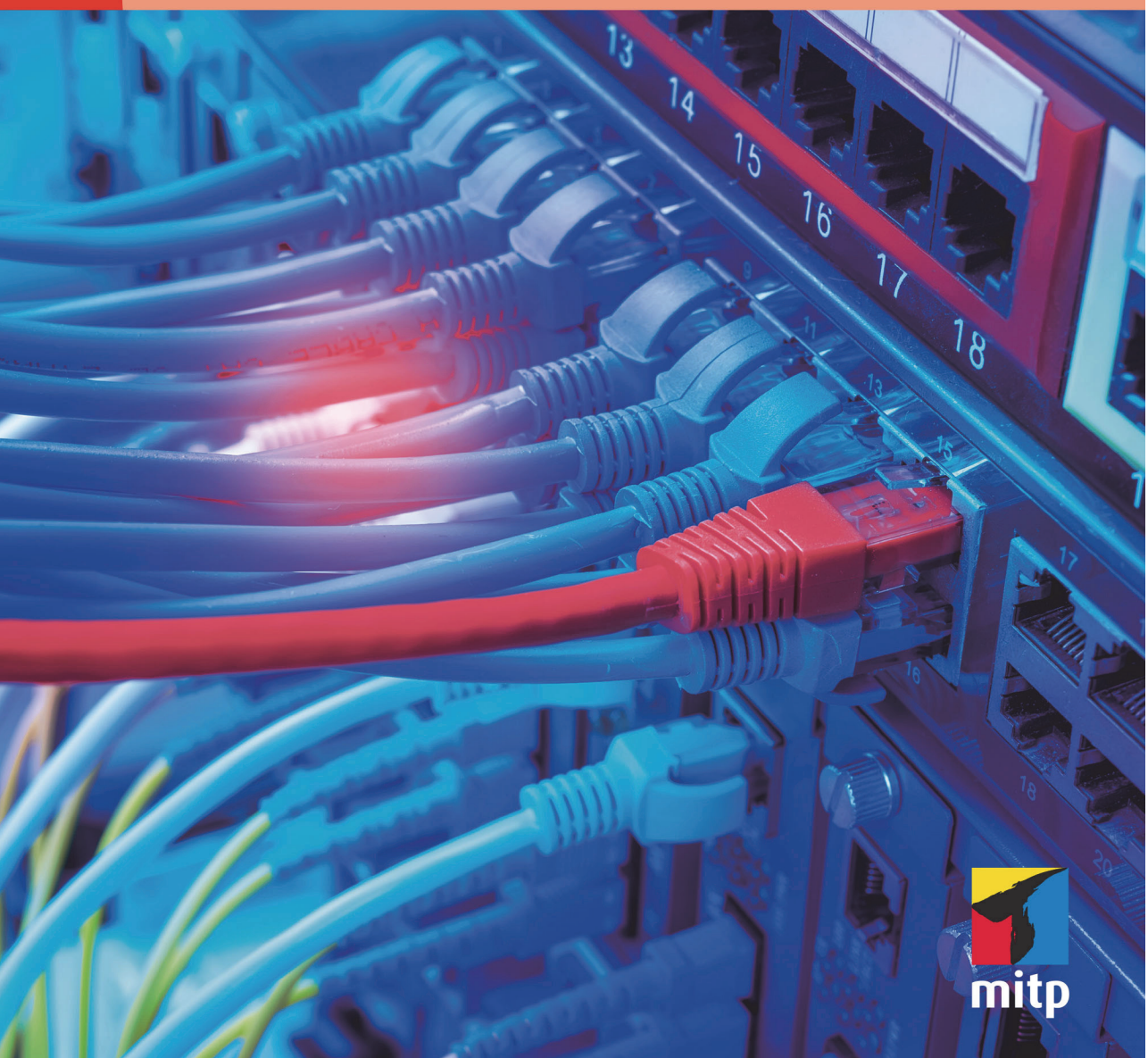
Eric Amberg | Daniel Schmid

Netzwerke

Verstehen, Einrichten, Administrieren

Mit umfassendem Praxisteil und
vielen Schritt-für-Schritt-Anleitungen



mitp

Eric Amberg, Daniel Schmid

Netzwerke

Verstehen, Einrichten, Administrieren

Mit umfassendem Praxisteil und vielen Schritt-für-Schritt-Anleitungen

mitp

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN 978-3-7475-1010-0
1. Auflage 2025

www.mitp.de
E-Mail: mitp-verlag@lila-logistik.com
Telefon: +49 7953 / 7189 - 079
Telefax: +49 7953 / 7189 - 082

Lektorat: Sabine Schulz, Nicole Winkel
Sprachkorrektorat: Jürgen Benvenuti, Nicole Winkel
Covergestaltung: Christian Kalkert
Bildnachweis:© xiaoliangge / stock.adobe.com
Satz: III-satz, Kiel, www.drei-satz.de

Inhaltsverzeichnis

Einleitung

Netzwerke sind das Fundament unserer digitalen Welt – sie verbinden Menschen, Maschinen und Systeme rund um den Globus. Egal ob E-Mail, Cloud-Dienste, Videostreaming oder IoT-Anwendungen: Ohne funktionierende Netzwerk-Infrastruktur läuft heute nichts mehr. Dieses Buch führt Sie fundiert und praxisnah in die faszinierende Welt der Computernetzwerke ein.

Sie lernen, wie Netzwerke aufgebaut sind, wie sie kommunizieren und welche Protokolle und Technologien dabei zum Einsatz kommen. Angefangen bei den Grundlagen der Datenübertragung und Netzwerkschichten über IP-Adressierung, Routing und Switching bis hin zu modernen Themen wie WLAN, VPN, Netzwerkvirtualisierung und Netzwerksicherheit – alle Inhalte sind systematisch aufbereitet, praxisorientiert und mit vielen Beispielen und Abbildungen verständlich erklärt.

Dieses Buch richtet sich an alle, die ein solides Verständnis für moderne IT-Netzwerke aufbauen möchten – sei es für die Ausbildung, Studium, berufliche Weiterbildung oder als Vorbereitung auf Zertifizierungen wie CompTIA Network+ oder Cisco CCNA. Der Fokus liegt dabei nicht nur auf theoretischem Wissen, sondern auch auf der praktischen Umsetzung: Zahlreiche Übungen und Konfigurationsbeispiele helfen Ihnen dabei, das Gelernte direkt anzuwenden.

Tauchen Sie ein in die Welt der Netzwerke – klar strukturiert und praxisorientiert.

Für wen ist dieses Buch geeignet?

Dieses Buch ist für Sie geeignet, wenn Sie sich praxisnah und umfassend mit dem Thema »Computernetzwerke« beschäftigen möchten – ganz gleich, ob Sie Einsteiger sind oder bereits über erste Vorkenntnisse verfügen. Die Zielgruppe umfasst insbesondere:

- Studierende und Auszubildende in IT-nahen Fachrichtungen
- Netzwerk- und Systemadministratoren
- IT-Fachkräfte, die ihr Netzwerkverständnis vertiefen möchten
- Quereinsteiger mit technischem Interesse
- Vorbereitungskandidaten für Zertifizierungen wie CompTIA Network+ oder Cisco CCNA

Das Buch eignet sich sowohl zum systematischen Einstieg als auch zur gezielten Vertiefung einzelner Themenbereiche. Die Inhalte sind so aufgebaut, dass sie ein solides praxisorientiertes Fundament für den Aufbau, Betrieb und die Analyse von Netzwerken schaffen.

Auch wenn das Lesen allein bereits einen guten Überblick vermittelt, profitieren Sie am meisten von diesem Buch, wenn Sie aktiv mitarbeiten – etwa durch das Nachvollziehen von Beispielkonfigurationen oder das eigenständige Umsetzen kleiner Netzwerkaufbauten. Viele Kapitel bauen inhaltlich aufeinander auf, gleichzeitig kann das Buch aber auch als Nachschlagewerk dienen: Verweise innerhalb des Buchs helfen Ihnen, schnell die für ein Thema relevanten Grundlagen zu finden.

Inhaltsübersicht

Das Buch ist in fünf Teile gegliedert. Nachfolgend stellen wir Ihnen die Inhalte kurz vor, damit Sie sich ein Bild vom Aufbau und der Struktur machen können.

Teil I – Grundlagen

In diesem ersten Teil lernen Sie die technischen Grundlagen moderner Computernetzwerke kennen. Kapitel 1 » Grundlagen moderner Computernetzwerke« gibt Ihnen einen Überblick über die Funktionsweise und Prinzipien von IT-Netzwerken. In Kapitel 2 widmen wir uns den kabelgebundenen Übertragungstechnologien, also der physischen Basis jeder Netzwerkkommunikation. Kapitel 3 bis 7 beschäftigen sich mit dem Internet Protocol (IPv4 und IPv6), der IP-Adressierung, Subnetting, ARP, ICMP und den grundlegenden Routing-Mechanismen. Hier lernen Sie, wie Datenpakete ihren Weg durch Netzwerke finden. Kapitel 8 behandelt die zentralen Transportprotokolle TCP und UDP. In Kapitel 9 lernen Sie wichtige Infrastrukturdienste wie DHCP und DNS kennen. Den Abschluss dieses Teils bildet Kapitel 10 »Wichtige Netzwerkanwendungen«, in dem wir zentrale Netzwerkanwendungen wie SSH, Mailserver, Webserver und weitere Netzwerkdienste betrachten.

Teil II – Praxis: Aufbau eines Netzwerks

In diesem Teil setzen Sie das erlernte Wissen praktisch um. Kapitel 11 zeigt, wie Sie eine virtuelle Laborumgebung mit VirtualBox aufbauen – eine ideale Testumgebung für Experimente und Übungen. Kapitel 12 erklärt die IP-Grundkonfiguration unter Windows und Linux. Im weiteren Verlauf erfahren Sie in Kapitel 13, wie Switches und Router eingerichtet werden. Kapitel 14 und 15 widmen sich der Konfiguration typischer Serverdienste wie DHCP, DNS, Webserver, Mailserver und andere. Kapitel 16 geht einen Schritt weiter und zeigt die Einrichtung einer Active-Directory-Domäne. In Kapitel 17 »Einrichtung eines Heimnetzwerks mit einem SoHo-Router« lernen Sie, wie Sie ein einfaches Heimnetzwerk mit einem SoHo-Router aufbauen können. Kapitel 18 befasst sich mit typischen Problemen und deren systematischer Behebung – dem Troubleshooting.

Teil III – WLAN & Co – Drahtlose Netzwerke

Teil III widmet sich der drahtlosen Kommunikation. In Kapitel 19 erhalten Sie eine Einführung in WLAN und die Funktionsweise drahtloser Netzwerke. Kapitel 20 führt Sie Schritt für Schritt durch die praktische Einrichtung eines WLANs, einschließlich typischer Konfigurationsoptionen und Sicherheitsaspekten. Kapitel 21 erweitert den Blick auf weitere drahtlose Technologien, die heute ebenfalls im Netzwerkbereich relevant sind – etwa Mobilfunk, Satellitenkommunikation, Bluetooth und andere.

Teil IV – Netzwerksicherheit

Dieser Teil führt Sie in die Grundlagen der Netzwerksicherheit ein. Kapitel 22 behandelt die zentralen Bedrohungen für Netzwerke und zeigt, wie Sie Risiken durch gezielte Schutzmaßnahmen minimieren können. In Kapitel 23 richten wir Firewalls ein und betrachten deren Rolle in modernen Sicherheitskonzepten. Kapitel 24 behandelt VPN-Technologien – sowohl IPsec-basierte als auch SSL/TLS-gestützte VPNs – und erklärt, wie sichere Tunnel für die Datenübertragung aufgebaut werden. Kapitel 25 zeigt, welche sicheren Protokolle und Dienste (z. B. HTTPS, SFTP) in der Praxis eingesetzt werden und wie Sie diese implementieren.

Teil V – Netzwerkkonzeption und Cloud Computing

Im letzten Teil dieses Buchs geht es um die Planung und den Aufbau von Netzwerk-Infrastrukturen. Kapitel 25 vermittelt Grundlagen der Netzwerkplanung: Sie lernen, wie man Anforderungen analysiert, Netze strukturiert plant und Aspekte wie Skalierung, Redundanz und Segmentierung berücksichtigt. Kapitel 26 führt Sie in die Welt des Cloud Computings ein und vermittelt grundlegende Konzepte wie IaaS, PaaS und SaaS. Im abschließenden Kapitel 27 setzen Sie das Gelernte praktisch um und lernen anhand konkreter Beispiele, wie Sie eine Netzwerk-Infrastruktur in der Cloud – speziell bei AWS – entwerfen und konfigurieren.

Aktualität der Inhalte

Die Welt der IT entwickelt sich ständig weiter. Neue Tools kommen hinzu, bestehende Anwendungen erhalten Updates, grafische Oberflächen verändern sich und Konfigurationsschritte können sich von einer Softwareversion zur nächsten unterscheiden. Dieses Buch wurde mit größter Sorgfalt erstellt, alle Anleitungen wurden in funktionierenden Testumgebungen nachvollzogen und mit aktuellen Software-Versionen getestet. Dennoch möchten wir Sie darauf hinweisen, dass sich manche Darstellungen – etwa Benutzeroberflächen, Befehle oder Menüstrukturen – im Laufe der Zeit ändern können. Es ist daher möglich, dass bestimmte Abbildungen nicht mehr exakt mit dem aktuellen Stand der Software übereinstimmen oder einzelne Arbeitsschritte in einer neueren Version leicht anders funktionieren.

Lassen Sie sich davon nicht entmutigen. Die technischen Prinzipien, Protokolle und Konzepte, die diesem Buch zugrunde liegen – von IP-Adressierung über Routing bis hin zur Netzwerksicherheit –, sind weitaus langlebiger als einzelne Tools oder Konfigurationsmasken. Dieses Grundlagenwissen bleibt in der Regel über viele Jahre hinweg gültig und übertragbar – auch wenn sich eine Administrationsoberfläche, das Verhalten eines Kommandos oder die Position eines Menüpunktes verändert.

Sollten Sie beim Nachvollziehen von Anleitungen auf Unterschiede stoßen, nehmen Sie dies als Gelegenheit, eigenständig weiterzudenken, nachzulesen oder Alternativen auszuprobieren. Genau diese Fähigkeit – sich selbstständig durch neue oder veränderte Netzwerkumgebungen zu bewegen – ist eine der wichtigsten Kompetenzen, die Sie als Netzwerkprofi oder Administrator entwickeln können.

Über die Autoren

Eric Amberg ist selbstständiger Experte für IT-Netzwerke und -Sicherheit und hat in den letzten 25 Jahren zahlreiche Projekte aller Größenordnungen durchgeführt. Seine große Leidenschaft ist die Wissensvermittlung, die er in Büchern, Magazinen, Seminaren und Videotrainings stets praxisnah und lebendig präsentiert.

Daniel Schmid ist bei einem großen Energiekonzern im Bereich Netzwerke und Security tätig. Als Projektleiter für diverse große, teils internationale Projekte hat er in 20 Jahren viel Erfahrung in der Planung und Implementation sicherheitskritischer Infrastruktur gesammelt.

Eric und Daniel haben bereits viele gemeinsame Projekte erfolgreich umgesetzt und sind die Gründer der Hacking-Akademie (hacking-akademie.de).

Danksagung

Ein Buch wie dieses entsteht nicht im luftleeren Raum – es ist das Ergebnis intensiver Arbeit, Diskussionen, Recherchen, Rückmeldungen und Durchhaltevermögen. Ohne die Unterstützung zahlreicher Menschen hätte dieses Buchprojekt nicht zu dem werden können, was Sie nun in den Händen halten. Dafür möchten wir – Eric und Daniel – von Herzen Danke sagen.

Ein herzliches Dankeschön geht an Sabine Schulz und Nicole Winkel vom mitp-Verlag, die dieses Projekt mit großem Vertrauen begleitet haben. Vielen Dank für eure Unterstützung und den guten Austausch während der gesamten Entstehungsphase.

Der größte Dank gilt natürlich unseren geliebten Ehefrauen Kati und Rocío. Ihr habt uns über die gesamte Dauer hinweg den Rücken freigehalten, mit viel Geduld und Verständnis die zahlreichen Abende und Wochenenden toleriert, an denen wir tief in Netzwerkthemen versunken waren. Ohne eure Unterstützung wäre dieses Buch schlicht nicht möglich gewesen.

Und Daniel möchte an dieser Stelle noch eine ganz besondere Person würdigen: Dieses Buch ist auch dir gewidmet, Noelia. Wenn Papa oft im Büro saß, hast du ihn immer »arbeiten lassen« – mit erstaunlich viel Geduld und Verständnis für dein Alter. Danke, dass du nach getaner Arbeit immer mit deinem Lachen für den nötigen Ausgleich gesorgt hast.

Vielen Dank euch allen!

Berlin und Stuttgart, August 2025

Eric und Daniel

Teil I

Grundlagen

In diesem Teil:

In diesem ersten Teil legen wir das Fundament für ein solides Verständnis moderner Computernetzwerke. Ohne dieses Basiswissen lassen sich komplexere Themen und praktische Szenarien nur schwer nachvollziehen. Deshalb behandeln wir in diesem Abschnitt die zentralen Konzepte und Protokolle, die in modernen Netzwerken – vom Heimnetzwerk bis hin zu globalen Unternehmens-Infrastrukturen – eine Rolle spielen.

Wir führen Sie zunächst an die Hardware-Grundlagen heran und zeigen Ihnen, wie Bits und Bytes übertragen werden. Danach wenden wir uns dem Herzstück der Netzwerkkommunikation zu: dem Internet Protocol – sowohl in der heute noch dominanten Version 4 als auch in der zukunftsweisenden Version 6. Die zugehörigen Mechanismen wie Subnetting, Adressvergabe und Routing stehen ebenfalls im Fokus. Ergänzt wird das Ganze durch die zentralen Transportprotokolle TCP und UDP sowie durch grundlegende Netzwerkdienste wie DHCP, DNS und einige wichtige Netzwerkanwendungen, denen Sie vermutlich immer wieder begegnen werden.

Nachdem Sie diesen ersten Teil des Buches durchgearbeitet haben, kennen Sie die wichtigsten Komponenten eines Netzwerks, verstehen die grundlegenden Konzepte hinter den Protokollen der TCP/IP-Familie und haben einen guten Einblick in die elementaren Technologien, auf denen moderne Netzwerke basieren. In den weiteren Teilen greifen wir vieles davon wieder auf, erweitern Ihr Wissen um weitere Aspekte und vertiefen Ihr Verständnis in der Praxis.

Kapitel 1

Grundlagen moderner Computernetzwerke

Betrachten wir die rasante Entwicklung der EDV, so ist die Entstehung und Verbreitung von Computernetzwerken noch gar nicht so lange her – andererseits sehen wir auf rund 70 Jahre zurück, seit die ersten nennenswerten Computer das Licht der Welt erblickten. Zwar wurde das Internet in seinen Grundzügen bereits in den 1960er-Jahren entwickelt, jedoch wurden Computernetzwerke in Unternehmen erst in den 1980er-Jahren eingeführt. Nun, das ist inzwischen auch schon wieder rund 40 Jahre her – und angesichts der unglaublich schnellen Entwicklung in der Computertechnik kann man hier schon von Steinzeit sprechen.

In diesem ersten Kapitel sprechen wir über die Grundlagen heutiger IT-Netzwerke. Dabei fassen wir uns kurz, um den Umfang dieses Buchs nicht zu sprengen. Nach Abschluss dieses Kapitels haben Sie eine solide Übersicht und ein Grundwissen über folgende Themen:

- Die Historie von Computernetzwerken
- Normen und Standards
- Die wichtigsten Begriffe und Komponenten eines Netzwerks
- Räumliche Abgrenzung von Netzwerken (LAN, WAN etc.)
- Netzwerktopologien
- Die TCP/IP-Protokollfamilie
- Die Netzwerk-Referenzmodelle (OSI und TCP/IP)
- Zahlensysteme (Binär und Hexadezimal)

Damit legen wir die Grundlagen für die weiteren Kapitel dieses Buchs. Wir gehen nicht davon aus, dass Sie Vorwissen im Bereich der Netzwerktechnik mitbringen, von daher beginnen wir von Anfang an.

1.1 Die Entstehung der Computernetzwerke

Ende der 1960er-Jahre beauftragte das amerikanische Verteidigungsministerium (genauer die Abteilung *Advanced Research Project Agency* oder kurz: ARPA) verschiedene Universitäten und Computerhersteller damit, ein Datennetz zu konzipieren, das redundante (also mehrfach vorhandene) Datenwege ermöglichte, um beim Ausfall eines Knotens keinen *Single Point of Failure* zu haben, der das gesamte Netzwerk lahmlegen würde.

> Ein *Single Point of Failure* ist eine einzelne notwendige Komponente in einem System, deren Ausfall den Ausfall des gesamten Systems zur Folge hat.

1969 wurde ein Testlauf mit einem halben Dutzend von vernetzten Systemen gestartet und unter dem Projektnamen ARPANET in Betrieb genommen. Es hatte zum Ziel, verschiedene Universitä-

ten und das Verteidigungsministerium dezentral miteinander zu verbinden, um Forschungsergebnisse untereinander auszutauschen. Die Verbindungen wurden über Telefonleitungen aufgebaut. Im Laufe der Jahre erweiterte sich das ARPANET und wurde mit neuen Technologien versehen. Eine Übersicht über das ARPANET 1977 zeigt Abbildung 1.1.

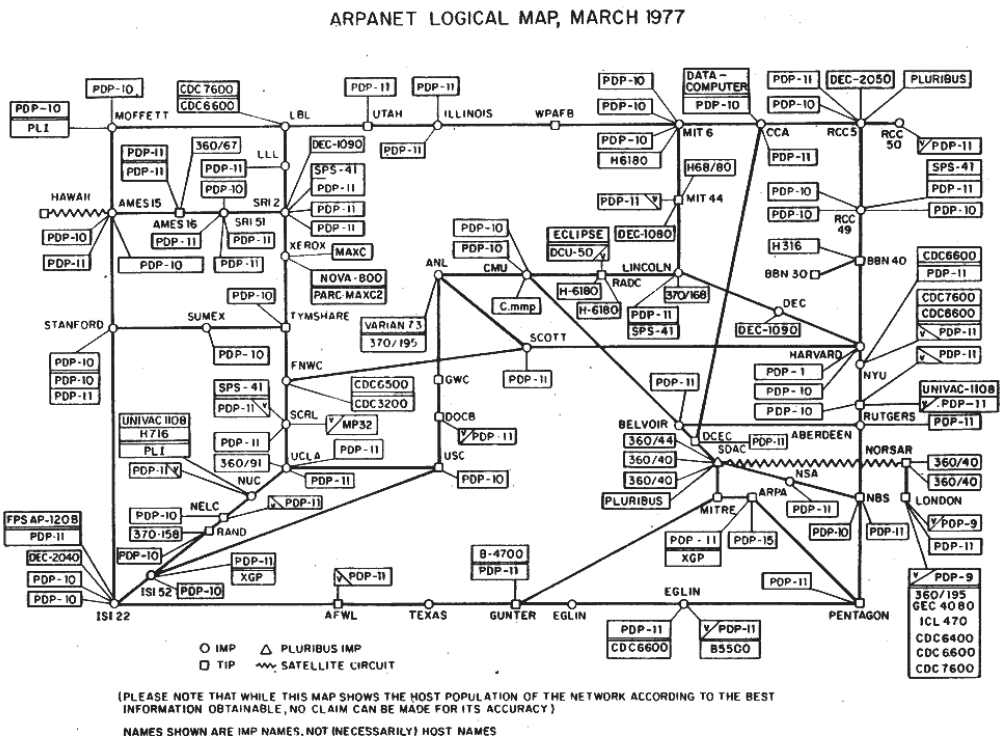


Abb. 1.1: Das ARPANET 1977 (Quelle: Wikipedia)

Die Verbindung über das Telefonnetz wurde durch sogenannte *Packet-Switching*-Technologien verdrängt, die die Datenübermittlung über Pakete ermöglichte, statt einen kontinuierlichen Datenstrom zu erzeugen. Damit konnten Verbindungen von mehreren Systemen gleichzeitig verwendet werden, da es keine dediziert geschalteten Leitungen zwischen den Kommunikationspartnern gab, sondern ein Netzwerk, das von allen Teilnehmern nach Bedarf genutzt werden konnte. Immer mehr Institutionen wurden an dieses neue Netzwerk angeschlossen. Schließlich wurde das Netzwerk auch von Unternehmen genutzt.

Beim Aufbau von dedizierten Verbindungen, wie es beim Telefon der Fall ist, spricht man dagegen von *Circuit Switching*. Hierbei werden immer zwei Systeme direkt zusammengeschaltet.

1.1.1 UNIX und C

Die weitere Entwicklung wurde durch zwei zentrale Komponenten ermöglicht: zum einen durch das Betriebssystem *UNIX* und zum anderen durch die Programmiersprache *C*, die von 1971 bis 1973 von *Dennis Ritchie* entwickelt wurde – übrigens, um genau dieses UNIX zu programmieren!

Kennen Sie den Spruch: »UNIX ist das Betriebssystem der Zukunft – schon seit 40 Jahren!«? Diese ironische Aussage entstammt einer interessanten Tatsache: Durch die Entwicklung von UNIX auf Basis der Programmiersprache C wurde eine einheitliche Betriebssystem-Plattform auf vielen verschiedenen Maschinenplattformen verfügbar und erleichterte so die Entwicklung von Netzwerkprotokollen und -anwendungen, da man nun endlich einen Quasistandard hatte. Dadurch wurde eine plattformübergreifende Kommunikation ermöglicht – das *Internet* war geboren!

UNIX schien eine goldene Zukunft bevorzustehen. Wie sich jedoch später herausstellte, sollte UNIX zwar die Zeit überdauern, jedoch diverse andere Betriebssysteme bezüglich der Bedeutung an sich vorbeiziehen lassen müssen.

1.1.2 TCP/IP

TCP/IP ist das »Protokoll« des Internets. Ein Protokoll ist ein Satz von Regeln und Prozessen, auf die sich die kommunizierenden Partner einigen. Da es verschiedene Ebenen und unterschiedliche Anwendungen innerhalb der Netzwerkkommunikation gibt, existiert eine große Anzahl von zusammenhängenden Protokollen, die als *Protokollfamilie* bezeichnet wird. *TCP/IP* ist daher eigentlich kein Protokoll, sondern eine ganze Protokollfamilie, wobei die beiden wichtigsten Protokolle, nämlich TCP (Transmission Control Protocol) und IP (Internet Protocol), lediglich die Namensgeber sind. Dennoch spricht man umgangssprachlich von *dem* TCP/IP-Protokoll.

Anfangs gab es im Internet (bzw. ARPANET) eine Reihe von konkurrierenden Protokollen – insbesondere die *ISO* (International Organization for Standardization) entwickelte einen umfassenden Protokollstapel namens *OSI* (Open Systems Interconnect).

Kommt Ihnen das bekannt vor? Schon mal vom *OSI-Modell* gehört? Vielleicht! Aber wussten Sie auch, dass OSI ursprünglich auch als eigenes Protokoll konzipiert wurde? In einigen sehr eingeschränkten Bereichen (z.B. beim Routing-Protokoll *IS-IS*) findet es auch heute noch tatsächlich Anwendung, jedoch konnte sich OSI gegenüber TCP/IP als Protokoll nicht durchsetzen – es war einfach zu überladen. Man entschied sich dafür, das einfachere und leichter zu implementierende Protokoll TCP/IP für das Internet zu nutzen.

Im März 1982 entschied das US-Verteidigungsministerium, dass TCP/IP *der* Standard für das ARPANET (und damit das zukünftige Internet) sein soll. Am 1. Januar 1983 erfolgte die komplette Umschaltung auf TCP/IP. Dieser Tag wurde *Flag Day* genannt.

TCP/IP wurde übrigens schon Anfang der 1970er-Jahre konzipiert – hätten Sie gedacht, dass dieses Protokoll schon so alt ist? *IPv4*, das bis heute gängige Standard-Netzwerkprotokoll, wurde 1978 vorgestellt und 1981 in **RFC 791** standardisiert. Ursprünglich wurde es im Rahmen von TCP entwickelt, doch 1978 wurde TCP in TCP und IP aufgeteilt, wodurch IP als eigenständiges Protokoll entstand. Verbunden sind die beiden jedoch bis heute. TCP ist in **RFC 793**, ebenfalls aus dem Jahr 1981, definiert.

Die *RFCs* (Request for Comment) sind die Dokumente, in denen die Komponenten des Internets inhaltlich und formal definiert werden. Mehr zu den RFCs Abschnitt 1.2.1.

TCP/IP besteht aus diversen Protokollen, die auf unterschiedlichen Netzwerkebenen arbeiten und aufeinander aufbauen. Zu diesem Thema kann man ganze Bücher füllen, und auch Sie werden im Rahmen dieses Buchs immer wieder mit einzelnen Protokollen des TCP/IP-*Stacks* (die englische

Fachbezeichnung für »Protokollfamilie«) konfrontiert werden. Wir kommen in Abschnitt 1.5 noch einmal darauf zurück. Wie auch immer: Das Internet hatte nun eine einheitliche Sprache – was die Verbreitung des größten Netzwerks dieses Planeten natürlich weiter förderte.

1.1.3 Ethernet

Ebenfalls Anfang der 1970er-Jahre begannen verschiedenen Unternehmen, wie z.B. IBM und Xerox, an lokalen Netzwerksystemen zu arbeiten, die die Computer innerhalb eines Standorts miteinander vernetzen sollten. Daraus entstand 1973 das ursprüngliche *Ethernet*. Es übertrug mit einer Geschwindigkeit von bis zu 3 Mbit/s.

Die Funktionsweise des ursprünglichen Ethernets könnte man als »koordiniertes Chaos« beschreiben. In Kapitel 2 » Kabelgebundene Übertragungstechnologien« erfahren Sie mehr Details.

Ethernet wurde ab 1980 vom *IEEE* (Institute of Electrical and Electronics Engineers) in der Arbeitsgruppe 802 weiterentwickelt und als *IEEE 802.3* standardisiert. Doch war Ethernet nicht der einzige Ansatz, den das IEEE verfolgte: Neben *Token Bus* (IEEE 802.4) wurde auch *Token Ring* (IEEE 802.5) als lokale Netzwerktechnologie entwickelt. Allerdings konnte sich langfristig nur *Ethernet* durchsetzen. Token Bus und Token Ring sind heutzutage de facto ausgestorben bzw. fristen nur noch ein Nischendasein in industriellen Produktionsnetzwerken und anderen, speziellen Netzwerken.

Im Zusammenhang mit der Einführung von Personal Computern wurde nun die Vernetzung von Arbeitsplatz-Computern möglich. Dies läutete eine neue Ära in der Unternehmenskommunikation ein – das *LAN* (Local Area Network) hielt Einzug in die Unternehmen.

1.1.4 Computernetzwerke heute

Es gab eine Zeit, da haben führende Computerexperten behauptet, dass niemals der Zeitpunkt kommen würde, an dem einzelne Mitarbeiter, geschweige denn Privatpersonen, einen eigenen Computer benötigen oder besitzen werden. Sie haben sich gründlich geirrt. Mittlerweile ist es ganz normal, dass jedes Familienmitglied (vielleicht mit Ausnahme des Hundes) über seinen eigenen PC, Laptop oder sein Tablet verfügt.

Ebenso selbstverständlich ist die Vernetzung der Computer untereinander geworden. Konnten sich früher nur Unternehmen den Aufbau eines lokalen Netzwerks mit Internetanbindung leisten, ist dies zwischenzeitlich für jeden »Otto-Normal-Haushalt« zur Selbstverständlichkeit geworden. Schließlich wollen mittlerweile nicht nur PC und Laptop ins Internet, sondern auch Smartphones, Tablets und der Fernseher sowie der Blu-ray-Player, smarte Assistenten wie Alexa etc. – und alle Daten müssen untereinander synchronisiert werden.

In fast allen Unternehmen existieren heutzutage Computernetzwerke. Fällt die EDV aus, liegt nicht selten der komplette Betrieb lahm. Viele Unternehmen, besonders größere, sind komplett abhängig von ihrer EDV und verlieren viel Geld, wenn vitale Systeme ausfallen.

Die meisten Menschen beschäftigen sich allerdings nur so weit mit der Materie, wie es notwendig ist, um mit dem Computer möglichst effektiv arbeiten zu können. Mit anderen Worten: Anwender von Computernetzwerken möchten einfach nur, »dass es funktioniert«. Alles andere ist nicht von Bedeutung.

Jedoch existieren hochkomplexe Prozesse hinter simplen Aktionen wie z.B. dem Aufrufen einer Website. Verschiedenste Komponenten sind beteiligt und arbeiten perfekt über eindeutig definierte Schnittstellen zusammen. Der Anwender vor dem PC macht sich keine Gedanken darüber, dass die

Daten zunächst über sein lokales Netzwerk in das Netzwerk seines Internetproviders gesendet werden. Auf der Seite des Anwenders steht vielleicht ein DSL-Router oder ein Kabelmodem, der (bzw. das) die Daten irgendwohin weiterleitet. Punkt! Dahinter steckt für den Anwender einfach eine Blackbox – irgendetwas, das funktioniert, dessen Funktionsweise er aber nicht verstehen muss (vgl. Abbildung 1.2).

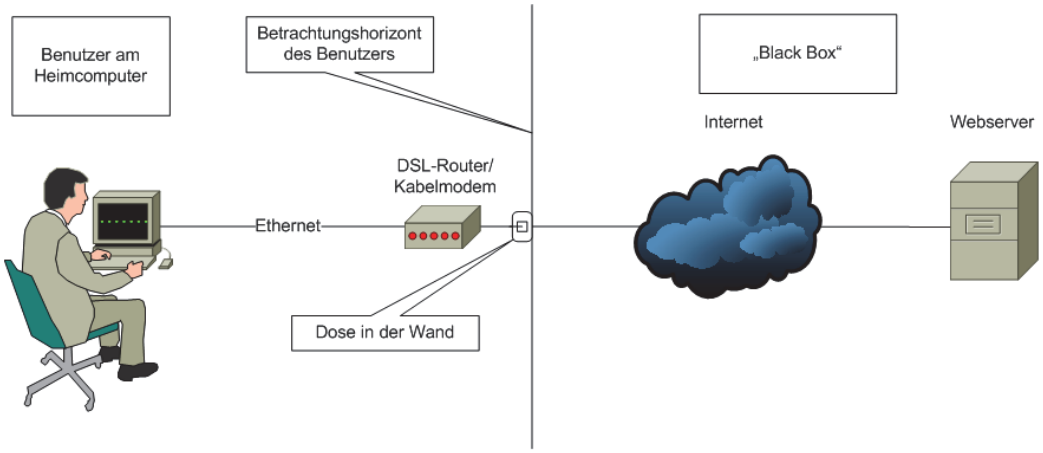


Abb. 1.2: Die Sicht des Benutzers auf das Netzwerk

Der Provider seinerseits nimmt das Datenpaket vom DSL-Router/Kabelmodem über die Punkt-zu-Punkt-Verbindung entgegen und leitet es durch sein eigenes Netzwerk hindurch entweder zum Ziel-Netzwerk oder zu einem angebundenen Provider. Dort endet sein Zuständigkeitsbereich, über den weiteren Verlauf macht er sich keine Gedanken.

Eine kurze Begriffsklärung: Ein *Provider* ist ein Anbieter von Telekommunikationsdiensten. Dies betrifft in unserem Fall in der Regel die Internetanbindung, kann aber auch Hostingdienste und Ähnliches umfassen.

Der Administrator des Unternehmens, das den aufgerufenen Webserver bereitstellt, ist dafür verantwortlich, dass das Datenpaket mit der Anfrage des Browsers zum Zielserver geleitet wird. Dieser steht aller Wahrscheinlichkeit nach auch wieder in einem lokalen Netz, das von diesem Unternehmen betrieben wird.

Merken Sie was? Jeder hat seine eigene Perspektive, seinen eigenen Blickwinkel. Wir unterscheiden im Businesskontext vier Hauptbereiche:

- **Heimnetzwerke:** Es gibt viele Menschen, die per Homeoffice von zu Hause arbeiten und darauf angewiesen sind, dass das Computernetzwerk und die Internetanbindung funktionieren. Hierbei liegt das Hauptaugenmerk auf der Anbindung der (vergleichsweise wenigen) lokalen Computer an das Internet bzw. genauer gesagt an den Provider.
- **Mobiler Benutzer:** Viele Mitarbeiter eines Unternehmens benötigen von überall Zugriff auf Ressourcen des Unternehmens. Vertriebsmitarbeiter z.B. benötigen aktuelle Präsentationen oder Daten, die auf den Servern des Unternehmens gespeichert sind, wie z.B. E-Mail. Hierzu wird ein Fernzugriff (Remote Access) bereitgestellt, in der Regel über VPN-Technologien (VPN = Virtual

Private Network). Dies sind gesicherte Verbindungen zum Unternehmens-Netzwerk. Im Grunde ist der Zugriff durch den mobilen Benutzer ein Sonderfall des Homeoffices, da in beiden Fällen dieselben Technologien zum Einsatz kommen.

- **Provider-Netzwerke:** Sie stellen die Internetwolke dar. Provider sind die Verbindungsglieder zwischen den lokalen Netzwerken. Hier geht es primär um die Bereitstellung von Schnittstellen für die lokalen Netzwerke und das Routing im Internet. Weiterhin kommt es aufgrund der hohen Datenlast auf effektive und leistungsstarke Systeme an. Die Optimierung der Datenübertragung ist hier ein wichtiges Thema.
- **Unternehmens-Netzwerke:** Fast jedes Unternehmen benötigt ein funktionierendes Computernetzwerk, um effektiv arbeiten zu können. E-Mail, Datenbanken, Datei- und Druckdienste, Webservices und viele andere Netzwerkanwendungen sind unverzichtbarer Bestandteil der Unternehmensprozesse. Fällt das Netzwerk aus, sind viele Unternehmen komplett handlungsunfähig. Hier gilt es, eine sichere, stabile und robuste Netzwerkinfrastruktur aufzubauen und zu administrieren.

Ein Unternehmens-Netzwerk kann und wird in vielen Fällen aus mehreren Standorten bestehen. Oftmals gibt es eine *Zentrale* (engl. headquarter) und eine oder mehrere *Filialen* (engl. branch offices). Während in den einzelnen Standorten LANs implementiert werden, werden die Standorte untereinander mittels WAN-Technologien miteinander verbunden. Entweder wird hierzu das Internet verwendet oder das Unternehmen nutzt einen dedizierten Anschluss, der vom Provider bereitgestellt wird. Zu den Begriffen LAN und WAN siehe Abschnitt 1.3.1.

1.2 Normen und Standards

In den Anfangszeiten der Computer und Computernetzwerke entwickelte jedes Unternehmen seine eigenen Lösungen. Diese Lösungen waren nur auf die eigenen Systeme ausgelegt und somit *proprietär*. Das bedeutet, dass es keine Interoperabilität zwischen den Systemen verschiedener Hersteller gab. Das war ein großes Problem, da somit die Skalierbarkeit und Flexibilität fehlte.

Durch die Normierung und Standardisierung von Technologien und Prozessen wird es möglich, dass Systeme verschiedener Hersteller miteinander vernetzt werden und kommunizieren können. Dies ist eine Grundvoraussetzung für die globale Vernetzung und das Internet. Es werden Anforderungen definiert, die jeder Hersteller erfüllen muss, wenn er eine bestimmte Komponente entwickelt und anbieten möchte. In diesem Abschnitt werfen wir daher einen Blick auf Institutionen, die im Rahmen der Netzwerkkommunikation Normen und Standards definieren oder bestimmte Aspekte zentral verwalten.

1.2.1 Internet-Standardisierungsorganisationen

Für die Weiterentwicklung und Standardisierung der Internet-Technologien existiert eine Reihe von wichtigen Institutionen, die wir Ihnen nachfolgend kurz vorstellen.

Internet Society

Die Dachorganisation des Internets heißt *Internet Society* (ISOC) und wurde 1992 gegründet. Sie ist eine Nichtregierungsorganisation und hat die Aufgabe, die Internetstruktur zu pflegen und weiterzuentwickeln. Sie besteht aus 150 Organisationen in über 170 Ländern und hat ihren Hauptsitz in den USA. Unter der ISOC sind verschiedene andere Organisationen und Gremien vereint, die jeweils spezifische Aufgaben wahrnehmen. Eine Übersicht über die wichtigsten Gremien finden Sie in Abbildung 1.3.

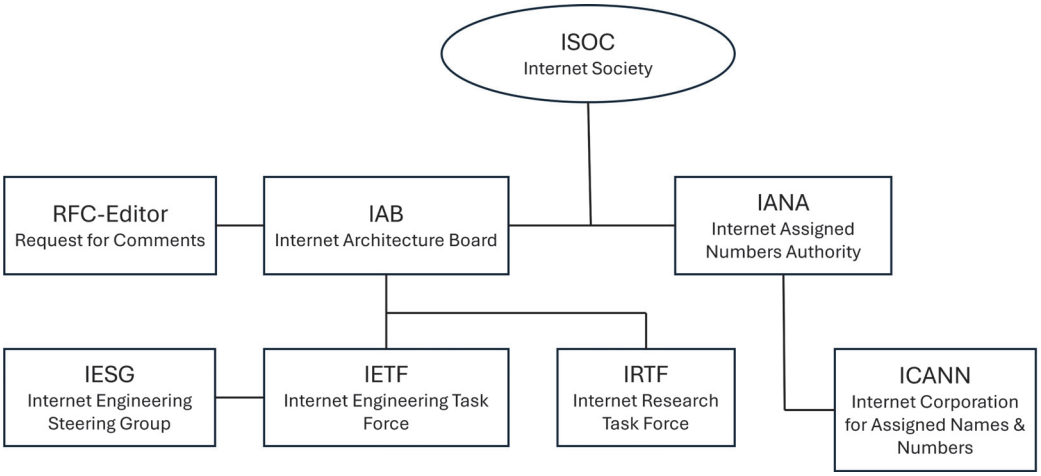


Abb. 1.3: Die ISOC und ihre untergeordneten Institutionen

Diese Institutionen haben die folgenden Aufgaben:

- **IAB (Internet Architecture Board)**: Dieses Komitee unterstützt die ISOC beratend und wahrt den Überblick über die Architektur und die Standardisierungsaktivitäten der IETF.
- **RFC-Editor**: Diese Institution ist der Herausgeber der RFCs (Request for Comments). Früher hatte diese Funktion eine einzige Person inne, nämlich *Jonathan Postel*. Er verstarb jedoch 1998. Die RFCs sind die wichtigsten Standardisierungsdokumente für Technologien und Prozesse, die im Internet und auch in lokalen Netzwerken verwendet werden. In diesem Buch verweisen wir immer wieder auf die entsprechenden RFCs. Diese haben verschiedene Zustände, z.B. *Draft* (Entwurf), *Proposed Standard* (vorgeschlagener Standard) oder *Internet Standard*. Letzterer ist verpflichtend und muss von allen Herstellern eingehalten werden. Viele *Proposed Standards* sind allerdings auch bereits de facto Standards geworden, die in der Praxis fast immer so umgesetzt werden. RFCs können einen anderen Status erhalten, werden aber im Nachhinein nicht verändert. Für Updates werden neue RFCs erstellt.
- **IANA (Internet Assigned Numbers Authority)**: Sie ist eine der ältesten Institutionen des Internets und wurde ursprünglich ebenfalls durch *Jonathan Postel* repräsentiert. Die IANA verwaltet zentrale technische Ressourcen des Internets, darunter die IP-Adressblöcke, Protokollnummern und die Root-Zone des *Domain Name Systems* (DNS). Die IPv4- und IPv6-Adressblöcke werden an sogenannte *Regional Internet Registries* (RIR) vergeben. Für jeden Kontinent gibt es eine: *ARIN* (Nordamerika), *RIPE* (Europa), *APNIC* (Asien und Pazifik), *LACNIC* (Lateinamerika und Karibik) und *AfriNIC* (Afrika). Die RIRs vergeben ihrerseits Teile dieser Adressblöcke an regionale Internetprovider.
- **ICANN (Internet Corporation for Assigned Names and Numbers)**: Diese Institution wurde 1998 gegründet, um die globale Verwaltung des Internets zu koordinieren. Ihr wurde die IANA organisatorisch unterstellt. Dies wird jedoch vertraglich regelmäßig neu ausgehandelt. Die ICANN ist für die Vergabe von Top-Level-Domains (TLDs) und andere organisatorische Aufgaben wie die Akkreditierung von Domain-Registraren zuständig.
- **IETF (Internet Engineering Task Force)**: Sie stellt eine Arbeitsgruppe des IAB dar und ist eine der wichtigsten Organisationen, da sie sich mit der technischen Weiterentwicklung des Internets befasst. Das Ziel sind neue Internetstandards und Best Practices, um die Funktionalität, Stabilität und Sicherheit des Internets zu verbessern. Die IETF ist offen für freiwillige Mitarbeit von

Herstellern, Netzbetreibern, Forschern oder Netzwerktechnikern aus der ganzen Welt. Es existiert keine förmliche Mitgliedschaft oder Mitgliedsvoraussetzung.

- **IESG (Internet Engineering Steering Group)**: Sie ist für die Leitung der IETF zuständig und an den Standardisierungsverfahren und der Genehmigung von Standards beteiligt.
- **IRTF (Internet Research Task Force)**: Ist ebenfalls eine Arbeitsgruppe des IAB und besteht aus Forschern im Bereich Netzwerktechnik mit dem Schwerpunkt Internet. Ihre Ziele sind die Erforschung und Entwicklung neuer Technologien. Die IRTF ist inhaltlich und personell eng mit der IETF vernetzt.

1.2.2 IEEE-Standardisierung für lokale Netze

Es gibt viele Technologien und Prozesse, die auch in lokalen Netzwerken zum Einsatz kommen. Somit spielt die Arbeit der oben genannten Institutionen auch in Unternehmens-Netzwerken eine große Rolle. Jedoch gibt es auch insbesondere eine Institution, die diverse Standards für Technologien in lokalen bzw. nicht globalen Netzwerken festgelegt hat. Dabei handelt es sich um das *Institute of Electrical and Electronics Engineers*, kurz: IEEE.

Hierbei handelt es sich um einen weltweiten Berufsverband von Ingenieuren der Bereiche Elektrotechnik und Elektronik sowie Informatik. Seine mehr als 400.000 Mitglieder in über 150 Ländern der Erde machen das IEEE zum größten technischen Berufsverband der Welt.

> Das IEEE standardisiert Kommunikationstechnologien, Hardware und Software und ist im Gegensatz zur ISOC nicht auf das Internet spezialisiert.

Die Arbeitsgruppe 802 beschäftigt sich mit Netzwerk- und Übertragungsstandards. Die jeweiligen Standards beginnen alle mit 802 und erhalten durch Punkt getrennt eine laufende Nummer, optional gefolgt von einem oder mehreren Buchstaben, um Weiterentwicklungen und Versionsstände zu kennzeichnen. Einige dieser Standards kennen Sie vielleicht oder haben zumindest schon einmal davon gehört:

- *IEEE 802.3* – der ursprüngliche Ethernet-Standard
- *IEEE 802.3u* – Fast Ethernet (100 Mbps)
- *IEEE 802.5* – Token Ring
- *IEEE 802.11* – der ursprüngliche Wireless-LAN-Standard
- *IEEE 802.11b/g* – Übertragungsstandard mit 11 bzw. 54 Mbps
- *IEEE 802.11ax* – einer der neueren WLAN-Standards mit bis zu 9600 Mbps
- *IEEE 802.1X* – Standard zur Authentifizierung in Rechnernetzen

Vermutlich werden Sie im Laufe Ihrer Netzwerk-Karriere immer wieder über Spezifikationen der IEEE-802-Reihe stolpern. Eine Übersicht enthält der Wikipedia-Artikel unter `de.wikipedia.org/wiki/IEEE_802`.

1.3 Komponenten eines Computernetzwerks

Woraus besteht nun also solch ein Computernetzwerk? Was sind typische Komponenten und Begriffe, denen Sie aller Wahrscheinlichkeit nach immer wieder begegnen werden? Welche Ebenen, Strukturen und Abgrenzungen werden unterschieden? Das schauen wir uns in diesem Abschnitt näher an.

1.3.1 Räumliche Abgrenzung von Netzwerken

Bevor wir uns die physischen Komponenten ansehen, müssen wir zunächst eine grundsätzliche Unterscheidung bezüglich der Art des Netzwerks machen. Die Frage ist: Wo befindet sich unser Netzwerk, was umfasst es und welche Funktion hat es?

LAN

Die grundlegenden Netzwerke werden als *LAN* (Local Area Network) bezeichnet. LANs umfassen klassischerweise die Vernetzung innerhalb von Gebäuden. Befinden sich zwei miteinander vernetzte Gebäude in räumlicher Nähe, also z.B. auf demselben Gelände, so spricht man auch noch von einem *LAN*, wobei hier oft der Terminus *Campus-Netzwerk* verwendet wird. LANs werden hauptsächlich über Ethernet und WLAN-Technologien implementiert.

Wichtig

LANs sind *nicht* dadurch gekennzeichnet, wie viele Geräte in dem jeweiligen Netzwerk angeschlossen sind. Es kann sich um zwei Geräte in einem Home-Office-Netzwerk handeln oder um Tausende Geräte in einem Campus-Netzwerk.

PAN

Ein *PAN* (Personal Area Network) ist für die Vernetzung von Kleingeräten innerhalb eines Raums gedacht und ist eine Sonderform der lokalen Netzwerke. Zur Datenübertragung wird oft eine Drahtlos-Technologie wie WLAN, Bluetooth oder IrDA verwendet.

WAN

Wenn Standorte untereinander verbunden werden sollen, stellt sich die Wahl, ob wir eine direkte Verbindung zwischen den Standorten wünschen oder ob wir das Internet nutzen möchten. Grundsätzlich bezeichnen wir aber alle Netzwerkverbindungen, die über den Einzugsbereich eines *LAN*s hinausreichen, als *WAN* (Wide Area Network). Ein typisches Beispiel ist die Anbindung einer Filiale an den Hauptsitz über eine Standleitung.

MAN

Eine Sonderform des WANs ist das *MAN* (Metropolitan Area Network). Es wird für die Verbindung zwischen Standorten innerhalb eines Stadtgebiets verwendet. Hierfür wird in der Regel ein sogenannter *Backbone* aufgebaut, also eine Übertragungsinfrastruktur, an die sich einzelne Standorte (LANs) anschließen können. MANs können eine Ausdehnung von bis zu 100 Kilometern haben.

GAN

Als *GAN* (Global Area Network) bezeichnen wir weltumspannende Netzwerke. Das größte GAN ist das Internet. Große Unternehmen und bestimmte Provider betreiben ihre eigenen GANs. Die Verwendung des Internets ist jedoch für die weltumspannende Vernetzung mittlerweile der Häufigkeitsfall, da die Anbindung günstig und – ggf. unter Berücksichtigung entsprechender Redundanz – auch ausreichend zuverlässig ist.

Das Internet

Typisch für LANs und WANs ist, dass sie klare und eindeutige Grenzen haben. LANs gehören einem Unternehmen, WANs werden über Provider realisiert, die dedizierte Standleitungen oder Technologien bereitstellen, für deren einzelne Anschlüsse die Unternehmen Geld zahlen müssen. GANs und MANs sind Sonderformen, die keine grundsätzlich neuen Regeln einbringen.

Das Internet jedoch ist der Zusammenschluss aller Provider und (theoretisch) all deren Kunden. Im Grunde könnten Sie jedes System auf der ganzen Welt erreichen, das an das Internet angebunden ist.

Diese Schnittstellen zwischen einzelnen Providern werden übrigens über die Internet-Knotenpunkte (*IX* für *Internet Exchange* genannt) bereitgestellt. Diese auch als *Peering Points* bezeichneten Knotenpunkte dienen den Providern als Übergangspunkte zwischen zwei Provider-Netzen. Es existieren ca. 340 Internet-Knoten weltweit. Der größte Knotenpunkt in Deutschland ist der *DE-CIX* in Frankfurt am Main, wobei *CIX* für *Commercial Internet Exchange* steht.

Im Internet ist es egal, ob Sie einen Server ansprechen möchten, der im Nebenhaus steht oder auf der anderen Seite der Welt. Aus finanzieller Sicht ist die Distanz zwischen den Kommunikationspartnern – im Gegensatz zu Standleitungen – im Internet ohne Bedeutung! Es fallen grundsätzlich nur die Kosten an, die durch die Anbindung des jeweiligen Standorts an das Internet entstehen.

1.3.2 Physische Komponenten

Bisher ging es nur um abstrakte Begriffe und es wurde allerlei Terminologie in den Raum geworfen. Nun werden wir konkret: Wie ist denn nun ein solches Computernetzwerk physisch aufgebaut? Betrachten Sie Abbildung 1.4.

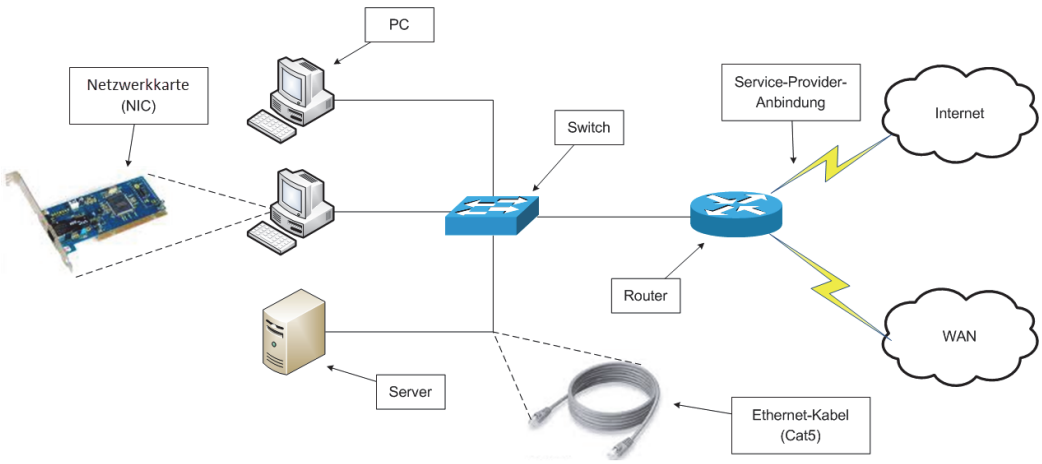


Abb. 1.4: Physische Netzwerkkomponenten

Natürlich ist dies nur ein sehr einfaches Modell – aber es reicht völlig aus, um einige grundlegende Komponenten eines Computernetzwerks vorzustellen:

- **Computer der Endanwender**: Sie stellen die Schnittstelle der Benutzer zum Netzwerk dar und bestehen in der Regel aus PCs, Laptops oder Ähnlichem. Auf ihnen werden verschiedene Arten

von Anwendungen ausgeführt: *Betriebssysteme* sind die Schnittstellen zwischen dem Benutzer, den Anwendungsprogrammen und der Hardware. *Lokale Programme* laufen nur lokal auf dem Computer und interagieren nicht mit anderen Systemen oder Programmen im Netzwerk. *Netzwerkprogramme* sind auf Endgeräten der Anwender in der Regel Client-Anwendungen, die vornehmlich keine eigenen Daten bereitstellen, sondern auf den Datenbestand von anderen Systemen (Servern) zugreifen.

- **Server**: Sie bieten bestimmte Netzwerkdienste an. Die PCs greifen auf den oder die Server zu, um z.B. Informationen aus einer Datenbank zu erhalten, eine Datei zu öffnen oder zu speichern, ein Dokument auszudrucken, eine Website anzeigen zu lassen etc. Daher nennt man diese Art der Kommunikation auch *Client-Serveranwendungen*. Sprechen Endgeräte auf gleicher Ebene untereinander, sprechen wir von *Peer-to-Peer-Kommunikation*.
- **Netzwerkkarte**: Um mit dem Netzwerk zu kommunizieren, benötigen die PCs und Server Netzwerkkarten, auch *NICs* (Network Interface Cards) genannt. Sie stellen die Schnittstelle für die Anbindung ans Netzwerk bereit. Nach außen hin enthält eine NIC lediglich eine Ethernet-Buchse und eine oder mehrere Leuchtdioden, die den Status anzeigen. Oftmals sind die Netzwerkschnittstellen heutzutage direkt auf dem Mainboard implementiert und nicht mehr eigenständige Karten, die in das Mainboard in entsprechende Slots eingesteckt werden.
- **Ethernet-Kabel**: In den meisten Fällen wird der Computer über ein Ethernet-Kabel an einen Switch angeschlossen. In der Praxis geschieht dies oft über sogenannte *Patch-Panel*. Das sind Verbindungselemente für die Gebäudeverkabelung, da diese Kabel häufig unter dem Boden verlegt werden, und am Arbeitsplatz lediglich eine Ethernet-Buchse bereitstellen. Am Patch-Panel enden diese Kabel und münden in eine weitere Ethernet-Buchse, an der ein Kabel angeschlossen wird, das z.B. zu einem Switch führt. Mehr über die verschiedenen Kabelvarianten lernen Sie in Kapitel 2.
- **Switch**: Der Switch ist ein sogenannter *Sternverteiler*. Im Switch treffen sich die Systeme und werden physisch miteinander verbunden. Früher wurden hierfür *Hubs* verwendet, aber diese Geräte sind heutzutage kaum noch anzutreffen – im Unternehmensumfeld sind sie praktisch ausgestorben. Switches werden fast ausschließlich für Ethernet-Verkabelung und damit nur im LAN verwendet. Im Gegensatz zu Hubs verfügen sie über eine gewisse Intelligenz.
- **Router**: Switches sind in der Regel an Router angebunden. Router sind die Bindeglieder zwischen einzelnen Netzwerken. Entweder verbinden Router verschiedene LAN-Subnetze (z.B. verschiedene Etagen oder Nachbargebäude) miteinander oder sie realisieren die Anbindung von lokalen Netzwerken an andere Standorte (per WAN) bzw. an das Internet. Router können zudem noch zahlreiche andere Funktionen bereitstellen, insbesondere NAT (Network Address Translation), VPN-Tunnel (Virtual Private Network) und Firewall-Funktionalität.

Hinweis

Auf WLAN und seine Komponenten gehen wir gesondert in Kapitel 19 ff. ein. Daher lassen wir das Thema zunächst außen vor und beschränken unsere Betrachtung auf die kabelgebundenen Technologien, die nach wie vor die Basis moderner Netzwerke sind.

1.3.3 Netzwerkanwendungen

Die verschiedenen Netzwerkkomponenten dienen der Verbindung von Computern in einem Netzwerk und deren Kommunikation untereinander. Dies wird softwareseitig durch die Netzwerkanwendungen realisiert. Es gibt hauptsächlich zwei Arten von Netzwerkkommunikation: *Client-Server* und *Peer-to-Peer*. Bei einer Client-Server-Architektur greift eine Client-Anwendung (z.B. ein Brow-

ser) auf eine Serveranwendung (z.B. einen Webserver) zu. Das ist die wichtigste Architektur in der Netzwerkkommunikation. Peer-to-Peer-Netzwerke werden eher in besonderen Situationen genutzt, z.B. im *Darknet*, wenn Daten auf verschiedene Systeme verteilt sind. In diesem Fall sind die Computer gleichzeitig Clients und Server.

Schauen wir auf einige gängige Client-Serveranwendungen:

- **World Wide Web (WWW)**: Server stellen Webseiten mit Informationen und Downloads bereit, auf die mit Web-Clients, meistens Browsern, mittels HTTP(S) zugegriffen werden kann. WWW ist die wohl wichtigste Anwendung im Internet.
- **File Transfer Protocol (FTP)**: Bietet die Möglichkeit, Dateien herunterzuladen oder hochzuladen. Wird heutzutage oft durch HTTP(S) ersetzt.
- **Datei- und Druckdienste**: Sowohl UNIX/Linux als auch Windows stellen Netzwerkzugriffsmöglichkeiten auf Datenspeicher bereit, die auf einzelnen Systemen liegen. Der Dateiserver speichert die Dateien und der Client greift via SMB (Microsoft Windows) oder NFS (Linux) darauf zu. Auch Drucker können in dieser Form im Netzwerk bereitgestellt werden.
- **Zentrale Objekt- und Zugriffsverwaltung**: Über Netzwerkdienste wie *Active Directory* können Domänen erstellt werden, die von Domänencontrollern gesteuert werden. In der Domänenstruktur können verschiedene Ressourcen und der Zugriff darauf zentral verwaltet werden.
- **Datenbankanwendungen**: Die strukturierte Datenspeicherung in Datenbanken ist eine der Grundlagen für die Bereitstellung von Daten im Rahmen vieler Anwendungen. Auf die Daten kann gezielt zugegriffen werden. Die Datenspeicherung geschieht auf verschiedene Arten. Es gibt auf SQL basierende Datenbanken, sogenannte NoSQL-Datenbanken und Verzeichnisse, wie z.B. LDAP. Der Datenbankserver stellt eine Schnittstelle bereit, über die durch eine Client-Anwendung auf die Daten zugegriffen werden kann. Meistens sind diese Clients direkt in die Anwendungen integriert. Dem Anwender wird eine Oberfläche angeboten, über die er die Daten abrufen, erstellen oder ändern kann.
- **E-Mail**: Als eine der ältesten Anwendungen des Internets überhaupt ist E-Mail auch heute noch sehr wichtig und überall präsent. Mailclients sind die Schnittstelle des Benutzers. Dieser kann damit Mails versenden und empfangen. Die Mails werden über den eigenen Mailserver an den Mailserver des Empfängers gesendet. Dort kann der Empfänger seine Mail einsehen bzw. durch seinen eigenen Mailclient in sein lokales Postfach herunterladen.
- **Instant Messaging**: Live Chats erfreuen sich großer Beliebtheit und werden sowohl im privaten als auch im beruflichen Umfeld genutzt. Sie sind ein guter Mittelweg zwischen einer E-Mail und einem Telefonat.
- **Voice-und Video-over-IP**: Eine der neueren Entwicklungen im Netzwerkbereich ist die Überführung bereits vorhandener Technologien in Datennetze, wie Telefonie und Video. Das bringt viele Vorteile mit sich: Wegfall eines separaten Fernsprechnetzwerks, Integration in die vorhandene Infrastruktur, Redundanz, zusätzliche Features und Kostenersparnis.

Natürlich gibt es noch viele weitere Netzwerkanwendungen. Dies soll zunächst eine erste Übersicht sein, um sich zu orientieren. Im Laufe des Buchs werden wir noch auf viele Aspekte der oben genannten Anwendungen detaillierter eingehen.

1.4 Netzwerktopologien

Netzwerktopologien sind ein Thema, das seit der Urzeit der Computernetzwerke eine Rolle spielt: In welcher Form werden die Systeme miteinander vernetzt? Wie Sie gleich sehen werden, müssen wir dabei in physische und logische Topologien unterscheiden.

Hinweis

Kurz zur Begriffsbestimmung: Aktive Systeme im Netzwerk werden auch als *Knoten* bezeichnet. Dabei kann es sich um ein Endgerät oder eine aktive Netzwerkkomponente wie z.B. einen Router handeln. Endgeräte werden darüber hinaus als *Host* bezeichnet. Diesen Begriffen werden Sie in diesem Buch häufig begegnen.

1.4.1 Bus

Die ersten Ethernet-Netzwerke wurden als Bus-Topologie implementiert. Jeder Computer war »in Reihe« mit dem jeweiligen Nachbarn physisch verbunden. Dies wurde über Koaxialkabel mit *BNC-Stecker* (British Naval Connector) mittels T-Stück realisiert (vgl. Abbildung 1.5).

Abb. 1.5: Koaxialkabel mit BNC-Stecker und T-Stück

Die Bus-Topologie stellt sich schematisch wie in Abbildung 1.6 dar.

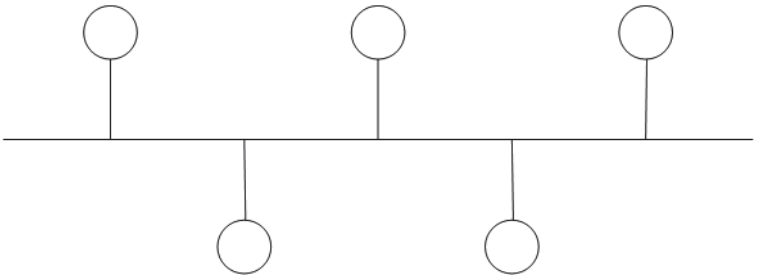


Abb. 1.6: Busverkabelung: Die Kreise stellen die Netzwerkknoten dar.

Der große Nachteil von physischen Bus-Topologien ist, dass alle Knoten an einem Kabelstrang hängen, der einen *Single Point of Failure* darstellt. Ist eine Stelle im Netzwerk defekt, wirkt sich das unter Umständen auf das gesamte Netzwerk aus. Mittlerweile werden Ethernet-Netzwerke nicht mehr in dieser Form implementiert.

1.4.2 Stern

Bei einer Stern-Topologie werden die Knoten an einem zentralen Verteiler angeschlossen, der zwischen den Knoten vermittelt. In lokalen Netzwerken ist das heute regelmäßig ein Switch, früher ein Hub. Die Stern-Topologie stellt sich schematisch dar, wie in Abbildung 1.7 gezeigt.

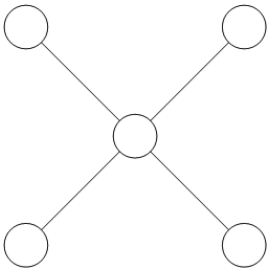


Abb. 1.7: Stern-Topologie

Im Falle eines Hubs oder Switches liegt physisch eine Stern-Topologie vor, logisch ist die Kommunikationsverbindung jedoch als Bus implementiert. Näheres dazu im nächsten Kapitel.

Stern-Topologien haben den Vorteil, dass sie relativ einfach zu implementieren sind und dass die Fehlersuche ebenfalls vereinfacht wird. Andererseits haben wir hier erneut einen *Single Point of Failure*. Fällt der zentrale Punkt – im LAN der Switch – aus, bedeutet das den Ausfall der gesamten Netzwerkkommunikation aller Knoten, die an diesem zentralen Punkt angeschlossen sind. Im Umkehrschluss führt der Ausfall eines Endpunkts oder einer Filiale nicht wie beim Bus zum Ausfall des gesamten Netzwerks.

1.4.3 Ring

Ring-Topologien spielten früher auch im LAN eine Rolle. Namentlich in Token-Ring-Netzwerken nach IEEE 802.5. Hier wurde ein physischer Ring aufgebaut, an dem alle Knoten angeschlossen waren. Der schematische Aufbau stellt sich dar, wie in Abbildung 1.8 gezeigt.

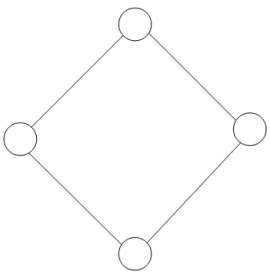


Abb. 1.8: Schematische Darstellung einer Ring-Topologie

Mittlerweile ist Token Ring jedoch nur noch in wenigen Produktionsnetzwerken anzutreffen. Heute werden Ring-Topologien jedoch noch immer in Backbone-Netzwerken z.B. in MANs eingesetzt. Auch in LAN-Umgebungen kommen sie noch vor in Form ringförmig verbundener Switches, um Redundanz zu gewährleisten.

1.4.4 Punkt-zu-Punkt

Obwohl eigentlich keine echte Topologie, sind Punkt-zu-Punkt-Verbindungen jedoch häufig bei WAN-Anbindungen anzutreffen. Punkt-zu-Punkt-Verbindungen bestehen schlicht aus zwei Endpunkten, zwischen denen sich meistens nichts außer der Leitung befindet (vgl. Abbildung 1.9).

Abb. 1.9: Schematische Darstellung einer Punkt-zu-Punkt-Verbindung

Oftmals sind Router in dieser Form miteinander verbunden, jedoch kann die Punkt-zu-Punkt-Topologie auch als Bestandteil anderer Topologien auftreten. Auf höheren Ebenen der Netzwerkkommunikation sind auch virtuelle Punkt-zu-Punkt-Verbindungen möglich.

1.4.5 Gemischte Topologien

Topologien können auch miteinander kombiniert werden (vgl. Abbildung 1.10).

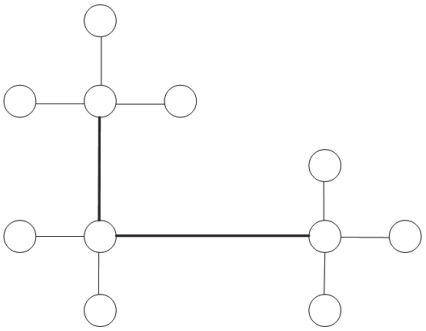


Abb. 1.10: Stern-Bus-Topologie

Im Beispiel in der Abbildung sind die Knoten über eine Stern-Topologie miteinander angebunden, aber die Sternverteiler sind als Bus verbunden. Werden Systeme, z.B. Router, über diverse Wege miteinander verbunden, sprechen wir auch von *teilvermascht* (engl. partial meshed) oder *vollvermascht* (engl. full meshed), je nachdem, ob nur ein Teil der Knoten redundant angebunden ist oder ob alle Knoten mit allen verbunden sind (vgl. Abbildung 1.11).

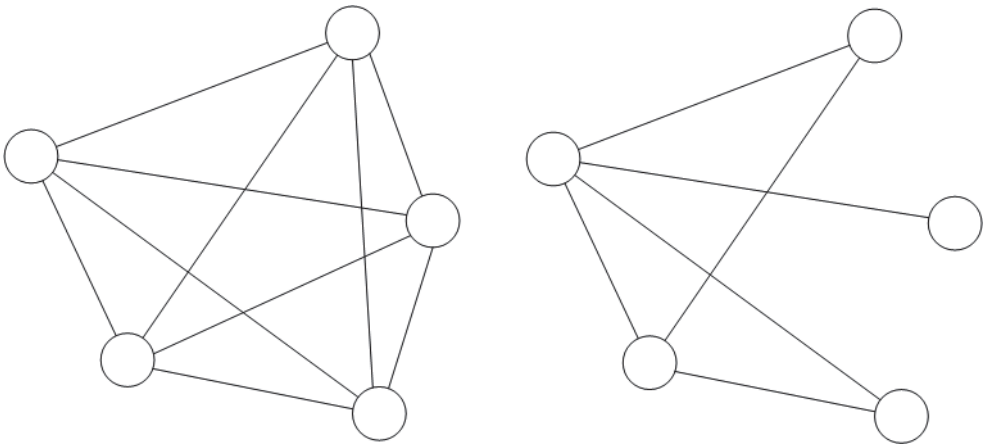


Abb. 1.11: Links ein vollvermaschtes (full meshed) und rechts teilvermaschtes (partial meshed) Netzwerk

Denken Sie daran, dass sich Topologien auf die physische und logische Ebene sowie Standortverbindungen beziehen können. Sie müssen also die Netzwerktopologie im jeweiligen Kontext betrachten. Über VPN und andere Tunneltechnologien können Systeme wie Router logisch direkt miteinander verbunden sein, wobei der physische Weg über viele Router führt.

1.5 Überblick über die TCP/IP-Protokollsuite

Sie haben bereits in Abschnitt 1.1.2 einen ersten Kontakt mit der TCP/IP-Protokollfamilie gehabt. Weitere Bezeichnungen sind:

- TCP/IP-Protokollsuite
- TCP/IP-Protokoll-Stack (bzw. engl. TCP/IP Protocol stack)
- TCP/IP (als Synonym für die gesamte Protokollfamilie)

Wie bereits erwähnt, besteht TCP/IP aus diversen Einzelprotokollen, die aber auch miteinander in Verbindung stehen.

1.5.1 Netzwerkebene

Wir können grob zwischen der Netzwerkebene und der Anwendungsebene unterscheiden. Auf der Netzwerkebene arbeiten generische Protokolle, die für alle Anwendungen gleichermaßen nutzbar sind und allgemeine Aufgaben der Netzwerkkommunikation übernehmen. Zu den TCP/IP-Protokollen der Netzwerkebene gehören die folgenden. Sie sind in aufsteigender Reihenfolge gemäß der Netzwerk-Referenzmodelle geordnet:

- **ARP** – das *Address Resolution Protocol:* Es löst logische IP-Adressen in Hardware-Adressen (MAC-Adressen) auf.
- **IP** – das *Internet Protocol:* Es ist das zentrale Protokoll der Suite und regelt die logische Adressierung sowie die Wegfindung. Es existiert als IPv4 und IPv6.
- **ICMP** – das *Internet Control Message Protocol:* Ist ein wichtiges Protokoll zur Übertragung von Status- und Fehlerinformationen im Netzwerk.
- **TCP** – das *Transmission Control Protocol:* Dies ist das am häufigsten verwendete Transportprotokoll für Anwendungsdaten im Internet.
- **UDP** – das *User Datagram Protocol:* Eine Alternative für TCP mit weniger »Overhead«, also weniger Features, dafür einfacher und schneller.

1.5.2 Anwendungsebene

Die Anwendungsebene kann weiter unterteilt werden, jedoch finden wir hier im Allgemeinen spezifische Protokolle für bestimmte Anwendungen. Dazu gehören z.B. die folgenden:

- **HTTP** (Hypertext Transfer Protocol) – Anwendung: WWW
- **FTP** (File Transfer Protocol) – Anwendung: Dateiübertragung
- **Telnet/SSH** – Anwendung: Remotezugriff via Kommandozeile
- **SMTP** (Simple Mail Transfer Protocol) – Anwendung: E-Mail
- **DNS** (Domain Name System) – Anwendung: Namensauflösung
- **DHCP** (Dynamic Host Configuration Protocol) – Anwendung: IP-Konfigurationszuweisung
- **NTP** (Network Time Protocol) – Anwendung: Zeitsynchronisation
- **SIP** (Session Initiation Protocol) – Anwendung: VoIP-Management

Jedes Anwendungsprotokoll hat seine eigene Funktion und transportiert anwendungsspezifische Daten. Viele Anwendungen im Internet stellen ihre eigenen Protokolle bereit – daher existieren unzählige Anwendungsprotokolle, von denen wir nur eine Auswahl in diesem Rahmen betrachten können.

Im Laufe dieses Buchs werden Sie die verschiedenen Protokolle von TCP/IP besser kennenlernen. Auch werden Sie die Verbindungen zwischen den Protokollen erkennen und wissen, auf welchen Ebenen welche Protokolle zu welchem Zweck eingesetzt werden.

1.6 Die Netzwerk-Referenzmodelle

In der Frühzeit der Computernetzwerke entwickelten viele große Hersteller von Computersystemen ihre eigenen Netzwerkprotokolle und -modelle. Diese Technologien wurden nur auf den eigenen Systemen implementiert und deren Details wurden nicht veröffentlicht. Damit konnte ein IBM-System z.B. nur mit einem anderen IBM-System sprechen – eine herstellerübergreifende Kommunikation war nicht möglich.

Später allerdings wurden die Spezifikationen einiger Protokolle, wie z.B. *SNA* (Systems Network Architecture) von IBM, veröffentlicht (1974), sodass Hersteller dieses Protokoll bei sich implementieren konnten. Dies war jedoch nicht ganz uneigennützig, da die großen Anbieter dadurch an Marktmacht gewinnen und die Entwicklung nach ihren Vorstellungen beeinflussen wollten. Für SNA z.B. stand bereits lange vor den heutigen Standards ein entsprechendes umfassendes Referenzmodell zur Verfügung.

Für eine freie Entwicklung der Netzwerkkommunikation bieten sich jedoch offene Standards an. Hierzu entstanden insbesondere zwei Referenzmodelle, die die Netzwerkkommunikation in Schichten unterteilen und deren jeweilige Funktionen klar beschreiben: das *OSI-Referenzmodell* und das *TCP/IP-Referenzmodell*.

1.6.1 Das ISO-OSI-Referenzmodell

In Computernetzwerken werden Dienste unterschiedlichster Art bereitgestellt, und die Zusammenhänge sind teils äußerst komplex. Auch ohne Modell ist schnell ersichtlich, dass Funktionen und Fehler auf völlig unterschiedlichen Ebenen liegen können. So ist eine Übertragungsstörung aufgrund eines Kabelbruchs eine ganz andere Geschichte, als wenn eine Firewall die Kommunikation blockiert.

Ab 1979 entwickelte die *International Organization for Standardization* (ISO) ein Modell, das *Open Systems Interconnect* (OSI) genannt wurde und seit 1983 standardisiert ist. Dieses Modell sollte als Designgrundlage für die Kommunikationsprotokolle und -prozesse in Computernetzwerken dienen. Ursprünglich entwickelte die ISO auch ein auf diesem Modell beruhendes gleichnamiges Protokoll, das jedoch keine weite Verbreitung fand und den Wettbewerb gegen TCP/IP verlor.

Das OSI-Referenzmodell unterteilt die gesamte Netzwerkkommunikation in sieben aufeinander aufbauende Schichten (engl. layer). Jede dieser Schichten umschreibt bestimmte, klar umrissene Aufgaben. Weiterhin kann jede Schicht nur mit der jeweils angrenzenden Nachbarschicht, darunter oder darüber, kommunizieren – Schichten können nicht übersprungen werden. Dementsprechend sind klare Schnittstellen zwischen den einzelnen Schichten definiert. Die einzelnen Schichten sind in Abbildung 1.12 aufgeführt.

OSI-Schicht		Ebene	Beispiel-Protokolle und Verfahren	Einheiten	Hardware
7	Application	Application	HTTP, FTP, SMTP	Data	Gateways (Protokoll-Umwandler)
6	Presentation		ASCII, MP3, Encryption		
5	Session		NetBIOS		
4	Transport	Network	TCP, UDP	Segment	
3	Network		IP, ICMP, IGMP	Packet	Router, Layer-3-Switch
2	Data Link		Ethernet, Frame Relay, ARP	Frames	Switch, Bridge
1	Physical			Bits	Repeater, Hub

Abb. 1.12: Das ISO-OSI-Referenzmodell in der Übersicht

Die Begriffe haben wir hier bewusst in der englischen Version belassen, da diese in der Literatur weitaus häufiger vorkommen als deren deutsche Übersetzung. Nachfolgend finden Sie eine Erläuterung der einzelnen Schichten:

Schicht 7 – Application Layer (Anwendungsschicht)

Dies ist die oberste Schicht in der Netzwerkkommunikation. Sie stellt die Schnittstelle, also das Interface, für den Benutzer bzw. die Netzwerkanwendung dar. Die verschiedenen Netzwerkprogramme, wie z.B. Browser, E-Mail-Client etc., sind auf dieser Schicht angesiedelt. Außerdem werden die dazugehörigen Anwendungsprotokolle, wie z.B. HTTP(S), FTP, SMTP etc., dieser Schicht zugeordnet. Weiterhin übernimmt der Application Layer auch die Benutzerauthentifizierung.

Eselsbrücke: Stellen Sie sich bei dieser Schicht vor, wie Sie eine Website in Ihrem Browser aufrufen.

Schicht 6 – Presentation Layer (Präsentationsschicht)

Hier wird eine Normierung der Daten vorgenommen. So könnte die Textdatei z.B. im ASCII- oder EBCDIC-Format versendet werden oder aber der Film im MPEG-4-Format vorliegen. Doch auch die Datenkompression sowie Verschlüsselung von Daten fällt in diese Schicht.

Eselsbrücke: Stellen Sie sich bei dieser Schicht vor, wie Sie aus einer Audiodatei ein MP3-File erzeugen.

Schicht 5 – Session Layer (Sitzungsschicht)

Diese Schicht definiert die Kommunikation zwischen zwei Netzwerkknoten auf *Anwendungsebene*, sogenannte *Sessions* (bzw. Sitzungen). Hierzu steuert und überwacht diese Schicht den Aufbau, Verlauf und Abbau dieser Sessions. Namentlich *NetBIOS*, das Windows-Netzwerkprotokoll, arbeitet auf dieser Ebene.

Eselsbrücke: Stellen Sie sich bei dieser Schicht vor, wie Sie auf eine Datei in einer Windows-Netzwerkfreigabe zugreifen.

Schicht 4 – Transport Layer (Transportschicht)

An dieser Stelle verlassen wir die Anwendungsebene und begeben uns auf die Netzwerkebene. Der Transport Layer ist die höchste Schicht, die der Netzwerkebene zugerechnet wird. Waren die bisherigen Funktionen spezifisch für jede Anwendung, so sind die Protokolle und Aufgaben der unteren vier Schichten eher generisch, also grundsätzlich unabhängig von der Anwendung. Die wichtigsten Protokolle des Transport Layers in der Praxis sind *TCP* und *UDP*. Auf dieser Ebene werden Funktionen wie Segmentierung, Multiplexing, Flusskontrolle und die Fehlerkorrektur realisiert.

Wenn Sie sich zum ersten Mal mit dem OSI-Modell beschäftigen, wird es Ihnen vielleicht etwas schwerfallen, diese Begriffe aufzunehmen, da Ihnen die Assoziationen fehlen. Doch keine Sorge: In Kapitel 8 »Die Transportprotokolle TCP und UDP« kommen wir im Rahmen von TCP auf diese Mechanismen zurück. Dort lernen Sie, wie Multiplexing (durch die Ports), Flusskontrolle und Fehlerkorrektur in der Praxis funktionieren.

Interessanterweise beziehen sich die *Flusskontrolle* und die *Fehlerkorrektur*-Mechanismen nur auf das Protokoll TCP. Dagegen ist UDP unzuverlässig (unreliable), hat von den angesprochenen Mechanismen lediglich das *Multiplexing* sowie die *Segmentierung* eingebaut und überträgt nur nach »best effort«, also nach bestem Wissen und Gewissen, jedoch ohne Garantie. Trotzdem ist auch dieses Protokoll der Transportschicht zugeordnet, da es – genau wie TCP – eine Art generische Ladefläche für die Nutzdaten enthält.

Eselsbrücke: Stellen Sie sich bei dieser Schicht einen Lkw mit einer Ladefläche vor (TCP und UDP), auf der beliebige Nutzlast (die Anwendungsprotokolle) transportiert werden kann. Kommt der Lkw am Ziel an, sucht er sich eine ganz bestimmte Laderampe (den Port) aus, an dem er seine Last ablädt.

Schicht 3 – Network Layer (Vermittlungsschicht)

Auf dieser Schicht geschehen viele essenzielle Prozesse der Adressierung und Wegfindung. Schauen wir auf die einzelnen Funktionen des Network Layers:

- *Aufteilung in Pakete:* Die Dateneinheiten des Network Layers werden Pakete (Packets) genannt.
- *Logische Adressierung:* Konkret sind das hier die IP-Adressen des Absenders und Empfängers eines Datenpakets.
- *Routing:* Die Wegfindung und Pflege der Routing-Tabellen eines Routers obliegt ebenfalls dem Network Layer.

Eine der beiden Kernkomponenten von Netzwerken, der *Router*, ist der dritten Schicht, dem Network Layer, zugeordnet. Der *Switch* dagegen ist nicht ganz so intelligent in seiner Logik wie ein Router und muss sich daher mit der nächstniedrigeren Schicht, dem *Data Link Layer*, begnügen, den wir Ihnen gleich im Anschluss vorstellen.

Eselsbrücke: IP-Netzwerke (Subnetze) sind wie Straßen, einzelne IP-Hostadressen vergleichbar mit Hausnummern. Router sind wie Straßenkreuzungen mit Ampeln und Hinweisschildern: Demnach ist das IP-Protokoll übrigens nichts anderes als das Auto selbst bzw. der fahrbare Untersatz.

Schicht 2 – Data Link Layer (Sicherungsschicht)

Die Sicherungsschicht regelt den Zugriff auf das Übertragungsmedium. Demnach ist auch die physische Adressierung hier angesiedelt. Hierzu gleich eine Anmerkung: Im Gegensatz zur logischen Adresse ist die physische Adresse fest und grundsätzlich nicht veränderbar. Es gibt eine ganze Reihe von Synonymen für diesen Begriff, z.B. Hardware-Adresse, Burned-In Address (BIA) und insbesondere MAC-Adresse.

MAC (Media Access Control) ist die untere der beiden Teilschichten, in die der Data Link Layer weiter unterteilt werden kann. Sie ist hardwarenäher und regelt im engeren Sinne den Zugriff auf das Übertragungsmedium. Die obere Teilschicht heißt *LLC* (Logical Link Control) und übernimmt Flusskontrollfunktionen auf dieser Ebene. Hierzu werden z.B. Prüfsummen an eine Dateneinheit angehängt.

Eselsbrücke: Denken Sie bei dieser Schicht an Netzwerkkarten und Switches. Sie implementieren Funktionen des Data Link Layers.

Schicht 1 – Physical Layer (Bit-Übertragungsschicht)

Die unterste Schicht des OSI-Modells beinhaltet die physischen Eigenschaften des Netzwerks. Wie die (in diesem Fall treffende) deutsche Bezeichnung aussagt, geht es hier um die Übertragung der einzelnen Bits. Zu den Festlegungen des *Physical Layers* gehören also Dinge wie:

- Kabelspezifikationen (z.B. Cat5)
- Frequenz- und Spannungswerte (was bedeutet 0, was 1?)
- Definition der Steckverbindungen und Pin-Belegungen (z.B. RJ45)

Die Hardware auf dieser Schicht umfasst:

- Repeater (Signalverstärker zwischen zwei Segmenten)
- Hubs (die Vorgänger der Switches, auch als *Multiport-Repeater* bezeichnet)
- Modems

Eselsbrücke: Denken Sie bei dieser Schicht an die Verbindung des Computers mit dem Switch per Patchkabel. Sowohl der Kabeltyp als auch der Stecker sind auf dieser Ebene spezifiziert.

Kapselung im OSI-Modell

Die einzelnen Schichten sind für bestimmte Funktionen zuständig. Um die jeweiligen Verwaltungsinformationen jeder Schicht zu transportieren, werden sogenannte *Header* vor die Nutzdaten gesetzt. Jede Schicht fügt ihren eigenen Header hinzu. Diesen Prozess bezeichnet man als *Kapselung* (encapsulation).

Die einzelnen Datenabschnitte, die sich aus den Headern und den Nutzdaten zusammensetzen, werden im OSI-Modell *PDUs* (Protocol Data Units) genannt. Dementsprechend gibt es sieben PDUs, wobei von Schicht 7 bis Schicht 2 immer neue Header hinzukommen. Schicht 2 (Data Link Layer) fügt optional noch einen Trailer (das FCS-Feld bzw. die Prüfsumme) hinzu (siehe Abbildung 1.13).

Sie sehen in der Abbildung sehr schön das Prinzip: Der Header der übergeordneten Schicht wird zu den Nutzdaten der untergeordneten Schicht gezählt, sodass diese sich nicht um den Inhalt dessen, was sie selbst einkapselt, kümmern muss. Auf dem Empfängersystem entfernt jede Schicht den ihr zugehörigen Header, sodass letztlich nur noch die Nutzdaten übrig bleiben, mit denen die Anwendung arbeitet.

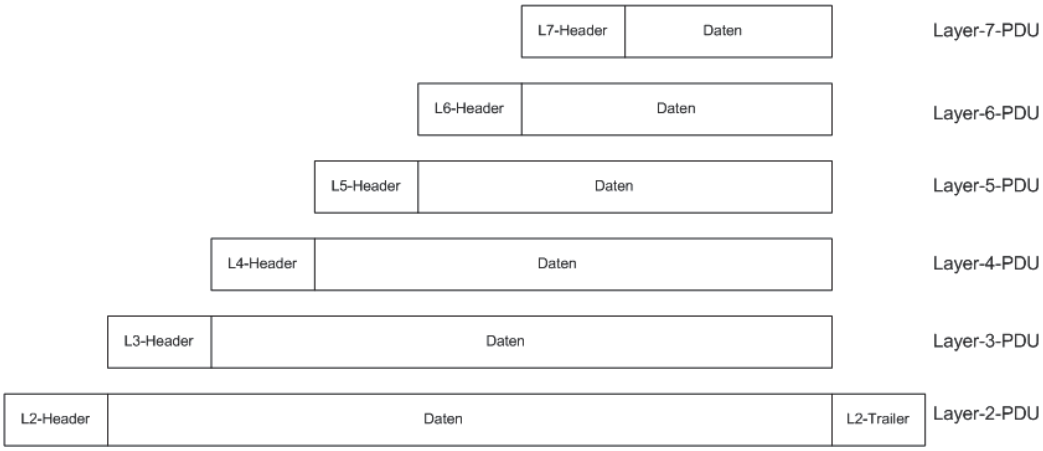


Abb. 1.13: Die OSI-PDUs

1.6.2 Das TCP/IP-Modell

Neben dem OSI-Modell existiert ein zweites Modell mit ganz ähnlichen Schichten: das TCP/IP-Referenzmodell. Es wurde bereits ab 1970 entwickelt und begann mit einer Studie der ARPA (Advanced Research Projects Agency), die wiederum dem amerikanischen Verteidigungsministerium (Department of Defense, DoD) untersteht. Dementsprechend wird dieses Modell auch als *DoD-Modell* bezeichnet. Das TCP/IP-Referenzmodell ist ähnlich wie das OSI-Modell aufgebaut, unterscheidet im Gegensatz zum OSI-Modell jedoch nur vier Schichten, die aber völlig ausreichen, um alle wichtigen Netzwerkfunktionalitäten und -prozesse abzubilden. Die vier Schichten sind in Abbildung 1.14 dargestellt.

TCP/IP-Referenzmodell	
4	Application Layer
3	Transport Layer
2	Internet Layer
1	Link Layer

Abb. 1.14: Die Schichten des TCP/IP-Referenzmodells

Im Gegensatz zum OSI-Modell ist es weit weniger komplex ausgelegt und bezieht sich auch nur auf die im TCP/IP-Stack verwendeten Protokolle. Es definiert keine Standards für Übertragungsmedien oder -techniken.

Wenn wir Ihnen im Folgenden die einzelnen Schichten vorstellen, werden Sie die Ähnlichkeit zum OSI-Modell bemerken. Am Ende dieses Abschnitts werden wir das TCP/IP-Modell mit dem OSI-Modell vergleichen.

Schicht 4 – Application Layer (Anwendungsschicht)

Das TCP/IP-Modell kennt ebenfalls den Bereich der Netzwerkanwendungen. Im Gegensatz zum OSI-Modell werden jedoch keine detaillierten Unterscheidungen getroffen – die Schichten 5 bis 7 werden beim TCP/IP-Modell einfach unter dem *Application Layer* zusammengefasst. Er umfasst also alle Protokolle, die mit den Netzwerkanwendungen direkt zusammenarbeiten, wie z.B. HTTP(S), FTP, SMTP, Telnet, SSH etc.

Schicht 3 – Transport Layer (Transportschicht)

Diese Schicht können Sie nahezu eins zu eins aus dem OSI-Modell übertragen. Der Transport Layer stellt sogenannte *Ende-zu-Ende-Verbindungen* (End-to-End-Connections) her. Das bedeutet, dass die Netzwerkknoten auf dieser Schicht direkt miteinander kommunizieren. Die generischen Transportprotokolle TCP und UDP werden diesem Layer zugeordnet.

Schicht 2 – Internet Layer (Internetschicht)

Während das OSI-Modell den *Network Layer* definiert (allerdings als Schicht 3), übernimmt diese Funktion im TCP/IP-Modell der *Internet Layer*. IP-Adressierung, Routing etc. sind diesem Layer zugeordnet, ebenso wie die Protokolle *IP*, *ICMP* und andere sowie die Hardware-Komponente *Router*.

Schicht 1 – Link Layer (Netzzugangsschicht)

Obwohl die Netzzugangsschicht im TCP/IP-Modell spezifiziert ist, enthält sie keine Protokolle der TCP/IP-Familie. Nun ja, keine bis auf ARP, das *Address Resolution Protocol*, das genutzt wird, um IP-Adressen in MAC-Adressen aufzulösen. Dieses ist zwischen den Welten als Vermittler angesiedelt. Wir erklären Ihnen die Funktionsweise von ARP in Kapitel 5 »ARP und ICMP«. Der Link Layer entspricht den unteren beiden Schichten des OSI-Modells (*Data Link Layer* und *Physical Layer*).

Kapselung im TCP/IP-Modell

Während die gekapselten Datenabschnitte im OSI-Modell allgemein *PDU*s heißen, haben die Kapselungen im TCP/IP-Modell jeweils einen speziellen Namen:

- Application Layer: *Daten* (keine Kapselung im Sinne der Netzwerkkommunikation)
- Transport Layer: *Segmente (Segments)* bei TCP und *Datagramme (Datagrams)* bei UDP
- Internet Layer: *Pakete (Packets)* bzw. *IP-Pakete*
- Link Layer: *Rahmen (Frames)*

Beachten Sie, dass die Bezeichnung der Kapselung damit auch eindeutig die Schicht bzw. Ebene definiert, in der wir uns befinden. So werden Pakete von einem Router weitergeleitet und Rahmen (hier ist die englische Bezeichnung *Frames* geläufiger) von einem Switch. Wir werden in diesem Buch noch häufiger auf diese Begriffe zu sprechen kommen.

1.6.3 Vergleich OSI- und TCP/IP-Modell

Wir haben es bereits erwähnt: Beide Referenzmodelle sind relativ einfach zu vergleichen. Verschaffen wir uns also noch einmal einen kurzen Überblick in Abbildung 1.15.

In Wirklichkeit sind die Übereinstimmungen nicht ganz so direkt, wie die Abbildung suggeriert. Während das TCP/IP-Referenzmodell die Funktionalitäten der TCP/IP-Protokollfamilie exakt abbildet, stimmen die Zuordnungen im OSI-Modell nur bedingt, da dieses Modell einzelnen Schichten nur allgemeine Netzwerkfunktionalitäten zuordnet. Betrachten Sie dies als eine eher näherungsweise Zuordnung. Zum Verständnis der Zusammenhänge reicht das jedoch völlig aus.

OSI	TCP/IP
Application Layer	Application Layer
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer
Network Layer	Internet Layer
Data Link Layer	Link Layer
Physical Layer	

Abb. 1.15: Vergleich zwischen OSI- und TCP/IP-Modell

Tipp

In der Praxis wird häufig ein Mix aus beiden Modellen genutzt. Das TCP/IP-Modell fasst die drei oberen Schichten des OSI-Modells zum Application Layer zusammen, was sich in der Praxis meist als ausreichend darstellt. Dagegen ergibt es – gerade beim Troubleshooting – oft Sinn, die unteren beiden Schichten des OSI-Modells, also Data Link und Physical Layer, zu unterscheiden.

1.7 Zahlensysteme

In der Informationstechnologie und insbesondere auch in der Netzwerktechnik stolpern Sie immer wieder über binäre und hexadezimale Zahlen, daher legen wir hier einige Grundlagen.

1.7.1 Bits und Bytes – das Binärsystem

Wenn wir Menschen Zahlen darstellen, nutzen wir in der Regel das *Dezimalsystem*. Wir unterscheiden dabei in Einer-, Zehner-, Hunderter- und Tausender-Stellen etc. Diese kommen zustande, indem wir die Basis 10 potenzieren. Von rechts nach links wird den einzelnen Stellen damit eine Wertigkeit verliehen (vgl. Tabelle 1.1).

Stelle	4	3	2	1
Wertigkeit	10^3=1000	10^2=100	10^1=10	10^0=1

Tabelle 1.1: Die Wertigkeiten des Dezimalsystems

Diese Wertigkeit ist nichts anderes als ein Faktor, womit die Ziffer der entsprechenden Stelle multipliziert wird. Nehmen wir z.B. die Zahl 1294. Wir multiplizieren die einzelnen Ziffern von rechts nach links mit ihren jeweiligen Wertigkeiten und addieren die Ergebnisse. Dann ergibt sich die folgende Rechnung:

4 x 1 + **9** x 10 + **2** x 100 + **1** x 1000

Für das Dezimalsystem stehen pro Stelle zehn verschiedene Ziffern (0 bis 9) zur Verfügung. Natürlich kennt jeder dieses System und nutzt es täglich, meist ohne sich viel Gedanken darum zu machen.

Leider rechnen Computer nicht wie Menschen. Während wir für gewöhnlich das *Dezimalsystem* verwenden, nutzen Computer das *Binärsystem*. Die kleinste Einheit im Binärsystem ist das *Bit*. Es kann genau zwei Zustände annehmen: 1 und 0.

Man spricht auch davon, dass ein Bit *gesetzt* (also 1) oder *nicht gesetzt* (also 0) ist.

Packt man 8 Bits zusammen, erhält man ein *Byte*. Ein Byte besteht also aus 8 Bits, die einzeln entweder gesetzt oder nicht gesetzt sein können, aber immer zusammengehören. Damit daraus etwas Vernünftiges entstehen kann, hat jedes Bit im Byte eine bestimmte Wertigkeit – und die basiert auf den Potenzen der Zahl 2 (daher *Bi*närsystem). Nachfolgend in Tabelle 1.2 die Bits und deren Wertigkeiten im Byte.

Bit	8	7	6	5	4	3	2	1
Wert	128	64	32	16	8	4	2	1
	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

Tabelle 1.2: Wertigkeit der Bits in einem Byte

Ein Byte kann demnach 256 verschiedene Werte annehmen, nämlich 0 (kein Bit gesetzt) bis 255 (alle Bits gesetzt). Nachfolgend in Tabelle 1.3 einige Beispiele zur Verdeutlichung:

Dezimalzahl	Byte-Wert
4	0000 0100
128	1000 0000
163	1010 0011
255	1111 1111

Tabelle 1.3: Beispiele für die Umrechnung von Dezimal- in Binärzahlen

Gerade beim Subnetting im Rahmen der IP-Adressierung werden Sie intensiv mit Binärzahlen zu tun haben, daher lohnt es sich, das Konzept zu verstehen.

1.7.2 Größenordnungen

Stuttgart liegt von Berlin ca. 630 km entfernt. Natürlich könnten wir auch sagen, dass die Distanz 630.000 Meter beträgt, aber die Zahl wäre unnötig lang. Um Zahlenausdrücke kürzer zu gestalten, nutzen wir Multiplikatoren. Sie sagen also nicht 100.000 Meter, sondern 100 Kilometer und meinen damit 100 x 1000 Meter, da der Begriff »Kilo« im Dezimalsystem die Multiplikation mit 1000 beschreibt.

Auch im Binärsystem gibt es diese Multiplikatoren, die auf der Basis von 1024 erfolgen, da die Werte der jeweiligen Stellen um Zweierpotenzen wachsen:

- 1 Kibibyte (KiB) = 1024 Bytes
- 1 Mebibyte (MiB) = 1024 Kibibytes
- 1 Gibibyte (GiB) = 1024 Mebibytes
- 1 Tebibyte (TiB) = 1024 Gibibytes

Hinweis

Vielleicht sind Sie jetzt irritiert, da Sie mit den Begriffen *Kilobyte*, *Megabyte*, *Gigabyte* etc. gerechnet haben? Tatsächlich wird dies oft auch noch so genutzt, jedoch ist formal der Multiplikator »Kilo« das 1.000-fache des Ausgangswertes, also 1.000 Byte. Demnach ist korrekterweise ein Megabyte = 1.000 Kilobyte = 1.000.000 Byte. Die sogenannten *Binärpräfixe* mit der Silbe »bi« wurden eingeführt, um den Zweierpotenzen Rechnung zu tragen. Allerdings werden die festgelegten Normen nicht überall konsequent verwendet. Da die Multiplikatoren 1000 und 1024 mehr oder weniger nahe beieinanderliegen, ist das in der Größenordnung meistens kein Problem in der Praxis. Dennoch sollten Sie den Unterschied kennen.

Während die Größe von Daten und Speichermedien in Byte bzw. als ein Multiplikator von Byte angegeben werden, bleiben wir für die Angabe von Datenraten bei der Datenübertragung bei den Bits. Gemessen wird die Datenrate pro Sekunde.

Hier werden nach wie vor die Begriffe *Kilobit* (Kbit), *Megabit* (Mbit) oder *Gigabit* (Gbit) genutzt. Da es keine Potenz in der Berechnung der Werte gibt, sondern einfach nur eine Anzahl an Binärziffern (Bits), ist die Sache klar: Eine Datenrate von 1 Kilobit/s bedeutet, dass 1.000 Bits pro Sekunde übertragen werden. Ein Megabit/s bedeutet die Übertragung von 1.000.000 Bits pro Sekunde.

Hinweis

Im Übrigen wird häufig das Wort *Bandbreite* genutzt, um die Kapazität einer Leitung zu beziffern. Ursprünglich stammt das Wort aus der analogen Übertragung mittels Frequenzen, die verschiedene Bänder zur Verfügung gestellt haben. Auch heute werden diese Bänder noch in der drahtlosen Übertragung verwendet (z.B. 2,4-GHz- oder 5-GHz-Band). Je mehr Bandbreite eine Kommunikation nutzen kann, desto mehr Daten können über die Frequenzen transportiert werden. Allerdings wird das Wort Bandbreite auch oft in der Netzwerktechnik verwendet, um die maximale Datenübertragungsrate auszudrücken. Für die Menge der tatsächlich übertragenen Daten wird in der Netzwerktechnik meistens von *Datenrate* oder *Durchsatz* gesprochen.

1.7.3 Das Hexadezimalsystem

Neben dem Binärsystem treffen wir in der Informationstechnologie häufig auf ein zweites Zahlensystem: das *Hexadezimalsystem*. Es arbeitet mit einer Basis von 16er-Potenzen. Durch die Nähe zum Binärsystem ($16=2^4$) können Binärzahlen somit einfacher und kürzer dargestellt werden. Es funktioniert folgendermaßen:

Da wir hier pro Stelle 16 mögliche Werte haben, bedient sich das Hexadezimalsystem noch einiger Buchstaben des Alphabets, nämlich A bis F. Betrachten Sie die Gegenüberstellung aus Tabelle 1.4:

Dezimal	Binär	Hexadezimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5

Tabelle 1.4: Gegenüberstellung der Zahlensysteme

Dezimal	Binär	Hexadezimal
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Tabelle 1.4: Gegenüberstellung der Zahlensysteme (Forts.)

Das ist zugegebenermaßen etwas gewöhnungsbedürftig. Der große Vorteil liegt in der Komprimierung der Darstellung: Sie können mit dem Hexadezimalsystem nämlich ein Byte mit zwei Stellen darstellen – im Dezimalsystem benötigen Sie drei Stellen. Schauen wir uns die Wertigkeiten der ersten vier Stellen des Hexadezimalsystems in Tabelle 1.5 einmal an.

Stelle	4	3	2	1
Wertigkeit	16^3=**4096**	16^2=**256**	16^1=**16**	16^0=**1**

Tabelle 1.5: Die Wertigkeiten im Hexadezimalsystem

Jeder Hexadezimalwert (von 0 bis F, sprich: 15) wird entsprechend mit der Wertigkeit seiner Stelle multipliziert. Nehmen wir nur die ersten beiden Stellen rechts, ergibt sich ein Wertebereich von dezimal 0 x 16 + 0 x 1 = **0** bis 15 x 16 + 15 x 1 = **255**. Dies wiederum entspricht genau einem Byte – voilà!

Hier die gute Nachricht: Sie werden in fast allen Fällen immer nur mit zwei Stellen im Hexadezimalsystem rechnen müssen! Die schlechte Nachricht ist, dass Sie fast zwangsläufig über hexadezimale Zahlendarstellungen stolpern werden. Sie finden Hexadezimalzahlen z.B. bei der Darstellung von MAC-Adressen oder IPv6-Adressen. Machen Sie sich also besser gleich damit vertraut!

In Tabelle 1.6 sehen Sie einige Beispiele für hexadezimale Werte.

Dezimalwert	Hexadezimalwert
25	19
230	E6
255	FF
1.024	04 00
4.096	10 00

Tabelle 1.6: Beispiele für Hexadezimalwerte

Kapitel 2

Kabelgebundene Übertragungstechnologien

Auch wenn drahtlose Technologien zur Datenübertragung ein fester Bestandteil moderner IT-Netzwerke sind, werden die meisten Netzwerke heutzutage nach wie vor hauptsächlich über kabelgebundene Technologien realisiert. In diesem Kapitel lernen Sie daher einige wichtige Übertragungstechnologien kennen, die auf den unteren beiden Schichten des OSI-Modells, also dem *Physical Layer* und dem *Data Link Layer*, angesiedelt sind.

Dabei können wir ganz grob zwischen LAN- und WAN-Technologien unterscheiden. Im LAN wird fast ausschließlich Ethernet genutzt. Da diese Technologie für moderne Netzwerke so entscheidend ist, werden wir uns zu einem großen Teil in diesem Kapitel damit befassen. Sie lernen, wie Ethernet und das Switching funktionieren und welche wichtigen Features in professionellen Umgebungen genutzt werden. Dazu zählen insbesondere Virtuelle LANs (VLANs), aber auch das Spanning Tree Protocol (STP). Außerdem werfen wir einen Blick auf einige gängige WAN-Technologien, dazu gehören Metro Ethernet, MPLS und andere.

2.1 Kabel und Stecker

Bevor wir uns mit den eher logischen Aspekten der Datenübertragung befassen können, müssen wir zunächst die physischen Komponenten betrachten. Daher beginnen wir mit einem Blick auf die Kabel und Stecker, die in Computernetzwerken im Allgemeinen und Ethernet im Speziellen zum Einsatz kommen. Die Standardisierung erfolgt über das IEEE, das wir Ihnen schon im vorigen Kapitel vorgestellt haben. Genauer ist die Arbeitsgruppe 802.3 für die Ethernet-Standardisierung zuständig.

Die Nomenklatur der Ethernet-Standards erfolgt meistens auf die folgende Art:

```
Übertragungsrate+Übertragungstechnik+Kabeltyp
```

In der Netzwerktechnik wird vorwiegend die *Basisbandübertragung* genutzt, bei welcher der Frequenzbereich gleich dem Nutzsignal ist und keine Modulation auf eine Trägerfrequenz erfolgt. Daher steht meistens »BASE« in der Mitte der Bezeichnung. Ihr steht die *Breitbandübertragung* gegenüber, die Modulationstechniken nutzt, um mehrere Signale gleichzeitig auf verschiedenen Frequenzbändern zu übertragen.

2.1.1 Koaxialkabel-Standards

Wie Sie bereits im vorigen Kapitel gelernt haben, wurden Ethernet-Netzwerke anfangs als physischer Bus implementiert. Hierzu wurden hauptsächlich zwei Standards, basierend auf Koaxial-Kupferkabeltypen, verwendet:

1. **10BASE2 (RG 58)** – das sogenannte *Thinnet-Kabel* (auch: Cheapernet). Es wurde für die Anschlüsse eines Computers verwendet, der an seiner Netzwerkkarte eine BNC-Buchse hatte.

BNC steht u.a. für *British Naval Connector* (es gibt noch andere Bedeutungen) und bezeichnet einen Bajonettverschluss. Die Kabelenden wurden durch einen 50-Ohm-Widerstand abgeschlossen, um Signalreflexionen zu verhindern. Die maximale Datenrate beträgt 10 Mbit/s und ein Segment darf maximal 185 Meter lang sein, bevor ein Repeater das Signal wieder verstärken muss. Daher wurde auf 200 Meter aufgerundet und im Standard eine 2 geschrieben.

2. **10BASE5 (RG-8)** – das sogenannte *Thicknet-Kabel* (auch: Yellow Cable). Es wurde für größere Netzwerke (z.B. in Universitäten) verwendet und ermöglicht bei gleicher maximaler Datenrate eine maximale Segmentlänge von 500 Metern. Die Geräte wurden über Transceiver und 15-polige AUI-Stecker angeschlossen und das Signal wurde mittels Vampirklemme abgegriffen. Das heißt, dass eine Nadel, ähnlich wie ein Vampirzahn, in das Kabel »beißt«, um durch die Ummantelung zum relativ dicken Kupferdraht zu gelangen.

Diese Art der Verkabelung war teuer, komplex, unflexibel und fehleranfällig. Daher wird sie in heutigen Netzwerken nicht mehr verwendet (ausgenommen sind evtl. alte Produktionsnetzwerke). Wir gehen daher nicht näher darauf ein.

Hinweis

Koaxialkabel sind jedoch nicht ausgestorben. Sie werden z.B. beim Kabelfernsehen und allgemein bei Kabel-Internetanschlüssen verwendet.

2.1.2 Twisted-Pair-Standards

Koaxialkabel wurden in der Netzwerktechnik bald von Twisted-Pair-Kabeln abgelöst. Ein Twisted-Pair-Kabel ist flexibler, günstiger und ermöglicht eine skalierbare Vernetzung von Gebäuden. Dafür bedarf es eines oder mehrerer Sternverteiler, also einem Hub oder Switch (Abschnitt 2.2.3). Im Laufe der Zeit wurden zahlreiche Twisted-Pair-Standards entwickelt, um den immer höheren Anforderungen an höhere Übertragungsraten gerecht zu werden. Die Entwicklung ist hier noch nicht abgeschlossen, sodass es in Zukunft voraussichtlich weitere Standards geben wird.

Aufbau eines Twisted-Pair-Kabels

Bei Twisted-Pair-Kabeln (TP) handelt es sich um verdrillte Adernpaare in einer Ummantelung (vgl. Abbildung 2.1).

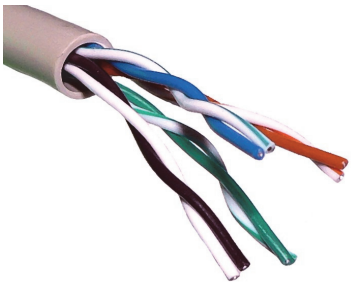


Abb. 2.1: Die Adernpaare werden verdrillt und in einer Kunststoffhülle zusammengefasst.

Die Verdrillung reduziert elektromagnetische Störsignale (engl. electromagnetic interference, EMI) und Übersprechen, also die ungewollte Signalübertragung von einem Kabel oder Leiter auf ein benachbartes Kabel oder einen anderen Leiter. Dennoch sind TP-Kabel gegenüber Koaxialkabeln anfälliger gegenüber den genannten Störungen, zudem ist die Dämpfung höher, sodass diese Kabel eine geringere maximale Länge haben. Auch die mechanische Empfindlichkeit ist höher als bei Koaxialkabeln.

Die Nutzung von TP-Kabeln bringt gegenüber Koaxialkabeln jedoch einige Vorteile mit sich, welche die Nachteile mehr als aufwiegen:

- Die Kabel sind deutlich günstiger herzustellen.
- TP-Kabel sind flexibler im Mindestbiegeradius und weniger bruchanfällig.
- TP-Kabel sind in fast jedem Gebäude in Form von Telefonleitungen bereits vorhanden (die sind allerdings für die Datenübertragung nur bedingt geeignet).

Twisted-Pair-Kabel werden schon sehr lange für die unterschiedlichsten Zwecke eingesetzt. Es existieren verschiedene Arten von TP-Kabeln.

Die Twisted-Pair-Kategorien

Twisted-Pair-Kabel werden entsprechend ihrer Leistungsfähigkeit und ihrer Spezifikation in Kategorien eingeteilt. Lassen Sie uns an dieser Stelle einen Blick auf die vorhandenen Kategorien werfen – auf die Details der in den Bemerkungen genannten Ethernet-Standards kommen wir später noch zurück (vgl. Tabelle 2.1).

Kategorie	Bandbreite	Bemerkung
Cat1	100 KHz	Alter Telefondraht
Cat2	1,5 MHz	Hausverkabelung für ISDN
Cat3	16 MHz	In Amerika Standard für Telefonverkabelung, wurde oft für 10Base-T verwendet
Cat4	20 MHz	Ebenfalls insbesondere in Amerika verbreitet
Cat5/5e	100 MHz	Verwendung für Fast-Ethernet (100 Mbit/s) und in der Überarbeitung als 5e auch für Gigabit-Ethernet (1000 Mbit/s)
Cat6A	500 MHz	Für 10-Gigabit-Ethernet konzipiert
Cat7/7A	600-1000 MHz	Globaler Standard außerhalb der USA, wird immer als S/FTP-Kabel angeboten (siehe nächster Abschnitt) und ist die Standardverkabelung für Gebäude
Cat8, 8.1 und 8.2	1600-2000 MHz	Bislang höchste Übertragungskapazität, für 40-Gigabit-Ethernet (40GBASE-T) geeignet

Tabelle 2.1: Twisted-Pair-Kategorien

Für Netzwerktechnik hat sich mittlerweile der Bereich ab Cat5 aufwärts etabliert, Kategorien darunter spielen hier keine Rolle mehr. Cat5e wurde nach einer Neufassung der Normen wieder als Cat5 bezeichnet, sodass heutzutage die Bezeichnungen Cat5 und Cat5e synonym sind.

Geschirmte und ungeschirmte TP-Kabeltypen

Eine weitere Unterscheidung liegt in der Abschirmung der Kabel. TP-Kabel werden sowohl ohne Abschirmung als auch mit verschiedenen Ummantelungen angeboten. Sie werden nach ISO/IEC 11801 unterschieden und bezeichnet. Dazu zählen unter anderem:

- **UTP:** *Unshielded Twisted Pair*, ungeschirmte Adernpaare und ohne Gesamtschirm. Während dieser Kabeltyp im deutschsprachigen Raum recht wenig verbreitet ist, wird er weltweit am häufigsten eingesetzt.
- **STP:** *Shielded Twisted Pair*, abgeschirmtes Kabel, wobei zwei Varianten unterschieden werden:
  - **S/STP:** *Screened Shielded Twisted Pair*, sowohl die Adernpaare als auch die Ummantelung werden mit einem Drahtgeflecht geschützt.
  - **F/STP:** *Foiled Shielded Twisted Pair*, während die Adernpaare mit einem Drahtgeflecht geschützt werden, besteht der Gesamtschirm unter der Ummantelung aus Folie.
- **FTP:** *Foiled Twisted Pair*, eine Sammelbezeichnung für unterschiedliche Arten von Abschirmung durch Aluminiumfolie. Es können sowohl zwei als auch vier Adern oder auch ausschließlich die Ummantelung geschirmt werden. Hierzu finden sich Varianten, wie z.B. S/FTP (siehe Abbildung 2.2).

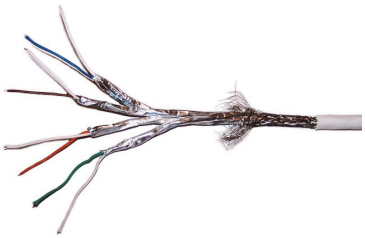


Abb. 2.2: Aufbau eines S/FTP-Kabels

Es gibt noch einige andere Varianten und teilweise wurden die Bezeichnungen auch geändert. Bei Kabeln ab der Kategorie 7 ist UTP nicht mehr zugelassen, allerdings werden auch Kabel der Kategorie 6a kaum als UTP angeboten.

Der RJ-45-Stecker

TP-Kabel bestehen aus zwei oder vier Adernpaaren. Um die Signale am Ende des Kabels an die Schnittstelle (den Port) weiterzuleiten, werden üblicherweise RJ-45-Stecker verwendet (vgl. Abbildung 2.3).

Die Pin-Belegungen sind genormt und basieren auf der ebenfalls normierten Farbgebung der einzelnen Adern. Es existiert jeweils ein durchgängig eingefärbter und ein teilgefärbter Draht. Hierbei wird unterschieden in EIA/TIA-568A und EIA/TIA-568B. In Abbildung 2.4 sehen Sie die Farbcodes am Beispiel von EIA/TIA-568A, dem am häufigsten eingesetzten Standard.

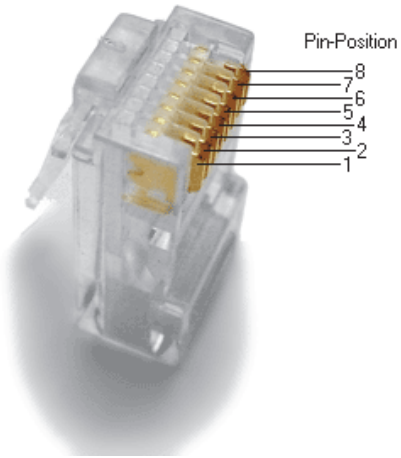


Abb. 2.3: RJ-45-Stecker (Quelle: Aaron Kaase, Wikipedia)

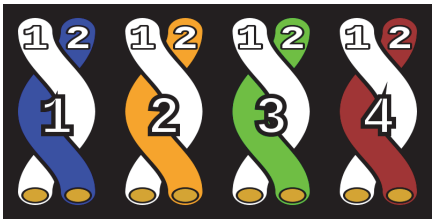


Abb. 2.4: Die Adernpaare gemäß TIA-568A (Quelle: Pumbaa80)

Im Übrigen werden bei höheren Ethernet-Standards mit Verkabelung ab Kategorie 7 etwas andere Stecker als RJ-45 genutzt, da die Pins hier zu nahe beieinanderliegen, um bei den erforderlichen hohen Frequenzen Übersprechen zu verhindern. Es stehen hier zwei Stecker zur Auswahl: GG45 und TERA. In der Praxis werden Sie jedoch voraussichtlich hauptsächlich mit RJ-45 zu tun haben.

Straight-Through und Crossover-Kabel

Gemäß dem Standard ist festgelegt, welche Adern für das Senden und welche für das Empfangen von Datensignalen verwendet werden. Verbinden Sie einen Knoten (z.B. einen PC) mit einem Sternverteiler (Hub oder Switch), sind die Pin-Belegungen in der Anschlussbuchse (Port) im Sternverteiler entsprechend vertauscht, sodass er auf den Adern, auf denen der angeschlossene Knoten sendet, empfängt und umgekehrt. Ein normales Kabel, das an beiden Enden im Stecker dieselbe Pin-Belegung hat, bezeichnen wir als *Straight-Through-Kabel*.

Verbinden Sie gleichartige Systeme (also Knoten) untereinander (z.B. einen PC direkt mit einem anderen PC), dann wären die Pin-Belegungen in der Buchse der NIC gleich und es käme zu einer Kollision von Sende- und Empfangsleitungen. Das kann durch eine Vertauschung der Adernpaare in der Steckerbelegung vermieden werden. In einem *Crossover-Kabel* sind die Adern 1 und 2 am einen Ende vertauscht und liegen am anderen Ende auf 3 und 6. Die PIN-Belegung stellt sich dar, wie in Abbildung 2.5 gezeigt.

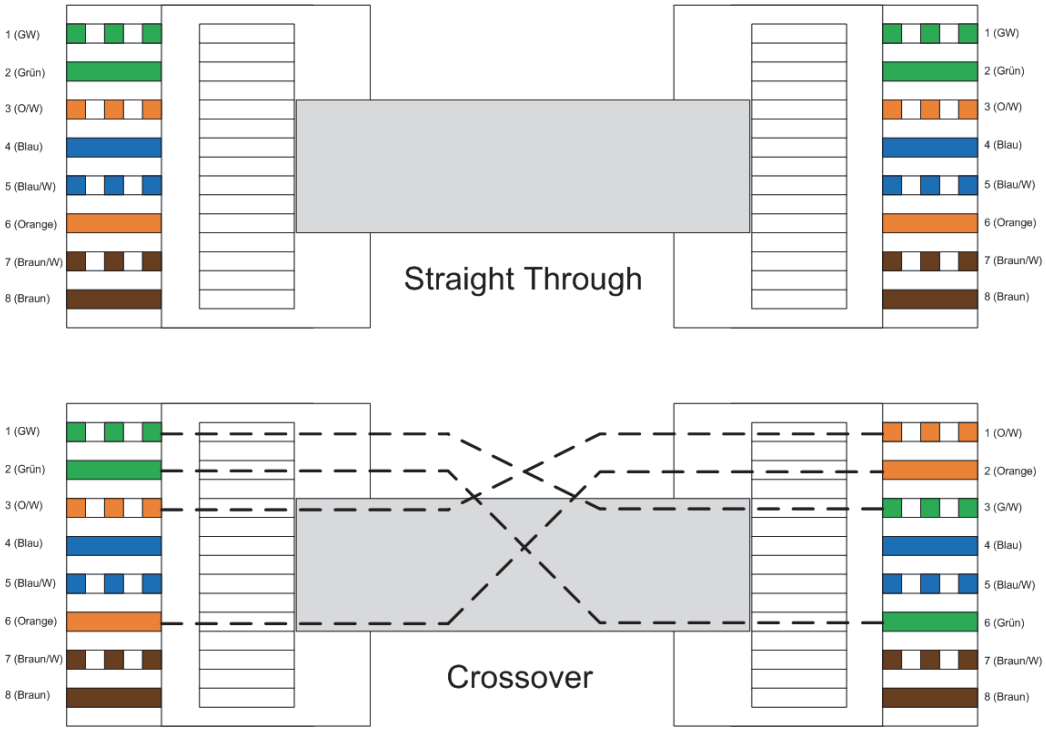


Abb. 2.5: Pin-Belegung bei Straight-Through- und Crossover-Kabeln

Das funktioniert, weil bis zum Ethernet-Standard für 100 Mbit/s maximale Datenrate (100BASE-TX) nur zwei Adernpaare für die Übertragung genutzt werden. Ab Gigabit-Ethernet (1000BASE-T) werden jedoch alle vier Paare verwendet. Um das Problem zu lösen, ist ab dem Gigabit-Ethernet-Standard für TP-Kabel festgehalten, dass in den Netzwerkports eine Funktion namens *Auto MDI-X* (MDI = Medium Dependent Interface) implementiert sein muss. Sie verdreht die Pin-Belegung im Port automatisch, wenn entsprechende Signale ankommen. Das heißt, dass sich die Geräte durch eine Aushandlung einigen, über welchen Ethernet-Standard sie kommunizieren. In diesem Fall kann immer ein Straight-Through-Kabel verwendet werden, sodass Crossover-Kabel generell heutzutage kaum noch genutzt werden, da in den meisten Netzwerkkarten und aktiven Anschlussports Auto MDI-X verbaut ist.

Ethernet-Medientypen mit TP-Verkabelung (Kupfer)

Die Standards für Ethernet mit verschiedenen Kabeln und maximalen Datenraten werden auch als *Medientypen* bezeichnet. Es gibt zahlreiche Medientypen, einige kommen häufiger vor als andere. In den meisten Standards ist eine maximale Kabellänge pro Segment von 100 Metern festgelegt. Nachfolgend in Tabelle 2.2 finden Sie einige wichtige.

Bezeichnung	Gängiger Name	IEEE-Standard	Kabel	Bemerkung
10BASE-T	Ethernet	802.3i Clause 14	Cat-3 oder Cat-5	Verwendet zwei Adernpaare
100BASE-TX	Fast Ethernet	802.3 Clause 25	Cat 5	Verwendet zwei Adernpaare
1000BASE-T	Gigabit Ethernet	802.3 Clause 40	Cat 5 oder besser	Verwendet vier Adernpaare
10GBASE-T	10 Gigabit Ethernet	802.3an	Cat 6 oder besser	Benötigt Cat 6a/7 für volle Segmentlänge
40GBASE-T	40 Gigabit Ethernet	802.3bq	Cat 8	30 m Segmentlänge
100GBASE-T	100 Gigabit Ethernet	802.3bq	Cat 8	Sehr selten, wird auch unter 802.3bq geführt

Tabelle 2.2: Gängige Ethernet-Medientypen für Ethernet mit TP-Verkabelung

Der heute gängige Standard ist 1000BASE-T. Er ist in den meisten modernen Computernetzwerken für die Anbindung der Endgeräte verbaut. Ältere Standards haben nach heutigen Maßstäben zumindest im Unternehmensumfeld eine zu geringe Bandbreite und Standards mit höheren Übertragungsraten sind zu teuer für die Büroverkabelung. Sie kommen insgesamt seltener vor, da diese Bandbreiten in der Regel eher für Backbone-Verbindungen zwischen zentralen Netzwerkkomponenten benötigt werden und dort oft mit Glasfaser realisiert werden. Damit wären wir beim nächsten Thema.

2.1.3 Glasfaser-Standards

Neben Koaxialkabel (eher historisch) und TP-Kabel wird Glasfaser (engl. fibre oder fibre optic) für die Übertragungstechnik bei Computernetzwerken verwendet. Während die bisher beschriebenen Medien, Koaxialkabel und Twisted-Pair-Kabel, die Signale elektrisch übertragen, nutzen Glasfaser-Technologien Licht als Übertragungsmedium. Die Vorteile von Glasfaserkabeln sind vielfältig:

- Glasfaserkabel ermöglichen eine höhere Übertragungsrate als Kupferkabel.
- Glasfaserkabel können über deutlich größere Entfernungen übertragen.
- Glasfaserkabel sind unempfindlich gegen elektromagnetische Störimpulse und besser geschützt gegen Abhören des Signals.

Auf der anderen Seite sind Glasfaserkabel deutlich empfindlicher gegen mechanische Belastungen, die Gefahr eines Kabel- bzw. Faserbruchs ist hier höher. Eine weitere Herausforderung bestand lange Zeit in der Anbindung an die aktiven Netzwerkkomponenten. Dabei wurden die Kabelenden meistens »gespleißt«, sozusagen verschweißt, um die Signalübertragung zwischen der Lichtquelle (Diode) und dem Kabel unter möglichst geringen Verlusten sicherzustellen. Diese Lösung war jedoch sehr aufwendig, erforderte ein Spleißgerät und Erfahrung. Ein einfaches Umpatchen (das Kabel mit einem anderen Anschluss verbinden) war dadurch ebenfalls ausgeschlossen. Mittlerweile gibt es diverse Steckertypen für das einfache Einstecken von Glasfaserkabeln in die passende Anschlussbuchse, auf die wir etwas später zu sprechen kommen.

Aufbau eines Glasfaserkabels

Bei der Anbindung von Glasfaserkabeln ist zu berücksichtigen, dass es sich in der Regel um ein Kabelpaar handelt, da die Signalübermittlung unidirektional ist – eine Glasfaser dient zum Senden, die andere zum Empfangen.

Vorsicht

Dementsprechend muss sichergestellt sein, dass die Kabel richtig gesteckt werden. Dies ist eine häufige Fehlerquelle!

Ein Glasfaserkabel besteht aus:

1. dem **Kern** (engl. core),
2. dem **Mantel** (engl. cladding) und
3. der **Schutzbeschichtung** (engl. coating oder buffer).
4. Darüber befindet sich die **äußere Hülle** (engl. jacket).

Vergleichen Sie dazu die Abbildung 2.6.

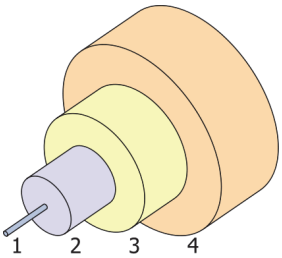


Abb. 2.6: Schematische Darstellung eines Glasfaserkabels (Quelle: Bob Mellish)

Die Signale werden über den Kern übertragen. Er besteht aus polymeren optischen Fasern. Hauptsächlich unterscheiden wir zwischen *Multimode-* und *Singlemode*-Glasfaser (engl. *single-mode fiber*). Bei der *Multimode-Faser* hat der Kern einen Durchmesser von meistens 50 m oder 62,5 m. Bei dieser Variante ist eine relativ große Streuung des Lichtsignals möglich, sodass die Übertragungsraten im Vergleich zu *Singlemode* deutlich geringer sind – der positive Aspekt sind die deutlich geringeren Kosten von *Multimode*-Glasfaser (vgl. Abbildung 2.7).

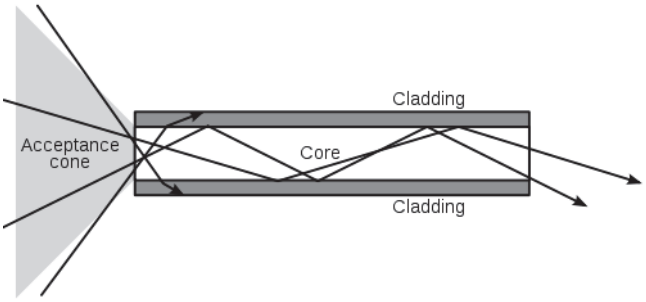


Abb. 2.7: Je nach Durchmesser ist mehr oder weniger Streuung möglich.

Singlemode-Fasern (auch: Monomode) haben einen sehr viel geringeren Durchmesser des Kerns, nämlich 3 bis 9 m. Dadurch wird das Licht mit deutlich weniger Streuung übertragen und in der Konsequenz sind deutlich höhere Übertragungsraten und größere Segmentlängen als bei Multimode möglich. Während bei Multimode LEDs oder VCSELs (bestimmte Laser) als Lichtquelle eingesetzt werden, wird bei Singlemode ein spezieller, sehr hochwertiger Laser verwendet, der das Licht senkrecht zum Querschnitt des Faserkerns einspeist und damit die Streuung minimiert.

Wie Sie es sicher schon vermuten, liegt der große Nachteil von *Singlemode* bzw. *Monomode* in den hohen Kosten. Derartige Kabel werden in der Regel von Providern nur für lange Übertragungsstrecken (WAN) eingesetzt. In Unternehmensnetzwerken kommen meistens *Multimode*-Glasfaserkabel zum Einsatz (Ausnahmen bestätigen die Regel).

Glasfaser-Kategorien

Analog zu den TP-Kabeln gibt es auch für Glasfaserkabel Kategorien mit unterschiedlichen Wellenlängen, Dämpfungen, Bandbreiten und Reichweiten. Sie werden nach IEC/ISO 11801 spezifiziert und haben Bezeichnungen wie OM1 bis OM5, OS1 und OS2. Im Gegensatz zu den TP-Kabeln, die Sie in jeglichen Farben beziehen können, sind die Farben für Glasfaserkabel festgelegt. OM1 und OM2 sind orange, OM3 aqua (hellblau), OM4 violett und OM5 lime (hellgrün). OS1 und 2 sind dagegen gelb. Wenn Sie die exakten Spezifikationen wissen möchten, können Sie sich unter `https://de.wikipedia.org/wiki/Lichtwellenleiter` detailliert informieren.

Glasfaser-Steckertypen

Im Gegensatz zu TP-Kabeln existieren diverse Steckertypen für Glasfaser-Verbindungen. Der gängigste Steckertyp für die Verkabelung in Unternehmensnetzwerken ist der *LC-Stecker* (engl. für Local Connector). Glasfaserkabel sind oft als Doppelkabel mit Duplex-Steckern oder als einzelne Kabel (simplex) erhältlich. In diesem Fall benötigen Sie zwei Kabel, da auf einem gesendet und auf dem anderen empfangen wird (vgl. Abbildung 2.8).

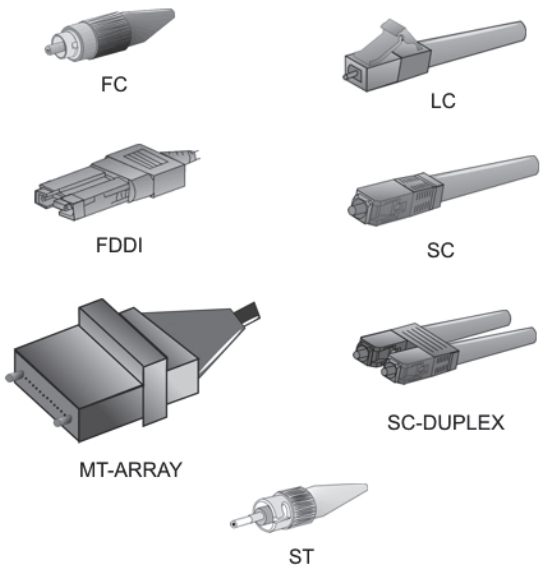


Abb. 2.8: Glasfaser-Steckertypen

Wichtig ist, dass für den jeweiligen Steckertyp und Übertragungsstandard auch eine dazu passende Anschlussbuchse am Patchfeld bzw. in der aktiven Netzwerkkomponente vorhanden sein muss. In Switches oder Routern werden dafür meist Adaptermodule (Small Factor Pluggables, SFPs) in dafür vorgesehene Slots eingesteckt. Durch Medienkonverter ist zudem ein Wechsel zwischen Glasfaser- und Kupferkabel möglich (vgl. Abbildung 2.9).

Abb. 2.9: Medienkonverter mit SFP (Von: photography taken by Christophe.Finot - Eigenes Werk, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=39936135)

Glasfaser ist nach wie vor deutlich teurer als TP-Verkabelung. Daher werden Glasfaserverbindungen genutzt, wenn es zum einen um große Datenraten geht und/oder zum anderen um große Distanzen, die es zu überbrücken gilt.

Ethernet-Medientypen mit Glasfaserverkabelung

Es gibt sehr viele Ethernet-Standards (bzw. Medientypen) für Glasfaser-Verbindungen. In Tabelle 2.3 eine Auswahl einiger wichtiger Varianten.

Bezeichnung	IEEE-Standard	Max. Segmentlänge	Beschreibung
100BASE-FX	802.3 Clause 26	400m/2000 m	Multimode, 400 m (halbduplex), 2000 m vollduplex (mit Switch)
100BASE-LX10	802.3 Clause 58	10 km	Singlemode
1000BASE-SX	802.3 Clause 38	2-5 km	Multimode
1000BASE-LX	802.3 Clause 38	5-10 km	Singlemode
10GBASE-SR	802.3ae	33-300 m	Reichweite abhängig vom Kabeltyp
10GBASE-LX4	802.3 Clause 53	240-300 m/10 km	Reichweite abhängig vom Kabeltyp
40GBASE-SR4	802.3ba	Mind. 100 m	OM3-Glasfaser Multimode
40GBASE-LR4	802.3ba	Mind. 10 km	OS2-Glasfaser Singlemode
100GBASE-SR4	802.3bm	Mind. 100 m	OM4-Glasfaser Multimode
100GBASE-LR4	802.3ba	Mind. 10 km	OS2-Glasfaser Singlemode
100GBASE-ER4	802.3bm	Mind. 40 km	OS2-Glasfaser Singlemode
400GBASE-LR8	802.3bs Clause 122	10 km	Singlemode

Tabelle 2.3: Wichtige Glasfaser-Medientypen

Auch für 800 Gbit/s wurde in **IEEE-802.3df** bereits im Jahr 2024 ein Medientyp spezifiziert und die Entwicklung geht weiter. Zudem werden Glasfaserkabel auch bei WAN-Technologien verwendet.

2.2 Ethernet-Grundlagen

Ethernet ist die kabelgebundene Vernetzungstechnologie, mit der Sie vermutlich am meisten zu tun haben. Nachdem Ethernet das Rennen um die erfolgreichste LAN-Technologie gewonnen hat, sind fast alle anderen Netzwerkvarianten für lokale Netzwerke nach und nach verschwunden, sodass Ethernet die einzig verbliebene Technologie ist, die heutzutage eingesetzt wird. Ausnahmen sind alte Produktionsnetzwerke, die seit Jahrzehnten fast unverändert laufen, aber die betrachten wir hier nicht näher. Nachfolgend lernen Sie die Grundlagen von Ethernet-Netzwerken kennen.

2.2.1 Von der Bus- zur Stern-Topologie

Bereits in Kapitel 1 » Grundlagen moderner Computernetzwerke« haben wir Ihnen die Anfänge der LAN-Verkabelung mit Ethernet vorgestellt und gezeigt, wie mit Koaxialkabeln, die Sie in diesem Kapitel noch einmal näher kennengelernt haben, eine physische Bus-Verkabelung realisiert wurde: Es wurden lange Kabel verlegt, an denen die einzelnen Geräte angeschlossen wurden. War die maximale Segmentlänge (185 Meter bei 10BASE2 bzw. 500 Meter bei 10BASE5) erreicht, wurden sogenannte *Repeater* eingesetzt, um das durch die Dämpfung abgeschwächte elektrische Signal aufzubereiten – also »aufzufrischen« – und in das nächste Segment zu leiten. Repeater haben keine weitere Logik eingebaut und arbeiten auf dem *Physical Layer*, also dem Layer 1 des OSI-Modells.

Da dieser Ansatz allerdings diverse, teilweise bereits angesprochene Nachteile mit sich brachte, wurde mit dem *Hub* als Sternverteiler eine neue Art der Verkabelung mit Stern-Topologie eingeführt. Ein Hub (engl. für Nabe) ist nichts anderes als ein *Multiport-Repeater* (vgl. Abbildung 2.10). Er hatte zwischen zwei und teilweise über 20 Ports und konnte somit als zentrale, aktive Komponente entsprechend viele Endgeräte mittels TP-Kabel anbinden. Auch eine Kaskadierung war möglich, sodass mehrere Hubs über Uplinks verbunden werden konnten und dadurch eine höhere Skalierbarkeit vorhanden war. Ein Hub arbeitet, genau wie der Repeater, auf dem Physical Layer.

Dabei ist zu berücksichtigen, dass es sich beim Hub zwar um eine physische Stern-Topologie handelt, die logische Topologie aber immer noch als Bus implementiert wurde. Um das zu verstehen, benötigen Sie etwas mehr Hintergrundwissen über die Technologie, auf der das ursprüngliche Ethernet basiert.

Abb. 2.10: Ein 8-Port-Hub mit Uplink-Port (rechts)

2.2.2 CSMA/CD

Diese Abkürzung steht für *Carrier Sense Multiple Access with Collision Detection*. Sie wurde im ursprünglichen Ethernet-Standard **IEEE 802.3** beschrieben. Nehmen wir diesen Begriff einmal auseinander, um ihn besser zu verstehen: *Carrier Sense* bedeutet, dass ein angeschlossener Knoten auf dem Carrier, also der Leitung bzw. dem Medium, lauscht und nur dann sendet, wenn er feststellt, dass das Übertragungsmedium frei ist, also kein anderer Knoten zu diesem Zeitpunkt sendet.

Hier herrscht also Konkurrenz, da nur ein Knoten gleichzeitig senden darf. Das Konzept funktioniert deswegen, weil Computer keinen endlosen Strom an Daten senden, sondern diese in PDUs, also *Packet Data Units* als abgeschlossene Einheiten in Form von Paketen bzw. eigentlich *Frames* versendet werden. Das heißt, es gibt immer wieder Zeiträume, in denen ein wartender Knoten ein Zeitfenster findet, in dem er seine eigenen PDUs auf die Reise schicken kann. Das ist in etwa vergleichbar mit dem Einfädeln auf die Autobahn, auch wenn der Vergleich etwas hinkt, weil die Signale in alle Richtungen gesendet werden, es gibt also nicht nur eine Richtung, wie z.B. bei Token Ring, wo sich ein Token immer im Kreis bewegt.

Multiple Access beschreibt die Tatsache, dass diverse Knoten an dieses Medium (das Kabel) angeschlossen sein können. Die *Collision Detection* bezieht sich auf den Fall, dass zwei Knoten zum selben Zeitpunkt feststellen, dass das Medium frei ist und beide zeitgleich senden. In diesem Fall entsteht eine Kollision. Diese wird von den Transceivern der Knoten bemerkt, die daraufhin ein sogenanntes *Jam-Signal* senden, um alle anderen Knoten über die Kollision zu informieren.

Im Falle einer Kollision warten die betreffenden Knoten für eine zufällig generierte Zeitspanne, bevor sie erneut versuchen, ihre PDUs zu versenden. Dies soll verhindern, dass die Kollision zwangsläufig erneut auftritt. Letztlich kann man sagen, dass CSMA/CD das organisierte Chaos darstellt. Dafür hat es jedoch recht gut funktioniert, auch wenn die effektive Datenübertragungsrate mit der Anzahl aktiver Knoten erheblich sinkt. Die entsprechend häufig auftretenden Kollisionen reduzieren die Effizienz eines auf CSMA/CD basierenden Ethernet-Netzwerks erheblich.

Ein Hub ist intern nichts anderes als ein einziges Medium, an dem die Knoten über TP-Kabel angeschlossen sind. Er implementiert also eine logische Bus-Topologie, auch wenn es sich physisch um einen Stern handelt. Hubs leiten die eingehenden Frames an alle anderen Ports außer dem weiter, von dem der Frame empfangen wurde. Sie enthalten keinerlei Weiterleitungslogik darüber hinaus. Dementsprechend gab es genauso viele Kollisionen wie in der physischen Bus-Topologie.

2.2.3 Bridges

Wäre es bei diesem Konzept geblieben, hätte Ethernet vermutlich nicht das Rennen um die beste LAN-Technologie gewonnen. Jedoch wurde in der nächsten Evolutionsstufe die *Bridge* eingeführt. Sie arbeitet auf dem Data Link Layer, also auf Layer 2. Eine Bridge verbindet Netzwerksegmente, die durch Hubs gebildet werden, und setzt dabei eine bestimmte Logik ein, die die Basis für heutige Ethernet-Netzwerke bildet. Dabei sammelt die Bridge die Hardware-Adressen, also MAC-Adressen, die als Absenderadresse im Ethernet-Header enthalten sind. In dieser Form baut sie eine Tabelle auf, die eine Zuordnung der MAC-Adressen der angeschlossenen Knoten zu einem der Bridge-Ports enthält (siehe Abbildung 2.11).

Oft hat eine Bridge nur zwei Ports, um zwei Segmente miteinander zu verbinden. Erhält sie einen Frame an ihrem Port 1, dessen Ziel-MAC-Adresse auf der anderen Seite am Port 2 bekannt ist, leitet sie den Frame dorthin weiter. Ist die Ziel-MAC-Adresse jedoch im selben Netzsegment, verwirft sie den Frame. In dieser Form wurde es möglich, die Last und Kollisionswahrscheinlichkeit zu reduzie-

ren, da es nicht nur ein Medium (in diesem Sinne eine *Kollisionsdomäne*) für alle Knoten gibt, sondern mindestens zwei. Das erhöhte die Effizienz von Ethernet und die Skalierbarkeit.

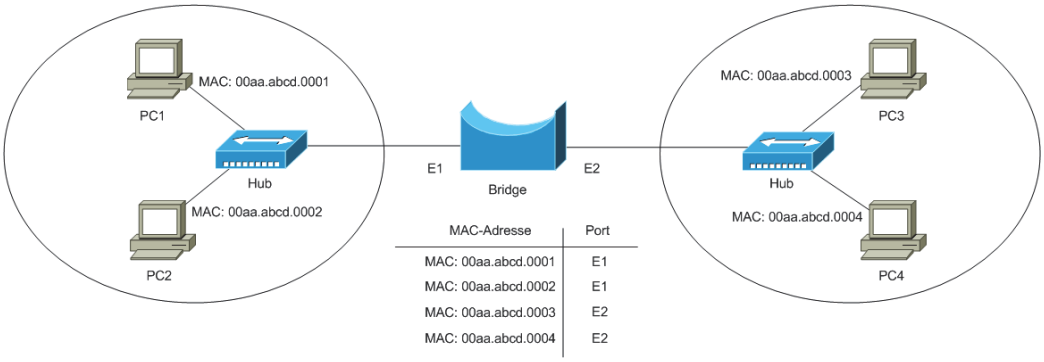


Abb. 2.11: Die Bridge führt eine MAC-Adresstabelle

Eine *Kollisionsdomäne* ist der Bereich eines Netzwerks, in dem Kollisionen durch gleichzeitiges Senden mehrerer Stationen auftreten können.

2.2.4 Switches

Verfolgt man dieses Konzept weiter, landet man fast zwangsläufig beim heutigen Switch. Ein Switch ist zunächst nichts anderes als eine *Multiport-Bridge*. Es erfolgt eine Mikrosegmentierung, sodass letztlich jeder Switchport eine eigene Kollisionsdomäne darstellt. Somit kann beim Einsatz von Switches auf Hubs verzichtet werden, da jeder Knoten direkt an den Switch angeschlossen wird.

Der Switch baut, analog zur Bridge, eine MAC-Adresstabelle auf, um jede Absender-MAC-Adresse einem seiner Ports zuzuordnen. Ein eingehender Frame wird auf seine Ziel-MAC-Adresse geprüft und der Frame nur an denjenigen Port weitergeleitet, an dem die Ziel-MAC-Adresse registriert wurde. Das macht das Weiterleitungskonzept sehr viel effizienter als das der Bridge.

Details zum Aufbau von MAC-Adressen und deren Verwendung im Zusammenhang mit der Netzwerkkommunikation erfahren Sie in Kapitel 5 »ARP und ICMP«, wenn wir über das *Address Resolution Protocol* (ARP) sprechen. An dieser Stelle nehmen Sie bitte erst mal zur Kenntnis, dass die MAC-Adressen die Grundlage der Weiterleitungslogik von Switches sind.

Switches gibt es in verschiedenen Größenordnungen, angefangen von einem Zwei-Port-Switch über gängige Home-Office-Switches mit 8 oder 12 Ports bis hin zu großen modularen Switches mit Karteneinschüben, die mehr als hundert Ports bereitstellen können. Zudem können Switches per *Stacking* miteinander verbunden werden, sodass mehrere physische Switches einen großen, logischen Switch als eine Einheit darstellen.

2.3 LAN-Switching

Der Switch ist die Grundlage moderner lokaler Netzwerke. Die Einführung von Switches war an sich bereits eine bahnbrechende Evolution, jedoch führten weitere Entwicklungen dazu, dass Ethernet alle anderen LAN-Technologien verdrängt hat. In diesem Abschnitt schauen wir uns grundlegende und erweiterte Technologien beim LAN-Switching an.

2.3.1 Grundsätzliche Funktionsweise des Switches

Knoten aller Art werden direkt am Switch angeschlossen. Dies hat zur Folge, dass Kollisionen sehr viel seltener auftreten können, da die miteinander kommunizierenden Systeme nur bei Bedarf zusammengeschaltet werden – daher das Wort »Switch« oder »Switching« (engl. switch = Schalter). Switches verbinden die Kommunikationspartner direkt während der Kommunikation – somit wird die volle Bandbreite des Mediums bereitgestellt, als ob nur zwei Knoten angeschlossen wären (vgl. Abbildung 2.12).

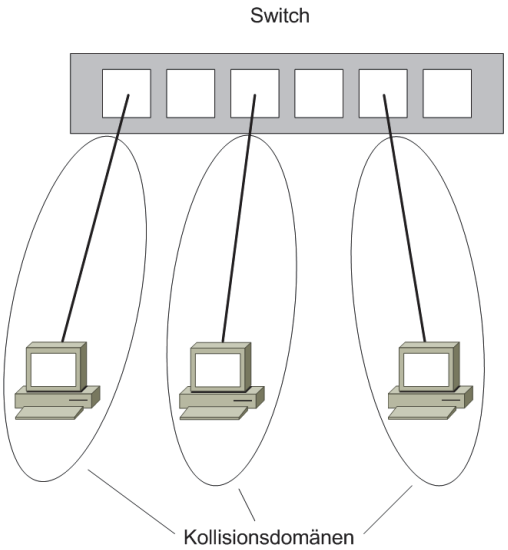


Abb. 2.12: Kollisionsdomänen sind auf ein Endgerät beschränkt.

Dafür haben Switches eine sogenannte *Backplane*, einen internen Hochgeschwindigkeitsbus, der ein Vielfaches der Bandbreite einzelner Anbindungen zur Verfügung stellt. Das ermöglicht es dem Switch, diverse angebundene Kommunikationspartner gleichzeitig mit der vollen Bandbreite zu versorgen. Höherwertige Switches haben eine stärkere Backplane, sodass mehr Systeme gleichzeitig bei voller Bandbreite kommunizieren können.

Kollisionen können nach diesem Prinzip nur noch zwischen zwei Kommunikationspartnern auftreten, die zusammengeschaltet wurden. Allerdings kann ein Switch nach wie vor auch an einen Hub angeschlossen werden. Dabei bildet der Hub eine eigene Kollisionsdomäne, wie das Beispiel in Abbildung 2.13 zeigt.