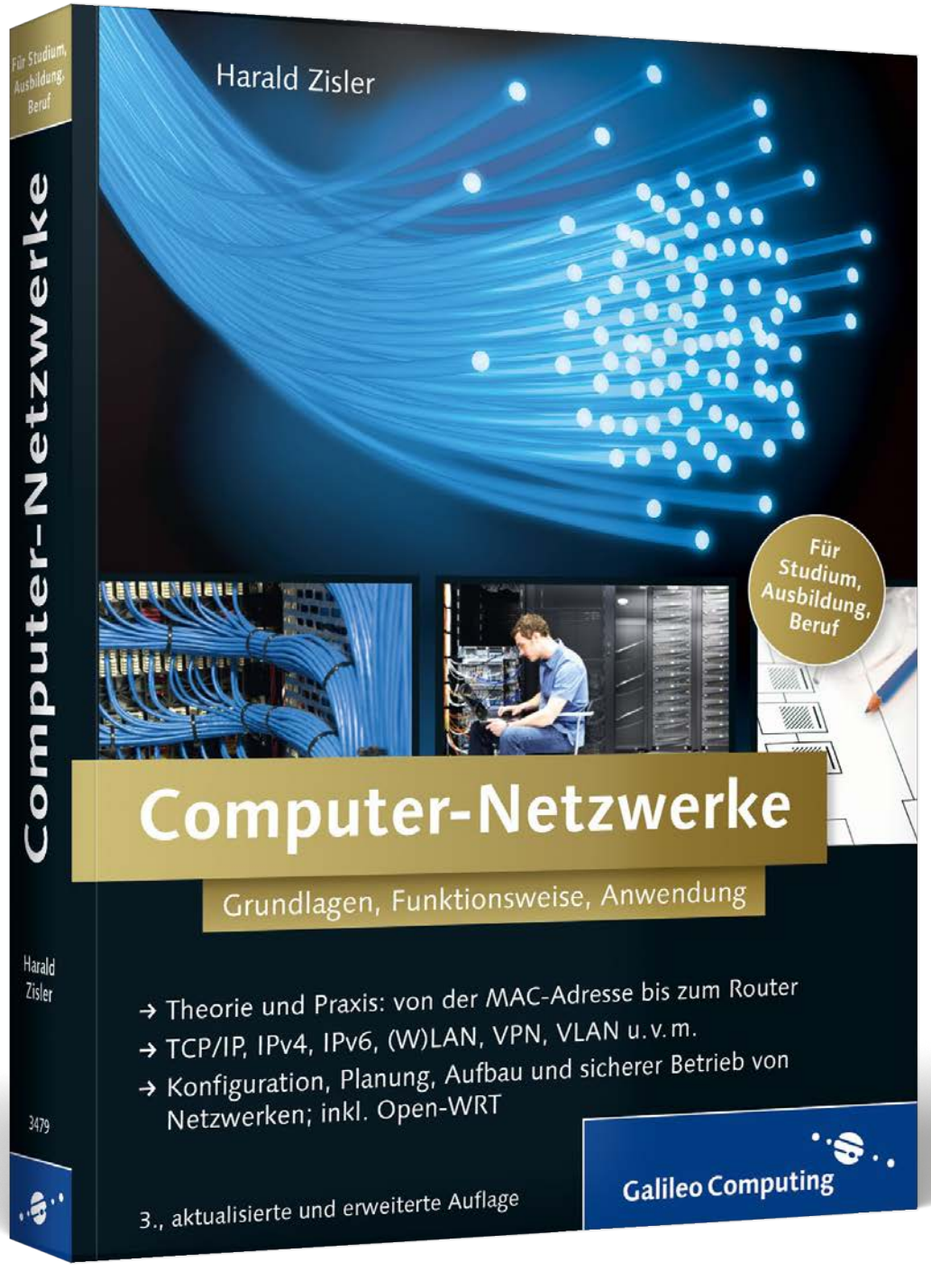


Leseprobe

Harald Zisler bietet Ihnen in dieser Leseprobe einen schnellen und unkomplizierten Zugang zu Theorie und Praxis von Computer-Netzwerken. Außerdem können Sie einen Blick in das vollständige Inhalts- und Stichwortverzeichnis des Buches werfen.

Harald Zisler

Computer-Netzwerke – Grundlagen, Funktionsweise, Anwendung

434 Seiten, broschiert, 3. Auflage 2014
24,90 Euro, ISBN 978-3-8362-3479-5

www.galileo-press.de/3758

Kapitel 1
Grundlagen moderner Netzwerke

Netzwerke sind Infrastruktureinrichtungen für den Daten- und Nachrichtentransport. Wie die Transporteinrichtungen auf der Schiene, der Straße, zu Wasser und in der Luft müssen sie auf maximales Transportaufkommen und hohe Betriebssicherheit hin ausgelegt werden.

Heute kommunizieren Sie weltweit über verschiedene Netzwerke hinweg. Im Idealfall funktioniert die Vernetzung so unauffällig, dass Sie weder eingreifen noch irgendwelche besonderen Dinge tun müssen. Sie versenden E-Mails, lesen Nachrichten, schauen Fernsehen, verlagern rechenintensive Vorgänge in eine »Cloud« oder arbeiten zu Hause an Ihrem Heimarbeitsplatz, stets vernetzt mit dem Rest der Welt.

Den Unterbau hierfür bildet die Netzwerktechnik, die zu Hause, in den Vermittlungsstellen der Telekommunikationsdienstleister oder in den Betrieben installiert ist. Hier wird gesendet, empfangen, weitergeleitet oder auch abgeblockt.

Ihr Netzwerk nehmen Sie meist nur wahr, wenn es nicht funktioniert. Spätestens dann sollten Sie die Grundlagen, die ich in diesem Buch beschreibe, kennen. Neben diesem Buch empfehle ich Ihnen noch, folgende Grundlagen- und weiterführende Literatur durchzuarbeiten:

- Tanenbaum, Andrew S./Wetherall, David J.: *Computernetzwerke.* 6., aktual. Aufl. München: Pearson Education 2014. ISBN 978-3-8689-4237-8.
- Lienemann, Gerhard/Larisch, Dirk: *TCP/IP – Grundlagen und Praxis.* 2., aktual. Aufl. Heidelberg: dpunkt 2013. ISBN 978-3-944099-02-6.
- Gerhard Lienemann: *TCP/IP – Praxis.* 3., aktual. Aufl. Hannover: Heise 2003. ISBN 978-3-936931-05-1.
- Hagen, Silvia: *IPv6. Grundlagen – Funktionalität – Integration.* 2. Aufl. Norderstedt: Sunny Edition 2009. ISBN 978-3-9522942-2-2.
- Blanchet, Marc: *Migrating to Ipv6.* 1. Aufl. Chichester: Wiley 2006. ISBN 978-0-471-49892-6.

- Kersken, Sascha: *IT-Handbuch für Fachinformatiker.* 6., aktual. u. erw. Aufl. Bonn: Galileo Press 2013. ISBN 978-3-8362-2234-1.
- Anderson, Al/Benedetti, Ryan: *Netzwerke von Kopf bis Fuß.* 1. Aufl. Köln: O'Reilly 2009. ISBN 978-3-89721-944-1.

1.1 Definition und Eigenschaften von Netzwerken

Die moderne Netzwerktechnik arbeitet *paketorientiert*. Es gibt keine einzigartigen, exklusiven 1:1-Verbindungen wie beim Telefon. Ihr Rechner sendet und empfängt die Informationen häppchenweise über eine offene Struktur. In dieser finden die Datenpakete automatisch ihren Weg zum Ziel. Ausfälle einzelner Netzwerkkomponenten führen nicht zum Abbruch der Kommunikation, solange es sich nicht gerade um den eigenen Zugang zum Internet oder Netzwerk handelt.

Netzwerk

Ein Netzwerk stellt eine Infrastruktur dar, die Datenendgeräten

- die (wahlfreie) Kommunikation untereinander,
- den Datenaustausch und
- die Nutzung gemeinsamer Ressourcen und Dienste

transparent ermöglicht.

Bei modernen Netzwerken müssen Sie sich nicht um die Einzelheiten der Verbindung kümmern. Das erledigt das »Netz« nach vorgegebenen Regeln, den *Netzwerkprotokollen*, selbst (siehe auch Tabelle 1.1). Die heutzutage gebräuchliche Protokollfamilie trägt den Namen *TCP/IP*.

Netzwerkprotokoll

Die Aufgabe eines Netzwerkprotokolls ist das Festlegen der Modalitäten für den Aufbau und das Trennen von Verbindungen, den Austausch von Daten und das Verhalten im Fehlerfall.

Netzwerkprotokolle stellen die Schicht zwischen der Hardware (Netzwerkkarte, Modem, funktechnische Einrichtung ...) und der jeweiligen Anwendung bzw. dem Anwender dar, der mit ihnen kommuniziert.

Die Netzwerkprotokolle benutzen verschiedene Methoden, um ihre Aufgaben mehr oder weniger zuverlässig erfüllen zu können (Tabelle 1.1).

Aufgabe	Umsetzung/Methode
Adressierung	Adressangaben, Übermittlung von Empfänger und Absender
Verbindungssteuerung	Befehle für den Aufbau und Abbau von Verbindungen
Flusssteuerung	Transportquittungen, Regelung des Datenflusses durch Start-/Stopp-Anweisungen
Fehlererkennung	Prüfsummen, Quittungen, Verfallszeit (Time-out) überwachen, Nummerierung der Informationsblöcke
Fehlerkorrektur	Anforderung von Paketwiederholungen, Korrekturverfahren

Tabelle 1.1 Aufgaben von Netzwerkprotokollen

Durch die frei zugänglichen Standards, die mit den Netzwerkprotokollen gegeben sind, funktioniert die Kommunikation heute zwischen den unterschiedlichsten Geräten (Abbildung 1.1). Es ist vollkommen egal, ob es sich um einen Großrechner oder ein VoIP-Telefon handelt oder welches Betriebssystem ein Laptop benutzt: alle Teilnehmer werden vom Netz gleichermaßen bedient. Es liegt ein *heterogenes* Netz vor, in dem die Partner mehr oder weniger gleichberechtigt miteinander verbunden sind.

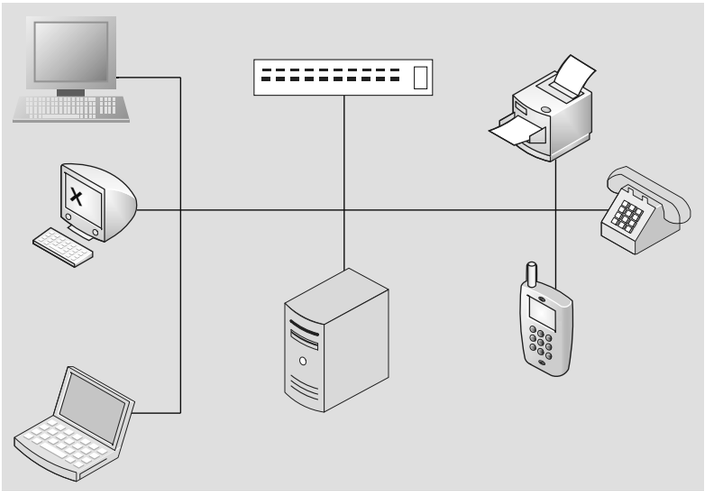


Abbildung 1.1 Heterogenes Netzwerk

Netzwerkprotokolle arbeiten entweder *verbindungsorientiert* oder *verbindungslos*. Beides bietet Vor- und Nachteile. Sie finden bis heute keine klare Befürwortung oder gar Lehrmeinung zugunsten der (alleinigen) Verwendung eines der beiden Verfahren. In der Praxis wurde die akademische Diskussion dagegen schon entschieden. Verfügt eine Anwendung selbst über transaktionssichernde Maßnahmen (z. B. Datenbank), wird normalerweise den verbindungslosen Protokollen der Vorzug gegeben. Anwendungen ohne eigene übertragungssichernde Methoden verwenden meist die verbindungsorientierten Protokolle, z. B. *telnet* für Fernsitzungen oder *ftp* für Datenübertragungen.

Verbindungsorientiertes Netzwerkprotokoll

- Aufbau einer Verbindung zwischen den Kommunikationspartnern vor der Datenübertragung
- Die Kommunikationspartner geben sich untereinander gegenseitig zu erkennen, bevor die Nutzdaten übertragen werden.
- Abbau einer Verbindung nach der Datenübertragung
- Vorteil: höhere Sicherheit der Verbindung
- Nachteil: höhere Rechner- und Netzwerkbelastung

Verbindungsloses Netzwerkprotokoll

- Daten werden in in sich geschlossenen Datagrammen »auf gut Glück« versandt.
- Vorteil: höherer Datendurchsatz, weniger Netzlast
- Nachteil: Flusskontrolle und Fehlerkorrektur nehmen übergeordnete Schichten (Anwendungen) vor, was zu höherer Rechnerbelastung führt.

1.2 Die Netzwerkprotokollfamilie TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) ist die Netzwerkprotokollfamilie unserer Tage. Dabei ist sie älter als manche andere, die schon wieder Geschichte ist. Erste Grundlagen stammen bereits aus den 1960er-Jahren. In den 1970er-Jahren rief die US-Regierung das ARPA-Projekt (Advanced Research Projects Agency) ins Leben, das die Netzwerktechnologie vor allem hinsichtlich militärischer Nutzbarkeit weiterentwickelte. Bereits 1974 aber wurde eine neue Protokollbasis geschaffen. R. Kahn, V. Cerf und Y. Dalal legten in RFC 675 die noch heute gültigen Grundzüge der TCP/IP-Protokollfamilie fest. Diese sollten Sie kennen, wenn Sie sich eingehender mit Netzwerken befassen.

Grundzüge der TCP/IP-Protokollfamilie

- architekturunabhängige Netzwerktechnologie
- Verbindungen von und zu allen Netzwerkteilnehmern
- Quittungen bei Verbindungen
- Anwendungsprotokolle nach allgemeinen Standards
- Vermittlungsebene mit verbindungslosem Protokoll
- Paketvermittlungsrechner als Netzknoten
- Sicherungsfunktionen in Transportprotokollen
- dynamisches Routing
- standardisierte Netzwerk-Anwendungsprogramme

Der Siegeszug der TCP/IP-Protokollfamilie begann mit der Implementierung im UNIX-Derivat 4.2BSD, des ein Projekt der Universität von Kalifornien in Berkeley ist. Nach US-Recht gehören Entwicklungen und Forschungsergebnisse von öffentlichen Forschungs- und Bildungseinrichtungen dem amerikanischen Volk und sind damit für jedermann verfügbar. So konnten Hersteller anderer Betriebssysteme günstig darauf zurückgreifen, und die IT-Welt blieb damit von verschiedenen Auslegungen der Protokolle verschont.

1.3 OSI-Schichtenmodell und TCP/IP-Referenzmodell

Schichtenmodelle erklären anschaulich das Zusammenspiel von Hardware, Netzwerkprotokollen und Anwendungen. Sie helfen Ihnen, auch scheinbar komplizierte Vorgänge leichter zu verstehen. Unabhängig von tatsächlich existierenden Hard- und Softwareprodukten finden Sie die einzelnen Instanzen und deren Verknüpfungen untereinander übersichtlich dargestellt. Die Modelle helfen Ihnen, Ihre Netzwerke zu planen, aufzubauen und zu unterhalten.

Es ist aber nicht so, dass in einem Schichtenmodell (und in der Realität) die Schichten der gleichen Ebene miteinander kommunizieren! Der Weg der Information läuft von oben nach unten zum Übertragungsmedium und von dort aus wieder von unten nach oben (Abbildung 1.2).

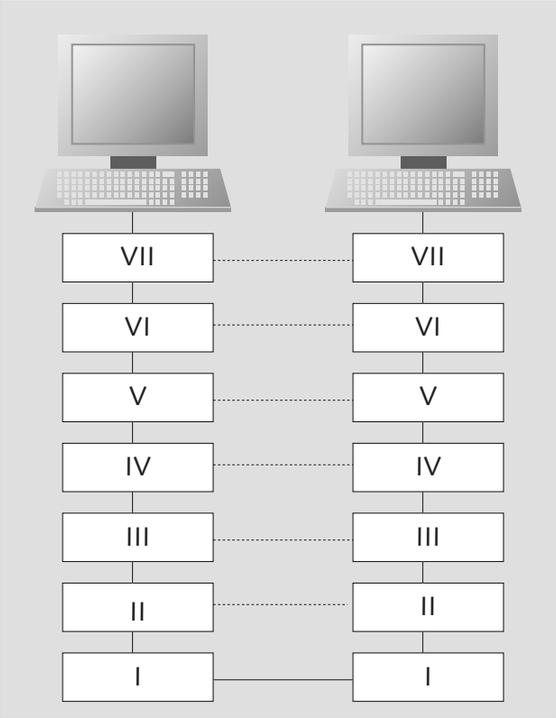


Abbildung 1.2 Virtuelle (gestrichelte, waagrechte Linien) und die reale Kommunikation im OSI-Schichtenmodell

Grundsätzlich gilt für alle Netzwerk-Schichtenmodelle

- Eine Ebene in einem Schichtenmodell stellt ihre Dienste der darüberliegenden Ebene zur Verfügung.
- Eine Ebene eines Schichtenmodells nimmt die Dienste der unter ihr liegenden Ebene in Anspruch.
- Schnittstellen bilden den Übergang zwischen den einzelnen Schichten.
- Innerhalb einer Schicht kommen Protokolle zum Einsatz. Diese ermöglichen die Kommunikation innerhalb dieser Ebene.
- Eine Veränderung in einer niedrigeren Schicht bewirkt keine Änderung in den darüberliegenden Ebenen (z. B. zieht der Wechsel einer Netzwerkkarte keine Neuinstallation eines Webservers nach sich).

- Eine Veränderung in einer höheren Ebene bewirkt keine Änderung in den darunterliegenden Ebenen (z. B. benötigt ein Software-Update für einen Webserver keine neue Netzwerkkarte).
- Die Schichtenmodelle stellen die verschiedenen Funktionsebenen einheitlich dar.
- Bei der täglichen Arbeit hilft Ihnen ein Schichtenmodell bei der Beschreibung von Problemen beim Betrieb von Netzwerken.
- Bei der Beschaffung von Netzwerkkomponenten greifen die Anbieter in ihren Produktbeschreibungen ebenfalls auf Begriffe aus Schichtenmodellen (meist OSI) zurück. Schon aus diesem Grund sollten Sie damit vertraut sein.
- Sie können mit einem Schichtenmodell komplizierte Vorgänge verständlicher darstellen.

Das *OSI-Schichtenmodell* (Open Systems Interconnection Model; ISO 7498-1, DIN ISO 7498) wurde von der *International Organization for Standardization* (*ISO*) bereits 1984 als Modell für die Kommunikation zwischen Rechnern entworfen. Es besteht aus sieben in sich abgeschlossenen Schichten (Tabelle 1.2).

Layer/ Ebene	Bezeichnung	Betrifft
VII	Anwendungsschicht/ Application Layer	Interaktion mit Anwendungen, die Netzwerkzugriff benötigen, Server-Client-Anwendungen
VI	Darstellungsschicht/ Presentation Layer	standardisierte Kodierungs-, Konvertierungs- und Kompressionsverfahren, z. B. MPEG, TIFF, GIF, ASCII
V	Kommunikationsschicht/Session Layer	Anforderung von Sitzungen und Datenströmen, Zweiwegekommunikation von Anwendungen verschiedener Endgeräte, z. B. SMB-Protokoll für Druck und Verbindung zu Windows-Freigaben
IV	Transportschicht/ Transport Layer	Flusskontrolle, verbindungslose und verbindungsorientierte Dienste, Kommunikationskontrolle, Verbindungsauf- und -abbau, Kommunikation zwischen Netzwerk und Anwendung, TCP- und UDP-Protokoll
III	Vermittlungsschicht/ Network Layer	Routing, logische Adressierung, IP-Protokoll, Quality of Service

Tabelle 1.2 OSI-Schichtenmodell

Layer/ Ebene	Bezeichnung	Betrifft
II	Sicherungsschicht/ Data Link Layer	Flusssteuerung, Datenübertragung, Zugriffssteuerung, Fehlererkennung, MAC-Adressen
I	physikalische Schicht/ Physical Layer	Kupfer- und Glasfaserkabel, Signalformen, Wellenlängen bei optischer Übertragung, Funkfrequenzen für WLAN, Richtfunk, UMTS usw. und kabelgebundene Übertragung im LAN, MAN oder WAN

Tabelle 1.2 OSI-Schichtenmodell (Forts.)

Für die TCP/IP-Protokollfamilie existiert ein eigenes Referenzmodell. Dessen Aufbau ist weitaus weniger detailliert als der des OSI-Schichtenmodells und orientiert sich vielmehr an der Zusammenarbeit innerhalb der TCP/IP-Protokollfamilie (Tabelle 1.3).

TCP/IP-Schicht	Enthält	Entspricht OSI-Schicht
Anwendungsschicht/ Application Layer	FTP, HTTP, POP, SMTP, SSH, TELNET, NFS-MOUNT, DNS ...	V bis VII
Transportschicht/ Transport Layer	TCP, UDP, SCTP	IV
Internetschicht/ Internet Layer	Internetprotokoll (IPv4, IPv6)	III
Netzzugangsschicht/ Link Layer, Host to Network	Techniken für Punkt-zu-Punkt-Datenübertragungen (z. B. PPP)	I und II

Tabelle 1.3 TCP/IP-Referenzmodell im Vergleich mit dem OSI-Schichtenmodell

Das sind die wesentlichen Unterschiede zum OSI-Schichtenmodell:

- Das TCP/IP-Referenzmodell gilt nur für die TCP/IP-Protokollfamilie. Das OSI-Schichtenmodell ist dagegen neutral, Sie können es auf alle Netzwerke anwenden.
- Das TCP/IP-Referenzmodell benutzt weniger Ebenen.
- Das OSI-Modell benutzt eine Ebene nur für Hardware.
- Das TCP/IP-Referenzmodell verschmilzt die OSI-Ebenen I und II sowie V, VI und VII. Es ist damit weniger detailliert.

1.4 Räumliche Abgrenzung von Netzwerken

Zum Netzwerker-Latein gehören auch Begriffe, mit denen Sie die räumlichen Begebenheiten eines Netzwerkes beschreiben können. Schließlich gibt es Komponenten, die Sie im Haus, auf dem Grundstück oder gar weltweit verwalten und warten müssen. Die Bezeichnungen benötigen Sie auch oftmals beim Erstellen von Netzplänen.

Räumliche Netzwerkbereiche

- **LAN** (Local Area Network): innerhalb eines Gebäudes
- **MAN** (Metropolitan Area Network): Verbindungen zwischen Gebäuden in der Nähe (Grundstück, Stadtgebiet, Campus)
- **WAN** (Wide Area Network): Fernstrecken, weltweit
- **Intranet**: privates, nicht öffentliches Datennetzwerk (LAN bis WAN von der Ausdehnung her möglich)
- **Internet**: weltweites, öffentliches Datennetzwerk

1.5 Regel- und Nachschlagewerk für TCP/IP-Netze (RFCs)

»Wissen, wo es geschrieben steht« ist auch im Netzwerkbereich wichtig. Die Regeln der TCP/IP-Protokollfamilie sind in den *Requests for Comments* (*RFC*) in englischer Sprache festgelegt. Sie finden sie im Internet unter *http://www.rfc-editor.org*. Sie benötigen diese, wenn Sie Programme mit Netzwerkbezug schreiben wollen, oder ganz einfach dann, wenn Sie eine Leistungsbeschreibung erstellen. Aber auch bei Funktionsübersichten von Netzwerkgeräten werden oft nur die RFC-Nummern angegeben – Details können Sie dann in diesen selbst nachlesen.

Bei umfangreichen Fundstellen in den RFCs habe ich deren Nummern einfach der Reihe nach angegeben. Für manche Themen existieren oftmals mehrere, gleichwertige Dokumente, durch die Sie sich durcharbeiten sollten. Damit Sie aber zu manchen Themen die »Einstiegs-RFCs« leichter finden, habe ich diese **fett** hervorgehoben.

Die RFCs unterliegen gewissen Sprachregelungen. Sie schaffen Klarheit und Eindeutigkeit. Sie geben auch Auskunft über den Status (Tabelle 1.4) und die Verwendbarkeit der jeweiligen Regel (Tabelle 1.5), die Sie mehr oder weniger in jedem RFC-Dokument mit dem jeweiligen Schlüsselbegriff hinterlegt finden.

Status	Bedeutung
Proposed Standard	Spezifikation des (künftigen) Standards
Experimental	Testphase außerhalb von Produktivumgebungen
Draft Standard	Vorstufe zum Standard, nach mindestens zwei voneinander unabhängigen Implementierungen und vollständiger Protokollprüfung
Standard	anzuwendendes, verbindliches Protokoll
Informational	lesenswerte Information
Historic	veraltet, keine Verwendung

Tabelle 1.4 Statusangaben der RFCs

Verwendbarkeit	Anwendung der Regel ist
required	zwingend
recommended/suggested	empfohlen
elective	freigestellt
limited use	eingeschränkt
not recommended	nicht empfehlenswert

Tabelle 1.5 Angaben zur Verwendbarkeit von RFCs

Wenn Sie hier im Buch Angaben von RFC-Nummern finden, so können Sie diese auf der IETF-Seite (*http://www.ietf.org*) aufrufen und lesen. In manchen Kapiteln begegnet Ihnen eine wahre Flut dieser Nummern. Hier geben Sie auf der IETF-Seite einen Begriff anstelle der vielen RFC-Nummern ein. Sie erhalten eine Auflistung mit Links zu den Dokumenten als Ergebnis. Im Buch aufgeführte und nicht in der Auflistung enthaltene RFCs können Sie im Anschluss dann einzeln aufrufen, falls notwendig.

1.6 Prüfungsfragen

1. Wann sind RFC-Dokumente verbindlich anzuwenden?
2. Sie verbinden auf einem Werksgelände mehrere Gebäude. Wie bezeichnen Sie ein derartiges Netzwerk?

Die Auflösungen finden Sie in Anhang B, »Auflösungen zu den Prüfungsfragen«.

Kapitel 2
Netzwerktechnik

Kabel und Funkstrecken bilden den Unterbau des Datenverkehrs.
Sie müssen unabhängig von den Netzwerkprotokollen funktionieren.

In der Umgebung von Datennetzwerken finden Sie Kabel, Stecker und Antennen. In einem Gebäude können Sie auf verschiedene Entwicklungsstufen der Netzwerktechnik treffen. Oftmals ist ein Netzwerk über Jahre gewachsen. Auch das Anwendungsumfeld bestimmt die eingesetzte Technik. Bereiche wie der Maschinenbau setzen vor allem auf eingeführte und bewährte Komponenten. Ihnen begegnen hier deshalb Verkabelungen, die in der Bürokommunikation schon länger kaum noch eingesetzt werden. Aus diesem Grund habe ich hier auch ältere und sehr alte Standards dargestellt.

Die Darstellung physikalischer Details der einzelnen Standards überlasse ich meist der nachrichtentechnischen Literatur:

- Werner, Martin: *Nachrichtentechnik. Eine Einführung für alle Studiengänge.* 7., erw. u. aktual. Aufl. Wiesbaden: Vieweg+Teubner 2010. ISBN 978-3-8348-0905-6.
- Meyer, Martin: *Kommunikationstechnik. Konzepte der modernen Nachrichtenübertragung.* 5., korr. Aufl. Wiesbaden: Vieweg+Teubner 2014. ISBN 978-3-658-03375-0.
- Sauter, Martin: *Grundkurs Mobile Kommunikationssysteme. UMTS, HSDPA und LTE, GSM, GPRS, Wireless LAN und Bluetooth.* 5., überarb. u. erw. Aufl. Wiesbaden: Vieweg+Teubner 2013. ISBN 978-3-658-01461-2.

Ich stelle Ihnen die Technik vor allem aus dem Blickwinkel von Planern, Beschaffern und Betreuern vor, also nach Anforderungen und Leistungsmerkmalen. Im OSI-Schichtenmodell finden Sie die elektrische und optoelektronische Netzwerkausrüstung im Layer 1 (physikalische Schicht). Das TCP/IP-Referenzmodell weist hierfür die Netzzugangsschicht (Link Layer) zu.

2.1 Elektrische Netzwerkverbindungen und -standards

Standards im Netzwerkbereich helfen Ihnen, überhaupt ein funktionierendes Netzwerk aufzubauen. Genormte Kabel, Stecker, Funkfrequenzen und -modulationsverfahren ermöglichen es Ihnen, Geräteeinheiten verschiedener Hersteller miteinander zu verbinden.

Standards im Netzwerkbereich tragen natürlich Bezeichnungen, zum einen welche für die Verkabelung, zum anderen für das Regelwerk.

Verkabelungsbezeichnungen bei Netzwerken

Die Bezeichnung des Verkabelungstyps wird aus der Angabe der maximalen Übertragungsrate, der Übertragungstechnik, der maximalen Segmentlänge (Zahl) oder des Kabels gebildet:

[ÜBERTRAGUNGSRATE][ÜBERTRAGUNGSTECHNIK][KABEL]

100Base-TX bedeutet eine maximale Übertragung von 100 Mbit/s im Basisband und die Verwendung von verdrillten Adernpaaren (Twisted Pair) in Kupfertechnik. Der Begriff *Basisbandübertragung* sagt aus, dass der vom Nutzsignal verwendete Frequenzbereich gleich dem übertragenen ist.

Während Sie auf die obige Verkabelungsbezeichnung in allen Katalogen und Produktbeschreibungen stoßen, begegnen Ihnen die IEEE-Nummern eher selten. Aber auch diese sollten Ihnen geläufig sein.

IEEE-Standards

Das *Institute of Electrical and Electronics Engineers (IEEE)* legt unter anderem auch Standards für die Netzwerktechnik fest, die auch als ISO-, EN- und DIN-Normen übernommen werden.

Kabel oder Funk? Bei den elektrischen Netzwerkverbindungen können Sie zwischen diesen beiden Möglichkeiten wählen oder sie auch kombinieren.

Vor- und Nachteile elektrischer, kabelgeführter Netzwerke

Vorteile:

- kostengünstige Verkabelung
- Endgeräte (Netzwerkkarten, Switches ...) verbreitet und preiswert
- Verlege- und Verkabelungsarbeiten ohne großen Aufwand durchführbar

Nachteile:

- elektrisches Potenzial führend
- benötigt eigene Trassenführung
- Störungen durch äußere elektromagnetische Felder möglich

Vor- und Nachteile funkgestützter Netzwerke (WLAN)

Vorteile:

- (fast) keine Installationsarbeiten
- volle Flexibilität innerhalb von Räumen
- weniger »Kabelsalat« um den PC herum

Nachteile:

- Frequenzressourcen müssen mit anderen geteilt werden
- nicht abhörsicher
- nicht sicher vor Störungen und störenden Beeinflussungen
- für die Datensicherheit hoher Aufwand notwendig (stets neueste Kryptografietechnik)
- In der Rechtsprechung gilt bei missbräuchlicher Nutzung durch Dritte oftmals Betreiberhaftung.
- langsamere Datenübertragung als bei kabelgebundener Technik
- höherer Anschaffungspreis
- Zuverlässige Funkverbindungen können nicht immer garantiert werden (z. B. Stahlbetondecken und -wänden, Altbauten mit dicken Vollziegel- oder Granitmauern).

Jetzt lernen Sie zunächst die Netzwerkstandards kennen. Damit erhalten Sie Auskunft über die Leistungsfähigkeit und teilweise über die technischen Mindestanforderungen bei der Verkabelung. Sie können nämlich größtenteils Endgeräte mit verschiedenen Standards miteinander in einem Netz betreiben, wenn die Verkabelung dem neuesten Standard entspricht. Im Klartext bedeutet das, dass Sie beispielsweise einen alten Printserver, der Daten mit 10 Mbit/s erhalten kann, in einem Gigabit-LAN weiter betreiben können (wenn Ihnen die Geschwindigkeit so ausreicht).

2.1.1 Netzwerke mit Koaxialkabeln

Falls Sie von zeitgemäßer Hardware umgeben sind, überspringen Sie einfach diesen Abschnitt. Wenn Sie bei »Ausgrabungen« in einem weitläufigen Netzwerk auf recht kurios wirkende Netzwerkgegenstände stoßen, dann lesen Sie hier weiter. Bei alten, »gewachsenen« Bestandsnetzen oder auch im Maschinenbau treffen Sie immer noch die »Altlasten« vom Beginn der Netzwerktechnik an, weshalb ich deren Funktion hier erkläre. In der Praxis werden Sie diese Gerätschaften stets durch neue Technik ersetzen.

10Base-5, IEEE 802.3, Clause 8, Thicknet, Yellow Cable

Das klassische Ethernet verwendet Koaxialkabel als Medium. Sie müssen die beiden Kabelenden mit einem Schluckwiderstand (50 Ω) abschließen, da sich sonst stehende Wellen ausbilden können. Diese führen zu Spannungsmaxima und -minima im Leitungsweg und stören damit die Kommunikation. (Achtung Physik: Das Kabel hat 50 Ω Wellenwiderstand, Stehwellen bauen sich in Abhängigkeit von Frequenz und Leiterlänge [Resonanzlängen] auf.)

Beim *Thick Wire* wurde der Anschluss über die sogenannte *Medium Access Unit* (*MAU*) hergestellt. Die MAU-Einheit verfügt über einen teilisolierten Stachel (*Vampire Tab*), der das Schirmgeflecht des Koaxialkabels durchdringt. Das leitende Stachelende dringt in den Innenleiter ein und stellt damit die elektrische Verbindung her. An dieser Vorrichtung finden Sie auch den *Transceiver*, der wie in der Funktechnik auch für das Senden und Empfangen zuständig ist. Über ein bis zu 15 m langes Kabel war damit das *Attachment Unit Interface* (*AUI*) verbunden, das über eine SUB-D-15-Steckverbindung am Ethernet-Controller des Netzwerkteilnehmers angeschlossen war.

10Base-2, IEEE 802.3, Clause 10, Thin Wire Ethernet, Cheapernet

Beim *Thin Wire Ethernet* kann das Kabel mittels T-Stück direkt mit dem Teilnehmergerät verbunden werden (AUI und MAU sind schon in der Netzwerkkarte integriert). Die Verlegung und die Anschlüsse müssen nach genauen Regeln erfolgen, andernfalls ist ein Totalausfall des Netzes sehr wahrscheinlich.

Bei den Koaxialkabel-Netzen existiert kein zentrales Gerät, das einen Knoten bildet. Vielmehr liegt eine Bus-Struktur (Abbildung 2.1) vor. Darum musste das Kabel durch jeden Raum gezogen werden, von dem nur vermutet wurde, dass hier einmal irgendetwas angeschlossen werden könnte.

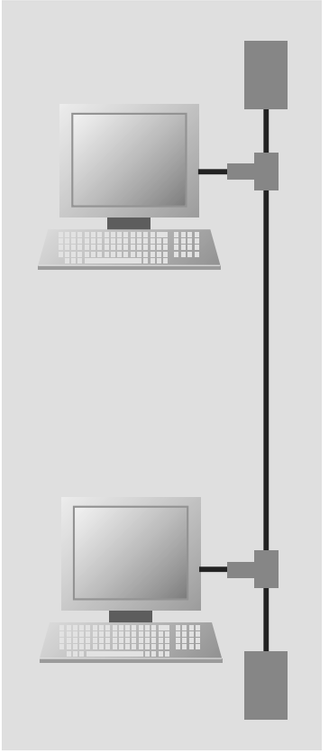


Abbildung 2.1 Bus-Struktur von Netzwerken mit Koaxialkabeln

Die Netzwerkteilnehmer teilen sich die »Ressource« Koaxialkabel; Sie können sich dies wie einen Funkverkehrskreis vorstellen. Über das Verfahren *Carrier Sense Multiple Access/Collision Detection* (*CSMA/CD*) wird erreicht, dass stets nur ein Teilnehmer sendet. Im Kollisionsfall wird das *Jam-Signal* gegeben, worauf jeglicher Sendeverkehr verstummt, bevor nach einiger Zeit ein Teilnehmer wieder aktiv wird. Dieses Verfahren verhindert damit aber hohe Übertragungsraten.

Die Verwendung von Koaxialkabeln bringt einen hohen Grad an Funkentstörung mit sich, der meist nur von der Glasfaser übertroffen wird. Ein Teilnehmer kann entweder senden oder empfangen (Halbduplex-Verfahren). Die (theoretische) Übertragungsrate beträgt in allen Fällen 10 Mbit/s. Die wichtigsten Daten finden Sie in Tabelle 2.1.

Eigenschaften	Thicknet	Thinnet
Weitere Namen	Yellow Cable	Cheapernet
Bezeichnung	10Base-5	10Base-2
Norm	IEEE 802.3, Clause 8	IEEE 802.3, Clause 10
Kabel	RG-8	RG-58 (Abbildung 2.2)
Anschluss	MAU-AUI	BNC
Maximale Länge	500 m	185 m
Nutzungshinweise	maximal 100 angeschlossene Transceiver	maximal 30 Teilnehmer

Tabelle 2.1 Daten von Netzwerken mit Koaxialkabeln

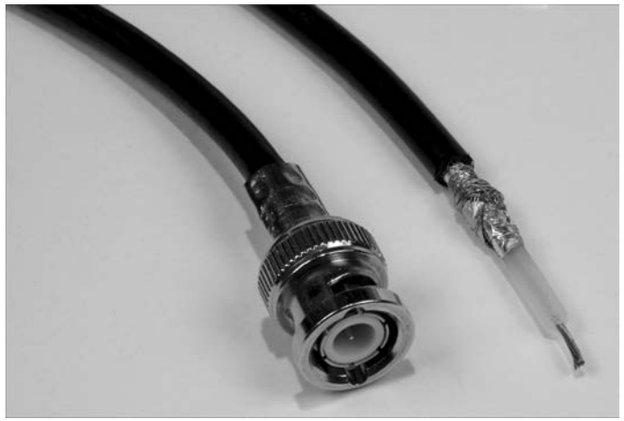


Abbildung 2.2 BNC-Stecker und Koaxialkabel Cheapernet (10Base-2)

2.1.2 Netze mit Twisted-Pair-Kabeln

Die Verkabelung mit Koaxialkabeln stieß natürlich bald an ihre Grenzen. Die mangelnde Erweiterbarkeit und vor allem die unpraktische Leitungsführung zu den Arbeitsplätzen hemmten den Ausbau der Netzwerktechnik enorm. Durch die Entwicklung zentraler Komponenten, die einen Netzknoten bilden können (Hub, Switch), konnte

man nun eine sternförmige Netzwerkstruktur (Abbildung 2.3) anlegen. Die Verkabelung dafür wird mit Kabeln ausgeführt, die verdrillte Adernpaare besitzen. Diese Vereinfachung ermöglicht nicht nur eine übersichtlichere Installation, sondern auch fast immer einen höheren Datendurchsatz, da das Endgerät allein mit dem Knotengerät kommuniziert.

Alle Netze mit *Twisted-Pair-Kabeln* (*TP*) verwenden den »*Western-Stecker*« (*RJ45*) und haben eine maximale Länge von 100 m. Alle Teilnehmer können, wenn ein Switch als Netzknoten eingesetzt wird, gleichzeitig senden und empfangen (*vollduplex*). Kommen Hubs zum Einsatz, wird nur *halbduplex* übertragen. Bei Hubs herrschen hinsichtlich der Kollisionen die gleichen Verhältnisse wie bei den Koaxialkabel-Netzen. Weitere Informationen über die Geräte selbst finden Sie in Abschnitt 4.5.2, »Hubs – Sammelschiene für TP-Netze«.

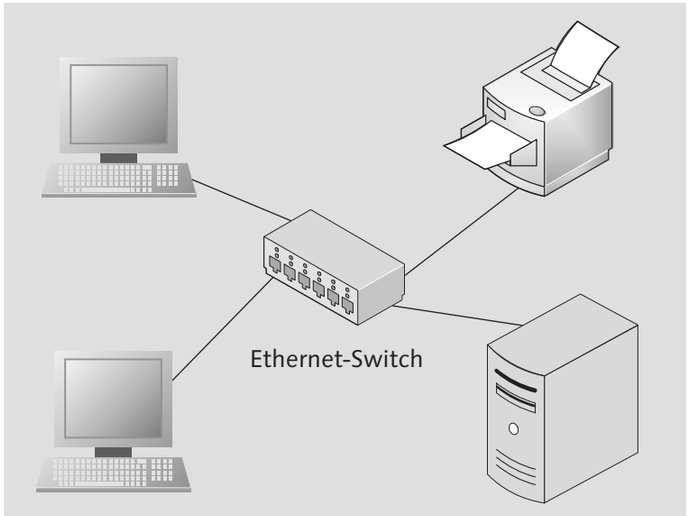


Abbildung 2.3 Sternförmige Netzwerkstruktur

Für Netze mit Twisted-Pair-Kabeln wurden aufeinander aufbauende Standards mit immer höheren Übertragungsraten geschaffen. Die Kabel bekamen dabei zusätzliche Schirmungen. Endgeräte arbeiten mit höheren Frequenzen und effektiveren Übertragungsverfahren. In Tabelle 2.2 finden Sie neben den Kenndaten der Standards auch die notwendigen Kabelkategorien. Damit können Sie auch bei Bestandsnetzen beurteilen, ob ein nächsthöherer Standard angewendet werden kann oder ob Sie neue Kabel nachrüsten müssen.

Bezeichnung	10Base-T	100Base-TX	1000Base-T	10GBase-T
Weitere Namen	Ethernet	Fast Ethernet	Gigabit Ethernet	10 Gigabit Ethernet
Norm	IEEE 802.3j	IEEE 802.3, Clause 25	IEEE 802.3, Clause 40	IEEE 802.3an
Kabel	Cat. 3–7	Cat. 5–7	Cat. 5–7	Cat. 7
Hinweise	Hubs oder Switches als Netzknoten	Switches als Netzknoten	Switches als Netzknoten, Benutzung aller vier Doppeladern zur Unterdrückung von Signalechos	Switches als Netzknoten, Benutzung aller vier Doppeladern zur Unterdrückung von Signalechos

Tabelle 2.2 Übersicht von Netzen mit TP-Kabeln

2.1.3 Aufbau, Bezeichnung und Kategorien von Twisted-Pair-Kabeln

Betrachten Sie Netzwerkabel hinsichtlich Materialqualität, Verarbeitung und Art des Aufbaues. Diese Größen entscheiden, ob die Kommunikation zuverlässig funktionieren wird. Wenn Sie zwei Netzwerkgeräte miteinander verbinden, so fließen die Informationen mittels hochfrequenter Wechselströme durch die kleinen Kupferadern. Wenn Sie schlecht geschirmte Kabel einsetzen, so stört dies bei der Datenübertragung den Radio-, Funk- und Fernsehempfang in der näheren Umgebung. Das ist zum einen nicht zulässig und sorgt zum anderen natürlich für Konflikte mit den Nachbarn.

Achtung Physik: Die nutzbare Lauflänge der Netzwerkkabel wird zum einen durch die Dämpfung beschränkt, zum anderen auch durch die Abflachung der Signalflanken. Der Abflachungseffekt nimmt mit der zurückzulegenden Strecke der Signale zu. Sind die Signalflanken zu breit, können die Netzwerkkarten keine Informationen mehr aus dem Signal auslesen. Sie können das selbst nachvollziehen. Leihen Sie sich ein Oszilloskop aus (Messgerät, mit dem man elektrische Schwingungen am Bildschirm darstellt). Lassen Sie sich das Signal am sendenden Gerät anzeigen. Sie werden mehr oder weniger Rechtecksignale sehen. Nach dem Anschluss beim Empfänger dagegen sehen Sie die Signale trapezförmig.

Gleich noch ein Hinweis aus der Praxis: Sparen Sie nicht an der falschen Stelle. Hochmoderne Gebäudeverkabelung und Patchkabel mit Klingeldraht-Feeling schließen sich aus!

Standards konsequent einhalten

Alle weiteren passiven Netzwerkkomponenten wie

- Patchfelder,
- Wanddosen und
- Patchkabel

müssen dem gleichen oder einem höherwertigen Standard als dem der Gebäudeverkabelung entsprechen. Andernfalls können Normwerte (Reichweite, Signalgüte) nicht eingehalten oder Funkstörungen in der Umgebung hervorgerufen werden!

Zu Netzwerkkabeln finden Sie sowohl Angaben zum Aufbau und zur Schirmung als auch eine Einteilung in eine Kategorie. Sie werden feststellen, dass bei höherwertigen Kategorien auch der Schirmungsaufwand (und natürlich der Preis) steigen.

Wenn Sie ein Netzwerkkabel erwerben möchten, geben Sie die Kategorie an. Der Handel arbeitet mit dieser Bezeichnung. Am Kabelmantel finden Sie normalerweise aber auch die Angaben zum Aufbau und zur Schirmung neben der Kategorie aufgedruckt. Weitere Produktmerkmale können die Vermeidung umweltschädlicher Werkstoffe (z. B. PVC) und eine erhöhte Zug- oder Trittfestigkeit sein.

Angaben zur Schirmung bei Netzwerk- und Fernmeldekabeln

Form:

AA/BCC gemäß *ISO/IEC-11801 (2002)E*

Schirmung (Gesamt- und Adernpaarschirmung):

U ungeschirmt

F Folienschirm

S Geflechtschirm

SF Geflecht- und Folienschirm (nur bei Gesamtschirmung)

Adernanordnung:

TP Twisted Pair (verdrillte Adern)

QP Quad Pair

Die Einteilung in Kabelkategorien finden Sie in Tabelle 2.3. Sie entstand durch die fortschreitende Weiterentwicklung und Verbesserung von Kabeleigenschaften. Höhere Verbindungsgeschwindigkeiten erfordern Kabeltypen, die die Übertragung immer höherer Frequenzen bei immer guten Dämpfungswerten ermöglichen. Für die höchste Kabelkategorie (derzeit Cat. 7) müssen Sie natürlich mit einem höheren Meterpreis als beim »Allerweltskabel« Cat. 5 rechnen. Bei Neuverkabelungen sollten Sie aber nicht unbedingt Kabel und Dosen nach dem älteren Standard einbauen. Sie verlieren schnell die Möglichkeit, Nutzen aus künftigen, schnelleren Standards zu ziehen.

Cat.	Qualität/Verwendung
1	Telefonkabel für analoge Sprach- und Faxübertragungen. Die Adern sind parallel gezogen. Keine Abschirmung, kein Schutz vor Übersprechen oder Beeinflussung von außen. Nicht für Netzwerkzwecke geeignet. Maximale Betriebsfrequenz 100 kHz.
2	wie Cat. 1, aber bis maximal 1 MHz geeignet, »ISDN-Kabel«
3	Geeignet für 10Base-T, Telefon, ISDN. Maximale Betriebsfrequenz 16 MHz, verdrillte Adernpaare, keine Schirmung. Die Verdrillung bietet ein wenig Schutz gegen Übersprechen bzw. störende Beeinflussungen von außen. Das ungeschirmte Kabel kann jedoch Funkanwendungen beim Betrieb stören (Unshielded Twisted Pair, UTP).
4	Nur in den USA verwendet/erhältlich, hier in Europa ohne Belang. Maximale Übertragungsrate 20 Mbit/s, keine Schirmung (UTP).
5	Normen: Class D aus ISO/IEC 11801:2002, EN 50173-1:2002, EIA/TIA-568A-5. In Altanlagen vor 2002 eventuell nicht tauglich für 1000Base-T! Maximale Betriebsfrequenz 100 MHz. Mit Gesamtschirmung üblich (S/UTP, F/UTP oder SF/UTP). Einsatz von 10Base-T bis 1000Base-T möglich. Für 10GBase-T eingeschränkt einsetzbar (maximal 22 m!).
6	Bessere Qualität von Leitung und Schirmung, maximale Betriebsfrequenzen: Cat. 6: 250 MHz, Cat. 6E: 500 MHz.
7	Diese Kabel verfügen über eine äußere Schirmung sowie über eine Einzelschirmung der Adernpaare (S/FTP, F/FTP oder SF/FTP). Sie sind grundsätzlich für alle Anwendungen von 10Base-T bis 10GBase-T geeignet. Die maximale Betriebsfrequenz beträgt 600 MHz. Normen: ISO/IEC-11801 (2002)E, IEEE 802.3an.

Tabelle 2.3 Kabelkategorien

Für die Ergänzung bestehender Netze können Sie meist das SF/UTP-Kabel (Gesamtschirm aus Geflecht und Folie, ungeschirmte, verdrillte Adernpaare) für eine Verkabelung gemäß Cat. 5 verwenden (Abbildung 2.4).

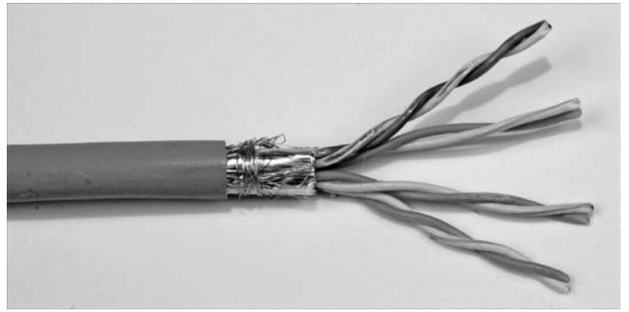


Abbildung 2.4 Netzwerkkabel SF/UTP für Cat.-5-Verkabelung

Wenn Sie umfangreiche Ergänzungen oder Neuerschließungen mit Netzwerkleitungen planen, verwenden Sie aber besser das noch aufwendiger geschirmte Kabel SF/FTP (Abbildung 2.5) gemäß Cat. 7. Hier treten praktisch kaum Übersprecheffekte oder gegenseitige Beeinflussungen der Adernpaare auf, da diese nochmals eine eigene Abschirmung tragen. Natürlich ist dieses Kabel etwas steifer und schwerer.

Abbildung 2.5 Netzwerkkabel SF/FTP nach Cat. 7

2.1.4 Stecker- und Kabelbelegungen

Nachdem Sie den Aufbau und die Verwendbarkeit von Datenleitungen kennengelernt haben, erfahren Sie jetzt einiges darüber, wie diese mit Steckern, Patchfeldern und Anschlussdosen verbunden werden.

Datenleitungen verfügen über acht Adern, die jeweils paarweise verdrillt sind und einen Wellenwiderstand von 100 Ω aufweisen. Somit stehen maximal vier Adernpaare zur Verfügung. Nicht alle Netzwerkstandards nutzen dies aus, eine Zeit lang integrierte man mit einem ungenutzten Adernpaar den Telefonanschluss von Arbeitsplätzen und schuf damit die *Universelle Gebäudeverkabelung (UGV)*. Was sich vor einigen Jahren noch als die geniale Sparlösung erwies, stellt jetzt die große Fortschrittsbremse dar. Sie können kein Gigabit-Ethernet nutzen, weil Sie dafür alle Adernpaare brauchen, eines aber eben für das Telefonnetz benutzt wird. Meist bleibt Ihnen also nur die Möglichkeit, irgendwie eine eigene Telefonverkabelung zu organisieren.

Im Folgenden zeige ich Ihnen, wie die Kabel und Stecker belegt werden. Sie müssen das nicht unbedingt auswendig lernen (außer Ihre tägliche Arbeit besteht künftig im Auflegen von Netzwerk-Anschlussdosen). Hauptsache, Sie wissen, wo Sie die Angaben im Ernstfall schnell nachschlagen können.

Bei der Adernbelegung Ihrer Verkabelung müssen Sie sich an international gültige Normen halten: EIA/TIA-568A (Tabelle 2.4) und/oder EIA/TIA-568B (Tabelle 2.5). Die Belegung ist vom jeweiligen Netzwerkstandard hinsichtlich der benötigten Adernpaare abhängig.

Pin	10Base-T, 100Base-T	1000Base-T	Farbkennzeichnung/Adernfarbe
1	TX+	DA+	weiß/grün
2	TX-	DA-	grün
3	RX+	DB+	weiß/orange
4	frei	DC+	blau
5	frei	DC-	weiß/blau
6	RX-	DB-	orange
7	frei	DD+	weiß/braun
8	frei	DD-	braun

Tabelle 2.4 Belegung nach EIA/TIA T568 A (MDI)

Pin	10Base-T, 100Base-T	1000Base-T	Farbkennzeichnung/Adernfarbe
1	TX+	DA+	weiß/orange
2	TX-	DA-	orange
3	RX+	DB+	weiß/grün
4	frei	DC+	blau
5	frei	DC-	weiß/blau
6	RX-	DB-	grün
7	frei	DD+	weiß/braun
8	frei	DD-	braun

Tabelle 2.5 Belegung nach EIA/TIA T568 B (MDI)

Grundregeln der Netzwerkverkabelung

- Innerhalb der Gebäudeverkabelung wird nur eine Belegungsnorm verwendet. Hauptsächlich kommt EIA/TIA-568B zum Einsatz.
- Verwenden Sie Patchkabel, die alle acht Adern 1:1 verwenden.
- Sonderfall Crosskabel: Ein Ende ist nach EIA/TIA-568A, das andere nach EIA/TIA-568B belegt.
- Schließen Sie stets die Schirmungen an die vorgesehenen Klemmen/Anschlusspunkte an Dosen, Steckern und Patchfeldern an.

Mit einem *Cross-over-Kabel* (Tabelle 2.6) können Sie z. B. zwei PCs ohne eine weitere Komponente (etwa einen Switch) miteinander verbinden. Sie haben die volle Geschwindigkeit zur Verfügung. Wenn Sie nicht mehr Geräte zum Verbinden haben, ist damit Ihr Netzwerk schon komplett. Haben Ihre Rechner mehrere Netzwerkanschlüsse, können Sie eine zusätzliche Verbindung abseits des »Arbeitsnetzes« für Zwecke der Datenhaltung und -sicherung schaffen (Backbone).

Ob es Ihnen gelingt, zwei Netzwerkteilnehmer miteinander zu verbinden, hängt nicht zuletzt von der mediumabhängigen Schnittstelle (*Medium Dependent Interface*, *MDI*) ab. Diese stellt den Zugang zum Übertragungsmedium bei Twisted-Pair-Kabelnetzen her.

Verbindungen mit MDI, MDI-X und Auto-MDI(X)

- **MDI**: Zwei MDIs können Sie nicht mit einem 1:1-Patchkabel verbinden, Sie benötigen hierfür ein Cross-over-Kabel.
- **MDI-X**: Hier sind die Adernpaare entsprechend gekreuzt. Sie können mit einem Patchkabel ein MDI mit einem MDI-X verbinden. Sie benötigen in dem Fall kein Cross-over-Kabel!
- **Auto-MDI(X)**: Bestimmte aktive Netzwerkkomponenten (Switches, Router) sind in der Lage, selbsttätig die Kabelbelegung zu ermitteln, und passen sich automatisch an.

An allen Kabeln kommt der achtpolige »Western-Stecker«, Typ RJ45, zum Einsatz. Die Kontakte sind durchnummeriert (Abbildung 2.6).

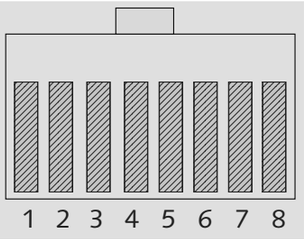


Abbildung 2.6 Belegung RJ45-Stecker, Ansicht von vorne mit oben liegender Rastnase

Die Dose oder ein MDI (Abbildung 2.7) sind damit verkehrt herum belegt.

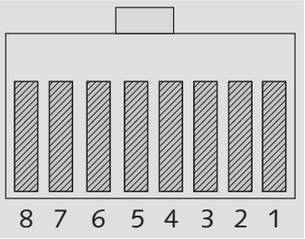


Abbildung 2.7 RJ45-Buchse (Dose, MDI) in Vorderansicht mit oben liegender Aussparung für die Rastnase des Steckers

Sie können ein Cross-over-Kabel oder einen Adapter kaufen, der die Adernpaare tauscht. Wenn Sie das passende Werkzeug haben, ist so ein Kabel aber auch schnell hergestellt. Wenn Sie mit einem Kabeltester arbeiten, brauchen Sie die Tabelle 2.6 ebenfalls.

Pin Stecker 1		Pin Stecker 2
1	→	3
2	→	6
3	→	1
4	→	7
5	→	8
6	→	2
7	→	4
8	→	5

Tabelle 2.6 Belegung Cross-over-Kabel

2.1.5 Anschlusskomponenten für Twisted-Pair-Kabel

Sie verbinden Geräte (fast) niemals fest mit dem Netzwerkkabel. Ihre PCs, Drucker, Printserver, WLAN-Accesspoints, Router und Switches verfügen über eine RJ45-Buchse. *Netzwerk-Anschlussdosen* und *Patchfelder* werden hingegen zur Leitungsseite fest verkabelt. Am Patchfeld (Abbildung 2.8) liegen die Leitungen zu den einzelnen Anschlussdosen auf. Mit den Patchkabeln verbinden Sie Ihre Geräte mit der Netzwerk-Anschlussdose oder – meist im Fall zentraler Komponenten (Switch, Router etc.) – mit dem Patchfeld.

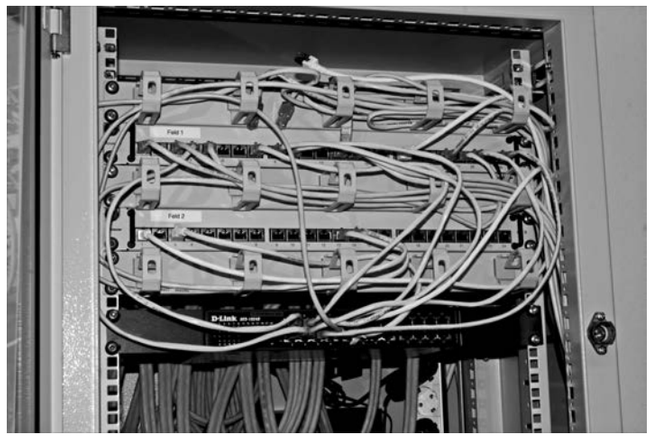


Abbildung 2.8 Netzwerkschrank mit Patchfeld und Switch

Netzwerk-Anschlussdosen und Patchfelder werden Sie überwiegend in der *Schneid-Klemmtechnik*, auch *LSA* (ohne **L**öten, **S**chrauben, **A**bisolieren) genannt mit ihrem gebäudeseitigen Kabel verbinden.

Sehen Sie sich die nachstehenden Details genau an, bevor Sie Ihre erste Netzwerkleitung verlegen. Betrachten Sie zunächst die Bestandteile einer Netzwerk-Anschlussdose im Einzelnen (Abbildung 2.9). Sie besteht (von links nach rechts) aus dem Abschirmdeckel für die Rückseite, dem Dosenkörper (hier zwei Anschlüsse in LSA-Technik) und dem abschirmenden Frontdeckel. Die Kunststoffabdeckung mit Beschriftungsfeldern müssen Sie extra besorgen. Sie haben hier ein großes Angebot an Farb- und Designvarianten.

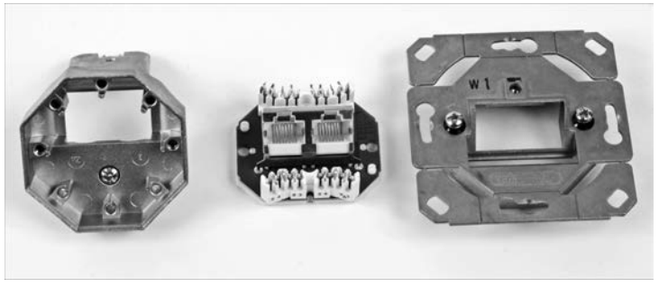


Abbildung 2.9 Bestandteile einer Netzwerk-Anschlussdose

Betrachten Sie den Dosenkörper genauer (Abbildung 2.10). Sie können hier die einzelnen Adern in den LSA-Klemmen deutlich erkennen. Auf den einzelnen Klemmen wird von manchen Herstellern sogar der Farbcode zu EIA/TIA-568A oder -B aufgedruckt, sodass auch Handwerker ohne Netzwerkkenntnisse Installationsarbeiten vornehmen könnten.

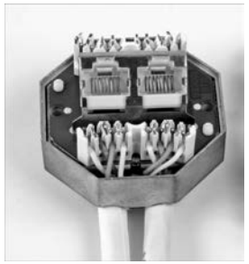


Abbildung 2.10 Dosenkörper einer Netzwerk-Anschlussdose im Detail

RJ45-Stecker hingegen bringen Sie mittels Crimptechnik am Kabel an. Dazu finden Sie in Abschnitt 2.1.7, »Montage von RJ45-Steckern«, eine Schritt-für-Schritt-Anleitung.

2.1.6 Herstellung von Kabelverbindungen mit der Schneid-Klemmtechnik (LSA)

Die Schneid-Klemmtechnik, die auch als LSA (ohne **L**öten, **S**chrauben, **A**bisolieren) bezeichnet wird, bringt Vorteile wie hohe Kontaktdichte und -sicherheit. Zudem sparen Sie viele Arbeitsschritte ein. Die LSA-Technik ist schon seit den 1970er-Jahren Standard im Fernmeldebereich.

Natürlich benötigen Sie auch das passende Werkzeug. Zum sauberen und sicheren Entfernen des Kabelmantels verwenden Sie einen *Abmantler* (Abbildung 2.11). Damit schneiden Sie sich nicht in die Finger und durchtrennen auch nicht gleich das Schirmgeflecht, das unter dem Kabelmantel liegt. Außerdem ziehen Sie mit diesem Werkzeug den Mantelabschnitt ab.

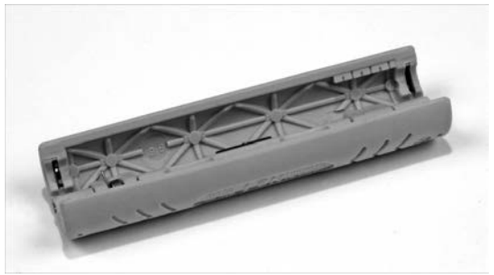


Abbildung 2.11 Abmantler

Der Abmantler besitzt an beiden Enden Schneiden mit verschiedenen Öffnungsweiten. Für Netzwerkkabel verwenden Sie die mit der weiteren Öffnung.

Für das Herstellen der Schneid-Klemm-Verbindung benötigen Sie das *LSA-Anlegewerkzeug* (Abbildung 2.12). Dies hat vorne eine Spitze und eine Andruckvorrichtung. Bei einigen Varianten finden Sie im Griff ausklappbare Zusatzwerkzeuge. Eines davon ist der sichelartige »Enterhaken«. Damit können Sie Adern aus der Schneid-Klemmleiste herauslösen.

In Abbildung 2.12 sehen Sie auch eine LSA-Leiste abgebildet, wie sie zum festen Verdrahten von Fernmeldekabeln oder zum Verlängern von Netzwerkkabeln eingesetzt wird. Sie wird Ihnen aber meist nur im Telefonbereich begegnen. Für die fotografische Darstellung eines Schneid-Klemm-Vorganges war sie aber die bessere Wahl.

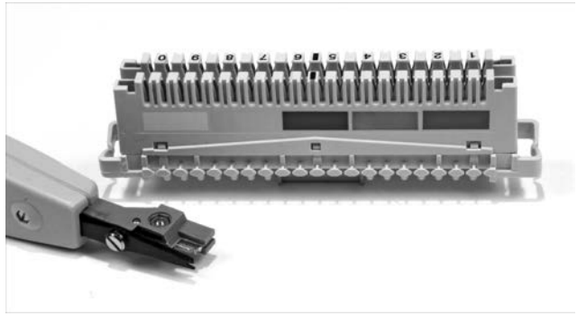


Abbildung 2.12 LSA-Anlegewerkzeug und LSA-Klemmleiste

LSA, Schneid-Klemmverbindungen

- kein Abisolieren von Einzeladern
- Berührungsschutz durch tief liegende Kontaktklemmen
- teilweise Farbcodierung bei Netzwerk-Anschlussdosen
- Anlegewerkzeug kürzt Überstände der Adern auf notwendiges Maß

So stellen Sie eine Schneid-Klemmverbindung her:

1. Drücken Sie die Schneiden des Abmantlers an den Außenmantel des Netzwerkkabels, ohne dabei zu viel Kraft aufzuwenden. Drehen Sie den angedrückten Abmantler um 180°, und versuchen Sie, das abgetrennte Stück des Kabelmantels abzuziehen. Wie viel Sie vom Außenmantel abnehmen müssen, hängt von der Beschaffenheit der Dose oder des Patchfeldes ab.
2. Entflechten Sie das äußere Schirmgeflecht (das klappt am besten mit einer kleinen Drahtbürste), und ziehen Sie es in eine Richtung, gegebenenfalls mit einem vorhandenen Folienschirm. Dies wird später mit der dafür vorgesehenen Aufnahme an der Dose oder dem Patchfeld verbunden.
3. Falls die Adernpaare ebenfalls über eine Schirmung verfügen, ziehen Sie diese in Richtung des schon abstehenden, äußeren Schirmgeflechts. Auch dieses muss dann zusammen mit der Aufnahme verbunden werden.
4. Legen Sie die erste der freigelegten Adern in die richtige Schneid-Klemme (Farbcode oder Nummer beachten, siehe auch Tabelle 2.4 und Tabelle 2.5). Die einzelne Ader liegt dabei lose mit etwas Überstand auf (Abbildung 2.13).

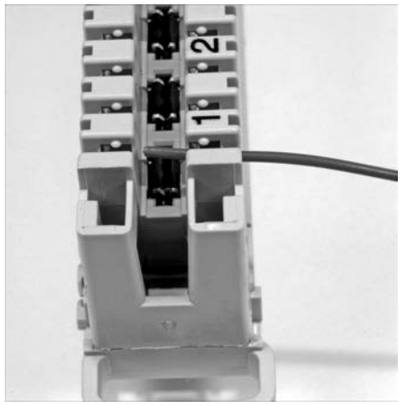


Abbildung 2.13 Lose aufliegende Einzelader

5. Bringen Sie Ihr Anlegewerkzeug in Position. Der klotzartige Teil zeigt zur abgehenden Ader, der schmale Teil (Schneide) zum Überstand (Abbildung 2.14). Drücken Sie nun mit einer schnellen, kraftvollen Bewegung das Werkzeug gegen die Leiste. Sie arbeiten dabei gegen eine Feder. Nach einem deutlich spürbaren Ruck mit einem schnappenden Geräusch nehmen Sie das Werkzeug weg. Durch die Kraft von oben haben Sie die Ader in die scharfkantigen Kontakte gedrückt. Dabei wurde die Isolierung durchdrungen und der elektrische Kontakt hergestellt (Abbildung 2.15). Anschließend verfahren Sie mit den restlichen Adern genauso.
6. Wenn Sie die Verbindung auflösen wollen, müssen Sie die Ader mit einer Häkelnadel oder, falls vorhanden, dem »Enterhaken« aus dem Anlegewerkzeug entgegen der Druckrichtung abziehen.

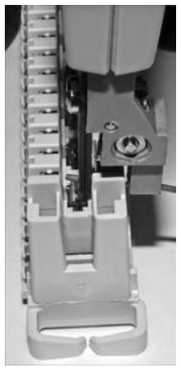


Abbildung 2.14 Die richtige Position des Anlegewerkzeugs

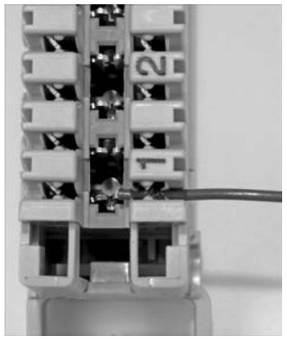


Abbildung 2.15 Fertig hergestellte Schneid-Klemmverbindung

2.1.7 Montage von RJ45-Steckern

Sie können leicht einmal in die Situation kommen, RJ45-Stecker an Netzwerkkabel montieren zu müssen. Vielleicht sind im Rechenzentrum die Standard-Patchkabel einfach zu kurz. Oder Sie müssen für den Messestand schnell und kostengünstig eine provisorische Verkabelung aufbauen, die ohne Netzwerkdosen auskommt (oder auch nur für die Studentenbude ...). Kurz und gut, die notwendigen Handgriffe sollten Sie kennen und beherrschen.

Der RJ45-Stecker besteht aus drei Teilen: dem Steckerkörper, der Kammplatte und der Tülle (Abbildung 2.16, von link nach rechts):

- **Steckerkörper:** Er besteht aus einer metallischen Außenhülle, die mit dem oder den Schirmgeflecht(en) des Kabels verbunden wird. Dadurch bleibt die durchgehende Schirmung zwischen Endgerät und Verteilung erhalten, und Sie vermeiden funktechnische Störungen und Qualitätsminderungen bei den übertragenen Signalen. Ferner verfügt der Steckerkörper über acht Kontakte.
- **Kammplatte:** Dieses kleine Kunststoffteil hält die Adern des angeschlossenen Kabels in Position.
- **Tülle:** Sie bildet die Verlängerung des Kabelmantels. Diese Tüllen erhalten Sie in verschiedenen Farben, sodass Sie damit auch Kennzeichnungen vornehmen können.

Abbildung 2.16 Bestandteile des RJ45-Steckers

Jetzt kennen Sie die Bestandteile des Steckers. Besorgen Sie sich einen Abmantler (Abbildung 2.11) und eine Crimpzange, Kabel- und Steckermaterial, dann können Sie durchstarten! Gehen Sie nach der folgenden Schritt-für-Schritt-Anleitung vor. Versuchen Sie es einmal, es ist nicht schwer.

1. Falls notwendig, schneiden Sie das Kabel auf die gewünschte Länge zu.
2. Schieben Sie jetzt bereits die Tülle richtig herum auf das Kabelende. Dieser Handgriff wird immer wieder vergessen, und Sie würden sich ärgern, wenn Sie den aufgebrachten Stecker wieder abschneiden müssten.
3. Entfernen Sie mit dem Abmantler 2 cm des Kabelmantels (Abbildung 2.17).

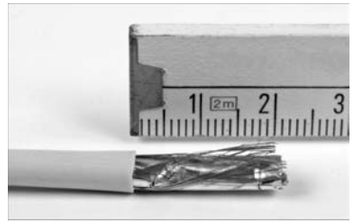


Abbildung 2.17 Das Kabelende; 2 cm des Außenmantels sind entfernt.

4. Legen Sie die verdrillten Adernpaare von der Schirmung (Folie, Geflecht) des Kabelmantels frei, wie Abbildung 2.18 zeigt; bei Cat.-7-Kabeln auch die der Adernpaare selbst. Die Schirmung darf nicht entfernt werden, siehe den nächsten Schritt.

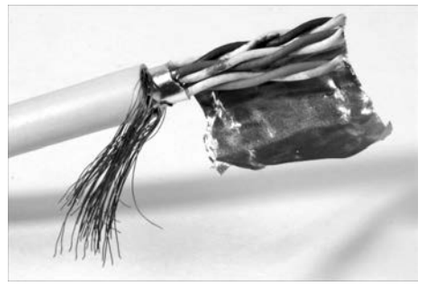


Abbildung 2.18 Freigelegte Adernpaare

5. Verdrillen Sie das Schirmungsmaterial nach hinten zur Tülle hin.
6. Ordnen Sie die Adern gemäß Tabelle 2.4, Tabelle 2.5 und Tabelle 2.6 sowie der Abbildung 2.6 an, und stecken Sie deren Enden durch die Kammplatte (Abbildung 2.19).

Abbildung 2.19 Zusammengedrillte Abschirmung, Adern durch Kammplatte gesteckt

7. Schieben Sie das so vorbereitete Kabelende in den Steckerkörper. Führen Sie das vorsichtig aus, die Adern dürfen nicht gestaucht werden (Abbildung 2.20)!

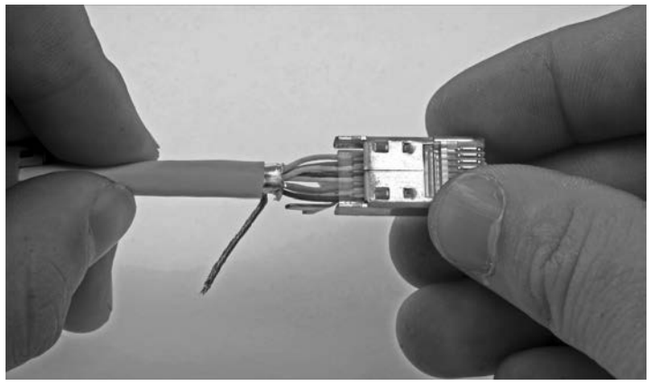


Abbildung 2.20 Einführen des vorbereiteten Kabels in den Steckerkörper

8. Richten Sie die verdrillte Schirmung so aus, dass sie zur Steckeroberseite zeigt. Die Steckeroberseite erkennen Sie daran, dass sich hier die Rastnase befindet. Bringen Sie die Schirmung in die hierfür vorgesehene Aufnahme (Abbildung 2.21). Damit ist der Stecker bereit zum Crimpen (Abbildung 2.22).

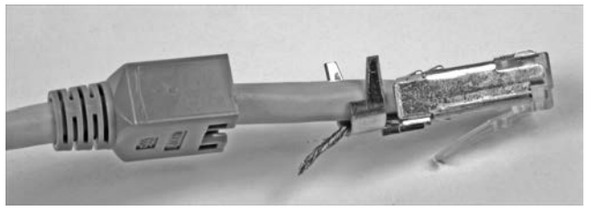


Abbildung 2.21 Crimpfertiger Stecker; das Schirmgeflecht liegt in der Schirmungsaufnahme.

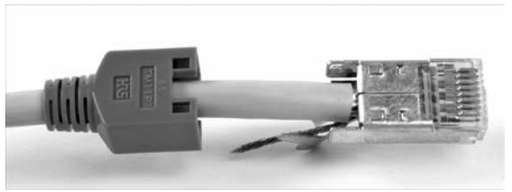


Abbildung 2.22 Crimpfertiger Stecker, Ansicht von unten

9. Nehmen Sie die Crimpzange zur Hand. Führen Sie den Stecker so in das Werkzeug ein, dass die Aufnahme für die Schirmung, die gleichzeitig auch die mechanische Zugentlastung bilden wird, zur passenden Werkzeugöffnung zeigt (Abbildung 2.23).

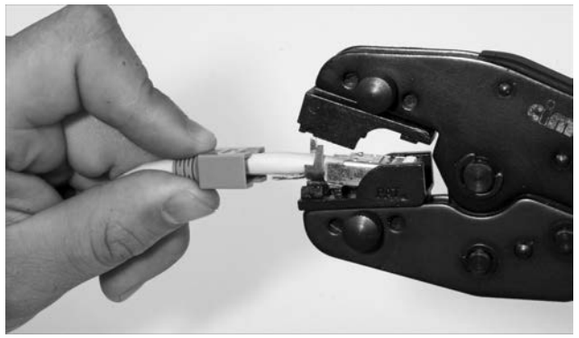


Abbildung 2.23 Einführen des RJ45-Steckers in das Crimpwerkzeug

10. Drücken Sie jetzt mit voller Kraft die Crimpzange zusammen. Der Stecker wird dadurch mit Schirmung und den Adern mechanisch und elektrisch verbunden.
11. Führen Sie eine Sichtkontrolle am fertigen Stecker (Abbildung 2.24) durch. Umschließt die Zugentlastung die Schirmung vollständig? Liegt sie fest an?

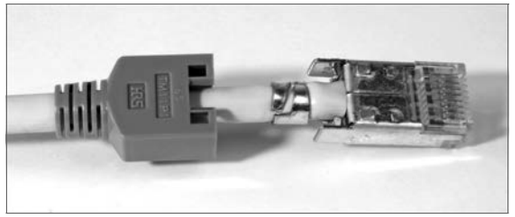


Abbildung 2.24 Fertig gecrimpter Stecker

12. Schieben Sie die Tülle auf den Steckerkörper.

Damit haben Sie den Stecker mit dem Kabel verbunden. Wie Sie Ihr Arbeitsergebnis gleich überprüfen können, lesen Sie im folgenden Abschnitt.

2.1.8 Prüfen von Kabeln und Kabelverbindungen

Wenn zwei Netzwerkteilnehmer absolut nicht zueinanderfinden können, sollten Sie durchaus einmal die beteiligen Patchkabel und die Gebäudeverkabelung (separat) testen. Nicht immer sind ausgefallene aktive Komponenten oder Konfigurationsfehler die Fehlerquelle!

Sie haben mehrere Möglichkeiten, die Kabelstrecke zwischen zwei Netzwerkteilnehmern zu prüfen. Im schlimmsten Fall haben Sie kein Mess- oder Prüfmittel zur Hand. Hier im Beispiel gehe ich von einem Verbindungsfehler zwischen einem PC und einem Switch aus. Arbeiten Sie sich Stück für Stück methodisch vor:

1. Bringen Sie den PC direkt zum Switch, und schließen Sie ihn mit dem gleichen Patchkabel an, das die Verbindung zum Patchpanel herstellt. Bekommt der PC hier trotzdem keine Verbindung, dann tauschen Sie das Patchkabel. Klappt es jetzt wieder nicht, liegt der Fehler entweder beim PC oder beim Switch.
2. Der PC bekommt beim direkten Anschluss an den Switch eine Netzwerkverbindung. Klappte es erst nach dem Kabeltausch, dürfte das Problem schon meist behoben sein. Wenn es nicht dieses Kabel war, dann verbinden Sie den gerade benutzten Port vom Switch wieder mit dem Patchpanel. Prüfen Sie, ob Sie hier auch den richtigen Steckplatz für die Netzwerk-Anschlussdose benutzen. Wenn bis hierher alles sicher ist, müssen Sie das Gebäudekabel prüfen. Nehmen Sie aber vorsichtshalber ein funktionierendes Patchkabel für den Anschluss zwischen Wanddose und PC mit.
3. Schließen Sie den PC mit einem funktionierenden Patchkabel an die vorgesehene Wanddose an. Bekommt der PC jetzt Verbindung, war das vorher verwendete Kabel defekt. Wenn es aber wieder nicht klappt, bleibt Ihnen nur, Patchpanel und Wanddose zu öffnen und die Schneid-Klemmverbindungen nochmals nachzubearbeiten (»nachtackern«).

Tipp

Entfernen Sie defekte Netzwerkkabel sofort, damit diese nicht versehentlich erneut eine Störungsquelle bilden können!

(Tipp aus der Praxis: Stecker abschneiden, dann bleibt das Kabel auch in der Schrottkiste!)

Funktioniert die Verbindung immer noch nicht, benötigen Sie entweder weitere Messmittel oder externe Hilfe, die über diese Möglichkeiten verfügt.

Mit einem einfachen Netzwerktester (Abbildung 2.25), den Sie im Elektronikhandel und -versand sehr günstig erwerben können, grenzen Sie solche Fehler leichter ein. Ich zeige hier ein vielfach verbreitetes Modell, das unter vielerlei Modellbezeichnungen im Handel ist.

Abbildung 2.25 Einfacher Netzwerktester

Der Tester verfügt über zwei Netzwerkanschlüsse und einen Satelliten für den Fall, dass eine Einzelstrecke zu messen ist. Das Gerät prüft jede Ader und die Schirmung einzeln. Sie können per Hand von Ader zu Ader schalten oder überlassen das dem Gerät, das dann den Wechsel eigenständig vornimmt.

Das Fehlerbeispiel bleibt das gleiche wie gerade: Die Strecke zwischen einem PC und einem Switch funktioniert nicht. Mit dem kleinen Netzwerktester gehen Sie wie folgt vor:

- Prüfen Sie die beteiligten Patchkabel. Dazu stecken Sie jedes Kabel mit beiden Steckern am Netzwerktester (Abbildung 2.26) ein. Schalten Sie das Gerät ein, und drücken Sie die Taste AUTO. Das Gerät schaltet nun Ader für Ader durch. Die obere LED-Zeile gibt an, welche Ader geprüft wird. An der unteren sehen Sie, ob diese auch durchgängig ist. Solange die leuchtenden LEDs die gleiche Adernnummer markieren, ist das Kabel (außer es ist ein Cross-over-Kabel) in Ordnung. Ist es kein Cross-over-Kabel und leuchten unterschiedliche Adernnummern auf, liegt eine Vertauschung vor. Bleibt in der zweiten LED-Zeile die LED dunkel, wenn die darüberliegende leuchtet, ist diese entweder nicht vorhanden oder unterbrochen.

Abbildung 2.26 Prüfung der Patchkabel

Probleme mit Billig-Patchkabeln

Bei billigen Patchkabeln sind nicht alle Adern vorhanden. Dies führt zu Problemen, wenn Sie zwei Partner mit 1000Base-T verschalten wollen. Es liegt dann kein Fehler im Sinne der Messung vor.

- Prüfen Sie das Gebäudekabel. Schließen Sie den Tester am Patchpanel und den Satelliten (Abbildung 2.27) an der Netzwerk-Anschlussdose an. Starten Sie den Tester im Automatik-Modus, und gehen Sie zum Satelliten. Hier müsste im Idealfall in aufsteigender Reihenfolge eine LED nach der anderen einzeln aufleuchten.

Abbildung 2.27 Streckenprüfung mit Satellit

Ältere Gebäudeverkabelungen

Hier wurden meist nicht alle Adern 1:1 durchgeschaltet. Ziehen Sie die Tabellen 2.4 und 2.5 zurate. Möglicherweise wurden die Adern nur für 10Base-T oder 100Base-T aufgelegt. Stimmen hierfür die Durchgangsmessungen, liegt kein Fehler im eigentlichen Sinn vor.

Sie können diese Messung auch zu zweit durchführen. Idealerweise sind Sie mit Ihrem Helfer mittels Telefon oder mit PMR-Funkgeräten in Kontakt. In diesem Fall können Sie dann anstelle des Automatik-Modus von Hand Ader für Ader durchschalten, und der Helfer kann das Fehlerbild leichter erfassen.

Abbildung 2.28 Verkabelungstester LanTEK®II (Hersteller: IDEAL INDUSTRIES INC., USA)

Einfache Fehler (falsche, gar nicht aufgelegte oder unterbrochene Adern) können Sie also mit dem kleinen Netzwerktester ausfindig machen und beheben. Sie können aber durchaus auf heimtückischere Fehlerbilder stoßen. Um zu lange Gebäudekabel oder Signalprobleme (Dämpfung, Echos, Übersprechen) erkennen zu können, benötigen Sie andere, leider auch teurere Messgeräte, die Sie auch tageweise mieten können.

Derartige Messgeräte (Abbildung 2.28) ermitteln unter anderem Messwerte für die Kabellänge, die Dämpfung, den Widerstand, die Kapazität, die Impedanz und eventuelle

Signallaufzeitverzögerungen. Mit den Messadaptern für Koaxial-, Twisted-Pair- und Glasfaserkabel können Sie praktisch alle Arten von Netzen messen. Die ermittelten Messdaten übertragen Sie per USB-Schnittstelle auf Ihren Rechner zur weiteren Auswertung, z. B. für die Netzdokumentation nach Neu- oder Erweiterungsarbeiten am Netzwerk.

2.1.9 Kennzeichnen, Suchen und Finden von Kabelverbindungen

Beschriften Sie bei Verkabelungsarbeiten beide Enden immer eindeutig.

Beschriftung von Kabeln für und während Verkabelungsarbeiten

- Fast immer die beste Lösung: Dosennummer (z. B. Zimmer 15 im Erdgeschoss, 1. Dose, im Uhrzeigersinn gezählt: 015/1)
- Gut zum Finden von Patchkabel-Verbindungen: laufende Nummer am Kabel, an beiden Enden. Bei Gebäudeverkabelung müssen Sie eine Liste führen, welche Nummer zu welcher Dose bzw. welchem Switchport gehört.
- Die Beschriftung muss dauerhaft sein. (Permanent-Filzschreiber oder Aufkleber, der über gute Klebeeigenschaften verfügt)
- Bei kleinen Netzen, die ohne Patchfelder/Wanddosen auskommen müssen, verwenden Sie Nummern oder Ringe (Kabelbinder) zur Kennzeichnung.

Was ist aber, wenn Sie auf ein Netzwerk treffen, bei dem nichts beschriftet wurde? Was ist, wenn Dosen keine Bezeichnungen tragen und Sie nicht einmal wissen, ob bei Doppeldosen auch »richtig herum« aufgelegt wurde? Was ist, wenn Sie bei einem provisorischen Netzwerk vor einem dicken Kabelbündel ohne jede Markierung stehen? Wie finden Sie genau die gesuchte Leitung, wenn Ihr Vorgänger alles sauber und akribisch per Barcode-Aufkleber (Praxisfall!) beschriftet hat und Sie keinen Leser dafür zur Hand haben? Der kleine Kabeltester aus dem letzten Abschnitt hilft beim Suchen nur sehr begrenzt weiter. Sie müssen nämlich jeden Port am Patchpanel einzeln prüfen und im gesamten Gebäude mit dem Satelliten jede Dose »besuchen«. Natürlich, bei einem kleinen Netzwerk mit zehn oder zwanzig Anschlüssen mögen Sie damit noch zurechtkommen, aber wenn das Ganze größere Dimensionen aufweist, ist die Arbeit mit dem Gerät kein Vergnügen.

Abhilfe schafft ein *Leitungssuchgerätesatz*. Dieser besteht aus dem Geber (Abbildung 2.29, links) und dem Empfängertastkopf (rechts in Abbildung 2.29). Der Geber besitzt zum Anschluss an die zu suchende Leitung sowohl einen RJ45-Stecker als auch ein Paar Federklemmen (rot für die Signalader, schwarz für die Erdung).

Der Geber des Leitungssuchgerätesatzes besitzt einen Hochfrequenzgenerator (»Sender«), der an ein offenes Adernende oder eine Netzwerk-/Telefondose angeschlossen

wird. Am anderen Ende, meist dem Verteiler, suchen Sie mit dem Tastkopf die Leitung heraus. Der Tastkopf gibt ein akustisches und optisches Signal ab, wenn das Signal entdeckt wird. Zunächst finden Sie das Kabel dadurch heraus, weil der Tastkopf das Signal schon bei Annäherung schwach vernimmt.

Abbildung 2.29 Leitungssuchgerätesatz

Drücken Sie mit der Messspitze (Abbildung 2.30) auf die zutreffende, signalführende Ader, hören Sie dieses Signal laut und kräftig, und die Leuchtanzeige zeigt das Signal an. Bei alten, ungeschirmten Netzen (Cat. 3 oder einer nur ISDN-tauglichen Verkabelung) müssen Sie sehr misstrauisch sein. Prüfen Sie sehr sorgfältig, denn hier kann das Signal des Geberteils durch Übersprecheffekte scheinbar auf mehreren Adern vorhanden sein. Auch hier gilt, dass nur das am lautesten herstellbare Prüfsignal am Tastkopf die zutreffende Ader markiert.

Abbildung 2.30 Arbeiten mit dem Tastkopf an einem Adernbündel

Im Grunde finden Sie damit die betreffende Leitung recht schnell. Beschriften oder markieren Sie dann aber auch die Leitung, damit Sie diese später nicht wieder suchen müssen.

Die Handhabung des Tastkopfes am Patchfeld kann etwas schwierig sein. Für den Test mit der direkten Berührung können Sie verschiedene Hilfsmittel gebrauchen:

- Nehmen Sie ein Patchkabel und das Innenleben einer Netzwerkdose. Stecken Sie das Kabel am »lautesten« Port am Patchfeld und der Netzwerkdose an. Mit der Messspitze des Tastkopfes können Sie am LSA-Anschlussblock direkt auf die Adern zugreifen.
- Verwenden Sie ein Patchkabel, und schneiden Sie einen Stecker ab. Kämmen Sie die Adern aus, isolieren Sie die Enden knapp ab, und schieben Sie eine Kammplatte (siehe RJ45-Stecker, Abbildung 2.19 und Abschnitt 2.1.7, »Montage von RJ45-Steckern«) über die Adernenden, sodass kein Kurzschluss möglich ist. Diese freien Enden berühren Sie mit der Spitze des Tastkopfes.

2.1.10 Power over Ethernet (PoE)

Mit diesem Verfahren wird für Kleinverbraucher eine Versorgungsspannung von 48 Volt und maximaler Strom von 350 Milliampere bereitgestellt. Diese Versorgungstechnik hat an sich keinen Einfluss auf die Datenübertragung, jedoch sollten Sie nur die neueste Speisetechnik einsetzen, damit keine Netzwerkkomponenten beschädigt werden, die PoE nicht unterstützen. Bei 10Base-T und 100Base-T werden freie Adern des Netzwerkkabels, bei 1000Base-T die signalführenden (mit-)benutzt. Meist wird diese Technik zum Betrieb von VoiP-Telefonen, kleinen Switches oder WLAN-Accesspoints benutzt.

2.2 Lichtwellenleiter, Kabel und Verbinder

Bevor Sie Ihre erste Glasfaserstrecke aufbauen, machen Sie zunächst einen kleinen Abstecher in die Physik und die Geschichte dieser Technik. Mit etwas Grundwissen vermeiden Sie Fehler bei der Planung und dem Aufbau Ihres Lichtwellenleiter-Netzes.

Lichtwellen werden reflektiert, wenn sie schräg auf den Übergang von einem Medium auf das andere treffen. Sicher kennen Sie den Effekt aus dem Alltag: Wenn Sie schräg auf eine Wasseroberfläche blicken, sehen Sie kaum etwas davon, was sich unter dieser befindet. Erst wenn Sie nahezu senkrecht nach unten auf das Wasser sehen, erkennen Sie die Dinge unter Wasser.

Lichtwellenleiter ermöglichen derzeit die schnellste und breitbandigste Kommunikation überhaupt. Gebräuchlich sind zurzeit Verfahren mit zwei Adern, eine für die Sendung und eine für den Empfang. Es wird stets mit einer Wellenlänge (= Farbe) gearbeitet.

Die Entwicklungslabors haben Entwicklungen wie das Senden und Empfangen mit einer einzigen Faser geschaffen. Damit würden die Leitungskapazitäten bei konsequenter Umsetzung verdoppelt. In Laborversuchen werden Geschwindigkeiten von 1 Tbit/s angepeilt. Auch wurden schon Verfahren entwickelt, die mehrere verschiedenfarbige Laser auf einer Faser arbeiten lassen. Allerdings können die »normalen« Netzwerkteilnehmer wie PCs diese Geschwindigkeiten selbst noch nicht nutzen. Sie sind einfach zu langsam dafür.

Neben der absoluten Unempfindlichkeit gegenüber elektrischen Einflüssen stehen auch die relativ hohe Abhörsicherheit und der geringere Platzbedarf am Leitungsweg auf der Habenseite. Nachteilig ist dagegen, dass es ein optisches Verfahren ist, bei dem Sie eben nicht schnell ein paar Adern auf eine LSA-Leiste tackern können. Zum Verbinden zweier Fasern brauchen Sie spezielle Spleißgeräte, die die Fasern miteinander verschweißen. Sie kleben Stecker an die Faser, müssen das Faserende polieren und mit dem Spezialmikroskop begutachten. Für die Messungen an den Leitungen benötigen Sie spezielle Geräte. Allerdings gibt es für die Gebäudeverkabelung schon vorkonfektionierte Kabel, die Sie einfach in den Trassenweg einziehen. Zentrale Netzwerkgeräte wie Switches sind schon seit Langem auch mit Lichtwellenleiteranschlüssen im Handel. Netzwerkkarten für PCs sind circa vier- bis fünfmal so teuer (100 Mbit/s) wie die »elektrische« Ausführung. Baugruppen für 1 Gbit/s kosten einige Hundert Euro. Ihr Einsatz wird deshalb nur wichtigen Server-Rechnern vorbehalten sein.

Vor- und Nachteile von Netzwerken mit Glasfaserkabeln

Vorteile:

- höchste Signalbandbreiten möglich
- keine elektromagnetischen Beeinflussungen von außen
- ohne elektrisches Potenzial
- darf zusammen mit Stromleitungen in einem Kanal/Rohr geführt werden
- keine Übersprecheffekte
- relativ hohe Abhörsicherheit
- darf in explosionsgefährdeten Bereichen verwendet werden
- wirtschaftlich, da höherer Investitionsschutz wegen längerer Nutzungsdauer

Nachteile:

- hoher Anschaffungspreis für aktive Netzwerkkomponenten
- Neue Werkzeuge und Messmittel müssen beschafft werden.
- Kein automatisches Erkennen und Einstellen der Übertragungsgeschwindigkeit, beide Partner müssen konstruktiv dieselben Eigenschaften aufweisen.
- Im Normalfall benötigen Sie immer zwei Fasern für eine Verbindung (Senden und Empfangen).

2.2.1 Übersicht über die Netzwerkstandards mit Glasfaserkabel

Für Ihre Planungen und Beschaffungen müssen Sie die Netzwerkstandards für Glasfasernetze kennen.

Auch im Bereich der Glasfasernetzwerke hat die »Evolution« verschiedene Standards (Tabelle 2.7) hervorgebracht. Sie können im Gegensatz zur Kupfertechnik aber keinen Mischbetrieb dahingehend verwirklichen, dass verschieden schnelle Komponenten auf einer Faser miteinander kommunizieren. Hierfür benötigen Sie Medienkonverter, die die Netzkosten erhöhen. In Tabelle 2.7 finden Sie auch Angaben zur IEEE-Norm und der Lichtquelle.

Bezeichnung	Maximale Länge	Beschaffenheit
10Base-FL	2 km	Faser: Multimode, OM1 bis OM4 Wellenlänge: 850 nm Lichtquelle: LED Norm: IEEE 802.3 Clause 18
100Base-FX	400 m/2 km	Faser: Multimode, OM1 bis OM4 Wellenlänge: 1310 nm Lichtquelle: LED Norm: IEEE 802.3 Clause 26 Reichweite von 2 km, wenn Switches oder Bridges miteinander verbunden sind

Tabelle 2.7 Netzwerkstandards optischer Netze

Bezeichnung	Maximale Länge	Beschaffenheit
100Base-SX	300 m	Faser: Multimode, OM1 bis OM4 Wellenlänge: 850 nm Lichtquelle: LED Norm: IEEE 802.3 Clause 38
1000Base-LX	550 m/2 km	Faser: Multimode, OM1 bis OM4 Wellenlänge: 1310 nm Lichtquelle: Laser Norm: IEEE 802.3 Clause 38 Reichweite: 550 m alternativ: Faser: Monomode, OS1 Wellenlänge: 1310 nm Lichtquelle: Laser Reichweite: 2 km
1000Base-SX	500 m	Faser: Multimode, OM1: 300 m, OM2 bis OM4: 500 m Wellenlänge: 850 nm Lichtquelle: VCSEL-Laser Norm: IEEE 802.3 Clause 38
10GBase-LR	10 km	Faser: Monomode, OS1 Wellenlänge: 1310 nm Lichtquelle: Laser Norm: IEEE 802.3ae
10GBase-SR	300 m	Faser: Multimode, OM3 bis OM4 Wellenlänge: 850 nm Lichtquelle: VCSEL-Laser Norm: IEEE 802.3 ae
10GBase-ER	40 km	Faser: Monomode, OS1 Wellenlänge: 1550 nm Lichtquelle: DFB-Laser Norm: IEEE 802.3ae 2002

Tabelle 2.7 Netzwerkstandards optischer Netze (Forts.)

Bezeichnung	Maximale Länge	Beschaffenheit
10GBase-LX4	300 m/10 km	Faser: Multimode, OM1 bis OM4 Wellenlängen (Multiplexbetrieb): 1275 nm, 1300 nm, 1325 nm und 1350 nm Dient der Übertragung auf (älteren) Multimodefasernetzen. Lichtquelle: vier Laser Norm: IEEE 802.3 Clause 48 alternativ Faser: Monomode, OS1 Reichweite: bis 10 km

Tabelle 2.7 Netzwerkstandards optischer Netze (Forts.)

Beachten Sie unbedingt, mit welcher Lichtquelle Ihr Netz arbeitet. Besonders Laser schädigen das Augenlicht, wenn Sie in ein offenes Faserende blicken. Planen Sie deshalb unbedingt Schutzmaßnahmen gegen unbeabsichtigtes Austreten des Laserlichtes ein (Zugangssperren zu Netzwerkkomponenten, Warnhinweise für Service-Personal usw.)!

2.2.2 Aufbau und Funktion von Glasfaserkabeln

Sie werden auf verschiedenartige Glasfaserkabel stoßen. Einige Bestandteile sind stets die gleichen. Wenn Sie Lichtwellenleiter-Kabel (LWL) über verschiedene Arten von Strecken verlegen (in/außerhalb von Gebäuden, Stammkabel, Einzelverbindungen), benötigen Sie diese Informationen.

Der *Außenmantel* bietet Schutz vor Einflüssen aller Art (je nach Ausstattung auch gegen Nässe, Nagetiere und starke mechanische Belastungen). Er nimmt jedoch keine Zugkräfte auf. Dafür finden Sie darunter als nächste Schicht das Zugentlastungsgarn aus Kevlar. Wiederum darunter treffen Sie auf die Adern (Hohl-, Kompakt- oder Bündeladern), die die Fasern beherbergen. Die Fasern selbst sind durch verschiedene Gellagerungen oder *Coatings* (Ummantelungen) geschützt. Das Primärcoating umschließt die Faser selbst. Auf das Sekundärcoating stoßen Sie nicht bei allen Kabeltypen. An seiner Stelle finden Sie weiche Füllmassen, in denen die vom Primärcoating geschützte Glasfaser liegt. Daraus ergeben sich verschiedene Aderquerschnitte:

Querschnitte verschiedener Adern von Glasfaserkabeln

- **Vollader**: Sekundärcoating aus hartem Material, Primärcoating aus weichem Material, Faser
- **Kompaktader**: Sekundärcoating aus hartem Material, gelartige Füllmasse, Primärcoating aus weichem Material, Faser
- **Hohlader**: Kunststoffröhrchen, Füllmasse, Primärcoating, Faser
- **Bündelader:** Kunststoffröhrchen, Füllmasse, mehrere Fasern im eigenen Primärcoating

Die Glasfaser selbst besteht aus dem *Glasmantel*, der vom Primärcoating umgeben ist, und dem *Glaskern*. Die Lichtwellen werden am Übergang vom Kern zum Mantel reflektiert.

Lichtwellenleiter bekommen Sie in zwei Ausführungen: Monomode (auch Singlemode genannt) und Multimode. Sie können die beiden Typen nur mittels aktiver Komponenten miteinander verbinden. Um Fehlinvestitionen zu vermeiden, sollten Sie sich die Kabeleigenschaften und Einsatzgebiete, die mit den beiden Begriffen verbunden sind, genau einprägen.

Eigenschaften der Monomode-Glasfaser (Abbildung 2.31)

- Physik: Das Licht wird senkrecht zur Schnittfläche des Faserkerns eingestrahlt. Der Lichtstrahl breitet sich in einer einzigen Wellenführung aus (Mono-/Singlemode). Die Monomode-Fasern sind allesamt *Stufenindexfasern*, die Brechzahl beim Übergang vom Glaskern zum Glasmantel ändert sich abrupt.
- Übertragungseigenschaften: geringe Dämpfung und Signallaufzeiten, hohe Signaltreue (Signalform wird kaum verändert)
- Einsatz: Punkt-zu-Punkt-Verbindungen über weite Strecken (WAN)
- Gebräuchliche Wellenlängen: 1550 nm und 1310 nm
- Maße: Kerndurchmesser 9 µm (Altnetze/Übersee: 10 µm), Glasmantel 125 µm
- Stellt hohe Anforderungen an Spleiß- und Steckverbindungen.
- höherer Preis

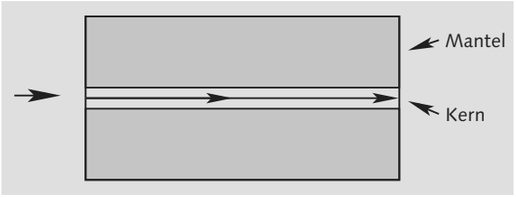


Abbildung 2.31 Verlauf der Lichtwellen in einer Monomode-Faser

Eigenschaften von Multimode-Glasfasern

- Physik: Das Licht wird schräg auf die Schnittfläche des Faserkerns gegeben. Dadurch wird es am Übergang vom Glaskern zum Glasmantel in flachem Winkel reflektiert.
- Übertragungseigenschaften von Multimode-Fasern mit Stufenindex (Abbildung 2.32): Mittlere Dämpfung, geringe Bandbreite, Signale werden durch die verschiedenen Laufzeiten der einzelnen Moden mit zunehmender Entfernung »unscharf« (Modendispersion). Multimode-Fasern mit Stufenindex werden nicht mehr verbaut.
- Übertragungseigenschaften von Multimode-Fasern mit Gradientenindex (Abbildung 2.33): Bandbreite über 1 GHz, relativ niedrige Dämpfung. Die einzelnen Moden erreichen zu relativ gleicher Zeit das Faserende, was die Ausprägung von »unscharfen« Signalen (Modendispersion) über weite Lauflängen gering hält. Diese Fasern werden bei Erweiterungen und Neubauten verwendet.
- Einsatz: in lokalen Netzen bis 2 km (LAN, MAN)
- Gebräuchliche Wellenlängen: 1310 nm und 850 nm
- Maße: Kerndurchmesser 50 µm (Altnetze: 62,5 µm), Glasmantel 125 µm
- Stellt weniger hohe Anforderungen an Spleiß- und Steckverbindungen.
- günstigerer Preis, höhere Verbreitung

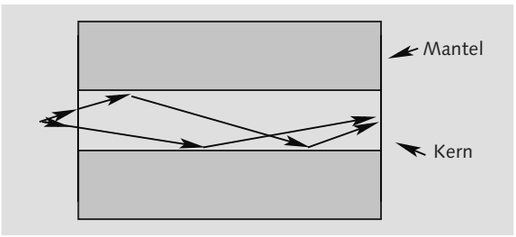


Abbildung 2.32 Lichtwellenverlauf in einer Multimode-Faser mit Stufenindex

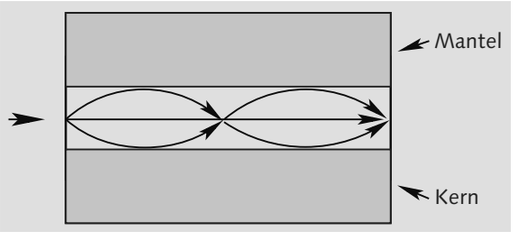


Abbildung 2.33 Lichtwellenverlauf in einer Multimode-Faser mit Gradientenindex

Glasfaserkabel bekommen Sie in verschiedenen Kategorien im Handel. Sie unterscheiden sich hinsichtlich Nutzbandbreite und Reichweite (Tabellen 2.8, 2.9).

Faserkategorie IEC/ISO 11801	Entspricht IEC 60793-2-10-	Standards aus EN 50173-1
OM1	A1b	60793-2-10
OM2	A1a	60793-2-10
OM3	A1a.2	60793-2-10
OM4	A1a.2 Ed.2.0	60793-2-10
OS1	(IEC 60793-2-50)-B.1.1	60793-2-50

Tabelle 2.8 Normenverweis für Faserkategorien; OM1 bis OM4 betreffen Multimode-Fasern, OS1 Monomode-Fasern.

Die Normenvorgaben zur Dämpfung sind Mindestwerte! Viele Hersteller bieten Ihnen Produkte an, die diese deutlich unterschreiten. Sie tragen allerdings hauseigene Bezeichnungen. In Tabelle 2.9 ist auch die noch sehr neue Norm OS2 enthalten.

Faserkategorie	OM1	OM2	OM3	OM4	OS1	OS2
Kerndurchmesser	62,5 µm	50/62,5 µm	50 µm	50 µm	9 µm	9 µm
Dämpfung db/km bei 850 nm	3,5	3,5	3,5	3,5	–	–
Dämpfung db/km bei 1310 nm	1,5	1,5	1,5	1,5	1	0,4

Tabelle 2.9 Normenvorgaben zur Dämpfung

2.2.3 Dauerhafte Glasfaserverbindungen

Dauerhafte Glasfaserverbindungen begegnen Ihnen an jeder Verlängerung bei WAN-Strecken. Aber auch kurze Stücke mit fest verbundenem Stecker werden dauerhaft mit der Gebäudeverkabelung zusammengefügt.

Für eine dauerhafte Verbindung müssen Sie Glasfasern miteinander verschweißen. Mit jeder Übergangsstelle erhöht sich die Dämpfung und verringert sich die Reichweite geringfügig.

Wenn Sie Glasfasern miteinander verschweißen möchten, benötigen Sie ein (teures) Spleißgerät. Sie sehen damit die beiden Faserenden stark vergrößert auf einem kleinen Monitor. Unter diesem »Mikroskop« führen Sie die Enden aneinander und lösen den Lichtbogen aus, der den Schmelzvorgang bewirkt. Dies geschieht alles mit feinmechanisch höchster Präzision. Die Verbindungsstelle wird zusätzlich mit einer aufgecrimpten Metallklammer gesichert.

An den Verbindungsstellen sind die Faserenden blank, dort ist also der Glasmantel sichtbar. Erst nach einigen Zentimetern wird er vom Primärcoating bedeckt. Der Außenmantel und das Zuggarn aus Kevlargarn enden bereits in der Zugentlastung. Die so offenliegenden Kabel werden in der Spleißbox (Abbildung 2.34) vor mechanischen und klimatischen Umwelteinflüssen geschützt.

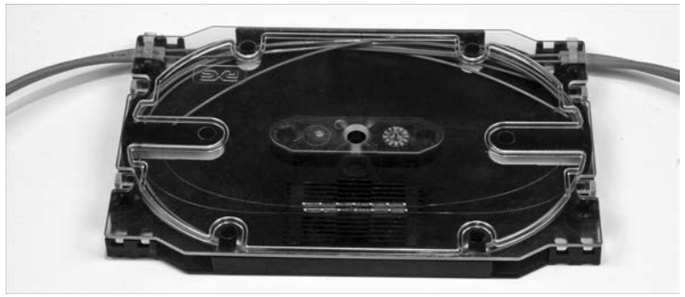


Abbildung 2.34 Spleißbox

2.2.4 Lichtwellenleiter-Steckverbindungen

Es gibt leider viele verschiedene LWL-Steckverbinder. Beim Einkauf von aktiven Netzwerkkomponenten sollten Sie deshalb auf eine einheitliche Ausstattung achten.

Steckverbindungen für Glasfaserkabel funktionieren im Prinzip so, dass die polierten Steckerenden mit dem Faserkern aneinandergepresst werden und der Lichtstrahl die Schnittflächen überwindet. Besonders bei Monomode-Fasern mit nur 9 µm Kerndurchmesser werden hier sehr hohe Anforderungen an die Präzision von Stecker und Kupplungshalterung gestellt. Natürlich haben auch die LWL-Steckverbindungen eine Dämpfung.

Ein LWL-Stecker besteht aus einer *Ferrule* (gegebenenfalls Doppelferrule), die die Faser aufnimmt, und dem Steckergehäuse. Das Steckergehäuse nimmt die Ferrule und die Zugentlastung für das Kabel auf. Es dient auch der Führung und Verriegelung in der Kupplungshalterung.

Für die klassischen Steckverbinder (SC, ST) müssen Sie mehr Platz als für Kupferanschlüsse von RJ45-Buchsen und -Steckern einplanen. Jedes Kabel führt zwei Fasern, und für jede brauchen Sie einen Steckplatz. Damit finden Sie auf einem Patchpanel weniger Platz vor. Mit den miniaturisierten Steckernormen LC und MTRJ wurde dieses Problem aber schon weitgehend gelöst.

Fast alle Stecker nehmen nur eine Faser auf, daher können Sie für den paarweisen Einsatz Duplexklammern verwenden, die damit quasi einen Stecker bilden.

Zum Befestigen von Steckern an den Kabelenden benötigen Sie in jedem Fall Spezialwerkzeug. Hauptsächlich werden Sie folgende zwei Verfahren antreffen:

Verbindung von LWL-Steckern mit dem Kabel

- **Klebetechnik**: Die Faser (Glasmantel und -kern) führen Sie in den mit Kleber gefüllten Stecker ein. Den Kleber lassen Sie aushärten, die Faser schneiden Sie am Ferrulenende ab. Die Schnittfläche polieren Sie und kontrollieren sie im Mikroskop auf Riefen und sauberen Schliff hin. Atmen Sie den Polierstaub nicht ein, er darf auch nicht auf Nahrungsmittel gelangen. Halten Sie den Arbeitsplatz sauber!
- **Anspleißen**: Es werden vorgeklebte Stecker angeboten, die Sie mit dem LWL-Spleißgerät mit der Faser verbinden.

Die so bearbeiteten Kabel müssen Sie mit einem Messgerät neu überprüfen (lassen). Damit erkennen Sie, ob es wie bei den Spleißstellen überhaupt geklappt hat und wie hoch die Einfügedämpfung ist.

Wenn Sie über großzügige Kabeltrassen und -kanäle verfügen, können Sie ganz einfach vorkonfektionierte Kabel über den Fachhandel einkaufen und selbst einziehen. Vergessen Sie aber auch hier nicht, aussagekräftige Beschriftungen an den Kabelenden anzubringen!

Im Laufe der Zeit hat die Industrie eine Anzahl verschiedener Steckertypen entwickelt. Häufig treffen Sie die Typen SC, ST, LC und MTRJ an. Sie unterscheiden sich hinsichtlich ihrer Einfügedämpfung, ihrer Faseranzahl und ihres Platzbedarfes (Tabelle 2.10).

Typ	Abbildung	Norm IEC 61754-	Einfügedämpfung		Einsatz
			Multimode-Faser	Monomode-Faser	
ST	2.35	2	0,2 dB	0,15 dB	eine Faser, LAN/WAN
SC	2.35	4	0,2 dB	0,20 dB	eine Faser, LAN/WAN
MTRJ	2.36	18	0,2 dB	0,40 dB	zwei Fasern, LAN/WAN
LC	2.37	20	0,2 dB	0,12 dB	eine Faser, LAN/WAN

Tabelle 2.10 Einfügedämpfung und Einsatzgebiete gebräuchlicher LWL-Stecker

Besonderheiten ausgewählter LWL-Stecker

- **ST-Stecker**: Er besitzt eine Metallhülle und wird mittels Bajonettsicherung am Gegenstück befestigt. Keramikferrule 2,5 mm Durchmesser (Abbildung 2.35 links)
- **SC-Stecker**: Kann mit der Duplexklammer zu einem Paarstecker zusammengefügt werden. Keramikferrule 2,5 mm Durchmesser (Abbildung 2.35 rechts)
- **MTRJ-Stecker**: Platzbedarf wie RJ-45-Stecker. Wird meist in aktiven Komponenten (Switches) verwendet, da hohe Anschlussdichte realisierbar. Nicht für dicke Kabel verwendbar. Kunststoff-Doppelferrule (Abbildung 2.36)
- **LC-Stecker**: Etwa halber Platzbedarf von SC-Steckern, Keramikferrule 1,25 mm Durchmesser, Einsatz an aktiven Komponenten (Abbildung 2.37)

Abbildung 2.35 ST-Stecker (links), SC-Stecker in Duplexklammer (rechts), Ferrulenschutzkappe (Mitte)

Abbildung 2.36 MTRJ-Stecker

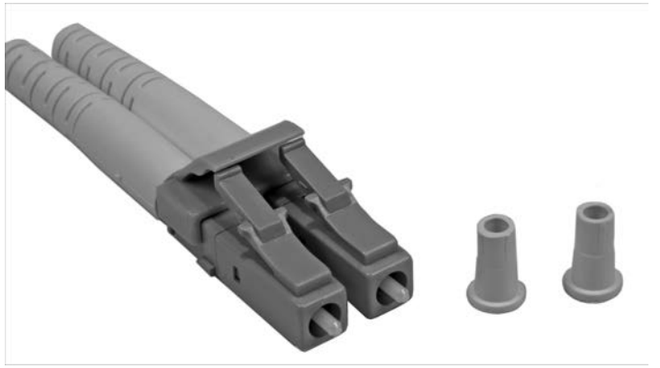


Abbildung 2.37 LC-Stecker paarweise in Duplexklammer mit Ferrulenschutzkappen

2.2.5 Umgang mit der LWL-Technik

Beim Umgang mit Glasfasertechnik müssen Sie einige Regeln einhalten, um sich oder die Technik nicht zu gefährden.

Normalerweise kommen in Netzwerken erst ab 1 Gbit/s Übertragungsgeschwindigkeit Laser zum Einsatz, aber das kann in besonderen Fällen auch schon auf Netze mit 100 Mbit/s zutreffen.

Laserstrahlen schädigen Gewebe, auch wenn sie nur über eine scheinbar sehr geringe Leistung verfügen. Doch die punktförmig einwirkende Energie kann ausreichen, um im Auge die Netzhaut, gegebenenfalls auch die Hornhaut dauerhaft zu schädigen. Nicht alle Laserstrahlen liegen im Bereich des sichtbaren Lichtes. Die Bereiche von 1500 nm bis 1300 nm sind für das menschliche Auge nicht erfassbar. Nur die Wellenlänge von 850 nm wird als rot wahrgenommen. Beachten Sie das Warnzeichen (Abbildung 2.38)!

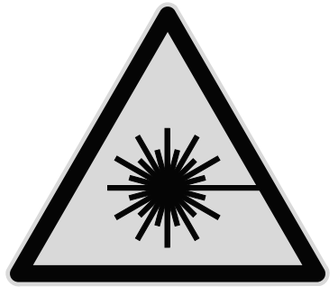


Abbildung 2.38 Warnung vor Laserstrahl

Schutzmaßnahmen bei LWL-Netzwerkanlagen

- Blicken Sie niemals in offene LWL-Buchsen oder Stecker!
- Verschließen Sie LWL-Buchsen an Medienkonvertern, Patchfeldern und Switches stets mit den passenden Schutzkappen, wenn kein Kabel angeschlossen wird!
- Installieren Sie LWL-Netzwerkkomponenten möglichst außerhalb allgemein zugänglicher Räume!
- Sichern Sie LWL-Mess- und Prüfgeräte in Arbeitspausen!

Offene LWL-Kabelenden sind gefährlich! Berühren Sie besonders die kleinen Abschnitte nicht, die bei Verkabelungsarbeiten anfallen. Glasmantel und -kern durchdringen bei senkrechtem Druck mühelos Ihre Haut. Die Glasteile können nicht operativ entfernt werden. Der Körper kann sie nur über eine Abstoßungsreaktion loswerden, die mit Entzündungen und Eiterungen verlaufen kann. Das Einatmen von Glasfaserabschnitten und Schleifstaub (Steckerbearbeitung) schädigt Ihre Lunge, genauso die Verdauungsorgane bei der Aufnahme über Nahrung und Trinken!

Schutzmaßnahmen vor Verletzungen durch Glasfaserteile

- Berühren Sie niemals die Enden einer Glasfaser! (Abbildung 2.39)
- Reinigen Sie nach Arbeiten am Glasfasernetz das Umfeld der »Baustelle« sorgsam von Faserresten und Schleifstaub. Wirbeln Sie hierbei keine Teilchen auf! Verwenden Sie feuchte Reinigungstücher und -Lappen, und entsorgen Sie diese anschließend in verschließbaren Plastiksäcken.
- Essen und trinken Sie nicht im Umfeld von Arbeiten an Glasfaserleitungen! Lagern Sie an solchen Stellen auch keine Nahrungsmittel.

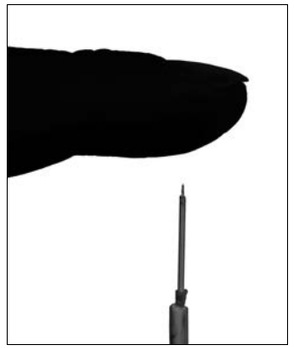


Abbildung 2.39 Verletzungsgefahr an offenen LWL-Kabelenden

Abbildung 2.40 Hier droht Gefahr für LWL-Komponenten!

Achten Sie auf Sauberkeit im Umfeld von LWL-Anschlusskomponenten. Mit Staub, Schmierfilm oder Kratzern überzogene Stecker und Buchsen mindern die Übertragungsqualität und führen zu Störungen bei der Datenübertragung.

Schutz der Glasfasertechnik vor schädlichen Einflüssen

- Verschließen Sie unbenutzte Steckerenden und Buchsen von LWL-Komponenten stets mit den zugehörigen Schutzkappen.
- Berühren Sie Steckerenden niemals mit dem Finger! (Abbildung 2.40)
- Vermeiden Sie Staub und Kondensatbildung (Wasser- und Fettdampf) im Umfeld von LWL-Komponenten.
- Verschmutzte Austrittsflächen an LWL-Steckern reinigen Sie mit reinem Isopropylalkohol. Andere Reiniger haben Zusatzstoffe (Seifen, Duftstoffe), die einen Schmierfilm bilden und zurückbleiben.
- Decken Sie bei Bauarbeiten LWL-Komponenten staubdicht ab.
- Quetschen und knicken Sie keine LWL-Kabel.
- Unterschreiten Sie die Biegeradien nicht! Wird der Biegeradius unterschritten, findet die Reflexion der Lichtwellen am Übergang vom Glaskern zum Glasmantel nicht mehr statt. Der Licht- oder Laserstrahl trifft in das Primärcoating. Die Verbindung wird mit Dämpfung beaufschlagt oder unterbrochen.
- Wenden Sie bei LWL-Steckverbindungen keine Gewalt an! Die Ferrule kann beschädigt werden, und es platzen Teile im vorderen Bereich ab. Genauso gut aber können LWL-Buchsen ausleiern. Der Licht- oder Laserstrahl wird dann nicht mehr genau zentriert.

2.2.6 Aufbau eines einfachen Leitungs- und Kabeltesters

Wenn Sie einmal vor einem Bündel unbeschrifteter Glasfaserkabel sitzen, die von allen möglichen Räumen ankommen, hilft Ihnen ein kleines Gerät (Abbildung 2.41) vielleicht weiter. Leitungssuchgeräte, wie aus der Kupfertechnik bekannt, scheiden bei Glasfasern leider aus.

Das Innenleben des Testers besteht aus einer Blinkschaltung für LEDs (Bausatz vom Elektronikversender). Die LED wird gegen einen anderen, sehr hellen Typ gleicher Stromaufnahme (hier 20 mA) getauscht. Bohren Sie den Korpus der LED vorsichtig ein Stück auf, sodass anschließend eine 2.5-mm-Ferrule eines ST-Steckers gut sitzt. Sie können auch einen LED-LWL-Geber für 850 nm Wellenlänge benutzen, wenn erhältlich. Bauen Sie die Schaltung zusammen mit einer Batteriehalterung und einem Schalter in ein Kleingehäuse ein – fertig!

Sie können das Gerät um einen passenden Satelliten ergänzen, der mittels Fototransistor eine Signaleinrichtung schaltet (LED, Summer ...).

Abbildung 2.41 Eigenbau-LWL-Tester mit Adapterkabel ST

2.2.7 Prüfen von LWL-Kabeln und -Verbindungen

Mit dem Eigenbau-LWL-Tester können Sie einfach Patchkabel »auf Durchgang« prüfen. Stecken Sie hierzu ein Ende des Kabels an den Tester, und ermitteln Sie am anderen Ende den Stecker mit dem Lichtaustritt. Markieren Sie die zutreffende Faser an beiden Kabelenden am Kabelmantel. Für MTRJ- und LC-Stecker müssen Sie sich einen Adapter fertigen (lassen) oder besorgen.

Wenn Sie in der Gebäudeverkabelung LWL-Leitungen auf Durchgang prüfen oder ganz einfach eine Leitung suchen möchten, sollten Sie sich an folgenden Arbeitsschritten orientieren:

Prüfen und Suchen in der LWL-Gebäudeverkabelung

- **Vorbereitungen am Patchfeld**: Grenzen Sie den Bereich der zu prüfenden Anschlüsse ein (Stockwerk, Zimmer).
- **Vorbereitungen bei der LWL-Anschlussdose im »Zielraum«**: Stellen Sie sicher, dass sich keine Komponenten (Medienkonverter, Switch mit LWL-Uplink, PC mit LWL-Netzwerkkarte) in Betrieb befinden und an das LWL-Netz angeschlossen sind. Es besteht sonst unter Umständen eine Verletzungsgefahr für die Augen!
- **Netzwerkdose**: Verbinden Sie mit dem LWL-Einzelfaserkabel die beiden Buchsen der Strecke. (Netzwerkdosen sind in der Regel immer duplex.)
- **Patchfeld**: Stellen Sie eine Verbindung des Testers mittels Einfaserkabel mit dem vermutlich zutreffenden Steckplatz her. In der unbenutzten Buchse des Duplexanschlusses sollten Sie das (blinkende) Lichtsignal sehen können, wenn die Strecke in Ordnung ist (Hin- und Rückleitung). Andernfalls lassen Sie den Tester eingeschaltet und sehen bei der Netzwerkdose nach, ob dort das Lichtsignal ankommt. Gegebenenfalls ist eine Faser falsch aufgelegt oder unterbrochen.

Wenn Sie Messungen (Dämpfung, Länge, Qualität) vornehmen wollen, benötigen Sie ein Messgerät wie das in Abbildung 2.28.

2.3 Datenübertragung per Funktechnik

Mit der Funktechnik können Sie auf verschiedene Arten Daten übertragen. Viele Funkdienste (im Sinne der VO Funk) übertragen Text, Bild, Ton und Daten aller Art digital per Funk. Von den Mobilfunknetzen (GSM, UMTS oder auch WIMAX) werden Datenübertragungsdienste gegen Gebühr angeboten. Außer den Funkdiensten im klassischen Sinn kennen Sie sicherlich das verbreitete WLAN.

2.3.1 WLAN (Wireless LAN, Wi-Fi)

Mit dem WLAN zog das Internet in die Haushalte ein. »Kabellos Surfen« öffnete die PCs der Privatkunden für den Anschluss an die weite Welt. WLAN beschäftigt elektrosensitive Menschen genauso wie die Gerichte, die hierzulande mit einer recht uneinheitlichen Rechtsprechung über »Schwarzsurfen« und missbräuchliche Nutzung von WLAN-

Zugängen nicht gerade für Rechtssicherheit sorgen. Ganz allgemein gesagt, ist die Datenübertragung in der Regel langsamer als bei kabelgebundenen Netzen. WLAN-Netze sind auch oftmals das Ziel von Angriffen. Sie erkennen, dass hier verschiedene Interessen aufeinanderprallen. Lesen Sie aber zunächst die technischen Details.

Technische Details des WLANs

- **Frequenzbereich und Sendeleistung**:
  2400–2450 MHz mit 100 mW effektiv abgestrahlter Leistung
  5150–5250 MHz mit 200 mW effektiv abgestrahlter Leistung, nur innerhalb geschlossener Räume, die Anwendung darf andere Nutzer des Frequenzbereiches nicht stören.
- **Antennen**:
  Als Antennen kommen sowohl Rundstrahl- als auch kleine Richtantennen zum Einsatz. Dabei darf die vorgegebene effektive Strahlungsleistung (EIRP) nicht überschritten werden. Der Antennengewinn wird hierbei hinzugerechnet.
- **Einschränkungen**:
  Die genannten Frequenzbereiche werden auch von anderen Nutzern belegt (Shared Medium). Insofern sind Störungen bzw. Leistungsminderungen bei der Datenübertragung möglich. Außerdem kann es bei einer hohen Dichte von WLAN-Nutzern ebenfalls zu Ressourcenengpässen kommen.
- **Übertragungsrate/Reichweite**:
  Die Übertragungsrate beträgt standardmäßig maximal 54 Mbit/s (schnellere Verfahren bis 600 Mbit/s). Die Reichweite wird bis maximal 250 m angegeben.
- **Normen**:
  IEEE 802.11 (a–y) (Tabelle 2.11)
- **Endgeräte**:
  eingebaut in Notebooks, USB-Sticks, PCMCIA- und Cardbus-Steckkarten für Notebooks, Erweiterungskarten für PCs
- **Netzwerkkomponenten**:
  WLAN-Zugangspunkte und WLAN-Router

Auch das WLAN hat sich über die Jahre weiterentwickelt, und das Institute of Electrical and Electronics Engineers (IEEE) hat dafür entsprechende Standards definiert (Tabelle 2.11).

Norm IEEE 802.11	Merkmale
-	maximal 2 Mbit/s, 2,4 GHz-Band, veraltet
a	54 Mbit/s (effektiv ca. 50 % davon), 5 GHz
b	11 Mbit/s (effektiv ca. 50 % davon), 2,4 GHz, bei Altgeräten noch im Einsatz
g	54 Mbit/s (effektiv ca. 40 % davon), 2,4 GHz, sehr verbreitet
n	600 Mbit/s, 2,4 GHz und 5 GHz, beherrschen immer mehr Neugeräte (2010)
p	27 Mbit/s, 5,8 GHz für die Vernetzung von Fahrzeugen untereinander

Tabelle 2.11 Auswahl von gängigen WLAN-Normen

2.3.2 Datenübertragung über öffentliche Funknetze

Die Datenübertragung über die Mobilfunknetze bietet Ihnen den Internet- und Netzwerkzugriff ohne ortsfeste Anbindung. Sonderfälle ortsfester Datenfunknutzer stellen Mess- und Überwachungsgeräte außerhalb vorhandener Infrastrukturnetze dar, z. B. Pegelmesser an Gewässern, Wetterstationen, aber auch Notrufeinrichtungen von Aufzügen, Backup-Verbindungen von Brandmeldeanlagen. Dabei stehen Ihnen je nach Angebot vor Ort verschiedene Leistungsmerkmale zur Verfügung:

Leistungsmerkmale der Datenübertragung über Mobilfunknetze

- **CSD**: 9,6 kbit/s bis 14,4 kbit/s, leitungsvermittelt
- **HSCD**: bis 57,6 kbit/s (je Richtung 28,8 kbit/s), Kanalbündelung
- **GPRS**: 53,6 kbit/s, paketorientiert
- **EDGE**: je Zeitschlitz 59,2 kbit/s, praktisch 220 kbit/s Download, 110 kbit/s Upload (erweitert GPRS zu E-GPRS und HSCD zu ESCD)
- **UMTS**: 144 kbit/s bis 384 kbit/s
- **HSDPA**: 1,8 Mbit/s (veraltet), 3,6 Mbit/s und 7,2 Mbit/s
- **LTE**: Nachfolger von UMTS und UMTS-Erweiterungen, 100 Mbit/s Download, 50 Mbit/s Upload in den ersten verfügbaren Netzen (2010)
- **LTE-Advanced**: Nachfolger von LTE, erwartet: 1 Gbit/s Download

Als Endgeräte finden Sie meist diverse USB-Sticks im Handel. Einsteckkarten für PCs oder Router bieten nur Spezialausrüster an. Sie finden aber auch WLAN-Router mit einem USB-Steckplatz für einen HSDPA-Stick.

Falls Sie einen Internetzugang in einer DSL-freien Zone (auch ohne LWL-Anschlussmöglichkeit) benötigen, ist in einigen Gebieten vielleicht WIMAX (nach IEEE 802.16) eine Alternative. Der in Deutschland genutzte Frequenzbereich liegt bei 3,5 GHz, die maximale (theoretische) Datenrate beträgt 3,5 Mbit/s. Von den Anbietern werden Ihnen Download-Raten von 1 oder 2 Mbit/s angeboten. Verbesserungen sind in Entwicklung, Standard: IEEE 802.16j-2009.

2.3.3 Powerline Communication (PLC)

Warum verwenden Sie nicht einfach die schon vorhandenen Stromleitungen für den Datentransport? Sie müssen keine zusätzlichen Kabel durch Büros oder auch heimische Wohnstuben ziehen. Einfach einstecken – und die PCs sind verbunden. Die Werbung flüstert es Ihnen so ein. Zumindest eines stimmt: Sie brauchen keine zusätzlichen Datenkabel. Was nicht in den bunten Prospekten steht, lesen Sie in den nächsten Zeilen.

PLC dient dem Datentransport über Stromversorgungsleitungen. Das Verfahren war schon in der »vordigitalen« Ära zum Ansteuern von »Nachtstromverbrauchern« (Nachtspeicheröfen, Waschmaschinen ...) in Benutzung und arbeitete ursprünglich bis zu einer Frequenz von 148,5 kHz (damit konnten Schwachlasttarife überhaupt erst verwirklicht werden). Mit der Erweiterung der Nutzung auf die Anbindung von Haushalten an das Internet bzw. zur Datenkommunikation innerhalb eines Betriebes/Haushaltes wurden die Nutzfrequenzen angehoben. Es werden mittlerweile bis zu 200 Mbit/s als Übertragungsrate erzielt.

Mit PLC-Geräten können Sie Störungen des Rundfunkempfangs und anderer Funkdienste in Ihrer Umgebung verursachen, da die benutzten Stromleitungen in der Regel nicht abgeschirmt sind und daher wie Sendeantennen wirken. Funkstellen in der Nachbarschaft, die auf den gleichen Frequenzen arbeiten, können wiederum die Datenübertragung stören oder gar unmöglich machen. Geräte mit schlechter Funkentstörung verringern die Übertragungsrate genauso wie mehrere PLC-Anwender an einer Phase (bis zum Zähler- oder Hausanschluss, teilweise auch grundstücksübergreifend). In letzterem Fall kommt übrigens hier wie beim 10Base2 der CSMA-Zugriff zum Einsatz.

PLC-Modems verschiedener Hersteller arbeiten nicht immer zusammen. Selbst bei unterschiedlichen Modellreihen aus dem gleichen Haus konnte dies schon beobachtet werden.

Es besteht die Gefahr, dass Überspannungen aus natürlichen und technischen Quellen den PLC-Adapter beschädigen und gegebenenfalls auf das angeschlossene Gerät (PC, Modem) durchschlagen.

Im gewerblichen/beruflichen Bereich ist die Anwendung von PLC für Datennetze ohne Bedeutung, bei der Energieversorgung wird sie im Zusammenhang mit den »Smart Grids« an Bedeutung gewinnen, hier im Normalfall aber bei geringen Datenraten und niedrigen Frequenzen.

In Sonderfällen (Maschinenbau) können Sie die PLC-Technik zusammen mit geschirmten Stromkabeln aber gut einsetzen. Setzen Sie entsprechende Sperrmittel ein, damit die Signale nicht in das ungeschirmte Stromnetz eintreten können. Treffen Sie Maßnahmen, dass Überspannungen nicht zu Folgeschäden bei den Datenverarbeitungseinrichtungen führen. Prüfen Sie durch Messungen, ob die strom- und signalführende Leitung frei von störenden Impulsen ist (Elektromotoren, Steuerungen, Lampendimmern ...). Ist das nicht der Fall, so müssen Sie ein »sauberes« Stromnetz aufbauen, das frei von den genannten Störungen ist.

2.4 Technische Anbindung von Rechnern und Netzen

Am Ende eines Netzwerkkabels finden Sie immer eine Vorrichtung, die die Daten zum Nutzsignal aufbereitet. Auch in Hubs und Switches finden Sie die als *Transceiver* (Kunstwort aus *Transmitter* und *Receiver*) bezeichneten Vorrichtungen. Die Schnittstelle zwischen dem Transceiver und dem weiteren Gerät trägt in Abhängigkeit von der Übertragungsgeschwindigkeit eine eigene Bezeichnung:

- *Attachment Unit Interface* (AUI) bei 10 Mbit/s
- *Media Independent Interface* (MII) bei 100 Mbit/s
- *Gigabit Media Independent Interface* (GMII) bei 1 Gbit/s
- *10Gigabit Media Independent Interface* (10G-MII)

Sie finden die technischen Vorrichtungen unter anderem auf Netzwerkkarten, im Innenleben von USB-Sticks oder auf den Hauptplatinen von Rechnern.

2.5 Weitere Netzwerkkomponenten

Sie machen irgendwann auch einmal Bekanntschaft mit weiteren Netzwerkkomponenten, die entweder durch den Fortschritt bereits überholt sind oder einfach seltener ein-

gesetzt werden. Wichtig ist, dass Sie einfach wissen, dass es diese Dinge gibt und wofür man sie einsetzt:

- **Repeater** gehören zum Layer 1 des OSI-Schichtenmodells. Ihre Aufgabe besteht in der Umgehung von Längenbegrenzungen einzelner Netzwerksegmente mit gleichem Medium. Das Signal wird hier nicht nur pegelmäßig verstärkt, sondern auch wieder mit der notwendigen Flankensteilheit versehen, also »aufgefrischt«. Hat ein Repeater mehrere Anschlüsse, spricht man auch von einem Hub (diese sind in dieser Reinform aber nicht mehr gebräuchlich, sondern wurden in der Praxis durch die Switches abgelöst).
- **Medienkonverter** verbinden verschiedenartige Übertragungsmedien miteinander. An zentraler Stelle kommen sie meist unmittelbar neben Switches mit »Kupfertechnik« vor, wenn wegen größerer Streckenlängen auf Glasfaser umgesetzt werden muss. Am anderen Ende der Strecke, z. B. in einem Büro, wird wiederum auf »Kupfer« umgesetzt. Dazu werden entweder einzelne Medienkonverter verwendet (ein Switchport = ein Anschluss = »volle« Geschwindigkeit), oder es wird ein Mini-Switch mit LWL-Port mit gebräuchlicherweise fünf oder acht Anschlüssen eingesetzt. (Einen Switchport teilen sich im Extremfall fünf oder acht Teilnehmer, entsprechend langsamer sind diese angebunden.)
- **Hubs** stellen den Netzknoten bei der Twisted-Pair-Verkabelung dar. »Blanke« Hubs ohne weitere Ausstattung sind nichts anderes als eine Art Sammelschiene für die sternförmig abgehenden Netzwerkleitungen. Das Signal wird wie in einem Repeater behandelt.

2.6 Zugriffsverfahren

Sobald sich mehr als zwei Partner ein Medium (WLAN, Koaxialkabelnetz, Hub) teilen, benötigen Sie Verfahren, die das Miteinander regeln. Sie dürfen das direkt mit dem klassischen Funkverkehr vergleichen, wo sich die Partner gegenseitig zum Senden auffordern müssen oder eine Leitstelle für »Funkdisziplin« sorgt.

2.6.1 CSMA/CD, Kollisionserkennung

Wenn Sie Rechner über »geteilte« Medien verbinden, kommt es leicht vor, dass zwei oder mehrere Teilnehmer gleichzeitig senden. Der sendende Transceiver erkennt dies anhand der Signalspannung zwischen den eigenen Zeichen und gibt das *JAM-Signal* auf das Medium. Alle weiteren Teilnehmer erkennen nun, dass es zu Kollisionen gekommen ist, und stellen ihre Aussendungen zunächst ein bzw. verharren »auf Empfang«.

Durch gesetzte Timer bleibt dieser Zustand für kurze Zeit bestehen, und eine Station beginnt nun mit ihrer Aussendung. *CSMA/CD* (Carrier Sense Multiple Access/Collision Detection) begegnet Ihnen bei 10-Mbit/s-Netzen (10Base-5, 10Base2 und 10Base-T mit Hub).

2.6.2 CSMA/CA, Kollisionsvermeidung

Bei WLAN-Netzen werden Kollisionen von vornherein vermieden. Erkennt die Funkeinrichtung, dass niemand anders den Kanal belegt, wird er mit dem *Request-to-send-Signal* (*RTS*) reserviert. Kommt keine Kollision zustande, halten sich alle weiteren Partnerstationen mit dem Senden zurück, und die Funkeinrichtung beginnt mit der Datenübertragung. Nach der Übertragung der »Nutzlast« wird der Kanal mit dem *Clear-to-Send-Signal* (*CTS*) wieder für andere Nutzer freigegeben.

2.7 Prüfungsfragen

1. Welche Betriebsgefahren gehen von LWL-Netzwerkanlagen aus?
2. Warum sollten Sie niemals ungeschirmte Netzwerkkabel (UTP) verwenden?
3. Mit welcher Maßnahme wird in WLAN-Netzen verhindert, dass mehrere Stationen gleichzeitig senden?
4. Sie sollen ein Netzwerk errichten, über das sehr vertrauliche Daten übertragen werden. Auf welche Übertragungstechniken sollten Sie dabei verzichten?

Die Auflösungen finden Sie in Anhang B, »Auflösungen zu den Prüfungsfragen«.

Kapitel 10
Netzwerkpraxis

Netzwerke schaffen!

In diesem Kapitel finden Sie zusammengefasste Informationen zur Planung, zum Bau und zum Betrieb von Netzwerken. Sie finden hier Anregungen für die Umsetzung eigener Projekte.

10.1 Planung von Netzwerken

Die Planung eines Netzwerks können Sie in verschiedene Phasen unterteilen. Damit erreichen Sie mehr Klarheit und schaffen mehr Entscheidungsspielraum. Bevor Sie den ersten Meter Netzwerkkabel verlegen (lassen), haben Sie bereits

- den Bedarf und
- den Ist-Zustand ermittelt,
- die räumlichen und baulichen Verhältnisse erkundet,
- sich Gedanken über die Ausfallsicherheit gemacht und
- Investitionssicherheit und Unterbringung durchdacht.

10.1.1 Bedarf ermitteln

Für Nachrüstungen und Neubauten müssen Sie die Zahl der Netzwerkanschlüsse überschlägig ermitteln.

Wie viele Netzwerkanschlüsse Sie in einem Betrieb benötigen, hängt überwiegend vom tatsächlichen Gebrauch der EDV ab. Bei Verkabelungsprojekten versuchen die Bauherren oft die Kosten dadurch zu drücken, dass sie auf Nachrüstmöglichkeiten und den Einsatz von mobilen Mini-Switches setzen. Einfache und kostengünstig vorzunehmende Nachrüstungen sehen Sie sowieso vor. Beim Einsatz von Mini-Switches sollten Sie aber Folgendes bedenken:

- Bei zugriffsintensiven Netzwerkteilnehmern wird die Kapazität der Zuleitung zum Hauptswitch mit jedem aktiven Anschluss des Mini-Switchs geteilt. Damit werden die Zugriffe für die angeschlossenen Geräte verlangsamt (Abbildung 10.1).

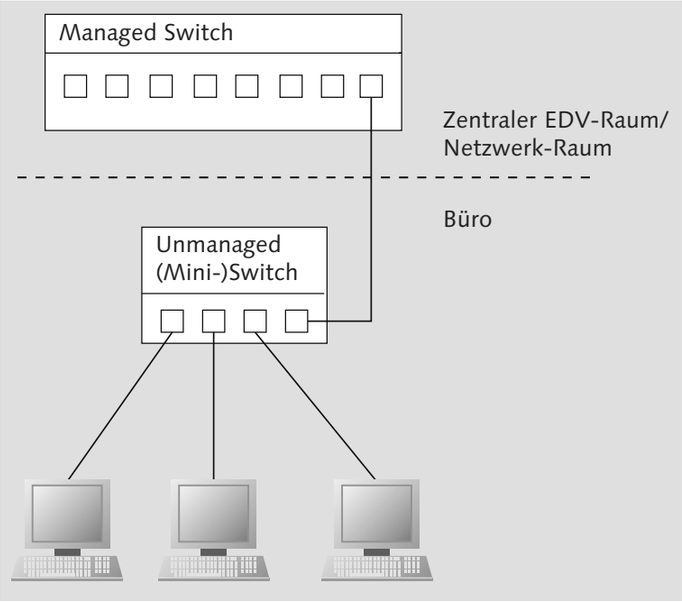


Abbildung 10.1 Weiterverteilung mit Mini-Switch

- Sicherheitsmaßnahmen am Haupt-Switch wirken meist nur beim Mini-Switch, nicht bei daran angeschlossenen PCs und Druckern.

Sehen Sie deshalb nur 1:1-Anschlussmöglichkeiten zum zentralen Switch vor!

Wie viele Anschlüsse Sie je Arbeitsplatz vorsehen müssen, hängt natürlich von der Art des Geräteeinsatzes ab:

- Wie viele PCs oder Thin Clients benutzt eine Person an einem Arbeitsplatz?
- Verwenden Sie Netzwerkdrucker/Printserver?
- Müssen mitgebrachte Außendienst-Laptops am gleichen Arbeitsplatz angeschlossen werden, oder sehen Sie für diese Personen eigene Büros vor?
- Haben Sie vor, Voice-over-IP als Haustelefon einzusetzen?
- Werden Überwachungskameras, Fernwirkeinrichtungen, Steuerungen, Besucherterminals, Werbemonitore usw. eingesetzt?

- Maschinen: Wie viele Anschlüsse hat eine Maschine, und wie viele kommen zum Einsatz?
- Administrative Arbeitsplätze: Betreiben Sie mehrere Netze (»Echtnetz« und »Schattennetz«)?
- Arbeiten Sie mit Reserveräumen?
- Liegt das Gebäude in einem Überschwemmungsgebiet? (Eventuell müssen Sie die Lage des EDV-Raumes anpassen.)
- Sind Erweiterungen in der nahen, planbaren Zukunft für Sie schon vorhersehbar?

Nach Ihren Erhebungen richten sich:

- die Zahl der Anschlüsse, also der Netzwerkdosen und Zuleitungen in den Räumen
- die Zahl der Anschlüsse am zentralen Switch
- die Leistungsmerkmale des zentralen Switchs
- die Zahl der Anschlüsse am zentralen Patchfeld
- die Aufnahmefähigkeit der Kabeltrassen
- der Bau neuer Kabeltrassen
- die Größe und die zusätzliche Ausstattung zentraler Netzwerk- und Rechnerräume
- zusätzliche Maßnahmen, wie die Berücksichtigung einer höheren Brandlast und die eventuelle Erweiterung der Sicherheitstechnik
- rechtliche Rahmenbedingungen (Unfallverhütungsvorschriften, Baurecht etc.)

10.1.2 Ermitteln des Ist-Zustands

Bei Erweiterungen und Erneuerungen der Netzwerkinfrastruktur müssen Sie abwägen, was Sie von der vorhandenen Technik noch über längere Zeit verwenden können.

Für Ihre Entscheidung müssen Sie Folgendes feststellen:

- Reichen die Anschlüsse im Arbeitsplatzbereich aus?
- Ist die Übertragungsgeschwindigkeit für Ihre Anwendungen noch über einen längeren Zeitraum ausreichend?
- Sind die verbauten Kabel noch für höhere Geschwindigkeiten nutzbar?
- Sind die verbauten Kabel mit dem Telefonnetz kombiniert (strukturierte Verkabelung, gemeinsame Nutzung der Kabel für Telefon und 100Base-T-Netze)?
- In welchem Zustand befinden sich die zentralen Einrichtungen?

- Haben zentrale Komponenten wie Switches und Patchfelder noch freie Kapazitäten?
- Verfügt der zentrale Switch über zeitgemäße Ausstattungsmerkmale (Sicherheit, VLAN usw.)?
- Sind zentrale Komponenten nach derzeitigen und vorhersehbaren künftigen Kriterien ausreichend untergebracht, gesichert und gegebenenfalls klimatisiert?
- Mit welchem Aufwand lassen sich Erweiterungen installieren?
- Sind eventuell vorhandene Kabeltrassen aufnahmefähig?
- Stehen weitere Sanierungsmaßnahmen für das Gebäude an?

Die Antworten auf diese Fragen fließen in Ihre Planungen mit ein. Bei einem Neubau haben Sie natürlich keine »Altlasten« zu berücksichtigen.

10.1.3 Berücksichtigung räumlicher und baulicher Verhältnisse

Bei einem Neubau können Sie meist die Bedürfnisse der Netzwerktechnik in vollem Umfang berücksichtigen. Anders sieht es bei Bestandsbauten aus. Hier müssen Sie bei der Einbringung der neuen Netzwerktechnik auf weitere Gegebenheiten Rücksicht nehmen:

- Denkmalschutz: Wie können Sie trotzdem Kabelkanäle oder Unterputz-Leitungen in das Gebäude einbringen?
- Bausubstanz: Haben Sie Feuchtigkeit im Gebäude?
- Grundriss: Wie lässt sich das Leitungsnetz am effektivsten anordnen?
- Sicherheit: Wie kann der EDV-Raum einfach und effektiv geschützt werden?
- Telefonnetz: Ist hier eine ausreichende Infrastruktur vorhanden? Können hier Kabelarbeiten zusammengefasst werden?
- Klimatisierung: Wie können Sie die eventuell notwendige Klimatechnik im Rechnerraum unterbringen?
- Stromversorgung: Reicht die Gebäudestromversorgung aus? Wo können Sie eine USV-Anlage unterbringen?
- Brandschutz: Hat das Einbringen der Verkabelung und die damit verbundene Erhöhung der Brandlast Folgen?
- Brandmeldeanlage: Ist eine solche Anlage vorhanden oder notwendig?
- Zutrittskontrolle/Alarmanlage: Ist eine Anlage vorhanden oder muss eine errichtet werden?

10.1.4 Investitionssicherheit

Auch bei der Planung des Netzwerks stehen Sie zwischen kaufmännischen Zwängen und technischer Vernunft. Falsches Sparen führt aber auch hier dazu, dass Sie später mit eventuell teuren Nachrüstmaßnahmen »belohnt« werden. Schenken Sie deshalb einigen Punkten Beachtung:

- Sind für Sie Erweiterungen des Netzes absehbar?
- Können Sie bereits jetzt günstig die Voraussetzungen für solche Erweiterungen schaffen (mehr Trassenplatz, mehr Einbauplatz für Switches und Patchfelder, Auslegung von USV und Klimatechnik)?
- Verwenden Sie die Verkabelungstechnik mit der höchstmöglichen Übertragungsgeschwindigkeit.
- Raumanbindung: Setzen Sie zusätzliche Leerrohre ein, oder sehen Sie größere Kabelkanäle vor.
- Sehen Sie eine leichte Austauschbarkeit der Verkabelung vor. Zu solchen Maßnahmen gehören neben Leerrohren und Kabelkanälen mit mehr Platz *Zugdosen* und weiter gefasste Radien in der Kabelführung.
- Switch(es): Können Sie diese Geräte einfach per gesichertem Webzugang konfigurieren, oder müssen Sie auf systemabhängige proprietäre Software zurückgreifen?
- Switches: Können und dürfen Sie diese selbst konfigurieren?
- Zentrale Komponenten (Switch, USV, Klima): Wie lange und unter welchen Kosten und Bedingungen gewähren Hersteller oder Lieferanten zentraler Komponenten eine unbedingte Schadenersatzleistung (Garantie)? Welche Zeiten werden für die Wiederherstellung der Funktionsbereitschaft angeboten? Unterscheiden Sie zwischen Reaktionszeit und Reparaturzeit. Können Sie günstig eine Garantieverlängerung abschließen?
- Zentrale Komponenten: Wer kommt zur Behebung einer Störung? Hat der Kundendienst eine lange Anfahrt?
- Zentrale Komponenten: Achten Sie auf vollständige IPv6-Kompatibilität.

10.1.5 Ausfallsicherheiten vorsehen

In Grenzen können Sie Ihre Netzwerkinfrastruktur vor Ausfällen schützen. Hauptsächliche Gründe für einen Ausfall können sein:

- Stromausfall: Hiergegen setzen Sie ein USV-Konzept ein (unterbrechungsfreie Stromversorgung).
- Funktionsausfall Switch: Halten Sie entweder ein Reservegerät oder Reservebaugruppen vor, oder bilden Sie den zentralen Switch aus mehreren managebaren kleineren Einzelgeräten. Von den kostengünstigen Einzelgeräten beschaffen Sie eines oder mehrere als Ausfallreserve.
- Kabelschaden: Schaffen Sie die Möglichkeit des leichten Kabelwechsels, sehen Sie auch Reserveleitungen in wichtigen Bereichen des Betriebs vor.
- Klimatisierung: Verteilen Sie, wenn möglich, die Arbeit auf mehrere Anlagen.
- Abhängigkeit von Kundendiensten: Achten Sie bei Ihrer Auswahl darauf, dass Sie und gegebenenfalls Ihre Kollegen bei Ausfällen so viel wie möglich selbst beheben können.
- VoIP: Wenn das LAN ausfällt, ist niemand telefonisch erreichbar. Es sollte zumindest eine kleine Telefonanlage für Geschäftsleitung, EDV und Hausmeister sowie wichtige Abteilungen mit Kundenkontakt oder gefahrenorientierten Arbeiten installiert sein. Meist ist in größeren Betrieben eine Brandmeldeanlage installiert, die einen eigenen Anschluss an das Telefonnetz besitzt. Diesen können Sie auf mehrere ISDN-Kanäle »aufweiten« lassen und dafür nutzen. Verzichten Sie aber sowohl auf DECT-Telefone (sie funktionieren nicht bei Stromausfall) als auch auf Funktelefone für das öffentliche Netz. Bei Letzteren erwarten Sie vielerlei Probleme, vom leeren, ungepflegten Akku bis hin zur Tatsache, dass niemand die Nummern der anderen Geräte kennt.

10.1.6 Zentrales oder verteiltes Switching

Je nachdem, wie Ihr Gebäude beschaffen ist, können Sie die zentralen Komponenten entweder in einem zentralen Raum oder nach Gebäuden bzw. Stockwerken unterteilt unterbringen. Die zentrale Unterbringung (Abbildung 10.2) bietet Ihnen Vor- und Nachteile:

- Einen zentralen, gegebenenfalls überwachten Raum: In diesem sind auch andere Komponenten wie Router, Server und das zentrale Patchfeld untergebracht.
- Anschlussmöglichkeit an die USV
- Ein großer Switch oder mehrere kaskadierte Geräte tragen zur Erwärmung des EDV-Raums bei.

Die verteilte Unterbringung der Switches auf dem Betriebsgrundstück oder im Haus ist sicher bei besonders umfangreichen Installationen auch eine Überlegung wert:

- Ein kompletter Netzausfall ist (fast) unmöglich.
- Es kommt zu keiner zusätzlichen Erwärmung durch die Switches.
- Ersparnis bei der Verkabelung, da zu den einzelnen Räumen hin kürzere Verbindungen genutzt werden (stockwerksweise, flurweise usw.).

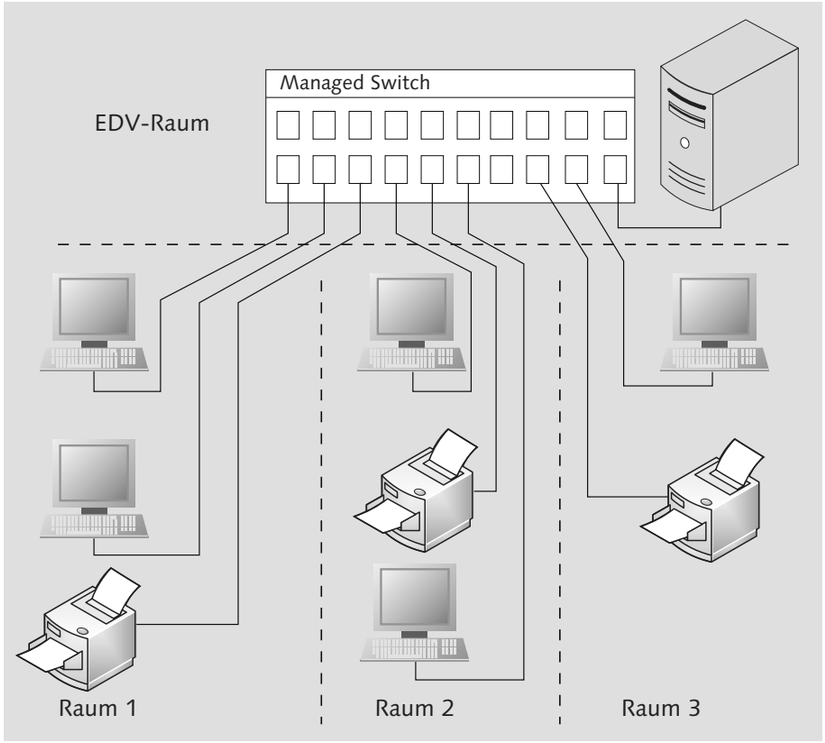


Abbildung 10.2 Zentraler Switch

- Aber: Sie benötigen managebare Switches, die das *Port Trunking* (Link Aggregation) unterstützen. Einige Anschlüsse der Switches werden hierfür benötigt und stehen nicht für den Anschluss von Netzwerkteilnehmern zur Verfügung (siehe Abschnitt 4.6.3, »Verbindungen zwischen Switches (Link Aggregation, Port Trunking, Channel Bundling)«, und Abbildung 10.3).
- In bestimmten Fällen können Sie die Trunking-Verbindungen auch in Glasfasertechnik ausführen. Dies ist sogar notwendig, wenn die zulässigen Leitungslängen überschritten werden. Insgesamt ist die gemischte Ausführung (Kupfer/LWL) kostengünstiger als eine reine Glasfaserverkabelung.

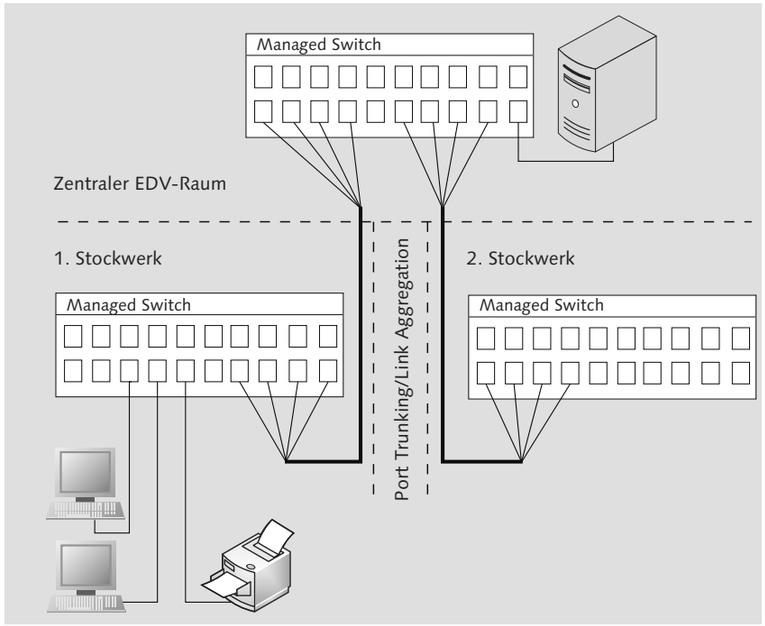


Abbildung 10.3 Verteiltes Switching

10.2 Netzwerke mit Kupferkabeln

Besonders räumlich kleinere Netze können Sie noch auf Jahre hin günstig in Kupfertechnik betreiben:

- Für Verkabelungsarbeiten benötigen Sie nur einfache Werkzeuge.
- Sie haben geringere Kosten für Router und Switches.
- Die Standardnetzwerkanschlüsse der Endgeräte (PCs, Thin Clients und Printserver) reichen aus.
- Mögliches Problem: Potenzialunterschied zwischen zwei Gebäuden, die Sie per Kupferkabel verbinden möchten. Diese eine Verbindung führen Sie besser in Glasfasertechnik aus.
- Beachten Sie: Die Schirmungen fest verbauter Netzwerkkabel müssen durch einen Fachmann mit dem Potenzialausgleich des Gebäudes verbunden werden.

Technische Erläuterungen zu Kupferkabeln finden Sie in Abschnitt 2.1.2, »Netze mit Twisted-Pair-Kabeln«.

10.2.1 Kabel (Cat. 5 und Cat. 7)

Für die Ergänzung von älteren Bestandsnetzen können Sie in Einzelfällen noch das Kabel nach Cat. 5 verbauen. Bei Neuinstallationen oder umfangreichen Ergänzungen verwenden Sie lieber Cat. 7. Es ermöglicht nicht nur schnellere Datenverbindungen, es ist auch hinsichtlich seiner Schirmung deutlich besser.

Wenn Sie Kabel nach Cat. 7 verbauen, werden Sie immer noch auf die herkömmlichen RJ45-Steckerverbindertechnik zurückgreifen, auch wenn diese nicht der Cat.-7-Norm entspricht. Bis 1 Gbit/s können Sie damit übertragen. Ob sich noch neuere Normen mit höherer Geschwindigkeit für die Datenübertragung auf Kupfernetzen durchsetzen, ist nicht klar. Bevor Sie hierauf warten, verwenden Sie besser die Glasfasertechnik.

10.2.2 Anforderungen an Kabeltrassen und Installationskanäle

Ihre Kupferverkabelung benötigt eigene Kabeltrassen und Installationskanäle. Sie dürfen die Netzwerkkabel nicht zusammen mit Stromkabeln in einem gemeinsamen Kanal führen (Abbildung 10.4). Wenn Sie am gleichen Ort einen Netzwerk- und Stromanschluss benötigen, müssen Sie daher getrennte Kabelkanäle oder solche mit zwei getrennten Kammern (Abbildung 10.5) verwenden. Gleiches gilt für Leerrohre.

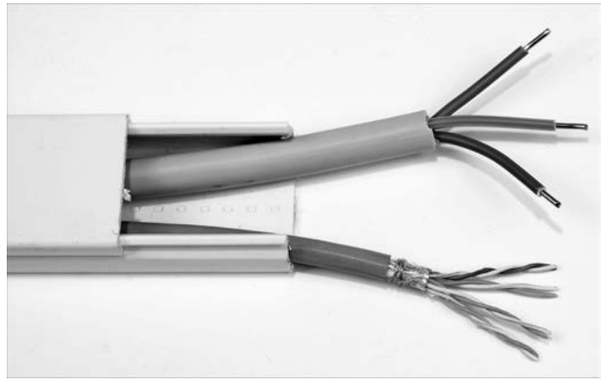


Abbildung 10.4 Verboten: gemeinsame Führung von Strom- und Netzwerkkabeln

Kabelrinnen, die Sie entlang von Geschossdecken, aber auch Hallendächern (z. B. in Verbrauchermärkten, Werkhallen) anbringen lassen, müssen das Gewicht der Kabel sicher tragen. Denken Sie auch an mögliche Nachrüstungen, die vielleicht hierin verlegt werden.

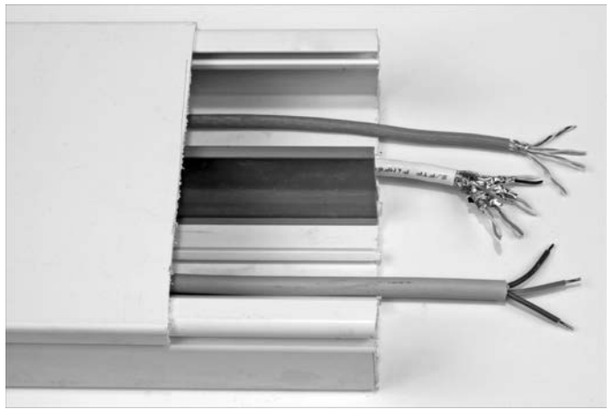


Abbildung 10.5 Richtig: Strom- und Netzwerkkabel befinden sich in getrennten Kammern des Kabelkanals.

Die Kabelrinnen sollen auch nicht so überquellen, dass Kabel beschädigt werden können. Bringen Sie nur so viele Kabel in Kabelkanäle ein, dass Sie den Deckel noch ohne Druck und Gewalt wieder anbringen können. Bei Leerrohren ziehen Sie nur so viele Kabel ein, dass Sie jederzeit defekte Kabel herausziehen können.

Achten Sie darauf, dass über Ecken und Kanten geführte Kabel nicht geknickt werden. Wenn es für Sie möglich ist, schaffen Sie größere Biegeradien.

Lassen Sie sich auch von einem Brandschutz-Experten hinsichtlich weiterer Maßnahmen in Sachen Brandlast beraten. Zwischen Brandabschnitten verlaufende Kabeltrassen benötigen unter Umständen ein Brandschott.

Ihre Netzwerkkabel sollten Sie vor Nässe, Fraßschäden (Lagerhausbetriebe!) und anderen Beschädigungen geschützt führen.

10.2.3 Dosen und Patchfelder

Bringen Sie Netzwerkdosen und Kabelkanäle so an, dass diese nicht beschädigt werden:

- In Werks- und Lagerhallen, aber auch in Verbrauchermärkten und an ähnlichen Orten besteht die Gefahr, dass Sie mit Flurförderzeugen Kabelkanäle und Dosen regelrecht »abrasieren«. Hier bringen Sie einmal in Palettenhöhe (ca. 10 cm über dem Boden) und nochmals je 50 cm und 100 cm über dem Boden Schutzkeile an der Wand an. Damit weisen Sie an der Mauer entlangschrammende Fahrzeuge und ihre Lasten ab (Abbildung 10.6).

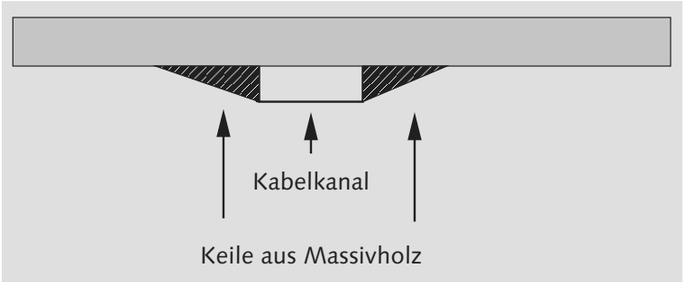


Abbildung 10.6 Schutzkeile für Aufputzkabelkanäle und Netzwerk-Anschlussdosen

- Im Umfeld von Kleinkindern (Arztpraxen, Kindertagesstätten, Kindergärten oder auch zu Hause im Kinderzimmer) können Sie die Dose mit einem RJ45-Blindstopfen vor kleinen »Elektrikerfingern« schützen.
- In Werks- und Lagerhallen mit hohem Staubanfall bewahren Sie Ihre Netzwerkdosen mit diesen Blindstopfen vor übermäßiger Verschmutzung der Kontakte.

Patchfelder verwenden Sie in der Hauptverteilung beim Switch (Abbildung 10.7) oder als Stockwerksverteiler. Sie sollten diese vor unbefugtem Zugriff schützen. Achten Sie darauf, dass sie vom Elektrofachmann an den Potenzialausgleich des Gebäudes angeschlossen werden.

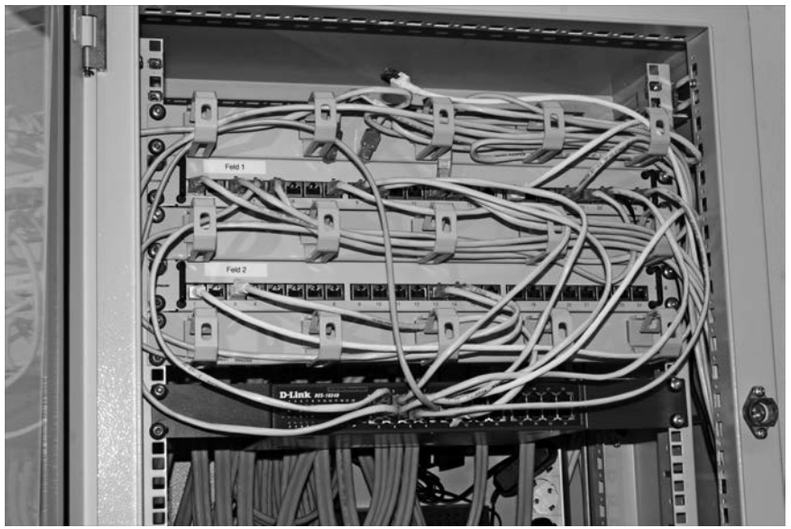


Abbildung 10.7 Netzwerkschrank mit Patchfeldern und Switch

Wie Sie die Patchfelder unterbringen, hängt vor allem von deren Größe und Menge ab. Hohe Anschlusszahlen montieren Sie in eigenen Netzwerkschränken, wie die aktiven Komponenten auch. Hier ist es wichtig, dass Sie keine zu langen Patchkabel zum Verbinden benötigen. Beschriften Sie jedes Patchkabel an beiden Enden jeweils in Steckernähe mit einer laufenden Nummer. Bei vielen Verbindungen können Sie sich bei Konfigurationsarbeiten die Kabelnummer und die Steckplätze an Switch und Patchfeld notieren. Im Störungsfall werden Sie das schnelle Auffinden der beteiligten Komponenten sehr schätzen. Kleine Patchfelder können Sie in entsprechenden Schränken hochkant montieren, womit Sie Aufbautiefe einsparen.

Patchfelder sollten Sie ebenso vor Feuchtigkeit schützen. Nicht benutzte Anschlüsse verschließen Sie mit den vorhin erwähnten RJ45-Blindstopfen und schützen damit die Kontakte vor Verschmutzung.

10.3 Netzwerke mit Glasfaserkabeln

Für räumlich größere Netze, aber auch bei Neubauten empfehlen sich Glasfaserkabel. Vor dem Bau oder der Erweiterung Ihres Netzes müssen Sie aber für Ihre Planung auf einige Besonderheiten Rücksicht nehmen:

- Sie können Glasfaserkabel zusammen mit Stromleitungen in einem Kanal, einer Kabelrinne oder einem Leerrohr gemeinsam verlegen (Abbildung 10.8).
- Sie brauchen keine Rücksicht auf einen möglichen elektrischen Potenzialunterschied zwischen zwei Gebäuden zu nehmen.
- Glasfaserkabel benötigen keinen Anschluss an den Potenzialausgleich eines Gebäudes.
- Für die Installationsarbeiten von Glasfasern benötigen Sie Spezialwerkzeuge.
- Für Messungen und die Fehlersuche an Glasfaserstrecken brauchen Sie (teure) Messgeräte.
- Sie können dadurch Kosten sparen, dass Sie vorkonfektionierte Kabel in räumlich kleineren Netzen verwenden. An diesen befinden sich bereits an beiden Enden die Steckverbinder. Dies können Sie nutzen, wenn Sie für die Leitungsführung vor allem Kabelrinnen und zu öffnende Kanäle verwenden. Sie müssen die Kabel dann nur über kurze Strecken durch Mauer- und Deckendurchbrüche ziehen. Wenn Sie Leerrohre verwenden, sollten diese innen eine glatte Oberfläche aufweisen. Bedenken Sie auch, dass Sie die Kabel mit einem Stecker oder Steckerpaar durch das Rohr ziehen und schieben müssen. Es darf hier also nicht zu eng werden, sonst wird das Kabel beim Einbringen beschädigt.

- Sie können einen gemischten Betrieb mit herkömmlicher Kupferverkabelung einrichten. Dies können Sie vor allem bei Bestandsnetzen so handhaben. Aber auch für schnelle Backbones zwischen Etagen-Switches oder Gebäuden können Sie die Glasfasern einsetzen. Die Versorgung der Arbeitsplätze geschieht dann wiederum über die Kupferverkabelung (Abbildung 10.3). Weitere Informationen finden Sie in Abschnitt 2.2, »Lichtwellenleiter, Kabel und Verbinder«.

Abbildung 10.8 Gemeinsame Führung von Glasfaser- und Stromkabeln

10.3.1 Kabeltrassen für LWL-Kabel

Sie können Glasfaserkabel wie Kupferkabel auch durch Leerrohre, Kabelkanäle und Kabelrinnen führen:

- Beachten Sie bei der Verlegung unbedingt die vom Hersteller angegebenen minimalen Biegeradien. Anders als ein Kupferkabel können Sie ein LWL-Kabel nicht »um die Ecke« verlegen. Sie müssen Platz für »runde« Führungen vorsehen.
- Auch Glasfaserkabel dürfen keiner Staunässe ausgesetzt werden. Für diese Zwecke gibt es aber speziell ummantelte Kabel.
- Vermeiden Sie große mechanische Beanspruchungen Ihrer LWL-Kabel. Diese können besonders bei der gemeinsamen Führung mit Stromkabeln auftreten.
- Bei längeren Strecken benötigen Sie Platz für die sichere und trockene Aufbewahrung der Spleißboxen. Dafür verwenden Sie abschließbare Unter- oder Aufputzschränke. Im Freien auf dem Werks- oder Campusgelände benutzen Sie entsprechende Verteilerkästen. Im Gegensatz zu herkömmlichen Spleißmuffen, die Sie in Kabelschächten unterirdisch unterbringen, erreichen Sie hier die Kabel bei jeder Witterung. Stellen Sie den Kasten aber so auf, dass er nicht durch Fahrzeuge, Flurförderzeuge oder Lastkräne beschädigt werden kann. Eventuell bauen Sie einen entsprechend starken mechani-

schen Schutz auf. Wenn Sie Ihr Gelände nicht gegen den Zutritt Unbefugter schützen können, bringen Sie die Kästen so unauffällig und stark gesichert wie nur möglich unter.

- Auch Glasfaserkabel erhöhen die Brandlast!

10.3.2 Dosen und Patchfelder

Dosen und Patchfelder können Sie genauso anbringen, wie Sie es von der Kupfertechnik her gewohnt sind. Sichern Sie Aufputzkanäle und Dosen, wie für die Kupferkabel in Abschnitt 10.2.3, »Dosen und Patchfelder«, gezeigt wurde. Einige Besonderheiten müssen Sie wegen der andersartigen Betriebsgefahren beachten:

- Sichern Sie ungenutzte LWL-Dosen und Steckplätze an Patchfeldern und Medienkonvertern so ab, dass niemand in die Öffnungen blicken kann (Unfallverhütung, Augenschutz).
- Die Schutzabdeckungen verhindern auch, dass Staub, Ölfilme und Feuchtigkeit die empfindliche Optik verschmutzen.
- Bauen Sie das räumliche Umfeld von Patchfeldern und Medienkonverterleisten wegen nicht abzusehender Weiterentwicklungen großzügig auf.
- Auch bei den Patchkabeln müssen Sie Biegeradien beachten. Sparen Sie deshalb nicht mit Halterungen, an denen die Kabel zugfrei geführt werden.

10.3.3 Medienkonverter

Für gemischte Netzwerke benötigen Sie Medienkonverter zur Signalumsetzung. Diese erhalten Sie in verschiedenen Bauformen:

- 19-Zoll-Einbau-Leiste oder -Feld (EDV-Raum, Stockwerksverteiler)
- Modul für Switches (Bauformen GBIC, SFP, XFP)
- Einzelgerät zur Montage in einer Wanddose, auf Hutschiene oder Aufputz
- Mini-Switch mit einem LWL-Anschluss
- Tischgerät mit einem Kupferanschluss

Bei Medienkonvertern handelt es sich um aktive Komponenten. Für diese müssen Sie einen Stromanschluss vorsehen. Verwenden Sie 19-Zoll-Felder im EDV-Raum, müssen Sie die eventuell entstehende Abwärme in Ihre Klimatisierungsberechnung mit einbeziehen. Ein Beispiel für ein Tischgerät finden Sie mit dem *Edimax ET-913MSC+*. Er setzt von 1000Base-T nach 1000Base-SX (Multimode) um. Er verfügt über einen RJ45- und einen SC-Duplex-Anschluss. LEDs für die Link-Kontrolle und Aktivität befinden sich an

der Frontplatte. Sie können mehrere dieser Konverter im Rack ET-920MCR zusammenfassen und in Ihrem Netzwerkschrank im EDV-Raum unterbringen.

10.3.4 LWL-Multiplexer

Mittels LWL-Multiplexer verbinden Sie auch weiter auseinanderliegende Firmenstandorte. Die Glasfaserverbindung stellt Ihnen Ihr Telekommunikationsdienstleister zur Verfügung. Meist werden zwei oder vier Monomode-Fasern bereitgestellt. Sie können je Faserpaar einen herkömmlichen Medienkonverter für Monomode-Fasern anschließen. Sie schaffen damit eine Kopplung zum entfernten LAN mit 10 oder maximal 100 Mbit/s.

Wenn Sie einen LWL-Multiplexer zur Standortverbindung benutzen, erhöhen Sie die Verbindungsgeschwindigkeit enorm. Sie können dabei Übertragungsraten zwischen 1 Gbit/s und 10 Gbit/s nutzen.

Der Multiplexer teilt den Datenstrom auf mehrere Wellenlängen auf, die er gleichzeitig in eine Faser einspeist. Beim Empfänger werden die verschiedenfarbigen Signale wieder zu einem Datensignal zusammengesetzt. Eine weitere Variante filtert auf der Empfängerseite die einzelnen Farben aus und gibt diese zur weiteren Konvertierung (optisch/optisch oder optisch/elektrisch) weiter. Damit ist es Ihnen möglich, Port-Trunking zwischen zwei Switches über ein WAN zu benutzen. LWL-Multiplexer arbeiten mit verschiedenen Verfahren:

- **WWDM**, *Wide Wavelenght Division Multiplex*
- **CWDM**, *Coarse Wavelength Division Multiplex*; Übertragungsraten bis 10 Gbit/s über 70 km ohne Repeater sind möglich.
- **DWDM**, *Dense Wavelength Division Multiplex*; Übertragungsraten von 10 bis 100 Gbit/s über 80–200 km werden erreicht.

LWL-Multiplexer dieser Art finden Sie unter anderem auf der Webseite *www.lambdaline.com/de* der Firma DeltaNet AG (Dietikon, Schweiz) dargestellt.

10.4 Geräte für Netzwerkverbindungen und -dienste

Bei der Kupferverkabelung haben Sie nach wie vor die RJ45-Steckverbindung als Standard. Hier können Sie hinsichtlich der Anschlusstechnik keine Fehler machen. Bei Glasfaserkomponenten müssen Sie immer auf die Anschlussnormen achten.

10.4.1 Netzwerkkarten

Neue PCs und Notebooks verfügen über eingebaute Netzwerkanschlüsse. Netzwerkkarten kaufen Sie im Reparaturfall und zur Aufrüstung.

Netzwerkkarten für PCs werden von allen gängigen Betriebssystemen unterstützt. Alle neueren Typen unterstützen Übertragungsraten bis 1 Gbit/s. Sie stellen sich aber auch automatisch auf 100 Mbit/s oder 10 Mbit/s ein. Weit verbreitet sind Netzwerkkarten mit dem Chipsatz der Firma Realtek (Tabelle 10.1).

Chipsatz	10Base-T	100Base-TX	1000Base-T	Steckplatz
RTL8139	X	X	–	PCI
RTL8169	X	X	X	PCI
RTL8111	X	X	X	PCI-Express

Tabelle 10.1 Chipsätze der Firma Realtek

Für Ihren Server verwenden Sie spezielle Netzwerkkarten. Diese sind für den harten Dauergebrauch ausgelegt. Einige Modelle benötigen einen PCI-EXPRESS-x8-Einbauplatz. Dafür bekommen Sie 10 Gbit/s Übertragungsrate für LWL (*Ethernet Server Adapter X520-SR2* der Firma Intel, 2 × LC-Anschluss, Multimode). LWL-Netzwerkkarten für Büro-PCs sind eher selten im Einsatz (z. B. *Allied Telesis AT 2916SX/SC*, SC-Duplex, 1000Base-SR, Multimode, PCI-Steckplatz).

Der Handel bietet ferner sogenannte USB-Netzwerkkarten an. Technisch gesehen sind diese Adaptergeräte. Mit ihnen können Sie Rechner über den USB-Anschluss an Ihr Netzwerk anbinden.

10.4.2 WLAN-Router und -Sticks

In Privathaushalten finden Sie oft WLAN-Router vor, mit denen die Verbindung zum Internet hergestellt wird. Oftmals werden diese Geräte nicht über den Handel, sondern über den Telekommunikationsdienstleister bezogen. Einige dieser Geräte verfügen über einen zusätzlichen USB-Anschluss. Über den stecken Sie ein UMTS- oder LTE-USB-Funkmodem an. Fällt die DSL-Verbindung aus, arbeiten Sie drahtlos weiter. Auch in Gegenden mit keiner oder sehr schlechter DSL-Anbindung stellen solche Geräte den Internetanschluss her.

Allgemein finden Sie bei diesen Geräten meist eine Firewall, einen DHCP-Server, PAT/NAT und manchmal sogar einen VPN-Client vor.

Der Router WL0082 aus dem Hause LogiLink (Abbildung 10.9) eignet sich wegen seiner Größe für den Außendienst- oder Hotelzimmereinsatz. Ihr Notebook verbinden Sie dabei per LAN-Kabel mit dem Mini-Router. An diesem steckt Ihr Funkmodem. Damit bauen Sie eine eigene Internetverbindung unabhängig von der Netzinfrastruktur des Hotels auf. Sie können damit unkompliziert VPN- oder SSH-Tunnelverbindungen betreiben. Den Mini-Router können Sie auch noch als WLAN-Accesspoint einsetzen.

Die WLAN-Funktechnik finden Sie praktisch in allen mobilen Rechnern. Wenn diese defekt geworden ist, benötigen Sie einen USB-WLAN-Stick als Ersatz. Mithilfe dieser Sticks können Sie auch PCs mit dem WLAN verbinden.

Abbildung 10.9 WL0082 von LogiLink

10.4.3 Router

Mit einem Router verbinden Sie Netze. Die notwendigen Geräte erhalten Sie in unterschiedlicher Leistungsfähigkeit und Softwareausstattung. Modelle mit hohem Datendurchsatz verfügen über mehrere Netzwerkschnittstellen und extra ausgeführte Wartungsanschlüsse. Einige dieser Hochleistungsrouter können Sie über eine eigene Backbone-Verbindung auch zu einem einzigen logischen Gerät vereinen. Achten Sie beim Einsatz dieser Geräte auf den Anschluss über eine unterbrechungsfreie Stromversorgung und auf die anfallende Abwärme, besonders beim Einbau in 19-Zoll-Schränke. Derartige hochprofessionelle Geräte werden u. a. von Cisco oder HP gefertigt.

Während Hochleistungsrouter sich oft ausschließlich der Aufgabe des Datentransports widmen, übernehmen die Kompaktgeräte in kleineren Firmen, Praxen und Privathaushalten weitere Aufgaben: NAT/PAT, Firewall, VPN-Client, Proxy- oder DHCP-Server. In viele dieser Geräte ist neben den üblichen Netzwerkanschlüssen auch WLAN, ggf. ein DSL- oder Kabelmodem, integriert, sodass man mit einem Gerät alle Bedürfnisse abdeckt.

Ein sehr verbreitetes Modell dieser Geräteklasse ist der *Linksys WRT54-GL* (Abbildung 10.10 und Abbildung 10.11).

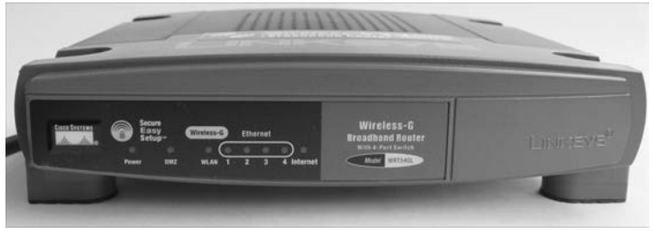


Abbildung 10.10 Linksys WRT54-GL, Frontseite

Abbildung 10.11 Linksys WRT54-GL, Anschlussseite

Dieser Router verwendet ein Linux-basiertes System (das durch das freie OpenWRT ersetzt werden kann). Falls Sie den Router ohne den Einsatz der mitgelieferten Setup-CD konfigurieren möchten, finden Sie in Tabelle 10.2 die notwendigen Daten für den ersten Zugriff.

IP-Adresse	192.168.1.1
Benutzername	(ohne)
Kennwort	admin

Tabelle 10.2 Zugriffsdaten für den »Linksys WRT54-GL«

Falls Ihr lokales Netz nicht die Adresse `192.168.1.0` aufweist, müssen Sie wenigstens einen PC mit einer Adresse aus diesem Netz versehen, z. B. `192.168.1.20`. Diese Adresse wird kaum von Routern mit DHCP-Dienst verwaltet, sodass ihre Verwendung eher nicht zu Problemen führen dürfte. In Microsoft Windows finden Sie diesen Punkt in der Systemsteuerung, unter Linux reicht (als Benutzer `root`, für die erste Netzwerkkarte) der Aufruf:

```
ip addr add 192.168.1.20/24 dev eth0
```

Laden Sie auf diesen PC gleich die aktuelle Firmware von der Herstellerseite *http://support.linksys.com/de-eu/support/routers/WRT54GL* herunter. Sie wird im Anschluss aufgespielt.

Verbinden Sie sich per Webbrowser nun mit dem Router, indem Sie dessen Adresse `192.168.1.1` eingeben.

Wechseln Sie in das Menü ADMINISTRATION, und darin wählen Sie FIRMWARE UPGRADE. Klicken Sie auf DURCHSUCHEN, und wählen Sie die neue Firmwaredatei aus. Abbildung 10.12 zeigt den Upgrade-Vorgang.

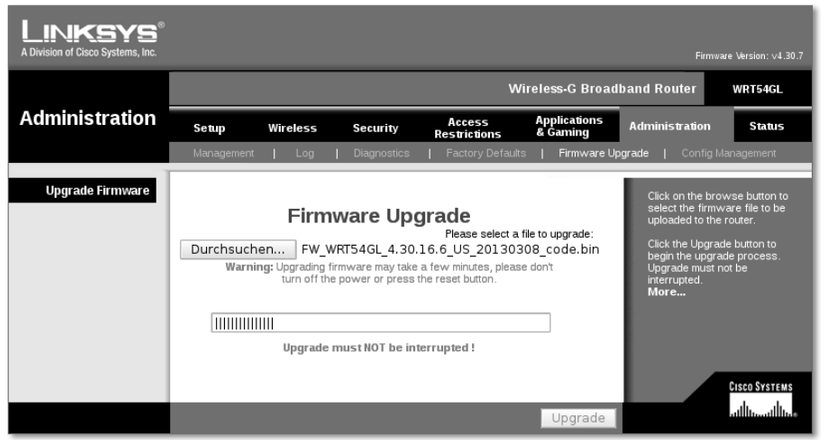


Abbildung 10.12 Firmware-Upgrade für den »Linksys WRT54GL«

Nach dem Upgrade starten Sie den Router nochmals neu und verbinden sich wieder mit dem Gerät.

Nach dem Aufruf landen Sie in der Maske, in der Sie Ihren DSL-Internetzugang und die Zeitzone einrichten können (Abbildung 10.13). Die DHCP-Einstellungen dürften für die meisten Anwendungsfälle unverändert verwendbar sein.

Abbildung 10.13 Einstellungen für Internetzugang und Zeitzone

Im folgenden Schritt sorgen Sie für sicherere Einstellungen bezüglich des Konfigurationszugangs (ADMINISTRATION • MANAGEMENT, siehe Abbildung 10.14). Ändern Sie in jedem Fall das Kennwort ab, und lassen Sie ausschließlich kabelgebundenen Zugang per HTTPS für die Weboberfläche zu. Stellen Sie auch die Möglichkeit des Remote-Managements und von UPnP ab.

Die weiteren Schritte, wie gegebenenfalls die Einrichtung eines WLANs, Zugriffbeschränkungen und weitere Verfeinerungen, nehmen Sie im Anschluss daran vor. Vergessen Sie nicht, Ihre Einstellungen zu sichern. Dazu gehen Sie zu ADMINISTRATION • CONFIG MANAGEMENT und klicken auf BACKUP (Abbildung 10.15).

Abbildung 10.14 Einrichtung des Konfigurationszugangs

Abbildung 10.15 Sichern der Einstellungen

Sie können diesen Kleinrouter auch zum Verbinden zweier Netze verwenden. Im Beispiel aus Abbildung 10.16 soll das Netz `192.168.1.0` mit `192.168.0.0` kommunizieren. Anstelle der vorhin gezeigten Internetverbindung wählen Sie hier STATIC IP und geben die Adresse des Routers im Zielnetz ein. Vergessen Sie den DNS-Eintrag nicht. Im Beispiel sehen Sie den Router des übergeordneten Netzes `192.168.0.1`.

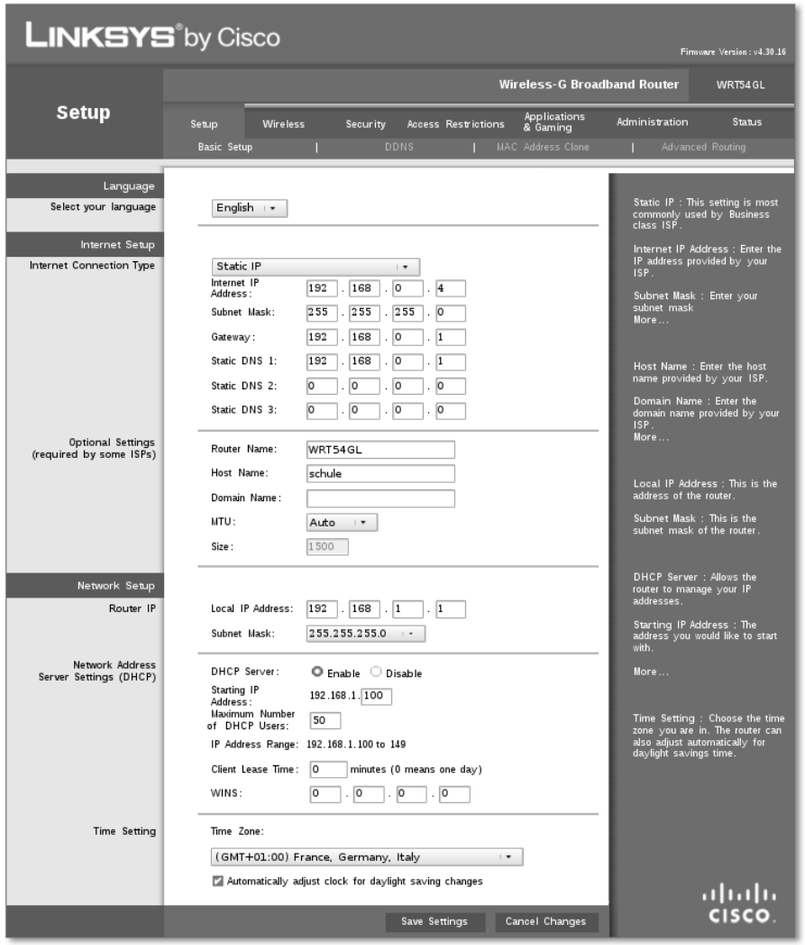


Abbildung 10.16 Verbindung zweier Netze

Auf dem WRT54GL und weiteren verschiedenen Routern und Kleinrechnern können Sie OpenWRT (*www.openwrt.org*) anstelle von proprietärer Firmware nutzen. Das Linux-

basierte System verleiht den meisten Geräten zusätzliche Eigenschaften, wie z. B. die Fähigkeiten eines VPN-Clients, und zumindest oftmals schnellere Sicherheitsupdates. Wenn Sie den Wunsch haben, es einzusetzen, sehen Sie auf der Webseite nach, ob Ihr Routermodell unterstützt wird. Ältere Konstruktionen wie der Linksys WRT54GL können wegen Speichermangel nicht die neuesten Entwicklungen nutzen. Diese laufen aber in jedem Fall auf diversen Kleinrechnern (z. B. dem Raspberry Pi). Speziell für den Linksys WRT54GL werden im Internet Anleitungen zur Speicheraufrüstung gezeigt. Wenn Sie sich zutrauen, SMD-ICs aus- und einzulöten, erhalten Sie eine deutlich leistungsfähigere Hardware. Informieren Sie sich unter *http://wiki.openwrt.org/toh/linksys/wrt54g*!

Besonders beim WRT54GL ist die Hardwareversion wichtig. Sie finden die notwendige Angabe auf der Unterseite des Geräts beim Barcode-Aufkleber von Seriennummer und MAC-Adresse (hier: v1.1).

Laden Sie sich von *http://downloads.openwrt.org/backfire/10.03.1/brcm-2.4/* die Datei *openwrt-wrt54g-squashfs.bin* herunter. Melden Sie sich am Router an, und führen Sie ein Upgrade mit der neuen »Firmware« wie in Abbildung 10.12 gezeigt durch. Nach erfolgtem Upload startet der Router neu. Dieser Vorgang kann bis zu zwei Minuten dauern. Das Gerät ist anschließend per `telnet` unter der Adresse `192.168.1.1` erreichbar. Geben Sie auf einer Linux/Unix-Shell oder im CMD-Fenster von Microsoft Windows `telnet 192.168.1.1` ein. Führen Sie als Erstes `passwd` (Vergabe eines sicheren Kennworts) aus. Beenden Sie die Sitzung mit `reboot`. Nach dem erneuten Start ist das Gerät nicht mehr per `telnet` erreichbar, sondern über `ssh`. Microsoft Windows-Benutzer benötigen `putty`, um per SSH eine Verbindung zur weiteren Konfiguration aufzubauen. Anwender von Linux, FreeBSD und Verwandte verbinden sich per Shell wieder mit dem Router: `ssh root@192.168.1.1`. Eine Sitzung wird stets mit `exit` beendet, außer Sie weisen einen Systemneustart an.

Die Entwickler von OpenWRT empfehlen, für eine »Notbetankung« per `tftp` folgende Einstellungen zu setzen und anschließend den Router neu zu starten:

```
nvram set boot_wait=on
nvram set boot_time=10
nvram commit && reboot
```

Melden Sie sich wieder an, und installieren Sie das deutsche Sprachpaket für die Weboberfläche:

```
opkg update && opkg install luci-i18n-german
```

Falls Sie per Shell am Router einen Internetzugang einrichten möchten, funktioniert dies so:

```
uci set network.wan.proto=pppoe
uci set network.wan.username='BENUTZERKENNUNG'
uci set network.wan.password='KENNWORT'
uci commit network
ifup wan
```

Als Paketsystem verwendet OpenWRT `opkg`, eine Abwandlung von Debians `dpkg`. In Tabelle 10.3 finden Sie die wichtigsten Aktionen der Softwareverwaltung aufgelistet.

Aktion	Kommando
Liste verfügbarer Pakete auf neuen Stand bringen	`opkg update`
Paket installieren	`opkg install PAKETNAME`
Installiertes Paket durch neuere Version ersetzen	`opkg upgrade PAKETNAME`
Installiertes Paket löschen	`opkg remove PAKETNAME`
Liste verfügbarer Pakete	`opkg list`
Liste von installierten Paketen, für die es neuere Versionen gibt	`opkg list-upgradable`
Liste installierter Pakete	`opkg list-installed`

Tabelle 10.3 Wichtige »opkg«-Kommandos

Übersichtlicher geschieht die Konfiguration des OpenWRT-Routers über die Weboberfläche. Rufen Sie in Ihrem Webbrowser einfach die Adresse `192.168.1.1` auf. Sie werden dann von der Statusseite begrüßt. Als dieser Screenshot erstellt wurde, war der Zugriff auf einen Zeitserver noch nicht konfiguriert, weshalb die Ortszeit noch in der Vergangenheit liegt (Abbildung 10.17) und die Oberfläche in englischer Sprache erscheint.

Nach einem Neustart (SYSTEM • REBOOT) erhalten Sie die deutschsprachige Oberfläche.

Konfigurieren Sie jetzt das Netzwerk. Dazu klicken Sie auf NETZWERK und erhalten eine Übersicht (Abbildung 10.18) über die aktiven Schnittstellen. Sie erreichen das jeweilige Einstellmenü entweder über die obere Leiste (hier: WAN und LAN) bzw. über die Schaltfläche BEARBEITEN in der rechten Hälfte des Bildes. Sie sehen in dieser Übersicht nur die aktiven Schnittstellen (WLAN war bereits vorher abgeschaltet).

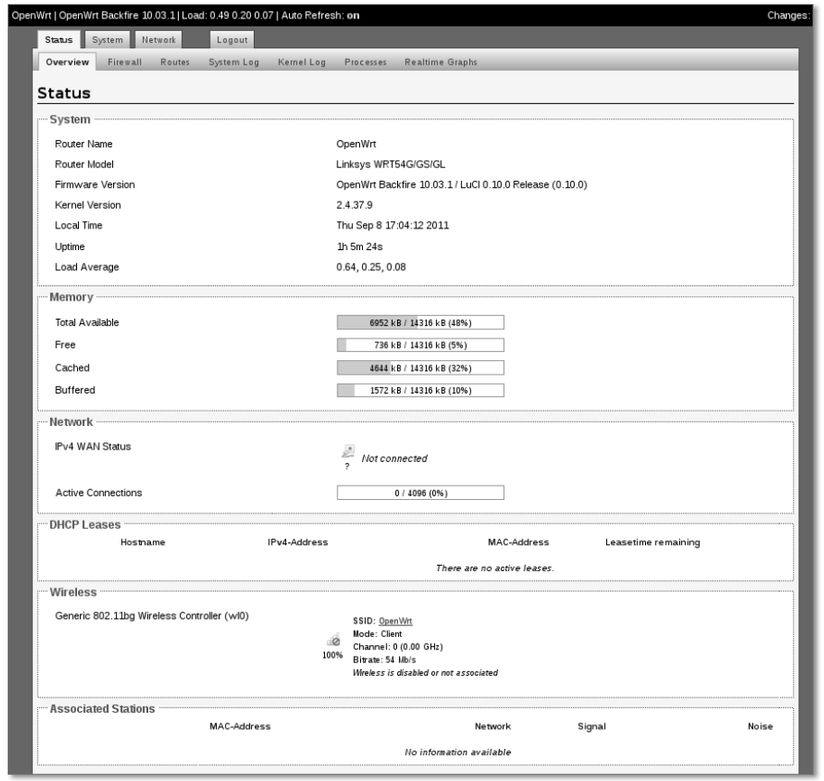


Abbildung 10.17 Statusseite bei erstmaligem Aufruf

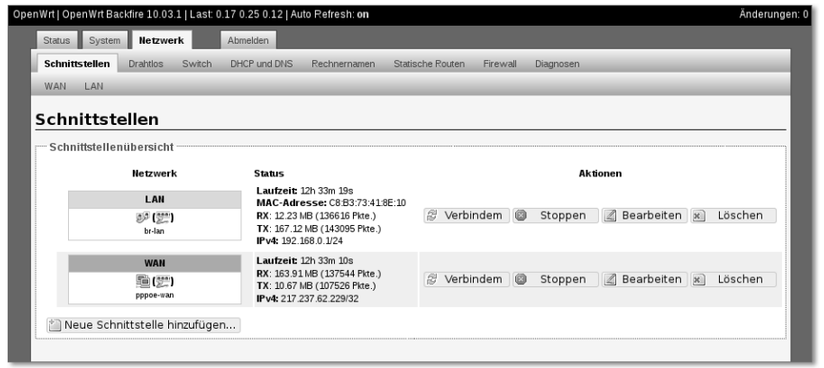


Abbildung 10.18 Übersicht über die Netzwerkschnittstellen

Konfigurieren Sie zunächst die Schnittstelle LAN (Abbildung 10.19). Hier vergeben Sie normalerweise eine feste IP-Adresse (STATIC ADDRESS). Geben Sie wenigstens die IP-Adresse und die Netzmaske ein. Im unteren Bereich der Einstellmöglichkeiten finden Sie Eintragungen zum DHCP.

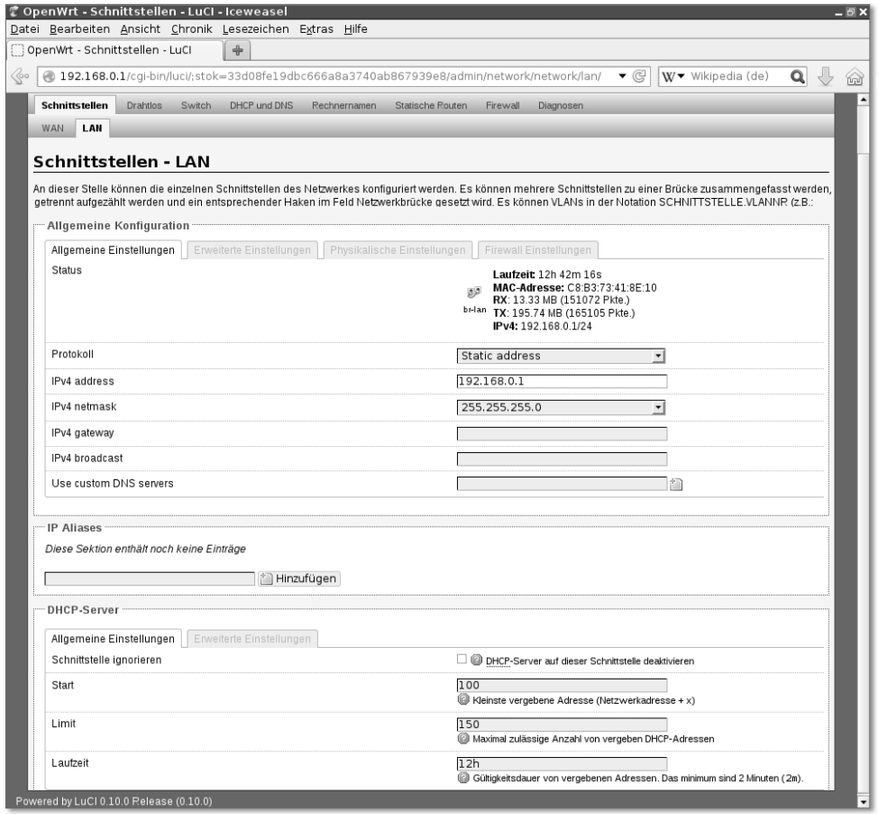


Abbildung 10.19 Konfiguration der LAN-Schnittstelle des Routers

Unter ERWEITERTE EINSTELLUNGEN können Sie unter anderem die MAC-Adresse und die MTU ändern. Bei PHYSIKALISCHE EINSTELLUNGEN können Sie Schnittstellen VLANs zuordnen und gegebenenfalls das Spanning-Tree-Protokoll aktivieren. In den FIREWALL EINSTELLUNGEN bestimmen Sie, zu welcher Zone die gerade bearbeitete Schnittstelle gehören soll (Abbildung 10.20).

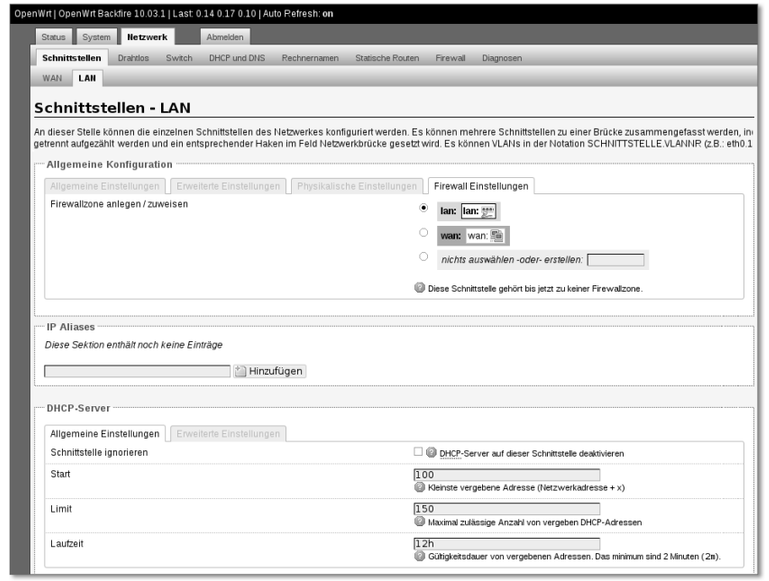


Abbildung 10.20 Zuordnung der Schnittstelle zu einer Firewall-Zone

Widmen Sie sich nun der WAN-Anbindung (Abbildung 10.21). Wählen Sie das zutreffende Protokoll, und geben Sie Ihre Zugangsdaten ein.

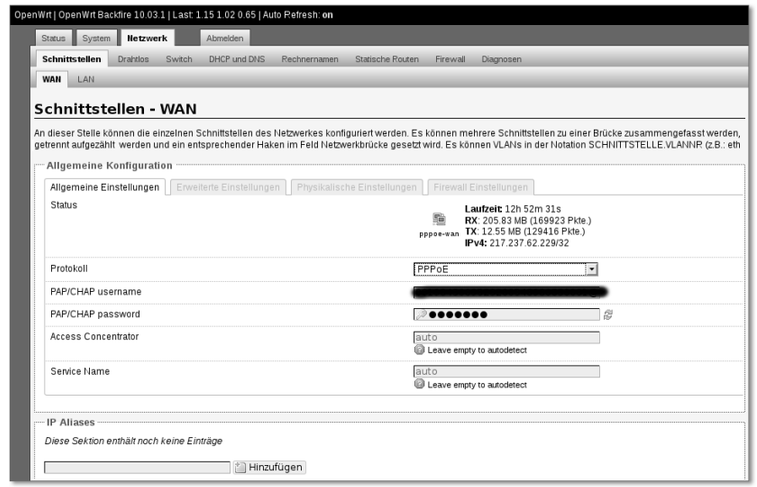


Abbildung 10.21 Einrichtung des Internet-Zugangs

Im Menü Erweiterte Einstellungen können Sie eigene Einstellungen für das Default Gateway, den vom Provider angebotenen DNS-Server, LCP und für die Verbindungsdauer vornehmen. Bei Physikalische Einstellungen setzen Sie gegebenenfalls den Punkt bei der zutreffenden VLAN-Schnittstelle. In den Firewall Einstellungen setzen Sie die Zone WAN (Abbildung 10.22).

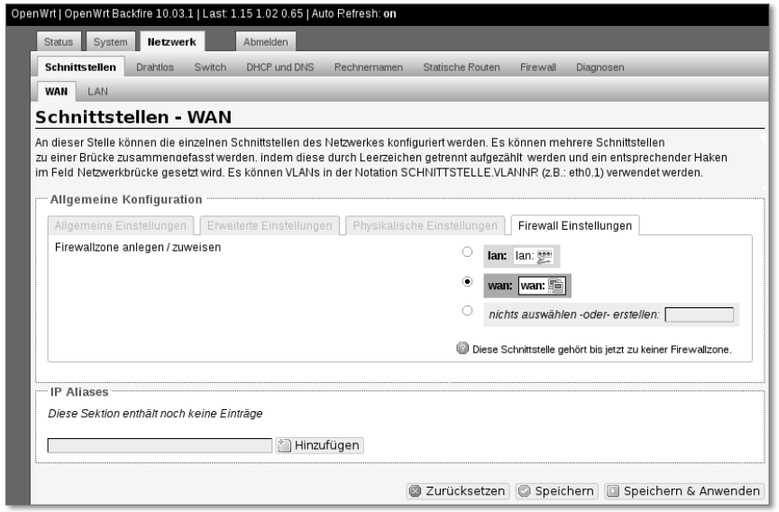


Abbildung 10.22 Zuordnung der Schnittstelle zu einer Firewall-Zone

Unter Drahtlos konfigurieren Sie, falls notwendig, das WLAN (Abbildung 10.23). Sie können das WLAN in dieser Maske aktivieren bzw. deaktivieren sowie den Kanal und die Sendeleistung festlegen. In Erweiterte Einstellungen legen Sie den Betriebsmodus und weitere technische Parameter fest (Abbildung 10.24).

Jeweils im unteren Bereich der WLAN-Konfiguration legen Sie die ESSID, den Betriebsmodus und die Zugehörigkeit zu einem Netzwerk (lan/wan) fest. Ein eigener Unterpunkt (WLAN-Verschlüsselung) ermöglicht es Ihnen, die hierzu notwendigen Festlegungen zu treffen. Unter Erweiterte Einstellungen im unteren Menübereich können Sie noch weitere Verfeinerungen einstellen.

Im Menü Netzwerk • Switch können Sie (weitere) VLANs konfigurieren.

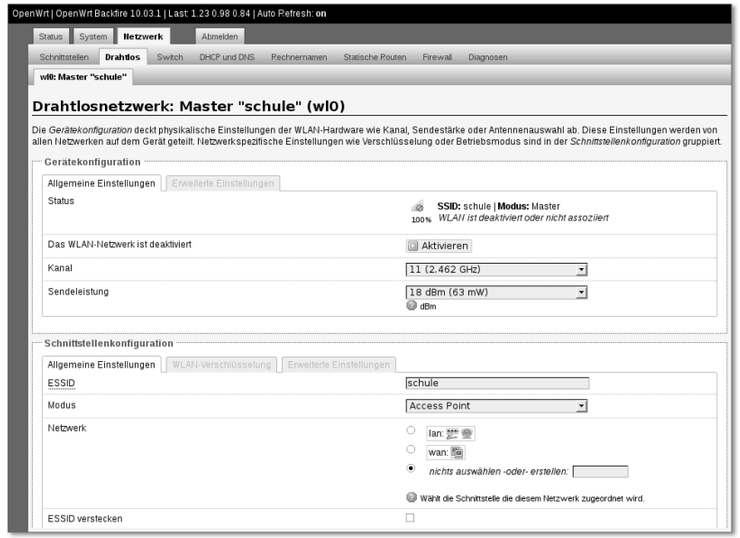


Abbildung 10.23 Festlegen technischer Parameter für das WLAN

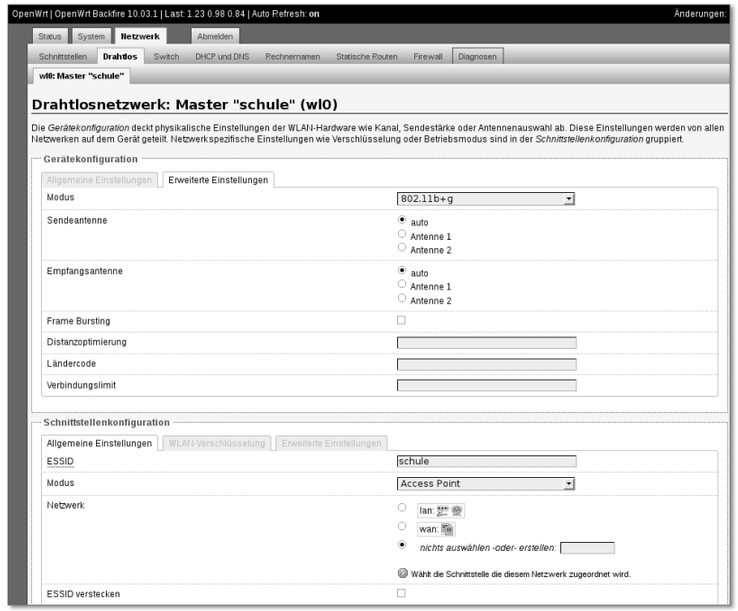


Abbildung 10.24 Erweiterte Einstellungen für das WLAN

Einstellungen zu DHCP und DNS nehmen Sie im gleichnamigen Menü (ALLGEMEINE EINSTELLUNGEN vor (Abbildung 10.25). Die weiteren Punkte ermöglichen u. a. die Verwendung einer eigenen *resolv.conf*- und *hosts*-Datei, den Betrieb eines TFTP-Servers und weiterer Einstellungen für den DNS- und DHCP-Server. Die Host-Einträge nehmen Sie dabei unter NETZWERK • RECHNERNAMEN vor. Statische Routen tragen Sie im gleichnamigen Punkt ein, wobei das Ziel ein einzelner Rechner oder ein Netzwerk sein kann.

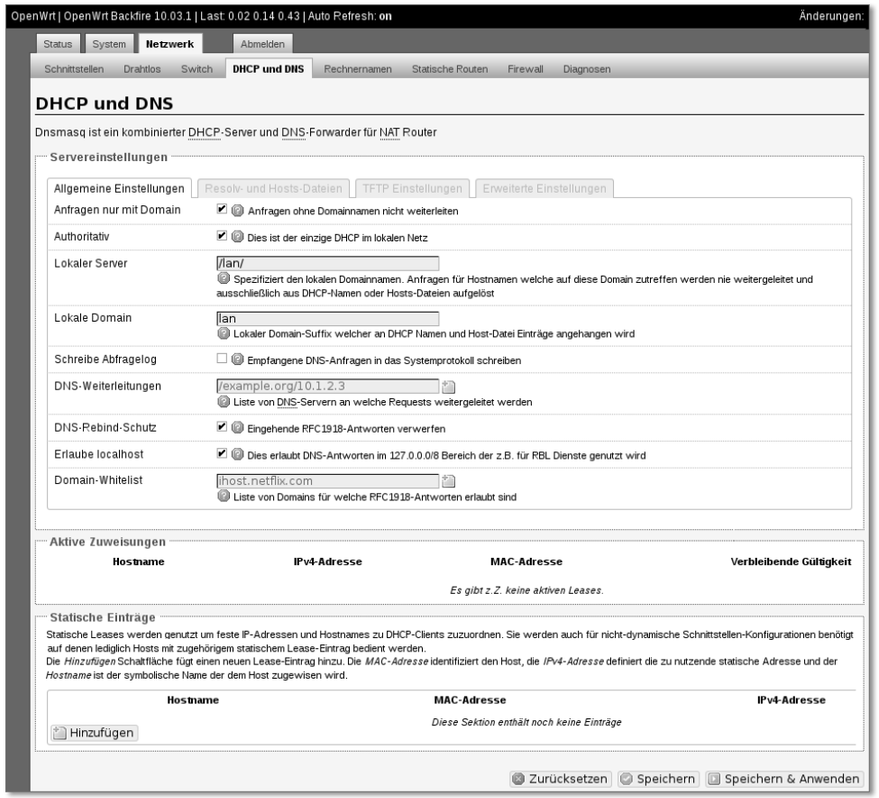


Abbildung 10.25 Einstellungen zu DHCP und DNS

Firewall-Einstellungen und -Regeln geben Sie unter NETZWERK • FIREWALL ein (Abbildung 10.26). Hier können Sie auch Port-Weiterleitungen definieren. Hierzu klicken Sie im Bereich WEITERLEITUNGEN auf HINZUFÜGEN. In der nun verfügbaren Maske (Abbildung 10.27) wird als Beispiel ein Webserver »durchgereicht«.

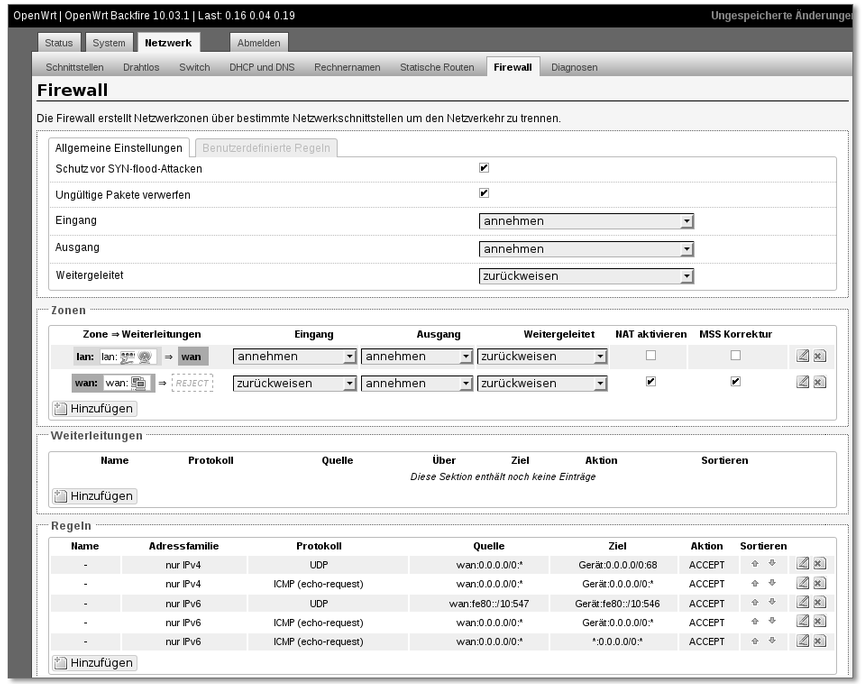


Abbildung 10.26 Firewall-Einstellungen

Abbildung 10.27 Port-Weiterleitung für Webserver einstellen

Über die Weboberfläche können Sie leicht kontrollieren, ob die WAN- und zum Teil auch die LAN-Anbindung des Routers funktioniert. Unter Netzwerk • Diagnosen stehen die Werkzeuge `ping`, `traceroute` und `nslookup` bereit.

Schränken Sie den Netzwerk-Zugriff auf den Router ein (System • Administration), und lassen Sie als Administrationszugang nur das LAN zu (Abbildung 10.28). In diesem Menü können Sie auch das Admin-Kennwort ändern. Für den SSH-Zugang können Sie zudem noch einen abweichenden Port verwenden.

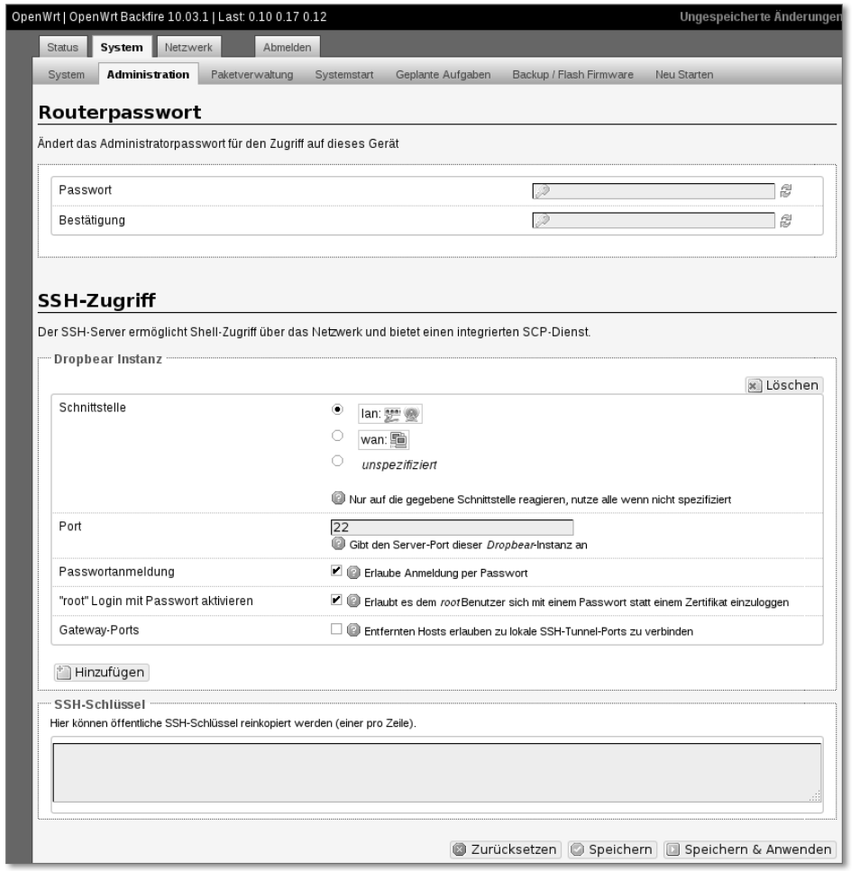


Abbildung 10.28 Administrationskennwort und Netzwerkzugriff einstellen

Unter System • Backup/Flash Firmware sichern Sie die Einstellungen (Generate archive) oder laden sie nach dem Rücksetzen (Upload archive). Das Rücksetzen

nehmen Sie mit Perform reset vor. Sollten Sie eine neue »Firmware« einspielen wollen, können Sie dies hier (Flash Image) vornehmen.

Als einfachen Router können Sie auch einen Kleinrechner wie den Raspberry Pi oder den Banana Pi einsetzen. Gegenüber »richtigen« Routergeräten fehlen hier ein integrierter Switch und ein zweiter Netzwerkanschluss. Den stellen Sie mittels eines USB-LAN-Adapters her. Die CPU- und Speicherausstattung ist besser als die der meisten Routergeräte. Dagegen sind die Kleinrechner nicht auf einen schnellen Datendurchsatz hin optimiert. Der Banana Pi übertrifft aber den Raspberry Pi hierbei erheblich. Unter *http://www.banana-pi.com/eacp_view.asp?id=64* war auch eine Router-Version davon zu sehen. Ob sie den Weg nach Europa findet, ist noch nicht absehbar.

Die Kleinrechner im Routereinsatz haben aber noch einen manchmal nicht zu unterschätzenden Vorteil. Sie können, falls Sie nicht die Weboberfläche benutzen möchten, jeden Adminstrationszugriff über das Netzwerk sperren. An den Kleinrechnern können Sie nämlich Tastatur und Bildschirm anschließen und per Shell-Zugriff arbeiten. Natürlich müssen Sie das Gerät dann entsprechend wegsperren, damit kein unbefugter Zugriff möglich ist.

Betrachten Sie das Vorgehen anhand des Raspberry Pi. Laden Sie das SD-Karten-Abbild *openwrt-brcm2708-sdcard-vfat-ext4.img* von *https://downloads.openwrt.org/barrier_breaker/14.07/brcm2708/generic* herunter. Weitere Informationen finden Sie auch auf der Projektseite *http://wiki.openwrt.org/toh/raspberry_pi*.

Unter Microsoft Windows benutzen Sie das Programm `win32diskimager`, um das Abbild auf die SD-Karte zu schreiben. Wenn Sie diesen Vorgang mittels eines Linux-Rechners erledigen wollen, gehen Sie analog Tabelle 9.3 oder wie nachstehend in Tabelle 10.4 beschrieben vor.

Aktion	Kommando	Abbildung
Feststellen der Gerätedatei	`dmesg` oder `lsblk`. Führen Sie `lsblk` vor und nach dem Einstecken der SD-Karte aus. Das neu hinzugekommene Gerät (hier: `sdc`) muss beschrieben werden	10.29
Schreiben des Abbildes auf die SD-Karte	`dd if=openwrt-brcm2708-sdcard-vfat-ext4.img of=/dev/sdc bs=1M conv=fsync`	10.30

Tabelle 10.4 Beschreiben der SD-Karte mit der Imagedatei unter Linux

Die Version »barrier_breaker« hat bereits eine mehr oder weniger komplette IPv6-Unterstützung. Die Weboberfläche verfügt über manche Erweiterung gegenüber der im WRT54GL gezeigten.

```
root@ZE6:~# # Vor Einlegen der SD-Karte
root@ZE6:~# lsblk
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sr0     11:0    1  1024M  0 rom
sda      8:0    0 111,8G  0 disk
├─sda1   8:1    0  93,1G  0 part /
└─sda2   8:2    0  18,7G  0 part [SWAP]
sdb      8:16   0 931,5G  0 disk
├─sdb1   8:17   0 838,2G  0 part /home
└─sdb2   8:18   0  93,3G  0 part /var
root@ZE6:~#
root@ZE6:~# # Nach dem Einlegen der SD-Karte
root@ZE6:~#
root@ZE6:~# lsblk
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sr0     11:0    1  1024M  0 rom
sda      8:0    0 111,8G  0 disk
├─sda1   8:1    0  93,1G  0 part /
└─sda2   8:2    0  18,7G  0 part [SWAP]
sdb      8:16   0 931,5G  0 disk
├─sdb1   8:17   0 838,2G  0 part /home
└─sdb2   8:18   0  93,3G  0 part /var
sdc      8:32   1   7,4G  0 disk
├─sdc1   8:33   1    20M  0 part /media/76A3-CAF6
└─sdc2   8:34   1    48M  0 part /media/bcbad195-d248-4e9b-854d-e644c3c8a0ad
root@ZE6:~#
```

Abbildung 10.29 Ermitteln der Gerätedatei mittels »lsblk«

```
root@ZE6:~# dd if=openwrt-brcm2708-sdcard-vfat-ext4.img of=/dev/sdc bs=1M conv=fsync
76+0 Datensätze ein
76+0 Datensätze aus
79691776 Bytes (80 MB) kopiert, 2,37416 s, 33,6 MB/s
root@ZE6:~#
```

Abbildung 10.30 Schreiben des Abbildes auf die SD-Karte

Abbildung 10.31 USB-LAN-Adapter für die WAN-Schnittstelle

Stecken Sie die SD-Karte in den Raspberry Pi, und schalten Sie das Gerät ein. Auf `192.168.1.1` können Sie sich per Web oder `telnet` anmelden. Vergeben Sie per `passwd` oder in der Weboberfläche ein Kennwort. Anschließend ist der Administrationszugang nur noch per SSH oder Web möglich. Bevor Sie aber die hier schon beschriebenen Konfigurationsarbeiten vornehmen können, muss noch der USB-LAN-Adapter (Abbildung 10.31) zum Laufen gebracht werden. Angesichts der Tatsache, dass ja noch kein WAN-Zugriff möglich ist, wurden die unten gelisteten Kernelmodule von *http://downloads.openwrt.org/barrier_breaker/14.07/brcm2708/generic/packages/base* zunächst auf einen PC heruntergeladen:

```
kmod-libphy_3.10.49-1_brcm2708.ipk
kmod-mii_3.10.49-1_brcm2708.ipk
kmod-usb-core_3.10.49-1_brcm2708.ipk
kmod-usb-net-asix_3.10.49-1_brcm2708.ipk
kmod-usb-net-mcs7830_3.10.49-1_brcm2708.ipk
kmod-usb-net_3.10.49-1_brcm2708.ipk
kmod-usb-ohci_3.10.49-1_brcm2708.ipk
kmod-usb-uhci_3.10.49-1_brcm2708.ipk
```

Melden Sie sich am Raspberry Pi per SSH an, und holen Sie die Kernelmodule per `scp`, wie in Abbildung 10.32 dargestellt.

```
root@OpenWrt:~# scp harald@192.168.1.20:/home/harald/Downloads/kmod* .
harald@192.168.1.20's password:
kmod-libphy_3.10.49-1_brcm2708.ipk                    100%   11KB  11.1KB/s   00:00
kmod-mii_3.10.49-1_brcm2708.ipk                       100%  651     0.6KB/s   00:00
kmod-usb-core_3.10.49-1_brcm2708.ipk                  100%  673     0.7KB/s   00:00
kmod-usb-net_3.10.49-1_brcm2708.ipk                   100%  696     0.7KB/s   00:00
kmod-usb-net-asix_3.10.49-1_brcm2708.ipk              100%   11KB  10.7KB/s   00:00
kmod-usb-net-mcs7830_3.10.49-1_brcm2708.ipk           100% 4213     4.1KB/s   00:00
kmod-usb-ohci_3.10.49-1_brcm2708.ipk                  100%  686     0.7KB/s   00:00
kmod-usb-uhci_3.10.49-1_brcm2708.ipk                  100%  683     0.7KB/s   00:00
root@OpenWrt:~#
```

Abbildung 10.32 Holen der Kernelmodule

Mit dem Kommando `opkg install PAKETNAME` installieren Sie die Pakete in dieser Reihenfolge:

- kmod-libphy
- kmod-mii
- kmod-usb-core
- kmod-usb-ohci
- kmod-usb-uhci
- kmod-usb-net

- kmod-usb-net-mcs7830
- mmod-usb-net-asix

Sollte dabei auf fehlende Abhängigkeiten hingewiesen werden, installieren Sie das dabei genannte Paket vorrangig. Anschließend rufen Sie nochmals den Befehl auf, der fehlgeschlagen war.

Fahren Sie nun mit `halt` den Raspberry Pi herunter, und machen Sie ihn stromlos. Schließen Sie den USB-LAN-Adapter an. Verbinden Sie den Kleinrechner nach einigen Sekunden wieder mit der Stromversorgung und melden sich wieder per Web daran an.

Klicken Sie auf NETWORK • INTERFACES und dort auf ADD NEW INTERFACE. Sie müssen den Namen `wan` dafür vergeben. Im GENERAL SETUP wählen Sie das zutreffende Protokoll (hier: statische Adresse, sonst Internetzugang) und geben die Daten hierfür ein (Abbildung 10.33).

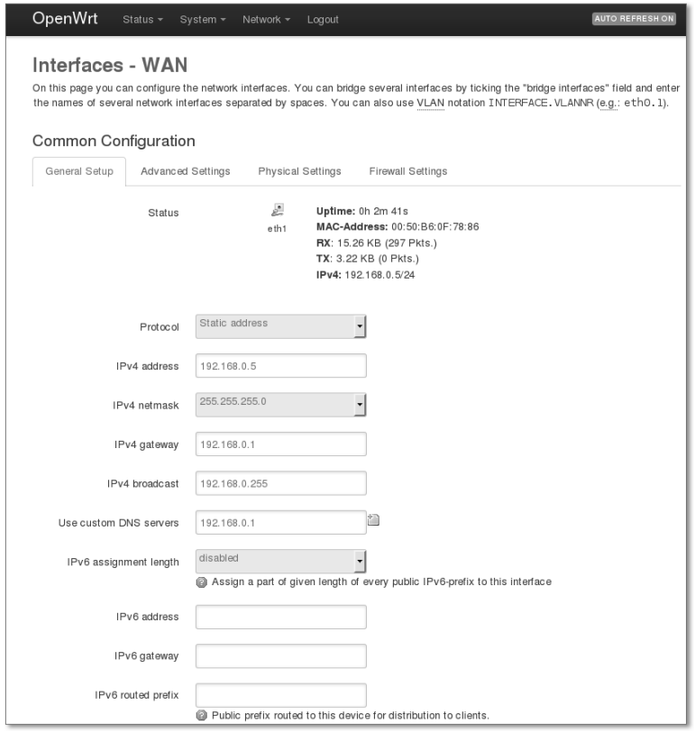


Abbildung 10.33 Konfiguration des USB-Adapters

Wechseln Sie nach PHYSICAL SETTINGS, und wählen Sie `eth1` (Abbildung 10.34) aus. Bestätigen Sie immer Ihre Eingaben mit SAVE & APPLY!

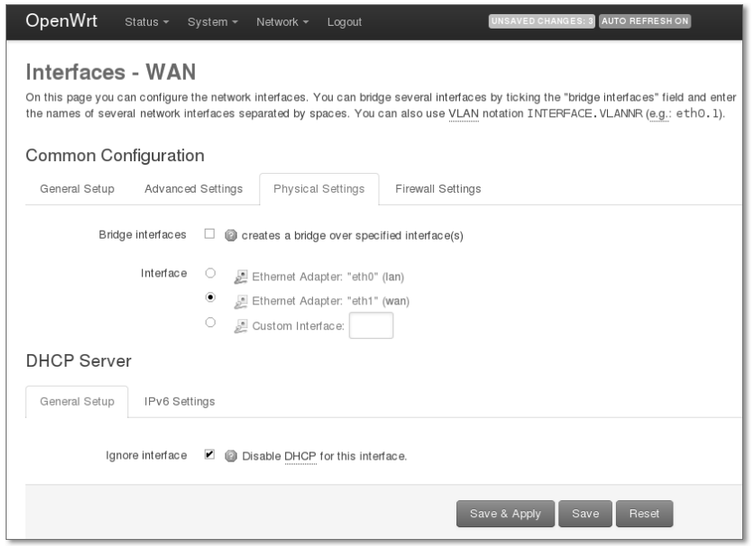


Abbildung 10.34 Zuordnung des USB-LAN-Adapters auf »eth1«

Prüfen Sie unter FIREWALL SETTINGS, ob `wan` als Firewall-Zone bestimmt ist.

Prüfen Sie bei NETWORK • DIAGNOSTICS die Funktion, und sichern Sie die Einstellungen auf einen PC (SYSTEM • BACKUP ...)!

Analog gilt das gezeigte Vorgehen für mit dem Raspberry Pi verwandte Rechner wie CubieTruck oder Banana Pi (bei Letzterem: sobald »stabile« Kartenimages vorliegen).

10.4.4 Switches

Switches erhalten Sie im Fachhandel in allen Größenordnungen. Sie können zunächst einmal grob zwischen *nicht managebaren* und *managebaren* Geräten unterscheiden. Dies ist nicht zwingend eine Frage der Größe. Auch für den Einbau in 19-Zoll-Schränke erhalten Sie nach wie vor Switches ohne Management-Modul.

Nach wie vor werden Sie noch Switches finden, die bei der Geschwindigkeit nicht über 100 Mbit/s hinauskommen. Das reicht zwar für kleine Büros und Privathaushalte aus. Bei einem Neukauf wählen Sie aber besser ein Modell, das 1 Gbit/s leistet und dabei aber auch die älteren Normen 100Base-T und 10Base-T unterstützt.

Sie bekommen kleine Tischgeräte (Abbildung 10.35), die vier oder mehr Anschlüsse besitzen. Maximal 64 Anschlüsse weisen 19-Zoll-Geräte auf. Für kleine Firmen, Kanzleien und Pensionen reicht oft eines dieser Geräte aus (Abbildung 10.36).

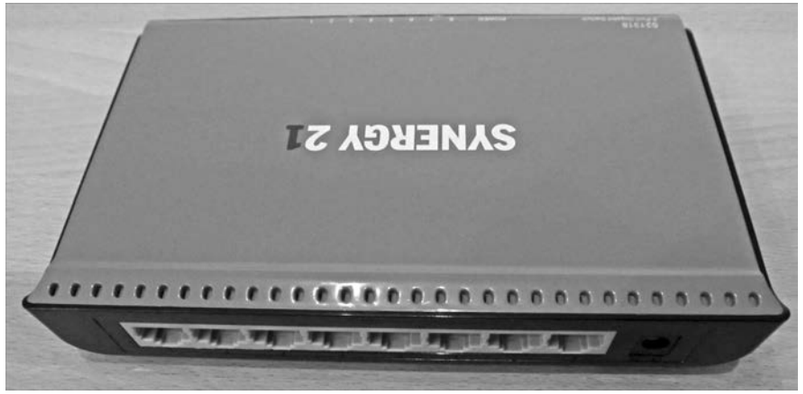


Abbildung 10.35 Tisch-Switch »S21318« der Firma Synergie 21, ohne Management-Modul

Abbildung 10.36 »DGS-1210-16« der Firma D-Link, managebar

Der in Abbildung 10.36 gezeigte Switch bietet sechzehn 1000Base-T-Anschlüsse. Weiter verfügt das Gerät über vier Einsteckplätze für SFP-Transceiver. Für jeden benutzten Einsteckplatz fällt allerdings ein 1000Base-T-Anschluss weg. D-Link bietet hierfür vier verschiedene Transceiver-Modelle an (Tabelle 10.5):

Modell	Typ	Faser	Wellenlänge	Reichweite
DEM-311GT	1000Base-SX	Multimode	850 nm	550 m
DEM-310GT	1000Base-LX	Monomode	1310 nm	10 km
DEM-314GT	1000Base-LX	Monomode	1310 nm	50 km
DEM-315GT	1000Base-LX	Monomode	1550 nm	80 km

Tabelle 10.5 Transceiver-Modelle von D-Link

Wenn Sie mehr »Switch« benötigen, wählen Sie Modelle, die über ein eigenes Backbone oder ein schnelles SFP-Modul miteinander koppelbar sind. Sie erhalten auch Switches mit einem schrankfüllenden Chassis, in das Sie verschieden bestückte Einschübe geben können. Damit bekommen Sie Ihren »Wunsch-Switch«, sogar mit Kupfer- und Glasfasertechnik gleichzeitig. Großgeräte dieser Art bieten Cisco und HP an.

Weitere Leistungsmerkmale von Switches sind redundante Netzteile, entsprechender Datendurchsatz, Power-over-Ethernet. Achten Sie bei einer Neubeschaffung in jedem Fall darauf, dass auch das Management-Modul IPv6-fähig ist. Vergleichen Sie die Größe der MAC-Adresstabelle und den Datendurchsatz je Port.

10.4.5 Printserver

Mit einem Printserver sorgen Sie dafür, dass ein Drucker über das Netzwerk erreichbar ist. In jedem Fall können Sie ihn unabhängig von den meist kurzen Anschlusskabeln zum PC da aufstellen, wo es Ihnen am besten erscheint. Sie können noch weitere Vorteile nutzen:

- Einsparung von Druckern; in größeren Büros teilen sich mehrere Arbeitsplätze ein Gerät.
- Drucker können getrennt vom Arbeitsplatz betrieben werden (Lärm, Staub).
- Wertvolle Spezialdrucker (Großformatgeräte, Foliendrucker, Plotter, Fotodrucker) bringen Sie in zentralen Räumen unter, die unter der Kontrolle der EDV-Administration liegen.
- Manchen Druckern liegt Spezialsoftware bei, mit der Sie bequem die Konfiguration und den Betrieb steuern können.
- Printserver sind vom Arbeitsplatz aus per Web konfigurierbar.

Die meisten externen Printserver (Abbildung 10.37) setzen einen Netzwerkanschluss (meist 100Base-T) auf einen einzigen USB- oder Centronix-Anschluss um. Sie bekommen besser ausgestattete Modelle, wie z. B. den Edimax PS-3103P mit drei Centronix-Anschlüssen. Am Edimax PS-3207U finden Sie zwei USB-2- und einen Centronix-Anschluss. Damit können Sie vor allem »Druckerecken« in Großraumbüros einrichten.

Sie erhalten mittlerweile viele Drucker mit eingebautem oder nachrüstbarem internen Printserver (z. B. Kyocera FS-1370DN). Hier finden Sie auch schon Modelle, die 1000Base-T unterstützen oder sogar einen LWL-Anschluss vorweisen. In Abbildung 10.38 sehen Sie einen internen Printserver für ältere Kyocera-Drucker (FS-1900, FS1010).

Abbildung 10.37 Externer Printserver

Abbildung 10.38 Interner Printserver

Ältere Printserver bergen Sicherheitsprobleme in sich:

- Jeder Benutzer kann die Einstellungen ohne Authentifizierung manipulieren.
- Der Printserver kann als Ablageort für Schadsoftware missbraucht werden.
- Die Druckdaten können nur unverschlüsselt an den Printserver geschickt werden.

Bei modernen Printservern (wie dem des Kyocera-FS1370DN) können Sie Ihre Druckdaten mit SSL-Verschlüsselung senden. Für die Änderung von Einstellungen müssen Sie sich authentifizieren.

10.4.6 Netzwerkspeicher (NAS)

Mit einem *Network Attached Storage* (*NAS*) schaffen Sie eine zentrale Möglichkeit, über Ihr lokales Netz eine zentrale Datenhaltung anzulegen. Sie können meist per SMB und NFS, auch oft mit FTP darauf zugreifen. Die Konfiguration nehmen Sie über eine Weboberfläche vor. Vielfach finden Sie diese Geräte als reine Datensicherungslösung im Einsatz.

Kleine »Netzwerkfestplatten« (Bezeichnung des Fachhandels) verfügen nur über eine Festplatte. Der Vorteil gegenüber einer reinen USB-Anstecklösung besteht in der geforderten Authentifizierung. Achten Sie beim Kauf vor allem auf die Netzwerkschnittstelle. Oft verfügen preisgünstige Modelle nur über einen 100Base-T-Anschluss. Damit zieht sich der Datentransfer bei größeren Volumen unnötig in die Länge.

Größere Geräte verfügen über mehrere Festplatten, die zu einem Raid-Verbund zusammengefasst sind. Sie finden hier auch mehrere LAN-Schnittstellen vor. Für die Leistungsaufnahme und Wärmeabgabe nehmen Sie Werte wie bei größeren PCs an. Rechnen Sie sich deshalb einmal aus, ob sich für Sie die Anschaffung so eines Geräts rentiert. Mit handelsüblichen Rechnerteilen bauen Sie sich selbst einen kostengünstigen Netzwerkspeicher auf. Als Betriebssystem verwenden Sie FreeBSD. Sie können dadurch das Dateisystem ZFS verwenden. Es bietet eine komfortable Datenträgerverwaltung an. Reicht der Plattenspeicher nicht mehr aus, bauen Sie eine weitere Platte in das Gerät ein und teilen in einer Zeile dem Speicherpool mit, dass das Plattengerät »dazugehört«. Sie müssen weder vorher eine Partition noch ein Dateisystem anlegen (»formatieren«). Mehrere Datenplatten fassen Sie mit RAID-Z2 (so wird das beim ZFS bezeichnet) zu einem Array zusammen.

FreeBSD bietet Ihnen zudem die Möglichkeit, mehrere Domains für Samba, NFS oder SSHFS innerhalb verschiedener Jails anlegen. Ein Jail ist ein stark abgeschotteter Teilbaum des Hauptdateisystems und stellt eine Erweiterung des `chroot`-Mechanismus dar. Jedes Jail verfügt über eine eigene IP-Adresse und wird in fast allen Punkten so konfiguriert, als wäre es ein eigenständiger Rechner.

10.4.7 Modems für den Netzzugang

Ein Modem stellt für Sie die Verbindung von Ihrem Rechner zu einem entfernten Rechnersystem über die normale Fernmeldeinfrastruktur her. Die Geräte erhalten Sie als Baugruppe oder als externe Einheit. In manchen Notebooks finden Sie Modems fest eingebaut vor.

Sie können Modems hinsichtlich der Fernmeldetechnik unterscheiden:

- **Analoge Modems** (Abbildung 10.39): Ältester Telefonstandard, Transferrate maximal 57 kbit/s. Sie benutzen meist die serielle Schnittstelle (maximal 115 kbit/s, Anschluss über SUB-D-9- oder SUB-D-25-Stecker, auch USB-Modelle im Handel).
- **ISDN-Modems** (Abbildung 10.40): ISDN-Standard, 64 kbit/s (1 Kanal) oder 128 kbit/s (Kanalbündelung), Anschluss über SUB-D-9- oder SUB-D-25-Stecker, auch USB-Modelle im Handel). In den USA und einigen anderen Ländern stehen nur 56 kbit/s je Kanal zur Verfügung.
- **DSL-Modems**: Digitaler Teilnehmeranschluss, Datenraten von 384 kbit/s bis 200 Mbit/s (VDSL2). DSL finden Sie in zwei Modi vor:
  - ADSL: Hier ist der Downstream schneller als der Upstream.
  - SDSL: Down- und Upstream sind gleich schnell. Anschluss über LAN-Kabel, RJ45.
- **Kabel-Modems**: Übertragung über das Netz der Kabelfernsehanbieter, Datenraten bis 32 Mbit/s derzeit möglich, 100 Mbit/s in Einführung. Anschluss über LAN-Kabel (RJ45).
- **Funkmodems für das GSM-Netz** (GPRS): zwischen 9,6 kbit/s und 55 kbit/s möglich, USB-Anschluss

Abbildung 10.39 Analog-Modem älterer Bauart

Abbildung 10.40 ISDN-Modem

- **Funkmodems für UMTS, HSDPA (Abbildung 10.41), LTE und LTE Advanced**: Die maximal erzielbaren Datenraten liegen bei 384 kbit/s, 14,1 Mbit/s (üblich sind 7,2 Mbit/s) und 3–50 Mbit/s bzw. bis zu einem GBit/s.

Die Funkmodems mit USB-Anschluss können Sie an geeigneten Routern anstecken. Sie versorgen damit ein lokales Netzwerk mit Internetzugang.

Abbildung 10.41 USB-Funkmodem für HSDPA

Ein Analog- oder ISDN-Modem eignet sich kaum mehr zur Internetanbindung. Bei den heute üblichen Webseiten müssten Sie mit diesen Geräten lange Wartezeiten für Übertragung und Aufbau in Kauf nehmen. Allenfalls für die Herstellung von Wartungsverbindungen können Sie diese Art der Verbindung nutzen. Für die Anbindung von Computerkassen und Warenwirtschaftsterminals eignet sich diese Anbindung ebenso.

Auf einen Blick

Inhalt

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

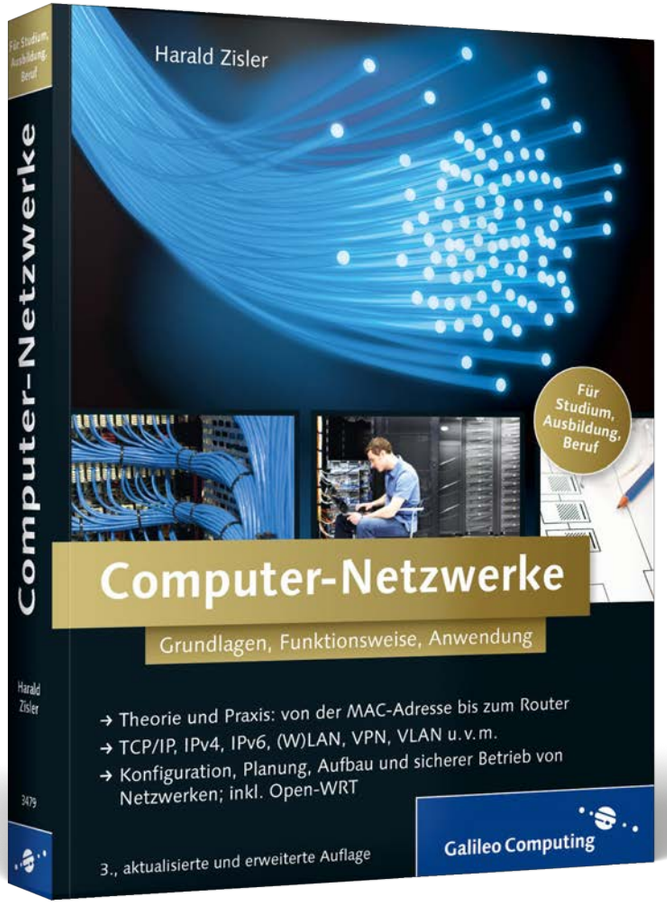
V

W

X

Y

Z



Harald Zisler beschäftigt sich seit 1996 in Theorie und Praxis mit Computer-Netzwerken. Er ist Autor technischer Fachbücher und verfasst Artikel in Fachzeitschriften in den Themenkreisen EDV und Kommunikationstechnik. Zudem befasst er sich intensiv mit FreeBSD, Linux, Datenbanken, Datenschutz und Datensicherheit.

Harald Zisler

Computer-Netzwerke – Grundlagen, Funktionsweise, Anwendung

434 Seiten, broschiert, 3. Auflage 2014
24,90 Euro, ISBN 978-3-8362-3479-5

www.galileo-press.de/3758