Netzwerke

Verstehen, Einrichten, Administrieren

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.

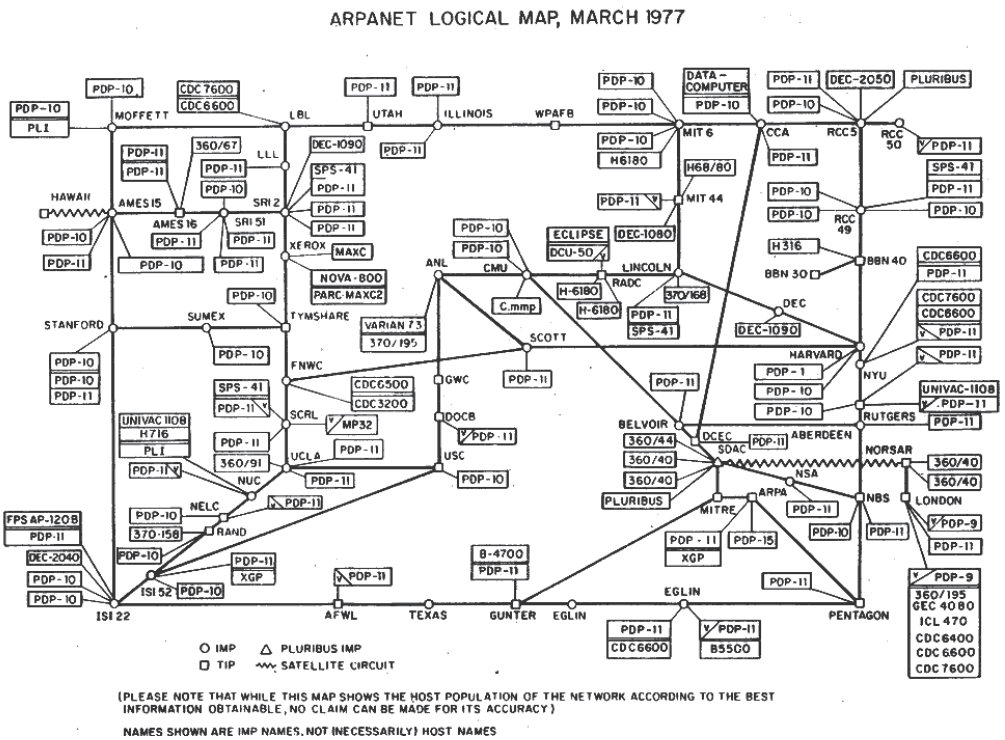

Abb. 1.1: Das ARPANET 1977 (Quelle: Wikipedia)

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).

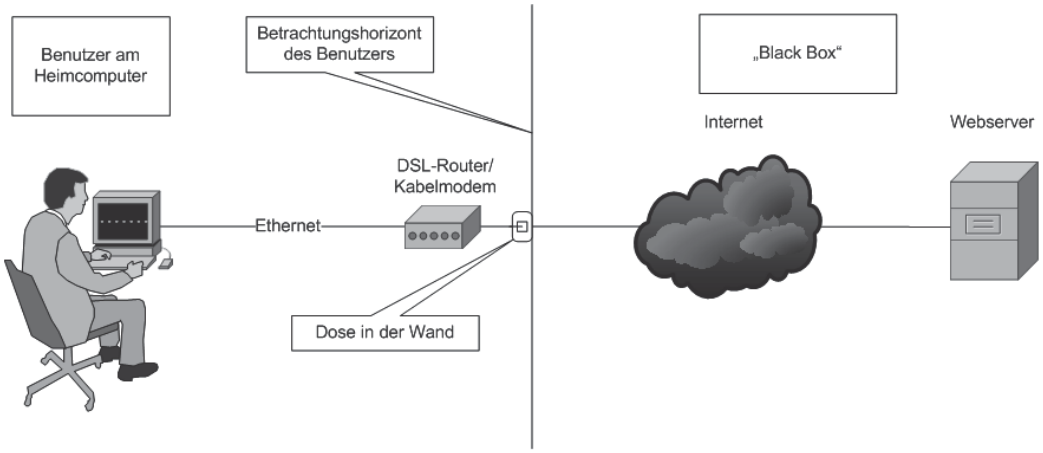

Abb. 1.2: Die Sicht des Benutzers auf das Netzwerk

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.

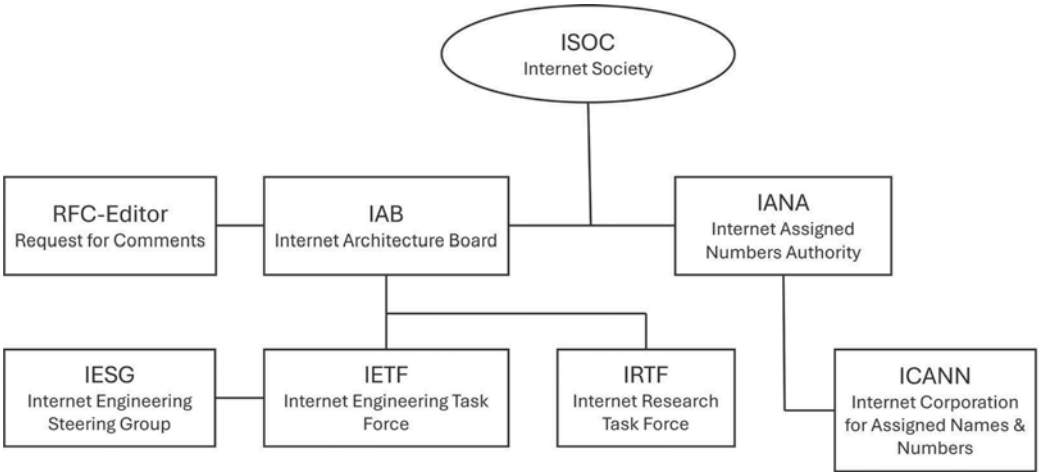

Abb. 1.3: Die ISOC und ihre untergeordneten Institutionen

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.

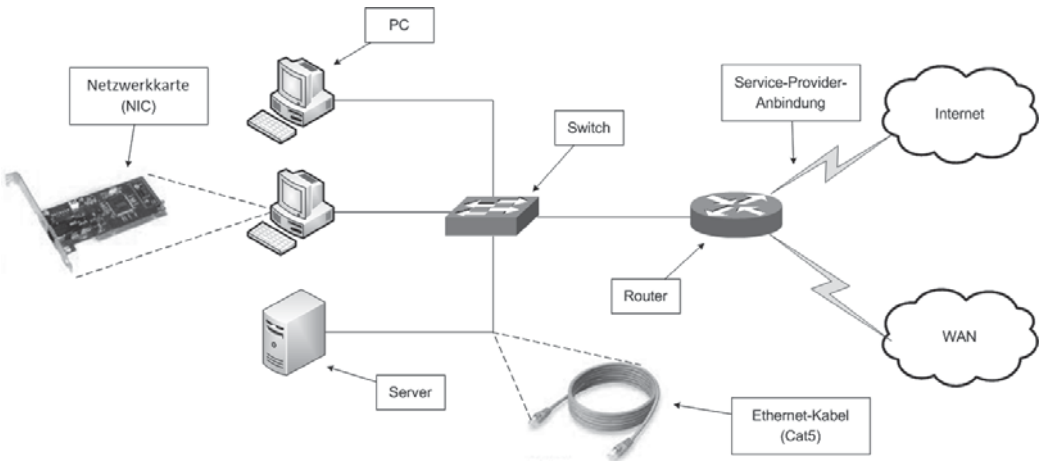

Abb. 1.4: Physische Netzwerkkomponenten

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).

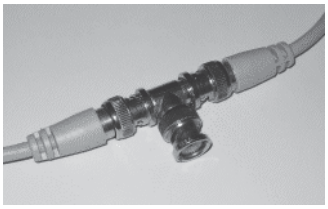

Abb. 1.5: Koaxialkabel mit BNC-Stecker und T-Stück

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

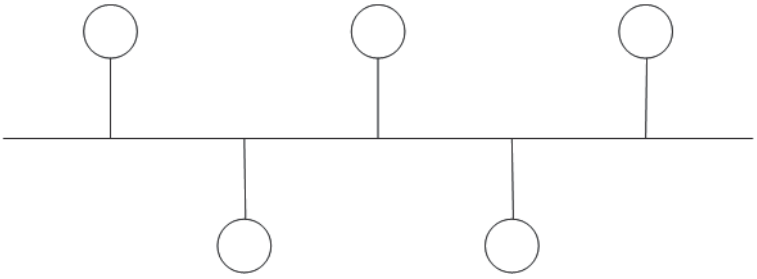

Abb. 1.6: Busverkabelung: Die Kreise stellen die Netzwerkknoten dar.

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.

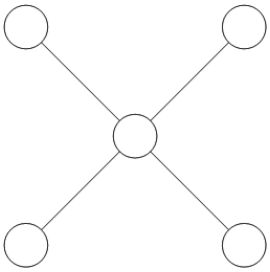

Abb. 1.7: Stern-Topologie

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.

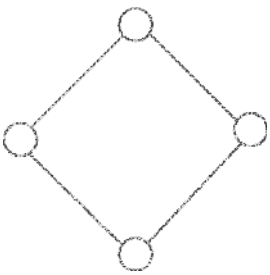

Abb. 1.8: Schematische Darstellung einer Ring-Topologie

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).

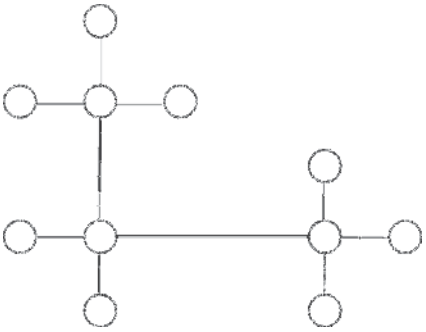

Abb. 1.10: Stern-Bus-Topologie

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).

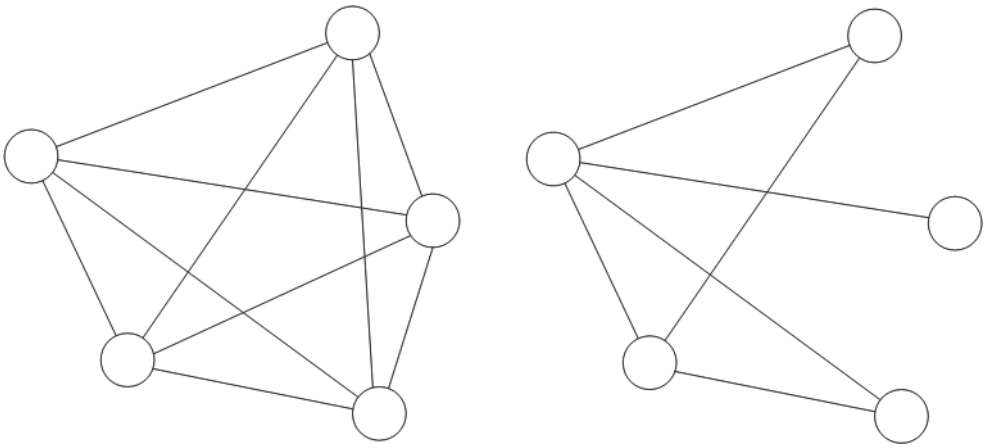

Abb. 1.11: Links ein vollvermaschtes (full meshed) und rechts teilvermaschtes (partial meshed) Netzwerk

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