ihrem Servicekoffer zur Verfügung haben.

Normen für die Dämpfungsmessung

Die Bestimmungen für die Dämpfungsprüfung bei Multimode-Glasfaserkabeln sind im ANSI/TIA/EIA-526-14A-Standard (bei Multimodefaser) und ANSI/TIA/EIA-526-7-Standard (bei Monomodefaser) festgelegt. Dieser Standard sieht zwei grundsätzliche Prüfverfahren vor:

- ✓ Methode A.1
- ✓ Methode B

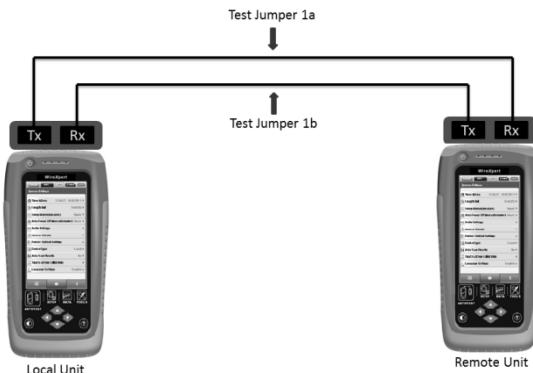
Methode A.1

Bei der **Methode A.1** erfolgt eine **Dämpfungsmessung** für Glasfaserstrecken, ohne jedoch die entsprechenden Verluste, welche durch Verbindungselemente hervorgerufen werden, zu berücksichtigen. Um eine Aussage über die Glasfaserverbindung zu treffen, werden bei der Methode A.1 zwei LWL-Patchkabel (je Seite) sowie zwei Adapterstücke benötigt. Vor der eigentlichen Messung werden die Dämpfungswerte der beiden Patchkabel sowie der Adapterstücke bestimmt. Als Testergebnis erhalten Sie den Dämpfungswert der entsprechenden Glasfaserstrecke. Allerdings beinhaltet das Messergebnis nur einen Anschluss der Verbindungsstrecke.

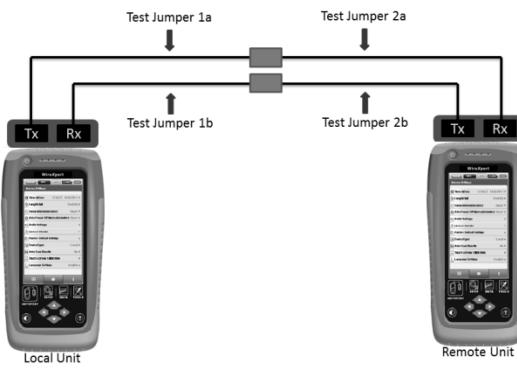
Diese Methode ist besonders für die Dämpfungsmessung von Weitverkehrsverbindungen geeignet. Bei längeren Distanzen wird die Dämpfung in einer Glasfaser hauptsächlich durch die eigentliche Faser und nicht durch die Anschlüsse verursacht. Bei einer strukturierten Gebäudeverkabelung hingegen ist diese Messmethode nicht genau. In Gebäudenetzwerken sind die Übertragungsstrecken relativ kurz. Für die Ermittlung der Gesamt-dämpfung einer Glasfaserverbindung in Gebäuden ist es erforderlich, dass alle Anschlüsse in das Messergebnis mit einbezogen werden, da bei kurzen Verbindungsstrecken die Dämpfung überwiegend durch die Verbindungs-elemente verursacht wird.

Methode B

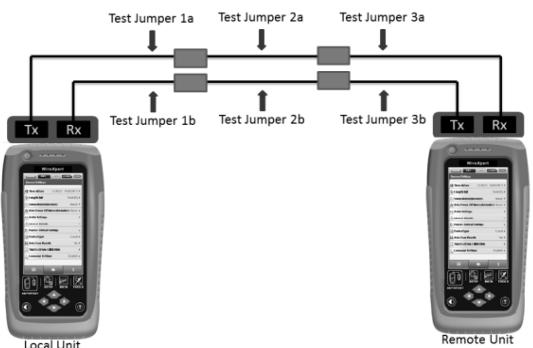
Mit der **Methode B** werden überwiegend **Glasfaserverbindungen** gemessen, bei denen die Dämpfung hauptsächlich durch die Steckeranschlüsse entsteht. Da bei der Methode B hauptsächlich die Dämpfung der beiden Enden einer Glasfaserstrecke berücksichtigt wird, eignet sich diese besonders für Dämpfungsmessungen in Gebäudenetzwerken. Eine umfangreiche Referenz ist in der nachfolgenden Tabelle dargestellt. Die Messungen erfolgen entweder mit ein/zwei oder drei Referenzkabeln und dazugehörigen Adapters. Die aktuelle Normung sieht die Messung mit drei Referenzkabeln vor.



Ein-Jumper-Messung mit einem Patchcord



Zwei-Jumper-Messung mit 2 Patchcords + Adapter



Drei-Jumper-Messung mit 3 Patchcords + 2 Adapters

Verfahren	IEC 14763-3	IEC 61280-4-1 (Multimode)	IEC 61280-4-2 (Monomode)	TIA-526-14A (Multimode)	TIA-526-7 (Monomode)
Ein-Jumper Messung	eine Kabelmessung	Methode 2	Methode A1	Methode B	Methode A.1
Zwei-Jumper Messung	-	Methode 1	Methode A2	Methode A	Methode A.2
Drei-Jumper Messung	drei Kabelmessungen	Methode 3	Methode A3	Methode C	Methode A.3

Weitere Informationen zu den Messverfahren von Lichtwellenleitern finden Sie hier:

- ✓ <http://webshop.atlantiksysteme.de/media/products/FOT-Guide.pdf>
- ✓ <http://www.lwltechnik.de/files/elementare-messverfahren-probe.pdf>
- ✓ <https://www.mittelstandswiki.de/wissen/LWL-Verkabelung>
- ✓ https://www.cabling.datwyler.com/fileadmin/mediapool/userfiles/download/white_papers_2013/Datwyler-WP-FO-Verkabelung.pdf
- ✓ <https://www.ip-insider.de/testmethoden-fuer-glasfaser-verbindungen-a-595905/>

6.9 Übungsszenario: Dämpfungsmessung durchführen

Im Unternehmen wurden Umbauarbeiten am DV-Schrank durchgeführt. Unter anderem wurde das Glasfaser-Patchpanel ausgebaut und im Anschluss an die Umbauarbeiten erneut eingebaut. Die Aufgabe besteht darin, alle acht Glasfaseranschlüsse ausgehend von diesem DV-Verteilerschrank zum Wandverteilerschrank im Schulungsraum auf Durchgängigkeit zu prüfen. Die Überprüfung soll anhand einer Dämpfungsmessung erfolgen.

Erforderliches Material und Prüfmittel

Bei der Durchführung einer optischen Dämpfungsmessung benötigen Sie folgende Geräte beziehungsweise Materialien:

- ✓ optische Lichtquelle
- ✓ optisches Leistungsmessgerät
- ✓ LWL-Kupplung (baugleich mit einer Kupplung der zu messenden Strecke)
- ✓ LWL-Patchkabel (Kerndurchmesser muss identisch mit dem Durchmesser der zu messenden Strecke sein)

Lichtquelle und Leistungsmesser anschließen

- Schalten Sie die optische Lichtquelle und den optischen Leistungsmesser ein und warten Sie ca. eine Minute, damit sich die Elektronik bzw. die Lichtquelle kalibriert hat. Bei rauen Umgebungsverhältnissen wie beispielsweise beim Einsatz im Außenbereich sollten Sie ggf. etwas länger warten.

Referenzwert ermitteln und speichern

- Verbinden Sie das LWL-Patchkabel mit dem Leistungsmesser und mit der Lichtquelle über das entsprechende Kupplungsstück.
- Am Endgerät mit Display sehen Sie nun einen Leistungswert in der Anzeige. Speichern Sie diesen ermittelten Wert mit der entsprechenden Taste oder Tastenkombination als Referenz. Durch den Tastendruck wird dann auf den relativen dB-Wert gesetzt.

Der Referenzwert beinhaltet die Dämpfungswerte der Anschlusskabel und ist Ihre Grundlage für alle nachfolgenden Messreihen. Der so gemessene Referenzwert legt die nachfolgenden Messungen sozusagen auf ein Niveau, bei welchem Ihre verwendeten Patchkabel und das Kupplungsstück nicht berücksichtigt sind.



Aufbau für Referenzmessung

Dämpfungswert der Glasfaserstrecke messen

- Nehmen Sie die Lichtquelle und schließen Sie diese an den LWL-Port der zu messenden Glasfaserstrecke an. Der optische Leistungsmesser wird an das andere Ende der Glasfaserstrecke angeschlossen. Der nach Messende im Display angezeigte Wert entspricht dem Dämpfungswert Ihrer Übertragungsstrecke.

Ursachen für zu hohe Dämpfungswerte

Wenn die Dämpfung einen zu hohen Wert anzeigt, kann das verschiedene Ursachen haben. Im Wesentlichen sollten Sie in solch einem Fall Folgendes beachten:

- ✓ Reinigen Sie vor der Messung alle Stecker Ihrer Messkabel z. B. mit einem Reinigungsstift oder einer Reinigungsbandkassette.
- ✓ Verwenden Sie nur die vom Hersteller vorgegebenen Messkabel inkl. deren Referenzstecker.
- ✓ Überprüfen Sie, ob die LWL-Stecker gut in der Kupplung einrasten (dies gilt auch für die Pigtail-Seite).
- ✓ Tauschen Sie nötigenfalls die LWL-Anschlusskabel (Kupplung) aus.
- ✓ Wurden Billigstecker (Kupplungen) verwendet?
- ✓ Stimmen die Kerndurchmesser der Messkabel mit dem Stammkabel überein (beide 50 µm bzw. 62,5 µm)?
- ✓ Bei Lichtquellen mit 850 nm sind die gemessenen Werte meistens niedriger als beispielsweise bei 1300 nm.
- ✓ Wurde das Glasfaserkabel sauber verlegt? Gibt es starke Knickstellen?

Wiederholen Sie die Dämpfungsmessung für jede zu prüfende Glasfaserstrecke. In der Aufgabenstellung sind hierfür acht Messungen erforderlich. Bedenken Sie aber, dass eine Dämpfungsmessung bei Multimodefasern von beiden Seiten zu erfolgen hat. Nur so kann eine definitive Aussage über die Funktionalität respektive Qualität der Übertragungsstrecke getroffen werden. Bei Monomodefasern ist die Messung in einer Richtung ausreichend, da es keine richtungsabhängigen Dämpfungseffekte gibt.

6.10 Übung

Fragen zu Messgeräten

Übungsdatei: --

Ergebnisdatei: uebung06.pdf

1. Worauf sollten Sie beim Einsatz eines Messgerätes achten? Nennen Sie drei Aspekte und stellen Sie jeweils die wichtigsten Fragen.

7 Installationsrichtlinien für die Verkabelung

In diesem Kapitel erfahren Sie

- ✓ welche Normen Sie bei einer strukturierten Verkabelung einhalten müssen
- ✓ wie die Einteilung für eine strukturierte Verkabelung erfolgt
- ✓ welche Richtlinien Sie für Kupferkabel einhalten sollten
- ✓ welche Richtlinien Sie für Glasfaserkabel einhalten sollten

Voraussetzungen

- ✓ Wissen über den Aufbau von Verkabelungen
- ✓ Wissen über den Aufbau von Datenkabeln
- ✓ Wissen über die Eigenschaften von Glasfaserkabeln

7.1 EN 50173 und weitere Standards

Allgemeines über die Norm EN 50173

Eine anwendungsneutrale (von den zu nutzenden Diensten unabhängige) und strukturierte Verkabelung ist heutzutage für ein Unternehmen genauso erforderlich und wichtig wie beispielsweise Stromversorgung oder Heiztechnik. Damit eine anwendungsneutrale Verkabelung einheitlich durchgeführt werden kann, wurden in der EN 50173 entsprechende Vorgaben für diesen Verkabelungsstandard entwickelt.

In Europa wurde diese Norm im März 1994 unter der Bezeichnung **EN 50173** als strukturierte, anwendungsneutrale Gebäudeverkabelung veröffentlicht. Da bis zum damaligen Jahreswechsel kein Widerspruch einging, wurde diese Norm im Juli 1995 von der CENELEC (Comité Européen de Normalisation Électrotechnique) verabschiedet.

Bedingt z. B. durch Weiterentwicklungen im Bereich Ethernet (Stichwort „Gigabit“) war bereits Ende 1999 absehbar, dass Erweiterungen der Norm nötig werden würden. Dies führte in den Folgejahren zu den Neuauflagen EN 50173:2000, EN 50173:2003 bis zur aktuellen Version EN 50173:2011. Im Wesentlichen wurden dabei die Link-Klassen D (bis 100 MHz) überarbeitet und die Link-Klassen E (bis 500 MHz) und F (bis 1000 MHz) modifiziert. Parallel dazu wurden die Anforderungen an Kabel der Kategorie 6A, 7A und 8 festgelegt sowie neue LWL-Kabelspezifizierungen in die Norm integriert.

Inzwischen stellt die EN 50173 eine sechsteilige Normenserie dar, die zuletzt im Oktober 2018 geändert wurde. Sie enthält verschiedene Anwendungsszenarien im Verkabelungsbereich:

- ✓ EN 50173-1: Teil 1: Allgemeine Anforderungen
- ✓ EN 50173-2: Teil 2: Bürobereiche
- ✓ EN 50173-3: Teil 3: Industriell genutzte Bereiche
- ✓ EN 50173-4: Teil 4: Wohnungen
- ✓ EN 50173-5: Teil 5: Rechenzentrumsbereiche
- ✓ EN 50173-6: Teil 6: Verteilte Gebäudedienste (z. B. Gebäudeautomation und Gebäudeleittechnik, Sicherheitstechnik, Funkanbindung, Video, Schwesternruf, sonstige Überwachung)

Das Deutsche Institut für Normung (DIN) übernimmt im Allgemeinen inhaltlich auch Europanormen und schreibt zur Gültigkeit der Normen auf ihrer Webseite: „DIN-Normen werden spätestens alle fünf Jahre auf Aktualität überprüft. Entspricht eine Norm nicht mehr dem Stand der Technik, so wird ihr Inhalt überarbeitet oder die Norm zurückgezogen.“ Daher ist es stets notwendig zu prüfen, welche Version einer Norm zum Zeitpunkt der Betrachtung zur Anwendung kommen muss.

Allgemein soll diese Normung eine Planungssicherheit für mehrere Jahre und für alle gewünschten Dienste liefern. Im Kern beinhaltet sie dabei eine Dreiteilung der Verkabelungsstruktur in einen primären, sekundären und tertiären Bereich.

Die EN 50173 definiert:

- ✓ ein anwendungsneutrales Verkabelungssystem, das herstellerunabhängig ist und universell eingesetzt werden kann
- ✓ eine Verkabelungsstruktur, bei der sich nachträgliche Änderungen mit überschaubarem und geringem Mehraufwand durchführen lassen
- ✓ eine theoretische Grundlage, die bereits vor der eigentlichen Installation als Planungshilfe und als Leitfaden bei der Projektierung verwendet werden kann
- ✓ eine Normung für alle Segmente, die anhand dieser Vorgaben ihre Entwicklungen für die Verkabelungssysteme gezielt durchführen können

Anwendungsbereich

In der EN 50173 wird ein universell einsetzbares Verkabelungssystem definiert, das sowohl für einzelne Gebäude als auch für Gebäudekomplexe verwendet werden kann. Berücksichtigt werden dabei Verkabelungen mit symmetrischen Kupferkabeln sowie Lichtwellenleitern.

Die EN 50173 wurde für Standorte mit einer Ausdehnung von bis zu 3.000 m sowie einer Bürofläche bis 1.000.000 m² optimiert. Die in dieser Norm festgelegte Verkabelung unterstützt die Übertragung folgender Informationen:

- | | | |
|-----------|---------|---------|
| ✓ Sprache | ✓ Daten | ✓ Video |
|-----------|---------|---------|

Die Norm EN 50173 legt zudem fest,

- ✓ wie der Mindestumfang und die Struktur für ein universelles Verkabelungssystem aussehen
- ✓ welche Anforderungen an eine Realisierung für ein Verkabelungssystem gefordert sind
- ✓ welche Anforderungen an die einzelnen Verkabelungsstrecken zwischen den Anwendungspunkten gestellt werden

Weitere Standards

Neben der EN 50173 sind weitere Normungen zur Installation der Kommunikationsverkabelung, deren Prüfung und von begleitenden elektrotechnischen Maßnahmen zu berücksichtigen. Dies umfasst:

- ✓ DIN EN 50174-1: Installationsspezifikation und Qualitätssicherung (10/2018)
- ✓ DIN EN 50174-2: Installationsplanung und Installationspraktiken in Gebäuden (10/2018)
- ✓ DIN EN 50174-3: Installationsplanung und Installationspraktiken im Freien (11/2017)
- ✓ DIN EN 50346: Prüfen installierter Verkabelung (02/2010)
- ✓ DIN EN 50310: Anwendung von Maßnahmen für Erdung und Potentialausgleich in Gebäuden mit Einrichtungen der Informationstechnik (12/2019)

Die Anforderungen an Rechenzentren sind in der *DIN EN 50600: Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren* beschrieben.

Die Norm unterteilt sich in allgemeine Konzepte, Design, Betrieb und Kenngrößen. Für die Installationsrichtlinien ist insbesondere der Teil 2–4 (siehe nachfolgenden Auszug) zu beachten:

- ✓ DIN EN 50600-1: Allgemeine Konzepte (08/2019)
- ✓ DIN EN 50600-2-2: Stromversorgung und Stromverteilung (08/2019)

- ✓ DIN EN 50600-2-3: Regelung der Umgebungsbedingungen (08/2019)
- ✓ DIN EN 50600-2-4: Infrastruktur der Telekommunikationsverkabelung (07/2015)
- ✓ DIN EN 50600-2-5: Sicherungssysteme (08/2016)
- ✓ DIN EN 50600-3-1: Informationen für das Management und den Betrieb (08/2016)
- ✓ DIN EN 50600-4-1: Überblick über und allgemeine Anforderungen an Leistungskennzahlen (06/2017)
- ✓ DIN EN 50600-4-2: Kennzahl zur eingesetzten Energie (08/2019)
- ✓ DIN EN 50600-4-3: Anteil erneuerbarer Energien (08/2019)

7.2 Struktur nach ISO/IEC 11801

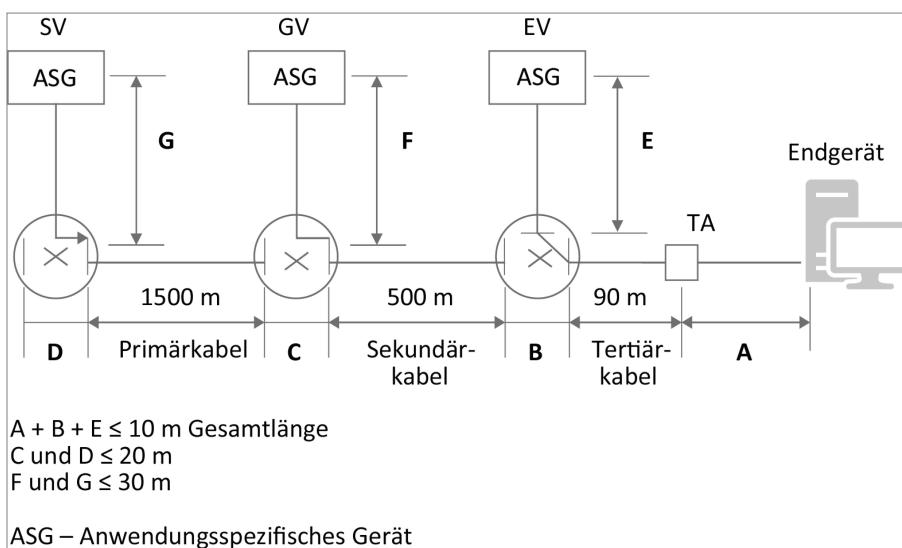
Strukturelle Einteilung gemäß ISO/IEC 11801

Der grundsätzlichen Forderung nach einem herstellerunabhängigen und dienstneutralen Verkabelungssystem wurde mit der internationalen Norm ISO/IEC 11801 Rechnung getragen. Die adäquate deutschsprachige Ausgabe hierfür ist die EN 50173.

Ein anwendungsneutrales und universelles Verkabelungssystem setzt sich aus diesen funktionellen Einheiten zusammen:

- ✓ Standortverteiler (SV)
- ✓ Primärkabel
- ✓ Gebäudeverteiler (GV)
- ✓ Sekundärkabel
- ✓ Etagenverteiler (EV)
- ✓ Tertiärkabel
- ✓ Kabelverzweiger (KV)
- ✓ informationstechnische Anschlüsse (TA) am Arbeitsplatz

Ein universelles Verkabelungssystem besteht aus drei Teilsystemen der Verkabelung: Primär-, Sekundär- und Tertiärverkabelung. Die Teilsysteme der Verkabelungen bilden eine universelle Verkabelungsstruktur. Mithilfe von Verteilern können so beliebige physikalische Topologien wie Bus, Stern und Ring realisiert werden.



Primärverkabelung

Die Primärverkabelung wird auch als Campus Backbone bezeichnet. Sie beschreibt die Verbindung zwischen Gebäudeverteilern (Hauptverteiler) und Standortverteilern über Lichtwellenleiter (Singlemode) in Ring- oder Stern-Topologie. Bildlich gesprochen kümmert sich dieser Bereich um die Verkabelung von Keller zu Keller der einzelnen Gebäude und stellt das Bindeglied zwischen den einzelnen Sekundärbereichen dar. Als weitere Aufgabe wird hier oft auch die Anbindung an den Provider (WAN-Anbindung) realisiert.

Sekundärverkabelung

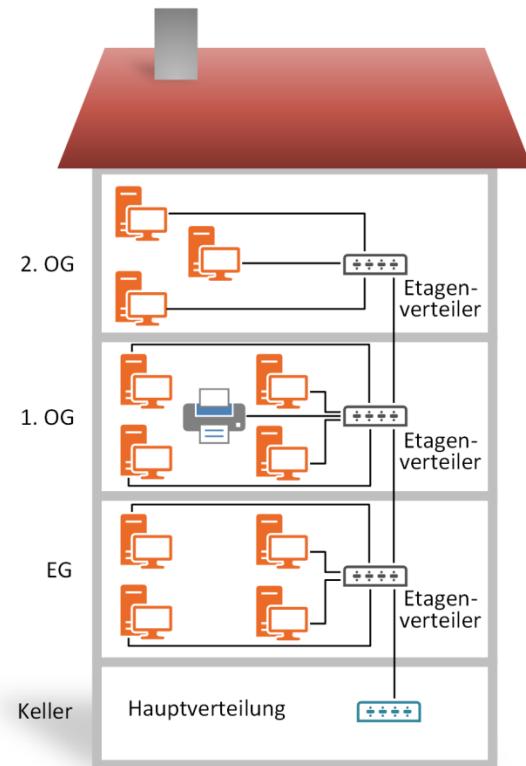
Gemeint ist damit die Verkabelung zu den Etagen, ausgehend vom Gebäudeverteiler. Jede Etage erhält dabei einen Etagenverteiler. Auch hier werden grundsätzlich Lichtwellenleiter (Multimode) zur Potentialtrennung zwischen den Etagen verwendet. Die maximale Länge sollte laut Norm nicht über 500 m hinausgehen.

Tertiärverkabelung

Dieses Verkabelungssystem verbindet den Etagenverteiler mit den Anschlussdosen. Diese Verbindung sollte nach Möglichkeit unterbrechungsfrei sein. In Ausnahmefällen kann maximal ein Kabelverteiler zwischen Etagenverteiler und Anschlussdose eingesetzt werden. Die übertragungstechnischen Eigenschaften dürfen dadurch nicht beeinflusst werden. Die Tertiärverkabelung wird hauptsächlich mit Twisted-Pair-Kabeln realisiert.

Etagenverteiler

Die EN 50173 empfiehlt, pro 1.000 m² Bürofläche einen Etagenverteiler einzuplanen. Dieser kann sowohl aktive als auch passive Komponenten enthalten. Je nach Bedarf können auch mehrere zusammenhängende Bürostockwerke über einen Etagenverteiler versorgt werden.



Strukturierte Gebäudeverkabelung mit Etagenverteiler

Informationstechnischer Anschluss

Informationstechnische Anschlüsse können sich in einem Bodentank, in der Wand oder in einem Kanalsystem befinden. Zwei Anschlüsse für jeden Arbeitsplatz sind das Minimum. Jeder Anschluss wird mit einem Twisted-Pair-Datenkabel belegt.

Empfohlene Medien für die Verkabelung:

Teilsystem	Medium	Verwendung
Tertiärsystem	Symmetrische Datenkabel LWL-Kabel	Kommunikation der Systeme auf Etagenebene Ausdehnung: 90 m + 10 m Patchkabel bei Twisted Pair
Sekundärsystem	LWL-Kabel (Multimode/Singlemode) Symmetrische Datenkabel	Kommunikation der Systeme innerhalb eines Gebäudes etagenübergreifend Ausdehnung: 500 m bei LWL
Primärsystem	LWL-Kabel (Singlemode) Symmetrische Datenkabel	Campuskommunikation (zwischen Gebäuden) Ausdehnung: 1500 m bei LWL

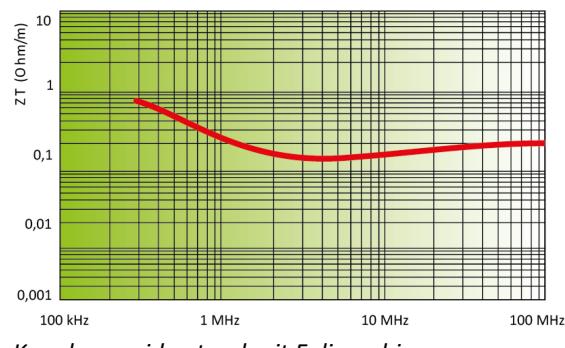
7.3 Richtlinien für Kupferkabel

Schirmung

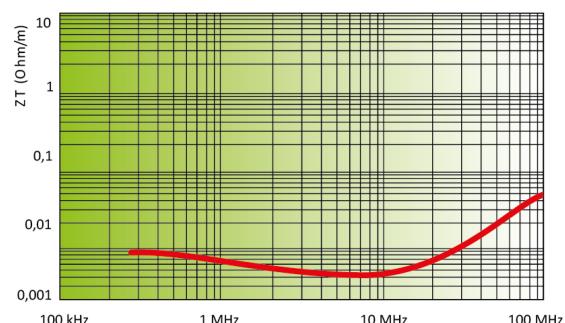
In der EN 50173 wird der maximale Kopplungswiderstand auch Transferimpedanz genannt, auf 50 mOhm bei 1 MHz und 100 mOhm bei 10 MHz definiert. Dieser Kopplungswiderstand ist jedoch nur mit großem Aufwand in der Schirmung zu erreichen. Schirmaufbauten wie doppeltes Aluminiumband mit kreuzweiser Verseilung oder längseinlaufende Bänder aus sehr dicker Aluminiumfolie führen zu einem Kopplungswiderstand von ca. 80–95 mOhm bei 10 MHz.

Der Kopplungswiderstand ist ein Maß für die Güte der Schirmung und wird definiert als das Verhältnis der Spannung längs des Schirms des gestörten Systems zu dem Strom des störenden Systems.

Der sogenannte Kombischirm besteht aus Aluminiumfolie und einem darüberliegenden Kupfergeflecht. Bei einer Überdeckung von mehr als 65 % lassen sich Kopplungswiderstände von 5–10 mOhm bei 10 MHz realisieren.



Kopplungswiderstand mit Folienschirm



Kopplungswiderstand mit Kombischirm

Brandverhalten

Datenkabel werden in der EN 50173 nicht nur nach ihren elektrischen und mechanischen Werten spezifiziert. Es wird auch ein zugelassenes Brandverhalten definiert. Nach ISO 882.3 werden im Bündelbrandtest klare Vorgaben über das Verhalten des Datenkabels bei Bränden getroffen. Ein Kabel darf nach diesen Spezifikationen nicht von alleine in Brand geraten oder einen Brand fortleiten, sondern muss nach Erlöschen des Feuers ebenfalls sofort aufhören zu brennen. Ein geringfügiges Nachglimmen ist erlaubt, muss aber in einem zeitlich sehr engen Rahmen beendet sein. Es ist vorgeschrieben, ausschließlich halogenfreies Kabel mit verminderter Brandfortleitung einzusetzen.

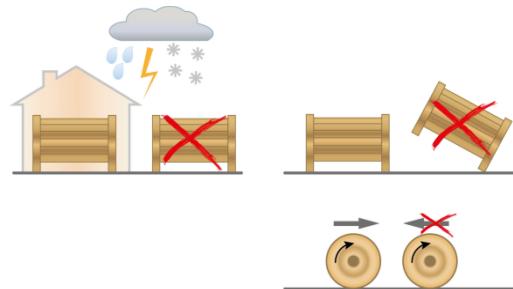
Biegeradien

Da Sie bei der Kabelverlegung nicht immer davon ausgehen können, dass die Kabel in dafür vorgesehene Kabelwannen oder auf optimalen Kabelwegen verlegt werden, hat die Norm dies berücksichtigt und einen Biegeradius von $8 \times d$ ($d = \text{Kabelaußendurchmesser}$) während der Installation vorgeschrieben. Kurzzeitiges Unterschreiten der vorgeschriebenen Mindestradien kann das Kabel nicht dauerhaft schädigen. Sie sollten aber beim Verlegen von Datenkabeln darauf achten, dass die Kabel nicht über scharfe Kanten oder mit zu hohem Krafteinsatz eingezogen werden. Zur Abhilfe können Sie scharfe Kanten mit einem entsprechenden Kantenschutz umhüllen oder bei zu geringen Biegeradien die entsprechenden Bohrungen vergrößern. Zu geringe Biegeradien können bei den erforderlichen Abnahmemessungen zu erhöhten Dämpfungs- und Kapazitätswerten führen. Sind die gemessenen Werte über den geforderten Normwerten, ist ein Austausch des so beschädigten Kabels zwingend erforderlich.

Lagerung und Transport

Die Datenkabel müssen vor, während und nach dem Verlegen vor mechanischer Beschädigung und dem Eindringen von Feuchtigkeit geschützt werden. Folgende wichtige Regeln sind für Transport und Lagerung einzuhalten:

- ✓ Die vom Kabelhersteller vorgegebenen Transport- und Lagervorschriften einhalten
- ✓ Lagerort bereits vor einer Anlieferung festlegen
- ✓ Geeigneten Lagerort wählen (trocken und vor Einflüssen wie beispielsweise Frost oder direkter Sonneneinstrahlung geschützt)
- ✓ Sorgfältiger Transport auf der Originalkabeltrommel
- ✓ Kabeltrommeln nur in Richtung des aufgewickelten Kabels rollen
- ✓ Kabelenden mit entsprechenden Abschlusskappen schützen
- ✓ Stöße an der Kabeltrommel vermeiden
- ✓ Kabeltrommeln nur liegend transportieren und einlagern



Fachgerechte Verlegung

Folgende allgemeine Regeln sind für eine fachgerechte Verlegung zu beachten:

- ✓ Beachten Sie die vom Hersteller vorgeschriebenen Temperaturbereiche (i.d.R. -5°C bis 70°C).
- ✓ Beachten Sie die vom Hersteller vorgegebenen und zulässigen Zugkräfte.
- ✓ Zur Vermeidung von zu hohen Zugkräften, sollten Sie ein Abroll-Gerät verwenden.
- ✓ Verwenden Sie nur einen einheitlichen Typ von Datenkabeln für die Verbindung zwischen Verteiler und Anschlussdosen.
- ✓ Rollen Sie das Kabel nur so weit aus wie nötig. So vermeiden Sie mechanische Beschädigungen (Überfahren, Überrollen).
- ✓ Rollen Sie das Kabel nicht inmitten von Bereichen mit Personenverkehr aus, sondern immer seitlich an einer Wand entlang (Sturzgefahr/mechanische Belastung der Kabel).
- ✓ Nehmen Sie die Kabelverlegung direkt von der Kabeltrommel vor.
- ✓ Vermeiden Sie die Einwirkung von Druck auf den Kabelmantel.
- ✓ Glätten Sie grobe Mauerdurchbrüche zur Vermeidung von Beschädigungen des Mantels beim Einziehen und späterer Befestigung.
- ✓ Scharfe Kanten auf der Verlegestrecke müssen mit einem Kantenschutz versehen werden.
- ✓ Verlegen Sie bei Mauerdurchbrüchen oder Kernbohrungen die Kabel „locker“.
- ✓ Wenn Sie mehrere Kabel durch ein Rohr führen müssen, dann sollten Sie diese zusammenbündeln.

Einhaltung des Biegeradius

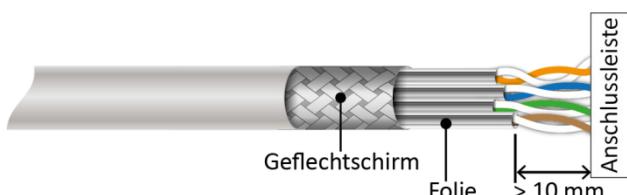
- ✓ Grundsätzlich ist der erlaubte Biegeradius beim Verlegen das 15fache vom Kabeldurchmesser. Nach dem Verlegen und dem Befestigen entspricht der Biegeradius dem 10fachen Kabeldurchmesser.
- ✓ Achten Sie vor allem beim Einziehen in Installationsrohre oder Kabelschächte auf die Einhaltung dieser Biegeradien.
- ✓ Die Kabelkanäle müssen bei Richtungsänderung über einen genügend großen Radius verfügen.
- ✓ Beim Einlauf in Kanal- oder Rohrsysteme und vor allem bei Mauerdurchbrüchen sind geeignete Umlenk-elemente einzusetzen.

Schutz vor EMV–Einflüssen

- ✓ Es sollten bevorzugt Datenkabel mit einer Folien- und/oder Geflecht-Schirmung verwendet werden.
- ✓ Es ist darauf zu achten, dass das Kabel auf beiden Seiten für Folie und/oder Geflecht vollständig geerdet wird.
- ✓ Eingesetzte Kabelverlegungssysteme aus Metall müssen geerdet werden.
- ✓ Starkstromkabel sollten nach Möglichkeit nicht mit Twisted-Pair-Kabeln gekreuzt werden. In Ausnahmefällen sollte der Winkel bei einer Kreuzung 90° betragen und die Strecke der Kreuzung so kurz wie möglich sein.
- ✓ Zur Einhaltung der Abstände von Daten- zu Energiekabeln sollten Trennstege in Kanalsystemen verwendet werden.

Auflegen von symmetrischen Kabeln

- ✓ Die Verseilung der Adernpaare ist möglichst bis kurz vor dem Auflegen beizubehalten. Die Aufdrillung darf 10 mm nicht überschreiten, um das Übersprechen zu vermeiden.
- ✓ Es ist darauf zu achten, dass der Schirm des Datenkabels einen guten Kontakt zu Datendose bzw. Patchpanel hat.
- ✓ Der Beidraht muss mit der Abschirmung gut kontaktiert werden. Einige Anschlüsse sehen eine eigene Schneidklemme für den Beidraht vor.
- ✓ Das Kabel muss an der vorgesehenen Zugentlastung befestigt werden.
- ✓ Die Biegeradien dürfen keinesfalls unterschritten werden.



Aufteilung eines S/STP-Kabels

7.4 Besonderheiten für LWL-Kabel

Grundsätzlich gelten für Transport, Lagerung, Verlegung und Handhabung von LWL-Kabeln dieselben Vorschriften wie für Kupferkabel. Gerade bei LWL-Kabeln ist besonderes Augenmerk auf den vom Hersteller vorgeschriebenen Biegeradius zu richten.

Der Einsatz von Glasfaserkabeln erfordert viel Erfahrung und Know-how und sollte deshalb nur von erfahrenen Installateuren erfolgen. Eine fehlerhafte Installation kann schnell zu hohen Dämpfungswerten oder sogar zum Defekt eines LWL-Kabels führen.

Mögliche Ursachen für hohe Dämpfungswerte:

- ✓ Verunreinigungen der Faser
- ✓ unterschiedlicher Fasertyp
- ✓ unterschiedliche Kerndurchmesser
- ✓ beschädigte Stirnfläche der Faser
- ✓ falsche Stirnflächengeometrie der Faser
- ✓ Abstand der Stirnflächen zu groß
- ✓ falsches Einsetzen der Faser in den Stecker

Eine LWL-Strecke sollte grundsätzlich möglichst wenige Verbindungsstellen (Spleiße oder Steckverbindungen) enthalten. Es ist grundsätzlich zu beachten, immer denselben Kerndurchmesser zu verwenden.



Grundsätzlich müssen die in der EN 50173 spezifizierten Kategorien der LWL-Faser Beachtung finden. Dies sind für Multimodefasern die Kategorien OM1, OM2, OM3, OM4 und OM5, wovon heute nur die Kategorien OM3 bis OM5 dem Stand der Technik entsprechen. Für den Einsatz von Monomodefasern (Singlemode) sind es die Kategorien OS1 und OS2, wobei die Verwendung der Kategorie OS2 empfohlen wird.

7.5 Kennzeichnung und Beschriftung

Beschriftung von Datenkabeln

Eine eindeutige, dauerhafte und sinnvolle Beschriftung ist für eine Dokumentation oder spätere Fehlersuche unbedingt notwendig. Wichtige Regeln zur Beschriftung vor und während der Installation sind:

- ✓ Das Beschriftungsschema für die Kabel ist vor der Verlegung festzulegen.
- ✓ Jedes Kabel ist an den Enden vor dem Einziehen mit einem wasserfesten Stift zu beschriften.
- ✓ Die Beschriftung sollte in den Kabelplänen vermerkt werden.
- ✓ Die Beschriftung „Kabel“ muss nach dem Auflegen auf der Verteilerseite eindeutig zu erkennen sein. Hier können Beschriftungskabelbinder oder Beschriftungsbänder verwendet werden.

Wichtige Regeln zur Beschriftung nach der Installation

- ✓ Im Verteiler sollte ein eindeutiges Schema zur Beschriftung verwendet werden.
- ✓ Die Kennzeichnung der Anschlussdosen muss mit der Kennzeichnung des Verteilers übereinstimmen.
- ✓ Die Beschriftung der Verteiler und Anschlussdosen ist auf entsprechende Pläne und Aufbauzeichnungen zu übernehmen.
- ✓ Die Beschriftung der Verteiler und Anschlussdosen sollte den Bezeichnungen in den Messprotokollen entsprechen.
- ✓ LWL-Kabel sollten zur besseren Erkennung an der gesamten Strecke dauerhaft (z. B. mit Beschriftungsbändern/-kabelbindern: „Vorsicht – LWL-Kabel“) gekennzeichnet werden.

8 Planung und Dokumentation von Netzwerken

In diesem Kapitel erfahren Sie

- ✓ wie Sie eine strukturierte Verkabelung planen und realisieren
- ✓ welche Anforderungen Sie berücksichtigen müssen
- ✓ wie Sie eine Dokumentation erstellen

Voraussetzungen

- ✓ Wissen über passive Komponenten
- ✓ Wissen über die Installationsrichtlinien
- ✓ Wissen über die Normen der strukturierten Verkabelung

8.1 Planung eines Netzwerks

Vorbereitende Maßnahmen

Ziel einer flächendeckenden Verkabelung ist die Ausstattung der Arbeitsplätze mit dienstneutralen informationstechnischen Anschlüssen. Dabei ist es unerheblich, für welchen Dienst der Anschluss vorgesehen ist. Die wichtigsten technischen Größen für eine Verkabelung werden in den von der EN und ISO/IEC festgelegten Normen geregelt. Wer vor der Aufgabe steht, für sein Unternehmen die Kommunikationsinfrastruktur zu planen oder neu einzuführen, sollte dies anhand einer gut durchdachten Strategie angehen. Schnelle Entscheidungen oder gar Aktionen über Nacht sind hier nicht ratsam. Diese gehen meistens mit höheren Folgekosten einher und resultieren in einem Chaos an Teilnetzwerken mit unterschiedlicher zum Teil auch proprietärer Ausstattung und geringen oder gar keinen Erweiterungsmöglichkeiten.

Der erste Schritt für die Durchführung einer Verkabelung ist die Grundüberlegung, wie die Ideallösung aussehen soll. Hierzu ist es notwendig, alle erforderlichen Unterlagen zu sammeln und diese auszuwerten:

- ✓ Holen Sie sich Übersichtspläne der Räumlichkeiten, der Gebäude und des Geländes.
- ✓ Wenn mehrere Standorte angeschlossen werden, überprüfen Sie die physikalischen Gegebenheiten und Voraussetzungen der Standorte (eventuell direkt vor Ort).
- ✓ Definieren Sie, wie der informationstechnische Anschluss aussehen soll bzw. welche Dienste für die einzelnen Standorte benötigt werden.
- ✓ Skizzieren Sie Ihre Lösung in Form eines Blockdiagramms (ausgehend vom Verteilerstandort).
- ✓ Definieren Sie den Ausstattungsstandard je Arbeitsplatz. Ermitteln Sie die Mengen der informationstechnischen Anschlusseinheiten (z. B. Technologie der Anschlüsse [Kupfer/LWL], Anzahl der Ports je Arbeitsplatz, Klasse der Technologie, Kosten je Arbeitsplatz).
- ✓ Berücksichtigen Sie bereits zukünftige Erweiterungen.

Sie sollten in jedem Fall Ihre gewünschte Lösung zu Papier bringen, egal ob dies nun in Form von Zeichnungen, Skizzen oder schriftlich ist. Ausgehend von der Festlegung der Ideallösung können Sie dann die Mittel und Methoden wählen, mit denen Sie dieses Ziel erreichen.

Lichtwellenleiter- oder Kupferverkabelung

Eine sehr wichtige Entscheidung ist die, ob Sie Glasfaser- oder Kupferkabel verwenden. Im Tertiärbereich werden Sie in der Regel auf Twisted-Pair-Verkabelung setzen, im Primär- und Sekundärbereich sowie im Rechenzentrum (aufgrund der Potentialtrennung) fast ausschließlich LWL nutzen. Steht diese Entscheidung fest, müssen spezifische Anforderungen bezüglich Qualität und technischen Merkmalen festgelegt werden. Für den Backbone bzw. für die etagen- und gebäudeübergreifende Anbindung sollten bzw. müssen Sie in jedem Fall Glasfaser einsetzen. Alternativ können Sie für kurze Strecken bei der Etagenanbindung oder der Anbindung von DV-Verteiler-schränken untereinander auch Kupferdatenkabel verwenden.

Bedenken Sie jedoch, dass Sie bei dieser Lösung unter Umständen bei einem Technologiewechsel oder bei höheren Datenraten einen Flaschenhals schaffen, sofern Sie nicht die Kategorie 8.1/8.2 nutzen. Bei dieser Variante sollten Sie sich gleich überlegen, ob Sie nicht wenigstens das Glasfaserkabel mit verlegen, um eine spätere Erweiterung zu gewährleisten. Die Gesamtkosten werden in so einem Fall auch anfallen, aber Sie haben immer die Option, ohne größere bauliche Maßnahmen auf eine höhere Datenrate aufrüsten zu können. Zudem reduzieren Sie Ihre Investitionskosten und haben die Folgekosten nur für den Fall, dass Ihr Backbone tatsächlich nicht mehr den Anforderungen genügt.

Bei Vorgabe der maximalen Kabellänge und der höchstzulässigen Fehlerrate ist auch der maximale Datendurchsatz festgelegt. Dabei ist es dann egal, ob ein Kupferkabel oder ein Lichtwellenleiter verwendet wird. Lichtwellenleiter sind dann von Vorteil, wenn es darum geht, größere Entfernungen zu überbrücken oder wenn sichere Daten in einer störempfindlichen Umgebung gefordert sind. Im industriellen Umfeld mit Maschinen, die starke elektrische Felder produzieren, oder in Bereichen, die abhörsicher sein müssen, sollten Sie sich ebenfalls für Glasfaserkabel entscheiden.

Ein Argument, das auch klar für den Einsatz von Glasfaserkabeln spricht, ist der Bandbreitenbedarf am Arbeitsplatz. Heute entworfene Anwendungen werden schon in kurzer Zeit zu unserem ständigen Begleiter werden. Hochauflösende Grafiken mit fotorealistischen Bildern, Multimedia-Anwendungen, Live-Video am Arbeitsplatz und Desktop-Videokonferenzen lassen die am Arbeitsplatz benötigte Bandbreite drastisch ansteigen.

Da die strukturierte Verkabelung auf der Basis von Twisted-Pair-Kabeln am häufigsten zum Einsatz kommt, sind die entsprechenden Komponenten weit verbreitet und dementsprechend preisgünstig. Auch die Verarbeitung der Kupfertechnik ist weniger aufwendig als die von Glasfasern und kann von entsprechenden Fachfirmen durchgeführt werden.

Fiber-to-the-Desk

Die überragenden Vorteile einer Glasfaserverkabelung – installationsbedingte und auch übertragungstechnische – liegen klar auf der Hand. Die Versorgung bis zum Arbeitsplatz hängt letztendlich von den Kosten ab. Die Verlege- und Anschlussarbeiten sind in der Regel nur geringfügig teurer als bei Kupferkabeln. Die hauptsächlichen Kosten liegen bei den aktiven Komponenten wie beispielsweise Switchen oder Netzwerkkarten.

Denkmalgeschützte Gebäude

Denkmalgeschützte Gebäude stellen häufig eine besondere Herausforderung an die gebäudetechnische Ausstattung dar. Hier sollten Sie sich von einem Architekten beraten lassen, der bereits Erfahrungen mit solchen Gebäuden hat. Ansonsten gelten auch hier die gleichen Standards für die Verkabelungsmaßnahmen wie bei herkömmlichen Gebäuden. Als Alternative kann auch ein gemischtes Konzept mit WLAN-Komponenten zur Disposition stehen, wie es z. B. in vielen Museen der Fall ist.

Campusbereich

Für die Anbindung von Gebäuden untereinander müssen Sie sich in jedem Fall für Glasfasern entscheiden. Da im Campusbereich lediglich das Backbone-Netz betrieben wird, ist die Anzahl der Kabel sowie die Dichte der Fasern pro Kabel von geringerer Bedeutung, allerdings sollten Sie für eventuelle Erweiterungen einige Fasern als Reserve vorhalten. Wenn möglich, sollten Sie eine zweite, redundante Glasfaserstrecke verlegen, auch wenn Sie diese nicht in Betrieb nehmen. Im Falle eines Kabelschadens, beispielsweise durch Erdarbeiten, haben Sie dann immer noch die Möglichkeit, auf die redundante Strecke auszuweichen. Die Leitungsführung dieser Ausweichstrecke sollte nach Möglichkeit nicht parallel zur Hauptstrecke legen.

Grundsätzlich sollten Sie bei allen Punkten der Planung und der Vorbereitung den Bezug zur Praxis nicht verlieren. Denn was nützt eine optimale Planung, wenn die Umsetzung in die Praxis holprig verläuft. Nur eine gesunde Mischung aus den vier relevanten Faktoren Kosten, Zeit, Qualität und Investitionsschutz führt Sie zum gewünschten Ergebnis.

8.2 Anforderungen an die Infrastruktur

Für die Verkabelung im Tertiärbereich sollten Sie bereits bei der Planung bestimmte Voraussetzungen an Ihre Kommunikationsinfrastruktur stellen. Bei der Auswahl von Datendosen und Patchfeldern sollten Sie sich möglichst auf ein einziges System festlegen (RJ-45, GG45, ARJ45, TERA).

Achten Sie bei diesen Komponenten darauf, dass eine langfristige Verfügbarkeit der Komponenten sowie kurze Lieferzeiten der Komponenten gewährleistet sind. Sie haben keinen Vorteil, wenn Sie ein Produkt einsetzen, das derzeit kostengünstig verfügbar ist, bei dem aber nur ein einzelner Lieferant (Exklusivvertrieb) verfügbar ist.

Datendosen und Patchpanel

Für Datendosen und Patchfelder gilt in jedem Fall, dass sie die geforderten Leistungsmerkmale gemäß EN 50 173 und ISO/IEC DIS 11 801 im installierten Zustand erfüllen müssen. Dies gilt insbesondere für die Link- und Channelperformance als wesentliches Leistungsmerkmal. Der Einsatz modularer Systeme hat den Vorteil, die informationstechnische Einheit am Arbeitsplatz variabel zu halten. Ein späteres Nach- oder Umrüsten kann durch den einfachen Austausch der entsprechenden Einsätze erfolgen. Nachteilig bei solchen Systemen sind die höheren Anschaffungskosten.

Verlegekabel

Datenkabel für den Tertiärbereich müssen alle derzeit verwendeten Netzdienste unterstützen. Verwenden Sie bevorzugt hochwertigere Datenkabel, auch wenn die benötigten Dienste mit einer geringeren Bandbreite auskommen. Das Kabel sollte für einen späteren Standard, der größere Übertragungsbandbreiten benötigt, ausgelegt sein. Stimmen Sie unter Berücksichtigung zertifizierter Systemwerte alle verwendeten Kabel wie Anschlusskabel, Patchkabel und Verlegekabel im Tertiärbereich aufeinander ab. Überprüfen Sie im Vorfeld, ob die Übertragungsreichweiten der Twisted-Pair-Verlegekabel 100 Meter inklusive der Anschlusskabel (Patchkabel) nicht überschreiten.

Nach aktueller Normungslage ist die Überschreitung der maximalen Distanz von 100 m kein Ausschlusskriterium mehr. Vielmehr ist nun die Einhaltung der in der Norm beschriebenen Übertragungsgrenzwerte zu gewährleisten. 

Somit sind bei Einhaltung dieser Werte auch Übertragungsstrecken länger 100 m als normkonform zu bewerten. Bei der Planung sollte aber die 100-m-Marke nicht überschritten werden. Viele Kabelhersteller ermöglichen heute normgerecht Reichweiten von 120 Meter.

Aus brandschutztechnischen Gründen müssen Sie grundsätzlich ein halogenfreies Datenkabel einsetzen. Alle Hersteller haben dies auch im Programm. Fordern Sie in jedem Fall vor dem Einsatz eines Datenkabels das zugehörige Datenblatt des Herstellers an und überprüfen Sie die erforderlichen Merkmale. Dies gilt auch für Glasfaserkabel. Hier sollten Sie vor allem auf die Biegeradien beim Verlegen sowie im verlegten Zustand achten. Prüfen Sie, ob bei der Trassenführung diese erforderlichen Biegeradien eingehalten werden können. Der Einsatz von Außenkabeln ist abhängig von der Kabeltrasse. Im Inhouse-Bereich können Sie durchaus auch Innenkabel verwenden oder sogenannte Universalkabel (Bezeichnung A/I). Führt Ihre Kabeltrasse jedoch durch Kellerräume oder befindet sie sich in Lagerhallen, dann sollten Sie sich für ein Außenkabel mit metallfreiem Nagetierschutz entscheiden.

Besonders in Rechenzentren sowie zentralen und dezentralen Netzwerk-Verteilerknoten werden vorrangig beidseitig vorkonfektionierte Mehrfachkabel (Trunkkabel) verlegt. Ein Trunkkabel vereint vier bis acht vierpaarige Einzelkabel mit einem gemeinsamen Außenmantel. Vorteilhaft sind die schnelle sowie anschlussfertige Installation, geringerer Platzbedarf sowie reduzierte Brandlasten. Um unnötige Kabelreserven in der Verkabelungsstrecke zu vermeiden, muss im Vorfeld eine exakte Längenermittlung der Trunkkabel vorgenommen werden. Einige Systemhersteller bieten daraus abgeleitet nun auch einseitig vorkonfektionierte Kabel an – das nicht konfektionierte Kabelende ist dann am Patchfeld aufzuschalten.

Server- und Netzwerkschränke

Überprüfen Sie beim Einsatz von Server- und Netzwerkschränken, welche Anforderungen der Schrank erfüllen muss und auf welche Eigenschaften Sie verzichten können. Berücksichtigen Sie bereits bei der Definition der Anforderungen an die Server- und Netzwerkschränke auch die Datensicherheit.

Folgende Fragestellungen ergeben sich für DV-Schränke:

- ✓ Ist ein Schwenkrahmen (Drehrahmen) notwendig?
- ✓ Von wo aus erfolgt die Kabeleinführung (oben, unten, seitlich)?
- ✓ Wird eine Sichttür (ESG-Glas oder Kunststoff) benötigt oder ist eine Stahlblechtür ausreichend?
- ✓ Sollen die Seitenwände abnehmbar sein?
- ✓ Ist eine Rücktür erforderlich oder reicht eine Rückwand aus?
- ✓ Sind Front- und Rücktür abschließbar und/oder zu überwachen?
- ✓ Ist es nötig, die Seitenwände gegen unbefugtes Öffnen zu sichern und/oder zu überwachen?
- ✓ Wird eine Schrankbeleuchtung mit Schalter benötigt oder reicht die Raumbeleuchtung aus?
- ✓ Ist ein Schranküberwachungssystem vorgesehen und soll die Weiterbearbeitung von Alarmmeldungen erfolgen?
- ✓ Sind genügend Stromanschlüsse (Steckdosenleiste) und ausreichend separate Stromkreise im Schrank vorhanden?
- ✓ Ist eine zusätzliche Belüftung oder Klimatisierung erforderlich?
- ✓ Soll eine USV zur Überbrückung von Ausfällen im Schrank integriert werden?

Überprüfen Sie anhand dieser und eigener Punkte, welche Bedürfnisse berücksichtigt werden müssen und welche Voraussetzungen ein Server- oder Netzwerkschrank für Ihr Unternehmen erfüllen muss. Prüfen Sie auch, ob es sinnvoll ist, mehrere Schränke aufzustellen, z. B. für die Trennung der aktiven und passiven Komponenten oder zukünftige Erweiterungen. Skizzieren Sie den Schrankaufbau bzw. die Schrankaufbauten, um die Übersicht über die Ausstattung und die damit verbundenen Reserven zu behalten. Wichtig dabei ist die Angabe der Komponenten in Höheneinheiten (HE). Wenn Sie sich bereits für aktive oder passive Komponenten entschieden haben, können Sie diese mit den Herstellerangaben in Ihrer Skizze kennzeichnen. Ein geeignetes Tool für die Dokumentation der Schränke ist beispielsweise die Software Visio (Microsoft) und die Verwendung sogenannter Shape-Sets, die viele Komponenten-Hersteller zum Download anbieten.

Bezeichnungen für Verteilerschränke

Der Verteilerbereich markiert den zentralen Punkt einer strukturierten Gebäudeverkabelung. Im Verteilerbereich befinden sich die technischen Ausrüstungen für ein Netzwerk. Sowohl aktive als auch passive Netzwerkkomponenten finden dort ihren Platz. Je nach Einsatzbereich werden die Schränke unterschiedlich bezeichnet:

- ✓ Standortverteiler (SV)
- ✓ Gebäudeverteiler (GV)
- ✓ Etagenverteiler (EV)

Standortverteiler

Der Standortverteiler oder Campus Distributor (CD) ist die zentrale Stelle auf einem Firmengelände bzw. in einem Firmengebäude. Er ist der Sternpunkt für den Anschluss der Gebäudeverteiler.

Gebäudeverteiler

Der Gebäudeverteiler oder Building Distributor (BD) existiert einmal pro Gebäude. Empfohlen wird eine sternförmige Verkabelung mit dem Standortverteiler. Um die Verfügbarkeit/Ausfallsicherheit der Verbindungen zwischen den Gebäudeverteilern zu erreichen, ist hier auch die Bildung einer Ringstruktur anzuraten.

Etagenverteiler

Etagenverteiler (auch als Floor Distributor (FD) bezeichnet) stellen die Zentrale innerhalb einer Etage dar. Sie versorgen eine Etage oder einen Etagenbereich mit Anschlüssen. Je nach Gebäudegröße kann ein Etagenverteiler auch ein Gebäudeverteiler sein.

Anforderungen an den Verteilerstandort

Bei der richtigen Auswahl der Standorte für Verteilerschränke sollten Sie genau prüfen, ob der entsprechende Raum auch geeignet ist. Ein winziger Abstellraum ist ebenso wenig geeignet wie ein Raum mit viel Publikumsverkehr. Der Standort für Verteilerschränke sollte immer so gewählt werden, dass nur bestimmte Personen Zutritt haben. Dies ist schon aus Gründen der Datensicherheit eine zwingende Voraussetzung.

Völlig ungeeignet sind beispielsweise auch feuchte und modrige Kellerräume. Sie sollten bei der Auswahl des richtigen Standortes immer die günstigste, zentralste Lage in einem Gebäude suchen, um die Kabelwege kurz zu halten. Auch die räumliche Ausstattung sollte in einem vernünftigen Einklang mit der Nutzung stehen. Bedenken Sie, dass in so einem Raum auch einmal administrative Aufgaben erledigt werden müssen. Unter Umständen dient der Verteilerstandort gleichzeitig als Standort für Ihre Server. An Standorten von Verteilerschränken sollten keine wasserführenden Leitungen, insbesondere keine druckführenden Leitungsstränge, existieren. Ausgenommen davon sind Leitungen für Klima-, Lüftungs- oder Löschanlagen. Lassen sich in Ausnahmefällen an den Verteilerschrankstandorten wasserführende Leitungen nicht vermeiden, sind diese abzukoffern bzw. mit Tropfrinnen zu versehen.

Folgende Anforderungen sollte ein idealer Verteilerraum erfüllen:

- ✓ sämtliche Türen fest abschließbar
- ✓ Umgebungstemperatur zwischen 18° C und 30° C (unnötige Kühlung ist heute ökologisch bedenklich, daher möglichst wenig Kühlung)
- ✓ Alternative zur Kühlung ist eine Belüftung mit Außenluft als sog. „freie Kühlung“
- ✓ Telefon-, Netzwerk- und Internetanschluss für den technischen Support
- ✓ ausreichende Beleuchtung
- ✓ ausreichend abgesicherte Stromversorgung (am besten durch eigene Stromkreise)
- ✓ genügend Stromanschlüsse (Steckdosen)
- ✓ zentrale Lage auf der Etage sowie im Gebäude
- ✓ Verteilerschrank nach Möglichkeit von drei Seiten zugänglich (zwei Seiten eingeschränkt sind das Minimum)

8.3 Ausstattung der Arbeitsplätze

Für die informationstechnische Anschlussdose am Arbeitsplatz sollten Sie eine geschirmte Anschlussdose mit einheitlicher Schnittstelle (RJ-45, GG45, ARJ45, TERA) verwenden. Benutzen Sie 2fach- oder 3fach-Anschlussdosen, auch wenn Ihnen ein Port als ausreichend erscheint. Bei späteren Erweiterungen sind dann bereits genügend Anschlussdosen vorhanden und müssen nicht erst eingebaut werden. Der Preisunterschied von 1fach- zu 2fach- oder 3fach-Anschlussdosen ist marginal. Die Dose muss so installiert sein, dass sie die geforderten Merkmale gemäß den Normen einhält.

Die Lage der Anschlussdosen sollte so gewählt werden, dass der Arbeitsplatz in direkter Nähe zur Dose liegt. Damit vermeiden Sie Stolperfallen und unnötigen Kabelsalat in den Büroräumen. Pro Arbeitsplatz sollten Sie immer mindestens drei Anschlussmöglichkeiten einplanen:

- ✓ Anschluss für Telefonie
- ✓ Anschluss für Daten
- ✓ Reserve oder weiterer Datenanschluss (für Netzwerkdrucker oder andere periphere Geräte)



Anschluseinheit

Auch wenn der Telefonieanschluss derzeit noch über ein getrenntes Leitungsnetz läuft, sollten Sie bereits bei der Installation einer neuen Kommunikationsinfrastruktur spätere Umstellungen berücksichtigen.

Berücksichtigen Sie auch, dass genügend Stromanschlüsse für die Geräte am Arbeitsplatz vorhanden sind. Sollte dem nicht so sein, so sollten Sie in jedem Fall für die notwendigen Stromanschlüsse sorgen. Auch hier gilt wieder, die Stromversorgung so nah wie nur möglich an den Arbeitsplatz zu legen. Auf Tischverteiler (wie die beliebten 3fach-Verteiler) ist tunlichst zu verzichten. Trennen Sie die Steckdosen für Netzwerktechnik mittels separater Stromkreise und spezieller Kennzeichnung mit Bezeichnungsschild und/oder farbigem Steckdoseneinsatz (grün, rot, orange) von der allgemeinen Arbeitsplatzversorgung.

8.4 Überspannungsschutz

Eine sehr häufige Ursache (über ein Viertel) für den Ausfall eines Netzwerks sind Schäden aufgrund von Überspannungen. Ereignisse wie diese verursachen jedoch nicht nur hohe Kosten für Reparaturen und Ersatzgeräte, sondern auch einen, unter Umständen, erheblichen Nutzungsausfall.

Die wichtigsten Störungen durch Überspannungen erfolgen durch:

- ✓ direkten und indirekten Blitzschlag
- ✓ Schaltvorgänge im Stromnetz
- ✓ statische Entladungen
- ✓ Dauerstörungen durch Starkstromleitungen
- ✓ Überspannungen im Stromnetz der Energieversorger

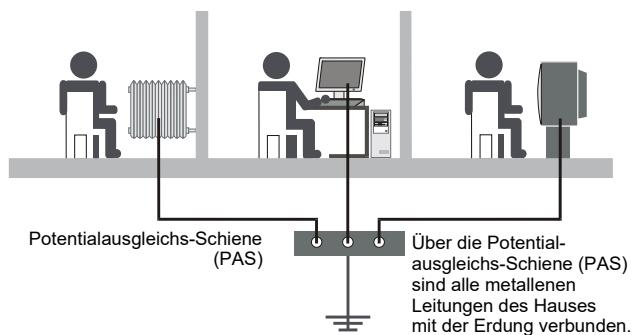
Bereits bei der Planung einer Kommunikationsinfrastruktur sollten Sie Maßnahmen gegen Überspannungen einleiten. Diese Maßnahmen können von der Auswahl der Streckenführung abseits von möglichen Störquellen bis zur Einbindung von speziellen Komponenten zum Schutz vor Störungen reichen.

Normen gemäß DIN VDE

Für die Planung und Errichtung von Blitzschutzeinrichtungen sind die VDE-Bestimmungen DIN VDE 0185 Teil 1 und Teil 2 zu beachten. Entsprechend dem aktuellen technischen Stand wird die Anwendung der europäischen Norm empfohlen (EN 61024). Inhalt dieser Norm ist der Schutz von Gebäuden gegen Feuer (zündender Blitz), Schutz gegen mechanische Zerstörung (nicht zündender Blitz) sowie der Schutz elektrischer Installationen innerhalb von Gebäuden. Speziell in der Norm DIN VDE 0185-305 werden Maßnahmen zum Schutz von Gebäuden mit umfangreichen elektronischen Einrichtungen gegen Blitzschlag beschrieben.

Ein vollständiger Blitzschutz besteht gemäß der DIN VDE 0185 aus einem äußeren und einem inneren Schutz. Beide ergänzen sich zum gesamten Blitzschutz und sollten nie getrennt gesehen werden. Alle Teile, die den Strom des Blitzes einfangen und ableiten, gehören zum äußeren Blitzschutzbereich. Der äußere Blitzschutz sorgt dafür, dass der Blitzstrom, im Falle eines Einschlages, gefahrlos zur Erde abgeleitet wird.

Alle erforderlichen Maßnahmen, die gegen die Wirkung des Blitzstromes arbeiten, werden zum inneren Blitzschutzbereich gezählt. Der innere Blitzschutz beginnt mit der Installation einer Potentialausgleichsschiene. Hierbei werden alle in ein Gebäude ein- und austretenden Kupferkabel in den Potentialausgleich einbezogen.



Schema für den Potentialausgleich

Grobschutz

Alle Kupferdatenleitungen, sowohl für Telefonie als auch für Netzwerktechnik, die in ein Gebäude verlaufen, werden mit einem Überspannungsschutz ausgestattet. Diese können einen Blitzstrom ableiten, ohne dass Geräte bei einem Blitzschlag Schaden erleiden. Bei der Benutzung von Lichtwellenleitern für die Anbindung zwischen Gebäuden wird dieser Schutz nicht benötigt. Sie sollten aber auch darauf achten, dass ein Grobschutz besonders bei den Stromanschlusskabeln in der nächsten Unterverteilung vorhanden ist.

Mittelschutz

Beim Mittelschutz werden die gefährdeten Leitungen vor ihrem Eintritt in die Anschluseinheit über eine Überspannungsschutzeiste geführt. Stromleitungen werden beispielsweise in der entsprechenden Etagenverteilung mit den passenden Überspannungsableitern ausgerüstet. Bei Fernmeldeleitungen werden sogenannte Überspannungsmagazine verwendet. Diese werden nachträglich auf die LSA+-Leisten aufgesteckt.

Feinschutz

Der Feinschutz wird direkt vor den Endgeräten installiert. Sie werden entweder vor den Anschlusskabeln der zu schützenden Geräte oder direkt im Kabelkanal integriert.

Ein Feinschutz ist nur wirksam, wenn im Netz vorher auch Grob- und Mittelschutz installiert sind. Der alleinige Einsatz von Feinschutzgeräten ist nicht zielführend und technisch als falsch zu bewerten.



8.5 Bauliche Maßnahmen

Die wichtigste Aufgabe im Vorfeld der auszuführenden Maßnahmen ist die Besichtigung der Räumlichkeiten, in welchen die Arbeiten durchgeführt werden. Nehmen Sie sich dafür genügend Zeit und prüfen Sie eingehend das Umfeld für die baulichen Maßnahmen. Wichtig hierbei sind folgende Punkte:

- ✓ Sind alle Stellen frei zugänglich oder sind z. B. Einbauschränke im Weg?
- ✓ Können die erforderlichen Durchbrüche ohne Folgen für die Statik gemacht werden? (Im Zweifel ist hochbauseitig ein Statiker hinzuzuziehen)
- ✓ Welche Brandschottung ist für den Verschluss der Durchbrüche erforderlich?
- ✓ Wie soll die Leitungsführung in den Räumlichkeiten erfolgen?
- ✓ Ist es erforderlich, eine Haupt-Kabeltrasse durch benutzte Arbeitsräume zu führen?
- ✓ Wo und wie soll die Haupt-Kabeltrasse verlaufen? Ist ein ausreichender Abstand zwischen Elektro- und Datenleitungen gegeben?
- ✓ Werden die Kabeldistanzen für Lichtwellenleiter und Twisted-Pair eingehalten?
- ✓ Welche brandschutztechnischen Gegebenheiten weisen die Räumlichkeiten auf? Gibt es für das Objekt ein aktuelles Brandschutzkonzept? Die Anforderungen der LAR 2005 für notwendige Flure und Treppenhäuser sowie Flucht- und Rettungswege sind zu beachten.
- ✓ Können die erforderlichen Biegeradien, besonders für LWL-Kabel, eingehalten werden?
- ✓ Sind zusätzliche Arbeiten (beispielsweise am Stromnetz) erforderlich?
- ✓ Ist eine klare Einteilung für den Überspannungsschutz vorhanden?
- ✓ Kann es zu Problemen mit dem Potentialausgleich kommen?
- ✓ Werden besondere Anforderungen an Form und Farbe der Leitungsführungskanäle gestellt? Gibt es Vorgaben zum Elektro-Flächenprogramm (sog. „Schalterprogramm“)?
- ✓ Sind zusätzliche Durchbrüche für Steigtrassen erforderlich?
- ✓ Werden Nebenleistungen benötigt (Malerarbeiten, Maurerarbeiten usw.)?
- ✓ Existieren spezielle bauliche Vorgaben (z. B. Krankenhaus, Flughafen etc.)

Klären Sie bereits im Vorfeld den Zeitraum, in dem lärmbelastete Arbeiten, wie beispielsweise das Bohren von Durchbrüchen, ausgeführt werden können. Sie sollten bei den baulichen Maßnahmen auch daran denken, dass andere Kollegen unter Umständen terminliche Aufgaben erledigen müssen.

8.6 Dokumentation

Die Erstellung einer Dokumentation für eine Kommunikationsinfrastruktur sollten Sie bereits während der Durchführung der Maßnahme beginnen. Dabei sind bestehende Vorgaben und Standards wie Dokumentationsrichtlinien und Kennzeichnungssysteme einzuhalten. Beispielhaft sei auf die Dokumentationsrichtlinie für Bauten des Bundes sowie das zugehörige Anlagenkennzeichnungssystem verwiesen. Die Dokumentation ist besonders wichtig, um künftige Erweiterungen zu planen oder wenn ein neuer Kollege eingearbeitet werden soll. Die Gesamtübersicht einer Kommunikationsinfrastruktur kann Ihnen beispielsweise eine schnelle Aussage über die Verfügbarkeit von freien oder belegten Anschlüssen geben. Grundsätzlich sollten Sie die gesamte Dokumentation Ihres Netzwerkes in einem einzigen Ordner ablegen. Unterteilen Sie Ihren Ordner in die entsprechenden Rubriken, wie beispielsweise aktive Komponenten.

Zu einer übersichtlichen Dokumentation gehören in jedem Fall:

- ✓ Aufbauzeichnungen
- ✓ Übersichtspläne und Strukturschemen
- ✓ Panel- und Anschlussbelegungen
- ✓ Messprotokolle der Glasfaser- und Kupferleitungen
- ✓ Herstellerverzeichnis für spätere Erweiterungen
- ✓ technische Beschreibungen aktiver Komponenten
- ✓ Wartungshinweise

Aufbauzeichnungen

Aufbauzeichnungen sollten alle eingebauten aktiven und passiven Komponenten mit Angabe der Höheneinheiten beinhalten. Anhand dieser Aufbauzeichnungen sind Sie in der Lage, sofort Auskunft über verfügbare Reserven in Ihrem Netzwerk zu erteilen. Auch für spätere Erweiterungen sind Aufbauzeichnungen eine gute Diskussionsgrundlage. Aufbauzeichnungen für Datenschränke sollten Folgendes beinhalten:

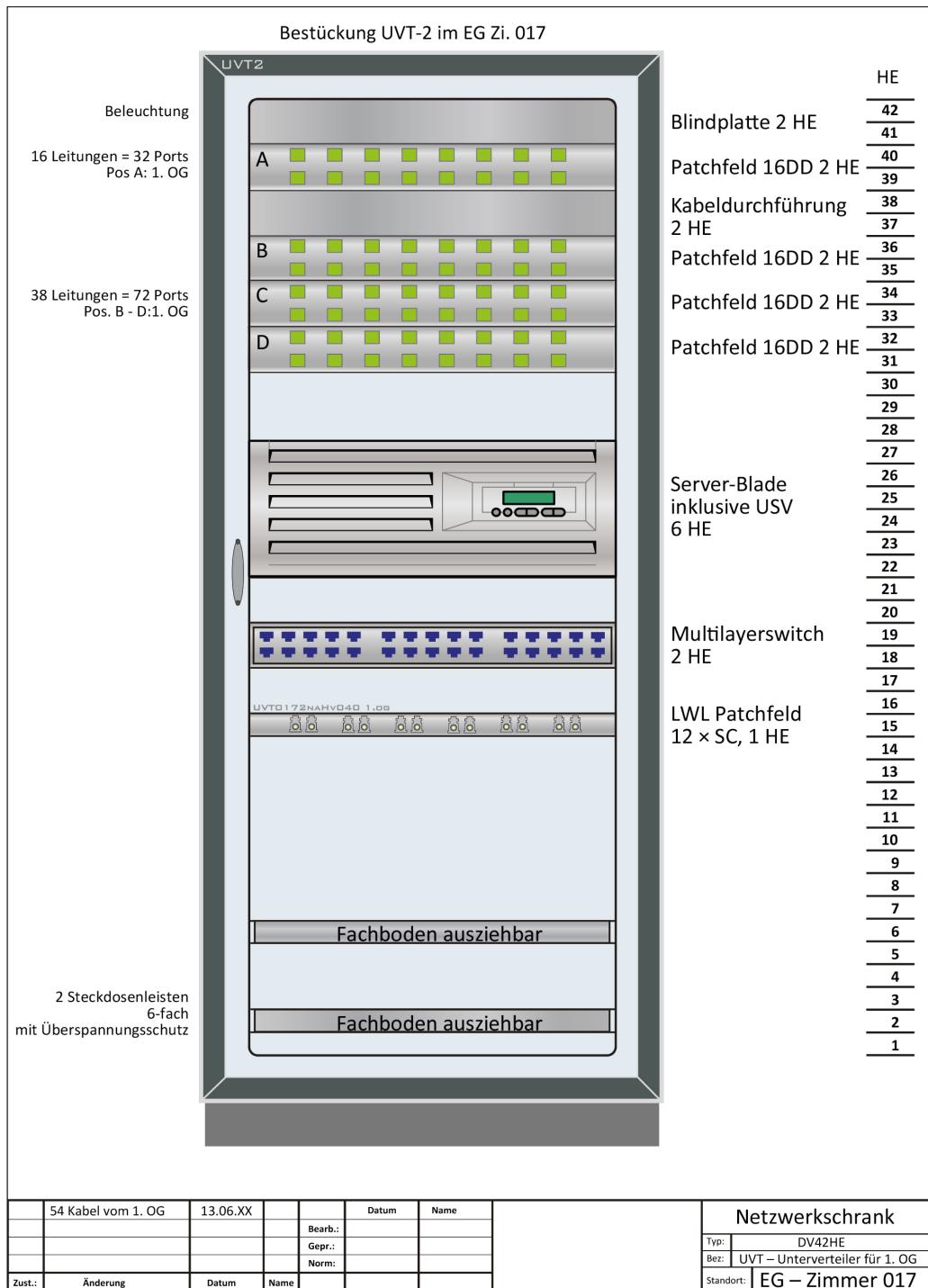
- ✓ Angaben zum Standort des Verteilers (Art, Etage, Zimmer, Nutzung)
- ✓ Angabe der Größe mittels Höheneinheiten
- ✓ Bezeichnung der Verteilerschränke
- ✓ Einteilung von Kupferpanels, Glasfaserpanels und aktiven Komponenten
- ✓ Hinweise zur Schrankbeleuchtung und Klimatisierung
- ✓ Beschreibung zu den verwendeten Schranküberwachungen (Sicherheitskontakte, Sensoren)
- ✓ Anzahl der Steckdosenleisten und Stromkreise
- ✓ Anzahl der Ports bzw. Kabel pro Panel
- ✓ Beschriftungsnomenklatur für die Anschlüsse

Die Dokumentation kann sowohl handschriftlich als auch mit Hilfe einer EDV-Anlage erfolgen. Der besondere Vorteil bei der Nutzung eines Computers liegt in der automatisierten Erfassung von Netzwerkparametern, die einheitliche Darstellung der Systeme und die einfache Überarbeitung der Unterlage. Weiterhin sind alle Beschriftungen eindeutig und klar lesbar und bedürfen keiner Interpretation von handschriftlichen Notizen.

Mithilfe von Screenshots und digitalen Fotografien können Konfigurationseinstellungen von Komponenten oder webbasierenden Systemen sauber dokumentiert und Schritt-für-Schritt-Anleitungen erstellt werden. Geeignet sind sowohl kommerzielle als auch Open-Source-Textverarbeitungssysteme (z. B. Word/Writer), Programme für die Erfassung von Notizen (z. B. OneNote/Evernote) und Anwendungen für die Erstellung von Zeichnungen, Schaltplänen und Raumplänen (z. B. Visio, Dia, Network Notepad).

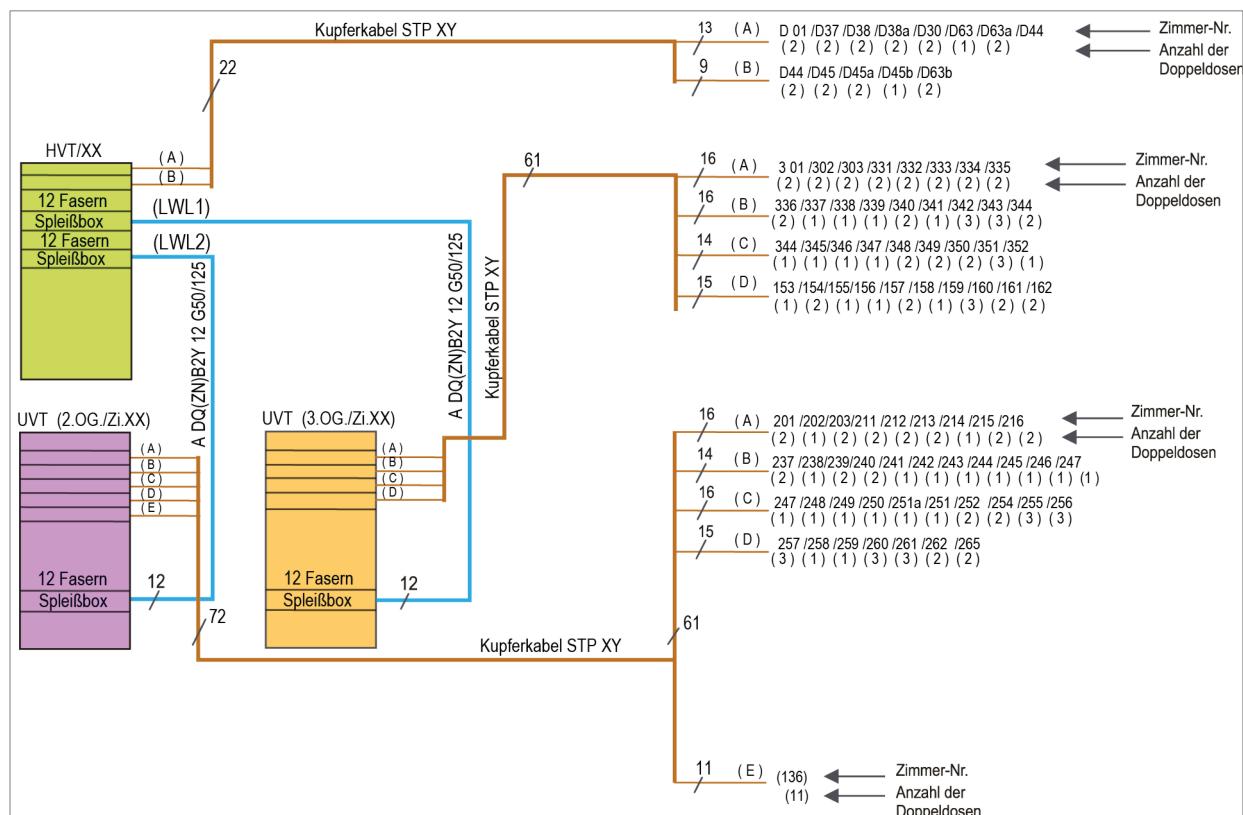
Ein Beispiel für die automatische Erfassung von Netzwerkparametern, Topologien und Diensten im Netzwerk wäre beispielsweise die Anwendung „Docusnap“. Tabellarische Darstellungen lassen sich mit einem Tabellenkalkulationsprogramm wie z. B. Excel oder Calc erstellen.

Das Ergebnis eines elektronisch dokumentierten Schranksystems finden Sie auf der nachfolgenden Seite.

*Schrankaufbauzeichnung*

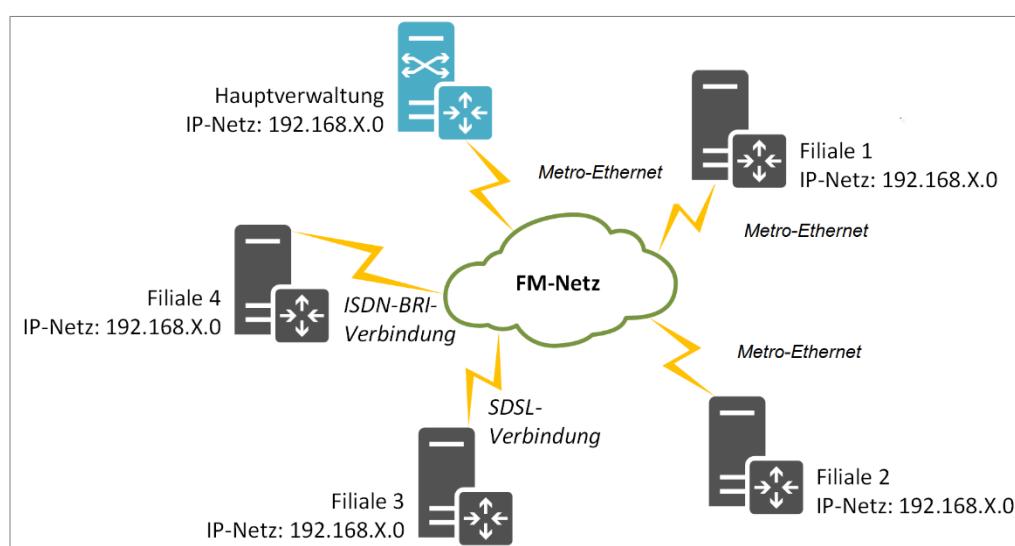
Übersichtspläne

Diese dienen dazu, eine vollständige Übersicht über die Infrastruktur eines Netzwerkes zu erhalten. Übersichtspläne sind in Form von Blockdiagrammen oder Verkabelungsübersichten auszuführen. Sie geben keine Auskunft über verfügbare Reserven. Es ist häufig sinnvoll, Übersichtspläne für aktive Komponenten und die passive Verkabelung getrennt voneinander zu erstellen. Solche Blockdiagramme können auch dazu verwendet werden, um ein Netzwerk in der Planungsphase darzustellen.



Übersichtsplan Gebäudeverkabelung

Die Vernetzung mehrerer Standorte über eine WAN-Struktur könnte beispielsweise so aussehen:



Übersichtsplan Netzstruktur und Verbindungen zum Provider

Panel-Anschlussbelegung

Panel-Belegungspläne beinhalten die laufende Nummerierung der Anschlusspanels (Kupfer, Glasfaser) sowie die jeweilige Zuordnung der Einzelkabel zu Zimmernummer und Etagenebene. Panelbelegungen sind besonders bei einer Inbetriebnahme oder auch bei der Fehlersuche sehr hilfreich. Der entsprechende Anschluss wird ermittelt und Sie können sofort erkennen, auf welcher Etage und in welchem Zimmer sich der entsprechende Anschluss befindet.

Patchfeld RJ 45 – 24 Port											
MONTEUR											
Buchse	Etage	Zimmer	Buchse	Etage	Zimmer	Buchse	Etage	Zimmer			
1			9			17					
2			10			18					
3			11			19					
4			12			20					
5			13			21					
6			14			22					
7			15			23					
8			16			24					

Patchpanel-Anschlussbelegung für Twisted-Pair-Verkabelung

Messprotokolle

Je nach Umfang und Anzahl Ihrer Netzwerkanschlüsse kann es passieren, dass Sie bis zu hundert oder mehr Messprotokolle für Ihre Ports haben. In so einem Fall ist es ratsam, die Messprotokolle auf einem Datenträger (CD-ROM) zu speichern und im Revisionsordner abzulegen. Es müssen alle Anschlüsse des gesamten Netzes überprüft werden. Eine spätere Fehlersuche ist auch bei einem sternförmigen Netzwerk mit mehreren Anschlüssen sehr aufwendig. Die Parameter für eine Abnahmemessung finden Sie in Abschnitt 6.5.

Bei Längenproblemen (Strecken über 90 Meter) sollten Sie das entsprechende Messprotokoll farbig kennzeichnen. Auch bei einer noch so guten Planung und Längenschätzung kann es zu Änderungen während der Arbeiten kommen. Achten Sie auch darauf, dass die Zuordnungen von Messprotokollnamen zu Zimmernummern eindeutig und immer aussagefähig sind.

Herstellerverzeichnis

Herstellerverzeichnisse beinhalten alle relevanten Angaben zu den verwendeten Produkten und deren Herstellern bzw. Lieferanten. Bei späteren Erweiterungen, Änderungen oder Reklamationen sind diese Angaben äußerst hilfreich, da Sie auf einen Blick alle Informationen für Ihre Bestellung zur Hand haben. Ein Herstellerverzeichnis wird in Form eines Tabellenblattes angelegt und fortlaufend gepflegt. Wenn Sie einen neuen Hersteller oder ein neues Produkt in Ihrem Netzwerk verwenden, dann sollten Sie die entsprechenden Angaben hierüber unbedingt im Herstellerverzeichnis ergänzen.

Folgende Angaben sollten Sie in einem Herstellerverzeichnis auflisten:

- ✓ Name und Anschrift der Hersteller bzw. Lieferanten
- ✓ Original-Herstellernummer und Artikelbezeichnung der passiven Komponenten
- ✓ Herstellerangaben und Datenblätter für die verwendeten Datenkabel (Kupfer, Glasfaser) und Steckverbinder
- ✓ Angabe zur Farbe der Anschlüsse (RAL9010 für reinweiß)

Dokumentation von aktiven Komponenten

Die den aktiven Komponenten beigefügten Dokumentationen beschreiben lediglich die Funktionsweise der Geräte und beinhalten die technischen Eigenschaften der entsprechenden Komponenten. Es werden aber keine Aussagen über die kundenspezifischen Daten der Komponenten getroffen. Diese sollten jedoch für spätere Wartungsarbeiten und eventuelle Ausfälle oder auch für die Fehlersuche ermittelt werden. Die kundenspezifische Dokumentation für aktive Komponenten sollte ähnlich aufgebaut sein wie ein Herstellerverzeichnis. Listen Sie alle Geräte tabellarisch auf und tragen Sie in einer eigenen Spalte den Standort des Gerätes ein.

Betrachten Sie die kundenspezifische Dokumentation Ihrer aktiven Komponenten als eine Art Inventarliste, die Sie als Netzwerkverantwortlicher zu erstellen und zu pflegen haben. Sie sollten dabei Folgendes in Ihrer Liste berücksichtigen:

- ✓ Standort der Geräte, mit Angabe von Gebäude, Etage und Raumnummer
- ✓ IP-Adresse der Komponenten (sofern vorhanden/ auch bei SNMP-Adaptoren)
- ✓ Seriennummer des Herstellers für ein Gerät
- ✓ Gewährleistungszeitraum und Austauschszenario (z. B. Vorort-Service, BringIn, etc.)
- ✓ genaue Herstellerbezeichnung des Gerätes (wichtig u. a. für die Ersatzteilbeschaffung)
- ✓ Art und Funktionsweise des Gerätes (z. B. 24-Port-Switch mit zwei modularen Steckplätzen)
- ✓ MAC-Adresse des Gerätes (sofern vorhanden)
- ✓ fortlaufende Gerätenummer bzw. interne Gerätetypbezeichnung (z. B. Switch_24P_EG_R251)
- ✓ Firmwareversion der Geräte

Viele aktive Komponenten besitzen die Möglichkeit, diese über das IP-Protokoll remote per telnet, ssh, http, https oder snmp zu verwalten. Bei diesen aktiven Komponenten können Sie über einen entsprechenden Menüpunkt Ihre Daten eintragen:

- ✓ System-Name (Gerätename)
- ✓ Kontaktperson (Administratorname)
- ✓ Konfigurationseinstellungen
- ✓ Gerätebeschreibung

Im Falle einer Fehlersuche helfen diese Informationen, da Sie umgehend Klarheit darüber erhalten, ob es sich bei der Komponente auch um das gewünschte Gerät handelt.



Wissenstest: Installation und Planung

9 Lokale Netzwerke (LAN)

In diesem Kapitel erfahren Sie

- ✓ wie Sie Ihren Bedarf an einem Wireless-System ermitteln und welche Voraussetzungen Sie schaffen müssen
- ✓ wie Sie ein Wireless-System realisieren können
- ✓ wie Sie einen kabelbasierenden Switch installieren und konfigurieren
- ✓ wie Sie Fehler am Switch lokalisieren können
- ✓ wie IP-Adressen aufgebaut sind und wie Sie diese umrechnen
- ✓ wie Sie Subnetze erstellen und was bei der Weiterleitung von IP-Paketen zu beachten ist
- ✓ wie Sie Router konfigurieren und prüfen

Voraussetzungen

- ✓ Wissen über den Aufbau von Verkabelungen
- ✓ Betriebssystem-Kenntnisse
- ✓ Grundkenntnisse im technischen Englisch
- ✓ Grundkenntnisse in der binären Schreibweise
- ✓ Wissen über die Funktionsweise von Routern

9.1 Wireless LAN (WLAN)

Einführung

In lokalen Netzen haben sich zwei Standards fest etabliert. Das sind einerseits der **Ethernet**- und andererseits der **WLAN**-Standard. Letzterer stellt eine Modifizierung des Ethernet-Protokolls über elektromagnetische Wellen dar. WLAN wird vorwiegend in Bereichen eingesetzt, wo eine Verkabelungsstruktur unzweckmäßig wäre bzw. nicht realisierbar ist, z. B.:

- ✓ Nutzer mit mobilen Geräten
- ✓ Einsatz im Heimbereich
- ✓ Nutzung im medizinischen Sektor
- ✓ Kommunikation an Orten mit Denkmalauflagen
- ✓ mobile Fahrzeugkommunikation

Neben dem Vorteil der standortunabhängigen Kommunikation der Nutzer zeigen die WLAN-Standards auch einige Schwächen. Das sind die geringeren Datenübertragungsraten gegenüber der drahtgebundenen Technologie, der langsamere Verbindungsaufbau, mögliche Störeinflüsse im Funknetz u. a. durch vorhandene Bluetooth- und DECT-Geräte, Überbelegungen des Frequenzbandes und das Feldstärkeproblem bei ungünstigem Standort des Nutzers.

Das WLAN-Protokoll wurde von der IEEE in den Standards IEEE 802.11 (WLAN) und IEEE 802.16 (WiMAX) festgeschrieben. Beide Standards legen unter anderem die genutzten Frequenzbereiche (2,4 bzw. 5GHz bei WLAN und 3,4–3,8 GHz bzw. 10–66 GHz bei WiMAX), die verwendeten Modulationsarten (DSSS, FHSS, OFDM), die erforderliche Sendeleistung und die Bruttodatenübertragungsraten (11/54/108/300/600/1300/6900 Mbit/s) fest. Weitere Informationen (in englischer Sprache) zum Stand der Norm IEEE 802.16 finden Sie hier:

https://en.wikipedia.org/wiki/IEEE_802.16

Da der nutzbare Frequenzbereich beschränkt ist, werden hohe Datenraten nur durch Bündelung der Frequenzkanäle in den jeweiligen Frequenzbereichen durch das MIMO-Verfahren erreicht. Die Nettoübertragungsraten liegen jedoch weit darunter (Faktor 2–4). Das liegt an folgenden Gründen:

- ✓ Eine ungenügende Ausrichtung des Endgerätes/Access-Points innerhalb der Funkzelle (geringe Feldstärke innerhalb der Funkzelle)
- ✓ Die integrierten Netzwerkkarten mobiler Endgeräte haben oft nicht die Protokollfunktionalität MIMO (engl. Multiple Input Multiple Output), um mehrere Kanäle des Access-Points für die Datenübertragung zu bündeln, integriert. Der MIMO-Standard (IEEE802.11ac) wird nur bei aktuellen Netzwerkkarten unterstützt.
- ✓ Der Protokoll-Overhead (WLAN-Header, IP/IPv6-Header, TCP/UDP-Header) beträgt ca. 3–7 %.
- ✓ Überlappungen der Frequenzkanäle und daraus resultierende Funkstörungen durch andere Access-Points in der gleichen Funkzelle beeinträchtigen die Übertragung.
- ✓ Die WLAN-Verschlüsselung reduziert die reale Übertragungsrate erheblich.

Während man früher WLAN-Netzwerke finden konnte, die im Peer-to-Peer Modus betrieben wurden, trifft man heute nahezu ausschließlich auf Konstrukte, die im Infrastrukturmodus betrieben verwenden. Beim Peer-to-Peer-Modus verbinden sich die WLAN-Geräte direkt miteinander, ohne einen Access-Point zu nutzen. Diese Betriebsart ist mit der einfachen Vernetzung von zwei Computern über ein Crossover-Kabel vergleichbar und besonders im Hinblick auf die Sicherheit technisch überholt.

WLAN-Access-Points können in verschiedenen Infrastruktur-Modi betrieben werden. Aufgrund unterschiedlicher Firmwareimplementierungen wird nicht jeder Modus auf jeder Hardware unterstützt:

- ✓ **Basis Service Set (BSS):** zur drahtlosen Anbindung von Systemen in einem Access-Point
- ✓ Ethernet-Bridge: zur Kommunikation zwischen Ethernet und WLAN (Bestandteil des BSS)
- ✓ Extended Service Set (ESS): die drahtgebundene Verbindung mehrerer Access-Points
- ✓ Wireless Distribution System (WDS): die drahtlose Verbindung mehrerer Access-Points
- ✓ Wireless Bridge: zur Erweiterung der Reichweite durch Bildung einer neuen Funkzelle. Die Datenübertragungsraten bleibt bestehen.
- ✓ Wireless Repeater: zur Erweiterung der Reichweite der Funkzelle. Die Übertragungsraten wird dabei um 50 % reduziert.

Besonders im Heimbereich sind die sogenannten „Router“ häufig mit einem WLAN-Access-Point ausgestattet und unterstützen auf dem Layer 2 PPPoE (Point to Point Protocol over Ethernet). Tatsächlich handelt es sich aber um ein Kombigerät, welches in aller Regel über eine Switch-Komponente, WLAN-Access-Point, DSL/Kabel-Modem, NAT (Network Address Translation) und Paketfirewall verfügt.

Der Access-Point dient zur Verbindung der Wireless-Clients mit dem Wired-Netzwerk. Das DSL/Kabel-Modem verbindet das gesamte Netzwerk mit einem WAN. Über den Switch können mehrere Geräte mit dem Kabelnetzwerk verbunden werden. NAT sorgt für die Umadressierung der (in der Regel privaten) Netzwerk IP-Adressen zur IP-Adresse der WAN-Schnittstelle und zurück.

9.2 WLAN-Sicherheitsaspekte

Sicherheit ab Werk

In den Access-Points, die heute überwiegend eingesetzt werden, wird das Setup größtenteils durch Plug&Play erleichtert. So kann ein Systemadministrator ohne viel Aufwand neu zugekaufte WLAN-Hardware in sein vorhandenes Netzwerk einbinden. Leider wird aufgrund der verwendeten Plug&Play-Einstellungen häufig nicht daran gedacht, die herstellerseitig konfigurierte SSID (Service Set Identifier) oder einfacher ausgedrückt, den Namen des Funknetzwerkes, zu ändern. Diese sollte unbedingt nachträglich vom Systembetreuer erledigt werden. So sollten Sie für Ihren Access-Point eine SSID wählen, die keine Rückschlüsse auf Ihre Infrastruktur zulässt und die SSID konfigurationstechnisch verbergen.

Access-Points antworten auf Broadcasts, um Clients das Auffinden von nahen APs zu ermöglichen. Dies kann jedoch auch von sogenannten „Wardrivern“ (Mobile Menschen mit Funknetzwerk-Scannern) genutzt werden, um nach installierten APs zu suchen. Schalten Sie die SSID-Broadcast-Funktion ab, wenn dies in Ihrer Hardware möglich ist. Achten Sie bereits beim Kauf von WLAN-Access-Points darauf, ob diese explizit eine Abschaltfähigkeit der Broadcast-Funktion besitzen. Auf diese Weise muss ein Client die SSID kennen, um überhaupt Zugang zum WLAN zu bekommen.

MAC-Filtering

Genauso wie kabelbasierende Netzwerkkarten besitzen auch WLAN-Karten und Access-Points eine MAC-Adresse. Viele Access-Points unterstützen die Verwendung einer MAC-Filterliste und lassen nur Verbindungen mit WLAN-Karten zu, deren MAC-Adresse für den Zugriff konfiguriert ist. Benutzen Sie dieses Feature und tragen Sie die in Ihrem Netzwerk erforderlichen MAC-Adressen der zugehörigen WLAN-Adapterkarten in die Filterliste auf dem Access-Point ein, um einem Missbrauch vorzubeugen. Denken Sie aber daran, dass auch MAC-Adressen von entsprechend ausgerüsteten Hackern gefälscht werden können. Leider ist der Verwaltungsaufwand für die Pflege von zugelassenen MAC-Adressen in Firmen so hoch, dass diese Schutzmaßnahme ab einer gewissen Firmengröße uninteressant wird. An dieser Stelle sollten Sie IEEE 802.1X nutzen, vorausgesetzt der Access-Point unterstützt dieses Protokoll. Das Abschalten des SSID-Broadcasts, MAC-Filtering sowie das Setzen einer Nicht-Default-SSID sollten zumindest den Gelegenheits-Surfer davon abhalten, zufällig in Ihr Netzwerk zu stolpern und dort zu versuchen, vertrauliche Daten einzusehen oder auf Ihre Kosten den Internetzugang zu nutzen.

WEP – Wired Equivalency Protocol

Das für WLANs ursprünglich angedachte Verschlüsselungsprotokoll WEP deutet schon in seinem Namen darauf hin, dass sein Einsatzzweck auf eine Sicherheit abzielte, die einer konventionellen Verkabelung entsprechen würde. Bevor die amerikanische Regierung die Krypto-Export-Regulierungen lockerte, wurde WEP mit einer Schlüssellänge von 40 Bits implementiert. Seit der Lockerung dieser Regulierung fanden sich zunehmend Produkte mit 128-Bit-Unterstützung für WEP. Ein Teil dieser 128 Bit ist der sog. Initialisierungsvektor (IV). Dieser IV ist eine Zufallszahl, die für jedes zu übertragende Paket neu generiert wird. Zusammen mit dem 104 Bit langen konstanten Preshared-Key (PSK englisch „vorher vereinbarter Schlüssel“) soll der IV dafür sorgen, dass selbst bei identischen Paketen, die verschickt werden, nicht dieselbe Verschlüsselungsschlüssel benutzt wird.

Die Verwendung des gleichen Schlüssels bei den versendeten Paketen hätte dann identisch verschlüsselte Pakete zur Folge. Seine Funktion kann ein bestimmter Initialisierungsvektor nur dann korrekt erfüllen, wenn er nur ein einziges Mal verwendet wird.

Shared Secret Keys

WEP arbeitet mit Shared Secret Keys. Das bedeutet für den Administrator, dass auf jedem WLAN-kompatiblen Gerät oder für jede WLAN-Karte derselbe WEP-Schlüssel installiert werden muss. Geräte mit unterschiedlichen Schlüsseln können nicht miteinander kommunizieren. Zusätzliche Probleme ergeben sich, wenn Sie in Betracht ziehen, dass Treibersoftware der WLAN-Karten die installierten WEP-Schlüssel teilweise unverschlüsselt in der Registry ablegt, wo sie von speziell konstruierten trojanischen Pferden oder von neugierigen Mitarbeitern problemlos ausgelesen werden können. Auch ein regelmäßiger Wechsel des WEP-Schlüssels, der empfehlenswert wäre, ist aufgrund der Verteilungsproblematik nur mit hohem Aufwand durchzuführen.

WEP bereits geknackt

Der Beweis, dass WEP nicht ausreichend sicher ist, wurde bereits im Sommer 2001 erbracht. WEP generiert fortlaufend Verschlüsselungsschlüssele, die auf dem installierten Shared Secret Key basieren. Die Analyse zeigte, dass diese generierten WEP-Schlüssele einander zu ähnlich waren, sodass ein Angreifer durch rein passives Mithören eine bestimmte Menge (ca. 5000 Pakete) an verschlüsselten Datenpaketen speichern konnte, um aus den gesammelten Informationen Rückschlüsse auf den verwendeten Shared Secret Key zu ziehen. Auf einschlägigen Internetseiten gibt es Tools (Airsnot, WEPCrack), die das Mithören und die anschließenden Analysen automatisieren und dem Hacker die mühsame Filterung und Berechnung des Secret Keys abnehmen.

Abhilfe für die größten Probleme

Nachdem die gravierenden Probleme von WEP bekannt geworden sind, wurde fieberhaft an besseren Sicherheitsprotokollen gearbeitet. Dabei wurde allerdings auch klar, dass diese neuen Standards nicht in Kürze verfügbar sein konnten.

Zusätzlich war abzusehen, dass man in einem neuen Standard nicht einfach einen neuen Verschlüsselungsalgorithmus vorschreiben kann, da in der bereits verkauften und im Einsatz befindlichen Hardware der verwendete RC4-Algorithmus hardwaremäßig implementiert worden war. Als Interimslösung wurde deswegen Ende 2002 der Standard WPA verabschiedet, der die wichtigsten Änderungen des endgültigen Sicherheitsstandards 802.11i vorwegnehmen sollte, und zwar in einer Form, in der er auch auf bereits verkaufter WEP-kompatibler Hardware läuft.

WPA

Wi-Fi Protected Access führt einen auf RC4 basierten neuen Algorithmus zur Verschlüsselung ein und verbessert das TKIP (Temporal Key Integrity Protocol). Des Weiteren wird die Authentifizierung der Datenframes statt mit dem unbrauchbaren CRC32 nun mit dem Michael-Algorithmus durchgeführt. (vgl. https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2012-08-1/NET-2012-08-1_03.pdf)

Als eine der wichtigsten Verbesserungen in WPA ist aber die Tatsache anzusehen, dass das festgelegte Passwort in WPA nicht mehr der Verschlüsselungsschlüssel selbst ist, sondern die Schlüssel mit kryptografisch gesicherten Methoden hergeleitet und regelmäßig erneuert werden. Die Schlüssel werden automatisch in einem Zeitraum erneuert, in dem es mit üblichen Methoden nicht mehr möglich erscheint, diese Schlüssel zu knacken.

Zusätzlich sieht WPA auch die Unterstützung von RADIUS-Servern (Remote Authentication Dial-In User Service) zur Authentifizierung der Funkteilnehmer vor. Dies ermöglicht es dem Administrator, die Authentifizierung einzelner Benutzer über den RADIUS-Server anhand von zentral gespeicherten Domänenaccounts einer Firma zu bewerkstelligen. Das ist eine deutlich elegantere Lösung, als allen Benutzern ein und denselben Preshared Key geben zu müssen.

802.11i/WPA2

Im Juni 2004 wurde der endgültige WLAN-Sicherheitsstandard mit der Bezeichnung IEEE 802.11i verabschiedet. Wi-Fi Protected Access 2 (WPA2) ist ein Teil des Standards. Die wesentlichen Kernpunkte, die im WPA schon vorweggenommen wurden (wie z. B. regelmäßige automatische Erneuerung der verwendeten Verschlüsselungsschlüssel, Radius-Authentifizierung), blieben erhalten.

Anstatt des betagten RC4-Verschlüsselungsalgorithmus bzw. seiner Ableitung TKIP und dem Michael-Algorithmus zur Authentifizierung wird hier nun der moderne Standardalgorithmus AES (Advanced Encryption Standard) verbindlich vorgeschrieben. Ein Funknetz, das mit 802.11i-Verschlüsselung betrieben wird, kann als wesentlich sicherer angesehen werden als ein WEP- oder sogar ein WPA-Netzwerk. Allerdings sollte man dabei beachten, dass bei Absicherung eines Netzes mit Preshared Keys die Sicherheit nur so hoch sein kann wie die Komplexität des verwendeten Preshared Keys (also die Passwörter).

Wi-Fi Protected Setup (WPS)

Dieser von der WiFi-Allianz verabschiedete Standard ermöglicht einen vereinfachten und sicheren Aufbau eines WLAN-Netzwerkes inklusive automatischer Festlegung der Verschlüsselungsverfahren und der Schlüssel. Dies geschieht beispielsweise über eine einmalige PIN-Eingabe am zu integrierenden Gerät, der Anmeldung per Knopfdruck oder durch einfaches Platzieren des Gerätes in der Nähe des Access-Points (Near Field Communication). Das WPS-Verfahren sollten Sie nur während der Einbindung neuer Geräte aktivieren. Ansonsten besteht bei der WPS-PIN-Methode die Möglichkeit, über eine Brute-Force-Attacke den PIN in kurzer Zeit zu ermitteln.

Managed WLAN

Großflächige WLAN-Netzwerke, wie sie für die Datenkommunikation in Warenlagern oder der IP-Telefonie in mehrstöckigen Bürogebäuden gebraucht werden, lassen sich nicht mehr effizient mit einzeln konfigurierten Access-Points (APs) realisieren. Allein schon die Pflege einer einheitlichen MAC-Zugangstabelle, würde es bei jeder Änderung erforderlich machen, die Konfigurationsseite eines jeden APs aufzusuchen, um die Änderungen per Hand einzutragen. Solche Problemstellungen werden in der Praxis mit einem Managed WLAN gelöst, wo jeder einzelne AP die Konfiguration von einem zentralen WLAN-Controller automatisch bezieht. Im Ergebnis verfügt jeder AP über die gleichen Einstellungen, und ein flächendeckendes Roaming innerhalb des gesamten Netzwerks ist problemlos möglich. Erweiterungen oder der Austausch von defekten AP-Geräten kann mit einer minimalen Ausfallzeit erreicht werden, allerdings sind die Kosten für die Anschaffung deutlich höher.

9.3 Übung: Wireless-System planen

In dieser Übung gehen Sie von folgendem Ist-Zustand des Netzwerks aus:

- ✓ 2 Windows-2016-Server
- ✓ 14 PC-Systeme (Betriebssysteme Windows 10 und CentOS Linux)
- ✓ 2 Netzwerkdrucker
- ✓ 1 Switch 10/100/1000 MBit/s mit 24-Port

Aufgabenstellung

- Zwei Notebooks mit integriertem WLAN und 1 PC sollen im vorhandenen Netz integriert werden.

Die beiden Laptops sollen mittels Wireless LAN an das bestehende Netzwerk angebunden werden. Die Mitarbeiter sollen sich frei mit dem Laptop in den Bürobereichen bewegen können. Des Weiteren muss noch ein PC mit einer WLAN-PCI-Karte ausgestattet werden. Da sich dieser PC in einem Büro befindet, das durch ein Treppenhaus von den anderen Büroräumen getrennt ist, und bauliche Maßnahmen vom Vermieter nicht genehmigt werden, bietet sich hier die Lösung per WLAN an.



Integrierte WLAN-Adapter sind seit Jahren Standard in mobilen Computern. Es sind aber auch Geräte im Einsatz, bei denen WLAN im Bedarfsfall per USB- oder PCI-Adapter nachgerüstet werden kann.

Voraussetzungen

- ✓ 1 freier Port am Switch
- ✓ 1 freie Steckdose 230 V für den Access-Point am Installationsplatz
- ✓ 1 WLAN Access-Point
- ✓ WLAN-Karten oder WLAN-USB-Sticks



EXO Router und Access-Point, Quelle: D-Link



MIMO-WLAN-PCIe-Karte, Quelle: D-Link



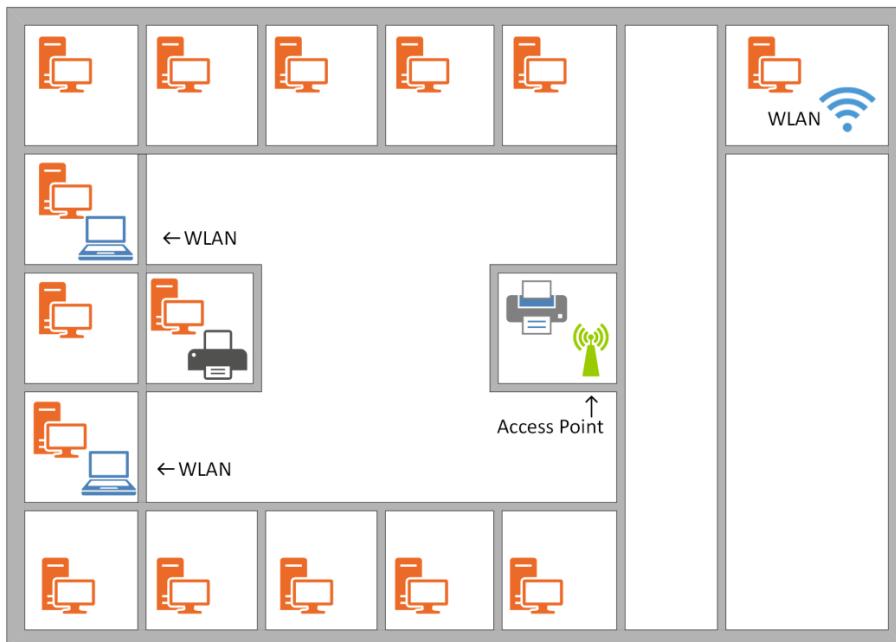
WLAN-USB-Adapter, Quelle: D-Link

Planungsgrundsätze

- ✓ Da die Reichweite des Funknetzes in Gebäuden etwa 30 Meter beträgt, sollte der Access-Point je nach örtlichen Gegebenheiten zentral montiert und funktechnisch ausgerichtet werden. Er muss mit dem bestehenden LAN verbunden werden.
- ✓ Es ist zu ermitteln, welche Datenübertragungsraten im WLAN und welche IEEE802.11-Standards erforderlich sind. Aktuell ermöglichen die meisten Access-Points Bruttodatenraten von 600 Mbit/s und mehr.
- ✓ Es sollte auch geprüft werden, ob der Access-Point gleichzeitig als Router für den Internetzugang dienen soll. Hierbei ist auf eine entsprechende Modellauswahl zu achten. Bei größeren Netzwerkstrukturen können mehrere Access-Points im Bridge-Modus eingesetzt werden, bei denen sich die Funkzellen jeweils überlappen müssen. So kann von einem Bereich in den anderen gewechselt werden.
- ✓ Vor der Installation sollte getestet werden, ob ein Access-Point für die flächendeckende Vernetzung ausreichend ist. Für diesen Test sollte ein Access-Point an der vorgesehenen Stelle installiert werden, um dann mit einem Mobil-Device die Ausleuchtung der Funkzelle (z. B. mit dem Tool HeatMapper) zu prüfen.
- ✓ Weiterhin ist darauf zu achten, dass Access-Points keinesfalls in Metall-Schränke eingebaut werden. Das Metallgehäuse (Faradayscher Käfig) würde den Access-Point sehr stark abschirmen. Dies mindert die Reichweite und die Übertragungsrate drastisch.

Wireless-System als LAN-Anbindung installieren und testen

Bei der Besichtigung der räumlichen Gegebenheiten wird festgestellt, dass sich in einem Gang ein Netzwerkdrucker befindet. Dieser liegt zentral und ist an eine Doppel-Datendose CAT-6A angeschlossen. Der zweite Port der Datendose ist frei und kann somit für die Verbindung des Access-Points verwendet werden.



Grundriss-Skizze

Das abseits liegende Büro hat eine geschätzte Entfernung von etwa 20 m, liegt also innerhalb der Reichweite des Access-Points. Auch die Arbeitsbereiche der beiden Laptops überschreiten die 30-Meter-Grenze nicht. Es ist also kein weiterer Access-Point nötig.

Anbindung des Access-Points über die Ethernet-Schnittstelle an das Netzwerk

Im Schrank befindet sich der 24-Port-Switch. Da bereits 16 PCs/Server und 2 Netzwerkdrucker an das Netzwerk angeschlossen sind, verbleiben 6 freie Ports. Über einen dieser freien Ports kann nun die Anbindung des Access-Points über die RJ-45-Dose im Drucker-Raum an das bestehende Netzwerk erfolgen.

WLAN-Karten einbauen und installieren

Nun kann die PCI-Express WLAN-Karte in den PC eingebaut oder ein USB-WLAN-Stick eingesteckt werden. Sie sollten aus Performancegründen darauf achten, dass bei dem WLAN-Adapter möglichst die MIMO-Funktionalität verfügbar ist. Da hier Windows 10 als Betriebssystem dient, wird die Karte durch Plug & Play automatisch erkannt. Es sollte jedoch überdacht werden, ob die vom Kartenhersteller mitgelieferten Treiber installiert werden, um ggf. zusätzliche Funktionsmerkmale zu nutzen.

WLAN konfigurieren

Alle aktuellen Access-Points verfügen über eine grafische Benutzeroberfläche bzw. mitgelieferte Software für die Konfiguration. Nach Studium der Bedienungsanleitung kann die WLAN-Verbindung konfiguriert werden. Für nicht mehr aktuelle Access-Points können Sie ggf. auch DD-WRT nutzen.

Info: Bei DD-WRT handelt es sich um eine quelloffene Linux-Distribution, die als Alternative für Router- bzw. Access-Point-Firmware fungiert und für Produkte z. B. von den Herstellern Allnet, Cisco, D-Link, Netgear u. a. eingesetzt werden kann. (<http://www.dd-wrt.com/site/support/router-database>).

Die Installation wird exemplarisch über die DD-WRT-Firmware dargestellt. Als Erstes sollten Sie den Wireless Mode ① überprüfen. Er ist per Default-Wert auf Access-Point (AP) eingestellt, d. h. der Access-Point übernimmt die Koordination der angeschlossenen Geräte zwischen Ethernet und WLAN. Der Wireless Network Mode ② erlaubt alle unterstützten WLAN-Protokolle (mixed). Sie sollten der SSID ③ der Funkzelle einen eindeutigen Namen geben und einen anderen nicht überlappenden Funkkanal ④ wählen. Im 2,4-GHz-Bereich sind viele Access-Points per Default auf Kanal 6 eingestellt. Wählen Sie sicherheitshalber einen anderen freien Kanal. Damit vermeiden Sie Funküberlappungen mit anderen Access-Points. Aus Sicherheitsgründen ist SSID Broadcast ⑤ abzuschalten. Die anderen Einstellungen können Sie mit Save übernehmen.

Physical Interface wl0 - SSID [linksys] HWAddr [68:7F:74:36:DA:B9]		Help	more...
Wireless Mode	AP	①	Wireless Network Mode: If you wish to exclude Wireless-G clients, choose <i>B-Only</i> mode. If you would like to disable wireless access, choose <i>Disable</i> . Note : when changing wireless mode, some advanced parameters are susceptible to be modified ("Afterburner", "Basic Rate" or "Frame Burst").
Wireless Network Mode	Mixed	②	
Wireless Network Name (SSID)	network_heim&AZ	③	
Wireless Channel	11 - 2.462 GHz	④	
Wireless SSID Broadcast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	⑤	
Sensitivity Range (ACK Timing)	2000	(Default: 2000 meters)	Sensitivity Range: Adjusts the ack timing. 0 disables ack timing completely for broadcom firmwares. On Atheros based firmwares it will turn into auto ack timing mode
Network Configuration	<input type="radio"/> Unbridged <input checked="" type="radio"/> Bridged		
Virtual Interfaces			
Add			
<input type="button" value="Save"/> <input type="button" value="Apply Settings"/> <input type="button" value="Cancel Changes"/>			

WLAN-Konfiguration mit der Firmware DD-WRT

Durch den Einsatz mehrerer Access-Points ist es möglich, innerhalb des WLAN-Netzes verschiedene WLAN-Gruppen einzurichten. Dies geschieht durch Zuweisung unterschiedlicher SSIDs auf den jeweiligen Access-Points. Sollen mehrere Access-Points zusammengefasst werden (Roaming), dann muss die zugewiesene SSID auf allen Access-Points identisch sein. Der WLAN-Client meldet sich dann automatisch am stärksten Access-Point an und wechselt den Access-Point selbstständig, wenn die Empfangseigenschaften nicht mehr für eine problemlose Datenübertragung ausreichen.

Weiterhin muss jeder Access-Point eine eindeutige IP-Adresse ① sowie einen Gateway- und DNS-Eintrag ② erhalten. Für die angeschlossenen Clients im LAN dient der Access-Point oft als DHCP-Server ③, womit sich deren Anmeldung vereinfacht. Hierzu vergeben Sie die Startadresse des DHCP-Adressen-Pools, die Anzahl der DHCP-User ④ und deren Gültigkeitsdauer sowie die Adressen der erforderlichen Nameserver ⑤.

Network Setup	
Router IP	
Local IP Address	192.168.1.100 ①
Subnet Mask	255.255.255.0
Gateway	192.168.1.1 ②
Local DNS	190.168.1.1
Network Address Server Settings (DHCP)	
DHCP Type	DHCP Server ③
DHCP Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Start IP Address	192.168.1.101
Maximum DHCP Users	50 ④
Client Lease Time	8400 minutes
Static DNS 1	192.168.1.1
Static DNS 2	217.44.127.9 ⑤
Static DNS 3	0.0.0.0
WINS	0.0.0.0
Use DNSMasq for DHCP	<input checked="" type="checkbox"/>
Use DNSMasq for DNS	<input checked="" type="checkbox"/>
DHCP-Authoritative	<input checked="" type="checkbox"/>

IP- und DHCP-Konfiguration des Access-Points

Wireless-Systeme testen

Nach Abschluss der Treiberinstallation bzw. Anpassung der Netzwerkprotokolle kann die WLAN-Verbindung getestet werden.

- ✓ Der Client muss sich in der Arbeitsgruppe bzw. Domäne anmelden können.
- ✓ Der Datentransfer zwischen Client und Server oder anderen Clients muss möglich sein (sofern freigegeben).
- ✓ Der Zugriff auf freigegebene Drucker muss gewährleistet sein.

Die Laptops müssen auch im Grenzbereich der Büroräume eine unterbrechungsfreie Funkverbindung haben. Dies sollte an verschiedenen Positionen im Gebäude getestet werden.

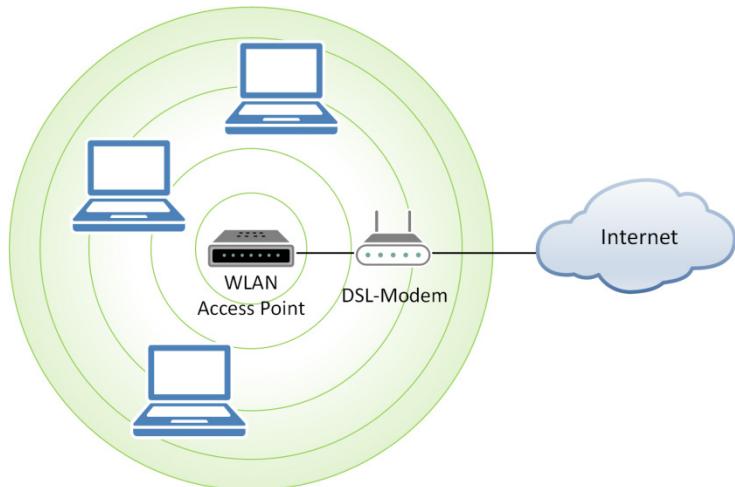
9.4 WLAN als drahtloser Internetzugang

Auswahl der Geräte

Wie bei der WLAN/LAN-Kopplung ist auch hier die Auswahl der Geräte von entscheidender Bedeutung. Je nach Anzahl der WLAN-Clients sollte auf eine ausreichende Übertragungsrate des Access-Points geachtet werden. Soll beispielsweise nur ein Notebook im Heimbereich einen drahtlosen Internetzugang erhalten, genügt ein Access-Point mit einer Übertragungsrate von 108 Mbit/s. Wenn sich mehrere Notebooks/PCs im WLAN befinden und somit ein Netzwerk bilden, sollte auf eine Ausführung mit mindestens 600 Mbit/s und mehr zurückgegriffen werden. So ist ein effizienterer Datenaustausch der Clients innerhalb des WLAN-Netzwerks möglich.

WLAN-Karten für Clients sind in folgender Anschlusstechnik verfügbar:

- ✓ PCI/PCI Express (für PC)
- ✓ USB (für Notebook/PC)



WLAN-Aufbau (Basic Service Set) in der Übersicht



Voraussetzung für WLAN als drahtlosem Internetzugang ist ein betriebsfähiger DSL/Kabel-Anschluss zu einem Provider. Die Authentifizierung gegenüber dem Provider erfolgt dabei mit PPPoE (PPP over Ethernet).

Installation und Inbetriebnahme des Access-Points

Nachdem der Access-Point angeschlossen wurde, ist er bereits betriebsbereit. Manche Access-Points sind so voreingestellt, dass ohne Konfiguration bereits eine Verbindung mit einem WLAN-Client hergestellt werden kann. Dies stellt jedoch ein Sicherheitsrisiko dar, sofern keine Verschlüsselung voreingestellt ist.

Installation und Inbetriebnahme des Clients

Um den Client im WLAN zu betreiben, müssen die entsprechende Hardware (z. B. WLAN-USB-Stick) und die mitgelieferte Software installiert werden. Detaillierte Angaben sind der Gebrauchsanweisung des jeweiligen Herstellers zu entnehmen. Nach einer fehlerfreien Installation kann bereits eine Verbindung zum WLAN hergestellt werden, um das Netzwerk zu konfigurieren. Die geschieht entweder über die mitgelieferte Software oder über einen Internet-Browser.

Konfiguration des Access-Points

Die detaillierte Konfiguration des Access-Points ist herstellerabhängig. Die wichtigsten Grundeinstellungen sind jedoch häufig identisch:

- ✓ Verschiedene Access-Points können als Router oder als Bridge funktionieren. Da in diesem Fall eine Verbindung zum Internet hergestellt werden soll, muss hier bei einem AP der IP-Router-Mode ausgewählt werden.
- ✓ Die TCP/IP-Parameter müssen auf DHCP gestellt sein, damit bei der Internetverbindung vom Provider eine IP-Adresse zugewiesen werden kann. Der Access-Point fungiert zum Provider als DHCP-Client und ins LAN als DHCP-Server.
- ✓ Anschließend werden die vom Internet-Provider erteilten Zugangsdaten unter PPPoE Username und Password eingegeben. Dabei muss Enable PPPoE aktiviert sein. Dies wird jedoch auch oft bei der Initialkonfiguration durch den Provider erledigt.
- ✓ Der Access-Point verfügt über einen integrierten DHCP-Server. Das bedeutet, dass an den Clients keine IP-Einstellungen vorgenommen werden müssen. Die IP-Adressen werden automatisch vergeben. Dieser Bereich kann unter DHCP-Setup verändert werden.

Aktuelle Tests haben gezeigt, dass noch einige wenige WLANs ungeschützt sind. So konnte beispielsweise von einem Parkplatz aus, mit einem Laptop, auf ein fremdes Firmennetzwerk zugegriffen werden. Die zur Verfügung stehenden Sicherheits-Features wie WPA2-Verschlüsselung und eventuell vorhandene Firewall sind unbedingt zu aktivieren. Zusätzlich sollte der Zugriff durch das Setzen von MAC-Adressen-Filtern verbessert werden.



Konfiguration der Clients

Nach erfolgreicher Installation wird die WLAN-Karte als Netzwerkkarte im Betriebssystem eingebunden. Durch die mitgelieferte Software kann der Client konfiguriert werden. Dort sind u. a. die Signalstärke, Empfangsqualität, Übertragungsgeschwindigkeit und die MAC-Adresse abzulesen. Bei aktiverter WPA2-Verschlüsselung ist darauf zu achten, dass der eingetragene Schlüssel (Preshared Key) mit dem des Access-Points übereinstimmt.

Ist beim Access-Point DHCP-Server für das LAN aktiviert, muss in den Eigenschaften der Netzwerkkarte der Clients unter TCP/IP-Eigenschaften die Einstellung *IP-Adresse Automatisch beziehen* aktiviert sein. Sollen statische IP-Adressen verwendet werden, muss dieses in den Netzwerkkarteneinstellungen entsprechend berücksichtigt werden.

Verwendung des DNS-Servers (Domain Name Service)

Um Namensauflösungen (Übersetzung von Netzwerknamen zu IP-Adressen: z. B. www.herdt.de) verwenden zu können, ist der Eintrag eines DNS-Servers erforderlich. Der DNS-Serverdienst wird seitens des Internet-Providers bereitgestellt. Die IP-Adresse des DNS-Dienstes wird im Access-Point über DHCP automatisch hinterlegt. Sie können auch einen alternativen DNS-Dienst statisch einstellen.

Fehlersuche im WLAN

Kann keine Verbindung vom Client zum Internet aufgebaut werden, kann dies verschiedene Ursachen haben:

- ✓ Befindet sich der Client im Sendebereich des Access-Points? (Signalstärke prüfen)
- ✓ Kann der Access-Point mit dem Befehl `ping` erreicht werden? (Netzwerkeinstellungen prüfen)
- ✓ Wurden die Zugangsdaten des Internet-Providers korrekt im Access-Point eingegeben? (PPPoE prüfen)
- ✓ Wurde bei aktiverter WPA2-Verschlüsselung der Schlüssel im Access-Point und im Client richtig eingegeben? (Preshared Key vergleichen)
- ✓ Wurde bei aktiviertem MAC-Adressen-Filter die MAC-Adresse richtig eingegeben? (Kontrolle der MAC-Filter-Tabelle)

Viele Hersteller von WLAN-Systemen integrieren einen WAN-Monitor oder Logfiles in ihrem System. Sie können bei der Fehlersuche von entscheidender Bedeutung sein. Darin ist u. a. zu sehen, ob überhaupt eine Verbindung zum Provider aufgebaut wird und ob die Anmeldung beim Provider korrekt erfolgt (korrekte Zugangsdaten).

9.5 Übung: Switch einrichten

Aufgabenstellung

In Ihrem Netzwerk wurden 16 zusätzliche PC-Arbeitsplätze durch eine Erweiterung der Verkabelung bereitgestellt. Sie sollen nun alle Arbeitsplätze mit einem Switch an das Netzwerk anbinden. Am vorhandenen Switch sind jedoch keine freien Ports mehr verfügbar. Sie müssen einen weiteren Switch in den Datenschrank einbauen und diesen in das bestehende Netzwerk integrieren. Zur Anbindung an das Backbone wird ein 10-Gbit-Up-Link-Modul verwendet. Anschließend ist es Ihre Aufgabe, die Verbindungen zu Ihrem Server und die Funktion des Switch-Gerätes zu überprüfen.

Checkliste

Bevor Sie den Switch auspacken und im Datenverteiler einbauen, sollten Sie Folgendes prüfen:

- ✓ Entspricht der gelieferte Switch Ihren Vorgaben für das Netzwerk?
- ✓ Haben Sie genügend Patchkabel? Benötigen Sie ggf. Cross-over-Patchkabel für eine direkte Switch-verbindung, sofern der Switch nicht über Auto-MDIX (automatisches Erkennen des Kabeltyps) verfügt?
- ✓ Ist im Datenschrank laut Aufbauzeichnung noch ausreichend Platz für das neue Gerät?
- ✓ Sind noch genügend freie Stromanschlüsse vorhanden, auch wenn der neue Switch eingebaut ist?

Auspacken und einbauen

- Legen Sie alle Komponenten griffbereit vor sich und packen Sie die Einzelkomponenten aus.
Besondere Vorsicht ist bei dem Up-Link-Modul geboten, da dieses durch elektrostatische Aufladungen zerstört werden kann.
- Überprüfen Sie nach dem Auspacken, ob das gesamte Zubehör vorhanden ist (Stromkabel, Befestigungswinkel, Dokumentation und ggf. notwendige Tools).
- Machen Sie sich mit der Dokumentation (Quick Installation Guide) für die Installation vertraut.
- Schieben Sie anschließend behutsam das Uplink-Modul in die vorgesehenen Positionen. Achten Sie dabei darauf, dass die Steckkontakte der Platine ordnungsgemäß einrasten.
- Nehmen Sie nun die mitgelieferten Befestigungswinkel und schrauben Sie diese seitlich an die dafür vorgesehenen Stellen.
Ziehen Sie die Schrauben fest an, da dies die einzige Halterung für den Switch darstellt.
- Anschließend bauen Sie die Kastenmuttern bzw. Gleitmuttern, je nach 19"-Profilschiene, auf die entsprechende Einbauhöhe für den Switch ein. Achten Sie beim Festschrauben darauf, dass die Schrauben fest angezogen sind und die Befestigungsbügel sich horizontal zum Schrank befinden. Sollte sich der eingegebauten Switch an der Rückseite nach unten neigen, sollten Sie die Befestigung am 19"-Schrank nochmals lösen und besser festschrauben. Ein unnötiges Kippen nach unten hat entsprechende Belastungen der Schrauben zur Folge, die dann auf die Dauer abgesichert werden könnten.



Befestigungswinkel für einen Switch

Funktionsprüfung

Wenn der Switch sachgemäß eingebaut ist, schließen Sie ihn an die Stromversorgung des Schrankes an. Der eingegebauten Switch führt nach dem Anlegen der Versorgungsspannung einen Selbsttest durch und überprüft seine Funktionsfähigkeit. Mithilfe der eingebauten Status-LEDs können Sie den Ablauf des Selbsttests verfolgen. Anhand der beigefügten Dokumentation können Sie dann nach erfolgter Selbstdiagnose den Status des Gerätes ermitteln.



Anhand der Status-LED können Sie die korrekte Funktionsweise Ihres Switches überprüfen. Leuchtet diese grün, liegen keine Störungen vor. Bei einer roten/orangen Status-LED-Anzeige ist Ihr Gerät defekt bzw. der Bootvorgang konnte nicht korrekt durchgeführt werden, und Sie müssen es ggf. austauschen.

Vorbereitung zur Konfiguration

Um einen Switch administrieren zu können, gibt es grundsätzlich drei Varianten:

- ✓ Konfiguration über eine vorhandene serielle Schnittstelle
- ✓ Administrierung über mitgelieferte Tools des Herstellers
- ✓ Konfigurieren über die Default-IP-Adresse des Gerätes mit Telnet/SSH bzw. http/https

Bei der Administration über die serielle Schnittstelle (RS232 oder COM) eines PCs oder Laptops müssen Sie das beiliegende serielle Anschlusskabel verwenden. Sofern Ihr Rechner über keine serielle Schnittstelle verfügt, hilft hier ein Seriell-to-USB-Adapter. Beim Switch befindet sich diese RS232-Schnittstelle an der Vorder- oder Rückseite des Gerätes. Die erforderlichen Übertragungsparameter für die serielle Verbindung entnehmen Sie der mitgelieferten Dokumentation des Gerätes. In vielen Fällen können Sie folgende Einstellungen benutzen:

Übertragungsrate	9.600 Baud
Datenbits	8
Parität	keine
Stop Bits	1
Flusskontrolle	keine bzw. ein

Wurde eine korrekte Verbindung zum Gerät erkannt, erhalten Sie nun die textbasierte Eingabeoberfläche (Command-line Interface). Die weiteren konfigurationstechnischen Schritte sind ausführlich in der dem Gerät beiliegenden Dokumentation beschrieben. Damit die Administrierung remote (entfernt) vorgenommen werden kann, benötigt das Gerät eine IP-Adresse. Bei konfigurierbaren Switchen ohne serielle Schnittstelle hat das Gerät eine Default-IP-Adresse bzw. ein beiliegendes Konfigurations-Tool zum Setzen der Adresse.

Die Schritte zur Vergabe einer IP-Adresse über eine serielle Verbindung sind:

- ▶ Stellen Sie eine physikalische Verbindung mit dem seriellen Schnittstellenkabel zwischen PC und Switch her.
- ▶ Starten Sie auf Ihrem Computer z. B. das Terminalprogramm PuTTY (der PuTTY-Client kann über die Webseite www.putty.org bezogen werden), stellen Sie die erforderlichen Übertragungsparameter ein und starten Sie den PuTTY-Client.
- ▶ Wählen Sie in der Switchkonfiguration den Punkt zum Eintrag der gewünschte IP-Adresse und Maske aus.
- ▶ Sichern Sie Ihre Eingaben und beenden Sie die Verbindung zum Switch.

Damit eine korrekte Funktion der eingegebenen IP-Adresse überprüft werden kann, können Sie den Befehl **ping <IP-Adresse des Gerätes>** verwenden.

Achten Sie darauf, dass eine korrekte Antwort nur erfolgen kann, wenn die IP-Adresse vom Gerät im gleichen Subnetzwerk liegt wie Ihr PC bzw. Laptop. Erhalten Sie eine Antwort vom Gerät, so ist die IP-Adresse richtig übernommen worden. Sollten Sie keine Antwort vom Gerät erhalten, prüfen Sie Folgendes:

- ✓ Hat Ihr System (PC, Laptop) am Netzwerk-Port über das angeschlossene Patchkabel einen Link?
- ✓ Hat Ihr System eine IP-Adresse und Maske aus dem gleichen Netzwerk?

Sind alle oben genannten Kriterien erfüllt, dann überprüfen Sie nochmals die Einstellungen an Ihrem Switch bezüglich der IP-Adresse und der Netzmaske. Sollte das Problem so nicht zu beheben sein, finden Sie im unten stehenden Absatz weitere Lösungsmöglichkeiten.

Link-Prüfung

Wurde die Diagnose erfolgreich abgeschlossen, dann können Sie mit dem Aufschalten der Verbindungsstrecken beginnen. Gehen Sie hierfür wie folgt vor:

- ▶ Schließen Sie das Patchkabel Ihrer PCs an die entsprechende Datendose an.
- ▶ Stellen Sie mit den Patchkabeln eine Verbindung zwischen Patchpanel und Switchport her.
- ▶ Überprüfen Sie, ob der angeschlossene PC eingeschaltet ist.

Wenn Sie diese drei Schritte ausgeführt haben und die Verbindungsstrecke vom Patchfeld zur Anschlussdose korrekt angeschlossen wurde, erhalten Sie an dem aufgeschalteten Switch-Port eine Link-Anzeige. Diese Link-Anzeige ist in den meisten Fällen eine grüne LED, welche die korrekte Verbindung vom Switch zur Netzwerkkarte im PC signalisiert. Wenn dieses nicht der Fall ist, sollten Sie noch einmal eine Sichtprüfung der hergestellten Verbindung auf korrekten Anschluss hin durchführen.

Konfiguration

Die erforderliche Administrierung eines Switches ist abhängig vom vorhandenen Netzwerkdesign. Standardmäßig ist ein Switch nach dem Einschalten in seiner Grundfunktionalität sofort einsatzbereit. In Abhängigkeit von seinem Funktionsumfang können bzw. sollten Sie folgende Einstellungen am Switch vornehmen:

- ✓ Ändern der administrativen Zugriffsrechte auf dem Gerät
- ✓ Setzen bzw. Modifizieren des Spanning-Tree-Protokolls (IEEE 802.1d/s/w)
- ✓ Angaben zum Switch wie beispielsweise Gerätename und Standort einstellen
- ✓ eventuell Einrichten eines Accounts für die User zur Abfrage von Statusinformationen
- ✓ Konfigurieren des oder der VLANs (IEEE 802.1Q)
- ✓ Class of Service (CoS) für die VLANs (IEEE 802.1p) bzw. Portpriorisierung festlegen
- ✓ Portsicherheit durch Setzen der MAC-Adressen, die über den Switch kommunizieren dürfen
- ✓ wenn andere Netzwerkteilnehmer das unterstützen (z. B. Server), Link Aggregation nach IEEE 802.1AX-2008 Clause 5 (früher IEEE 802.3ad bzw. unter dem Begriff „Trunking“ bekannt) einrichten. Dies dient zur Erhöhung des Datendurchsatzes und/oder zur Schaffung von Redundanz bei Leitungsausfällen.

Die Einstellungsoptionen von Switchen sind hersteller- bzw. produktabhängig. Managebare Switches sollten aber wenigstens über die oben aufgeführten Einstellungsmöglichkeiten verfügen. Die Konfigurationsoptionen sind umfassend in der Produktdokumentation (z. B. User Guide, Installation Guide) hinterlegt.

Uplink-Port

Uplink-Ports dienen zur hochperformanten Anbindung an das Backbone des Netzwerkes bzw. zur Verbindung zwischen Switchen. Sofern der Uplink-Port nicht benutzt wird, weil z. B. nur ein Switch im Netzwerk vorhanden ist, sollten Sie ihn für die Anbindung der Server verwenden.

Die Uplink-Ports verfügen über eine höhere Übertragungsrate als die restlichen Ports. Sofern der Switch über mehrere Uplink-Ports (in der Regel zwei) verfügt, können Sie darüber seine Verfügbarkeit (Redundanz) erhöhen. Dabei sind folgende Szenarien, die Sie über Konfigurationsparameter einstellen können, möglich:

- ✓ Ein Port ist aktiv, der zweite Port geht erst bei Ausfall des aktiven in Betrieb. Hierzu muss auf den Uplink-Ports das Protokoll Spanning-Tree (IEEE 802.1d/w/s) gesetzt sein.
- ✓ Beide Ports sind gleichzeitig aktiv. Dies ist mit der Konfiguration von Link Aggregation Control Protocol (LACP) auf den Ports realisierbar.

9.6 Fehleranalyse bei Switchen

Defekter Switch

Defekte Switches sind bei Neuanschaffung relativ selten. Da aber auch Netzgeräte bereits im Auslieferzustand defekt sein können, soll diese Fehlerquelle kurz dargestellt werden. Einen defekten Switch können Sie bereits beim Einschalten der Versorgungsspannung erkennen. Die häufigsten Merkmale sind:

- ✓ Der Switch läuft nicht an. Die LEDs bei der Selbstdiagnose bleiben aus.
- ✓ Die Status-LED beim Hochfahren des Gerätes leuchtet rot oder orange.

Link LEDs der Ports leuchten nicht

Diese Fehler sind häufig in der Praxis anzutreffen. Ihre Ursachen sind vor allem:

- ✓ Ein Switch-Port ist defekt.
- ✓ Eine Netzwerkkarte oder ein Patchkabel sind defekt.
- ✓ Die Anpassung der Übertragungsgeschwindigkeit (auto negotiation) schlug fehl.
- ✓ Das Datenkabel ist fehlerhaft oder falsch angeschlossen.
- ✓ Angeschlossener Port am Panel und Port an der Datendose stimmen nicht überein.

Bei nicht leuchtender Link-LED sollten Sie sich immer erst vergewissern, ob die Übertragungsstrecke korrekt verbunden und auch entsprechend gepatcht wurde. Wenn Sie sich nicht sicher sind, messen Sie noch einmal Ihre Übertragungsstrecke mit einem LAN-Messgerät nach. Denken Sie daran, dass auch ein Fehler in der Dokumentation oder Beschriftung zu einem falsch angeschlossenen Port führen kann.

Überprüfen Sie in jedem Fall die Patchkabel durch ein Austauschen gegen neue und funktionsfähige Kabel. Erst wenn Sie sicher sind, dass es nicht an der Übertragungstrecke sowie den Datendosen und Patchfeldern liegen kann, sollten Sie die Fehlersuche auf die aktiven Komponenten ausdehnen.

Überprüfen Sie, ob die Einstellungen der Netzwerkkarte und des gewählten Switch-Ports übereinstimmen. Hat beispielsweise die Netzwerkkarte eine fest eingestellte Übertragungsrate von 100 Mbit Half-Duplex, dann sollte auch der Port des Switches darauf eingestellt werden. Unterschiedliche Einstellungen können ggf. zu einer fehlerhaften Datenübertragung führen.

Prüfen Sie auch, ob die Netzwerkkarte ordnungsgemäß in Ihr Betriebssystem eingebunden ist und alle erforderlichen Protokolle und Bindungen vorhanden sind. Bei neuen Netzwerkkarten sollten Sie unbedingt deren Funktionsfähigkeit testen. Im Zweifelsfall können Sie auch eine bestehende, aber funktionierende Netzwerkkarte in den PC einbauen und den Link erneut prüfen.

Funktionstest mit Ping

Die einfachste Methode, eine Übertragungsstrecke zu prüfen, ist die Verwendung des Befehls *ping* im Terminalfenster (Eingabeaufforderung). Im Normalfall erhalten Sie bei einer funktionsfähigen Übertragungsstrecke eine Antwort auf Ihren gestellten Ping. Wenn Sie jedoch die Meldung *Zeitüberschreitung der Anforderung* erhalten, dann haben Sie entweder die falschen IP-Adressen verwendet oder die Übertragungsstrecke ist fehlerhaft.

Damit Sie die Fehlerursache lokalisieren können, sollten Sie die ping-Anforderung aufteilen. Um eine Prüfung von Teilstrecken durchführen zu können, benötigen Sie jedoch einen manageablen Switch mit einer konfigurierten IP-Adresse. Prüfen Sie hierzu die Verbindung vom Server zum Switch. Geben Sie an der Eingabekonsole den Befehl **ping <IP-Adresse Ihres Switch>** ein. Wechseln Sie nun zu dem neu aufgestellten PC und versuchen Sie von dort einen ping auf das Switch-Gerät. Erhalten Sie eine Rückantwort, dann ist die Übertragungsstrecke zum Switch korrekt.

Wiederholen Sie erneut den Ping-Befehl. Diesmal verwenden Sie jedoch die IP-Adresse vom Server. Erhalten Sie eine Rückantwort, so ist die Übertragungsstrecke in Ordnung. Erhalten Sie jedoch eine Fehlermeldung, können Sie davon ausgehen, dass der Switch-Port defekt ist oder falsch konfiguriert wurde. Führen Sie die beschriebenen Schritte auch unter Verwendung eines anderen Ports am Switch aus.

Aktuelle Windows-Betriebssysteme blockieren standardgemäß über die integrierte Firewall einen eingehenden Ping-Befehl. Um *ping* zu erlauben, müssen Sie die nachfolgenden Einstellungen in der Firewall durchführen:

Systemsteuerung → Windows-Firewall → Erweiterte Einstellungen → Eingehende Regeln → Datei- und Druckerfreigabe (Echoanforderung-ICMPv4 eingehend) für das vorhandene Firewall-Profil aktivieren.



9.7 IP-Routing verstehen und einrichten

Wozu die Netzwerkschicht benötigt wird

Wären zwei weit entfernte Netze, z. B. eines in Hamburg und eines in München über das Netzwerkkoppellement Hub miteinander verbunden, würden alle Daten aus Hamburg auch in München auftauchen und dort das Netz belasten, selbst, wenn die Pakete ausschließlich für Hamburg bestimmt sind (vgl. Hub 4.3). Würde man anstelle eines Hubs einen Switch verwenden, trüfe diese Aussage immer noch auf alle Broadcasts-Übertragungen zu. Auch ist es undenkbar, einen Switch zu entwerfen, der Millionen Geräte bedient. Dies wäre auch über eine Kaskadierung mehrerer Switches nicht machbar, da eine Flut von Broadcasts-Paketen auftreten würde und sich alle Millionen von MAC-Adressen merken müssten. Daher führte diese Problemstellung zur Entwicklung von Netzwerkgeräten, die auf der Vermittlungsschicht bzw. dem Network Layer arbeiten und zur Wegefindung IP-Adressen verwenden. Geräte, die auf der 3. Schicht des OSI-Modells arbeiten, werden als Router bezeichnet.

IP-Adressen

Im **Internet Protokoll der Version 4 (IPv4)** besteht eine Adresse aus 32 Bit. Aufgrund der besseren Lesbarkeit wurden die 32 Bit in vier Gruppen zu je acht Bit aufgeteilt, die in der dezimalen Notation mit einem Punkt voneinander getrennt werden. Die acht Bit großen Gruppen werden als **Oktette** bezeichnet. Jedes Oktett der IP-Adresse kann einen dezimalen Wert von 0 bis 255 annehmen.

Der IPv4-Adressraum mit seinen 32 Bit umfasst insgesamt 4.294.967.296 IP-Adressen. Der Übersicht halber wurden die Adressen in fünf **Klassen** unterteilt (A–E). Die Klassen A, B und C werden zur Adressierung von Geräten verwendet. Die Klasse D ist exklusiv für die Multicast-Funktion reserviert. Die letzte Klasse (E), wurde von der IANA als „for future use“ definiert und steht für zukünftige Zwecke zur Verfügung.

Die folgende Tabelle gibt eine Übersicht der IPv4-Adressklassen:

Klasse	Anfang der Adresse (binär)	IP-Adressbereich	Netzmaske	Max. Anzahl Hosts pro Netzwerk
A	0...	0.0.0.0 - 127.255.255.255	255.0.0.0	16.777.214
B	10...	128.0.0.0 - 191.255.255.255	255.255.0.0	65.534
C	110...	192.0.0.0 - 223.255.255.255	255.255.255.0	254
D	1110...	224.0.0.0 - 239.255.255.255		
E	1111...	ab 240.0.0.0		

Die Netzmaske

Die **Netzmaske** (engl. netmask) gibt einem Gerät die Information, welcher Teil einer IP-Adresse den Netzwerkteil der Adresse beschreibt und wieviele Bits zur Adressierung von Hostsystemen (Rechner und andere Netzwerkgeräte) innerhalb des Netzwerkabschnitts (Segment) verwendet werden. Für die Weiterleitung von Paketen in ein anderes Netzwerk ist nur der Netzwerkanteil (die Netzwerk-ID) interessant. Die Netzmaske ist keine Adresse, sondern eine Bitfolge, die es ermöglicht, den Netzwerk- und Hostanteil über eine binäre UND-Verknüpfung voneinander zu trennen. Sie besteht aus einer jeweils **zusammenhängenden fortlaufenden** Folge aus Einsen und Nullen und ist ebenfalls 32 Bit groß.

Gültige Netzmasken wären z. B.:

11111111 11111111 11111111 00000000 (255.255.255.0)
11111111 11111111 11100000 00000000 (255.255.224.0)

Netzmasken, bei denen sich Einsen und Nullen abwechseln wie bei „11111111 10001111 11111111 00000000“, sind für das Routen von Netzwerken **nicht** geeignet. Der Router würde hiermit eine falsche Routenentscheidung treffen oder eine Fehlermeldung ausgeben.

In diesem Buch werden binäre Werte zur besseren Lesbarkeit nach jeweils 8 Zeichen mit einem Leerzeichen getrennt.



CIDR (Classless Inter-Domain Routing)

Die Einteilung in Klassen ist durch Classless Inter-Domain Routing (**CIDR**) längst überholt. Mit CIDR entfällt die vorgeschriebene Zuordnung einer IP-Adresse zu einer Netzklasse. Es ist ein Verfahren zur besseren Nutzung des bestehenden 32-Bit-IP-Adressraumes und wurde 1993 eingeführt, um die Größe von Routing-Tabellen zu reduzieren und um die verfügbaren Adressbereiche besser auszunutzen. CIDR wird in den RFCs 1518, 1519 und 4632 beschrieben.

Aus der Sichtweise von CIDR gibt es nur ein Netz, das komplette Internet. Alle anderen Netzwerke sind **Subnetze** des Internets, die weitere Subnetze enthalten können, die wiederum Subnetze enthalten können usw. Lediglich die IP-Adressen aus dem Bereich der früheren Klasse D sind davon ausgenommen. Multicast ermöglicht das zeitgleiche Senden von Datenpaketen an viele Empfänger. Ein Beispiel hierfür wäre das Streamen eines Videos an eine definierte Benutzergruppe.

Die CIDR-Schreibweise

Jedes Netzwerk verfügt über seine eigene IP-Adresse, ist aber nur zusammen mit einer Netzmaske vollständig beschrieben. Ein Beispiel wäre das Netzwerk 192.168.1.0/**255.255.255.0**.

Mit CIDR hat sich eine weitere Schreibweise durchgesetzt. Da in einer Netzmaske die Anzahl der darin enthaltenen binären Einsen die Netzwerk-ID einer IP-Adresse definiert, ergibt sich die vereinfachte CIDR-Schreibweise (auch CIDR-Notation genannt), wie 192.168.1.0/**24**. Diese Notation beschreibt das Netz 192.168.1.0 mit einer Netzmaske mit 24 Einsen, die nachfolgend bis zur 32sten Stelle mit Nullen aufgefüllt wird, also dezimal 255.255.255.0.

Um nun die Netzwerk-ID aus einer IP-Adresse zu ermitteln, benutzt jedes Gerät, das IP-Pakete versendet, die boolesche Operation UND (engl. „AND“). Das Ergebnis einer AND-Operation ist nur dann 1, wenn alle verknüpften Bits auf 1 gesetzt sind.

Bit-Kombination	Ergebnis
1 AND 1	1
1 AND 0	0
0 AND 1	0
0 AND 0	0

Beispiel

Die IP-Adresse	192.168.1.20	binär	11000000 10101000 00000001 00010100
mit der Netzmaske	255.255.255.0	binär	11111111 11111111 11111111 00000000
<hr/>			
ergibt UND-verknüpft:			11000000 10101000 00000001 00000000
			----- Netzwerk ----- -- Host --

Die UND-Verknüpfung mit der Netzmaske ergibt hier die Netzwerk-ID 192.168.1.0. Der Hostanteil wird für die Weiterleitung eines Datenpakets nicht benötigt. Der Router erkennt durch den Vergleich mit den Einträgen in seiner sogenannten Routing-Tabelle, ob die IP-Adresse in einem der ihm bekannten Netzwerke vorkommt oder ob sie ihm unbekannt ist. Ist das Ziel bekannt, wird die Information über die Netzwerkschnittstelle verschickt, über die der Router das Zielnetzwerk erreichen kann. Andernfalls geht das Paket über die **Default-Route** heraus, die durch die Netzwerk-ID **0.0.0.0/0** gekennzeichnet ist und damit auf das gesamte „Internet“ verweist.

Richtlinien zur Adressierung

Es gibt Regeln für die Zuweisung von IP-Adressen. So sind insgesamt 3 Adressbereiche innerhalb der Adressklassen A–C für private oder Testzwecke vorgesehen, welche nicht in das Internet geroutet werden. Die Bereiche für private Adressen sind laut RFC 1918 (Address Allocation for Private Internet):

Klasse	Adressbereich	Verwendung
A	0.0.0.0 – 0.255.255.255	Platzhalter für „undefinede“ Adresse
A	10.0.0.0 – 10.255.255.255	private IP-Adressen (RFC 1918)
A	127.0.0.0 – 127.255.255.255	Loopback-Adressen (localhost bzw. 127.0.0.1)
B	169.254.0.0 – 169.254.255.255	Automatic Private IP Address (APIPA) *
B	172.16.0.0 – 172.31.255.255	private IP-Adressen (RFC 1918)
C	192.168.0.0 – 192.168.255.255	private IP-Adressen (RFC 1918)

* APIPA wurde von Microsoft entwickelt, um PCs mit gültigen IP-Adressen zu versorgen, falls der PC keinen DHCP-Server finden kann.

Die IP-Adressen aus diesen Bereichen sind keine offiziellen Adressen. Sie haben nur Gültigkeit im lokalen Netzwerk (Intranet). Sie können beliebig oft vorkommen und werden von Routern im Internet ignoriert. APIPA-Adressen (Automatic Private IP Addressing), die von Microsoft zur automatischen Konfiguration für Windows-Rechner ohne statische Adresse und ohne DHCP eingeführt wurden, werden ebenfalls nicht geroutet.

Nur offizielle IP-Adressen, die die Organisation IANA an regionale Organisationen (wie RIPE NCC) vergibt, sind einmalig und generell im Internet verwendbar.

Weitere Einschränkungen sind:

- ✓ Die IP-Adresse 0.0.0.0 ist für Geräte (Hosts) nicht verwendbar, da diese IP-Adresse die Adresse des gesamten Internets darstellt. Die Default-Route zeigt auf dieses Netz. Aus historischen Gründen sind alle IP-Adressen aus dem Bereich 0.0.0.0 bis 0.255.255.255 für Hosts nicht erlaubt.
- ✓ Die IP-Adresse 127.0.0.1 ist die Localhost-Adresse. Jedes Gerät, das mit IP-Adressen umgehen kann, erhält diese IP-Adresse automatisch als eigene Adresse. Auch alle anderen IP-Adressen aus dem Bereich 127.0.0.2 bis 127.255.255.255 gelten nur **intern** auf dem Gerät selbst. Lokale Netzwerkanwendungen benutzen diese IP-Adressen, um beispielsweise Dienste zu erreichen, die auf dem eigenen Gerät laufen.
- ✓ Die erste IP-Adresse in einem Netzwerk ist in Broadcastnetzen (Ethernet, WLAN) für das Netzwerk selbst reserviert. Kein Host darf sie erhalten.
- ✓ Die letzte IP-Adresse in einem Netzwerk ist für die Broadcast-Adresse des Netzwerkes reserviert. Kein Host darf sie erhalten.
- ✓ Die IP-Adresse 255.255.255.255 ist die generelle Broadcast-Adresse. Kein Host darf sie erhalten.
- ✓ Jede Host-Adresse innerhalb eines Netzwerkes darf nur einmalig vergeben sein.

Subnetze erstellen

Offizielle IPv4-Adressen sind rar. Genau aus diesem Grund unterteilen Provider oft die ihnen zur Verfügung stehenden Netzwerke, um ihren Kunden kleinere Netzwerkanteile zur Verfügung zu stellen. Bei Netzwerken mit privaten IP-Adressen steht die Erstellung von Subnetzen jedermann offen, da es hier viele IP-Adressen gibt.

Jedes Netzwerk, also auch ein Subnetz, wird durch eine eigene Netzmaske definiert. Die Anzahl der Segmente und die Anzahl der Hosts in jedem Segment sollten bekannt sein, bevor die Netzmaske für diese Netze definiert wird. Je mehr Subnetze entstehen, umso weniger Hosts haben darin Platz.

Bei der Unterteilung von Netzwerken muss eine entsprechende Einteilung in die verschiedenen Subnetze mit der passenden Anzahl an Hosts erfolgen:

- ✓ Legen Sie die IP-Adresse und die zugehörige Klasse für Ihr Netzwerk fest.
- ✓ Ermitteln Sie die Anzahl der Segmente sowie die Anzahl der erforderlichen Hosts pro Segment.
- ✓ Konvertieren Sie das entsprechende Oktett Ihrer IP-Adresse von der dezimalen Schreibweise in die binäre Darstellung.
- ✓ Zählen Sie die im Binärformat benötigten Bits für Ihre Subnet-ID.
- ✓ Die übrigen Bits Ihres Oktetts ergeben die Anzahl der Hosts und ihre spätere Host-IP-Adresse (Host-ID).
- ✓ Konvertieren Sie die entsprechenden Binärwerte in die dezimale Schreibweise.
- ✓ Ermitteln Sie abschließend die Subnetze und ihre zugehörigen IP-Adressbereiche.

Ein Adressierungsbeispiel

Sie möchten ein privates Klasse C Netzwerk in acht Teilnetze aufteilen. Jedes Teilnetz muss mindestens 20 Hostsysteme aufnehmen können. Da zur Bildung einer passenden Netzmase die entsprechenden Bits den logischen Wert „1“ aufweisen müssen, können Sie die entsprechende Netzmase nach folgendem Schema ermitteln:

Anzahl der Subnets:	8			
Benötigte Anzahl an Bits:	3 Bits (000 – 111, entspricht 8 Zuständen)			
Standard-Netzmase (dez.):	255.	255.	255.	0
Entsprechender Binärwert:	11111111.	11111111.	11111111.	000 00000
Plus zugehörige Subnet Bits:	111 00000			
Ergibt folgende Maske:	11111111.	11111111.	11111111.	111 00000
Neue Netzmase dezimal:	255.	255.	255.	224

Zusammenstellung der theoretisch möglichen Netzmasken für ein Netzwerk 192.168.1.0/24

Netzmase	CIDR-Notation	Anzahl der Subnets	Max. Anzahl der Hosts pro Subnet
255,255,255,128	/25	2	126
255.255.255.192	/26	4	62
255.255.255.224	/27	8	30
255.255.255.240	/28	16	14
255.255.255.248	/29	32	6
255.255.255.252	/30	64	2, für Point-to-Point-Verbindungen
255.255.255.254	/31	1	Ungültig in Broadcast-Netzen
255.255.255.255	/32		Definiert einen einzelnen Host

Ein Netzwerk lässt sich nicht nur in kleinere Teilnetze (Subnetting) unterteilen, sondern auch zu einem einzigen Netz mit vielen Hostsystemen vergrößern (Supernetting), indem man die Netzmase verkleinert.

So können Sie ein Netzwerk 192.168.0.0/23 definieren, das doppelt so groß ist wie ein herkömmliches Netzwerk der Klasse C und über den Adressbereich von 192.168.0.0 – 192.168.1.255 verfügt. Die erforderliche Netzmase ist dann 255.255.254.0, also eine mit insgesamt 23 binären Einsen. In diesem Netzwerk ist die IP-Adresse 192.168.1.0 für einen Host erlaubt, da es hier keine Netzwerkadresse ist. Laut CIDR ist auch dieses Netz ein Subnetz, da jedes Netz (außer dem Internet selbst) ein Subnetz des Internets darstellt.

Routing

Um Daten von einem Netzwerk zu einem anderen Netzwerk transportieren zu können, benötigen die involvierten Geräte Informationen darüber, welchen Weg sie nehmen sollen. Das Wort „Route“ gibt es auch im Deutschen, es bedeutet etwa „Wegbeschreibung“ oder „Strecke“.

Beispiel: Will ein Autofahrer von Berlin nach Zürich, Bahnhofstr. 21 fahren, gibt er die Adresse über sein Navigationsgerät ein. Dieses zeigt ihm dann die Entfernung zum Ziel mit Zeitangabe (aufgrund des im Navigationssystem vorhandenen Kartenmaterials) und den direkten Weg zum nächsten Punkt (Straße, Kreuzung, Kreisverkehr usw.) an.

Nicht ganz so verhält es sich mit Routern. Würden sie alle Netzwerke kennen, benötigten sie eine vollständige Netzwerkkarte des Internets. Dies erfordert viel Speicher- und Rechenkapazität und müsste bei Netzänderungen ständig aktualisiert werden. Ein Router kennt im Normalfall nur den Weg zum Zielnetzwerk über seinen nächsten Router (Hop). Deshalb wird Routing auch als Hop-by-Hop-Routing bezeichnet.

IP_Forward

Da etliche Softwarereprodukte am Markt sind, die versprechen, aus einem Rechner einen Router zu machen, und auch aktuelle Betriebssysteme oft dazu in der Lage sind, stellt sich die Frage, wann ein Gerät ein Router ist. Wenn Sie mehrere Netzwerkkarten einbauen, erhalten Sie damit noch keinen Router, auch wenn es Grundvoraussetzung ist, dass mindestens zwei Netzwerk-Karten vorhanden sein müssen.

Der Begriff „Netzwerk-Karte“ bedeutet hier, dass es nicht um Schnittstellen (Interfaces) geht, von denen eine Netzwerkkarte auch mehrere haben kann, die entweder unter mehreren IP-Adressen zugeordnet sind oder die als Verbund im Team arbeiten. Es muss bis auf wenige Ausnahmen eine eigenständige Hardware sein, die eine Netzwerkverbindung aufnehmen kann. Netzwerk-Devices können als Steckkarten vorkommen (im Format PCI, PCI-X, PCIe, Buscard etc.) oder auch auf dem Mainboard integriert sein.

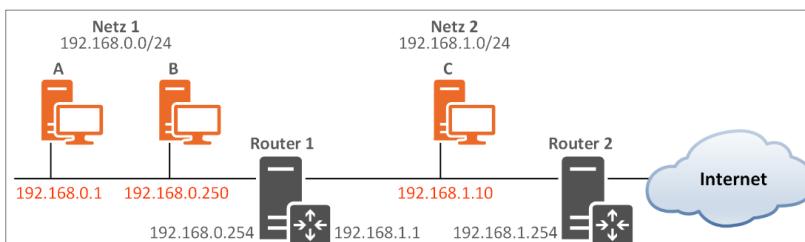
Wenn zwei oder mehr Netzwerkkarten in einem Rechner zusammen mit den passenden Treibern installiert sind, bedeutet dies nur, dass an mehreren Netzwerken Pakete an diesem Rechner ankommen können. Er leitet sie aber nicht weiter, solange eine Funktion nicht aktiv ist, die IP_Forward genannt wird. Auch andere Begriffe sind gebräuchlich, wie IP_Routing, IP-Weiterleitung oder Ähnliches. Diese Funktion wirkt wie ein Schalter, der eine Verbindung zwischen den Netzwerkkarten herstellt. Erst dann wird ein Gerät zum Router. Bei Hardware-Routern ist IP_Forward immer aktiv.

Beim Weiterleiten spielen aber auch weitere Funktionen eine Rolle, wie z. B. die eines IP-Filters. Ein Automatismus ist damit also nicht verbunden. Ein Hardware-Router sollte in den meisten Fällen den Vorzug erhalten, da er wesentlich zuverlässiger und nur auf diese Funktion ausgelegt ist. Rechner werden in der Regel nur dann als Router eingesetzt, wenn sie entweder Teil einer Firewall-Strategie sind („Bastion-Host“) oder zusätzliche Dienste wie Intrusion Detection System (IDS) oder Intrusion Prevention System (IPS) anbieten sollen.

Weitere Informationen finden Sie hier:

- ✓ https://de.wikipedia.org/wiki/Intrusion_Detection_System
- ✓ https://de.wikipedia.org/wiki/Intrusion_Prevention_System
- ✓ https://de.wikipedia.org/wiki/Bastion_Host

Die folgenden Beispiele sollen das Routing und die Bedeutung der Netzmaske (etwas vereinfacht) verdeutlichen. Angenommen, drei Rechner und zwei Router befinden sich in zwei Netzen:



Die Beispiel-Vernetzung

Fall 1: Rechner A will eine Verbindung zu Rechner B aufnehmen

Bei Ethernet ist eine Adressierung nur über die Hardware-Adresse (Ethernet- oder auch MAC-Adresse) möglich. Rechner A kennt diese noch nicht, nur die IP-Adresse von B. Um die Ethernet-Adresse zu ermitteln, benötigt er die Hilfe des Address-Resolution-Protokolls (**ARP**). Über ARP initiiert er einen Ethernet-Broadcast, auf den sich der Rechner mit der gewünschten IP-Adresse meldet und seine Ethernet-Adresse bekannt gibt. A kann nun einen Ethernet-Frame erstellen, ein IP-Paket darin einpacken und alles zusammen an B verschicken. B sendet ihm danach auf die gleiche Weise eine Antwort.

Fall 2: Rechner A will eine Verbindung zu Rechner C aufnehmen

Auch hier muss Rechner A eine Ethernet-Adresse ermitteln, bevor er einen Ethernet-Frame verschicken kann. Über ARP kann er aber die Ethernet-Adresse von C nicht herausfinden, da ein Router keine Ethernet-Broadcasts weiterleitet. Deshalb prüft er zunächst, ob sich C im selben Netz befindet. Hierzu benutzt er die **eigene** Netzmase, die er vom Administrator oder einem DHCP-Server erhalten hat, und ermittelt daraus (wie weiter oben beschrieben) die Netzwerk-ID der IP-Adresse des Zielrechners. Unterscheidet sich diese von der seiner eigenen Netzwerk-ID, weiß er, dass sich Rechner C nicht im selben Netzwerk befindet. Im Grunde ist dies auch der erste Schritt im Fall 1.

Sobald Rechner A weiß, dass sein Ziel außerhalb des eigenen Netzwerkes liegt, muss er per ARP die Ethernet-Adresse des Routers ermitteln, der als Default-Route bzw. als spezifische Route in seiner Netzwerkkonfiguration eingetragen ist. Er verschickt deshalb das IP-Paket verpackt in einem Ethernet-Frame an Router 1. Dieser schickt es, mit wenigen Änderungen im IP-Header (der TTL-Wert wird um 1 reduziert), in einem neuen Ethernet-Frame an Rechner C weiter, dessen Ethernet-Adresse er vorher per ARP ermittelt hat. Genauso schickt Rechner C seine Antwort an A zurück.

Fall 3: Angenommen, auf Rechner A hat der Administrator eine falsche Netzmase eingetragen. Sie lautet nun 255.255.255.192 (/25) und nicht mehr 255.255.255.0 (/24)

Wenn Rechner A mit dieser Netzmase ein Paket an B mit der IP-Adresse 192.168.0.250 versenden will, ist für ihn dieser Rechner nicht mehr im selben Netzwerk. Folglich verschickt er das Paket über seine Default-Route an Router 1. Dieser bügelt den Fehler aus, sofern er eine IP-Adresse im Bereich 192.168.0.1 bis 192.168.0.126 besitzt, und schickt das Paket an B. Dies erhöht den Verkehr auf der Leitung zum Router 1.

Fall 4: Angenommen, auf Rechner A hat der Administrator die falsche Netzmase 255.255.254.0 (/23) eingetragen

A will ein Paket an Rechner C verschicken. Dieser Fehler hat größere Folgen. Denn A nimmt an, dass sich C im selben Netzwerk befindet. Also versucht er, das Paket direkt zu versenden, ohne Router 1. Die Ermittlung der Ethernet-Adresse von C per ARP schlägt aus oben genannten Gründen fehl, sodass C auf diese Art nicht erreichbar ist.

Fall 5: Rechner A will mit einem Rechner im Internet Verbindung aufnehmen.

Rechner A versucht einen Ping auf die Internet IP-Adresse 195.125.204.193. A erkennt, dass sich diese IP-Adresse nicht in seinem eigenen Netzwerk befindet und schickt die Anforderung an Router 1. Router 1 kennt das Netz dieser IP-Adresse ebenfalls nicht und verschickt das IP-Paket über seine Default-Route an Router 2. Auch dieser versendet es weiter über seine Default-Route an einen Router des Providers, bis das IP-Paket an seinem Ziel ankommt.

Der Rechner 195.125.204.193 erstellt nun eine Antwort an die Adresse, die in dem Header des IP-Pakets als Absender eingetragen ist. Diese lautet 192.168.0.10 und ist damit eine private IP-Adresse. Der Rechner 195.125.204.193 schickt das Antwort-Paket an den Router, der in seiner Default-Route eingetragen ist. Dieser erkennt (durch eine Regel, die das Weiterleiten bestimmter Netze sperrt), dass es sich beim Zielnetz um ein privates Netz handelt, und leitet das Paket nicht weiter.

Die Antwort kommt nie bei A an, da private IP-Adressen nicht eindeutig lokalisierbar sind. Sie können viele Tausend Mal vorkommen! Erst wenn in Router 2 eine Adressumsetzung (Network Address Translation - NAT) eingerichtet ist, kann er in allen IP-Paketen zum Internet seine eigene offizielle IP-Adresse eintragen, die er per DHCP vom Provider erhalten hat. Erst dann können die Router im Internet das Antwort-Paket an Router 1 leiten.

Damit ein IP-Paket nicht auf ewige Zeiten im Internet kreist, gibt es im Header von IP-Paketen ein 8 Bit großes Flag mit Namen TTL (Time To Live). Jeder Router verringert den Wert der Zahl in diesem Flag, sobald er das IP-Paket annimmt. Ist der Wert danach größer als 0, bearbeitet er es weiter, ansonsten verwirft er es. Damit kann ein IP-Paket maximal 255 Router passieren, wenn der Anfangswert auf den Maximalwert 255 gesetzt ist. Die meisten Betriebssysteme verwenden kleinere Werte. Welche dies auf dem Zielgerät sind, kann das Programm Ping anzeigen.

Zur Prüfung einer Verbindung zwischen zwei Geräten eignet sich das Programm Ping. Mit dem Testprogramm Traceroute können Sie unter UNIX und Linux die Route verfolgen, welche die IP-Pakete auf dem Weg zu ihrem Ziel passieren. Unter Windows heißt dieses Programm Tracert.

```
C:\>tracert www.herdt.com

Routenverfolgung zu www.herdt.com [195.243.78.74]
über maximal 30 Hops:

 1      1 ms      1 ms      1 ms  fritz.box [192.168.178.1]
 2     76 ms     22 ms     23 ms  rds1-brln-de80.nw.mediaways.net [62.52.195.4]
 3     23 ms     22 ms     22 ms  bundle-ether21.0001.dbrx.01.ber.de.net.telefonica.de [62.53.20.202]
 4     22 ms     22 ms     26 ms  ae1-0.0002.prrx.01.ber.de.net.telefonica.de [62.53.16.43]
 5     21 ms     22 ms     22 ms  194.25.208.213
 6     36 ms     36 ms     78 ms  mz-eb1-i.MZ.DE.NET.DTAG.DE [62.154.40.142]
 7     34 ms     34 ms     35 ms  mz-eb1-i.MZ.DE.NET.DTAG.DE [62.154.40.142]
 8     35 ms     32 ms     34 ms  0160566-1-1-gw.MZ.DE.NET.DTAG.DE [80.148.180.224]
 9     34 ms     32 ms     32 ms  195.243.78.74

Ablaufverfolgung beendet.

C:\>
```

Eine Ausgabe von tracert unter Windows

In der Abbildung sehen Sie, dass auf der Route zum Rechner mit Namen www.herdt.com insgesamt 8 Router beteiligt waren. Sollte in einer Zeile eine Zeitüberschreitung vorkommen, besagt dies nur, dass sich der entsprechende Router nicht selbst meldet, er also Echo-Requests (Ping) nicht beantwortet. (siehe nachfolgenden Ausschnitt 7 + 8)

5	15 ms	16 ms	16 ms	microsoft2.bcix.de [193.178.185.104]
6	17 ms	16 ms	16 ms	ae22-0.icr02.ber20.ntwk.msn.net [104.44.233.81]
7	*	*	*	Zeitberschreitung der Anforderung.
8	*	*	*	Zeitberschreitung der Anforderung.
9	30 ms	31 ms	30 ms	be-4-0.ibr06.ams06.ntwk.msn.net [104.44.16.131]
10	31 ms	30 ms	30 ms	be-6-0.ibr02.ams21.ntwk.msn.net [104.44.18.190]

9.8 Routing-Befehle und Routing-Tabelle

Routing-Tabellen

IP-Adressen werden in einem Netzwerk anhand der Netzmaske in einen Netzwerkanteil (Netzwerk-ID) und in einen Hostanteil (Host-ID) aufgeteilt. Der Netzwerkabschnitt einer IP-Adresse ist bei Routern maßgebend für die Weiterleitung der Pakete. Welcher Teil der Adresse dem Netzwerkabschnitt zugeordnet wird, ist von der verwendeten IP-Adresse und der zugehörigen Netzmaske abhängig. Zur Weiterleitung der Pakete ist es nicht notwendig, dass Router die vollständige Adresse speichern. Vielmehr ist es ausreichend, wenn sich ein Router die Netzwerksegmente (Netzwerkabschnitte) merkt, an welche er die entsprechenden Pakete weiterleitet. Diese Netzwerksegmente werden in einer Tabelle des Routers (Routing-Tabelle) gespeichert. Sie beinhalten für den jeweiligen Router die Informationen, über welche Adresse bzw. über welches Interface ein Datenpaket in das Zielnetzwerk weiterzuleiten ist.

Die Informationen, die diese Routing-Tabellen enthalten, können statisch eingetragen oder auch dynamisch erlernt werden. Dynamische Routinginformationen werden mittels entsprechender Protokolle wie beispielsweise RIP (Routing Information Protocol) oder OSPF (Open Shortest Path First) ermittelt. Statische Einträge in Routing-Tabellen werden manuell bei der Konfiguration von Routern festgelegt. Statische Routen haben immer Vorrang vor dynamisch erlernten Routen.

Statisches Routing

Statisches Routing basiert auf einer manuellen Vorgabe des Weges zum nächsten Router. Diese Vorgaben werden beim Einrichten eines Netzwerkes getroffen und als fester Eintrag dort hinterlegt. Die Netzwerke sind jeweils einem Router zugeordnet, über den sie zu erreichen sind. Unbekannte Ziele werden über die Default Route weitergeleitet. Bei statischen Routing-Tabellen muss die genaue Konfiguration des Netzes bekannt sein.

Hierzu gehören beispielsweise die Anzahl und Lage der Router, die verwendeten Verbindungswege und deren Übertragungskapazität. Nachteil von statischen Routing-Tabellen ist, dass bei jeder vorgenommenen Änderung, wie beispielsweise neuen Übertragungswegen oder einer geänderten Infrastruktur, der Eintrag in der Tabelle manuell konfiguriert werden muss.

Dynamisches Routing

Bei einem dynamischen Routing lernt der Router die Netze von seinen Nachbarroutern und trägt diese in seine Routing-Tabelle ein. Gleichzeitig gibt er seine eigenen direkt angeschlossenen Netze an die Nachbarrouter weiter. Ein wesentlicher Vorteil bei dynamisch erstellten Routing-Tabellen ist die Möglichkeit, bei Ausfall einer Route automatisch eine Alternativroute zu nutzen. Dies bedingt jedoch redundante physikalische Wege zu den Nachbarnetzen. Ein dynamisches Verfahren wie das unter TCP/IP oft eingesetzte Routing-Protokoll OSPF zeichnet sich durch seine Flexibilität aus. Um diese zu erreichen, müssen die beteiligten Router ständig Informationen über die aktuell verfügbaren Routen und deren Wichtung austauschen. Anhand dieser Routinginformationen wählt das Protokoll dann die beste Route zum Zielnetz aus.

Abfragen von Routing-Tabellen

Die Einträge in Routing-Tabellen können mittels einfacher Befehle analysiert werden. Die Verwendung von Befehlen für die Ausgabe der Routing-Tabelle ist herstellerabhängig und kann in seiner Schreibweise durchaus etwas variieren.

Befehl	Konsole
route print / netstat -nr	Eingabekommando unter Windows
show ip route	Cisco Router / Juniper Router u. a.
ip route bzw. route	Linux/Unix

Als Übungsbeispiel öffnen Sie unter Microsoft Windows ein Eingabefenster für den Befehlsinterpret (cmd.exe) und geben den Befehl **route print** oder **netstat -nr** ein. Sie erhalten dann eine Auflistung der aktuell gültigen Routen ①.

```

C:\>route print
=====
Schnittstellenliste
13...00 ad 9a fa 23 dc ....VPN Client Adapter - VPN
25...74 e6 e2 1b c7 a5 ....Realtek PCIe GBE Family Controller
21...82 19 34 83 a1 94 ....Microsoft Hosted Network Virtual Adapter
5...80 19 34 83 a1 95 ....Microsoft Wi-Fi Direct Virtual Adapter
9....00 50 56 c0 00 08 ....Vmware Virtual Ethernet Adapter for Vmnet8
3....00 50 56 c0 00 01 ....Vmware Virtual Ethernet Adapter for Vmnet1
24....00 ff a4 8d 9f e9 ....Kaspersky Security Data Escort Adapter
10....80 19 34 83 a1 94 ....Intel(R) Wireless-N 7260
1.....Software Loopback Interface 1
32....00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
23....00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #4
37....00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #9

=====
IPv4-Routentabelle
=====
Aktive Routen:
  Netzwerkziel  Netzwerkmaske      Gateway      Schnittstelle Metrik ①
          0.0.0.0      0.0.0.0  192.168.178.1  192.168.178.163    50
        127.0.0.0      255.0.0.0  Auf Verbindung  127.0.0.1       331
        127.0.0.1  255.255.255.255  Auf Verbindung  127.0.0.1       331
  127.255.255.255  255.255.255.255  Auf Verbindung  127.0.0.1       331
  192.168.30.0  255.255.255.0  Auf Verbindung  192.168.30.1       291
  192.168.30.1  255.255.255.255  Auf Verbindung  192.168.30.1       291
  192.168.30.255  255.255.255.255  Auf Verbindung  192.168.30.1       291
  192.168.31.0  255.255.255.0  Auf Verbindung  192.168.31.1       291
  192.168.31.1  255.255.255.255  Auf Verbindung  192.168.31.1       291
  192.168.31.255  255.255.255.255  Auf Verbindung  192.168.31.1       291
  192.168.31.0  255.255.255.0  Auf Verbindung  192.168.178.163     306
  192.168.178.163  255.255.255.255  Auf Verbindung  192.168.178.163     306
  192.168.178.255  255.255.255.255  Auf Verbindung  192.168.178.163     306
        224.0.0.0  240.0.0.0  Auf Verbindung  127.0.0.1       331
        224.0.0.0  240.0.0.0  Auf Verbindung  192.168.178.163     306
        224.0.0.0  240.0.0.0  Auf Verbindung  192.168.31.1       291
        224.0.0.0  240.0.0.0  Auf Verbindung  192.168.30.1       291
  255.255.255.255  255.255.255.255  Auf Verbindung  127.0.0.1       331
  255.255.255.255  255.255.255.255  Auf Verbindung  192.168.178.163     306
  255.255.255.255  255.255.255.255  Auf Verbindung  192.168.31.1       291
  255.255.255.255  255.255.255.255  Auf Verbindung  192.168.30.1       291

=====
Ständige Routen:
  Keine
  
```

Eingabeaufforderung mit dem Befehl `route print`

Hinzufügen einer statischen Route

Einträge in statischen Routing-Tabellen müssen Sie manuell eintragen. Dies erfolgt mit entsprechenden Befehlen unter Angabe des Zielnetzes und der dazugehörigen Netzmaske. Mit dem Befehl **route add** können Sie beispielsweise auf Ihrem lokalen Rechner einen zusätzlichen Eintrag in die statische Routing-Tabelle vornehmen.

Befehl	Konsole
route add <Zielnetz> mask <Netmask> <gateway>	Eingabekommando unter Windows
ip route <Zielnetz> <Netmask> <Gateway>	Cisco Router / Juniper Router

9.9 IP-Hardware-Router einrichten

Vorbereitungen für die Konfiguration

Beispielhaft soll hierfür die Hardware eines LINKSYS-WRT54GL-Routers des Herstellers Cisco herangezogen werden. Als Betriebssystem auf dem Router kommt die Firmware DD-WRT zum Einsatz. Bei DD-WRT handelt es sich um eine quelloffene Linux-Distribution für WLAN-Router und Access-Points. Der in der Distribution integrierte Web-Server ermöglicht es Ihnen, die Konfiguration über Ihren Browser durchzuführen.

Der LINKSYS-Router kommt vorwiegend in kleinen und mittleren Firmen sowie im Heimbereich zum Einsatz. Er stellt einerseits eine WAN-Verbindung zum Provider (ISP) und andererseits LAN- und WLAN-Verbindungen für das lokale Netz zur Verfügung.

Router in Betrieb nehmen

- ▶ Lesen Sie sich zuerst die Dokumentation des Routers durch. Verbinden Sie anschließend den Router über die Ethernet-Schnittstelle mit Ihrem PC. Die Netzwerkkarte Ihres PCs oder Laptops sollte auf *IP-Adresse automatisch beziehen* eingestellt sein oder eine statische IP-Adresse im Bereich 192.168.1.2 - 254 mit der Maske 255.255.255.0 aufweisen.
- ▶ Öffnen Sie Ihren Web-Browser und geben Sie die IP-Adresse 192.168.1.1 im URL-Feld ein.

Konnte keine Verbindung aufgebaut werden, dann überprüfen Sie Folgendes:

- ✓ Wird ein Link am Router auf der Vorderseite bei „Ethernet“ angezeigt? Ist dies nicht der Fall, so ist dies ein Kabelproblem bzw. das Patchkabel steckt nicht am richtigen Port.
- ✓ Stimmt die IP-Adresse Ihrer Netzwerkkarte mit den o. g. Angaben überein?
- ✓ Erreichen Sie den Router (192.168.1.1) mit dem Ping-Befehl? Ist dies nicht der Fall, so ist der Router nicht im Grundzustand (Default-Zustand). Setzen Sie ihn durch Betätigen der Reset-Taste am Gerät zurück.

Router konfigurieren

Nachdem Sie über Ihren Browser den Zugriff auf den Router erlangt haben, werden Sie als Erstes aufgefordert, einen Nutzernamen ① und das Kennwort ② für den sicheren Zugriff auf das Gerät zu vergeben und mit *Change Password* zu bestätigen.

The screenshot shows a web-based configuration interface for a router. At the top, there is a navigation bar with tabs: Setup, Wireless, Services, Security, Access Restrictions, NAT / QoS, Administration, and Status. The 'Setup' tab is currently selected. Below the navigation bar, the title 'Router Management' is displayed. A message box contains the text: 'Your Router is currently not protected and uses an unsafe default username and password combination, please change it using the following dialog!'. Below this message box, there is a section titled 'Router Password' with three input fields: 'Router Username' (containing a redacted string), 'Router Password' (containing a redacted string), and 'Re-enter to confirm' (containing a redacted string). At the bottom of the form is a button labeled 'Change Password'.

Passwortvergabe

Danach können Sie über die Registerkarten folgende Einstellungen vornehmen:

- ✓ *Setup*: Grundeinstellungen für den Router
- ✓ *Wireless*: Einstellungen WLAN-Mode, SSID, Filter, Security
- ✓ *Services*: Einstellungen für das Service Management
- ✓ *Access Restrictions*: Zugriffseinschränkungen ins Internet (zeitlich, Protokoll, URL, Schlüsselwörter)
- ✓ *NAT / QoS*: Konfiguration der NAT und der Dienstgüte im WAN
- ✓ *Administration*: Parameter für das Router Management (u. a. Passwörter, Web Access und Remote Access)
- ✓ *Status*: Anzeige der aktuellen Konfiguration und des Systemzustandes

Für die Grundkonfiguration benötigen Sie die Menüpunkte *Setup* und *Wireless*.

WAN Setup		Help
WAN Connection Type		Automatic Configuration - DHCP: This setting is most commonly used by Cable operators.
Connection Type	PPPoE	Host Name: Enter the host name provided by your ISP.
User Name	User01020304	Domain Name: Enter the domain name provided by your ISP.
Password	*****	Local IP Address: This is the address of the router.
Service Name		Subnet Mask: This is the subnet mask of the router.
PPP Compression	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	DHCP Server: Allows the router to manage your IP addresses.
T-Home VDSL 7 Vlan Tagging	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Start IP Address: The address you would like to start with.
MPPE Encryption		
Force reconnect	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
STP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Router Name	DD-WRT	(3)
Host Name		
Domain Name		
MTU	Manual <input type="button" value="▼"/> 1492	(4)

Setup-Einstellungen WAN

Bei den Einstellungen *Setup*, *Basic Setup* müssen Sie die von Ihrem Provider (ISP) vorgegebenen Parameter wie Internetverbindungstyp ①, die Zugangsdaten ② und den Namen des Routers ③ einstellen. Bei einer PPPoE-Verbindung (Point to Point over Ethernet) sollten Sie zur Optimierung des Traffics die MTU ④ auf 1492 einstellen.

Auf dieser Registerkarte müssen Sie jetzt nur noch die Einstellungen für die LAN-Seite vornehmen. Das sind ggf. die Änderung der IP-Adresse des Routers ① und die Konfiguration des DHCP-Servers ②, damit die angeschlossenen Clients ihre IP-Adresse automatisch beziehen können. Sie legen beim DHCP-Server die Startadresse des Adressenpools ③, die Anzahl der zur Verfügung gestellten Adressen ④ und deren Gültigkeit fest. Optional können Sie noch die aktuelle Zeit ⑤ über einen Zeitserver (NTP) beziehen und danach alle Konfigurationsparameter über die Schaltfläche *Save* sichern.

Network Setup

Router IP

Local IP Address	192	168	1	100
Subnet Mask	255	255	255	0
Gateway	192	168	1	1
Local DNS	192	168	1	1

Maximum DHCP Users:
You may limit the number of addresses your router hands out. 0 means only predefined static leases will be handed out.

Time Settings:
Choose the time zone you are in and Summer Time (DST) period. The router can use local time or UTC time.

Network Address Server Settings (DHCP)

DHCP Type	DHCP Server
DHCP Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Start IP Address	192.168.1.101
Maximum DHCP Users	50
Client Lease Time	8400 minutes
Static DNS 1	201.223.44.14
Static DNS 2	201.43.79.222
Static DNS 3	0.0.0.0
WINS	0.0.0.0
Use DNSMasq for DHCP	<input checked="" type="checkbox"/>
Use DNSMasq for DNS	<input checked="" type="checkbox"/>
DHCP-Authoritative	<input checked="" type="checkbox"/>

Time Settings

NTP Client	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Time Zone	UTC+01:00
Summer Time (DST)	last Sun Mar - last Sun Oct
Server IP/Name	188.3.56.23

Buttons: Save, Apply Settings, Cancel Changes

Setup-Einstellungen LAN

Die Einstellungen für die WLAN-Schnittstelle werden über die Registerkarte **Wireless** eingerichtet. Die Basis-einstellung finden Sie detailliert im Abschnitt 9.3 unter dem Punkt *WLAN konfigurieren*.

Daneben muss noch die Sicherheit des WLANs gewährleistet werden. Dazu können Sie unter **Wireless, Wireless SECURITY** den höchsten Sicherheitsmodus ①, den Verschlüsselungsalgorithmus ② und einen sicheren Schlüssel ③ festlegen. Die gleichen Einstellungen müssen Sie dann auch auf den WLAN-Karten der angeschlossenen PCs übernehmen.

Wireless Security wlo

Physical Interface wlo SSID [dd-wrt] HWAddr [68:F7:43:36:DA:B9]

Security Mode	① WPA2 Personal
WPA Algorithms	② TKIP+AES
WPA Shared Key	③ <input type="password"/> Unmask
Key Renewal Interval (in seconds)	3600

Help more...

Security Mode:
You may choose from Disable, WEP, WPA Personal, WPA Enterprise, or RADIUS. All devices on your network must use the same security mode.

Buttons: Save, Apply Settings

Verschlüsselung WLAN

Weitere Konfigurationsparameter, wie z. B. die Einstellungen der internen Firewall oder das Zusammenschalten mehrerer Access-Points zu einem WLAN-Verbund, sind umfänglich in den Dokumentationen der Webseite www.dd-wrt.com/wiki hinterlegt.

9.10 IPv6

Bei den Zuwachsralten an Internetknoten war absehbar, dass ab dem Jahre 2012 keine neuen IPv4-Adressen mehr zur Verfügung stehen. Bereits Anfang der 90er-Jahre initiierte das IETF ein Projekt zu dieser Entwicklung und forderte im Dezember 1993 mit RFC 1550 und unter dem Kürzel IPng (IP next Generation) alle Beteiligten auf, Vorschläge für die Umstrukturierung der Adressen und notwendige Änderungen am neuen Internet-Protokoll zu machen. Im Dezember 1995 folgte mit RFC 1883 (dieses Mal unter dem Kürzel IPv6) die Veröffentlichung eines Diskussionspapiers, das seither noch mehrfach überarbeitet wurde. Die auffälligste Änderung betrifft die Erweiterung der Adressgröße von 32 auf 128 Bit, sodass sich die Anzahl der adressierbaren Hosts drastisch erhöht. Alle relevanten Standards zu diesem Protokoll sind bereits seit längerer Zeit in Kraft.

IPv6 ist **nicht kompatibel** mit der älteren Version IPv4 auf der gleichen Schicht (OSI Layer 3), aber **vollständig konform** zur darüber liegenden Transportschicht (OSI Layer 4). Alle relevanten Provider in Deutschland haben intern vollständig auf das IPv6-Protokoll umgestellt und es ist im praktischen Einsatz. Endnutzer können seit Anfang 2012 dieses Protokoll (sofern es zum Endkunden freigegeben ist) über ihre Provider nutzen.

Vorteile von IPv6

Die Vorteile von IPv4, wie z. B. die Stabilität des Protokolls und die Skalierbarkeit der Adressbereiche, wurden übernommen, optimiert und neue Funktionen hinzugefügt. Dazu zählen:

- ✓ Der Adressraum wurde stark erweitert (10^{12} Hosts und 10^9 Netzwerke), also ca. 340,28 Sextillionen Adressen, von denen erst sehr wenige vergeben sind.
- ✓ Jede Protokollfunktion nutzt ein eigenes Headerformat – damit können neue Protokolle ohne Änderung bestehender Funktionalität integriert werden.
- ✓ Das Routing zwischen IPv6-Netzen ist schneller, weil die Anzahl der Routen in das Zielnetz reduziert wurde und das Umsetzen der MTU (Maximum Transmission Unit) entfällt.
- ✓ Das Netzwerkmanagement wurde durch das Protokoll ICMPv6 verbessert.
- ✓ IPv4-basierende und IPv6-basierende Anwendungen (Dual Stack) sind gleichzeitig nutzbar – damit ist eine einfache Migration nach IPv6 möglich.
- ✓ Eine lokale IPv6-Adresse (local link address) wird automatisch bereitgestellt.
- ✓ Ein IPv6-Adressen-Präfix kann durch einen Router (stateless address autoconfiguration) bzw. eine IPv6-Adresse über DHCPv6 automatisch bereitgestellt werden.
- ✓ Die Multicastadressierung wurde umfassend erweitert.
- ✓ Die Möglichkeiten zur Überprüfung der Authentizität und Verschlüsselung (IPsec) sind integraler Bestandteil des Protokollstacks.
- ✓ Die Dienstgüte (Quality of Service) wurde über eine neue Label-Definition optimiert.
- ✓ Die Erreichbarkeit unter derselben Adresse (Mobile IPv6) in wechselnden Netzwerken wurde entscheidend verbessert.
- ✓ Die Nutzung von Jumbopaketen bis zu 4 GByte Größe ist möglich.

IPv6-Adresstypen

IPv4 verwendet vier Adresstypen:

- ✓ Netzwerkadresse – kennzeichnet das verwendete Netzwerk
- ✓ Unicast-Adresse – beschreibt die Datensendung zu einem Host innerhalb eines Netzwerks

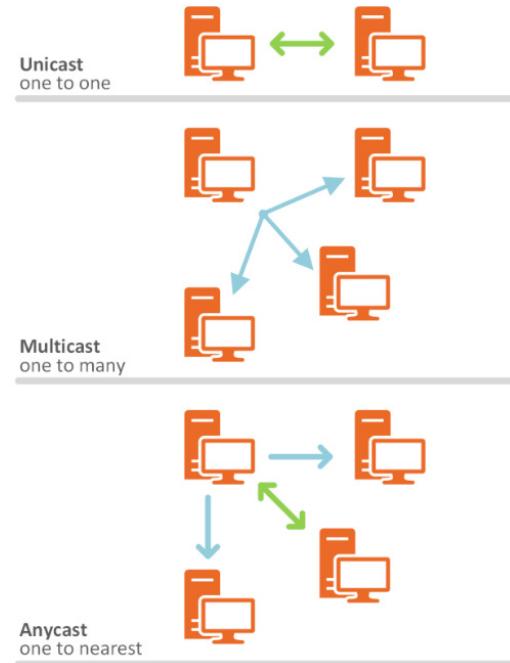
- ✓ Multicast-Adresse – adressiert eine Gruppe von Hosts innerhalb des Netzwerks
- ✓ Broadcast-Adresse – richtet sich an alle Hosts innerhalb des Netzwerks

Unter IPv6 existieren nur noch drei Adressarten. Die Adressarten Unicast und Multicast wurden in ihrer Funktionalität von IPv4 nach IPv6 übernommen. Die Multicast-Adresse unterscheidet sich etwas. Bei IPv4 adressiert sie eine Punkt-zu-Mehrpunkt-Verbindung (Point-to-Multipoint) im Intranet bzw. im Internet. Bei IPv6 werden diese Adressen im Node, am Link, im Intranet, administrativ und global genutzt.

Ein an eine Multicast-Adresse gesendetes Paket wird von allen Mitgliedern dieser Multicast-Gruppe verarbeitet. Ein Client nutzt z. B. die Multicast-Adresse, um seinen Router oder DHCPv6-Server zu finden. Das erste Byte einer Multicast-Adresse ist immer FF.

Eine Anycast-Adresse adressiert (genauso wie bei Multicast) eine Gruppe von Systemen in einem Netzwerk. Anycast findet vorwiegend bei Routern Anwendung. Bei einer Anfrage über diese Adresse antworten hingegen nicht alle im Netz vorhandenen Router, sondern nur derjenige, der am besten erreichbar ist.

Broadcast-Adressen werden bei IPv6 nicht mehr verwendet.



Adressarten IPv6

Adressenaufbau von IPv6

IPv6-Adressen werden nicht in dezimaler Schreibweise notiert wie IPv4-Adressen, sondern mit Hexadezimalzahlen. Dabei wird eine komplette Adresse von **128 Bit Länge** in acht Blöcke mit jeweils 16 Bits aufgeteilt. Die Trennung der Blöcke erfolgt nicht über einen Punkt, sondern über einen Doppelpunkt. Sofern sich in einem Block bzw. in mehreren aufeinander folgenden Blöcken nur Nullen befinden, kann die Darstellung **einmalig** durch die Zeichen „::“ vereinfacht werden. Bei der Angabe einer Portnummer bzw. HTTP-Adresse wird die gesamte IPv6-Adresse in eckige Klammern gesetzt und die Portnummer, wie bei IPv4 durch Doppelpunkt getrennt, angehängt.

Beispiele: [2001:ab13:4412:0000:ca11:4545:0000:1234]:80
[http://\[2001:2498:7654::654:3210\]:8080/](http://[2001:2498:7654::654:3210]:8080/)

Standardgemäß bilden die ersten 64 Bit die Netzwerk-ID (das Präfix) und die zweiten 64 Bit die Host-ID (das Suffix). Sollen diese Angaben variiert werden, ähnlich den Masken bei IPv4, dann wird die entsprechende Anzahl der Bits, die die Netzwerk-ID bilden, als Zahl hinter einem Schrägstrich ans Ende der IPv6-Adresse angefügt. Das folgende Beispiel stellt einen Präfix von 48 Bits dar bzw. die ersten 6 Bytes beschreiben die Netzwerk-ID.

Beispiel: 2001:ab13:4412:0000:ca11:4545:0000:1234 /48

Eine besondere Rolle spielen die ersten Bytes einer IPv6-Adresse, da diese fest definiert sind, so z. B. die hexadezimalen Angaben der ersten zwei Bytes **2001**, **2003** und **2A00** als Unicast-Adressvorgabe für europäische Provider oder **FE80** als Local Link Unicast. Die Local-Link-Adresse wird vom IPv6-Stack automatisch generiert und ermöglicht jedem System die Kommunikation im lokalen Netzwerk.

Beispiel: fe80:0000:0000:0000:4567:65ff:fedc:4717/64 oder bei Zusammenfassung der Null-Blöcke
 fe80::4567:65ff:fedc:4717/64

Die Local-Host-Adresse, die bei IPv4 als 127.0.0.1 dargestellt wurde, hat nun die Adresse 0000:0000:0000:0000:0000:0001 oder einfacher geschrieben ::1.

Für Internetverbindungen benötigt ein Client (Rechner) eine zusätzliche, offizielle Adresse (global unicast), die er normalerweise durch Anfrage an seinen Router generiert oder die von DHCPv6 bereitgestellt wird. Die Adresse des Routers muss er dabei nicht kennen, da er alle Anfragen per IPv6-Multicast verschickt. Der IPv6-Router sendet daraufhin das Präfix des öffentlichen Adressblocks, die Lease Timeout (Gültigkeitszeitraum des Präfixes), die MTU (die maximale Framegröße) und den Hop Count (ist identisch mit dem TTL bei IPv4).

Für globale Unicast-Adressen wurde von der IANA der Adressbereich von 2000 bis 3FFF freigegeben.

Beispiel: 2001:2211:7AAF:9AFE:4567:65ff:fedc:4717/64

9.11 IPv6-Routing

Für die aktuellen PC-Betriebssysteme besteht **kein Unterschied**, ob sie über IPv4 oder IPv6 routen. Dazu besitzen sie einen Dual Stack (RFC 4213), der beide Protokolle beherrscht. Die Applikation auf dem Rechner entscheidet, über welchen Stack das Paket in das Zielnetz befördert wird. Befindet sich die Zieladresse nicht im eigenen Netz, benötigt der Rechner für die Weiterleitung in ein anderes Netz den Router. Beim IPv6-Protokoll wird einem Endsystem automatisch die verfügbare Routeradresse für sein Interface zugewiesen, d. h., er erhält eine Standardroute (Default-Route) zum nächsten Router (Hop) seines Netzwerkes.

Alle Hersteller von Routern und Multilayer-Switchen haben die IPv6-Funktionalität in ihrer Firmware vollständig implementiert – mit Ausnahme einiger kleinerer SoHo-Router. Im Gegensatz zu den PC-Betriebssystemen ist der IPv6-Stack bei diesen Geräten mitunter ausgeschaltet und muss erst aktiviert werden. Dies geschieht über entsprechende Konfigurationsbefehle, die sich bei jedem Hersteller etwas unterscheiden.

Statisches Routen

Statisches Routen wird genutzt, wenn Sie eine feste Wegwahl in das Zielnetz vorgeben. Sie wird manuell in der Routing-Tabelle hinterlegt. Dabei gibt es, wie auch bei IPv4, zwei Varianten:

- ✓ Die Default-Route – über diese werden alle Pakete versandt, für die es keinen Eintrag in der Routing-Tabelle gibt.
- ✓ Die spezifische Route – hierüber werden nur Pakete versandt, für die ein Eintrag für das Zielnetz in der Routing-Tabelle existiert.

Da ein Endsystem sehr einfach durch das Neighbor-Discovery-Protocol seine Default-Route und auch seinen Adressen-Präfix für das Routen bekommt, konzentrieren wir uns im Weiteren auf die Routerkonfiguration. Dies soll beispielhaft auf dem CLI (command line interface) eines Cisco-Routers erläutert werden.

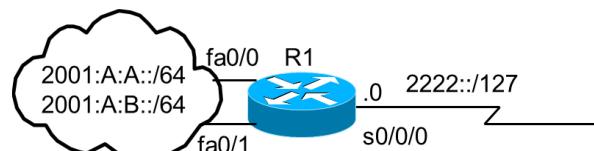
Dazu müssen Sie folgende Schritte durchführen:

- ▶ IPv6-Stack freischalten
- ▶ IPv6-Adressen auf den Netzwerkkarten einstellen und diese aktivieren
- ▶ spezifische oder Default-Route setzen

Der Router verfügt exemplarisch über drei Netzwerk-karten, zwei Fast-Ethernet-Interfaces (Name: fa0/0 und fa0/1) und ein serielles Interface (Name: s0/0/0). Die Host-ID soll auf der Fast-Ethernet 0/0 und 0/1 jeweils 1 und auf der seriellen Interface 0 betragen.

Das Aktivieren des IPv6-Stacks erfolgt mit dem Befehl:

R1(config)# *ipv6 unicast-routing*

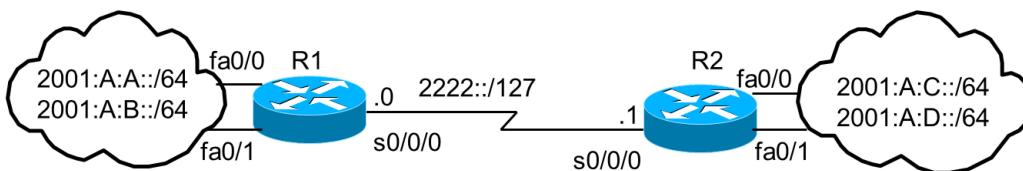


Setzen der Interface-Adressen und des Präfix:

```
R1(config)# interface fa0/0
R1(config-if)# ipv6 address 2001:A:A::1/64
R1(config-if)# no shutdown → Netzwerkkarte aktivieren
R1(config-if)# interface fa0/1
R1(config-if)# ipv6 address 2001:A:B::1/64
R1(config-if)# no shutdown → Netzwerkkarte aktivieren
R1(config-if)# interface s0/0/0
R1(config-if)# ipv6 address 2222::0/127 oder 2222::/127
R1(config-if)# no shutdown → Netzwerkkarte aktivieren
```

Durch das Konfigurieren der Adressen und die Aktivierung der Netzwerkkarte auf dem Router können nun Multicast-Anfragen (von der Adresse FF02::1) der Clients beantwortet werden. Sie verbreiten über das Neighbor-Discovery-Protocol so lange Anfragen, bis ein Router reagiert. Der Router antwortet nun auf diese und übermittelt dem Client u. a. seine Interfaceadresse. Damit bekommt er nun zwei Informationen: erstens die Adresse seines Default-Routers und zweitens seinen Präfix (2001:A:A::/64 bzw. 2001:A:B::/64), woraus er nun eine offizielle Adresse zum Routen bilden kann.

Als Letztes müssen Sie noch die Routen in andere Netze auf R1 und R2 setzen. Dazu müssen Sie wissen, wohin Sie routen möchten und welche IPv6-Adresse der Nachbarrouter hat. Im Beispiel werden auf dem Gerät R1 eine Default-Route und auf R2 (nachdem die Interfaces konfiguriert wurden) spezifische Routen gesetzt.



IPv6-Route

Default-Route auf R1:

```
R1(config)# ip route ::/0 2222::1 → Alle eintreffenden Pakete werden zu R2 (2222::1) geleitet.
::/0 kennzeichnet das gesamte IPv6-Internet mit der Präfixlänge von 0.
```

Spezifische Routen auf R2:

```
R2(config)# ip route 2001:A:A::/64 2222::0
R2(config)# ip route 2001:A:B::/64 2222::0 → Es werden Pakete für das Zielnetz (2001:A:AA/64 und
2001:A:B::/64) in Richtung R1 gesendet.
```

In lokalen Netzen (Intranet) werden Default-Routen immer in Richtung des Providers (Internet) gesetzt. Spezifische Routen werden dagegen vom Provider in Richtung des lokalen Netzes (Intranet) konfiguriert.



Dynamisches Routen

Dynamische Routing-Protokolle aktualisieren ihre Routing-Tabellen automatisch durch Lernen der Netze über ihre Nachbarrouter. Bei Änderung des Zustandes eines gelernten Netzes (z. B. Nichterreichbarkeit oder Veränderung der Netzparameter) wird dies dynamisch angepasst. Sie eignen sich, um beim Vorhandensein von redundanten Wegen Alternativrouten zu ermitteln und damit die Netzverfügbarkeit zu gewährleisten. Dies ist eine Eigenschaft, die statische Protokolle nicht aufweisen.

Da dynamische Routing-Protokolle alle verfügbaren Wege und Netze lernen, kann ein Problem entstehen, da die Kapazität jedes Routers begrenzt ist. Damit die Anzahl der zu lernenden Routen überschaubar bleibt, werden sie zu Verwaltungsinstanzen zusammengefasst. Diese Instanz, auch autonomes System (AS) genannt, ist ein Verbund von Routern und den daran angeschlossenen Netzen. Sie unterstehen einem Unternehmen oder einer Organisation. Die autonomen Systeme sind untereinander über sogenannte Core-Gateways miteinander verbunden. Für RIPnG wird keine AS-Nummer benötigt, da es nicht internetfähig ist.

Folgende standardisierte Routing-Protokolle finden unter IPv6 Anwendung:

- ✓ RIPnG (Routing Information Protocol next Generation)
- ✓ OSPFv3 (Open Shortest Path First Version 3)
- ✓ IS-IS (Intermediate System to Intermediate System Protocol)
- ✓ OLSR (Optimized Link State Routing Protocol)
- ✓ EIGRPv6 (Cisco Enhanced Interior Gateway Routing Protocol)
- ✓ BGP4 (Border Gateway Protocol Version 4)

Das RIPnG-Protokoll wird vereinzelt in lokalen Netzen eingesetzt. Es ist jedoch zunehmend von OSPFv3 abgelöst worden. Der letzte Standard (BGP4) hat seine Berechtigung im WAN und wird teilweise in den Netzwerken von Providern und ausschließlich zwischen den einzelnen ISPs (Netzverbund) eingesetzt.

Ein dynamisches Routing-Protokoll erfordert folgende Konfigurationsschritte:

- IPv6-Stack freischalten
- IPv6-Adressen auf den Netzwerkkarten einstellen und diese aktivieren
- Routing-Protokoll festlegen
- Routing-Protokoll auf den Netzwerkkarten freischalten

Das letzte Beispiel wird um ein dynamisches Routing-Protokoll (OSPF) ergänzt. Dazu benötigen Sie die autonome Systemnummer. Wir nutzen hier die AS 4711. Sofern Sie über das Internet kommunizieren wollen, benötigen Sie dazu jedoch eine offizielle AS-Nummer, die Sie über die ICANN (Internet Corporation for Assigned Names and Numbers) beantragen müssen.

Spezifisch gesetzte Routen werden immer zuerst genutzt, weshalb sie vorher aus dem letzten Beispiel entfernt werden müssen.

Löschen der spezifischen Routen auf R2:

```
R2(config)# no ip route 2001:A::/64 2222::0
R2(config)# no ip route 2001:A:B::/64 2222::0
```

OSPFv3-Protokoll auf R1 und R2 festlegen:

R1(config)# ipv6 router ospf 111	→	111 ist die Nummer des OSPF-Prozesses, die Sie frei vergeben können
R1(config-rtr)# router-id 1.1.1.1	→	Festlegen einer Router-ID
R1(config-rtr)# passive-interface fa0/0	→	Deaktivieren der OSPFv3-Routinginformationen
R1(config-rtr)# passive-interface fa0/1	→	in die Usernetze
R2(config)# ipv6 router ospf 111		
R2(config-rtr)# router-id 1.1.1.2		
R2(config-rtr)# passive-interface fa0/0		
R2(config-rtr)# passive-interface fa0/1		

OSPFv3 mit der AS-Nummer 4711 auf den Netzwerkkarten von R1 freischalten:

```
R1(config)# interface fa0/0
R1(config-if)# ipv6 ospf 111 area 4711
R1(config-if)# interface fa0/1
R1(config-if)# ipv6 ospf 111 area 4711
R1(config-if)# interface s0/0/0
R1(config-if)# ipv6 ospf 111 area 4711
```

OSPFv3 mit der AS-Nummer 4711 auf den Netzwerkkarten von R2 freischalten:

```
R2(config)# interface fa0/0
R2(config-if)# ipv6 ospf 111 area 4711
R2(config-if)# interface fa0/1
R2(config-if)# ipv6 ospf 111 area 4711
R2(config-if)# interface s0/0/0
R2(config-if)# ipv6 ospf 111 area 4711
```

Damit haben Sie die Grundfunktionen des OSPF-Protokolls erfolgreich auf den Routern eingestellt.

Die korrekte Funktion des OSPF-Protokolls können Sie mit folgenden Befehlen ersehen:

```
R2# show ipv6 route
```

IPv6 Routing Table - 9 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP, U - Per-user Static route, M - MIPv6, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, D - EIGRP, EX - EIGRP external

C	2001:A::/64 [0/0]	via ::, Fast-Ethernet0/0
L	2001:A::1/128 [0/0]	via ::, Fast-Ethernet0/0
C	2001:A:B::/64 [0/0]	via ::, Fast-Ethernet0/1
L	2001:A:B::1/128 [0/0]	via ::, Fast-Ethernet0/1
O	2001:A:C::/64 [110/65]	via FE80::60:FF:FE1:C, Serial0/0/0
O	2001:A:D::/64 [110/65]	via FE80::60:FF:FE1:C, Serial0/0/0
C	2222::/127 [0/0]	via ::, Serial0/0/0
L	2222::/128 [0/0]	via ::, Serial0/0/0
L	FF00::/8 [0/0]	via ::, Null0

Anhand der Einträge in der Routingtabelle des Routers R2 erkennen Sie, dass er durch das Protokoll OSPFv3 (O) die Netze von R1 dynamisch gelernt hat.

Plus **Wissenstest: Netzwerkkomponenten und Routing**

9.12 Fehlersuche in kabelgebundenen Netzwerken

Auswahl der Messgeräte

Mini-LAN-Tester

Mit einem Mini-LAN-Tester kann geprüft werden, ob alle verwendeten Pins eines Datenkabels vom Patchpanel bis zur Datendose korrekt durchgeschaltet sind. Sehr häufig besitzen Sender und Empfänger des Mini-LAN-Testers für jeden einzelnen Pin und den Schirm eine eigene LED. Ist beispielsweise Pin 3 aufgrund einer Beschädigung des Datenkabels unterbrochen, dann leuchtet die 3. LED am Empfänger des Mini-LAN-Testers nicht auf. Wird anstelle von LEDs ein Display verwendet, zeigt dieses die entsprechende Unterbrechung an.

Digitalmultimeter

Neben der Durchgangsprüfung von Kupferkabeln können mit einem digitalen Multimeter auch Spannungs- und Widerstandsmessungen ausgeführt werden. Bei einer Twisted-Pair-Verkabelung kann beispielsweise die korrekte Steckermontage geprüft werden. Mit ihm lassen sich schnell Kurzschlüsse zwischen den Adern und dem Schirm (sofern ein geschirmtes Twisted-Pair-Kabel eingesetzt wurde) oder defekte Ports an Datendosen und Patchpanels feststellen.

Leitungssuchgerät

Gerade in größeren Unternehmen mit einer hohen Kabeldichte erweist sich das Leitungssuchgerät als ständiger Begleiter. Wurden Datendosen und Patchpanels mangelhaft oder gar nicht beschriftet, kann mit dem Leitungssuchgerät der Port des gewünschten Kabels schneller identifiziert werden. Dies erfolgt ohne großen Aufwand, da der Sender direkt an der Datendose oder am Patchpanel angeschlossen werden kann. Der Empfänger meldet einen Signaltion, sobald er in der Nähe des entsprechenden Datenkabels ist. Patchpanel und Datendose müssen also nicht geöffnet werden.

Kabelmessgerät

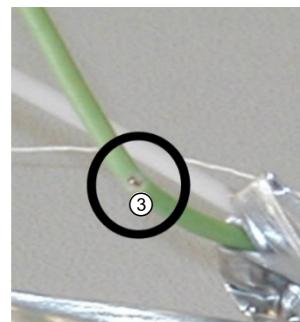
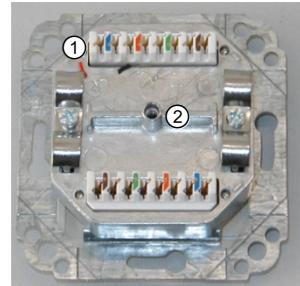
Mit einem Kabelmessgerät können die elektrischen Eigenschaften wie Kapazität, Impedanz und Rückflussdämpfung eines Datenkabels gemessen werden. Bei der Fehlersuche gibt es Aufschluss über die korrekte Verdrahtung der Übertragungsstrecke. Anhand einer im Display dargestellten Grafik werden Adernvertauschungen und -unterbrechungen sofort dargestellt und können so leicht beseitigt werden. Vor allem Beschädigungen am Datenkabel, die von außen nicht erkennbar sind (Aderabriß durch zu starke Zugkraft, verdeckte Scheuerstellen) können Sie mit einem Kabelmessgerät feststellen.

Szenario 1: Kurzschluss beheben

Bei einer Neuverkabelung eines Büros mit einem Datenkabel der Kategorie 6A werden zur Protokollierung die einzelnen Datenstrecken mit dem Kabelmessgerät geprüft. Bei einer Verbindung zeigt das Kabelmessgerät einen Kurzschluss zwischen Pin 1, 2, 3 und Schirm.

Vorgehensweise

- ▶ Öffnen Sie die betreffende Datendose und das Patchpanel und kontrollieren Sie die Anschlüsse an den LSA+-Leisten. Sind die einzelnen Adern korrekt an der LSA+-Leiste aufgelegt?
- ▶ Drahtreste von Kabeladern ① oder des Schirmgeflechts ② könnten die Ursache für einen Kurzschluss sein. Eventuelle Drahtreste müssen entfernt werden.
- ▶ Überprüfen Sie die Stelle, an der das Datenkabel abgemantelt wurde. Zu tiefe Schnitte mit einem scharfen Messer könnten das Datenkabel beschädigt und die Isolierung der einzelnen Adern verletzt haben ③. Auch eine zu fest oder falsch sitzende Schirmklemme an der Datendose/am Patchpanel kann durch Quetschungen des Kabels solche Fehler verursachen.
- ▶ Überprüfen Sie die RJ-45-Ports der Datendose und des Patchpanels. Messen Sie die einzelnen Kontakte in der RJ-45-Buchse zur LSA+-Anschlussleiste mit einer Durchgangsprüfung. Drahtreste des Schirmgeflechts könnten unter das RJ-45-Gehäuse gerutscht sein und auf der Platine einen Kurzschluss verursachen. Diese Stelle ist meist schwer zugänglich. Versuchen Sie, durch Klopfen und Ausblasen etwaige Drahtreste zu entfernen.



Verlauf des Datenkabels kontrollieren

- ▶ Kontrollieren Sie den Verlauf des Datenkabels. Sind auf der Strecke äußerliche Schäden zu erkennen? Gab es beim Einziehen der Datenkabel scharfe Kanten, vor allem bei längeren Strecken, die das Kabel beschädigt haben könnten? Ein direkter Schaden am Datenkabel kann in diesem Fall mit einem Multimeter festgestellt werden.
- ▶ Klemmen Sie das Datenkabel von der Datendose und dem Patchpanel ab und messen Sie die einzelnen Adern gegen den Schirm (Durchgangsprüfung).
- ▶ Sind am Datenkabel Knickstellen erkennbar?

Szenario 2: Rückflussdämpfung mindern

Bei einer Neuverkabelung eines Büros mit Datenkabeln der erweiterten Kategorie 6A werden zur Protokollierung alle Datenstrecken mit dem Kabelmessgerät geprüft. Bei einer Verbindung zeigt das Kabelmessgerät eine zu hohe Rückflussdämpfung.

Vorgehensweise

- ▶ Überprüfen Sie zuerst den einwandfreien Zustand der Akkus und der Messschnüre des Kabelmessgerätes. Führen Sie eventuell einen Nullabgleich durch.
- ▶ Wiederholen Sie die Messung.
- ▶ Tritt der Fehler erneut auf, überprüfen Sie die Länge des Datenkabels anhand der Messung. Die maximale Länge von 100 m sollte im Normalfall nicht überschritten werden.
- ▶ Öffnen Sie die entsprechende Datendose und das Patchpanel und überprüfen Sie den korrekten Sitz der Adern in den LSA+-Anschlussleisten.

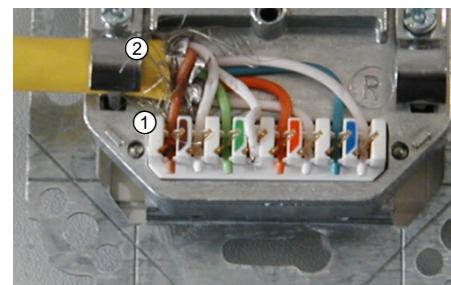
Häufige Ursachen für eine fehlerhafte Rückflussdämpfung sind schlechte Verdrillung und schlechte Abschirmung der Adern im Anschlussbereich. Die Schirmfolie und die Verdrillung der Doppeladern sollten so weit wie möglich an die LSA+-Anschlussleiste herangeführt werden.

Szenario 3: Unterbrechung am Pin beheben

Bei einer Neuverkabelung eines Büros mit einem Datenkabel der Kategorie 6A werden zur Protokollierung die einzelnen Datenstrecken mit einem zertifizierten Kabelmessgerät geprüft. Bei einer Verbindung zeigt das Kabelmessgerät eine Unterbrechung an Pin 1.

Vorgehensweise

- ▶ Öffnen Sie die betreffende Datendose und das Patchpanel und kontrollieren Sie die Anschlüsse an den LSA+-Leisten. Sind die einzelnen Adern korrekt an der LSA+-Leiste aufgelegt? ①
- ▶ Überprüfen Sie die Stelle, an der das Datenkabel abgemantelt ② wurde. Zu tiefe Schnitte mit einem scharfen Messer könnten das Datenkabel beschädigt und die Isolierung der einzelnen Adern verletzt haben. Auch eine zu fest oder falsch sitzende Schirmklemme an der Datendose/am Patchpanel kann durch Quetschungen des Kabels solche Fehler verursachen.
- ▶ Überprüfen Sie die RJ-45-Ports der Datendose und des Patchpanels. Messen Sie den betreffenden Kontakt in der RJ-45-Buchse zur LSA+-Anschlussleiste mit einer Durchgangsprüfung.



Nicht fachgerecht aufgelegte Datendose

Materialfehler sind auch bei namhaften Herstellern nicht auszuschließen. Haarrisse auf der Leiterplatte können beispielsweise die Ursache für eine Unterbrechung sein.

- ▶ Kontrollieren Sie den Verlauf des Datenkabels. Sind auf der Strecke äußerliche Schäden ③ zu erkennen? Gab es beim Einziehen der Datenkabel scharfe Kanten, vor allem bei längeren Strecken, die das Kabel beschädigt haben könnten? Sind am Datenkabel Knickstellen erkennbar?



Beschädigter Kabelmantel

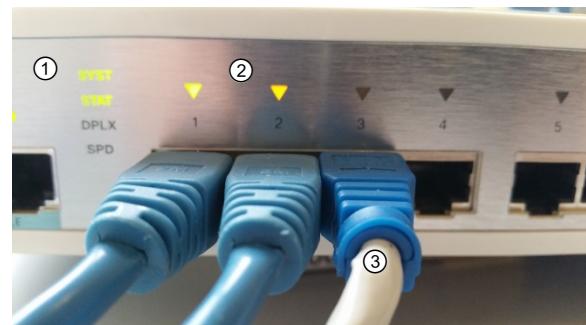
Szenario 4: Fehlende Netzwerkverbindung wiederherstellen

In einer Firma mit einem 1-Gbit-Netzwerk kann sich ein Benutzer nicht mehr am Netzwerk anmelden.

Vorgehensweise

- ▶ Ist der Switch an das Stromnetz angeschlossen und ist die System-LED aktiv ①? Dann ist der Switch wahrscheinlich vollständig funktionsfähig. Ist dies nicht der Fall, überprüfen Sie die Stromversorgung mit dem Multimeter bzw. starten Sie den Switch neu.

Leuchtet keine System-LED, liegt das Problem an der Stromversorgung (Steckdose liefert keine Spannung, Stromversorgungskabel bzw. Steckernetzteil ist defekt). Sollten dagegen die System-LEDs keinen korrekten Status anzeigen, ist der Switch defekt (z. B. durch Probleme mit der Firmware).



Link-Anzeige an einem Switch

- ▶ Wird an der Netzwerkkarte bzw. am Switch ein Link ② angezeigt? Sollte kein Link angezeigt werden, tauschen Sie das Patchkabel ③ zur Überprüfung aus.
- ▶ Befindet sich in der Nähe eine weitere Datendose? Schließen Sie zur Überprüfung den PC an dieser Datendose an. Vergessen Sie nicht, dass diese Datenverbindung auch am Switch vorhanden sein muss. Wird an der Netzwerkkarte nun ein Link angezeigt? Wenn dies nicht der Fall ist, überprüfen Sie die Datenverbindung mit dem Mini-LAN-Tester.
Bei Unterbrechungen verfahren Sie dann wie in Kap. 9.12 – Szenario 3 beschrieben.
- ▶ Wenn kein Link angezeigt wird, tauschen Sie die Netzwerkkarte aus.

Häufige Fehlerquellen (Zusammenfassung)

Fehler und Lösungen

Fehlerbeschreibung	Mögliche Lösung
Adernvertauschung laut Kabelmessgerät	Pinbelegung in der Datendose und dem Patchpanel prüfen und ggf. nach EIA/TIA 586B korrigieren
Kurzschluss zweier oder mehrerer Adern	LSA+-Anschlussleisten in der Datendose und am Patchpanel auf Drahtreste prüfen Kabelabmantelung auf Schnitte oder Quetschungen prüfen Kabelverlauf auf Beschädigung prüfen
Unterbrechung einer oder mehrerer Adern	Korrekte Sitz der Adern in den LSA+-Anschlussleisten von Datendose und Patchpanel prüfen kontakte zur LSA+-Anschlussleiste mit Durchgangsprüfung messen
Zu hohe Rückflussdämpfung	Zu langes Datenkabel (maximal 100 m) Folienschirm und Verdrillung der Adernpaare müssen so weit wie möglich an die LSA+-Anschlussleiste herangeführt werden. Defekte Einsätze bei modularen Systemen Nichteinhaltung der Farbcodierung nach EIA/TIA 586B
Kein Link am Netzwerkport	Defekte Patchkabel, defekte Netzwerkkarte, nicht funktionierender Switch Datenleitung mit einem LAN-Tester oder Protokoll-Analyser prüfen

10 Weitverkehrsnetze (WAN)

In diesem Kapitel erfahren Sie

- ✓ welche verschiedenen Arten von Weitverkehrsnetzen existieren
- ✓ welche Übertragungstechniken verwendet werden
- ✓ wie die Übertragungsraten eingesetzt werden

Voraussetzungen

- ✓ Grundlagen der Telekommunikation
- ✓ Grundlagen der Signalübertragung

10.1 Übertragungstechniken in Weitverkehrsnetzwerken

Integrated Services Digital Network

Die Abkürzung ISDN steht für „Integrated Services Digital Network“, was mit „dienstintegrierendes digitales Telekommunikationsnetz“ übersetzt werden kann. Da sich die englische Bezeichnung bereits weltweit durchgesetzt hat, wurde sie auch in den offiziellen Sprachgebrauch der Telekom übernommen. Jeder der vier Namensbestandteile in dieser englischen Bezeichnung verweist auf eine wesentliche Eigenschaft dieses Telekommunikationsnetzes.

Integrated (integriert)

Im ISDN werden alle Daten in digitalisierter Form übertragen. Dadurch ist es möglich, die Signale für Sprache, Texte, Bilder und Daten über dieselbe Leitung zu übermitteln. So ist nur noch ein Anschluss mit einer einheitlichen Rufnummernbasis nötig, um das gesamte Dienstangebot im ISDN zu nutzen. Gleichzeitig erleichtert es den Einsatz multifunktionaler Endgeräte, wie z. B. PCs, mit denen mehrere Dienste genutzt werden können.

Services (Dienste)

ISDN bietet nicht nur die Möglichkeit, viele der vorhandenen Kommunikationsdienste zu nutzen, es unterstützt außerdem Kommunikationsarten wie z. B. Bildtelefonie oder digitales Fax.

Digital

Im ISDN werden die Sprache und die Informationen aller verfügbaren Dienste in digitaler Form auf der Leitung übertragen. Dies geschieht, indem die zu übermittelnde Information in eine aus 0 und 1 bestehende Ziffernfolge verschlüsselt (binär codiert) wird.

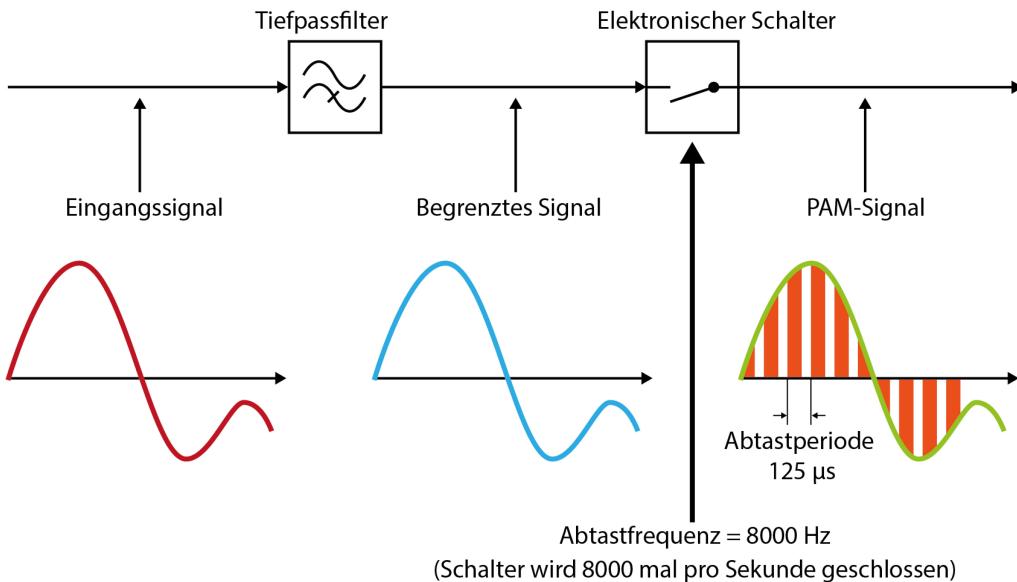
Beim Empfänger werden die Signale entschlüsselt und wieder hörbar bzw. lesbar gemacht. Vorteile der Digitaltechnik sind die bessere Übertragungsqualität (z. B. Telefon, Telefax) sowie eine geringere Fehlerquote und höhere Geschwindigkeit bei der Datenübermittlung gegenüber einem analogen Anschluss. Im analogen Telefonnetz werden, wie der Name schon sagt, die Signale als analoge Töne übertragen. Mit ihm ist ebenfalls eine Übertragung von Daten über analoge Modems möglich. Dies ist wegen der starken Konkurrenz von DSL, UMTS und LTE heutzutage aber kaum noch gebräuchlich.

Network (Netzwerk)

Der Netzausbau von ISDN ist weitgehend mit dem herkömmlichen Telefonnetz identisch. ISDN benötigt eine höhere Leitungsgüte als analoge Telefonie. Die bereits vorhandenen Telefonleitungen konnten in den meisten Fällen auch mit ISDN weitergenutzt werden. In Deutschland ist das gesamte Telefonnetz, auch das analoge, seit 1998 komplett auf digitale Vermittlungstechnik umgerüstet. Die ISDN-Technologie wurde zum Ende 2018 von der Deutschen Telekom eingestellt und wird noch bis 2020 von Vodafone unterstützt. Internetserviceprovider bieten als Ersatz SIP-Trunk an, welches einen Großteil der ISDN-Merkmale fast vollständig unterstützt.

Digitale Telefonie

Telefongespräche werden im ISDN ausschließlich digital übertragen. Das analoge Signal wird hinter dem Mikrofon mit einer elektrischen Schaltung abgetastet. In der Telefonie wird mit einem Frequenzbereich von 340 Hz bis 3,4 kHz gearbeitet. Um eine gute Sprachqualität zu gewährleisten, muss die Abtastung mit **mindestens** der doppelten höchsten Frequenz erfolgen (laut dem Nyquist-Shannon-Abtasttheorem). Im ISDN beträgt die Abtastrate 8000 Hz. Zusätzlich wird vor der Abtastung ein Filter geschaltet, der Frequenzen oberhalb 3400 Hz herausfiltert. Durch die Signalabtastung entsteht eine Folge von Impulsen. Die Hüllkurve dieser Abtastwerte ergäbe wieder das alte Signal. Das Verfahren zur Signalabtastung wird Pulsamplitudenmodulation (PAM) genannt.



Schaltbild der PAM

Die Impulse, die immer noch analog sind, können jetzt digitalisiert werden. Die Amplitudenwerte der einzelnen Impulse werden in Quantisierungsschritte eingeteilt, wobei jedem Quantisierungsschritt ein binärer Wert zugeordnet ist. Je mehr Quantisierungsschritte verwendet werden, desto originalgetreuer wird das übertragene Signal. Bei ISDN sind dies $2^8 = 256$ Quantisierungsschritte; damit ist jeder abgetastete Wert mit 8 Bit codiert. Die Bitrate des ISDN-Datenkanals beträgt also $8 \text{ Bit} * 8000/\text{s} = 64\text{kbit}/\text{s}$. Dieses Verfahren wird Pulscodemodulation (PCM) genannt.

Grundsätzlich werden zwei verschiedene Anschlüsse unterschieden:

- ✓ BRI: Basic Rate Interface, Basisanschluss
- ✓ PRI: Primary Rate Interface, Primärmultiplex-Anschluss

Basisanschluss (BRI)

Der ISDN-Basisanschluss umfasst drei eigenständige Kanäle:

- ✓ 2 Datenkanäle (B1 und B2; B=Bearer Channel)
- ✓ 1 Steuerkanal (D; D=Data Channel)

Für den ISDN-Basisanschluss (BRI) reicht die für das herkömmliche Telefonnetz verwendete Kupferdoppelader aus. Die Leitungsschnittstelle wurde von der Deutschen Telekom als UK₀-Schnittstelle definiert. Für die beiden Datenkanäle beträgt die Bitrate je 64 kbit/s, für den Steuerkanal 16 kbit/s.

Die beiden ISDN-Datenkanäle können unabhängig voneinander für jeden im ISDN angebotenen Dienst genutzt werden. Die für eine Kommunikation notwendige Zeichengabe (z. B. für den Verbindungsaufbau) erfolgt durch den Steuerkanal. Der Netzabschluss des ISDN BA wird durch ein sogenanntes Network Terminal (NTBA) gebildet. Dieser NTBA stellt die international genormte S₀-Schnittstelle über zwei gleichwertige RJ-45-Buchsen zur Verfügung, über die ein vieradriger passiver Bus (S₀-Bus) anschließbar ist. Dieser Bus stellt die Verbindung zwischen dem NTBA und dem oder den ISDN-Endgeräten her.

Speisung der Endgeräte

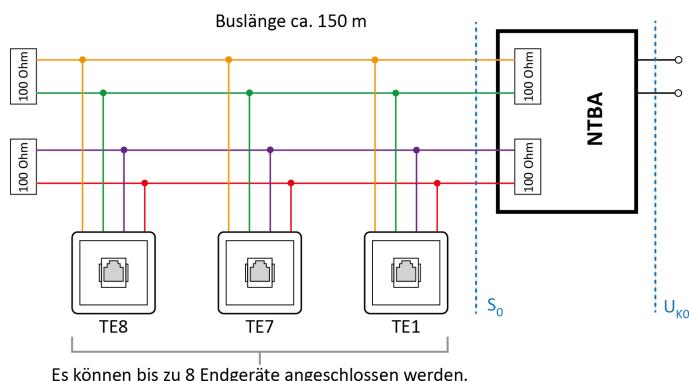
Die Speisung von Endgeräten kann bei geringem Leistungsbedarf der NTBA übernehmen, wenn er selbst am Stromnetz angeschlossen ist (Normalbetrieb). Wird er nicht aus dem Stromnetz versorgt, spricht man vom Notbetrieb. Der NTBA erhält dann einen geringen Strom von der Vermittlungsstelle und kann nur noch ein ISDN-Gerät mit sehr geringer Leistungsaufnahme versorgen. Haben Endgeräte einen großen Leistungsbedarf, benötigen sie einen eigenen Netzanschluss zum 230-V-Netz.

Ausgangswerte am NTBA	Normalbetrieb	Notbetrieb
Spannung	40 V +5 % / -15 %	40 V +5 % / -15 %
Leistung	4,5 W	0,41 W
Strombegrenzung im NTBA	150 mA	15 mA
Speisung am S₀-Bus	40 V +5 % / -40 %	40 V +5 % / -20 %

Beim passiven S₀-Bus dürfen maximal vier Endgeräte jeweils 1 W Leistung entnehmen. Darum reicht die Leistung des NTs für maximal vier Telefone.

Anschlussarten

Der Basisanschluss (BRI) bietet neben dem Anlagenanschluss, der sich nur für ein Endgerät (z. B. eine Telefonanlage) eignet, auch die bekannteste Anschlussvariante: den **Mehrgeräteanschluss**. Hier sind an einer Leitungslänge von bis zu 150 m (bei einem Aderndurchmesser von mindestens 0,6 mm) bis zu acht Endgeräte anschließbar. Diese Anschlusskonfiguration ist eine Punkt-zu-Mehrpunkt-Verbindung (Point-to-Multipoint).

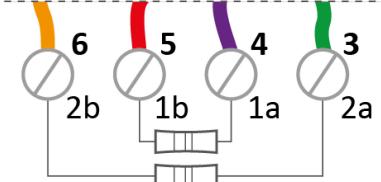


Schaltbild eines Mehrgeräteanschlusses

Der NTBA ist über ein Telefonkabel an der ersten von der Telekom im Gebäude eingerichteten TAE-Dose angeschlossen, welche die Verbindung zur örtlichen digitalen Vermittlungsstelle darstellt (DIVO).

Wird der NTBA an einem Ende des Busses platziert, sind am anderen Ende, d. h. in der letzten TAE-Dose, zwei Abschlusswiderstände zu je 100 Ohm (Toleranz 5 Ohm) anzuschließen, wie die nebenstehende Abbildung zeigt.

Dieses Anschlusschema muss unbedingt eingehalten werden: 1a und 1b bilden die Sendeaderne, 2a und 2b die Empfangsaderne des Busses. Jedes Paar ist am Busende mit einem 100-Ohm-Widerstand abzuschließen (zu terminieren), damit keine Reflexionen auftreten. Schließen Sie niemals einen Widerstand zwischen 1x und 2x an: Dort erzeugt der NTBA die Speisespannung für ISDN-Telefone. Eine Überlastung von NTBA und Widerständen wäre die Folge.

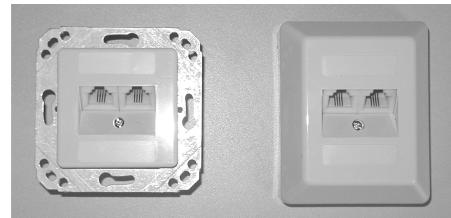


Abschlusswiderstände am ISDN

Wenn am zweiten Anschluss des NTBA ein weiterer ISDN-Bus angeschlossen ist, muss die interne Terminierung durch einen Jumper im NTBA abgeschaltet und die beiden Busse jeweils an den Enden mit 100-Ohm-Widerständen abgeschlossen sein. Es entsteht damit ein einziger durchgehender Bus.

Endgeräteanschlussdosen

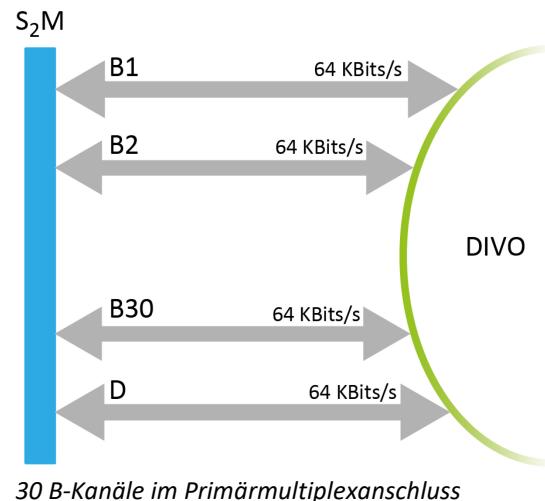
Endgeräteanschlussdosen für ISDN gibt es in den verschiedensten Ausführungen, zur Aufputz- und Unterputz-Installation und in einfacher oder zweifacher (mit 1 oder 2 Anschlüssen) Ausführung. Bei der Anschlusstechnik wird zwischen Schraubklemmen und LSA+-Technik unterschieden.



Anschlussdose für Auf- und Unterputzmontage

Primärmultiplexanschluss (PRI)

Die S₂M-Schnittstelle ist eine reine Punkt-zu-Punkt-Verbindung. Die Abschlusswiderstände haben nicht wie beim S₀-Anschluss 100 Ohm, sondern 120 Ohm, und die maximale Leitungslänge beträgt 200 m. Die S₂M-Schnittstelle hat 30 Nutzkanäle und einen wesentlich breiteren D-Kanal (64 kbit/s) als die S₀-Schnittstelle (16 kbit/s). Zusätzlich besitzt die S₂M-Schnittstelle einen eigenen Kanal zur Synchronisierung des Rahmens (mit ebenfalls 64 kbit/s). Die Verbindung eines S₂M-Anschlusses zwischen Vermittlungsstelle und Teilnehmer erfolgt entweder über zwei Kupferdoppeladern oder zwei Glasfasern.



30 B-Kanäle im Primärmultiplexanschluss

Die Unterbringung von insgesamt 32 Kanälen ermöglicht das Zeitmultiplexverfahren. Es handelt sich um eine Punkt-zu-Punkt-Verbindung mit einer Brutto-Datenrate von 2,048 Mbit/s. Verfahren wie Kollisionserkennung und Zugriffssteuerung sind nicht integriert. Die Endeinrichtung ist selbst für die Stromversorgung verantwortlich. Eine Stromversorgung über die Vermittlungsstelle ist nicht vorgesehen, d. h., bei einem Stromausfall kann der Betrieb nur mithilfe einer unterbrechungsfreien Stromversorgung (USV) aufrechterhalten werden.

Leistungsmerkmale des Euro-ISDNs

- ✓ Rufnummernübermittlung
- ✓ Halten einer Verbindung/Rückfragen/Makeln/Anklopfen
- ✓ Anrufweiterschaltung sofort/nach Zeit/bei besetzt
- ✓ Mehrfachrufnummer (MSN)
- ✓ Durchwahl
- ✓ Übermittlung der Tarifinformation
- ✓ Geschlossene Benutzergruppe
- ✓ Rückruf bei besetzt
- ✓ Sperren des Anschlusses – Vollsperrre/abgehend für Ausland/abgehend interkontinental
- ✓ Übertragungsrate 64 kbit/s pro Nutzkanal

Die Verfügbarkeit der Leistungsmerkmale ist abhängig von der gewählten Anschlussart (Anlagen- oder Mehrgeräteanschluss sowie Standard- oder Komfortanschluss). Analoge Endgeräte können am Euro-ISDN betrieben werden, sofern sie über eine ISDN-Telefonanlage oder einen Terminal-Adapter angeschaltet werden.

10.2 VoIP mit SIP-Trunk

Der ISDN-Standard basiert einerseits auf einer mittlerweile veralteten Technologie, zum anderen wird seit Jahren das Internet für die Telefonie (VoIP) immer mehr forciert. Ein paralleler Betrieb der Netze erfordert einen unwirtschaftlichen Personal-, Energie- und auch finanziellen Aufwand. Die Vorteile von VoIP (Voice over Internet Protocol) oder auch NGN (Next-Generation-Network) gegenüber ISDN sind folgende:

- ✓ Einheitliches Übertragungsprotokoll (IP/IPv6) für alle Dienstmerkmale (Voice, Video, Data)
- ✓ Kostenreduktion durch Nutzung vorhandener Standardtechnologien
- ✓ Flexibilität bei der Nutzung von Zugangs-Protokollen und einfache Skalierbarkeit bei der Anzahl der User
- ✓ Nutzung von Unified Communications (UC). Sie definiert für den User eine Telefonie- und/oder Multimedia-Kommunikation, unabhängig vom Netzwerk, dem verwendeten Endgerät (Telefon, Smartphone, Tablet, Notebook, ...) und der hierfür verwendeten Applikation
- ✓ Die Verfügbarkeit kann bei Netzwerkstörungen durch redundante Verbindungen (Trunks) über unterschiedliche ISPs (Internet Service Provider) gewährleistet werden
- ✓ SIP-Trunks unterstützen aktuelle Cloud-Technologien und virtuelle Contact Center
- ✓ Interoperabilität des SIP-Standards zwischen diversen Herstellern

SIP-Trunk

VoIP nutzt für die Kommunikation in den meisten Fällen den Standard **SIP** (Session Initiation Protocol). SIP dient zur Steuerung und Überwachung einer Kommunikationssitzung von Telefonaten, Multimedieverbindungen oder dem Austausch von Daten (z. B. Fax oder SMS). Es wird u. a. in den Standards RFC 3261-3263, 6086 und 6665 beschrieben. Jedes VoIP-Endgerät bzw. jede zugewiesene Rufnummer meldet sich separat beim SIP-Provider an.

Bei einem **SIP-Trunk** (bezeichnet die Bündelung von Sprachverbindungen über einen virtuellen Anschluss) meldet sich nur die lokale IP-basierende Telefonanlage (PBX Private Branch Exchange) beim SIP-Trunk-Provider an. Über diese lokale Verbindung laufen alle VoIP-Telefonate aller Nebenstellen. Die lokale IP-PBX verwaltet nun ein- und ausgehende Telefonate und kommuniziert mit allen Nebenstellen. Dabei muss die IP-PBX zwangsläufig nicht physisch lokal vorhanden sein, sondern kann sich auch virtuell in einer PBX-Cloud befinden. Ein SIP-Trunk ist relativ einfach zu implementieren, da nur eine Anmeldung der IP-PBX beim ISP realisiert werden muss. Analog verhält es sich, wenn Sie aus Verfügbarkeitsgründen weitere ISPs anbinden. Dadurch haben Sie sowohl eine effektive Kontrolle Ihrer Telefonate und gleichzeitig die Sicherheit des Anschlusses, da die ausgehenden Verbindungen von einer zentralen IP-PBX ausgehen.

10.3 DSL (Digital Subscriber Line)

Alle DSL-Varianten sind Übertragungstechniken im Breitbandformat. Sie werden über herkömmliche Telefonleitungen realisiert. Es gibt mehrere DSL-Verfahren. Hier die wichtigsten:

- ✓ ADSL (asymmetrical digital subscriber line)
- ✓ SDSL (symmetric digital subscriber line)
- ✓ HDSL (high data rate digital subscriber line)
- ✓ VDSL (very high bitrate digital subscriber line)

DSL wurde für die bereits bestehende Telefonverkabelung entwickelt. Die Übertragungsgeschwindigkeiten sind vom jeweiligen Verfahren abhängig. Weiterhin spielt die Leitungsqualität eine große Rolle. Je größer die Entfernung zum jeweiligen Benutzer, desto geringer wird auch die Übertragungsgeschwindigkeit. Deshalb kann DSL nur im Anschlussbereich einer Vermittlungsstelle realisiert werden. Die Entfernung zwischen Vermittlungsstelle und Benutzer kann maximal einige Kilometer betragen.

In der herkömmlichen analogen Telefonie liegt die höchste Übertragungsfrequenz bei 3,4 kHz. Diese Grenze wurde für DSL aufgehoben. Hier wird die gesamte Bandbreite der Kupferdoppelader verwendet. Ermöglicht wird dies durch die Verwendung von DSL-Modems. In diesem Modem wird das Signal mit dem DMT-Verfahren (Discrete Multi Tone Modulation) aufbereitet. Damit die Telefonleitung gleichzeitig für eine DSL-Verbindung und ein Telefongespräch genutzt werden kann, ist ein sogenannter Splitter erforderlich. Er trennt die Telefonsignale von den hochfrequenten DSL-Signalen.

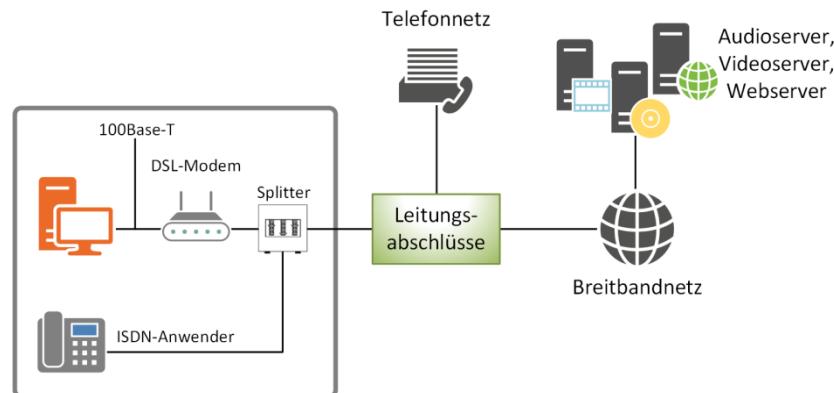
Grundsätzlich wird zwischen zwei verschiedenen DSL-Verfahren unterschieden. Diese werden als „symmetrisch“ und „asymmetrisch“ bezeichnet. Beim symmetrischen DSL ist die Übertragungsgeschwindigkeit vom und zum Benutzer (Upstream und Downstream) gleich. Beim asymmetrischen DSL unterscheiden sich die Übertragungsraten im Upstream (zum Internet hin) und im Downstream (vom Internet her). Beide Variationen eignen sich sehr gut für den schnellen Internetzugang, die Übertragung von Videodaten, Videokonferenzen u.v.m.

DSL-Variante	Übertragung	Downstream	Upstream	Reichweite mit TP
ADSL	asymmetrisch	bis zu 6 Mbit/s	bis zu 1,5 Mbit/s	ca. 5 km
ADSL2+	asymmetrisch	bis zu 25 Mbit/s	bis zu 3,5 Mbit/s	ca. 4 km
SDSL	symmetrisch	2,3 Mbit/s	2,3 Mbit/s	ca. 2,5 km
HDSL	symmetrisch	2 Mbit/s	2 Mbit/s	ca. 4 km
VDSL	asymmetrisch	bis zu 52 Mbit/s	bis zu 2,3 Mbit/s	ca. 0,5 km
VDSL2	symmetrisch	bis zu 100 Mbit/s	bis zu 100 Mbit/s	ca. 1 km
G.fast	symmetrisch	bis zu 1 Gbit/s	bis zu 1 Gbit/s	< 200 m

Die asymmetrischen DSL-Varianten sind eher für den Heimgebrauch gedacht. Sie bieten zwar eine hohe Übertragungsrate, die jedoch abhängig von der Bandbreite ist, die allen Teilnehmern gemeinsam zur Verfügung steht. Die wichtigsten Nachteile dabei sind, dass es einmal pro Tag eine Zwangstrennung gibt, die Upload-Rate wesentlich geringer als die Download-Rate ist („asymmetrisch“) und der Kunde oft keine statische (feste) öffentliche IP-Adresse erhält. Bei jeder neuen Einwahl ist daher eine andere öffentliche IP-Adresse möglich. Im Gegensatz dazu sind die symmetrischen DSL-Varianten eher für Firmen geeignet, da sie die oben genannten Nachteile nicht aufweisen und zudem von Haus aus meist mehrere statische IP-Adressen mitbringen.

ADSL-Verfahren

ADSL eignet sich sowohl für Firmen als auch für Privatanwender. Für die Realisierung ist in der Vermittlungsstelle ein DSLAM (DSL-Access-Multiplexer) und beim Benutzer ein DSL-Modem erforderlich, das im Router integriert ist.

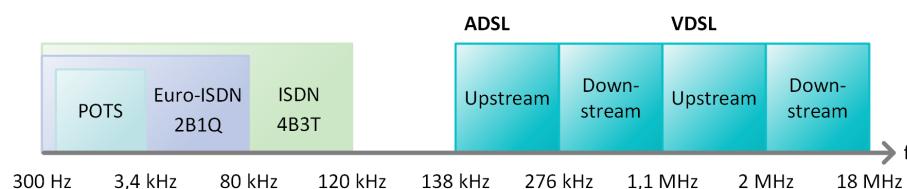


Schaltungsprinzip ADSL

ADSL ist in mehreren Versionen verfügbar und wurde von der ANSI (T1.413) und der ETSI genormt. Es verwendet zur Codierung das DMT (Discrete Multi Tone Modulation) und unterstützt in der Version ADSL2+ Übertragungsgeschwindigkeiten von bis zu 25 Mbit/s.

Bei der DSL-Technik wird die Übertragung auf viele schmale Hochfrequenz-Bänder („Bins“) mit je 4,3125 kHz Bandbreite verteilt. Die Anzahl der Bänder kann von 256 Trägern bei ADSL bis zu 4096 bei VDSL reichen. Das DMT-Modulationsverfahren baut in jedem Band eine eigene Verbindung auf. Der Frequenzbereich kann sich über mehrere MHz erstrecken und reicht damit in den Kurzwellenbereich. Gestörte Bänder (z. B. durch Rundfunksender) bleiben so lange abgeschaltet, bis die Störung vorbei ist.

Heutzutage bieten die Provider für DSL eine Flatrate an. Damit ist in dem monatlichen Preis das gesamte Übertragungsvolumen enthalten. Dennoch kann es besonders im Privatbereich vorkommen, dass manche Provider ab einem bestimmten Übertragungsvolumen die Leitung drosseln.



Frequenzbereiche der Telekommunikation

DSL light

Gegen Ende 2002 hat die Deutsche Telekom das T-DSL light eingeführt. Der Unterschied zum DSL liegt in der halben Downstream-Geschwindigkeit von maximal 384 kbit/s. Der Upstream erfolgt mit maximal 64 kbit/s. Durch die geringere Übertragungsrate ist eine Erhöhung der Reichweite möglich. So können auch Haushalte mit einem DSL-Anschluss versorgt werden, die mehr als 4 km von der nächsten Vermittlungsstelle entfernt sind.

HDSL (ITU-T G.991.1)

Für High Data Rate Digital Subscriber Line wurden in Europa Datenraten von 2,048 Mbit/s (E1-Leitung) und in den USA von 1,544 Mbit/s (T1-Leitung) spezifiziert. Die europäische Norm erfordert drei, die amerikanische nur zwei vorhandene Adernpaare. Es können Entfernung bis 5 km überbrückt werden. Der Nachfolger ist SDSL.

HDSL2

HDSL2 wurde Anfang 1998 als Normenvorschlag dem ANSI vorgelegt. Der Kern des Vorschlags betrifft die Leistung einer T1-Leitung über nur ein Adernpaar. Es ist in den Standard G.SHDSL übergegangen.

SDSL (ITU-T G.991.2)

Symmetric Digital Subscriber Line ist wie HDSL ein Vollduplexverfahren mit symmetrischen Übertragungsgeschwindigkeiten von bis zu 2,3 Mbit/s. Die maximale Reichweite liegt bei 3,5 km. SDSL ist auch unter dem Namen Single-Pair High-Speed Digital Subscriber Line bekannt, wobei die Abkürzung SHDSL zu Verwechslungen führen kann. Eine gleichzeitige Verwendung von Telefonen ist an einem SDSL-Anschluss nicht mehr möglich bzw. nur mit VoIP (Voice over IP) zu realisieren. Heute erhält man in der Regel einen G.SHDSL-Anschluss, wenn SDSL gewünscht wird.

G.SHDSL

G.SHDSL (Global Standard for Single-Pair High-Speed Digital Subscriber Line) fasst die Standards SDSL und HDSL2 zusammen (laut ITU-Standard G.991.2). Dabei ist die Übertragungsrate in beide Richtungen gleich groß, es handelt sich also um eine symmetrische Verbindung. Über eine Doppelader werden bis zu 2 Mbit/s, mit zwei Doppeladern bis zu 4 Mbit/s erreicht.

SHDSL

Symmetrical High-Density Digital Subscriber Line bzw. auch Symmetrical High Bitrate Digital Subscriber Line ist ebenfalls eine symmetrische Verbindung. Es wird darunter eine DSL-Standleitung verstanden, die bis zu 8 Mbit/s in beiden Richtungen bereitstellen kann.

VDSL (ITU-T G.993.1)

Very High Bitrate Digital Subscriber Line beruht auf denselben technischen Überlegungen wie ADSL und ist die schnellste DSL-Variante und für privaten Gebrauch ausgelegt. Es können folgende Datenraten realisiert werden:

- ✓ Downstream: zwischen 12,96 Mbit/s und 51,84 Mbit/s
- ✓ Upstream: zwischen 1,5 Mbit/s und 2,3 Mbit/s

Allerdings sind diese Angaben stark von der Entfernung zur Vermittlungsstelle abhängig. So hat sich bei etwa 1000 m Entfernung die maximale Übertragungsbandbreite bereits halbiert auf ca. 26 Mbit/s, in ca. 2000 m Entfernung sind nur noch Werte erreichbar, die denen von ADSL entsprechen. Der Nachfolgestandard VDSL2 bietet eine Obergrenze von 100 Mbit/s an.

Alle hier genannten Varianten von DSL basieren auf der gleichen Technik. Welche letzten Endes zum Einsatz kommt, hängt zum einen von den Leitungseigenschaften ab und davon, welche Länge und welchen Querschnitt die Leitung bis zur nächsten Vermittlungsstelle hat. Ein weiterer Punkt betrifft die Verfügbarkeit eines DSLAM (DSL-Access-Multiplexer). Weiter hängt es von den Vertragsvereinbarungen ab, welche Übertragungsrate der Provider in welcher Richtung freischaltet, wie viele öffentliche IP-Adressen aus welchen Adressbereichen er vergibt und welche zusätzlichen Leistungen und Garantien vereinbart sind (etwa die garantierte Verfügbarkeit usw.). Die erforderliche Hardware (Router mit DSL- und LAN-Interfaces) wird meist vom Provider ohne weitere Kosten zur Verfügung gestellt.

10.4 UMTS

UMTS bedeutet Universal Mobile Telecommunications System. Es wird auch als Mobilfunk-Standard der dritten Generation (3G) bezeichnet und bietet Geschwindigkeiten von 384 kbit/s bis zu 14,4 Mbit/s (aktuell 7,2 Mbit/s) mit dessen Übertragungsverfahren HSDPA. Im Jahr 2000 wurden in Deutschland UMTS-Lizenzen für 98 Milliarden DM (fast 50 Milliarden Euro) versteigert.

Datenübertragung per Handy war bis dahin schon im GSM-Standard (Global System for Mobile Communications) möglich. Die Bandbreite im GSM-Standard beträgt maximal 14,4 kbit/s, was für einfache E-Mails und text-basierende Internetseiten ausreichte. Neue Techniken wie HSCSD (Standard für Hochgeschwindigkeitskommunikation in GSM-Netzen, 76,8 kbit/s) oder GPRS (General Packet Radio Service, 115,2 kbit/s) verbesserten die Übertragungsrate. Diese können sich jedoch im Vergleich zu UMTS (bis zu 14,4 Mbit/s) nur dort durchsetzen, wo UMTS nicht verfügbar ist.

UMTS-Dienste

Im UMTS-Netz werden folgende Dienste angeboten:

- ✓ Information
 - ✓ Internet-Surfen
 - ✓ Interaktives Einkaufen
 - ✓ Online-Übersetzungen
 - ✓ Ortsbezogene Dienste (Wetterbericht, Verkehrsnachrichten etc.)
- ✓ Bildung
 - ✓ Virtuelle Schule
 - ✓ Online-Labor
 - ✓ Online-Bibliothek
 - ✓ Online-Wörterbuch
 - ✓ Training
- ✓ Unterhaltung
 - ✓ Audio on Demand (Musik-Downloads)
 - ✓ Spiele on Demand (LAN-Partys, Gameboy-Ersatz)
 - ✓ Handy-TV (DVB-H)
 - ✓ Videoclips
 - ✓ Virtuelle Führungen (Museen, Hotels, Kulturräume etc.)
- ✓ Kommunikationsdienste
 - ✓ Videotelefonie
 - ✓ Videokonferenz
 - ✓ Spracherkennungsdienste
 - ✓ Lokalisierung von Personen
 - ✓ E-Mail-Dienste
 - ✓ SMS-Dienste
- ✓ Dienste für die Geschäftswelt
 - ✓ Virtual Banking
 - ✓ Online bezahlen
 - ✓ Universelle SIM- und Kreditkarte
 - ✓ Überwachungsdienste (Überwachung mit WebCams)

Übertragungstechnik

UMTS verwendet das Wideband CDMA-Verfahren (Code Division Multiple Access), das sich stark vom bisher eingesetzten Zeitmultiplex-Verfahren bei GSM unterscheidet. Beim Wideband CDMA (W-CDMA) werden alle Daten innerhalb einer Funkzelle auf derselben Frequenz und zum gleichen Zeitpunkt übertragen. Zur Unterscheidung werden die Daten mit Codes versehen, die von Sender und Empfänger bestimmt werden. Ähnlich wie bei GPRS teilen sich die Teilnehmer die insgesamt zur Verfügung stehende Bandbreite einer Funkzelle.

Vorteile des Verfahrens:

- ✓ Hohe Übertragungsgeschwindigkeit (bis zu 14,4 Mbit/s)
- ✓ Multimediafähig
- ✓ Der Teilnehmer ist ständig online. Informationen sind dadurch jederzeit verfügbar und müssen nicht erst abgerufen werden.

Nachteile des Verfahrens:

- ✓ Sinkende Übertragungsrate bei zunehmendem Abstand zum Sendemast
- ✓ Sinkende Übertragungsrate bei Bewegung des Handys (z. B. im Auto oder Zug)

Bandbreite

Der entscheidende Unterschied zwischen der GSM- und der UMTS-Technologie liegt in der Bandbreite der genutzten Frequenzen. Im D- und E-Netz liegt diese bei 200 kHz. Die Bandbreite bei UMTS beträgt 5 MHz, also das 25fache. Nur so kann eine hohe Übertragungsrate ermöglicht werden.

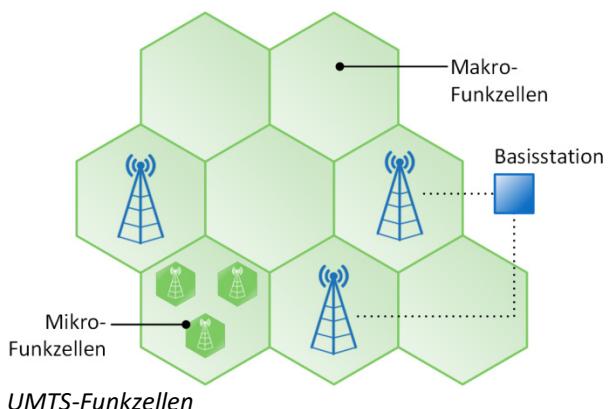
Zellenstruktur

Die Zellenstruktur hat sich bei UMTS gegenüber GSM grundlegend geändert. In GSM-Netzen haben alle Zellen die gleiche Größe, während im UMTS-Netz die Zellengröße variiert.

Es gibt folgende Zellentypen:

- | | |
|---|--|
| <ul style="list-style-type: none"> ✓ Picozelle ✓ Mikrozelle | <ul style="list-style-type: none"> ✓ Makrozelle ✓ Hyper- oder Umbrella-Zelle (Weltzelle) |
|---|--|

Die Picozelle ist die kleinste Zelle im UMTS-System und hat einen Durchmesser von etwa 100 Metern. Sie eignet sich für die Versorgung von Messen, Flughäfen oder großen Bürogebäuden. Die nächstgrößere Zelle ist die Mikrozelle. Sie hat einen Durchmesser von mehreren Kilometern und eignet sich für die Versorgung von Städten oder Stadtteilen. Die Makrozellen werden mit einem Durchmesser von etwa 20 Kilometern überwiegend für Vororte eingesetzt. Die größten Zellen werden als Hyperzellen bezeichnet und versorgen einen Bereich von mehreren Hundert Kilometern.



Bekannte Probleme mit UMTS

Die maximale Übertragungsrate von 14,4 Mbit/s wird von einigen Providern angeboten. Diese kann nur bei vollem Netzausbau erreicht werden, wenn sich der Teilnehmer nicht bewegt und sich nicht in einem Gebäude befindet. Bei einer Geschwindigkeit von 120 km/h auf der Autobahn beträgt die Übertragungsrate nur noch ein Fünftel. Bei Tempo 300 km/h im ICE sinkt die Übertragungsrate noch weiter ab. Im Juli 2010 waren in Deutschland bereits 70 % aller **Standorte**, an denen ein Mobilfunknetz verfügbar ist, mit UMTS oder HSDPA abgedeckt. Das bedeutet jedoch nicht, dass somit auch 70 % der Fläche Deutschlands abgedeckt waren. Versorgt sind oftmals nur die Ballungsgebiete. Aus diesem Grund wurden Multiband-Handys entwickelt, die sowohl im UMTS- als auch im GSM-Netz betrieben werden können.

Den aktuellen Stand der Netzabdeckung finden Sie jeweils auf den Webseiten der Provider, z. B.:

- ✓ <https://www.vodafone.de/hilfe/netzabdeckung.html>
- ✓ <https://www.telekom.de/start/netzausbau>

10.5 LTE

LTE bzw. Long Term Evolution ist der Mobilfunkstandard der vierten Generation (4G). Besonders im ländlichen Raum, der noch relativ wenig mit DSL erschlossen ist, verbessert LTE die Versorgung mit schnellen Internet-zugängen. LTE verwendet die **OFDM**-Technik (Orthogonal Frequency-Division Multiplexing). Die Datenübertragung kann damit einfach auf den Zustand eines Übertragungskanals angepasst werden. Frequenz-Lizenzen hierfür wurden 2010 für insgesamt 4,4 Milliarden Euro versteigert. Seit 2011 befindet es sich im Einsatz. Wie bei UMTS sind die Teilnehmer mit LTE permanent online.

Aktuell sind Datenübertragungsraten von <300 Mbit/s im Downlink und <70Mbit/s im Uplink möglich. Durch die garantierte Bandbreite, eine geringe Latenzzeit (<10 ms) und QoS (Quality of Service) ist es für die Protokolle des Internets bestens geeignet. Daneben nutzen Mobilfunkanbieter primär den 4G-Standard, da ihnen hierdurch ein kostengünstiger Migrationspfad von UMTS nach LTE ermöglicht wird.

Die Weiterentwicklung (LTE-Advanced) ermöglicht Downlink-Raten von <1000 Mbit/s und Uplink-Datenraten von <500 Mbit/s bei der Zuweisung von verschiedenen Bandbreiten und der CoMP/MIMO-Technik.

10.6 WiMAX

Worldwide Interoperability for Microwave Access (WiMAX) nutzt die Frequenzbänder von 2–66 GHz und wurde parallel zum WLAN-Standard (IEEE 802.11) entwickelt. Der dazu verabschiedete Standard (IEEE 802.16) beschreibt eine drahtlose Breitbandtechnik für ein Wireless Metropolitan Area Network, kurz WMAN. Der Standard ist sowohl für fest installierte Stationen (IEEE 802.16-2004, WiMAX fixed) als auch mobile Geräte (IEEE 802.16e-2005, WiMAX Mobile) konzipiert. Mit fest installierten Systemen sind Übertragungsraten bis 134 Mbit/s und bei mobilen Geräten bis zu 15 Mbit/s erzielbar. Mit dem Standard IEEE 802.16m (WiMAX 2) werden Geschwindigkeiten von <1000 Mbit/s erreicht.

In einem WiMAX-Netz sind Verbindungen über eine Distanz bis zu 50 Kilometern möglich. Da sich die Datenübertragungsrate jedoch mit zunehmender Entfernung verringert, bleiben in der Praxis weniger Kilometer. WiMAX hat seine eindeutigen Vorteile bei der flächendeckenden Umsetzung außerhalb von Ballungsgebieten, während LTE bei bandbreitenintensiven Traffic punkten kann. Ob sich eher LTE oder WiMAX durchsetzt, hat sich zugunsten von LTE entwickelt.

10.7 Weitere Übertragungsprotokolle

Metro-Ethernet

Metro-Ethernet ist eine Technologie, die seitens des Providers oder im Verbund von Providern Endkunden zur Verfügung gestellt wird. Sie hat im Normalfall nur eine lokale bzw. regionale Ausbreitung (Metropolitan Area Network). Der Kunde kann hiermit Standorte so verbinden, als wären sie im eigenen LAN. Die Latenzzeit ist jedoch mindestens um den Faktor 2 – 4 größer. Metro-Ethernet ermöglicht eine skalierbare Verfügbarkeit der Bandbreite von 1 Gbit/s – 10 Gbit/s und mehr. Im Folgenden werden Weitverkehrsprotokolle skizziert, die teilweise nur noch vereinzelt zum Einsatz kommen.

HDLC

Das High Level Data Link Control Protocol gehört zu den ältesten OSI-Protokollen. Es ist paketorientiert auf Schicht 2 angesiedelt und verfügt über einen eigenen Fehlerkorrekturmekanismus.

X.25

X.25 ist ein Standard für Paketvermittlung, der 1974 von der damaligen CCITT (heute ITU) als Empfehlung eingeführt wurde und sich in WANs sehr weit verbreitet hatte, mittlerweile aber als veraltet betrachtet werden kann. Die letzte Fassung stammt aus dem Jahr 1993. Es existiert ein weltweit gut ausgebautes Datennetz mit eigenen Vermittlungsknoten. Der Einsatz des X.25-Protokolls ist in Deutschland eher selten anzutreffen.

ATM

Asynchronous Transfer Mode ist eine verbindungsorientierte Switching-Technologie für hohe Bandbreiten. Die Normung wird nicht alleine von der ITU vorgenommen, sondern maßgeblich vom ATM-Forum. So wurde ATM von der ITU-T z. B. als Standard für B-ISDN vorgeschlagen. ATM hat heute nur noch eine Bedeutung in Weitverkehrsnetzen und für die Auskopplung des DSL-Signals am **DSLAM** (Digital Subscriber Line Access Multiplexer).

SMDS/CBDS

Switched Multimegabit Data Service wurde von Bellcore (Bell Communication Research, USA) in den 80er-Jahren für den Breitband-Datenverkehr über das Telefonnetz entwickelt. In Europa wird diese Technologie unter dem Namen CBDS (Connectionless Broadband Data Service) eingesetzt. Allerdings sind die Unterschiede marginal.

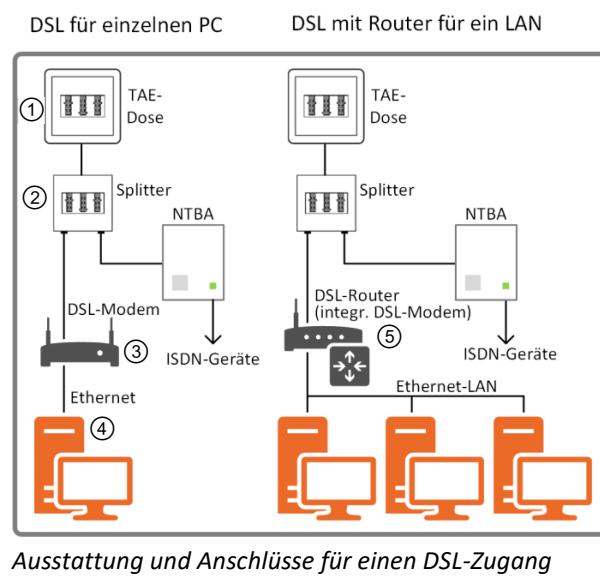
SMDS unterstützt nur verbindungslose Datenübertragung und findet vor allem in der Kopplung von LANs über große Entfernung und mit hoher Geschwindigkeit seinen Einsatz. Mit entsprechenden Routern kann SMDS zur völlig transparenten LAN-Kopplung eingesetzt werden.

10.8 Szenario: Internetzugang einrichten

DSL-Anschluss

DSL kann sowohl für die Anbindung eines einzelnen Computers als auch für größere Netzwerke zur Verfügung gestellt werden. Dazu ist grundsätzlich folgende Ausstattung erforderlich:

- ✓ ein **Telefonanschluss** ①, ISDN oder eine analoge Leitung, die zusätzlich zur Telefonie für den DSL-Einsatz genutzt wird
- ✓ ein **Splitter** ② (fachsprachlich auch BBAE, Breitbandanschlusseinheit, genannt) zur Trennung der Signale von DSL von den analogen oder ISDN-Diensten. Er trennt die eingehenden Signale von der Amtsleitung lediglich in Signale über und unter 138 kHz auf und ermöglicht so den parallelen Betrieb von Telefonie und DSL. Der Splitter ist im DSL-Modem integriert.
- ✓ ein **DSL-Modem** ③ (NTBBA, Network Termination Broadband Access), das Ethernet-Frames für eine Übertragung auf die DSL-Strecke über den Splitter moduliert
- ✓ eine Ethernet-**Netzwerkarte** ④ und Treiber für das **PPPoE-Protokoll** (Point to Point Protocol over Ethernet) für den Anschluss eines PCs



Ausstattung und Anschlüsse für einen DSL-Zugang

Aktuelle Router ⑤ beinhalten neben den Interfaces fürs LAN (Ethernet, WLAN) und WAN (DSL/PPPoE) den Splitter, die Modem-Funktionalität und weitere Features. Sie schicken die von Clients im LAN ausgehenden Anfragen über die Telefonleitung ins Internet. Ein Router bzw. das integrierte DSL-Modem nutzt dabei das PPPoE-Protokoll, um sich mit dem Benutzernamen und zugehörigem Passwort beim ISP (Internet Service Provider) zu autorisieren und so den Zugang zum Internet zu ermöglichen.

Der Router ist so konfiguriert, dass er bei Bedarf eine Internetverbindung über DSL herstellt. Die Leitung wird ggf. nach 24 Stunden seitens des Providers kurzzeitig zwangsetrennt, worauf sich der Router wieder mit dem Internet verbindet.

Was aber passiert bei einem Ausfall der DSL-Verbindung? Hier bieten einige Hersteller eine Redundanz über LTE-Modem (Fallback/Backup) an. In den Backup-Einstellungen des Routers wird dabei die DSL-Verbindung als primäre Internetverbindung und die LTE-Mobilfunkverbindung als sekundäre Internetverbindung genutzt.

Der Router baut zuerst eine Internetverbindung über die DSL-Verbindung auf. Kommt es nun zu einer DSL-Störung, baut der Router die Internetverbindung automatisch über die LTE-Mobilfunkverbindung auf. Sobald die DSL-Störung behoben ist, verwendet der Router automatisch wieder die ursprüngliche DSL-Verbindung.

Internetzugang mittels DSL-Router

Provider bieten DSL-Verträge an, zu denen ein DSL-Router mit/ohne weitere Kosten bereitgestellt wird, der eine entsprechende Eingabemaske bzw. ein Feld für die Eingabe eines Start-Codes dieses Providers anbietet. Bei diesem Router müssen Sie nur noch Ihre Zugangsdaten in diese Maske bzw. den mitgelieferten Code in dem Feld eintragen und im Router speichern. Die Sicherheitseinstellungen sind dabei meist vorkonfiguriert. Sie sollten dennoch diese Einstellungen überprüfen und soweit möglich anpassen.

Seit August 2016 ist der Zwang zur Nutzung eines Routers des Providers aufgehoben. In diesem Fall müssen Sie selbst die Wahl der geeigneten Hardware übernehmen. Das bedeutet auch, dass Sie sich über die Leistungsparameter, die genutzten Protokolle und die Schnittstellen gründlich informieren sollten. Vor dem Kauf müssen Sie mit Ihrem Provider in Kontakt treten, um die Zugangsdaten für die Internetnutzung zu erhalten. Dies sind:

- ✓ Benutzername und Kennwort für den Internetzugang
- ✓ RETCS-Name und Password für die Nutzung der VoIP-Telefone

Erst wenn Sie **alle** Informationen erhalten haben, steht der Nutzung eines „Fremd-Routers“ (Router, der nicht von einem Provider vorgeschrieben wurde) nichts mehr im Wege. Jedoch kann es im Einzelfall dazu kommen, dass bei Fehlfunktionen des Routers der technische Support des Providers Ihnen keine Unterstützung geben kann oder darf.

Ein Router mit integriertem DSL-Modem verfügt meist über mehrere Schnittstellen. Eine Schnittstelle verbindet ihn mit dem WAN (DSL), die anderen Schnittstellen stellen die Verbindungen zum LAN/WLAN her. Die DSL-Schnittstelle wird direkt mit der TAE-Dose verbunden. Der Anschluss eines Telefons auf dieser Leitung ist dann nicht möglich. Ihre Endgeräte werden an der LAN/WLAN-Schnittstelle angeschlossen:

- ▶ Stellen Sie den Router gemäß Bedienungsanleitung auf. Stellen Sie die erforderlichen Verbindungen mit den beiliegenden Patchkabeln her und schalten Sie ihn ein.
- ▶ Überprüfen Sie, ob alle Kontroll-LEDs die einwandfreie Funktion des Gerätes und des DSL-Anschlusses signalisieren.

Es gibt viele Router am Markt. Eine große Verbreitung in Deutschland haben Geräte der Berliner Firma AVM, bekannt unter dem Namen Fritz!Box. Deshalb bezieht sich das folgende Beispiel auf eine Version dieser Geräte.

Beachten Sie, dass die folgenden Einstellungen Beispiele darstellen, die nicht alle Router mit DSL-Schnittstelle anbieten bzw. die in der Konfiguration Ihres Routers in anderer Form erscheinen können.

Netzwerkvoraussetzung für den DSL-Router

Der Router ist in seinen Werkseinstellungen mit einer IP-Adresse vorbelegt. In dem hier verwendeten Beispiel sind die Werkseinstellungen wie folgt:

IP-Adresse	192.168.178.1
Subnetzmaske	255.255.255.0
DHCP-Server	aktiviert

Um den Router konfigurieren zu können, muss sich der PC, der zur Konfiguration benutzt wird, im gleichen Subnetz wie der Router befinden. Die IP-Adresse des Routers darf nicht bereits vergeben sein. Auch können Probleme auftreten, wenn bereits ein anderer DHCP-Server im Netzwerk aktiv ist. In diesem Fall ist zu empfehlen, den Router getrennt vom vorhandenen Netz zu konfigurieren.



Sind diese Voraussetzungen erfüllt, können Sie sich mittels Web-Browser (wie Internet Explorer, Firefox etc.) mit dem Router verbinden und mit der Konfiguration beginnen. Die folgende Beispielkonfiguration wurde mit einer AVM Fritz!Box 7490 durchgeführt.

Konfiguration mithilfe eines Web-Browsers

- Öffnen Sie Ihren Web-Browser und geben Sie im Feld die URL *fritz.box* ein. Der Startbildschirm der Fritz!Box wird angezeigt. Geben Sie hier die vorgegebenen Zugangsdaten ein.

The screenshot shows the Fritz!Box 7490 User Interface (UI) with the following details:

- Header:** FRITZ!Box 7490 (UI), FRITZ!NAS, MyFRITZ!, Help icon.
- Left Sidebar:** Übersicht, Internet, Telefonie, Heimnetz, WLAN, DECT, Diagnose, System, Assistenten.
- Central Content:**
 - Übersicht:** FRITZ!Box-Name: AVM7490, Aktueller Energieverbrauch: 40%, FRITZOS: 06.60.
 - Verbindungen:** Internet (IPv4, verbunden seit 19.11.2016, 03:31 Uhr, Anbieter: 1&1 Internet, IP-Adresse: 79.212.12.2), Internet (IPv6, verbunden seit 19.11.2016, 03:31 Uhr, Anbieter: 1&1 Internet, IPv6-Adresse: 2003: 6:37ff:f658: e49: 9ff: scb:b), Telefonie (6 Rufnummern aktiv), Online-Speicheverbunden.
 - Anschlüsse:** DSL (verbunden, 51,4 Mbit/s), LAN (verbunden (LAN 1, LAN 4)), WLAN (an, Funknetz 2,4 GHz: Mali), WLAN (an, Funknetz 5 GHz: Mali), DECT (an, 2 Schnurlosetelefone angemeldet), USB (verbunden, 1 Speicher (entfernen)).
 - Anrufe heute: 0** (list of calls with timestamps and duration).
 - Anrufbeantworter heute: 0** (Anrufbeantworter deaktiviert).
 - Heimnetz aktiv: 7** (BRW40B89AC8498D, WLAN - 2,4 GHz).
 - Komfortfunktionen:** Telefonbuch (2 Kontakte in Telefonbuch).
- Bottom:** Ansicht: Erweitert, Inhalt, Handbuch, Tipps & Tricks, Newsletter, avm.de.

Konfigurierte Übersichtsanzeige einer AVM Fritz!Box

- Klicken Sie auf *Internet* (unter *Verbindungsinformationen*) und danach im darunter erscheinenden Menü auf *Zugangsdaten*.

The screenshot shows the Fritz!Box 7490 User Interface (UI) with the following details:

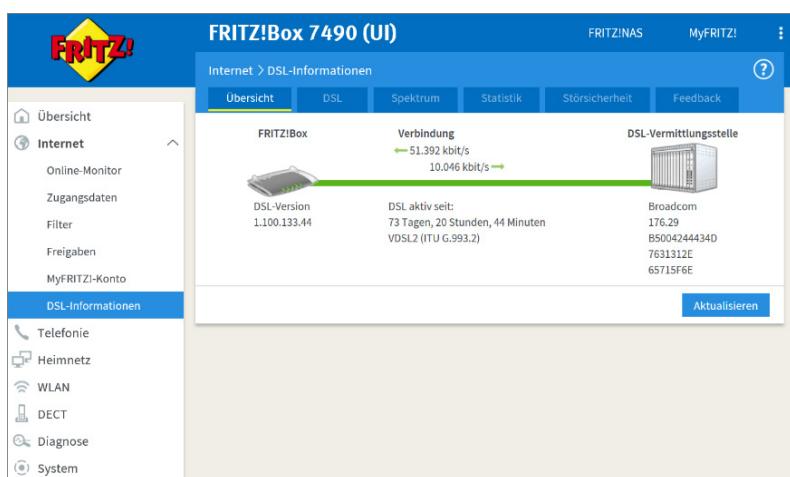
- Header:** FRITZ!Box 7490 (UI), FRITZ!NAS, MyFRITZ!, Help icon.
- Left Sidebar:** Übersicht, Internet (Online-Monitor), Zugangsdaten (selected), Filter, Freigaben, MyFRITZI-Konto, DSL-Informationen, Telefonie, Heimnetz, WLAN, DECT, Diagnose, System, Assistenten.
- Central Content:**
 - Internet > Zugangsdaten:** Internetzugang tab selected. Sub-sections include Internetanbieter (Wählen Sie Ihren Internetanbieter aus: 1&1 Internet) and Zugangsdaten (Geben Sie die Zugangsdaten ein, die Sie von Ihrem Internetanbieter bekommen haben. Internetzugangs-Kennung: 1und1/ 9139-709, Internetzugangs-Passwort: ****).
 - Verbindungseinstellungen:** (3) (Die Verbindungseinstellungen sind bereits auf die am häufigsten verwendeten Werte eingestellt. Bei Bedarf können Sie diese Werte verändern. Verbindungseinstellungen ändern). Includes a checkbox for "Internetzugang nach dem 'Übernehmen' prüfen".

Anschlusskonfiguration, Internetanbieter und Zugangsdaten

- ✓ Sie können nun die Anschlusskonfiguration des DSL-Zugangs durchführen. Durch die Wahl Ihres Internetproviders ① wird eine Voreinstellung des Routers vorgenommen.
- ✓ Im Feld darunter ② müssen Sie die postalisch erhaltenen Zugangsdaten eintragen, damit wird Ihre Verbindung gegenüber dem Provider autorisiert.
- ✓ Zusätzliche Verbindungseinstellungen können Sie im darunterliegenden Feld ③ auswählen.

Überprüfen der DSL-Verbindung

- Wechseln Sie in das Menü *Internet > DSL-Informationen*



Diese Übersicht liefert Ihnen in den einzelnen Menüpunkten Detailinformationen über den Verbindungsstatus der DSL-Verbindung, die Geschwindigkeit (Up- und Downstream), Statistiken und weitere Einstellungen des Routers.

Ändern des Kennwortes des Routers

Um die Sicherheit und Integrität Ihres Netzwerks zu gewährleisten, sollten Sie den Zugriff auf den Router mit einer regelmäßigen Änderung des Kennwortes schützen.

- Klicken Sie auf den Menüpunkt *System*.
- Wählen Sie *FRITZ!Box-Benutzer*.
- Wählen Sie danach den Reiter *Anmeldung im Heimnetz* aus.

Dort können Sie über den Button *Anmeldung mit dem FRITZ!-BOX-Kennwort* im angezeigten Feld den Login-Namen ändern und anschließend mit *Übernehmen* aktivieren.

Ändern der IP-Adresse

Das Ändern der IP-Adresse des Routers ist sinnvoll, wenn Sie das Gerät in eine bereits vorhandene Netzwerkstruktur einbinden wollen, in der die werkseitig konfigurierte Adresse bereits verwendet wird oder wenn die IP-Adresse nicht zur verwendeten IP Struktur passt. Baugleiche Geräte verwenden in den Werkseinstellungen die gleiche IP-Adresse, was ebenfalls eine Änderung notwendig machen kann.

- Wechseln Sie in das Menü *Heimnetz - Heimnetzwerkübersicht - Netzwerkeinstellungen - IPv4-Adressen*.
- Im Feld *IPv4-Adresse* können Sie eine neue Adresse für diesen Router setzen ①.
- Tragen Sie im Feld *Subnetzmaske* den entsprechenden Wert ein, der vom lokalen Netz genutzt wird, dem der Router angehören soll.
- Wollen Sie den Router als *DHCP-Server* nutzen, aktivieren Sie das Kontrollfeld ② und vergeben Sie den IP-Adressbereich, den die angeschlossenen DHCP-Clients nutzen sollen.

IPv4-Einstellungen des Routers

Fehlersuche am Router

Problem	Ursache	Behebung
Der Router wird vom Client nicht gefunden.	Der Client ist nicht auf DHCP eingestellt und hat eine statische Adresse, die nicht im Adressbereich des Routers liegt. Ihr PC oder der DSL-Router haben keine Netzwerkverbindung.	Überprüfen Sie die Netzwerkeinstellungen und Netzwerkverbindungen.
Die Internetverbindung kann über DSL nicht aufgebaut werden.	Fehler in den Zugangsdaten DSL-Anschluss gestört Fehlerhafte Verbindung über DSL-Schnittstelle Router-Betriebssystem abgestürzt	Überprüfen Sie bzw. wiederholen Sie die Eingabe der Zugangsdaten. Überprüfen Sie die LEDs am DSL-Router. „DSL“ muss dauerhaft leuchten. Eventuell liegt eine Störung beim Provider vor. Führen Sie einen Hardware-Reset des Routers durch (im Konfigurationsmenü: SYSTEM - ZURÜCKSETZEN). Achtung: Alle Konfigurationsdaten werden gelöscht.

ISDN-Anschluss

Wenn noch ein ISDN-Anschluss vorhanden ist, kann auch eine ISDN-Karte oder ein Router mit So-Interface eingesetzt werden. Hier ist weder ein Modulator noch ein Demodulator nötig, da die Übertragung digital erfolgt. Die Übertragungsgeschwindigkeiten bei einem Basisanschluss (BRI) liegen bei 64 kbit/s bzw. 128 kbit/s, wenn beide Kanäle gebündelt werden, sowohl beim Upstream als auch beim Downstream. ISDN-Karten gibt es als PCI-(PC) oder PCMCIA-Variante (Laptop), letztere gab es auch inkl. integriertem Analog-Modem. Die Installation unter Windows gestaltet sich dank beiliegender Treiber-CD einfach und auch unter den großen Linux-Distributionen sollte dies kein Problem sein. Vorreiter auf diesem Gebiet war die Berliner Firma AVM (<http://www.avm.de/>), für ISDN-Karten hat sich der Begriff FRITZ!-Karte eingebürgert.

Router mit ISDN-Interface können, je nach Ausstattung und mit Bündelung von Kanälen, auch höhere Übertragungsraten zur Verfügung stellen, wie z. B. ein Router an einem ISDN-Primärmultiplex-Anschluss (PRI).

Durch die in den letzten Jahren schnelle Verbreitung bezahlbarer DSL- und UMTS/LTE-Lösungen hat die Bedeutung der Datenübertragung durch Analog-Modems bzw. ISDN-Technik stark abgenommen. In bestimmten Anwendungsfällen (z. B. Fernsteuerung in Industrieanlagen) kann ein Einsatz dieser Technik aber durchaus noch sinnvoll sein.

Mobilfunk-Modem

Die Modem-Palette reicht von Geräten, die über die USB-Schnittstelle eines Computers angeschlossen werden bis zu mobilen Hotspots. Hierzu nutzen sie die Mobilfunkstandards GMS, UMTS und LTE. In etlichen Geräten wie Smartphones, Notebooks, Tablets etc. ist ein Mobilfunk-Modem oft bereits fest eingebaut. Das dadurch entstandene Mobilfunknetz bezeichnet man auch als WWAN (Wireless Wide Area Network). Eine Verbindung zum Internet ist mit UMTS/LTE-Modems, die eine Vernetzung über den UMTS/LTE-Standard bieten, relativ einfach einzurichten. Sie werden hauptsächlich als USB-Stick (Surf-Stick) vertrieben und ermöglichen mit einer eingelegten SIM-Karte über das integrierte Modem eine direkte Verbindung ins Internet. Ist keine Verbindung per UMTS/LTE möglich, verwenden sie stattdessen ein langsameres Übertragungsverfahren wie EDGE (Enhanced Data rates for GSM Evolution) und im schlimmsten Fall nur GSM (Global System for Mobile Communications). Mit einem derartigen UMTS/LTE-Modem erhalten Sie jedoch nur für den eigenen Rechner einen Zugang zum Internet. Durch die Installation eines Tools (z. B. Connectify, www.connectify.me) ist es jedoch möglich, den eigenen Rechner als mobilen Hotspot im Netz einzurichten.

Viele Router können mit einem derartigen USB-Stick automatisch eine Fallback-Lösung anbieten, wenn die DSL-Leitung gestört ist. Nicht alle Router beherrschen aber automatisches Fallback bzw. Fallforward, also den automatischen Übergang zurück auf die DSL-Leitung, wenn diese wieder benutzbar ist. Die Einrichtung erfolgt normalerweise unter Windows mit der Software, die direkt in dem Surf-Stick in einem Speicherbereich enthalten ist und auf die Windows nach dem Einsticken zugreifen kann. Falls die mitgelieferten Programme nicht mehr zu der verwendeten Windows-Version passen, müssen Sie aus dem Internet ein passendes Update herunterladen.



Startfenster eines USB-Sticks

Unter Linux bietet der NetworkManager eine relativ einfache Konfiguration an. Die erforderlichen Zugangsdaten erfragen Sie am besten bei Ihrem Provider. Für die wichtigsten Netzbetreiber finden Sie diese auch auf der Seite <https://www.teltarif.de/mobilfunk/internet/einrichtung.html>.



Der Kunde erhält mit Privatkundentarifen meist nur einen Zugang zum Internet über ein Netzwerk, das der Provider per Adressumsetzung (NAT/PAT) bereitstellt. Einige Funktionen (wie Port-Weiterleitungen, Fernkonfiguration etc.) sind dann ggf. nicht möglich. Auch ist die Latenzzeit erheblich höher (mindestens 40 ms im Gegensatz zu typischen 20–30 ms bei DSL).

Sofern Sie ein Smartphone und einen Vertrag mit mobiler Datennutzung besitzen, können Sie das Handy auch als mobilen Hotspot für das Internet nutzen. Mittels Tetherings (engl: anbinden) lassen sich über USB, Bluetooth oder WLAN, Endsysteme mit dem Smartphone verbinden. Das Smartphone baut seinerseits eine Verbindung zum Provider auf. Dazu sind am Beispiel von Android 6.0.1 folgende Schritte erforderlich:

- ▶ Öffnen Sie auf Ihrem Smartphone das Icon *Einstellungen*.
- ▶ Wechseln Sie in den Menüpunkt *Netzwerkverbindungen* und dann *Tethering und Mobile Hotspot* und wählen dort die Verbindungsart WLAN, USB oder Bluetooth aus.
 - ✓ Nachdem Sie z. B. WLAN (Mobile Hotspot) aktiviert haben, werden die WLAN-Parameter (eindeutige SSID, Verschlüsselung und Passwort) festgelegt.
 - ✓ Im Anschluss müssen Sie nur noch Ihr Endsystem (Notebook, PC, Tablet, ...) in den Netzwerk-einstellungen mit dem WLAN des Smartphones verbinden und das dazugehörige Passwort angeben. Auf dem Smartphone wird dann das verbundene Gerät angezeigt.

Um eine stabile Datenübertragungsrate zu erzielen, sollten Sie zusätzlich auf dem Handy unter dem Menüpunkt *Einstellungen - WLAN* den automatischen Wechsel zwischen dem 2,4-GHz- und 5-GHz-Band aktivieren.

11 Weitere Entwicklungen

In diesem Kapitel erfahren Sie

- ✓ wie die Ethernet-Technologie definiert ist
- ✓ was Power over Ethernet bedeutet
- ✓ wie Gigabit-Ethernet definiert wird
- ✓ wie ein Gigabit Interface Converter (GBIC) Modul aufgebaut ist
- ✓ welche neuen Mobilfunkstandards existieren

Voraussetzungen

- ✓ Wissen über das ISO/OSI-Schichtenmodell
- ✓ Wissen über den Aufbau von Glasfaserkabeln

11.1 Ethernet-Technologie

Historische Übersicht

Das Grundprinzip von Ethernet entstand durch ein Projekt an der University of Hawaii in den frühen 70er-Jahren. Anhand des bodengestützten Rundfunksystems ALOHA wurden neue Übertragungsprinzipien entwickelt, die später auch für Ethernet zentrale Bedeutung erlangten: „Das Management von Kollisionen und die Übertragung von Datenpaketen (Frames)“. Hier verständigten sich mehrere Stationen über einen gemeinsamen Kanal.

Im Jahr 1972 begann Xerox mit dem Betrieb eines experimentellen Ethernet-Systems. Sieben Jahre später entwickelte die DIX-Gruppe (DEC, Intel und Xerox) eine standardfähige 10Mbit/s-Ethernet-Konfiguration. Diese wurde dann 1982 von der IEEE unter der Bezeichnung 802.3-Standard für 10Base5 veröffentlicht. Die weltweite Anerkennung des Ethernet-Standards erfolgte 1985. Etwa zwei Jahre später kamen die ersten Twisted-Pair-Produkte und Multiprotokoll-Router in Deutschland auf den Markt. Die Standardisierung von Ethernet auf Twisted-Pair-Kabel (10BaseT) erfolgte 1991. Nur ein Jahr später wurde der 10BaseF-Standard für Ethernet über Glasfaserkabel veröffentlicht. Für Ethernet sind die Abschnitte 802.1, 802.2 und 802.3 von Bedeutung. In der Spezifikation nach 802.1 und 802.2 werden allgemeine Festlegungen der LAN-Architektur und des Logical Link Control (LLC) getroffen.

In der Spezifikation 802.3 wird u. a. der Zugriff auf das physikalische Medium (MAC-Schicht) für Busnetzwerke mit CSMA/CD (Carrier Sense Multiple Access with Collision Detection) definiert. Dieses Verfahren hat nur Bedeutung im Halbduplexbetrieb bis 100Base-T.

LLC-Teilschicht (Logical Link Control)

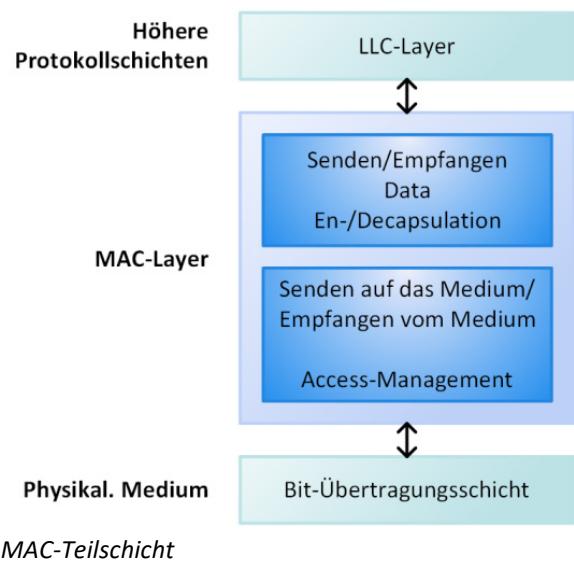
Diese Teilschicht verwaltet die Datenübermittlung und definiert die Verwendung von logischen Schnittpunkten, den SAPs (Service Access Points). Andere Computer können dann auf SAPs verweisen und Daten von der LLC-Teilschicht in die oberen OSI-Schichten übertragen. Sie findet nur noch bei älteren Protokollstacks Anwendung.

MAC-Teilschicht (Media Access Control)

Die MAC-Teilschicht kommuniziert direkt mit der Netzwerkkarte und ist verantwortlich für die fehlerfreie Datenübertragung zwischen Computer und Netzwerk. Sie bildet die Schnittstelle zwischen den höheren Protokollen und der physikalischen Bit-Übertragungsschicht.

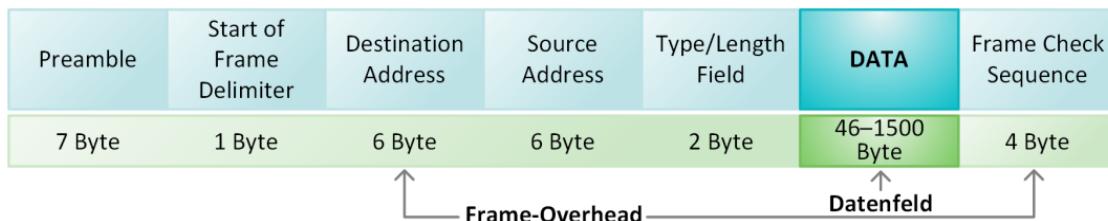
Ihre Dienste sind:

- ✓ die Aufbereitung von Frames zum Senden bzw. Empfangen
- ✓ Übergabe der Frames zum Senden auf das Medium mit Regelung des Zugriffs (Access Management)



Senden (Data Encapsulation)

- ✓ Von Layer 3 (Network Layer) wird ein Paket empfangen.
- ✓ Durch die Erzeugung eines Frames (Quell-MAC-Adresse, Ziel-MAC-Adresse, Typ- bzw. Längenfeld) wird ein vollwertiges Datenpaket aufgebaut.
- ✓ Dem Frame wird für die Verifizierung der Korrektheit eine Prüfsumme (Frame Check Sequence) hinzugefügt.
- ✓ Das Datenframe wird an das MAC-Sende-Modul übertragen, in dem es in einen seriellen Datenstrom zum Senden auf das Medium umgewandelt wird.



Frameaufbau

Empfangen (Data Decapsulation)

Bei Ethernet werden die Datenframes mittels einer Broadcast-MAC-Adresse (an alle Stationen im Layer-2-Netzwerk), einer Multicast-MAC-Adresse (an einige Stationen) oder mittels Unicast-MAC-Adresse (nur an eine Station) versendet. Anhand der Ziel-MAC-Adresse ermittelt jede Station selbst, ob ein empfangenes Datenpaket für sie bestimmt ist oder nicht. Nur korrekt adressierte Datenframes werden von der Netzwerkkarte weiterverarbeitet.

- ✓ Anhand der Prüfsumme wird das empfangene Datenpaket auf seine Korrektheit überprüft.
- ✓ Von einem gültigen Paket werden die Nutzdaten von den Frame-Daten gefiltert.
- ✓ Das Nutzdatenfeld muss zwischen 46 und 1500 Bytes lang sein. Weiterhin muss die Datenmenge ein Vielfaches von 8 Bit umfassen.
- ✓ Ein fehlerfreies Datenfeld (Maximum Transmission Unit [MTU] ist einwandfrei) wird an die darüberliegende Schicht (Layer 3) übergeben.

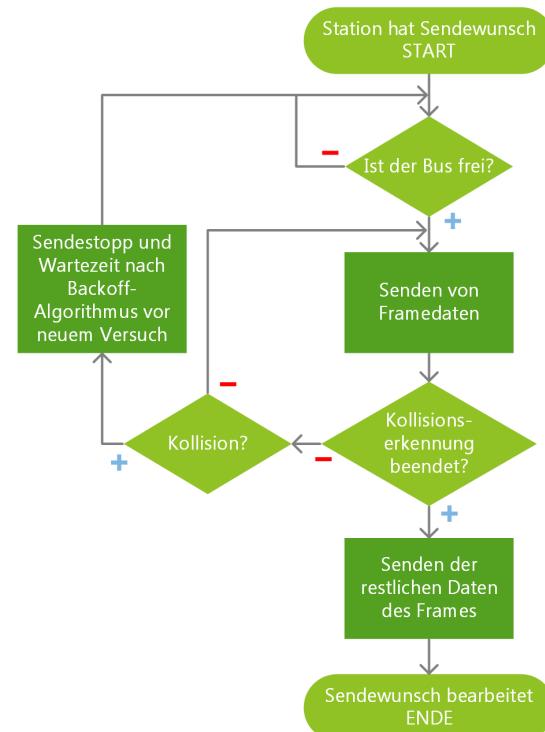
Datenframeübergabe an das Medium mit CSMA/CD

Das Ethernet bezeichnet man auch als eine shared-media- und shared-bandwidth-Architektur. Alle Stationen sind am selben Bus angeschlossen und nutzen gemeinsam die vorhandene Übertragungsbandbreite. Die Protokollschicht Medium Access Control (MAC) ist dafür verantwortlich, dass nicht mehrere Stationen gleichzeitig versuchen, Daten auf das Medium zu übertragen. Zu diesem Zweck wird von Ethernet das Zugriffsverfahren Carrier Sense Multiple Access with Collision Detection (CSMA/CD) eingesetzt.

Die Station überprüft, ob der Bus frei ist oder bereits von einer anderen Station benutzt wird (Carrier Sense). Falls auf dem Bus eine Datenübertragung erfolgt, findet kurz darauf eine erneute Überprüfung statt. Ist der Bus frei, beginnt die Station, ihre Daten zu senden. Trotzdem können Kollisionen durch gleichzeitiges Senden zweier Stationen nicht ausgeschlossen werden, beispielsweise in folgenden Fällen:

- ✓ Zwei Stationen möchten ungefähr zeitgleich eine Übertragung durchführen. Damit haben sie zur gleichen Zeit geprüft, ob der Bus frei ist. Da dies der Fall war, begannen auch beide zeitgleich zu senden, und es kommt zur Kollision.
- ✓ Die Stationen haben bezüglich des gesamten Busses eine große Entfernung zueinander. Aufgrund der Signallaufzeiten (bei den verwendeten Kupfermedien ca. 200.000 km/s) scheint der Bus frei zu sein. In Wirklichkeit hat jedoch am anderen Busende eine Station bereits begonnen, Daten zu senden.

In solchen Fällen senden mehrere Stationen auf dem gemeinsamen Übertragungsmedium (Multiple Access) und es kommt zu Kollisionen. Die einzelnen Stationen müssen Kollisionen entdecken. Daher überprüfen sie regelmäßig ihre eigene Sendung. Falls Kollisionen auftreten, wird der Sendevorgang sofort abgebrochen (Collision Detection). Nach einer bestimmten Wartezeit versucht die Station, ihre Daten erneut zu versenden.



Programmablauf beim CSMA/CD-Verfahren

Der Mechanismus zur Kollisionserkennung wird nicht während der ganzen Übertragungszeit angewandt. Bei 10- bzw. 100-Mbit/s-Netzen wird diese Überprüfung nur für die Übertragung der ersten 576 Bits durchgeführt. Es wird hier von 576 Bitzeiten gesprochen. Dieser Wert berechnet sich aus den kleinstmöglichen Frames von 64 Byte = 512 Bit plus einer Sperrzeit für die Kollisionserkennung. Deshalb wird die minimale Framegröße auf 512 Byte (Carrier Extentions) erhöht. Dadurch wird sichergestellt, dass die Erkennung von Kollisionen abwärtskompatibel zum CSMA/CD-Standard bleibt. Nach der vorgeschriebenen Kollisionserkennung kann die Station die verbliebenen Framedaten ohne weitere Überprüfungen versenden. Alle Stationen im Netz haben jetzt erkannt, dass der Bus belegt ist. Ist dies nicht der Fall, weil ...

- ✓ etwa die maximale Ausdehnung des Busses zu groß ist und/oder
- ✓ über Repeater/Hubs zu viele Netzsegmente gekoppelt wurden,

dann kommt es trotzdem zu Kollisionen, den sogenannten Late Collisions. Diese Kollisionen werden dann von der Sendestation nicht mehr erkannt und können nur von höheren Protokollebenen (z. B. Schicht 4 eines verbindungsorientierten Protokolls) korrigiert werden. Das CSMA/CD-Verfahren soll hier nur zur Veranschaulichung des Ethernet-Protokolls dienen. Es wird jedoch nur bei Ethernet und Fast-Ethernet im Halbduplexbetrieb angewendet.

11.2 PoE – Power over Ethernet

IEEE 802.3af/at/bt

Der Standard IEEE 802.3af bezeichnet ein Verfahren, mit dem es möglich ist, Endgeräte in einem Netzwerk mit Strom zu versorgen. Bisher wurden die einzelnen Endgeräte über das herkömmliche 230-Volt-Netz gespeist. Dies erfolgte entweder direkt oder über externe Steckernetzteile. Nachteil dieser Art der Stromversorgung ist, dass hierfür immer eine entsprechende 230-Volt-Steckdose zum Anschluss der Geräte erforderlich ist. Bei Power over Ethernet ist dies nicht mehr erforderlich. Die Speisung erfolgt über das achtadrige Netzwerkkabel vom Datenschränk zur RJ-45-Anschlussdose. Gerade an Orten, die schwer zugänglich sind oder über keine 230-Volt-Steckdose verfügen, ist der Einsatz von Power over Ethernet bestens geeignet.

Da der Leiterquerschnitt der bestehenden Netzwerkabnabel jedoch nicht für hohe Ströme ausgelegt ist, wird im Standard 802.3af geregelt, wie viel Leistung über die entsprechenden Adern bezogen werden kann. Außerdem regelt der Standard auch den Schutz von älteren Geräten, welche diese Technik noch nicht unterstützen. Der maximale Strom, der über ein Twisted-Pair-Kabel fließen kann, liegt bei etwa 350 mA. Die Spannung, mit der die angeschlossenen Netzgeräte versorgt werden, liegt zwischen 44 und 57 Volt. Der Standard IEEE 802.3at (PoE Plus) definiert Leistungsentnahmen bis 30 Watt. Die auf dem Markt befindlichen PoE-Lösungen sind bis zum Gigabit-Ethernet-Standard verfügbar. Außerhalb der Spezifizierung werden auch Ultra-PoE und Mega-PoE angeboten, welche eine Leistungsabgabe bis 80 W bzw. 95 W aufweisen.

PoE-Bezeichnung	Standard	Nutzbare Leistung
PoE	IEEE 802.3af	12,95 W
PoE+	IEEE 802.3at	21,90 W
PoE++	IEEE 802.3bt	70 bis 100 W

Unterschiede der Spannungsübertragung

Die Übertragung der eingespeisten Energie für Endgeräte verwendet zwei unterschiedliche Varianten:

- ✓ Speisung auf Adernpaaren, die bereits für die Datenübertragung genutzt werden
- ✓ Speisung auf Adernpaaren, die ungenutzt sind

Bei der Stromversorgung über bereits genutzte Adernpaare, der sogenannten Phantomspeisung, werden die zur Datenübertragung genutzten Pins 1/2 und 3/6 verwendet. Bei diesem Verfahren wird die Polarität der Versorgungsspannung nicht festgelegt. Die Polaritätszuweisung erfolgt erst am angeschlossenen Endgerät. Zu beachten ist dabei, dass ein gekreuztes Kabel (engl. Crossover) die Polarität wieder dreht. Zum Schutz der angeschlossenen Endgeräte müssen diese über eine entsprechende Eingangsbeschaltung verfügen.

Bei der Speisung über ungenutzte Adernpaare, auch Spair-Pair-Speisung genannt, werden die Pins 1/2 und 7/8 verwendet.

Unterschiede der Spannungsversorgung

Die Energiequelle für die Spannungsversorgung kann über zweierlei Methoden erfolgen:

- ✓ direkt durch den PoE-Switch im Serverschränk (Endspan)
- ✓ durch zwischengeschaltete Adapter (Midspan)

Die Nutzung der Endspan-Variante hat den Vorteil, dass Daten und Strom auf mehreren Ports über ein zentrales Gerät eingespeist werden. Der Verwaltungsaufwand reduziert sich dadurch erheblich. Auch im Fehlerfall reduziert sich die Suche auf ein Minimum.

Bei der Midspan-Variante werden immer zwei Geräte benötigt, die auf einer vorhandenen Twisted-Pair-Leitung eingeschleift werden:

- ✓ Power Supplying Equipment (PSE)
- ✓ Powered Device (PD)

Das PSE wird als Energiequelle nach dem aktiven Port an einem herkömmlichen Switch und vor dem 19-Zoll-Patchpanel im Serverschrank eingesetzt. Der RJ-45-Ausgang des PSE liefert dann die für PoE erforderlichen Signale und Spannungen. Das PD wiederum dient als Gegenstück und wird am anderen Ende der Leitung eingesetzt. Das PD wird zwischen der RJ-45-Anschlussdose und dem zu versorgenden Endgerät angeschlossen. Das PD fungiert wie ein Splitter und teilt an seinem Ausgang das PoE-Signal in eine separate Versorgungsspannung und das konventionelle Ethernet-Signal. Sind keine Steckdosen in der Nähe der zu betreibenden Endgeräte, kann man trotzdem mithilfe dieser Adapter ohne großen Aufwand herkömmliche Geräte nutzen.

Verwendete Endgeräte

Aufgrund der geringen Leistungen, die über Twisted-Pair-Kabel und die zugehörigen RJ-45-Stecker übertragen werden, kann nicht jedes beliebige Gerät diese Technologie verwenden. Geräte, die mit Power over Ethernet versorgt werden können, sind:

- ✓ VoIP-Telefone
- ✓ WLAN- und Bluetooth-Access-Points
- ✓ Webcams
- ✓ Handheld Computer
- ✓ intelligente Sensoren
- ✓ Gebäude-Sicherheits-Systeme
- ✓ kleinere Print-Server

Weitere Informationen zu PoE finden Sie hier:

- ✓ <https://www.elektronik-kompendium.de/sites/net/0807021.htm>
- ✓ https://de.wikipedia.org/wiki/Power_over_Ethernet

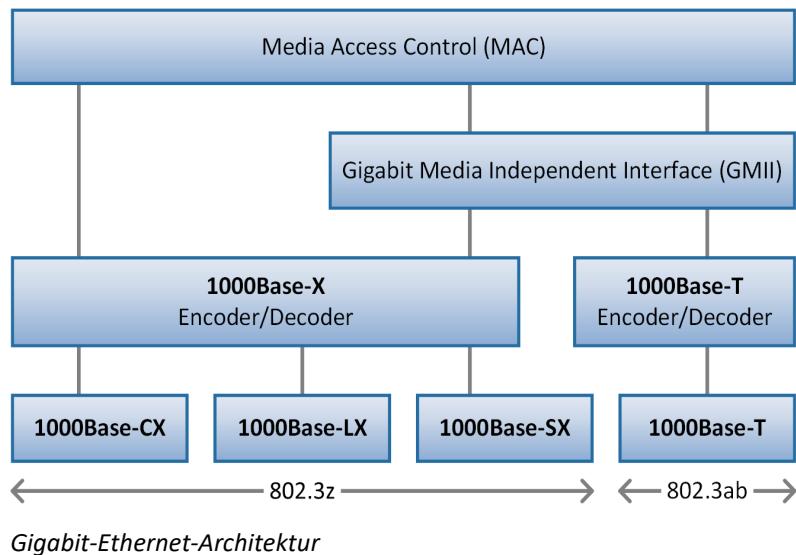
11.3 Gigabit-Spezifikation

Gigabit-Ethernet ermöglicht eine Verzehnfachung des Datendurchsatzes der Fast-Ethernet-Technologie mit Übertragungsraten von 1 Gbit/s. Für das Gigabit-Ethernet wurden im Jahr 1995 spezielle Arbeitsgruppen (802.3z und 802.3ab) gebildet. Der Einsatz dieser Technologie war besonders für den LAN-Backbone interessant. Gigabit-Ethernet ist mit dem bestehenden 802.3-Ethernet-Format kompatibel und nutzt dabei die PAM-5-Modulation (Pulsamplitudenmodulation mit 5 Stufen). Das Frame-Format von 802.3 und die Framelängenbegrenzungen zwischen 46 Byte und 1.518 Byte wurden übernommen. Zusätzlich ist es möglich, auch Jumboframes bis 9 Kilo-byte Größe zu nutzen. Gigabit-Ethernet unterstützt Stern-Topologien mit allen im Verkabelungsstandard ISO 11801 empfohlenen Übertragungsmedien. So entwickelte die Arbeitsgruppe 802.3z die Standards für Monomodefasern, Multimodefasern und STP-Kabel. Die Arbeitsgruppe 802.3ab konzentrierte sich auf die Standardisierung von Gigabit-Ethernet auf UTP-Kabeln im Anschlussbereich.

UTP-Kabel der Kategorie 5 können im Anschlussbereich mit einer Anschlusslänge von bis zu 100 m verwendet werden. Die Gigabit-Ethernet-Architektur beschreibt u. a. ein neues Modulationsverfahren (PAM5), die Signalübertragung auf allen vier Aderpaaren und zusätzliche Sicherungsmechanismen.

Grundsätzlich wird der Standard nach den physikalischen Medien MM (Multimodefiber), SM (Singlemodefiber), TP (Twisted Pair) und Coaxialkabeln unterschieden:

- | | | |
|-----------------------------|-----------------------------|----------------------------|
| ✓ 1000Base-LX(MM-/SM-Fiber) | ✓ 1000Base-ZX (SM-Fiber) | ✓ 1000Base-BX10 (SM-Fiber) |
| ✓ 1000Base-SX (MM-Fiber) | ✓ 1000Base-EX (SM-Fiber) | ✓ 1000Base-LX10 (SM-Fiber) |
| ✓ 1000Base-T (TP Cat. 5-6) | ✓ 1000Base-TX (TP Cat. 6-7) | ✓ 1000Base-CX (Coax) |



1000Base-LX

1000Base-LX ist eine Variante von Gigabit-Ethernet, die mit Glasfaserkabel mit einer langen Wellenlänge arbeitet. Dabei steht der Buchstabe L für Long Wavelength. Es wird ein Laser mit einer Wellenlänge von 1300 nm verwendet (von 1270 nm bis 1355 nm). Es können sowohl Multimodefasern als auch Monomodefasern eingesetzt werden. Die Reichweiten unterscheiden sich dabei. Mit Multimodefasern von 62,5 µm und 50 µm wird eine Entfernung von 550 m überbrückt. Bei einer Monomodefaser beträgt die Reichweite 5 km. Dabei ist zu berücksichtigen, dass es sich um Punkt-zu-Punkt-Verbindungen in Full-Duplex handelt. Spezifiziert sind ferner die optische Sendeleistung mit -3 dBm, die minimale optische Sendeleistung mit -11,5 dBm und die optische Empfangsleistung mit -3 dBm. Als Stecker kommt oft der Duplex-SC-Stecker zum Einsatz.

1000Base-SX

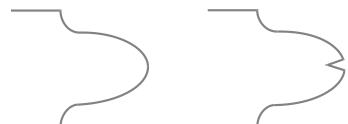
Diese Gigabit-Ethernet-Variante gleicht der LX-Variante. Jedoch wird hier ein Laser mit kurzer Wellenlänge (Short Wavelength) eingesetzt. Mit dem 850-nm-Laser werden je nach Glasfaserdurchmesser der Multimodefasern in der Praxis Entfernungen von 270 m (62,5 µm) bzw. 550 m (50 µm) erreicht. Bei diesen Entfernungen ist zu berücksichtigen, dass es sich wie bei 1000Base-LX um eine Punkt-zu-Punkt-Verbindung im Full-Duplex ohne CSMA/CD handelt. Die mittlere optische Sendeleistung ist ebenso wie die mittlere Empfangsleistung mit 0 dBm spezifiziert. 1000Base-SX verwendet vorwiegend ebenfalls den Duplex-SC-Stecker.

Probleme bei 1000Base-LX und 1000Base-SX

Beim Einsatz von LWL-Kabeln mit Multimodefasern kann es zu Fehlübertragungen kommen. Bei einigen Multimodefasern dominieren bestimmte Modengruppen, wenn als Lichtquelle ein Laser eingesetzt wird. Jede optische Faser kann nur eine begrenzte Anzahl an Moden führen. Abhängig vom Winkel, in dem der Lichtstrahl in die Faser eingekoppelt wird, gibt es zwischen den einzelnen Moden Laufzeitunterschiede. Um diese Differenzen auszugleichen, werden Fasern mit Gradientenprofil eingesetzt. Die Brechzahl nimmt dabei vom Kernmittelpunkt zum Mantel hin stetig ab.

Bei idealen Verhältnissen besitzt eine Gradientenfaser ein „glattes“ Brechzahlprofil, wodurch die Laufzeitunterschiede ausgeglichen werden. Weist das Brechzahlprofil jedoch eine Kerbe auf, kann es zu Impulsverzerrungen kommen.

Durch das Conditional Launching wird eine ausgeglichene Anregung aller Moden in der Faser ermöglicht. Der Einsatz von Kompensationsmodulen (Mode Conditioner) erfolgt bei 1000Base-SX in den Transceivern und bei 1000Base-LX extern auf dem Steckerkabel.



Brechzahl mit idealer Gradientenfaser und mit Knick

1000Base-CX

Die CX-Variante ist für Gigabit-Ethernet über Twinax-Kabel mit 150 Ohm standardisiert. Die 1000Base-CX-Variante eignet sich für Endgeräteanschlüsse mit einer Entfernung von 25 m. Aufgrund der relativ kurzen Reichweite stelltte diese Gigabit-Ethernet-Technologie über Kupferkabel lediglich eine Übergangslösung dar.

1000Base-T

1000Base-T beschreibt die Standardisierung der Gigabit-Ethernet-Technologie über Kupferkabel der Kategorie 5 – 6 für den Anschlussbereich mit bis zu 100 m Länge. Der MAC-Layer bleibt bis auf die höhere Geschwindigkeit gegenüber dem klassischen 10-Mbit/s-Ethernet und dem Fast-Ethernet unverändert. Die Basisprinzipien von 1000Base-T entstammen der 100Base-T2-Technik (100 Mbit/s auf Kategorie-3-Kabeln über zwei Adernpaare). Bei dieser Technik wird also mit vier Adernpaaren gearbeitet.

Für die Übertragung von 1 Gbit/s im Vollduplex-Modus ist es erforderlich, dass jedes Adernpaar in jede Richtung 250 Mbit/s überträgt. Laut Spezifikation ist diese Geschwindigkeit für Kabel der Kategorie 5 zu hoch. Der Standard beschreibt dort eine Bandbreite von 100 MHz. Nachteilig wirkt sich bei diesen hohen Übertragungsgeschwindigkeiten das Übersprechen zwischen den Adernpaaren aus. Der Standard 1000Base-T berücksichtigt diese Einschränkungen und sieht eine Forward Error Correction (Verfahren zur Fehlerkorrektur) vor.

Um der Problematik des Trunking (Parallelschaltung mehrerer Ethernet-Links) gerecht zu werden, wurde eine Link-Aggregation-Schicht (Link-Bündelung) integriert. Diese Schicht wird zwischen höheren Ebenen oder dem LLC eingefügt. Mit ihr ist es möglich, dass über mehrere MAC-Subschichten parallel gearbeitet werden kann. Damit wird eine gute Leitungsredundanz erreicht, da bei Ausfall einer Leitung mit geringerer Kapazität weitergearbeitet werden kann. Zusätzlich wird mit dieser Funktion eine grobe Skalierung der Bandbreite erreicht.

Die Grenze

Als bremsender Faktor für die maximale Datenrate von 1 Gbit/s stellten sich die elektrischen Eigenschaften von TP-Kabeln heraus. Es ist nicht möglich, Daten mit einer unendlichen Datenrate auf einem TP-Kabel zu übertragen. Die bei der Gütebestimmung wichtigen Kriterien waren bisher die Dämpfung, die Nahnebensprechdämpfung und die Fernnebensprechdämpfung. Da bei 1000Base-T auf allen Adernpaaren gleichzeitig Daten übertragen werden, hat jedes Paar drei benachbarte Paare. Diese rufen eine Beeinflussung in Form einer Störung auf das eigene Signal hervor. Durch Unregelmäßigkeiten im Kabel (z. B. Übergänge im Wellenwiderstand) kommt es zu Reflexionen, die das eigentliche Signal überlagern. Grund dafür kann eine schlechte Kabelkonfektionierung oder der Einsatz qualitativ niederwertiger Verbindungselemente sein. Als Bewertungskriterium gilt dabei die Rückflussdämpfung, die der Reflexion entgegenwirkt. Ein Kabel ist umso besser, je höher die Rückflussdämpfung ist. Durch eine höhere Rückflussdämpfung ist das reflektierte Signal entsprechend schwächer.

Eine schlechte Kabelkonfektionierung (z. B. Aufheben der Verdrillung in der Anschlussdose) kann sich sehr negativ auf die elektrischen Eigenschaften des Kabels auswirken.

Codierungsverfahren

Beim Gigabit-Ethernet wird alle 8 ns (125 MHz) ein 8 Bit breites Datenwort über das GMII (Gigabit Media Independent Interface) an den Physical Layer (PHY) übergeben. Das Datenwort mit einer Länge von 8 Bits kann dabei $2^8 = 256$ verschiedene Bitkombinationen annehmen. Um alle Kombinationen ohne Informationsverluste übertragen zu können, muss ein Codierungsverfahren eingesetzt werden, das mindestens 256 verschiedene Symbolkombinationen liefert. Eine Drei-Level-Codierung (MLT-3) wie bei 100Base-TX hätte auf vier Adernpaaren nur $3^4 = 81$ übertragbare Symbolkombinationen geliefert. Selbst bei einem Vier-Level-Codierungsverfahren wären es nur $4^4 = 256$ Symbolkombinationen gewesen, was zwar für die Datenübertragung, aber nicht für Kontrollinformationen ausgereicht hätte.

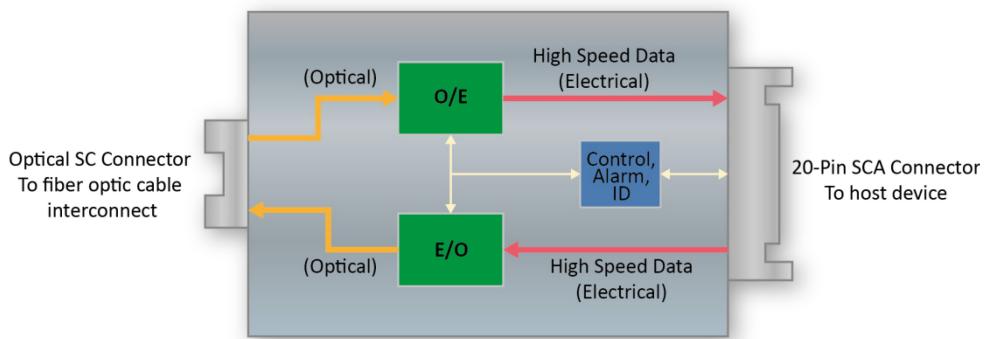
Erst das speziell für 1000Base-T entwickelte Fünf-Level-Codierungsverfahren (PAM5) brachte 625 mögliche Symbolkombinationen, von denen 113 für Kontrollfunktion und Fehlererkennung verwendet werden. Für jede 125-MHz-Periode übergibt der GMII acht Bits, die einer Kombination von 256 möglichen Bitkombinationen entsprechen. Die PAM5-Codierung erzeugt daraus eine Symbolkombination, die während der Periode über vier Adern übertragen wird. Dabei werden pro Adernpaar jeweils zwei Bits übertragen.

Bezogen auf die Datenrate ergibt sich bei der Verwendung von vier Adernpaaren und der Übertragung von zwei Bits pro Periode ein Teilungsfaktor von $4 \times 2 = 8$. Dies führt bei einer Datenrate von 1000 MBit/s zu einer Übertragungsrate von 125 MBit/s pro Adernpaar, was dem 100Base-TX entspricht.

11.4 Gigabit Interface Converter (GBIC)

GBIC-Modul

Die Übernahme der physikalischen Schicht von Fibre Channel (FC-PH) als Teil der Gigabit-Ethernet(GE)-Spezifikation (IEEE 802.3z) hat zur Verbreitung des Fibre-Channel-Protokolls (Hochgeschwindigkeits-Übertragungstechnik) wesentlich beigetragen. Sowohl FC als auch GE erlauben den Einsatz unterschiedlicher physikalischer Medien wie UTP-Kabel oder Glasfaserkabel. Um die Entwicklung und Implementierung von Geräten der FC- und GE-Systeme zu vereinfachen, wurde vom Small-Form-Factor-(SFF-)Komitee ein Standard definiert, der als Gigabit Interface Converter-(GBIC-)Modul bekannt wurde.



Im Grundsatz ist das GBIC-Modul ein Vollduplex-Daten-Transceiver (Sender und Empfänger) mit zwei Daten-Ports. Einer der Ports ist für optische Daten vorgesehen und kann u. a. als Duplex-SC-Steckverbinder ausgeführt werden. Der andere Port ist elektrischen Signalen vorbehalten und als ein 20-Pin-SCA-Steckverbinder ausgeführt. Diese Seite des GBIC-Moduls ist mit dem Host-Gerät verbunden und verarbeitet elektrische Signale wie Steuerung, Alarm, Modul-Identifizierung und schnelle serielle elektrische Daten. Bei Verwendung dieser beiden Datenports wandelt GBIC gleichzeitig die Daten von elektrisch zu optisch (E/O) und von optisch zu elektrisch (O/E).

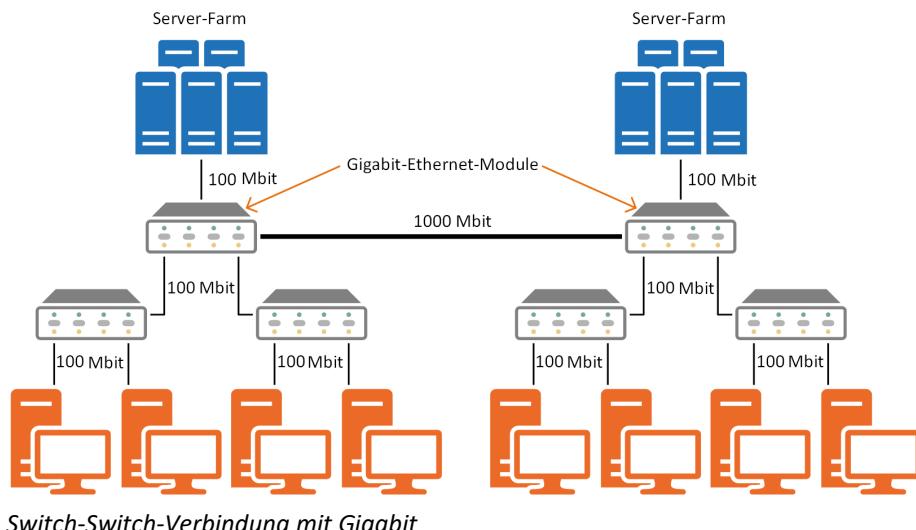
Durch die Übernahme der FC-PH-Konformität für GBIC-Module eignen sich diese nicht nur für FC-, sondern auch für GE-Systeme und für andere firmeneigene Anwendungen, die serielle Übertragungsleitungen hoher Bandbreite benötigen. GBIC-Module sind als „heiß steckbare“ (engl. hot pluggable) Bausteine konzipiert. Sie können in das Host-Gerät gesteckt oder aus diesem entfernt werden, ohne dass das Gerät ausgeschaltet werden muss.

Diese Voraussetzung ist wichtig bei Geräten, bei denen eine Ausfallzeit von null wünschenswert ist. Der hot pluggable Charakter der GBIC-Module vereinfacht Upgrades und Wartung ohne Systemausfall. Um die Packungsdichte der physikalischen Ports auf den Geräten zu erhöhen, wechseln die Hersteller zu kleineren Bauformen (Mini-GBIC). Diese werden auch als SFP-Interface-Module (Small Form-Factor Pluggable) bezeichnet.

11.5 Konfigurationsbeispiele

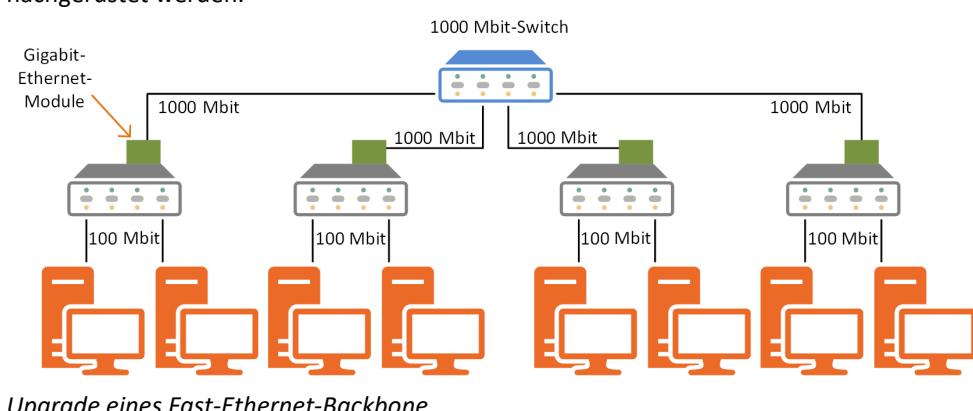
Upgrade von Switch-zu-Switch-Verbindungen

Durch den Einsatz der Gigabit-Ethernet-Technologie wird die Verbindungsgeschwindigkeit von 100-Mbit-Switches um den Faktor 10 erhöht. Die dadurch zur Verfügung stehende Bandbreite der Switch-Switch-Verbindung ermöglicht es, dass eine wesentlich höhere Anzahl an Endgeräten ohne Performance-Engpässe über den Backbone kommunizieren können.



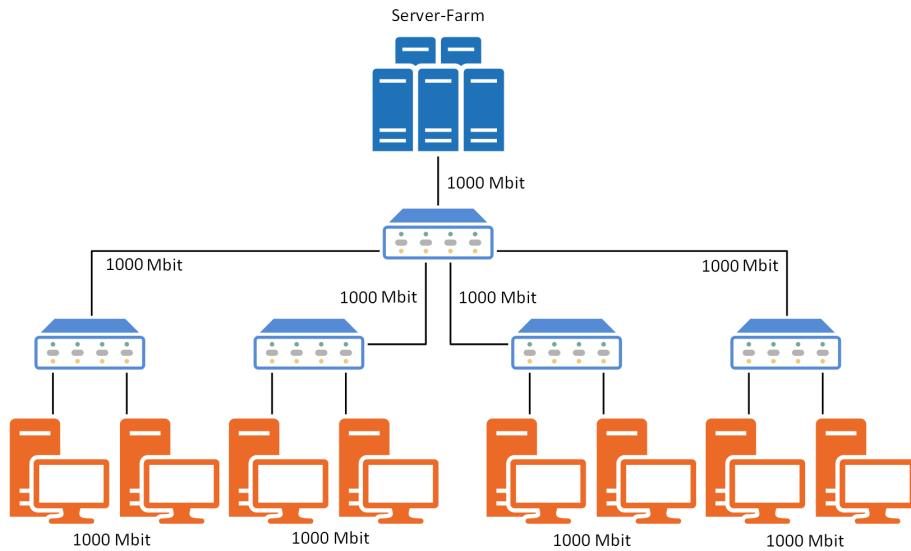
Upgrade eines Fast-Ethernet-Backbone

Die im Backbone installierten 10/100-Ethernet-Switche werden durch Gigabit-Ethernet-Switche ausgetauscht. Modular aufgebaute Systeme können problemlos durch den Einsatz der entsprechenden Gigabit-Module nachgerüstet werden.



Gigabit-Komplettlösung

Durch den Einsatz entsprechender Gigabit-Ethernet-Adapter kann die Datenrate von 1000 MBit im gesamten Netzwerk genutzt werden. Zukünftige Netzwerkanwendungen aus dem multimedialen Bereich (z. B. Video) mit hohem Datentransfer benötigen eine hohe Bandbreite, um einen reibungslosen Arbeitsablauf zu ermöglichen.



Komplettlösung mit Gigabit

11.6 2,5- und 5-Gigabit-Ethernet

Das Bestreben, die ältere vorhandene Kupferverkabelung (Klasse D und E) weiterhin nutzen zu können und gleichzeitig mehr Datendurchsatz zu erzielen, führte bei IEEE zur Normierung 802.3bz (2.5GBase-T und 5GBase-T). Beide Verfahren basieren auf 10-Gigabit-Ethernet (10GBase-T) mit der Reduzierung der Datenrate um den Faktor 2 bzw. 4. Auch entsprechen 2,5 und 5 Gbit/s genau den maximal für Cat5e- und Cat6-Kabel definierten Datenraten bei 100 m Kabellänge. Vor dem Einsatz ist jedoch die Verkabelung qualifiziert zu prüfen, ob sie sich für diese Ethernet-Varianten auch eignet.

11.7 10-Gigabit-Ethernet

10-Gigabit-Ethernet über Glasfaser und Kupfer

Immer mehr Anwendungen in einem Netzwerk fordern immer größere Bandbreiten. Viele Gigabit-Ethernet-Anbindungen sind bereits kurze Zeit nach deren Inbetriebnahme stark ausgelastet. Durch den 10-Gigabit-Ethernet-Standard besteht die Möglichkeit, die benötigten Bandbreiten weiter auszubauen. Für eine 10-Gigabit-Ethernet-Anbindung sind grundsätzlich folgende Medien geeignet:

- ✓ Glasfaserkabel
- ✓ Kupferleitungen

10-Gigabit-Ethernet über Glasfaser

Bei Glasfaserkabeln unterscheidet der Standard IEEE 802.3ae mehrere Varianten:

- ✓ 10 GBase-LX4 bei 1310 nm
- ✓ 10 GBase-LX1 bei 1310 nm
- ✓ 10 GBase-LW bei 1310 nm
- ✓ 10 GBase-SR bei 805 nm
- ✓ 10 GBase-ER bei 1550 nm
- ✓ 10 GBase-SW bei 850 nm
- ✓ 10 GBase-EX bei 1550 nm

Hierbei bezeichnet der erste Buchstabe nach 10 GBase die benutzte Wellenlänge:

- ✓ Long (1310 nm)
- ✓ Short (850 nm)
- ✓ Extreme Long (1550 nm)

Der zweite Buchstabe steht für die verwendete Codierung des Bitstromes. Bei Weitverkehrsnetzen verwendet man Komponenten mit dem Buchstaben „W“ für WAN. Bei herkömmlichen Netzwerken werden Module mit dem Buchstaben „R“ als Bezeichnung für LAN eingesetzt. Die letzte Ziffer nach dem Netwerktyp gibt an, ob ein Wellenlängen-Multiplexverfahren angewendet wird oder nicht. Dabei bezeichnet die Zahl die Anzahl der eingesetzten Wellenlängen. Die Zahl 4 sagt beispielsweise aus, dass ein Wave-Division-Multiplexing (WDM)-Verfahren mit 4 Wellenlängen eingesetzt wird.

Vorhandene Strukturen

Mit 10GBase-SR-Modulen können vorhandene Multimodefasern benutzt werden, um in einem Netzwerk kurze Strecken zu überbrücken. Überbrückbare Distanzen sind in der Größenordnung zwischen 20 und 80 Metern anzusiedeln. Wird eine Multimodefaser mit einem Bandbreite-Längen-Produkt von 2000 MHz x km verwendet, können sogar Strecken bis zu 300 Metern überbrückt werden. Bei bestehenden Singlemodefasern in einem vorhandenen Netzwerk werden hingegen die 10GBase-LR-Module eingesetzt. Bei einer Wellenlänge von 1310 nm lassen sich auf einer Reichweite von bis zu 10 km Daten problemlos übertragen.

10-Gigabit-Ethernet über Kupfer

Eine Übertragung der Daten auf Twisted-Pair-Leitungen nach dem Standard IEEE 802.3an (10GBase-T) erfolgt beim 10-Gigabit-Ethernet auf allen vier Adernpaaren. Dabei wird der Datenstrom für das Senden (Tx) von Daten auf zwei Adernpaare mit je 2,5 Gigabit/s pro Adernpaar aufgeteilt. Gleiches gilt für das Empfangen (Rx) von Daten. Somit ist es möglich, den Full-Duplex-Betrieb mit je 10 Gigabit/s an Daten für Senden und Empfangen zu realisieren. Je nach verwendetem Kabeltyp können Übertragungsstrecken auf einer Länge bis zu 100 Metern überbrückt werden.

Verwendeter Kabeltyp	Reichweite
Kategorie 6A, geschirmte Leitungen (FTP)	100 m
Kategorie 7, geschirmte Leitungen (FTP)	100 m
Kategorie 7A, paargeschirmte Leitungen (S/FTP)	100 m
Kategorie 8, paargeschirmte Leitungen (S/FTP)	100 m

11.8 25- und 40-Gigabit

Mit dem Standard IEEE 802.3bq ist es seit 2017 möglich, über eine Kupferverkabelung (Cat 8.1 und 8.2) Datenraten von 25 Gbit/s (25GBase-T bzw. 40GBase-T) zu erzielen. Gleichzeitig sinkt jedoch die empfohlene Länge auf 30 m. Für darüberhinausgehende Übertragungsraten (100 Gbit/s) sind einerseits nur noch eine maximale Länge von 8 m erlaubt und andererseits 4 bzw. 10 spezielle Kabel notwendig. Daher liegt der Focus auf Lichtwellenleitern.

Derzeit arbeitet die IEEE an den Drafts für 200 Gbit/s und 400 Gbit/s. Dazu werden bei Lichtwellenleitern sowohl mehrere Adern als auch mehrere Wellenlängen für den Einsatz diskutiert.

11.9 Anforderungen an industrielle Gerätschaften

Um den Anforderungen im Produktionsbereich gerecht zu werden, müssen die verwendeten Ethernet-Komponenten entsprechende Voraussetzungen erfüllen. Hierzu zählen:

- ✓ Befestigung auf einer Tragschiene (Hutschiene)
- ✓ Spannungsversorgung über 24 Volt Gleichstrom
- ✓ erhöhter Schutz gegen elektromagnetische Störungen
- ✓ erweiterter Temperaturbereich (0 Grad bis +60 Grad bei Standard-Modellen)
- ✓ besserer Schutz gegen Feuchtigkeit (etwa 95% rel. Luftfeuchtigkeit)
- ✓ besonderer Schutz gegen Eindringen von Staub
- ✓ besonderer Schutz gegen Spritzwasser
- ✓ Schutz gegen Schmierstoffe und Öle
- ✓ Rüttelfestigkeit beim Einsatz an Maschinen
- ✓ erhöhte Ausfallsicherheit
- ✓ hohe Zuverlässigkeit im Betrieb
- ✓ Meldekontakt für Störungen

Industrial Ethernet gewinnt immer mehr an Bedeutung, da sich der Ethernet-Standard in Produktionsstätten weiter verbreitet. Durch die rauen Bedingungen in der Fertigung werden aber auch höhere Anforderungen an die Datenverkabelung und die Anschlusspunkte gestellt. Die Qualität der übertragenen Informationen und Daten muss über den gesamten Transportweg gesichert werden und Störungen an den Anschlusspunkten sind entsprechend zu minimieren. Störungen treten besonders an den RJ-45-Steckern der Anschlussdosen und deren Buchsen auf. Daraus ergeben sich nachfolgende Probleme:

- ✓ schlechte Kontakte durch Eindringen von Schmutz und Staub
- ✓ Lockern der Verbindung durch Vibrationen
- ✓ Kabelbrüche durch bewegliche Maschinenteile
- ✓ fehlende Erdung an den Maschinen

Zur Vermeidung von Störungen an den Anschlüssen der Twisted-Pair-Kabel haben verschiedene Hersteller eine eigene Produktlinie für den Einsatz im industriellen Bereich entwickelt. Diese Komponenten sind speziell für den Einsatz in der Industrie ausgelegt. Sie verfügen über stabile und geschützte Gehäuse und entsprechen dem IP-67-Standard (International Protection). Um eine gewisse Ausfallsicherheit zu erhalten, ist es sinnvoll, die Ethernet-Verkabelung zur Anbindung der benötigten Maschinen als Ringstruktur auszuführen. Im Störungsfall ist dann nur eine Maschine oder ein Teilbereich der Fertigungsanlage betroffen und nicht die komplette Produktion.

11.10 Neue Mobilfunkstandards

Es ist absehbar, dass bisherige Mobilfunkstandards bald an ihre Grenzen stoßen. Die grundsätzlichen Ziele neuer Standards sind u. a.:

- ✓ Versorgung ländlicher Gebiete
- ✓ geringerer Energieverbrauch der Endgeräte
- ✓ bessere Mobilität
- ✓ Vereinfachung der Architektur und der Protokolle
- ✓ Sicherheit und Verfügbarkeit der Dienste

Dafür ist eine weitere, engere Verknüpfung bestehender und in Planung befindlicher Dienste und Systeme im Mobilfunkbereich notwendig. Die schwerpunktmaßigen Bereiche, um den o. g. Anforderungen gerecht zu werden, werden nachfolgend klassifiziert:

- ✓ die Integration von Systemen, d. h. die vollständige Zusammenarbeit unterschiedlicher Geräte, wie z. B. Smartphones, Tablets, Notebooks, Kameras, Navigationssysteme unter dem Aspekt der Nutzung der gleichen Dienste und der damit verbundenen Sicherheitsaspekte
- ✓ die Zusammenführung von Prozessen, wie z. B. Arbeitsprozessen und die interaktive Kommunikation
- ✓ die Optimierung und Konvergenz der Infrastruktur bezüglich der Dienste (LTE, WiMax, 5G) und der erforderlichen Bandbreiten
- ✓ die Informationsintegration, d. h. die uneingeschränkte Nutzung und Verknüpfung zwischen den Informationsarten Voice, Video und Daten
- ✓ die Web-Integration, die eine vollständige Einbindung mobiler Endgeräte in Web 2.0 ermöglicht
- ✓ der Kostenbereich, der neue und flexible Modelle seitens der Provider bereitstellen muss
- ✓ die Konvergenz, d. h. die Nutzung der gleichen Dienste, sowohl im beruflichen als auch im privaten Umfeld

Mobilfunkstandard der 5. Generation (5G)

An 5G wurde weltweit intensiv geforscht. 2019 wurden in Deutschland die Nutzungslicenzen versteigert. Es soll LTE ergänzen bzw. später ablösen. Die Neuerungen von 5G können erst in den Frequenzen oberhalb von 6 GHz genutzt werden. Wegen der höheren Frequenz wird es notwendig, die Funkzellen in Städten engmaschiger auszubauen, als dies bei den Vorgängertechniken der Fall war. Das 3rd Generation Partnership Project (3GPP) als Standardisierungsorganisation hat im Dezember 2018 mit dem Release 15 die ersten Standards veröffentlicht, die auch die Funktion von 5G beinhaltet. Weitere Neuerungen werden im Release 16 (März 2020) erwartet.

Erste Teile des 5G-Mobilfunkstandards sollen im Jahr 2020 einsatzfähig sein und Datenübertragungsraten von 10–20 Gbit/s mit einer sehr niedrigen Latenzzeit < 1 ms und einer hohen Verfügbarkeit ermöglichen. Bis 2025 soll sich laut der „5G Strategie für Deutschland“ die Gesellschaft zu einer so genannten „Gigabitgesellschaft“ entwickeln. Die Publikation finden Sie hier: <https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/098-dobrindt-5g-strategie.pdf>

11.11 Weitere Technologien

Li-Fi (Light Fidelity)

Li-Fi wurde abgeleitet von Wi-Fi (WLAN) und soll in Zukunft die bestehende Funk-Technologie ergänzen oder in Teilen ersetzen. Es basiert auf dem physikalischen Visible Light Communication (VLC) Verfahren, welches das Lichtspektrum vom Infrarot- bis zum Ultraviolettbereich nutzt. Durch die Breite des Lichtspektrums können theoretisch Datenübertragungsraten > 200Gbit/s umgesetzt werden (real sind es zur Zeit Datenraten < 10 Gbit/s).

In einer speziellen Lampe werden LEDs im Lichtspektrum hochfrequent ein- und ausgeschaltet. Das hochfrequente Schalten ist für das menschliche Auge nicht wahrnehmbar. Die Lampe dient als HotSpot. Ein Sensor empfängt die Lichtsignale und setzt sie in elektrische Signale für ein Endgerät um. Für die Kommunikation ist eine direkte Sichtverbindung notwendig. Bei einer Blockierung der Verbindung durch andere Objekte wird die Übertragung unterbrochen. Durch die direkte Kommunikation wird grundsätzlich auch dem Sicherheitsaspekt Rechnung getragen. Es gibt bereits einige Prototypen von Li-Fi. Wann es zur Serienreife kommt, hängt von den zukünftigen Anforderungen ab.

WLAN-Mesh

Mesh (engl. Masche) ist eine Lösung, wenn ein WLAN-Netz allein für eine Location nicht ausreicht. Durch bauliche Gegebenheiten werden WLANs langsam oder weisen Unterbrechungen auf. Mesh kompensiert dieses Problem, indem mehrere verteilte Geräte, zusätzliche WLAN-Netze erzeugen und diese zu einer einzelnen Funkzelle zusammenfassen. Das gesamte WLAN verwendet einen einheitlichen Namen und ein einziges Passwort.

SD-WAN (Software-defined WAN)

Software-defined WAN (SD-WAN) ist ein Konzept, ein Enterprise-WAN (Wide Area Network) zu installieren, welches sich der Mechanismen von SDN (Software-defined Networking) bedient. SD-WAN setzt die Überwachung und das Management des Internetverkehrs von den physischen Geräten auf die Applikation um, welches die Funktion von SDN über ein virtuelles Overlay abbildet. Dieser Ansatz ermöglicht eine Automatisierung und zentrale Überwachung des Intranets/Internets. Das Management des Internetverkehrs kann über unterschiedliche Verbindungen in Realtime (Echtzeit) realisiert werden.

Powerline-Adapter

Auch im Bereich von Powerline-Adaptoren hat sich einiges getan. Neben höheren Übertragungsraten (theoretisch bis 1200 Mbit/s) findet man heute diverse Geräte, die über mehrere TP Ports (bis zu 3 Stk.) und einen integrierten WLAN-Access-Point verfügen. Hiermit kann leicht, über die bestehende 230-V-Verkabelung, eine Vernetzung zu weit entfernten Räumen realisiert werden, ohne mit WLAN-Repeatern arbeiten zu müssen. Auch die Verschlüsselungsstandards wurden durch Einführung des Homeplug AV2 Standards auf 128-Bit AES erhöht.

Trends

Umfragen zu aktuellen IT-Trends von marktorientierten Organisationen wie beispielsweise dem Bitkom (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.) zeigen, dass die permanente und ortsunabhängige Verfügbarkeit von Informationen wiederholt als sehr wichtig bewertet wird.

Aktuelle und zukünftige Entwicklungen im mobilen Bereich zielen darauf ab, den Informationsaustausch weiter zu optimieren. Dies bedeutet, dass die Applikationen und Systeme verstärkt untereinander autark kommunizieren (z. B. über sensorische Netzwerke). Dem Nutzer müssen nur noch die augenblicklich wichtigen Informationen zur Verfügung gestellt werden. Beispielhaft seien hier erwähnt:

- ✓ Fahrzeug-Kommunikation (Car2Car, V2V) über WLAN/UMTS/LTE/WiMAX: Mittels situationsabhängiger Geschwindigkeitsanpassung der Fahrzeuge wird der Verkehrsfluss optimiert. Dazu müssen relevante Verkehrsinformationen zwischen den Fahrzeugen kontinuierlich ausgetauscht werden. Das Ziel dieser Entwicklung wird die weitgehend fahrerlose Routenführung darstellen. Daneben können verkehrsbeeinflussende Faktoren in Echtzeit ausgetauscht werden.
- ✓ Sensornetzwerk für Container: Die Logistik erfordert die ständige Überwachung und Nachverfolgung der Warenbewegungen über eine globale Positionsbestimmung. Sensorische Netzwerke liefern die Informationen, z. B. für den aktuellen Standort, den Ladungsinhalt, die Verfügbarkeit und den Nachweis der Echtheit der Waren über RFIC (Radio Frequency Integrated Circuit) und GPS-Anbindung.
- ✓ Body Area Networks (mit Sensoren ausgestattete Personen): z. B. Pulsmesser für Jogger, Patientenüberwachung nach Erkrankungen, permanente Zustandskontrolle von pflegebedürftigen Personen
- ✓ Sensornetzwerke im industriellen Bereich: z. B. für die Überwachung von Produktionsprozessen, für den Nachweis des Betriebsverhaltens und der Fertigungsqualität, für die Fehlerdiagnose im Fertigungsprozess oder für den automatisch gesteuerten Produktionsablauf zwischen den Fertigungsbereichen
- ✓ Mobiles Agrarbusiness: z. B. Sensorsteuerungen für die Überwachung und Optimierung von landwirtschaftlichen Produktionsprozessen, für den Herkunftsnnachweis und die Verfolgung von tierischen und pflanzlichen Rohstoffen und die Lagerlogistik
- ✓ Internet of Things (IoT): z. B. die selbstständige Kommunikation von Systemen untereinander (Industrie 4.0 und SmartHome)



Wissenstest: Netzwerktechnik – Überblick

Bildquellenverzeichnis

- S. 39, Optische SC-Steckverbinder, © MICROSENS GmbH & Co. KG
S. 53, Gigabit-Micro-Switch für Kabelkanaleinbau, © MICROSENS GmbH & Co. KG
S. 54, SFP Transceiver für 1-Gbit-Ethernet, © MICROSENS GmbH & Co. KG
S. 56, Industrieswitch mit Erweiterungsmodul, Profi Line Modular Basis-Switch, Erweiterungsmodul, Spannungsversorgung 48 VDC für PoE/PoE+, © MICROSENS GmbH & Co. KG
S. 58, Medienkonverter mit R-J45- und LWL-Verbindung, © MICROSENS GmbH & Co. KG
S. 61, NIC mit RJ-45- bzw. Antennenanschluss, © D-Link (Deutschland) GmbH
S. 62, PC-interner Gigabit-Ethernet Bridging Konverter, © MICROSENS GmbH & Co. KG
S. 70, LWL-Patchkabel Vergleich SC- mit LC-Stecker (unten), © MICROSENS GmbH & Co. KG
S. 75, RJ45-Stecker, © EFB-Elektronik GmbH
S. 76, AMJ-S-Modul, Hersteller: Telegärtner, © MICROSENS GmbH & Co. KG
S. 76/77, Twisted-Pair-Kabel mit Geflechtschirm, Sortiertes Twisted-Pair-Kabel, AMJ-S-Modul bestücken, Fertiges AMJ-S-Modul, © MICROSENS GmbH & Co. KG
S. 78, Messgerät zum Qualifizieren von Twisted-Pair-Kabeln, © Softing IT Networks GmbH
S. 80, CAT6-RJ45-Datendose in Einzelteilen, © EFB-Elektronik GmbH
S. 81, LSA+-Anlegewerkzeug, © EFB-Elektronik GmbH
S. 86, Verifizierer (Kabeltester): CableMaster 600, © Softing IT Networks GmbH
S. 89, Qualifizierer: NetXpert 1400, © Softing IT Networks GmbH
S. 90, Switch-Informationen, Kabelverdrahtungstest, © Fluke Networks (flukanetworks.com)
S. 91, Zertifizierer: WireXpert 4500, © Softing IT Networks GmbH
S. 95, Permanent-Link-Messung und Channel-Link-Messung, © Softing IT Networks GmbH
S. 95, NEXT Messung, Return Loss Messung, ACR-N Messung, © Softing IT Networks GmbH
S. 97, Visible Fault Finder und Reinigungskassette, © JDSU (jdsu.com)
S. 98, OTDR5000 als Videomikroskop, © Softing IT Networks GmbH
S. 99, OTDR-Messgerät, © Softing IT Networks GmbH
S. 99, Ergebnis einer OTDR-Messung an einer Multimodefaser, Abnahmemessung mit ICON-Darstellung, © JDSU (jdsu.com)
S. 101, Optischer Sender und Empfänger, © JDSU (jdsu.com)
S. 102, Ein-Jumper-Messung mit einem Patchcord, Zwei-Jumper-Messung mit 2 Patchcords + Adapter, Drei-Jumper-Messung mit 3 Patchcords + 2 Adapter, © Softing IT Networks GmbH
S. 103, Aufbau für Referenzmessung, © JDSU (jdsu.com)
S. 130, EXO Router und Access-Point, WLAN-USB-Adapter, MIMO-WLAN-PCI-Karte, © D-Link (Deutschland) GmbH

1	Außenkabel	36	D
10-Gigabit-Ethernet	190	62, 139	Dämpfung
1000Base-CX	187	136	17, 29
1000Base-LX	186	156	Dämpfungsmessung
1000Base-SX	186	94	100, 101
1000Base-T	62, 187, 188	21	Dämpfungsmessung durchführen
10-Gigabit-Ethernet-Standard	31		103
11801	26		Data
5			6
50173	26	189	Datagramm
5G	193	53	Datendienste
8			12
802.1	181	29	Datendosen
802.11i	129	163	Datendosen, industrieller Einsatz
802.2	181	163, 164	Datendosen, Kupfer
802.3	181	13	Datendosen, LWL-Verkabelung
802.3ab	185	42	Datenkabel, Beschriftung
802.3af	184	174	Datenübertragungsrate
802.3at	184	16	Datenverbund
802.3bq	192	156	DCS
802.3z	185	109	DECT
A			40, 41
Ableitung	14	23	DECT ECO
Ableitungsbelag	15, 16	12	Default-Route
Abschirmung	23	174	Dienstprotokolle
Access-Point, Konfiguration	134	163, 179	Differential Mode Delay
Access-Points	43, 45, 52, 127, 131	52, 53	Digitalmultimeter
ACR	92	52	DiMF
ACR-F	93	46	DIN VDE 0185
ACR-N	92	142	DIN VDE 0292
Address Resolution Protokoll	145	127	Dioxin
ADM, Add-Drop-Multiplexer	60	34	Dispersion
ADPCM	41		DIVO
ADSL	167		DMT, Discrete Multi Tone
AES	129		Modulation
AiMF	23		168
Akzeptanzwinkel	28		Dokumentation
Anlagenanschluss	164		112
Anschluss, informations-technischer	108		Dokumentation, kundenspezifische
Anschlussdose, LWL	74		125
Anschlussdose, modulare	76		Downstream
Anschlusstechnik	26		167, 169
ANSI	169		DSLAM
Anycast	153		168
AP	45		DSL-Modem
APIPA-Adressen	142		168, 174
ARJ45	27, 70, 76		DSL-Router, Kennwort ändern
ARP	145		177
ATM	173		DSL-Router, Voraussetzungen
Aufbauzeichnungen	121		175
			DSL-Verbindung überprüfen
			177
C			DSSS
Campusbereich		115	44
CCITT		173	Dual Cabel
Channel Link		95	12
CIDR		141	Dual Stack
CIDR-Notation		141	154
CIDR-Schreibweise		141	DWDM
CIP		47	60
Cladding		27	Dynamisches Routen
Class of Service		53	155
Classless Inter-Domain Routing		141	E
Codierungsverfahren		187	echoplex
Common ISDN Access Profile		47	7
Crimpnest		85	EIGRPv6
Crimp-Spleißschutz		38	156
Crimptechnik		85	Einfügedämpfung
Crimpzange		85	92
CSMA/CD		181, 183	Elektromagnetische Wellen
CWDM		59, 60	11
			EMV
			26
			EN 50173
			105
			Endspan
			184
			Enhanced Small Form-Factor
			Pluggable
			54
			Ersatzschaltung
			14

ESS	127	H	ISDN-Datenkanäle	164
ESSID	46		ISDN-Dosen	81
Etagenverteiler	107, 117		IS-IS	156
Euro-ISDN	166		ISO	26
F			ISO/IEC 11801	107
Fachboden, 19"	66		Isolationsverlust	16
Faser, Aufbau	34		Isolationswiderstand	19
Faserklasse	32		Isolator	14
Fasertyp	33		Isopropylalkohol	85
Fehlanpassung	19		ISP	166
Feinschutz	119		K	
Fernmeldedienste	12		Kabel, Einsatzbereiche	24
Fernnebensprechen	18		Kabel, konfektionierte	78
Ferrule	85		Kabel, symmetrische	21
Festader	34		Kabel, unsymmetrische	21
Festanschluss	9		Kabelhalter	84
FEXT	18		Kabelmantel	22
Fiber-to-the-Desk	114		Kabelmessgerät	158
Fibre Channel	188		Kabeltester	88
Firmware	90		Kabelverzweiger	107
Flame Retardant	22		Kaltfließen	24
Flatrate	168		Kapazität	14, 16
Forward Error Correction	187		Kapazitätsbelag	15, 16
Frames	181, 182		Kategorien gemäß ISO/IEC	26
Frequenzsprung-Verfahren	44, 47		Kevlarschneider	84
Frequenzumtastung	41		Klebespleiß	38
Fresnelreflexionen	99		Koaxialkabel	21, 24
full duplex	7		Kollisionsdömane	51
Funktionsverbund	7		Kombischirm	109
G			Kommunikation	8
G.SHDSL	169		Kommunikationsinfrastruktur	115
GAP	41		Kompaktader	34
Gateway	58		Komponenten, aktive	49, 64
GBIC	188		Komponenten, passive	64
Gebäudeverteiler	107, 108, 117		Kopplungswiderstand	18, 109
Geflechtschirm	76		Kupferkabel	10
GG45	27, 70, 75		L	
Gigabit Bridging Einbau-Konverter	62		LACP	55, 138
Gigabit Media Independent			Längenmessung	92
Interface	187		LAN-Messgeräte	88, 91
Gigabit-Ethernet	62, 185, 186		LAN-Zertifizierer	96
Glasfaser	27		Lastverbund	7
Glasfaserkabel	28		Laufzeit	19
Glasfaserkabel,			Leistungsmessgerät	101
Dämpfungsmessung	100		Leiterkonstruktion	21
Glasfaserkabel, Einsatzbereiche	37		Leiterlänge	14
Glasfaserkabel, Spezifikation	35		Leiterquerschnitt	14
Gleichstrom-Widerstand	92		Leiterwiderstand	14
GMSK	41		Leitfähigkeit	14
GPRS	170		Leitfähigkeit, elektrische	14
Gradientenindex	31		Leitungssuchgerät	158
Gradientenindex-Profilfaser	32		Lichtwellenleiter	10, 27
GSM-Standard	170		LightCrimp Plus	83
			Link LED	139

LLC	181	Netzwerk	7	Polymer Cladded Fiber	38				
Localhost-Adresse	142	Netzwerkanschluss	68	Port Aggregation	55				
Low Radiation	41	Netzwerkkarten	61	Potentialausgleich	119				
Low Smoke Zero Halogene	22	Netzwerkschränke	65	Power Sourcing Equipment	185				
LSA+	80	Netzwerkschränke, Kühlung	66	Powered Device	185				
LTE	172	Netzwerkschränke, Verkabelung	66	Powersum	93				
LWL	27	NEXT	18	Powersum NEXT	19				
LWL-Kabel	112	NIC	61	PPPoE	174				
LWL-Patchkabel	69, 70	Non Corrosive	22	Präfix	153				
M									
MAC	181, 182	Normen für die Dämpfungsmessung	101	Primärmultiplexanschluss	165				
Mantelstripper	84	NTBA	164, 165	Primärverkabelung	108				
Manteldurchmesser	31	NTBBA	174	Primary Coating	27				
Matrize	85	Nullabgleich	95	Private Branch Exchange	166				
Medienkonverter	58	NVP	93	Private IP-Adressen	142				
Mehrgeräteanschluss	164	Nyquist-Shannon Abtasttheorem	163	PROFINET	57				
Messergebnisse, grafische Darstellung	90	O							
Messkabel	101	OFDM	44, 172	Promiscous Mode	62				
Messprotokolle, Kupfer	124	OLSR	156	Protokoll	6				
Messtechnik, analoge	89	OM Klassen	32	PSE, Power Sourcing Equipment	185				
Messtechnik, digitale	89	Optical Mode	29	Pulsamplitudenmodulation	185				
Messtechnik, vektorielle	89	Orthogonal Frequency-Division Multiplexing	172	Pulscodemodulation	163				
Metalle	14	OS Klassen	32	Q					
Metro-Ethernet	173	OSI-Schichtenmodell	9	Qualifizieren	90				
Michael-Algorithmus	129	OSPF	147	Quarzglas	27				
Microstripper	84	OSPFv3	156	R					
Micro-Switch	53	Oszilloskop	87	RADIUS	129				
Midspan	184	Oszilloskop, analoges	87	Rapid Spanning Tree	52				
Mikrosegmentierung	53	Oszilloskop, digitales	88	Rayleighstreuung	99				
MIMO	127	OTDR	98	Realteil	17				
Mini-LAN-Tester	158	P							
Mittelschutz	119	Patchfeld	115	Reinigung	97				
MMCpro	27	Patchkabel	34	Repeater	50, 52				
MMF	32	Patchkabel, Kupfer	69	Repeater, buffered	51				
Mobilfunk-Modem	179	Patchkabel, LWL	70	Repeater, Multiport	50				
Modulation	41	Patchpanel	71, 81	Repeater, optischer	50				
Monomodefaser	31	Patchpanel, LWL	73	Repeater, Remote	50				
Multicast	153	Patchpanel, modulare	72	Repeating-Modus	46				
Multilayer Switch	58	PCF	37	RIP	147				
Multimodefaser	30	PD, Powered Device	185	RIPE NCC	142				
Multiple Spanning Tree	52	PDU	7	RIPnG	156				
Multiplexer, optische	59	Permanent Link	94	RJ-45	26, 70, 75				
N									
Nachlauffaser	100	Physical Layer	187	Roaming	46				
Nahnebensprechen	18	Piconet	47	Router	57				
NAT	145	Pigtails	34	Router, Konfiguration	176				
Nebensprechen	18	PiMF	23	Router, konfigurieren	149				
netmask	140	Ping	139, 146	Router, Multiprotokoll	57				
Network Address Translation	145	Plastic Optical Fiber	37	Routing	144				
Network Termination		Plastik-Faser	27	Routing, dynamisches	147				
Broadband Access	174	PoE, Power over Ethernet	64, 184	Routing, statisches	147				
Netzmaske	140	POF	37	Routing-Tabelle	147				
		Point to Point Protocol over Ethernet	174	Rückflussdämpfung	19, 92				
				Rückstreumessung	99				
				Ruggedized Switch	56				

S

SO-Schnittstelle	164	Stecker-/Kabelfarben	36	Verkabelungstypen	91		
S2M	165	Sternverteiler	51	Verkürzungsfaktor	19		
Schirmung	23	Sternvierer	24	Verlegung, fachgerechte	110		
Schleifenunterdrückung	52	STP	25	Vermittlungseinrichtung	9		
Schleifenwiderstand	15	Stufenindex	30	Verteilung	23		
Schränke, Netzwerk-	65	Subnetze	142	Video	6		
Schränke, Server-	65	Suffix	153	Videomikroskop	98		
Schränke, Überwachung	67	Switch	53	ViMF	23		
Schrank-Kontroll-System	67	Switch, industrieller Einsatz	56	Visible Fault Finder	97		
Schutzbrille	84	Switch, manageable	54	VLAN	55		
SDN	194	Switch-Information	90	Voice	6		
SDSL	167, 169	Systeme, kabellose	10	VoIP, Voice over Internet Protocol	166		
SD-WAN	194	Systeme, leitergebundene	10	Vorlauffaser	100		
Segment	52	T					
Sekundärverkabelung	108	TDMA	42	Wählanschluss	9		
Serverschränke	65	T-DSL light	168	Wavelength Division Multiplexing	59		
Service Set Identifier	127	Telefonanlagen	81	W-CDMA	171		
SHDSL	169	TERA	27, 70, 76	WDS	127		
Short Wavelength	186	Tertiärverkabelung	108	Wellen, elektromagnetische	11		
Signal, Geschwindigkeit	19	Tethering	180	Wellenwiderstand	15, 17, 24		
Signalabtastung	163	Time To Live	146	WEP	128		
Signalgeber, digitaler	87	TKIP	129	Wideband CDMA-Verfahren	171		
Signalprüfung	86	Topologie	60, 108	Widerstand, ohmscher	14		
Signalübertragung	13, 28	Totalreflexion	28	Widerstand, spezifischer	14		
Signalverformung	20	traceroute	146	Widerstandsbelag	15		
Signalverzögerung	20	tracert	146	WiMAX	126, 172		
Simplex	7	TRILL	52	Wire Map	90		
Simplexkabel	35	Triple-Speed	61	Wired Equivalency Protocol	128		
Single Cable	12	Trunkkabel	116	Wireless Bridge	127		
Singlemodefaser	31	TSB	75	Wireless Distribution System	46		
SIP, Session Initiation Protocol	166	TTL	146	Wireless LAN	43		
SIP-Trunk	163, 166	twisted pair	18, 23, 25	Wireless Local Loop	42		
Small Form-Factor Pluggable	54	Twisted-Pair-Kabel	10	Wireless Personal Area Network	47		
SMDS	173	U					
SNMP	68	Übersichtspläne	123	Wireless Protected Access	129		
Spanning Tree	52	Übersprechen	24, 92	Wireless Repeater	127		
SPB	52	Übertragungssysteme	7	WLAN	126		
Spleiß, mechanischer	38	Überwachung, Schränke	67	WLAN, Client-Konfiguration	135		
Spleiß, thermischer	38	UMTS	170	WLAN, Fehlersuche	135		
Spreizband-Verfahren	44	Unicast	153	WPA	129		
SSID	43, 46, 127, 128	Universalanschluss	9	WPA2	129, 135		
SSID-Broadcast	128	Up-Link-Modul	136	WWAN	179		
Standortverteiler	107, 117	Uplink-Port	54	X			
Statisches Routen	154	Upstream	167, 169	X.25	173		
Stecker, ARJ45	70	UTP	25	Z			
Stecker, FC	39, 71	VCSEL	32	Zielplanung	113		
Stecker, GG45	70	VDSL	167, 169	Zutrittskontrolle	69		
Stecker, LC	39	Verdrahtungsmessung	91				
Stecker, MPO	71	Verdrillung	23				
Stecker, MTRJ	71	Verfügbarkeitsverbund	7				
Stecker, RJ-45	70						
Stecker, SC	39, 71						
Stecker, ST	71						
Stecker, TERA	70						