
1 Eine Einführung in Netzwerke

Lokale Netzwerke (LAN) waren lange Zeit die Domäne von Großunternehmen, die Mitarbeiterarbeitsplätze, zentrale Einrichtungen und Abteilungen miteinander per Datenkommunikation verbanden. Netzwerkprofis waren Inhaber von Geheimwissen, deren Sprache Du nicht verstehst ...

Einleitung

Heutzutage ist kein modernes Unternehmen, vom Rechtsanwaltsbüro und der Arztpraxis über mittelständische Betriebe bis zum weltweiten Megakonzern mehr ohne Computernetzwerk denkbar. Was Unternehmen als über Weitverkehrsnetze miteinander verbundene Inseln zur Steuerung globaler Geschäfte nutzen, hilft dem Arzt bei der Betreuung der Patienten.

Mit der zunehmenden Popularität und Verbreitung von Computern, gerade auch angesichts des Booms des Internets, halten LANs aber auch zunehmend in Privathaushalte Einzug. Die Vorteile liegen auf der Hand: Sind Festplatten, Drucker und Internet-Zugänge zwar wie die PCs selbst ständig im Preis gesunken, kann es doch recht teuer und unpraktikabel werden, die eventuell vorhandenen Rechner der ganzen Familie mit entsprechenden Ressourcen auszustatten. Da hilft ein LAN Kosten sparen – und vereinfacht den Austausch von Daten zwischen Vater und Tochter, Sohn und Mutter ganz entscheidend. Der Verbreitung von LANs unter Endverbrauchern ist natürlich eine Tatsache sehr förderlich: Selbst die Preise für Fast Ethernet, das eine Datenrate von 100 MBit/s bietet, sind nahezu ins Bodenlose gefallen; Fast-Ethernet-Netzwerkkarten gibt es heutzutage schon für 10–15 Euro auf dem Grabbeltisch beim Computerhändler um die Ecke.

Erst durch die Vernetzung der einzelnen Computer kommen deren Stärken richtig zur Geltung. Völlig neue Anwendungsmöglichkeiten halten durch den Einsatz der Netzwerke Einzug in Arbeitsalltag und Freizeit. Der Bedarf an IT-Fachkräften, die sich mit Netzwerken auskennen, wird daher immer größer – ebenso wie die Notwendigkeit für thematisch interessierte Privatleute, sich zumindest ein fundiertes Grundwissen über LANs und Netzwerktechniken anzueignen.

Ethernet stellt aus heutiger Sicht, mit mehr als 95% Marktanteil, den Marktführer im Bereich der lokalen drahtgebundenen Netzwerke dar und wird diese Position zweifellos noch lange halten können. Durch seine Einfachheit und mit seinem dennoch genialen Konzept haben immer neue

Weiterentwicklungen zur Marktdominanz erfolgreich beigetragen. Wegen der Vielfalt der technischen Ausführungen wird von einem Netzwerkadministrator allerdings ein immer breiteres Detailwissen verlangt. Erst mit dem gezielten Einsatz der zur Aufgabenstellung passenden Technik kommt das Netzwerk richtig in Fahrt. Das vorliegende Buch soll eine detaillierte Einführung zum Thema Ethernet liefern – Profis finden alle technischen Details bis hin zu Performance-Analyse und Troubleshooting, interessierte Laien Grundlagen, um ein Netzwerk aufbauen zu können und eventuell auch einfachere Probleme selbst zu lösen.

Dieses erste Kapitel schafft die notwendigen Grundlagen, um in den nachfolgenden Kapiteln das Thema Ethernet zu vertiefen. Neben den heute langsam aussterbenden Ethernet-Varianten mit einer Datenrate von 10 MBit/s werden auch die neuen Hochgeschwindigkeitsausführungen mit 100, 1000, 10.000, 40.000 und 100.000 MBit/s detailliert durchleuchtet. Der versierte Leser kann das Grundlagenkapitel übergehen oder zur Auffrischung seiner Kenntnisse verwenden.

1.1 Erforderliche Netzwerkelemente

Netzwerkelemente

Grundsätzlich sind für den Betrieb eines Netzwerks mindestens drei Elemente erforderlich. Erstens sind immer zumindest zwei Computer notwendig, die entweder untereinander Daten austauschen möchten oder gemeinsam eine vorhandene Ressource nutzen wollen. Dies ist erst möglich, wenn zweitens ein Weg vorhanden ist, um miteinander in Kontakt treten zu können. Weiterhin muss es Regeln geben, über die festgelegt wird, wie die Computer miteinander kommunizieren können. Betrachtet man nun diese drei grundlegenden Elemente eines Netzwerks, so lassen sich diese wie folgt einteilen:

- Ein Netzwerkdienst stellt einen Service bereit, über den die gemeinsame Nutzung einer Ressource ermöglicht wird.
- Das Übertragungsmedium stellt einen Kommunikationsweg zur Kontaktaufnahme oder zum Austausch von Daten bereit.
- Netzwerkprotokolle stellen Regeln dar, die eine Kommunikation zwischen Computern ermöglichen.

Bei der Betrachtung ist es wichtig, dass man den wesentlichen Unterschied zwischen dem Kontakt- und dem Kommunikationsweg und der eigentlichen Kommunikation versteht. Denn existiert über einen Kommunikationsweg die Möglichkeit, jemanden zu kontaktieren, so heißt das noch lange nicht, dass die beiden Kommunikationspartner sich auch tatsächlich verstehen. Erst wenn man mit jemandem kommuniziert, erreicht man ein gegenseitiges Verständnis. Dies wird deutlich, wenn man sich z. B. einen Telefonanruf nach China vorstellt. Wählt man die entsprechende Nummer und der gewünschte Teilnehmer hebt das Telefon ab, so ist der Weg zur Kommunikation vorhanden. Durch den Weg alleine ist allerdings noch

keine Kommunikation sichergestellt. Erst wenn beide dieselbe Sprache sprechen, also die gleichen Regeln verwenden, kann eine Kommunikation erfolgreich zustande kommen.

1.1.1 Netzwerkdienste

Die wesentliche Aufgabe eines Computernetzwerks besteht darin, die gemeinsame Nutzung von vorhandenen Ressourcen zu ermöglichen. Werden Ressourcen anderen Netzwerkteilnehmern zu Verfügung gestellt, so spricht man von sogenannten Netzwerkdiensten oder Services. Beispielsweise können über Netzwerkdienste Ressourcen in Form von Speichermedien oder Druckern von mehreren Teilnehmern gemeinsam genutzt werden. Dabei stehen sich immer ein Server, der einen Dienst zur gemeinsamen Nutzung zur Verfügung stellt, und ein Client, der den Dienst als solches nutzt, gegenüber. Beim Anbieten und der Nutzung von Netzwerkdiensten wird prinzipiell nach folgenden Arten unterschieden:

Netzwerkdienste

- Server, die einen Netzwerkdienst zur Verfügung stellen.
- Clients, die den Netzwerkdienst anderer nutzen.
- Peers, die Netzwerkdienste einerseits zur Verfügung stellen und parallel andere Netzwerkdienste nutzen.

Diese drei Bezeichnungen werden in der Regel fälschlicherweise dazu genutzt, um die Funktion eines Computers innerhalb des Netzwerks zu beschreiben. Allerdings bezeichnet ein Netzwerkdienst primär eine Software, die auf dem Computer ausgeführt wird. So können z. B. auf einem Computer zeitgleich eine Server- und eine Client-Anwendung betrieben werden. Daher ist die Betitelung für einen Computer in Bezug auf einen Netzwerkdienst eigentlich falsch. Man stelle sich z. B. ein kleines Unternehmen vor, das drei Arbeitsplatzrechner besitzt, die gemeinsam einen Drucker verwenden, und der Drucker ist direkt an einen der drei Arbeitsplatzrechner angeschlossen. Dadurch dient dieser Arbeitsplatz den anderen Rechnern als Druckserver. Über eine Freigabe bestimmter Verzeichnisse können die Arbeitsplatzrechner auf die Datenträger der anderen Arbeitsplatzrechner zugreifen. Somit kann der Arbeitsplatzrechner mit dem angeschlossenen Drucker auch gleichzeitig einen Client darstellen. Diese Art der Aufgabenverteilung beschränkt sich in der Regel auf Netzwerke mit nur wenigen Teilnehmern. Bei größeren Netzwerken mit mehreren Teilnehmern oder höherem Ressourcenbedarf erweist sich jedoch eine klare Trennung als sinnvoll. Entsprechend der Art und Weise, wie sich die Dienste innerhalb eines Netzwerks verteilen, können Netzwerke wie folgt klassifiziert werden:

- Peer-to-Peer-Netzwerk, in dem jeder Computer Netzwerkdienste zur Verfügung stellen kann und Netzwerkdienste anderer Computer nutzen kann. Kleinere Netzwerke basieren oft auf einem Peer-to-Peer-Netzwerk, bei dem keine dedizierten Server zum Einsatz kommen.

- Client-Server-Umgebung, bei dem die Rolle der Server, also der Computer, die einen Netzwerkdienst zur Verfügung stellen, und der Clients, die diese Netzwerkdienste nutzen, klar getrennt sind. Größere Netzwerke basieren grundsätzlich auf einer Client-Server-Umgebung, da sich ausschließlich diese Konstellation ab einer bestimmten Größe noch sinnvoll administrieren lässt.

1.1.2 Übertragungsmedien

Übertragungsmedien

Damit Computer miteinander in Kontakt treten können, wird ein Kommunikationsweg zwischen ihnen benötigt. Die Bildung eines Kommunikationswegs wird über Übertragungsmedien bereitgestellt. Im Netzwerkbereich kommt der Einsatz von verschiedenen Übertragungsmedien in Frage. Welches letztendlich verwendet werden kann, ist von der Netzwerktechnologie abhängig. Grundsätzlich kommen in drahtgebundenen LANs Übertragungsmedien auf der Basis eines elektrischen Leiters, wobei man die Daten über elektrische Impulse überträgt, oder von Lichtwellenleitern, bei denen die Daten mit Lichtimpulsen übertragen werden, in Frage. Als elektrische Leiter werden entweder Koaxialkabel oder mehradrige Kabel, bei denen jeweils zwei Adern als Adernpaar ausgeführt und miteinander verdreht sind, verwendet.

- ⇒ Das Koaxialkabel hat heute im LAN-Bereich für Neuinstallationen eigentlich keine Bedeutung mehr und wird in diesem Werk nur der Vollständigkeit halber dargestellt.

Das verdrehte Kabel wird entweder in einer geschirmten Version (Shielded Twisted Pair, STP-Kabel) oder in einer ungeschirmten Version (Unshielded Twisted Pair, UTP-Kabel) eingesetzt. Bei der abgeschirmten Version des TP-Kabels unterscheidet man zudem zwischen Kabeln, die nur einen Gesamtschirm um alle Adernpaare gemeinsam aufweisen, und Kabeln, die zusätzlich eine Schirmung um die jeweiligen Adernpaare aufweisen. Erstere werden teilweise S/UTP (Shielded/Unshielded Twisted Pair) genannt, Letztere manchmal S/STP (Shielded/Screened Twisted Pair) oder auch PiMF (Paar in Metallfolie). Bei den Lichtwellenleitern kommen ebenfalls verschieden Varianten, sogenannte Multimode- oder Monomode-Lichtwellenleiter, zum Einsatz.

Verglichen werden die verschiedenen Übertragungsmedien anhand des Aufwands für die Installation, der Kosten, der erzielbaren Reichweiten, der Datenraten, die sich über die Übertragungsmedien übertragen lassen, und der Störsicherheit (elektromagnetische Verträglichkeit). Je nach vorhandener Anforderung wird ein Übertragungsmedium ausgewählt, wobei bei der Auswahl primär die erzielbare Datenrate und Reichweite berücksichtigt werden.

- ⇒ In Kapitel 8 werden wir ausführlich auf die Datenübertragung mit elektrischen und Lichtwellenleitern eingehen.

1.1.3 Netzwerkprotokolle

Über ein Netzwerkprotokoll werden Regeln festgelegt, die den Informationsaustausch zwischen Computern ermöglichen. Durch die Nutzung einheitlicher Protokolle wird sichergestellt, dass die Computer miteinander kommunizieren und sich untereinander verständigen können. Dabei kann ein Protokoll aus einer einzigen Regel oder einem Satz von Regeln oder Standards bestehen. Beispielsweise wäre zwischen Menschen keinerlei Kommunikation möglich, wenn sie über keine einheitliche Sprache und kulturelle Regeln verfügten.

Netzwerkprotokolle

⇒ Wir werden in Kapitel 11 und 12 detailliert auf die Netzwerkprotokolle eingehen.

1.2 Die Netzwerktopologien

In Abhängigkeit von den verwendeten Netzwerktechnologien werden Computer auf unterschiedlichste Art und Weise miteinander verbunden. Die verschiedenen Formen der Verbindungen werden im Fachjargon als Netzwerktopologie bezeichnet. Bei Netzwerktopologien muss man generell zwischen der physischen und der logischen Topologie unterscheiden, die durchaus voneinander abweichen können. Die physische Topologie beschreibt, wie die Computer miteinander verbunden sind. Die logische Topologie hingegen beschreibt, in welcher logischen Beziehung die Computer beim Austausch der Daten zueinander in Verbindung stehen. Wie Sie in Kapitel 2 erfahren werden, ist beispielsweise das 10-MBit-Ethernet eine Netzwerktechnologie, die in der ursprünglichen Variante ein gemeinsames Übertragungsmedium verwendet, das in der Form einer Bus-Topologie zur Verfügung gestellt wird. Über ein spezielles Verfahren wird der Zugriff für den Datenaustausch auf dem gemeinsam genutzten Bus geregelt. Wird als Übertragungsmedium ein Koaxialkabel verwendet, so werden die Computer physisch über das Koaxialkabel, das den Bus darstellt, miteinander verbunden. Verwendet man als Übertragungsmedium ein verdrehtes Kupferkabel, so werden die Computer über einen Verteiler, der als Hub bezeichnet wird, sternförmig miteinander verbunden. Intern stellt der Hub ebenfalls einen Bus dar, bei dem über dasselbe Zugriffsverfahren die Daten auf das Netzwerk gebracht werden. Logisch betrachtet basiert das Ethernet in beiden Fällen immer auf einer Bus-Topologie, wogegen – physisch betrachtet – im ersten Fall eine Bus- und im zweiten Fall eine Stern-Topologie vorliegt.

Netzwerktopologien

*Physische und
logische Topologie*

Man unterscheidet bei den Netzwerktopologien zwischen der Bus-Topologie, der Ring-Topologie, der Stern-Topologie, der Maschen-Topologie und gemischten Topologien. Je nach verwendeter Netzwerktechnologie kommen von den vier genannten Netzwerktopologien logische und physische Topologien zum Einsatz. Die logische Netzwerktopologie ist grundsätzlich von der Netzwerktechnologie abhängig und kann innerhalb

*Verschiedene
Netzwerktopologien*

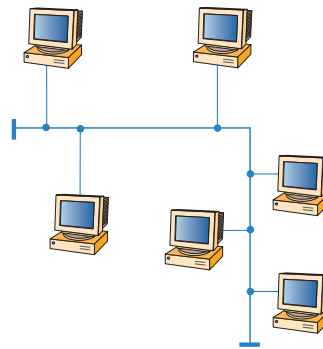
dieser prinzipiell weder geändert noch ausgewählt werden. Bei der physischen Betrachtung der verschiedenen Netzwerktopologien werden in erster Linie der Aufwand bei der Installation, bei einer eventuellen Rekonfiguration, bei einer Fehlersuche und die Anzahl der Komponenten beziehungsweise beteiligten Station, die von einem möglichen Fehler betroffen sind, betrachtet. Hier können unter Umständen innerhalb einer Netzwerktechnologie zwischen verschiedenen Netzwerktopologien die Vor- und Nachteile ausgewogen und, je nach Bedarf, eine Topologie ausgewählt werden. Um die Vor- und Nachteile der verschiedenen Netzwerktopologien vergleichen zu können, möchten wir im Folgenden auf die verschiedenen Netzwerktopologien eingehen.

Bus-Topologie

Bei der physischen Bus-Topologie wird ein Übertragungsmedium durch mehrere Teilnehmer gemeinsam verwendet. Die Verbindungswege zwischen den einzelnen Komponenten beziehungsweise Stationen sind dabei relativ kurz, da das Übertragungsmedium direkt ohne Umwege von Komponente zu Komponente verlegt werden kann (siehe Abb. 1–1).

Abb. 1–1

Die Bus-Topologie



Die beiden Enden des Bus werden mit einem Widerstand abgeschlossen, damit keine Reflexionen der elektrischen Signale auftreten können. Reflexionen sind in diesem Fall ein Teil des elektrischen Signals, der bei einem offenen oder falsch abgeschlossenen Ende (fehlender oder falscher Abschlusswiderstand) zurückgeworfen beziehungsweise reflektiert wird. Durch die Reflexion findet eine Überlagerung der elektrischen Signale statt, die die Datenübertragung auf dem Bus nachhaltig stört. Werden Daten von einem Computer ausgesendet, so breiten sich diese Daten in beide Richtungen des Bus aus. Der Vorteil der Bus-Topologie liegt darin, dass der Bus auf einfachste Weise nach Bedarf erweitert werden kann – vorausgesetzt, die maximale Ausdehnung ist noch nicht erreicht. Problematisch ist jedoch, dass die Erweiterung des Bus in der Regel nicht während des Netzwerkbetriebs durchgeführt werden kann, da der Bus für eine Erweiterung an mindestens einer Stelle kurzzeitig aufgetrennt werden muss. Der größte Nachteil liegt jedoch darin, dass der Bus aufgrund der vielen Verbindungsstellen sehr fehleranfällig ist und sich die Fehlersuche in

der Regel als aufwändig herausstellt. Typischerweise sind alle Komponenten oder Stationen von einem möglichen Fehler betroffen. Tritt ein Kabelbruch auf oder löst sich eine Verbindung, so zerlegt sich der Bus in zwei Teilnetzwerke, deren Kommunikation mehr oder weniger nur noch bedingt innerhalb des Teilnetzes stattfinden kann. Die Kommunikation ist innerhalb der Teilnetze gestört, da an den Bus-Enden die Abschlusswiderstände fehlen und es somit zwangsläufig zu Reflexionen kommen wird.

Bei der Ring-Topologie werden die Computer quasi in Reihe geschaltet, und der letzte Computer wird wieder mit dem ersten Computer verbunden. Auf diese Weise entsteht eine ringförmige Verbindung zwischen den Computern (siehe Abb. 1–2). Da der Ring vom letzten Computer wieder mit dem ersten Computer verbunden werden muss, benötigt man für die Bildung der Ring-Topologie zwangsläufig ein längeres Datenkabel als bei der Bus-Topologie. Durch die ringförmige Verbindung ergibt sich ein ununterbrochener Datenpfad, über den die Daten in eine Richtung übertragen werden und jeden Computer erreichen können. Nachteilig ist bei der Ring-Topologie, dass der Ring relativ fehleranfällig ist. Wird der Ring an einer Stelle unterbrochen, so ist die gesamte Kommunikation innerhalb des Netzwerks gestört. Vorteilhaft bei der Ring-Topologie ist die relativ einfache Fehlersuche: Man muss bei einem Fehler nur die Station ausfindig machen, die keine Daten mehr empfängt. Bedingt durch die Tatsache, dass die Daten immer nur aus einer Richtung kommen können, lässt sich der Fehler zwischen der Station, die keine Daten empfängt, und der benachbarten Station, die normalerweise die Daten senden müsste, festmachen. Möchte man den Ring erweitern, so ist dies nicht während des Netzwerkbetriebs möglich, da der Ring an mindestens einer Stelle aufgetrennt werden muss.

Ring-Topologie

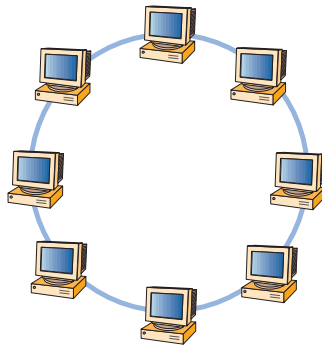


Abb. 1–2

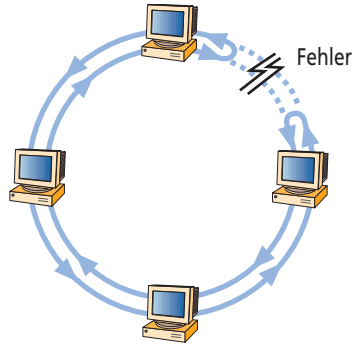
Die Ring-Topologie

Es gibt Ring-Topologien, bei denen der Ring doppelt ausgeführt ist, wie es beispielsweise bei der Netzwerktechnologie FDDI (Fibre Distributed Data Interface) der Fall war. Der doppelte Ring dient in diesem Fall als redundanter Weg, der dazu dienen kann, dass sich der Ring in einem Fehlerfall über den redundanten Weg wieder schließt. Auf diese Weise wird verhin-

dert, dass der Ring bereits bei einem Fehlerfall in Teilstücke zerfällt; dies geschieht so erst ab dem zweiten Fehlerfall oder wenn bei einem Fehler beide Ringe durchtrennt werden (siehe Abb. 1–3).

Abb. 1–3

*Der redundante Weg
bei doppelter Ring-
Ausführung*

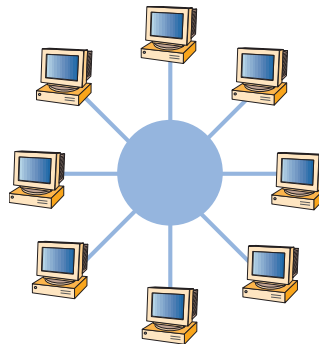


Stern-Topologie

Bei der Stern-Topologie werden die Computer sternförmig über einen zentralen Verteiler miteinander verbunden. Die Stern-Topologie kommt heutzutage bei Netzwerken vorwiegend zum Einsatz und bildet die Basis einer sogenannten Strukturierten Verkabelung (bestimmte Form einer modernen Verkabelung). Die Stern-Topologie erscheint zwar auf den ersten Blick von der Verkabelung her als sehr aufwändig, bietet jedoch den Vorteil, dass sich Störungen, beispielsweise in der Form eines Kabelbruchs, direkt nur auf einen Datenpfad und somit in der Regel auf einen Computer auswirken. Dadurch wird in der Gesamtbetrachtung ein relativ sicherer Datenaustausch innerhalb des Netzwerks gewährleistet und die Fehlersuche sehr einfach (siehe Abb. 1–4).

Abb. 1–4

Die Stern-Topologie



Der Installationsaufwand bei der Stern-Topologie ist, bedingt durch den geringen Planungsaufwand, ebenfalls relativ gering. Jedoch wird bei der Stern-Topologie sehr viel Datenkabel benötigt, da vom zentralen Verteiler zu jedem Computer eine eigene Datenleitung verlegt werden muss. Eine Erweiterung des Netzwerks kann jedoch ohne Probleme während des

Betriebs vorgenommen werden, da bei der Stern-Topologie kein Datenpfad des Netzwerks aufgetrennt werden muss. Man kann demnach bei der Stern-Topologie von einer Hot-Plugging-Funktion sprechen, da eine Erweiterung während des Netzwerkbetriebs problemlos möglich ist.

- ⇒ Die Stern-Topologie ist die heute am weitesten verbreitete Netzwerktopologie, die innerhalb moderner Netzwerktechnologien oder einer Strukturierten Verkabelung zum Einsatz kommt. Man spricht bei der Stern-Topologie auch oft von der Baum-Topologie, da sie der Struktur einer Strukturierten Verkabelung am meisten ähnelt.

Innerhalb einer Maschen-Topologie hat jeder Computer eine Punkt-zu-Punkt-Verbindung zu jedem anderen Computer des Netzwerks. Theoretisch benötigt demnach jeder Computer so viele Netzwerkanschlüsse wie er benachbarte Computer innerhalb des Netzwerks hat. Demnach ist die Maschen-Topologie als physische Netzwerk-Topologie nicht praktikabel und kommt nur als logische Topologie in Betracht. Die Maschen-Topologie ist allerdings eine sehr fehlertolerante Netzwerktopologie, wobei jedoch bedingt durch die große Anzahl von Punkt-zu-Punkt-Verbindungen und die Tatsache, dass die Daten nicht zu allen Computern übertragen werden, eine relativ hohe Bandbreitenverschwendung vorliegt. Der Aufwand für die Installation oder eine Erweiterung ist generell sehr hoch. Dasselbe gilt für eine Rekonfiguration, die sich durch die Vielzahl der Punkt-zu-Punkt-Verbindungen als schwierig erweist. Die Fehlersuche ist einfach, da jede Verbindung unabhängig von jeder anderen ist und sich Fehler demnach leicht einkreisen lassen. Durch die große Anzahl der Punkt-zu-Punkt-Verbindungen entstehen viele Verbindungen zwischen den einzelnen Computern innerhalb einer Maschen-Topologie. Demnach liegt bei einer Maschen-Topologie eine geringe Fehleranfälligkeit vor, die sich in der Form bemerkbar macht, dass bei einer Störung maximal ein Computer betroffen ist.

Maschen-Topologie

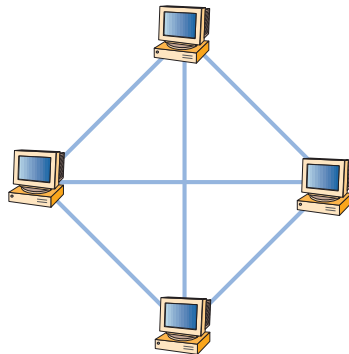


Abb. 1-5

Die Maschen-Topologie

- ⇒ Die Maschen-Topologie findet, bedingt durch die Punkt-zu-Punkt-Verbindung, vorwiegend als logische Topologie zwischen Routern Einsatz.

1.3 Einteilung der Netzwerke

Sobald zwei Computer mit Netzwerkkarten und entsprechender Software ausgestattet sowie über ein geeignetes Verbindungskabel miteinander verbunden sind, spricht man bereits von einem Netzwerk. Diese Form stellt natürlich die einfachste Form eines Netzwerks dar und kommt heutzutage vorwiegend im privaten Bereich vor. Innerhalb eines Unternehmens werden in der Regel mehrere Computer, deren Anzahl schnell auf 100, 1000 oder mehr ansteigen kann, über ein Netzwerk miteinander verbunden. Unabhängig von der Anzahl der vernetzten Computer findet der Datenaustausch nach denselben Grundprinzipien statt, natürlich vorausgesetzt, dass man sich bei der Betrachtung auf eine Netzwerktechnologie beschränkt.

Grundsätzlich werden die Netzwerke per Definition in Abhängigkeit von ihrer Ausdehnung in vier Gruppen, das Local Area Network (LAN), das Metropolitan Area Network (MAN), das Wide Area Network (WAN) und das Global Area Network (GAN), unterteilt.

LAN Die räumliche Ausdehnung eines LAN ist begrenzt, wobei sich seine zulässige Ausdehnung letztendlich durch die verwendete Netzwerktechnologie ergibt. Dabei können die Übertragungsgeschwindigkeit und die erzielbare Reichweite in einer Wechselbeziehung stehen. Je höher die Übertragungsgeschwindigkeit, umso niedriger ist die Reichweite, die bei den zur Verfügung stehenden Netzwerktechnologien erzielt werden kann. Ein LAN erstreckt sich in der Regel über ein Gebäude oder ein Firmengelände, wobei die Abgrenzung des LAN eher technisch geprägt ist und die genaue Abgrenzung per Definition letztendlich Sache des Betreibers ist. Bedingt durch die Tatsache, dass heute in der Regel mehrere Netzwerke beispielsweise über das Internet miteinander verbunden werden, wird die Klassifizierung eines Netzwerks als ein LAN immer schwieriger. Bei einem LAN kommen, je nach Übertragungsdistanz, verschiedene Übertragungsmedien zum Einsatz. Heutzutage typische und weitverbreitete Netzwerktechnologien für den LAN-Bereich sind Ethernet und Wireless LAN (WLAN).

MAN Bei dem MAN spricht man von Netzwerken, die sich von ihrer Ausdehnung her über den Bereich einer Stadt oder eines Ballungsgebiets erstrecken. Als Übertragungsmedium kommen bei einem MAN vorwiegend Lichtwellenleiter zum Einsatz, die die Datenübertragung über größere Distanzen erlauben.

WAN Das WAN erstreckt sich im Vergleich zum LAN über eine größere Entfernung, wobei sich die Entfernung über mehrere Städte ausdehnen kann. Das WAN stellt ein Verbindungsnetzwerk dar, über das mehrere Netzwerke zwecks Datenaustausch verbunden werden können. Die Ausdehnung eines WANs liegt in etwa in der Größenordnung von bis zu 1000 km. Die WANs basieren auf verschiedenen Technologien, wobei beispielsweise ATM als klassische WAN-Technologie angesehen werden kann.

GAN Das GAN unterliegt von der räumlichen Ausdehnung her praktisch keiner Begrenzung. Bei einem GAN kommen heutzutage als Übertragungs-

medium Datenkanäle zum Einsatz, die über Satelliten oder beispielsweise Unterseekabel bereitgestellt werden, weshalb das GAN theoretisch keiner Begrenzung unterliegt und sich um den gesamten Erdball erstrecken kann.

1.4 Die Netzwerktechnologien

Wollte man in der Vergangenheit zwei oder mehrere Computer in der Form miteinander verbinden, dass über ein Kabel ein Datenaustausch zwischen den Computern ermöglicht wurde, so waren neben Ethernet verschiedene Netzwerktechnologien dafür geeignet. Technologische Mitstreiter waren einst Token Ring, Fibre Distributed Data Interface (FDDI) oder Asynchronous Transfer Mode (ATM). Ethernet stellt unter diesen verschiedenartigen Möglichkeiten die heute am weitesten verbreitete Netzwerktechnologie dar, die sich als die LAN-Technologie durchgesetzt hat. Auch wenn alle Mitstreiter heute keine Bedeutung mehr haben, werden sie nachfolgend kurz betrachtet und ihre technischen Eckdaten dargestellt.

Netzwerktechnologien

Jede der genannten Netzwerktechnologien arbeitete in der Detailbetrachtung unterschiedlich; wollte man den Datenaustausch zwischen Netzwerken auf unterschiedlichen Netzwerktechnologien ermöglichen, so musste eine Anpassung zwischen den verschiedenen Netzwerken durchgeführt werden. Dazu konnte man sich beispielsweise Geräten wie Bridges oder Routern bedienen, über die der Datenaustausch zwischen den verschiedenen Netzwerken ermöglicht wurde.

Ethernet wurde 1983 vom Institute of Electrical and Electronics Engineers (IEEE) als Standard IEEE 802.3 definiert. Die erste Version des Ethernet arbeitete mit einer Datenrate von 10 MBit/s und nutzte als Übertragungsmedium ein Koaxialkabel. Das Koaxialkabel stellte dabei einen Daten-Bus dar, auf den alle angeschlossenen Computer für die Datenübertragung gleichberechtigt zugreifen konnten. Bis heute hat sich das Ethernet stark weiterentwickelt, wodurch Datenraten von 10, 100, 1000, 10.000, 40.000 oder 100.000 MBit/s möglich sind und eine Vielzahl von Übertragungsmedien unterstützt werden. Bei den Datenraten von 10, 100 und 1000 MBit/s wird im Halbduplexbetrieb als Zugriffsverfahren Carrier Sense Multiple Access with Collision Detection (CSMA/CD) verwendet (siehe Kap. 2).

Ethernet

Token Ring wurde 1985 von IBM vorgestellt und später durch den Standard IEEE 802.5 definiert. Token Ring arbeitet mit einer Basisband-Übertragungstechnik und ist ein Ringnetzwerk, in dem die Computer logisch zu einem Ring vernetzt sind. Als Zugriffsverfahren wird ein Token-Passing-Verfahren verwendet. Das Token Ring arbeitet mit einer Datenrate von 4 oder 16 MBit/s. War Token Ring in den neunziger Jahren vornehmlich im Bankenbereich etabliert, so hat es heute keinerlei Bedeutung mehr. Token-Ring-Produkte sind heute praktisch nicht mehr erhältlich.

Token Ring

Das Fibre Distributed Data Interface (FDDI) ist eine 100-MBit-Netzwerktechnologie, die speziell für Lichtwellenleiter konzipiert und deren

FDDI

Spezifikation 1989 verabschiedet wurde. Die Spezifikation basierte auf einem Vorschlag des American National Standard Institute (ANSI) und wurde von der International Organization for Standardization (ISO) normiert. Später wurde das FDDI auch für die Nutzung anderer Medien wie das STP- oder UTP-Kabel erweitert und dann auch als Copper Distributed Data Interface (CDDI) bezeichnet. FDDI nutzt wie Token Ring als Zugriffsverfahren Token Passing. Auch wenn viele Faktoren, wie beispielsweise die Fehlerredundanz, das integrierte Netzwerkmanagement, die zur damaligen Zeit verhältnismäßig hohe Bandbreite und die mögliche große Ausdehnung für FDDI sprachen, hat sich das FDDI wegen der relativ hohen Kosten und der Konkurrenz durch Ethernet nicht durchgesetzt.

ATM

Asynchronous Transfer Mode (ATM) ist für große Netze im LAN- oder WAN-Bereich konzipiert. ATM arbeitet mit relativ kleinen Datenpaketen, die eine einheitliche Länge von 53 Byte aufweisen und als Zellen bezeichnet werden. ATM unterstützt Datenraten von 25 MBit/s, 155 MBit/s, 622 MBit/s oder 1,2 GBit/s. Die Technologie arbeitet als schnelle, vereinfachte Paketvermittlung, wobei die Übertragung der Pakete über virtuelle Kanäle erfolgt. Ein virtueller Kanal wird auf Pfade nach Bedarf zwischen den Netzknoten über Switches geschaltet. Beim Verbindungsaufbau werden eine Dienstklasse sowie die Bandbreite zwischen dem Endgerät und dem Dienstanbieter vereinbart, die zusammen die Breite des virtuellen Kanals ergeben. Die Bandbreite eines virtuellen Kanals kann, je nach Bedarf, vergrößert oder verkleinert werden. ATM ist vom Ursprung her eine Technologie für Telekommunikationsnetze. Im Netzwerkbereich wird ATM mit einer sogenannten LAN-Emulation betrieben, damit sich ATM für die Anwendungen wie ein Ethernet- oder Token-Ring-Netzwerk verhält. ATM hat sich, bedingt durch seine Komplexität und die hohen Kosten, im Bereich der lokalen Netzwerke nicht durchgesetzt. Im Bereich der Weitverkehrsnetzwerke sieht die Situation etwas anders aus. Hier setzen alle großen Carrier häufig ATM ein, um beispielsweise Firmenverbindungen über größere Distanzen zu realisieren. Jedoch setzen heute immer weniger Carrier ATM ein und planen stattdessen, ATM durch 10Gigabit-Ethernet zu ersetzen.

1.5 Die Sprache der Computer

Informationsaustausch

Die Sprache der Computer basiert im Grunde auf dem Austausch von zwei logischen Zuständen, nämlich einer Eins und einer Null. Die kleinste Informationseinheit wird dabei als Bit bezeichnet, die entweder den Wert Eins oder den Wert Null annehmen kann. Eine Gruppe von acht Bits bezeichnet man heutzutage als Byte. Ein Byte kann, basierend auf der Tatsache, dass jedes Bit eines Bytes zwei Zustände annehmen kann, $2^8 = 256$ verschiedene Zustände repräsentieren. In der Regel wird die Eins durch einen vorhandenen Spannungspegel mit einem bestimmten Wert und eine Null durch einen Spannungspegel von 0 V signalisiert. Unabhängig davon,

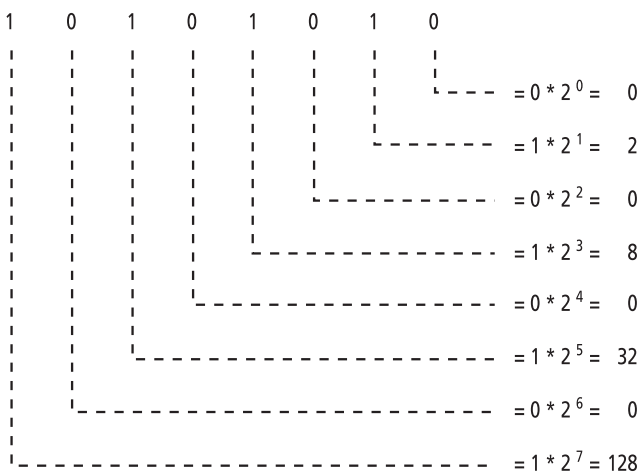
ob man direkt im Computer oder auf einer Leitung im Netzwerk den fließenden Datenstrom beobachten würde, so würde sich dieser durch den Wechsel zwischen logischen Einsen und logischen Nullen darstellen.

Normale Menschen sind es allerdings gewohnt, mit dem dezimalen Zahlensystem zu arbeiten. Darin gibt es 10 verschiedene Ziffern von 0 bis 9, über die sich 10 verschiedene Zustände darstellen lassen. Im dezimale Zahlensystem setzt sich aus Zahlen mit der Basis 10 zusammen: Die erste Ziffer einer Zahl wird mit dem Wert $10^0 = 1$, die zweite Ziffer mit dem Wert $10^1 = 10$ und die dritte Ziffer mit dem Wert $10^2 = 100$ usw. multipliziert. Der Unterschied zwischen dem Stellenwert der einzelnen Ziffern beläuft sich demnach immer auf den Faktor 10. Die erste Ziffer gibt den Wertebereich von 0 bis 9 an, die zweite Ziffer ergänzt den Wertebereich von 10 bis 99 usw. Die Zahl 387 ergibt sich beispielsweise aus

$$3 \times 10^2 + 8 \times 10^1 + 7 \times 10^0 = 3 \times 100 + 8 \times 10 + 7 \times 1 = 387.$$

Betrachtet man hingegen das Zahlensystem eines Computers, so basiert dieses auf nur zwei möglichen Zuständen, wonach man hierbei also mit einer Basis von 2 arbeitet. Dieses Zahlensystem bezeichnet man als binäres Zahlensystem, da jede Informationseinheit (Bit) zwei Zustände annehmen kann. Innerhalb eines Bytes, also acht Bits, hat das erste Bit die Wertigkeit von $2^0 = 1$, das zweite Bit die Wertigkeit von $2^1 = 2$, das dritte Bit die Wertigkeit von $2^2 = 4$ – bis zum achten Bit, das die Wertigkeit von $2^7 = 128$ hat. Bedingt durch diese Zuordnung spricht man vorzugsweise von Bit 0 bis Bit 7. Je nach Kombination der logischen Zustände von Bit 0 bis Bit 7 eines Bytes kann so ein Byte 256 verschiedene Zustände von 0 bis 255 annehmen. Wie in Abbildung 1–6 dargestellt entspricht die Bitfolge von 10101010 zum Beispiel

$$1 \times 2^7 + 0 \times 2^6 + 1 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0 = 170$$



Dezimalen Zahlensystem

Binäres Zahlensystem

Abb. 1–6

Die Zuordnung und Wertigkeit der Bits innerhalb eines Bytes

Durch jedes weitere Bit wird der mögliche Wertebereich des binären Zahlensystems verdoppelt (im dezimalen Zahlensystem bewirkt jede Stelle eine Verzehnfachung des Wertebereichs).

Tab. 1-1

Jedes Bit führt zu einer Verdoppelung des Wertebereichs.

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

Hexadezimalen Zahlensystem

Vorzugsweise arbeiten jedoch die EDV-Fachleute anstelle des binären mit dem hexadezimalen Zahlensystem. Das hexadezimale Zahlensystem arbeitet mit einer Basis von 16, wobei man für die 16 Ziffern die 0 bis 9 und die Buchstaben A bis F (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F) verwendet. Im EDV-Bereich wurde das hexadezimale Zahlensystem eingeführt, um die Darstellung der Bits innerhalb eines Bytes zu vereinfachen. Dabei wird ein Byte in zwei Teile von jeweils vier Bit aufgeteilt, die als Nibble bezeichnet werden (to nibble = anknabbern). Die 256 möglichen Zustände eines Bytes lassen sich somit durch zwei hexadezimale Zahlen ($16 \times 16 = 256$) darstellen, wobei die ersten vier Bits durch die erste hexadezimale Zahl und die weiteren vier Bits durch die zweite hexadezimale Zahl repräsentiert werden. Betrachtet man Tabelle 1-2, so kann man die Zuordnung der binären Zahlen und der hexadezimalen Zahlen von 0 bis F entnehmen.

Tab. 1-2

Die Zuordnung zwischen hexadezimalen Zahlen und binären Zahlen

Hex-Zahl	binäre Zahl	Hex-Zahl	binäre Zahl
0	0000	8	1000
1	0001	9	1001
2	0010	A	1010
3	0011	B	1011
4	0100	C	1100
5	0101	D	1101
6	0110	E	1110
7	0111	F	1111

Merkt man sich diese Zuordnung, so kann man relativ einfach die hexadezimale Zahl in die binäre Zahl und somit in das tatsächliche Bitmuster umwandeln. So entspricht beispielsweise der Hex-Wert von 0xAA der binären Zahl oder dem Bitmuster von 1010 1010. Würde man vergleichsweise versuchen, die entsprechende Dezimalzahl von 170 (0xAA) in das Bitmuster umzuwandeln, so ist dies erkennbar schwieriger.

⇒ In diesem Buch werden wir oft die hexadezimale Darstellung verwenden, die durch das vorgesetzte 0x erkennbar ist.

Betrachtet man nun typische Informationen wie beispielsweise einen Text, die in einem Computer verarbeitet werden, so muss eine logische Beziehung zwischen den möglichen Zuständen des in Computern verwendeten Zahlensystems und den uns bekannten Zeichen existieren. Dies wird durch den sogenannten American Standard Code for Information Interchange (ASCII-Code) realisiert. Der ASCII-Code weist jedem großen und kleinen Buchstaben des Alphabets, jedem Satzzeichen, jeder Ziffer und bestimmten Steuerzeichen einen bestimmten Wert zu. So entspricht zum Beispiel der Wert 65 (0100 0001) dem Großbuchstaben A und der Wert 97 (0110 0001) dem Kleinbuchstaben a. Auf diese Weise lassen sich alle uns bekannten Zeichen innerhalb eines Computers verarbeiten und über ein Netzwerk übertragen, indem die Informationen letztendlich ausschließlich in den zwei logischen Zuständen Null oder Eins codiert werden.

1.5.1 Die Datenübertragung

Grundsätzlich kommt für die Kommunikation eine parallele oder eine serielle Datenübertragung in Frage. Bei der parallelen Datenübertragung ist, neben ein paar Leitungen für bestimmte Steuersignale, für jedes Datenbit eine eigene Datenleitung vorhanden. Der Drucker, der direkt über die parallele Schnittstelle an einen Computer angeschlossen wird, ist ein klassisches Beispiel für eine parallele Datenübertragung. Bei dieser Methode kann so pro Zeiteinheit ein gesamtes Datenbyte übertragen werden. Nachteilig bei der parallelen Datenübertragung ist es, dass man für den Datenaustausch relativ viele Leitungen benötigt, was sich bei großen Distanzen als sehr kostspielig und aufwändig erweist (siehe Abb. 1–7).

*Parallele
Datenübertragung*

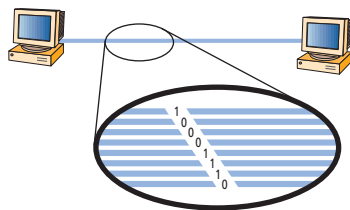


Abb. 1–7
*Die parallele
Datenübertragung*

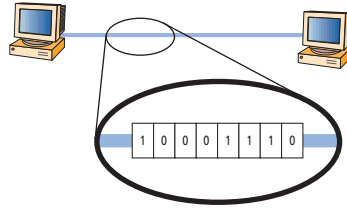
Eine Alternative zu der parallelen stellt die serielle Datenübertragung dar, bei der auf einer Datenleitung die Bits nacheinander übertragen werden. Für den Transfer eines Bytes werden demnach acht Zeiteinheiten benötigt. Die serielle Datenübertragung arbeitet deshalb mit niedrigen Zeiteinheiten, um die Dauer für die Übertragung eines Bytes zu verringern. Geht es darum, Daten über eine größere Distanz zu übertragen, so wird bevorzugt die serielle Datenübertragung angewendet, da diese im Minimalfall mit einer einzigen Datenleitung auskommt. In einem Netzwerk arbeitet man

*Serielle
Datenübertragung*

demnach grundsätzlich über eine serielle Verbindung, da es hierbei um die Datenübertragung über größere Distanzen geht (siehe Abb. 1–8).

Abb. 1–8

Die serielle
Datenübertragung



1.5.2 Asynchrone und synchrone Datenübertragung

Asynchrone
Datenübertragung

Um Daten aus einem Bitstrom gewinnen zu können, muss der eingehende Datenstrom über ein gewisses Zeitfenster abgetastet werden. Das dafür notwendige Zeitfenster wird über eine Taktquelle gewonnen. Man unterscheidet in der Nachrichtentechnik zwischen einer asynchronen und einer synchronen Datenübertragung. Bei der asynchronen Datenübertragung verwenden die Kommunikationspartner voneinander unabhängige Taktquellen. Werden Daten übertragen, so wird vor die Daten ein Startbit gesetzt, wodurch die Taktquelle auf der Seite des Empfängers gestartet wird. Nach dem Aussenden der Daten folgt ein Stopbit, mit dem die Datenübertragung beendet ist. Der Vorteil der asynchronen Datenübertragung liegt darin, dass keine Synchronisierung der Taktquellen benötigt wird und die Implementierung relativ einfach ist. Der Nachteil liegt darin, dass die Taktquellen voneinander abweichen können, weshalb die Größe der zu übertragenden Dateneinheiten nur relativ klein sein kann. Außerdem muss zu den Daten ein Start- und Stopbit gesendet werden, wodurch ein gewisser Overhead entsteht. Das asynchrone Verfahren kann nur bei geringen Datenraten angewendet werden.

Synchrone
Datenübertragung

Eine Alternative zu der asynchronen Datenübertragung stellt die synchrone Datenübertragung dar. Dabei wird das Taktsignal über die Datenleitung mit übertragen. Über das mitgesendete Taktsignal kann eine exakte Abstimmung der Bitimpulse erfolgen, weshalb man von einer synchronen Datenübertragung spricht. Die Kommunikationspartner laufen über den gesamten Zeitraum einer Verbindung synchron zueinander. Der Vorteil ist deutlich: Die Daten müssen nicht jedes Mal neu synchronisiert werden; das synchrone Verfahren ist auch bei höheren Datenraten anwendbar. Nachteilig bei diesem Verfahren ist natürlich die aufwändigere Implementierung.

Im Netzwerkbereich kann man prinzipiell laut allgemeiner Definition aus der Nachrichtentechnik von einer synchronen Datenübertragung sprechen, da der Takt immer vom Sender mit dem Datenstrom geliefert wird, also mit nur einer Taktquelle gearbeitet wird. Jedoch lässt sich für den Netzwerkbereich trotzdem asynchronen von synchron differenzieren:

Beim asynchronen Verfahren besteht zwischen der Aussendung zweier Datenpakete zwischen dem Sender und dem Empfänger keine Verbindung, weshalb sich die Kommunikationspartner bei jedem neuen Datenpaket neu synchronisieren müssen; beim synchronen Verfahren hingegen bleibt die Verbindung zwischen den Kommunikationspartnern bestehen, weshalb die Verbindung dauerhaft synchronisiert bleibt.

1.5.3 Die Frequenz

In der Elektrotechnik werden zwei verschiedene Spannungsarten unterschieden, die Gleichspannung und die Wechselspannung. Bei der Gleichspannung ist die Höhe und die Polarität der Spannung unabhängig von der Zeit stets gleich. Betrachtet man hingegen eine Wechselspannung, so ändert sich die Höhe und die Polarität der Spannung periodisch. Die Wechselspannung aus unserem Spannungsversorgungsnetz verändert sich beispielsweise in der Polarität und in der Höhe periodisch nach einer Sinusfunktion. Für den periodischen Spannungsverlauf wird eine bestimmte Zeit beansprucht, die als Periodendauer bezeichnet wird. In der Elektrotechnik gibt man über die Frequenz die Anzahl von Schwingungen pro Sekunde an, wobei die Frequenz und die Periodendauer in einem reziproken Zusammenhang stehen: Je niedriger die Periodendauer, desto höher ist die Frequenz. Man errechnet demnach die Frequenz nach der Formel $\text{Frequenz} = 1/\text{Periodendauer}$ und gibt sie in der Einheit Hertz (Hz) an. Dabei entspricht 1 Hertz einer Schwingung pro Sekunde. Unser Wechselspannungsversorgungsnetz arbeitet beispielsweise mit einer Frequenz von 50 Hz.

Frequenz

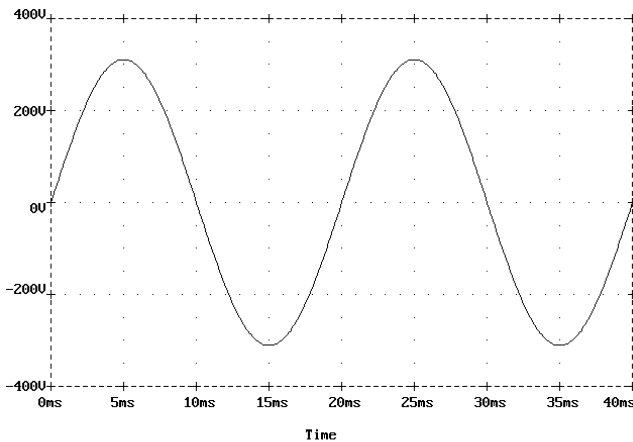


Abb. 1-9
*Verlauf einer 50-Hz-
Wechselspannung*

1.5.4 Das Datensignal

Datensignale

Die Übertragung der Informationen erfolgt durch den Austausch von binären Daten, die den Wert Null oder Eins annehmen können. Die elektrischen Signale, die dazu innerhalb eines Computers oder über ein Netzkabel übertragen werden, können entweder in einer rein digitalen oder in einer analogen Form genutzt werden. Innerhalb eines Computers und im Netzwerkbereich wird in der Regel die digitale Form verwendet. Obwohl auf einem Netzkabel ein digitales Datensignal eingespeist wird, muss man berücksichtigen, dass es sich hierbei ebenfalls um ein Analogsignal handelt (Fourier).

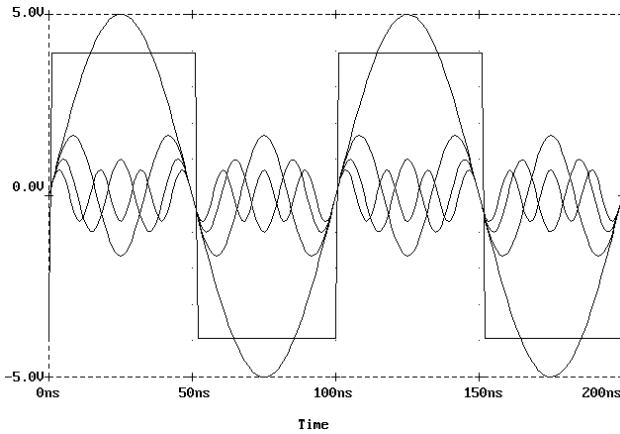
Die Signale, die über eine Datenleitung übertragen werden, unterliegen gewissen physikalischen Gesetzmäßigkeiten der Nachrichtentechnik, wie beispielsweise der Dämpfung, die das Datensignal entlang der Datenleitung in der Höhe des Signals abschwächt. Die Dämpfung ist allgemein umso höher, je höher die Frequenz des Datensignals ist. Bedingt durch diese Tatsache ist die maximal zu überbrückende Distanz begrenzt. Denn hat das Datensignal in der Höhe einen bestimmten Wert unterschritten, kann die Dateninformation nicht mehr eindeutig erkannt werden.

Fourier-Reihe

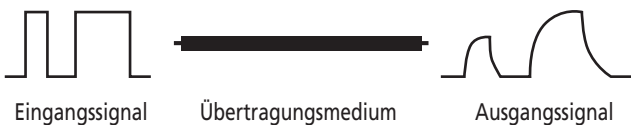
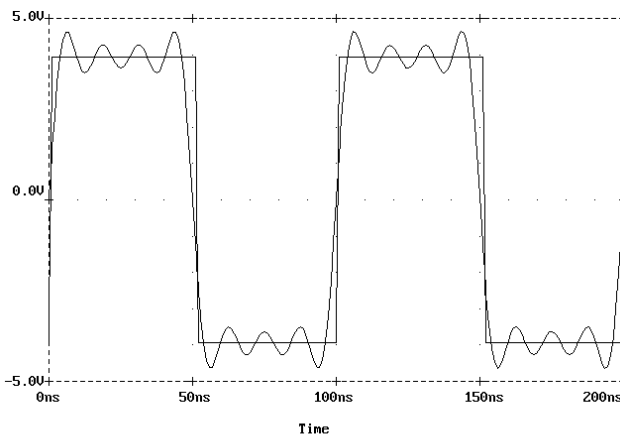
Ein Rechtecksignal besteht aus einer gewissen Grundfrequenz und aus Oberwellen der 3., 5. usw. Ordnung. Diese ganzzahligen Vielfachen der Grundfrequenz bezeichnet man auch als Harmonische. Laut der Fourier-Reihe lässt sich jede periodische Schwingung aus der Summe von Sinusschwingungen mit dem Vielfachen der Grundfrequenz zusammensetzen. Ein Rechtecksignal besteht demnach aus einer Überlagerung von harmonischen sinusförmigen Schwingungen (siehe Abb. 1–10).

Oberwellen eines Rechtecksignals

Die Fourier-Reihe gibt demnach auch indirekt Auskunft über die Verformung eines Datensignals und die Bandbreitenanforderung des Übertragungsmediums. Um ein Rechtecksignal einwandfrei übertragen zu können, ist es erforderlich, mindestens die 3. und 5. Oberwelle mitzuübertragen. Die 3. und 5. Oberwelle ist notwendig, damit das Rechtecksignal noch seine rechteckige Form beibehält und nicht wie ein abgerundetes Signal aussieht. Bedingt durch diese Tatsache muss bei der digitalen Datenübertragung nicht nur die Grundfrequenz, sondern auch noch die 3. und 5. Oberwelle mitübertragen werden. Bezogen auf das Übertragungsmedium ist demnach allgemein eine höhere Anforderung gestellt. Das Übertragungsmedium muss nicht nur die Grundfrequenz sauber übertragen können, sondern auch noch ihr 3- und 5faches. In der Praxis werden auf jeden Fall die Oberwellen immer stärker gedämpft, und die Ecken eines Rechtecksignals, das auf der einen Seite des Mediums eingespeist wird, weisen am Ende abgerundete Ecken auf (siehe Abb. 1–11).

**Abb. 1-10**

Laut der Fourier-Reihe setzt sich ein Rechtecksignal aus der Überlagerung von harmonischen Schwingungen zusammen.

**Abb. 1-11**

Verformung eines Rechtecksignals, das über ein Medium übertragen wird

1.5.5 Die Bandbreite

Unter der Bandbreite eines Übertragungssystems versteht man allgemein in der Nachrichtentechnik den Bereich von Frequenzen, der über ein Übertragungssystem problemlos, also ohne wesentliche Beeinflussung, übertragen werden kann. Die Dämpfung, die das Datensignal in seiner Höhe beeinflusst, ist umso größer, je höher seine Frequenz ist. Ist die Bandbreite des Datensignals kleiner als die Bandbreite des Übertragungsmediums, so kann man von einem geeigneten Übertragungsmedium ausgehen.

Bandbreite

1.5.6 Bitrate oder Datenrate

Die Bitrate oder Datenrate gibt die Anzahl der Bits an, die während einer Zeiteinheit von einer Sekunde übertragen werden. In der Netzwerktechnik ist es allgemein üblich, die Übertragungsgeschwindigkeit in Bit pro Sekunde anzugeben, wobei man als Präfix die entsprechenden Zehnerpotenzen kBit/s (kilo), MBit/s (Mega) und GBit/s (Giga) verwendet.

1.5.7 Baudrate

Baudrate Die Baudrate gibt die Anzahl der übertragenen Symbole pro Sekunde an. Ursprünglich wurde die Baudrate für die Signalisierungsgeschwindigkeit der Telegrafien verwendet, bei denen mit der Baudrate die Anzahl der übertragenen Morsezeichen pro Sekunde angegeben wurden. Die Einheit Baud wurde nach dem französischen Ingenieur Baudot benannt, der Fernschreiber konstruiert hatte. Heute verwendet man die Einheit Baud, um die Anzahl der Signalwechsel pro Sekunde anzugeben. Gerne wird die Bitrate mit der Baudrate gleichgesetzt, was von der Definition her falsch ist. Bei der binären Datenübertragung kann man, je nach verwendetem Codierungsverfahren, die Anzahl der Signalwechsel pro Sekunde mit der Anzahl der Bits gleichsetzen. Da dies jedoch oft zu Verwirrungen führt, sollte man im Netzwerkbereich für die Angabe der Übertragungsgeschwindigkeit vorzugsweise mit der Bitrate arbeiten.

1.5.8 Übertragungsfrequenz versus Übertragungsrate

Datenrate versus Übertragungsfrequenz

Die Datenrate darf grundsätzlich nicht mit der Übertragungsfrequenz gleichgesetzt werden. Die Datenrate gibt an, wie viele Daten, also Informationen ausgedrückt in Bit, innerhalb einer Zeiteinheit von einer Sekunde übertragen werden können. Die Übertragungsfrequenz ergibt sich aus der Übertragung der Daten und ist letztendlich davon abhängig, welches Codierungsverfahren bei der Datenübertragung verwendet wird. Das Codierungsverfahren beschreibt die Art und Weise, wie die Informationen dargestellt werden. Betrachtet man im Netzwerkbereich die heutigen Hochgeschwindigkeitslösungen, so wird in der Regel über spezielle Codierungsverfahren dafür gesorgt, dass die Übertragungsfrequenz, die bei der Datenübertragung auftritt, möglichst klein ist. Dies ist notwendig, da die Höhe der Übertragungsfrequenz letztendlich die Dämpfung bestimmt, die das Datensignal während der Übertragung über das Übertragungsmedium erfährt. Je höher die Dämpfung ist, desto niedriger ist die Reichweite, die erzielt werden kann.

1.5.9 Kanalkapazität

Wie viele Daten über einen Übertragungskanal übertragen werden können, wird mithilfe der Kanalkapazität beschrieben. Die Kanalkapazität gibt an, welche maximale Bitrate in einem frequenzbeschränkten, rauschbelasteten Übertragungskanal erzielt werden kann. Laut der Shannon'schen Informationstheorie (Claude Shannon, amerikanischer Informatiker, geb. 1916) wird die Kanalkapazität C nach der folgenden Formel beschrieben: $C = B \times \log_2(1 + S/N)$. C wird hierbei in Bit/s angegeben; B steht hier für die Bandbreite des Übertragungskanals in Hz, S für die Leistung des Nutzsignals und N für die Leistung des Störsignals. Das Verhältnis S/N beschreibt dabei das sogenannte Signal-Rauschverhältnis, also das Verhältnis zwischen dem übertragenen Signal und dem zufälligen Rauschen. Laut Informationstheorie begrenzt das Signal-Rauschverhältnis die Anzahl der Bits, die pro Symbol übertragen werden können. Oder anderes formuliert: Je besser das Signal-Rauschverhältnis ist, desto höher ist die erzielbare Datenrate.

Kanalkapazität

1.5.10 Paketvermittlung

Bei den Computernetzwerken wird für die Datenübertragung die gesamte Bandbreite des Übertragungsmediums jeweils für eine relativ kurze Zeit in Anspruch genommen. Das Übertragungsmedium verfügt in der Regel über eine hohe Bandbreite. Betrachtet man hingegen den Datenaustausch über eine ISDN-Leitung, so wird hier bei einer geringen Bandbreite die gesamte Bandbreite für einen gewissen Zeitraum dauerhaft in Anspruch genommen. Praktisch sieht dies in der Form so aus, dass man eine dedizierte Punkt-zu-Punkt-Verbindung zwischen den Verbindungspartnern für die gewünschte Dauer des Datenaustauschs schaltet; man spricht in diesem Fall von einer verbindungsorientierten Verbindung. Nachteilig ist natürlich bei diesem Verfahren, dass für die Dauer der geschalteten Verbindung die Leitung beziehungsweise der Kanal für andere Verbindungen nicht genutzt werden kann.

Paketvermittlung

In einem lokalen Netzwerk wird ein vorhandenes Medium gemeinsam verwendet (Shared Media), dies verhält sich ähnlich wie beim Funk oder einer Unterhaltung von mehreren Personen in einem Raum. Um die Daten zielgerichtet zum gewünschten Empfänger übertragen zu können, werden die Daten, die als Datenpakete zusammengefasst sind, mit Adressinformationen versehen. Die Datenpakete werden demnach ähnlich wie Briefe oder Pakete beim Versand über die Post verschickt. Diese Art der Kommunikation bezeichnet man als Paketvermittlung. Dafür muss keine dedizierte Verbindung zwischen den Kommunikationspartnern aufgebaut werden; deshalb spricht man hier von einem verbindungslosen Dienst.

1.5.11 Grundlegende Zugriffsverfahren

Zugriffsverfahren Bedingt durch die Tatsache, dass im Netzwerk ein Übertragungsmedium von allen Teilnehmern gemeinsam für die Datenübertragung verwendet wird (Shared Media), muss über ein geeignetes Zugriffsverfahren sichergestellt werden, dass innerhalb eines Zeitraums immer nur ein Teilnehmer Daten sendet. Denn ausschließlich dann, wenn diese Anforderung erfüllt ist, können die Daten fehlerfrei übertragen werden. Bei den Zugriffsverfahren für ein Shared Media wird allgemein zwischen zwei Zugriffsverfahren, dem deterministischen und dem nicht-deterministischen, unterschieden.

Deterministisches Zugriffsverfahren Beim deterministischen Verfahren wird der Zugriff auf das gemeinsam genutzte Medium über Konventionen geregelt. Der Zugriff auf das Medium erfolgt also zu einem bestimmten Zeitpunkt in Übereinstimmung mit den anderen Teilnehmern im Netzwerk. Bei Token-Ring- und FDDI-Netzwerken wird beispielsweise ein Token-Passing-Verfahren verwendet, das ein deterministisches Zugriffsverfahren darstellt. Dabei gibt ein Teilnehmer, der mit der Aussendung seiner Daten fertig ist, das Senderecht an einen anderen Teilnehmer im Netz weiter. Dieser Teilnehmer darf durch den Erhalt des Senderechts ebenfalls über einen bestimmten Zeitraum Daten versenden. Macht der Teilnehmer von seinem Senderecht jedoch keinen Gebrauch, so gibt er das Senderecht direkt an einen anderen Teilnehmer weiter, ohne Daten zu versenden. Das Senderecht wird bei dem Token-Passing-Verfahren über ein Token realisiert: Derjenige Teilnehmer, der das Token hat, ist berechtigt, Daten zu versenden. Da die Sendezeit für jeden Teilnehmer nach dem Erhalt des Token beschränkt ist und jeder Teilnehmer den Token erhält, d. h. kein Teilnehmer bei der Weitergabe des Token übergangen wird, stellt das Token-Passing-Verfahren ein faires Zugriffsverfahren dar. Denn das Zugriffsverfahren stellt sicher, dass nach einer bestimmten Wartezeit, deren maximale Dauer vorhersehbar ist, eine bestimmte Datenmenge von jedem Teilnehmer übertragen werden darf. In der Regel sind auf Token Passing basierende Netzwerke physisch als Ring-Topologie aufgebaut, bei denen sich der Nachfolger für die Weitergabe des Token aus der physischen Anordnung innerhalb des Rings ergibt.

Nicht-deterministisches Zugriffsverfahren Als weitere Zugriffsverfahren für ein Shared Media werden in den Netzwerken die nicht-deterministischen Verfahren verwendet, bei denen der Zugriff ebenfalls über bestimmte Konventionen geregelt wird, jedoch alle Teilnehmer in Bezug auf den Mediengriff in direktem Wettbewerb zueinander stehen. Bedingt durch diese Tatsache kann die Wartezeit und die Datenmenge, die zu einem bestimmten Zeitpunkt übertragen werden kann, nicht eindeutig vorhergesehen werden. Die Dauer der Wartezeit und die Datenmenge, die von jedem Teilnehmer übertragen werden kann, hängt beim nicht-deterministischen Verfahren stark von der Anzahl der Teilnehmer und der Datenmenge ab, die von den einzelnen Teilnehmer versendet wird. Beispielsweise ist das Zugriffsverfahren Carrier Sense Multiple Access Collision Detection (CSMA/CD), das beim Ethernet ver-

wendet wird, ein klassisches nicht-deterministisches Zugriffsverfahren. Bei CSMA/CD prüft ein Teilnehmer, der Daten versenden möchte, vor der Aussendung der Daten zuerst, ob das Übertragungsmedium frei ist. Wenn dies der Fall ist, sendet der Teilnehmer seine Daten aus. Kommt es dazu, dass zwei oder mehrere Teilnehmer zur selben Zeit versuchen, ihre Daten auszusenden, so gehen die Teilnehmer von einem freien Medium aus. In diesem Fall kommt es jedoch dazu, dass sich die Daten der sendenden Teilnehmer überlagern, wodurch die Daten unbrauchbar werden. In diesem Fall spricht man von einer Kollision. Durch ein Kollisionserkennungsverfahren wird dies erkannt, worauf die sendenden Teilnehmer die Aussendung ihrer Daten abbrechen. Tritt eine Kollision auf, so werden die Teilnehmer, deren Daten durch die Kollision unbrauchbar wurden, nach einer Wartezeit erneut versuchen, ihre Daten auszusenden. Die Wartezeit wird dabei von jedem Teilnehmer über einen bestimmten Algorithmus nach dem Zufallsprinzip ermittelt, so dass die Teilnehmer zu unterschiedlichen Zeitpunkten versuchen werden, ihre Daten erneut zu versenden, wodurch eine erneute Kollision vermieden werden soll. Die Wahrscheinlichkeit, dass mehrere Teilnehmer zur selben Zeit versuchen, ihre Daten zu versenden, und damit zwangsläufig gehäufte Kollisionen auftreten, steigt mit der Anzahl der Teilnehmer, die gemeinsam das Übertragungsmedium nutzen, und mit dem Datenvolumen, das von jedem Teilnehmer übertragen werden soll. Bedingt durch diese Tatsache kann der Zugriff auf das Übertragungsmedium, also die Wartezeit und die Datenmenge, die nach einem bestimmten Zeitpunkt übertragen werden kann, nicht vorhergesehen werden, weshalb man hierbei von einem nicht-deterministischen Zugriffsverfahren spricht.

⇒ Wir werden im Kapitel 2 „Ethernet“ detailliert auf das Zugriffsverfahren CSMA/CD eingehen.

1.6 Netzwerkarchitekturen

Die Kommunikation innerhalb eines Netzwerks wird anhand eines Netzwerkmodells beschrieben, wobei man sich das sogenannte Open-Systems-Interconnection-Referenz-Modell (OSI Reference Model) stützt. Das OSI-Referenzmodell wurde zwischen 1977 und 1984 (1984 in der ISO-Norm 7498 festgeschrieben) entworfen und ist in sieben Teilschichten unterteilt, die auch als Layer bezeichnet werden. Jede Schicht des OSI-Referenzmodells stellt eine bestimmte Funktion zur Verfügung, die als Dienst bezeichnet wird und einen funktionellen Beitrag für den Ablauf der Kommunikation zwischen zwei Computern leistet.

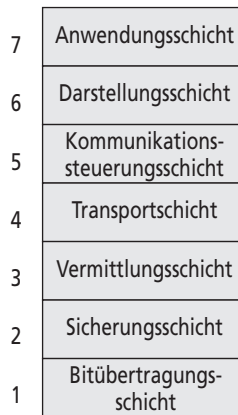
OSI-Referenzmodell

In den Anfängen der Netzwerktechnologien gab es viele firmenspezifische Standards. Zu dieser Zeit war es undenkbar, dass ein Datenaustausch zwischen Einrichtungen unterschiedlicher Hersteller möglich war. Man erkannte rechtzeitig diese Problematik und entwarf deshalb eine entsprechende Netzwerkarchitektur, die als Basis für die heutzutage offenen

Plattformen dient. Aus dieser Intention heraus entstand das OSI-Referenzmodell, das heutzutage allgemein als Grundlage für die Definition von Standards für offene Systeme im Kommunikationsbereich dient. Bei dem OSI-Referenzmodell handelt es sich allerdings ausschließlich um ein Modell, das eine Standard-Netzwerkarchitektur beschreibt und wesentlich zum Verständnis der funktionellen Zusammenhänge im Netzwerk beiträgt.

Abb. 1–12

Das siebenschichtige
OSI-Referenzmodell



Sieben Schichten

Jede Schicht im OSI-Referenzmodell, mit Ausnahme der untersten Schicht, hat eine darunter liegende Nachbarschicht und jede Schicht, außer der obersten Schicht, hat eine darüberliegende Nachbarschicht. Die Schichten stellen jeweils ihre Dienste der darüber liegenden Schicht zur Verfügung und nutzen ihrerseits die Dienste der darunter liegenden Schicht. Die Kommunikation zwischen den Schichten erfolgt über definierte Schnittstellen.

Dienste

Durch die Funktion beziehungsweise den Dienst einer Schicht wird in der Gesamtbetrachtung die Funktion einer darunter liegenden Schicht erweitert. Jede Schicht folgt beim Ausführen ihrer Funktion gewissen definierten Regeln, die als Protokolle bezeichnet werden. Die Kommunikation zwischen zwei Computern findet immer nur zwischen den Schichten der gleichen Ebene statt und wird als virtuelle Kommunikation bezeichnet. Damit die virtuelle Kommunikation zwischen zwei Computern stattfinden kann, müssen auf den gegenüberliegenden Schichten der gleichen Ebene jeweils dieselben Protokolle implementiert sein. Die Schichten derselben Ebene werden als Peers und die korrespondierenden Protokolle derselben Ebene als Peer Protocol bezeichnet. Die Peers tauschen während der Kommunikation ihre Informationen in einem Format aus, das auf beiden Seiten verstanden wird und als Protokoll-Dateneinheit (PDU = Protocol Data Unit) bezeichnet wird. Eine PDU ist in zwei Teile aufgeteilt, den Header für Protokollinformationen (Protocol Control Information, PCI) und die Dateneinheit (Service Data Unit). Der Dienst, der von einer Schicht zur

Verfügung gestellt wird, wird durch eine oder mehrere Arbeitseinheiten (Entities) umgesetzt. Der Zugriff auf die Arbeitseinheiten erfolgt über sogenannte Service Access Points (SAP); sie stellen quasi eine Adresse dar, über die auf die verschiedenen Funktionen zugegriffen werden kann.

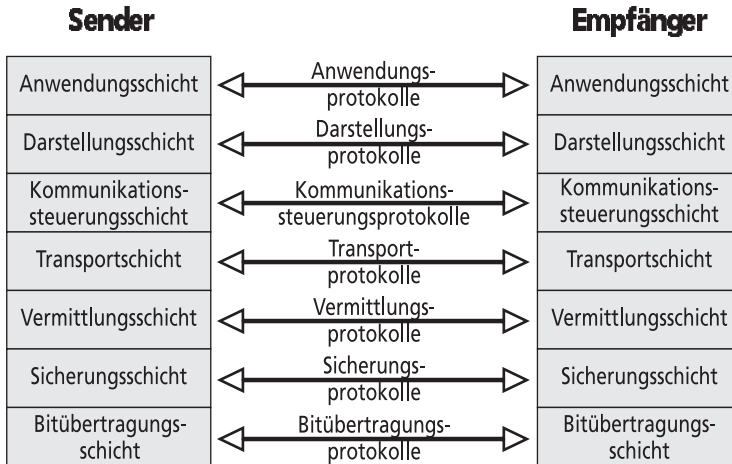


Abb. 1–13

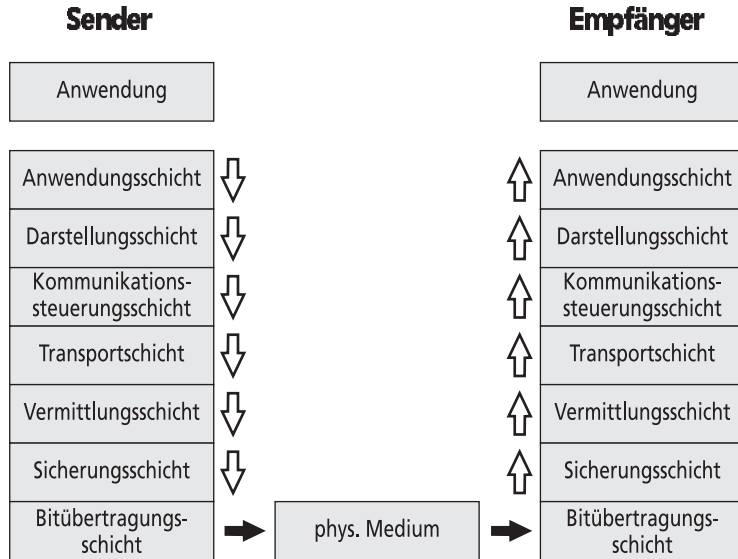
Die virtuelle Kommunikation findet immer auf derselben Ebene statt.

Wie bereits erwähnt, findet bei der Kommunikation zwischen zwei Computern die virtuelle Kommunikation jeweils auf derselben Ebene statt. Die Daten bewegen sich dabei von dem einen Computer vertikal nach unten bis zur untersten Schicht im Referenzmodell, der Bitübertragungsschicht. Auf der Bitübertragungsschicht bewegen sich die Daten horizontal zum Computer, mit dem kommuniziert werden soll. Auf diesem Computer laufen die Daten dann wieder vertikal nach oben in die einzelnen Schichten. Die Daten erreichen auf diese Weise die jeweils gleichen Schichten (Peers) auf dem gegenüberliegenden Computer, zwischen denen auch die Kommunikation jeweils stattfindet (siehe Abb. 1–14).

Virtuelle Kommunikation

Jede Schicht des OSI-Referenzmodells stellt unabhängig von den anderen Schichten bestimmte Funktionen oder Dienste zur Verfügung.

Abb. 1-14
Darstellung der
Kommunikationswege
innerhalb des
OSI-Referenzmodells



Die Bitübertragungsschicht

Bitübertragungsschicht

Die Bitübertragungsschicht, auch physikalische Schicht genannt (engl. Physical Layer), ist die unterste Schicht des OSI-Referenzmodells. Die Bitübertragungsschicht stellt einen Dienst bereit, mit dessen Hilfe die Daten als Bitstrom physikalisch über ein Übertragungsmedium von einem Computer zu einem anderen Computer übertragen werden können. Es handelt sich in dem Fall um eine ungesicherte und physikalische Verbindung, die nach Bedarf auf dem Übertragungsmedium auf- und abgebaut wird. Auf der Bitübertragungsschicht ist beispielsweise das Übertragungsmedium und damit verbunden die physikalischen Eigenschaften der Datensignale definiert, über die der Datenstrom auf dem jeweiligen Medium übertragen wird. Dazu gehören die Art und Größe des Datensignals, die Bit- oder Bytesynchronisation, die Codierungs- und Modulationsverfahren. Des Weiteren ist auf der Bitübertragungsschicht das Interface definiert, d. h. der physikalische Anschluss und die Art der verwendeten Verbindungselemente. Man kann zusammenfassend sagen, dass auf der Bitübertragungsschicht die elektrische und mechanische Definition des Interface und das Übertragungsmedium definiert werden.

Die Sicherungsschicht

Sicherungsschicht

Die Sicherungsschicht (engl. Data Link Layer) ist die zweite Schicht des OSI-Referenzmodells. Aufgabe der Sicherungsschicht ist es, einen fehlerfreien Datenaustausch zu gewährleisten. Dazu werden die Daten zu Einheiten zusammengefasst, die als Datenpakete oder Frames bezeichnet werden. Die Datenpakete haben ein bestimmtes Format und werden in der

Regel durch eine Prüfsumme ergänzt, über die eine Fehlererkennung möglich ist. Des Weiteren wird auf der Sicherungsschicht der Zugriff auf das Übertragungsmedium durch ein entsprechendes Zugriffsverfahren durchgeführt.

Die Sicherungsschicht wird in der Praxis in zwei Teilbereiche unterteilt, wobei der untere Teilbereich durch die verschiedenen standardisierten Netzwerktechnologien wie Ethernet oder Token Ring abgedeckt wird. Der obere Bereich umfasst Logical Link Control laut Standard IEEE 802.2. Der obere Teilbereich wird von allen IEEE-Netzwerktechnologien gleichermaßen verwendet, wodurch der Datenaustausch zwischen verschiedenen Netzwerktechnologien vereinfacht wird.

Die Vermittlungsschicht

Die nächste Ebene im OSI-Referenzmodell ist die Vermittlungsschicht, auch Netzwerkschicht genannt (engl. Network Layer). Sie sorgt für den eigentlichen Datentransfer zwischen den Computern, indem sie die Wegfindung (Routing) zwischen den Computern übernimmt. Stellen die unteren beiden Schichten nur eine Kommunikation zwischen zwei angrenzenden Computern innerhalb eines Netzwerks zur Verfügung, so bietet die Vermittlungsschicht eine Möglichkeit zur Kommunikation über die Grenzen eines Netzwerks hinaus. Die Daten werden dazu mit entsprechenden Ziel- und Quelladressen versehen, über die das zielgerichtete Routing durchgeführt werden kann. Die Adressierung auf der dritten Ebene ist von den darunter liegenden Schichten unabhängig; das Routing kann sich auf diese Weise über mehrere logisch strukturierte Netzwerke erstrecken. Erst durch die Adressierungsmöglichkeiten auf der dritten Ebene ist eine Bildung von hierarchisch untergliederten Teilnetzwerken möglich, zwischen denen ein Datenaustausch ermöglicht wird.

Vermittlungsschicht

Die Transportschicht

Die Transportschicht (engl. Transport Layer) ist auf der vierten Ebene platziert und vermittelt zwischen den drei obersten Schichten des OSI-Referenzmodells und den unteren vier Schichten, die das Transportsystem darstellen. Im Grunde tauschen zwei Programme untereinander Daten aus, wenn zwei Computer miteinander kommunizieren. Die Transportschicht sorgt dafür, dass die Daten der Vermittlungsschicht an die richtigen Programme auf dem Computer ausgeliefert werden. Diese Schicht sorgt so für die Zuverlässigkeit des Datentransfers und den gleichzeitigen Zugriff mehrerer Dienste oder Anwendungen auf dieselben Transportmechanismen. Die Transportschicht stellt damit für die übergeordneten Instanzen einen transparenten Datenkanal zur Verfügung.

Transportschicht

Auf der Transportschicht werden die Daten in kleine Teileinheiten aufgeteilt, wie sie von der Vermittlungsschicht weitergeleitet werden können (Fragmentierung). Auf der anderen Seite, der Empfängerseite, werden

die Daten von den Diensten der Transportschicht wieder zu einem gesamten Datenblock zusammengesetzt. Dabei wird von den Diensten der Transportschicht dafür gesorgt, dass die Daten empfangsseitig in der richtigen Reihenfolge ankommen, damit sie wieder eine logische Dateneinheit bilden.

Die Kommunikationssteuerungsschicht

*Kommunikations-
steuerungsschicht*

Die Kommunikationssteuerungsschicht, auch Sitzungsschicht genannt (engl. Session Layer), ist die fünfte Schicht im OSI-Referenzmodell. Sie stellt einen anwendungsorientierten Dienst zur Verfügung und sorgt für einen Verbindungsauf- und -abbau sowie die Darstellung der Übertragungsdaten in einer von der darüber liegenden Ebene unabhängigen Form. Der Anmeldevorgang wird im Fachjargon als Aufbau einer Sitzung (Session) bezeichnet. Eine Sitzung stellt die Grundlage für eine virtuelle Verbindung zwischen zwei Prozessen dar, die auf räumlich getrennten Computern ausgeführt werden. Die Sitzungsschicht ist für den Aufbau, die Überwachung und das Beenden einer Sitzung verantwortlich. Dabei kommen unterstützende Funktionen zum Tragen, wie zum Beispiel die Echtheitsbestätigung und die Sicherheitsmechanismen für den Zugriff auf Ressourcen.

Die Darstellungsschicht

Darstellungsschicht

Die Darstellungsschicht (engl. Presentation Layer) ist die sechste Schicht innerhalb des OSI-Referenzmodells. Sie ist für die Kommunikation und das Weiterreichen von Daten zwischen der Sitzungsschicht und den Anwendungen verantwortlich und beinhaltet bestimmte Funktionen, die für die Kommunikation innerhalb eines Netzwerks benötigt werden. Dazu gehören Schnittstellen zu Netzwerkressourcen wie beispielsweise Drucker oder Speichermedien. Auf der Darstellungsschicht wird festgelegt, in welcher Form die Daten dem Anwender präsentiert werden. Hierzu gehören beispielsweise die Art und die Länge des Datentyps. Ebenfalls kann auf der Darstellungsschicht eine Komprimierung oder Verschlüsselung von Daten eine Rolle spielen.

Die Anwendungsschicht

Anwendungsschicht

Die Anwendungsschicht (engl. Application Layer) ist die oberste und siebte Schicht des OSI-Referenzmodells; sie bildet das Bindeglied zwischen dem Anwender und den Anwendungsprozessen über das Netzwerk. Auf der Anwendungsschicht sind die anwendungsspezifischen Protokolle angesiedelt, wobei Details zu Programmen oder Anwendungen, die von den Netzwerkbenutzern während ihrer Arbeit im Netzwerk genutzt werden, auf der Anwendungsschicht enthalten sind. Zu den Protokollen gehören beispielsweise das File Transfer Protocol (FTP), mit dem Dateien über ein Netzwerk übertragen werden können, oder TELNET, mit dem remote

auf einen Computer zugegriffen werden kann und Befehle ausgeführt werden können.

Die Unterteilung des OSI-Referenzmodells

Betrachtet man die Dienste, die von den sieben Schichten bereitgestellt werden, so fällt auf, dass man das OSI-Referenzmodell in zwei Bereiche aufteilen kann. Die eigentlichen Transportmechanismen, die für die Datenübertragung über ein Netzwerk sorgen, sind auf den untersten vier Schichten angesiedelt. Die unteren beiden Schichten entsprechen dabei der Netzwerktechnologie, wie beispielsweise Ethernet. Die dritte und vierte Schicht beinhaltet die Protokolle wie TCP/IP oder IPX/SPX.

*Unterteilung des
OSI-Referenzmodells*

⇒ Die folgenden Kapitel dieses Buchs werden sich im Wesentlichen mit den unteren vier Schichten beschäftigen.

Die oberen drei Schichten des OSI-Referenzmodells sind anwendungsorientiert, sie bilden die Schnittstelle zu den Netzwerkanwendungen und den Netzwerkanwendern.

1.7 Ein Überblick über den Inhalt dieses Buchs

Der Autor hat das Buch mit dem Ziel geschrieben, praxisnahes Wissen für Ethernet-Netzwerke zu vermitteln. Dabei werden primär die unteren vier Schichten des OSI-Referenzmodells abgehandelt. Die ersten beiden Schichten beziehen sich in diesem Fall ausschließlich auf Ethernet und die dritte und vierte Schicht auf die heute gängigen Protokolle im Netzwerkbereich. Abgerundet werden diese Informationen durch die Beschreibung der gängigen Netzwerkdienste. Ziel ist es, die Funktionen eines Netzwerks zu verstehen, um diese in der Praxis bei der Fehlersuche oder Performance-Optimierung anwenden zu können.

Inhalt dieses Buchs

Kapitel 2 beinhaltet eine nahezu vollständige Darstellung der Ethernet-Technologie. Dabei werden Grundlagen zur Funktion des 10-MBit/s-Ethernet vermittelt.

Kapitel 2

Kapitel 3 beschreibt die Funktionsweise der Fast-Ethernet-Techniken für 100 MBit/s-Netze und geht ausführlich auf die Auto-Negotiation-Funktion ein.

Kapitel 3

Kapitel 4 widmet sich dem Gigabit-Ethernet, das heutzutage einen Informationsaustausch mit einer Datenrate von 1000 MBit/s über Glasfaser oder TP-Kabel ermöglicht.

Kapitel 4

Kapitel 5 behandelt die 10Gigabit-Ethernet-Technologie, die eine Datenübertragung von 10.000 MBit/s über Glasfaser oder TP-Kabel ermöglicht.

Kapitel 5

Kapitel 6 geht auf die neuen Highspeed-Varianten von Ethernet ein, die eine Datenrate von 40 GBit/s oder 100 GBit/s ermöglichen.

Kapitel 6

- Kapitel 7* Kapitel 7 beschreibt ausführlich die Berechnung der Längenrestriktionen für die maximal zulässige Ausdehnung einer Ethernet-Kollisionsdomäne. Zudem erläutert dieses Kapitel, wie die Stromversorgung von Endgeräten über TP-Kabel mit Power over Ethernet (PoE) und Power over Ethernet Plus (PoE+) realisiert werden kann. Des Weiteren geht dieses Kapitel auf das Thema Energy Efficient Ethernet (EEE) und das Link Layer Discovery Protocol (LLDP) ein.
- Kapitel 8* Kapitel 8 ergänzt die Grundlagen von Ethernet durch die bei Ethernet verwendeten Übertragungsmedien und die Betrachtung der physikalischen Parameter und Messgrößen.
- Kapitel 9* Kapitel 9 behandelt detailliert die verschiedenen Ethernet-Komponenten, die heutzutage in einem Ethernet-Netzwerk eingesetzt werden.
- Kapitel 10* Kapitel 10 zeichnet Konzepte für den Aufbau eines Ethernet-Netzwerks auf und liefert Grundlagen für die Performance-Analyse und -Optimierung.
- Kapitel 11* Kapitel 11 beschäftigt sich mit den Netzwerkprotokollen der TCP/IP-Protokollfamilie, die in heutigen LANs vorwiegend eingesetzt werden. Es werden Aufbau und Funktion der Protokolle im Einzelnen beschrieben. Abgerundet wird das Kapitel durch Grundlagen zur Berechnung von IP-Adressen und Subnetzen.
- Kapitel 12* Kapitel 12 widmet sich den Protokollen der Ebenen 5 bis 7 des OSI-Referenzmodells.
- Kapitel 13* Kapitel 13 schließlich behandelt die Fehleranalyse innerhalb eines Netzwerks. Hier liegt der Schwerpunkt auf der Protokollanalyse sowie auf der richtigen Platzierung der Protokollanalytoren innerhalb des Netzwerks.