ELEKTRONIK-KOMPENDIUM.DE

Netzwerk-Grundlagen

Was du über die Netzwerk-Grundlagen wissen solltest.

Einführung in die Grundlagen der Netzwerktechnik mit Grundbegriffen, Komponenten, Protokollen und Anwendungen.

Inhaltsverzeichnis

Grundlagen Netzwerktechnik

Ein Netzwerk ist die physikalische und logische Verbindung von mehreren Computersystemen. Jedes Netzwerk basiert auf Übertragungstechniken, Protokollen und Systemen, die eine Kommunikation zwischen den Teilnehmern eines Netzwerks ermöglichen. Ein einfaches Netzwerk besteht aus zwei Computersystemen. Sie sind über ein Kabel miteinander verbunden und somit in der Lage ihre Ressourcen gemeinsam zu nutzen. Wie zum Beispiel Rechenleistung, Speicher, Programme, Daten, Drucker und andere Peripherie-Geräte. Ein netzwerkfähiges Betriebssystem stellt den Benutzern auf der Anwendungsebene diese Ressourcen zur Verfügung.

Daraus ergeben sich einige Vorteile gegenüber unvernetzten Computern:

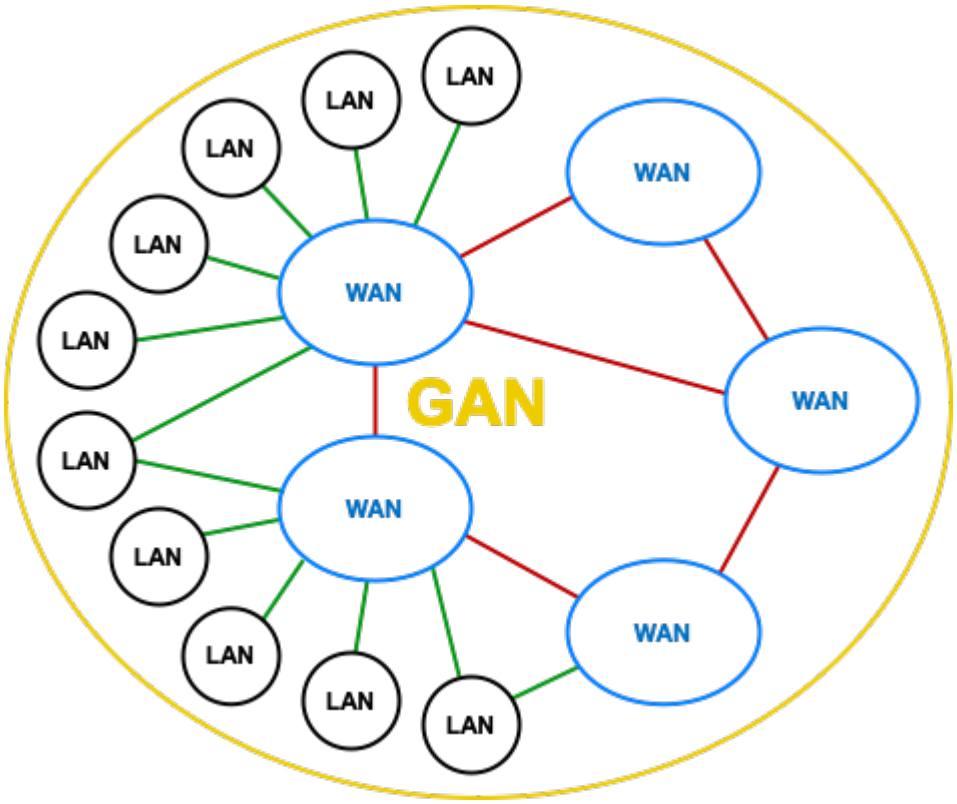
- Nutzen gemeinsamer Datenbestände
- Nutzen verfügbarer Ressourcen
- Teilen von Rechenleistung und Speicherkapazität
- zentrales Steuern von Programmen und Daten
- Durchsetzen von Berechtigungen und Zuständigkeiten
- Durchsetzen Datenschutz und Datensicherheit

Als es die ersten Computer gab, waren Peripherie-Geräte und Speicher sehr teuer. Die erste Möglichkeit, Peripherie-Geräte gemeinsam zu nutzen, waren manuelle Umschaltboxen. So konnte man zum Beispiel von mehreren Computern aus einen Drucker nutzen. Mit welchem Computer der Drucker verbunden war, wurde über die Umschaltbox bestimmt. Leider haben Umschaltboxen den Nachteil, dass Computer und Peripherie relativ nahe beieinander stehen müssen, weil die Kabellänge physikalisch bedingt begrenzt ist.
Der Bedarf zwischen mehreren Computern Daten auszutauschen und Ressourcen zu teilen führte dazu, Computer miteinander zu verbinden bzw. zu vernetzen.

Netzwerk-Dimensionen: LAN, WAN und GAN

Bestimmte Netzwerktechniken unterliegen Beschränkungen, die insbesondere die Reichweite und geografische Ausdehnung des Netzwerks begrenzt. Hierbei unterscheidet man zwischen verschiedenen Netzwerk-Dimensionen für die es unterschiedliche Netzwerktechniken gibt.

- PAN - Personal Area Network: personenbezogenes Netz, z. B. Bluetooth
- LAN - Local Area Network: lokales Netz, z. B. Ethernet und WLAN
- MAN - Metropolitan Area Network: regionales Netz
- WAN - Wide Area Network: öffentliches Netz, z. B. DSL und Mobilfunk
- GAN - Global Area Network: globales Netz, z. B. das Internet



In der Regel findet ein Austausch zwischen den Netzen statt. Das heißt, dass Netzwerk-Teilnehmer eines LANs auch ein Teilnehmer eines WANs oder eines GANs ist. Eine 100%ig klare Abgrenzung zwischen diesen Dimensionen ist nicht immer möglich, weshalb man meist nur eine grobe Einteilung vornimmt. So unterscheidet man in der Regel zwischen LAN und WAN, wobei es auch Techniken und Protokolle gibt, die sowohl im LAN, als auch im WAN zum Einsatz kommen.

- Warum vernetzen wir Computersysteme zu einem **LAN**? Um **gemeinsame Ressourcen** zu nutzen. Zum Beispiel Internet-Zugang, Drucker, Speicher, Rechenleistung, Dienste und Anwendungen.
- Warum verbinden wir uns mit einem **WAN**? Um **Dienste** von anderen zu nutzen oder um eigene Dienste anderen anzubieten. Zum Beispiel Datenverarbeitung und Informationsaustausch.
- Warum verbinden wir uns mit einem **GAN**? Um an einer weltweit verfügbaren **Kommunikationsanwendung** teilzunehmen. Zum Beispiel Internet, Telefonie, Messaging und E-Mail.

Protokolle in der Netzwerktechnik

In der Netzwerktechnik bestimmen Protokolle den Ablauf der Kommunikation zwischen den Systemen. Netzwerk-Protokolle sind eine Sammlung von Regeln, die den Ablauf einer Kommunikation zwischen zwei oder mehr Systemen festlegen. Ein Netzwerk-Protokoll definiert, wie die Kommunikation aufgebaut wird, wie und über was sich die Systeme austauschen und wie die Kommunikation wieder beendet wird. Während einer Kommunikation werden also nicht nur Informationen oder Daten ausgetauscht, sondern zusätzlich Protokoll-Informationen, die beim Empfänger verarbeitet werden. Typischerweise ist nicht nur ein Netzwerk-Protokoll für die Kommunikation

verantwortlich, sondern mehrere, die ganz bestimmte Teilaufgaben innerhalb der Kommunikation übernehmen. Die Einteilung erfolgt anhand eines Schichtenmodells. Ein Protokoll ist in der Regel einer bestimmten Schicht zugeordnet.

Schichtenmodelle

Weil ein Netzwerk möglichst universell sein soll, also von mehreren Teilnehmern und mehreren Anwendungen gleichzeitig genutzt werden soll, ist die Netzwerk-Kommunikation in Schichten aufgeteilt. Jede Schicht hat ihre Aufgabe und löst dabei ein bestimmtes Teilproblem einer Kommunikation. Sender und Empfänger müssen dabei mit dem gleichen Schichtenmodell arbeiten.
Es gibt verschiedene Schichtenmodelle, die sich in der Anzahl der Schichten und somit der Verdichtung der Aufgaben unterscheiden.

Datenübertragung im Netzwerk

Die Kommunikation kann grundsätzlich auf zwei Arten erfolgen. Entweder verbindungsorientiert oder verbindungslos.
Bei der verbindungsorientierten Datenübertragung wird vor dem Austausch der Daten erst eine logische Verbindung hergestellt. Während der Übertragung bleibt die Verbindung zwischen den Kommunikationspartnern aufrechterhalten. Die logische Verbindung bleibt solange bestehen, bis sie durch einen Verbindungsabbau beendet wird.
Bei der verbindungslosen Kommunikation wird keine logische Verbindung und damit auch keine dauerhafte Verbindung aufgebaut. Die Daten werden in kleine Einheiten geteilt. Die Übertragung jeder Einheit wird auf den meisten Protokoll-Schichten als abgeschlossener Vorgang behandelt. Je nach Technik werden die einzelnen Übertragungseinheiten allgemein als Paket oder Datenpaket bezeichnet. Protokolle bzw. die OSI-Schichten haben meist eigene Begriffe, die meist für das gleiche stehen.

OSI-Schicht	Typ (Deutsch)	Typ (Englisch)
Alle Schichten	Paket/Datenpaket	Packet
Anwendung	Nachricht	Message
Transport	Segment	Segment
Vermittlung	Datagramm	Datagramm
Sicherung	Rahmen	Frame
Bitübertragung	Bitfolge / Bitstrom	Bitstream

Ganz allgemein spricht man von Datenpaketen oder nur Paketen. Nimmt man es ganz genau, dann spricht man bei IPv4 von Datagrammen (RFC 891) und bei IPv6 von Paketen (RFC 2460) und bei TCP ist es das Segment.

Netzwerk-Adressen

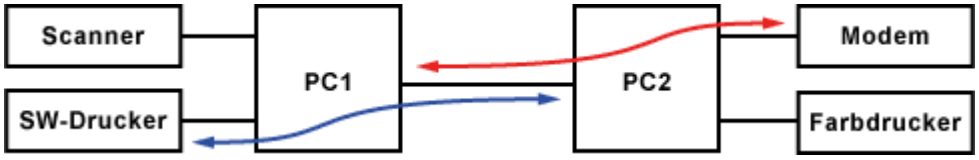
Innerhalb eines Netzwerks werden spezielle Netzwerk-Adressen verwendet, um Sender und Empfänger eines Datenpakets oder einer Nachricht zu adressieren. Dabei unterscheiden sich Netzwerk-Adressen anhand ihrer Funktion, Anwendungen und Protokoll-Schicht. Das bedeutet, dass eine Kommunikation auf jeder OSI-Schicht mit eigenen Adressen arbeitet.

Protokoll	Adresse
Anwendung	URL, Domain, E-Mail-Adresse, ...
Transport	Port
Vermittlung	IPv4-Adresse, IPv6-Adresse
Netzzugang	MAC-Adresse (IEEE)

Internet-Adressen ist ein Überbegriff für Netzwerk-Adressen, die im Internet verwendet werden.

Der Aufbau von Netzwerk-Adressen ist meistens hierarchisch. Das bedeutet, für die einzelnen Bestandteile einer Netzwerk-Adresse gibt es verschiedene verantwortliche Stellen. So stellt man sicher, dass Adressen eindeutig sind und deren Zuteilung nicht zu sehr zentralistisch ist.

Ein einfaches Netzwerk: Peer-to-Peer



In einem Peer-to-Peer-Netzwerk ist jeder angeschlossene Computer zu den anderen gleichberechtigt. Jeder Computer stellt den anderen Computern seine Ressourcen zur Verfügung. Ein Peer-to-Peer-Netzwerk eignet sich für bis zu 10 Stationen. Bei mehr Stationen wird es schnell unübersichtlich. Diese Art von Netzwerk ist relativ schnell und kostengünstig aufgebaut. Die Teilnehmer sollten möglichst dicht beieinander stehen.
Einen Netzwerk-Verwalter gibt es nicht. Jeder Netzwerk-Teilnehmer ist für seinen Computer selber verantwortlich. Deshalb muss jeder Netzwerk-Teilnehmer selber bestimmen, welche Ressourcen er freigeben will. Auch die Datensicherung muss von jedem Netzwerk-Teilnehmer selber vorgenommen werden.

Sicherheit in der Netzwerktechnik

Die globale, wie auch lokale, weltweite Vernetzung hat zu einer großen Bedeutung für die Computer- und Netzwerksicherheit geführt. Wo früher vereinzelt kleine Netze ohne Verbindungen nach außen für sich alleine standen, ist heute jedes noch so kleine Netzwerk mit dem Internet verbunden. So ist es möglich, dass aus allen Teilen der

Welt unbekannte Personen, ob mit guter oder böser Absicht, eine Verbindung zu jedem Netzwerk herstellen können.

TCP/IP

TCP/IP ist eine Protokoll-Familie für die Vermittlung und den Transport von Datenpaketen in einem dezentral organisierten Netzwerk. Es wird im LAN (Local Area Network) und im WAN (Wide Area Network) verwendet. Die zentrale Aufgabe von TCP/IP ist dafür Sorgen zu tragen, dass Datenpakete innerhalb eines dezentralen Netzwerks beim Empfänger ankommen. Dafür stellt TCP/IP die folgenden zentralen Funktionen bereit.

Ethernet und WLAN

Ethernet ist eine Familie von Netzwerktechniken, die vorwiegend in lokalen Netzwerken (LAN), aber auch zum Verbinden großer Netzwerke zum Einsatz kommt (WAN). Ethernet wird in der Regel als Synonym für ein lokales Netzwerk verstanden. Im Prinzip werden heute fast alle Vernetzungen im LAN und WAN mit Ethernet-Technik realisiert.

Wireless LAN, kurz WLAN, ist die allgemeine Bezeichnung für ein schnurloses lokales Netzwerk (Wireless Local Area Network). IEEE 802.11 ist ein Standard für eine technische Lösung, die den Aufbau eines Wireless LAN ermöglicht. IEEE 802.11 fand schnell Akzeptanz bei Herstellern und Konsumenten. Deshalb ist es die am weitesten verbreitete drahtlose Technik für ein WLAN.

Virtualisierung im Netzwerk

Typischerweise versteht man unter Virtualisierung den Parallelbetrieb von Betriebssystemen auf einer Hardware. Doch auch in der Netzwerktechnik wird virtualisiert. So lassen sich auf einer Netzwerk-Infrastruktur, bestehend aus Verteilkomponenten und Übertragungswegen, mehrere logisch voneinander getrennte Netzwerke betreiben.

Cloud Computing

Cloud Computing oder Cloud IT umfasst Anwendungen, Daten, Speicherplatz und Rechenleistung aus einem virtuellen Rechenzentrum, das auch Cloud (= Wolke) genannt wird. Die Bezeichnung Cloud wird deshalb verwendet, weil das virtuelle Rechenzentrum aus zusammengeschalteten Computern (Grid) besteht und die Ressource von keinem spezifischen Computer bereitgestellt wird. Die Ressource befindet sich irgendwo in dieser Wolke aus vielen Computern. Eine Anwendung ist keinem Server mehr fest zugeordnet. Die Ressourcen sind dynamisch und bedarfsweise abrufbar.

Grundbegriffe Netzwerktechnik

Folgende Grundbegriffe kommen im Zusammenhang mit Kommunikationssysteme und Netzwerke immer wieder vor. Die Reihenfolge der Grundbegriffe hat didaktische Gründe, weshalb hier auf eine alphabetische Sortierung verzichtet wurde.

LAN und WAN

Netzwerke unterscheidet man häufig in ihrer räumlichen und geografischen Ausdehnung. LAN ist die Abkürzung für Local Area Network. Damit wird oft ein lokal begrenztes Netzwerk bezeichnet, das je nach Organisationsgröße mehrere Tausend Teilnehmer umfassen kann. WAN ist die Abkürzung für Wide Area Network. Damit wird oft ein Weitverkehrsnetzwerk bezeichnet, dass dazu dient kleinere Netzwerke zu einem großen Netzwerk zusammenzuschalten.
Das LAN ist über einen Router mit einem größeren Netzwerk, dem WAN, verbunden. Darüber ist in der Regel eine Verbindung ins Internet möglich.

Node

Ein Node ist ein allgemeiner Begriff für eine physikalisch vorhandene Komponente in einem Netzwerk. Es handelt sich um ein Gerät, dass an einem oder mehreren Netzwerken angeschlossen ist. Dazu verfügt es über eine oder mehrere Schnittstellen. Ein Node kann ganz allgemein ein Host, ein Client oder ein Server sein.

Link

Ein physikalisches Netzwerk bezeichnet man manchmal auch als Link, was Verbindung bedeutet. Zu diesem Netzwerk gehören alle Nodes, die an dem selben Link angeschlossen sind bzw. die direkt miteinander verbunden sind.

Site

Ein Netzwerk und die daran angeschlossenen Nodes bilden eine Site, wenn sie einer gemeinsamen und zusammenhängenden Verwaltung unterstellt sind.
Dieser Begriff ist eher unüblich. Oft ist eine Site das lokale Netzwerk und wird als LAN bezeichnet.

Host

Ein Host ist ein Node ohne Router-Eigenschaft, die damit eine Endstelle in einem Netzwerk darstellt. Typischerweise wird ein Client oder Server als Host bezeichnet.

Knoten

Allgemein formuliert ist ein Knoten ein Verzweigungspunkt in einem Kommunikationsnetzwerk, an dem mehrere Verbindungen zusammenlaufen. Knoten sind im Telefonnetz die Vermittlungsstellen oder auch Telefonanlagen. In einem IP-

Netzwerk sind Router und in einem Ethernet-Netzwerk sind Switche die Knoten. Zugangspunkte zu einem Netzwerk, z. B. WLAN-Access-Points, werden häufig auch als Knoten bezeichnet.

Client

Ein Client ist ein Endgerät oder auch nur eine Software-Komponente, die von einer zentralen Stelle Dienste oder Daten anfordert oder über einen zentralen Zugang am Netzwerk teilnimmt. Der Client ist als Teil der Client-Server-Architektur in größere Zahl in allen Netzwerken zu finden.
Typische Hardware-Clients sind PCs, Smartphones, Tablets und Notebooks. Auf diesen laufen dann mehrere Software-Clients für unterschiedliche Dienste. WWW, E-Mail, Messaging, usw.

Server

Ein Server ist ein Computer, der Rechenleistung, Speicher, Daten und Dienste in einem Netzwerk bereitstellt und Zugriffsrechte verwaltet. Auf dem Server laufen mehrere Dienste und Anwendungen, die von anderen Netzwerk-Teilnehmern mit einem Software-Client über das Netzwerk angefordert werden.

Router

Ein Router ist ein Node, der Pakete weiterleitet, die nicht an ihn selbst gerichtet sind. In einem dezentralen Netzwerk ist der Übertragungsweg der Datenpakete nicht fest vorgegeben. Genau genommen weiß niemand in einem dezentralen Netzwerk über alle Verbindungen Bescheid.
Die einzelnen Router treffen bei jedem eingehenden Datenpaket erneut die Entscheidung, welchen Weg das Datenpaket geht.

Routing

Die Art und Weise, wie Datenpakete in einem dezentralen Netzwerk oder IP-Netzwerk verarbeitet werden, bezeichnet man als Routing. Man könnte Routing auch als Wegfindung bezeichnen. Dabei wird der Weg zum Ziel anhand mehrerer Kriterien (metric) ermittelt. Je mehr Kriterien berücksichtigt werden müssen, desto genauer und gezielter ist der Weg zum Ziel. Aber desto (zeit-)aufwendiger ist die Bestimmung oder Berechnung des Wegs.
In der Regel ist das maßgebliche Kriterium die Zieladresse und damit der kürzeste bzw. schnellste Weg zum Ziel. In gewisser Weise suchen sich die Datenpakete ihren Weg zum Empfänger selber. Beim Routing geht darum den optimalen Weg vom Sender zum Empfänger zu finden.
Das maßgebliche Hilfsmittel beim Routing ist die Routing-Tabelle, in der mögliche Routen festgelegt sind.

Subnetz

Ein Subnetz ist ein oder mehrere LAN-Segmente, die durch Router begrenzt werden und das gleiche IP-Adresspräfix verwenden. Statt Subnetz sind auch die Begriffe Netzwerksegment oder Link gebräuchlich.

Gateway

Ein Gateway ist eine Hardware oder Software oder eine Kombination daraus, die eine Schnittstelle zwischen zwei inkompatiblen Netzwerken darstellt. Das Gateway kümmert sich darum, dass die Form und Adressierung der Daten in das jeweilige andere Format oder Protokoll des anderen Netzes konvertiert werden.

Bridge

Eine Bridge bzw. Netzwerkbrücke verbindet zwei Teilnetze, die auf der Schicht 1 und 2 des OSI-Schichtenmodells arbeiten. Für die Hosts im Netzwerk ist die Bridge transparent, sie können sie nicht sehen.

In den Anfangszeiten von lokalen Netzwerken mit Ethernet stand der Begriff Bridge für ein Gerät zur Kopplung zweier Ethernet-Segmente. Die Bridge war eine wichtige Komponente, um große lokale Netzwerke zu betreiben. Die Segmentierung begrenzt die Größen der Kollisions-Domänen und das Risiko einer Schleifenbildung.

Einen Switch kann man auch als Multiport-Bridge betrachten.

Switching

Switching bedeutet, dass Verbindungen in einem Netzwerk aufgrund von Adressen geschaltet werden. In einem geswitchten Netzwerk bestimmt typischerweise die Empfängeradresse einen konstanten Pfad mit einer definierten Bandbreite, welchen Weg Datenpakete nehmen. Wenn ein Datenpaket abgeschickt wird, steht der Weg durch das Netzwerk praktisch schon fest.

Protokoll

In der Netzwerktechnik ist ein Protokoll der Ablauf einer Kommunikation zwischen zwei Systemen. In der Netzwerktechnik sind die Protokolle meist einer bestimmten Schicht des OSI-Schichtenmodells zugeordnet.

Domäne

Ein Domäne bezeichnet in der Netzwerktechnik ein logisches Subnetz, einen Namensbereich oder ein Objekt, das an der Spitze eines Verwaltungsbereichs steht. Im Zusammenhang mit Verzeichnisdienste und großen lokalen Netzwerken spricht man öfter von einer Domäne.

Ressourcen

In der Netzwerktechnik spricht man häufig von Ressourcen. In der Hauptsache meint man damit Speicher, auf dem man Daten ablegen kann. Dazu zählen aber auch Drucker, Server und andere Netzwerkgeräte, die einen Dienst bereitstellen, der zentral in einem Netzwerk zur Verfügung steht.

Datenpaket / Paket

In der Netzwerktechnik werden einzelne Übertragungseinheiten als Paket oder Datenpaket bezeichnet. Datenpakte werden neben den Daten mit eine Sender- und Empfänger-Adresse ausgestattet. Fehlerkorrektur und Verschlüsselung sind zusätzliche Merkmale.

Frame

Ein Frame ist ein logischer Rahmen, in dem sich ein Bit-Strom befinden. Frames werden von einer Netzwerkkarte oder einem Netzwerk-Interface über ein Übertragungsmedium gesendet und empfangen. Das Frame ist jeweils mit Daten und einem Protokoll-Header und einem Ethernet-Header versehen. Darin sind Start- und Endsequenzen, Kontrollzeichen, Adressen und Prüfsummen enthalten. Frames werden auch Pakete bzw. Datenpakete genannt. In Zusammenhang mit Ethernet bezeichnet man ein Datenpaket als Frame.

Datagramm

Ein Datagramm ist eine in sich geschlossene Einheit. Ein IP-Paket, das an den Netzwerk-Adapter (NIC, Network Interface Card) übergeben wird, wird als Datagramm bezeichnet.

Datenstrom / Datastream / Stream

Datastream oder Stream ist ein Datenstrom aus logisch zusammenhängenden Datenpaketen, die über ein Netzwerk übertragen werden. Die logische Verbindung der Datenpakete ist üblicherweise die Empfänger-Adresse. Auf IP-Ebene wäre das die IP-Adresse. Auf TCP- oder UDP-Ebene wäre das die Portnummer.
Die Datenpakete können aber auch auf der Anwendungsebene eine logische Verbindung zueinander haben.

Port

In der Netzwerktechnik kann ein Port eine Steckverbindung an einem Switch, Router, etc. oder eine logische Assoziation sein. Zum Beispiel der Zugang zum Netzwerk für einen WLAN-Client an einem WLAN-Access-Point.
Der Port bei den Protokollen TCP und UDP ist eine Art Adresse, die die Zuordnung zwischen einem Protokoll und einer Anwendung oder zwischen einem Datenstrom und einer Anwendung definiert.

Ein Port, egal ob logisch oder physisch, wird häufig durch eine Nummer oder Adresse gekennzeichnet.

Unidirektionale Kommunikation

Unidirektional bedeutet "in eine Richtung". Bei der unidirektionalen Kommunikation oder Übertragung zwischen zwei Teilnehmern steht nur ein Kanal zur Verfügung, der nur in eine Richtung genutzt werden kann. Einen Rückkanal gibt es nicht.

Bidirektionale Kommunikation

Bidirektional bedeutet "in beide Richtungen". Bei der bidirektionalen Kommunikation oder Übertragung können Signale, Daten oder Informationen in beide Richtungen fließen. Es gibt zwischen Sender und Empfänger zwei Kanäle. Einen Hin- und einen Rückkanal. Bei der Unterscheidung der Kanäle spricht man auch von Upstream und Downstream bzw. Uplink und Downlink.
Bei der bidirektionalen Übertragung unterscheidet man zwischen Halbduplex, bei der nur jeweils ein Kommunikationspartner senden und empfangen darf, und Vollduplex, bei der beide Kommunikationspartner gleichzeitig senden und empfangen dürfen.

Unicast, Multicast, Broadcast und Anycast

- **Unicast:** Unicast-Adressen adressieren genau einen Host. Die Übertragung erfolgt von einem Host zu einem anderen Host.
- **Multicast:** Hinter einer Multicast-Adresse verbergen sich eine ganze Gruppen von Hosts. Die Übertragung erfolgt von einem Host an mehrere Hosts.
- **Broadcast:** Broadcast-Adressen adressieren alle Hosts. Die Übertragung erfolgt von einem Host an alle anderen Hosts.
- **Anycast:** Anycast-Adressen werden von mehreren Hosts in einem Netzwerk verwendet. Die Übertragung erfolgt von einem Host an einen Host aus einer Gruppe bzw. einem Verbund.

Tunneling

Tunneling bezeichnet ein Verfahren, wenn ein Protokoll-Frame mit allen seinen Eigenschaften als Nutzdaten innerhalb eines anderen Protokolls eingebettet ist.

Masquerading

Masquerading bezeichnet das Verbergen ganzer Netze hinter einer einzigen IP-Adressen.

Masquerading findet ich häufig bei SOHO-Umgebungen, die vom Internet-Provider nur eine IP-Adresse bekommen und hinter dieser sich verschiedene Endgeräte verbergen, die alle eine Verbindung in das Internet benötigen. Das bedeutet, mehrere interne Adressen werden über ein NAT-Verfahren auf eine externe Adresse gebündelt. Von der

externen Seite sind die internen Rechner nicht direkt adressierbar, da von außen nur eine IP-Adresse sichtbar ist.

Bonding

Beim Bonding werden mehrere physikalisch vorhandene Leitungen zu einer logischen Leitung zusammengeschaltet. In der Regel um eine höhere Geschwindigkeit zu erreichen.

Topologie

Die Struktur des Netzwerks wird als Topologie bezeichnet. Bus, Ring und Stern sind typische Netzwerk-Topologien. Die Verbindungen innerhalb der Topologie erfolgt über Funk, Kupfer- oder Glasfaserkabel.

Backbone

Backbone ist eine Bezeichnung für die Hauptübertragungsstrecke in einem Netzwerk. Der Backbone verbindet in der Regel mehrere Netzknoten. Die Netzknoten sind die Zugangspunkte zum Backbone. Man spricht in dem Zusammenhang auch vom Kernnetz oder Core Network.
Bei größeren Vernetzungen mit mehreren Netzwerkstrukturen bildet ein Backbone die Infrastruktur im Hintergrund. Zum Beispiel um lokale Netze und Hochleistungssysteme miteinander zu verbinden. Ein Backbone wird dabei redundant ausgelegt.

Leitungen und Kabel

Die Begriffe Leitungen und Kabel werden häufig gleichwertig verwendet. Doch das ist nicht ganz richtig. Leitungen und Kabel kann man folgender Maßen unterscheiden. Kabel sind Leitungen, die im Boden oder auf hoher See (Meeresboden) verlegt werden. Was man sehen kann sind Leitungen, Kabel sieht man nicht wenn sie genutzt werden.

Umgangssprachlich sagen die meisten Menschen zur Leitung ein Kabel, was falsch (unfachlich) ist. Es ist die häufigste Fehlbenennung in der Elektrotechnik und Informationstechnik, noch vor der Glühbirne.

Kabel ist kürzer und damit das schneller gesprochene Wort. Daher ist der Begriff "Kabel" in vielen Bereichen üblich, auch wenn es falsch ist. So befinden sich auf der Kabeltrommel kein Kabel, sondern eine Leitung. Aber den Begriff Leitungstrommel wird man im Fachhandel sicher nicht finden. Netzwerkleitung sagt auch niemand, obwohl das korrekt wäre.

Netzwerk-Komponenten

In der Netzwerktechnik unterscheidet man zwischen aktiven und passiven Netzwerk-Komponenten. Während aktive Netzwerk-Komponenten eine eigene Logik haben, zählen die passiven Netzwerk-Komponenten zur fest installierten Netzwerk-Infrastruktur.
In der Regel dienen Netzwerk-Komponenten zur Kopplung der Netzwerk-Stationen. Man spricht deshalb auch von Kopplungselementen.

Passive Netzwerk-Komponenten

- Patchkabel und Installationskabel
- Anschlussdose
- Steckverbinder
- Patchfeld / Patchpanel
- Netzwerk-Schrank / Patch-Schrank

Hinweis: Zu den passiven Netzwerk-Komponenten zählen die Bestandteile der Verkabelung. Diese ist im OSI-Schichtenmodell nicht definiert.

Aktive Netzwerk-Komponenten

In kleinen privaten Netzwerken, haben Netzwerk-Komponenten noch klare Bezeichnung, wie Switch oder Router. In großen Unternehmensnetzwerken ist die Benennung der Kopplungselemente nicht immer eindeutig.

Switch

Ein Switch ist ein Kopplungselement, das mehrere Stationen in einem Netzwerk miteinander verbindet. In einem Ethernet-Netzwerk, das auf der Stern-Topologie basiert dient ein Switch als Verteiler für die Datenübertragung.

Router

Router verbinden Netzwerke mit unterschiedlichen Protokollen und Architekturen. Router finden sich häufig an den Außengrenzen eines Netzwerkes. Hier wird die Verbindung zu anderen Netzen und dem Internet geschaffen.

Gateway

Ein Gateway ist eine Hardware oder Software oder eine Kombination daraus, die eine Schnittstelle zwischen zwei inkompatiblen Netzwerken darstellt. Das Gateway kümmert sich darum, dass die Form und Adressierung der Daten in das jeweilige

andere Format und die Protokolle eines anderen Netzes konvertiert werden.

Firewall

Sicherheit ist immer ein Gesamtkonzept, in dem festgelegt ist, was wovor geschützt sein muss, was die Angriffsflächen sind und wie man diese schließt oder minimiert. In einem lokalen Netzwerk ist die Angriffsfläche die Schnittstelle zum Internet.

Server

Was ein "richtiger Server" ist, darüber lässt sich trefflich streiten. In den meisten Fällen wird es ein Computer mit einem leistungsstarken Prozessor, viel Arbeitsspeicher, mehreren Festplatten und großzügiger Netzwerk-Anbindung sein. Auf Servern werden zentrale Aufgaben bearbeitet, verwaltet und gespeichert.

Zuordung im OSI-Schichtenmodell (aktive Komponenten mit Verteilfunktion)

Schicht	Repeater	Hub	Bridge	Switch	Router	Gateway	Firewall
7						x	(x)
6						x	(x)
5						x	(x)
4					(x)	x	x
3				(x)	x	x	x
2			x	x		x	
1	x	x				x	

Software Defined Networking (SDN)

Zu Software Defined Networking, Software Defined Network oder softwaredefiniertes Netzwerk, kurz SDN, gehören Netzwerk-Komponenten, deren Funktionen sich individuell programmieren lassen. Gleichzeit ist eine übergeordnete Steuerung aller Netzwerk-Komponenten möglich.

Netzwerk-Adressen

Netzwerk-Adressen stehen meist in Zusammenhang mit einem bestimmten Übertragungsverfahren, Protokoll oder einer Zweckbindung. Das heißt, Netzwerk-Adressen erfüllen eine bestimmte Aufgabe.
Je nach Zweck weisen sie einen hierarchischen Aufbau auf. Über die OSI-Schichten hinweg ist zwischen den Adressen und Namen eine Adressauflösung oder Namensauflösung notwendig.

Aufgaben von Netzwerk-Adressen

- Informationen über Quelle bzw. Sender (Absender)
- Informationen über Ziel bzw. Empfänger
- Informationen über Weg und Richtung zum Empfänger

Ziele und Adressen im Netzwerk

- Unicast-Adressen: einzelnes Ziel
- Multicast-Adressen: Gruppe von Empfängern
- Broadcast-Adressen: alle Teilnehmer eines Netzwerks

MAC-Adresse

Der Standard IEEE 802.1 definiert den Media Access Control (MAC). Hier wird unter anderem die physikalische Adresse für Netzwerk-Schnittstellen festgelegt. Und das unabhängig von der Übertragungstechnik. Die sogenannte MAC-Adressen gelten zum Beispiel für Ethernet (IEEE 802.3), Bluetooth (IEEE 802.15) und WLAN (IEEE 802.11).

IPv4-Adresse

Die wichtigste Aufgabe von IP (Internet Protocol) ist, dass jeder Host in einem dezentralen TCP/IP-Netzwerk gefunden werden kann. Dazu wird jedem Hardware-Interface (Netzwerkkarte oder -adapter) eine logische IPv4-Adresse zugeteilt.

IPv6-Adresse

Eine IPv6-Adresse ist eine Netzwerk-Adresse, die einen Host eindeutig innerhalb eines IPv6-Netzwerks logisch adressiert. Im Gegensatz zu anderen Adressen hat ein IPv6-Host pro Interface mehrere IPv6-Adressen, die unterschiedliche Gültigkeitsbereiche haben. Zum Beispiel link-lokal und global.

Port-Nummern (TCP und UDP)

TCP- und UDP-Ports sind eine Software-Abstraktion, um parallele Kommunikationsverbindungen einer oder mehrerer Anwendungen voneinander

unterscheiden zu können. Ähnlich wie IP-Adressen zur Adressierung von Rechnern in Netzwerken dienen, adressieren Ports spezifische Anwendungen und ihre Verbindungen, die auf einem Rechner laufen.

Domain-Namen

Ein Domain-Name, kurz Domain, dient dazu, um Computer, die mit kaum merkbaren IP-Adressen adressiert sind, richtige Namen zu geben und gleichzeitig in eine hierarchische Struktur zu unterteilen.

URL

Der URL (nicht die) ist eine "einheitliche Angabeform für Ressourcen" in Netzwerken.

E-Mail-Adresse

Eine E-Mail-Adresse kennzeichnet das ungewöhnliche Zeichen "@" (Klammeraffe). Es wird als Trennzeichen zwischen Nutzername und dem Domain-Namen (Server-Adresse) verwendet. Darin unterscheidet sich die E-Mail-Adresse von anderen Internet- oder Netzwerk-Adressen.

Protokolle und Dienste zur Adressauflösung und Namensauflösung

Zur Adressierung von Computern werden nicht Namen, sondern Nummern verwendet. Es ist nicht möglich, einen Computer direkt mit seinem Namen anzusprechen. Doch numerische Adressen sind für Menschen schwer zu merken und zu verstehen. Doch die digitale Welt besteht aus 1en und 0en (binäre Adresse). Aus diesem Grund wurden Methode entwickelt, um eine Umwandlung bzw. Auflösung von Namen in numerische Adressen und umgekehrt zu realisieren. Dafür gibt es Protokolle und Dienste zur Adressauflösung und Namensauflösung.

IEEE 802

802 ist die Nummer für eine Projektgruppe des IEEE (Institute of Electrical and Electronics Engineers), welches standardisierte Protokolle- und Übertragungstechniken für Local und Metropolitan Area Networks (LAN und MAN) umfasst. Der Name der Projektgruppe 802 ist aus dem Startdatum Februar 1980 abgeleitet. Vom IEEE werden Standards entworfen, Techniken und Themen vorgeschlagen und in Arbeitsgruppen diskutiert.

IEEE 802 ist ursprünglich für LAN-Techniken, wie Ethernet (802.3), Token Bus (802.4) und Token Ring (802.5) verantwortlich. Weitere Projektteile sind Wireless LAN (802.11), Bluetooth (802.15.1) und WiMAX (802.16). Die Zahl hinter dem ersten Punkt kennzeichnet den Standard. Einzelne Standards innerhalb einer Gruppe werden mit einem angehängten Buchstaben oder weiteren Ziffern oder Jahreszahlen gekennzeichnet.

Das Projekt 802 dominiert die Standardisierung von lokalen Netzen, in denen hauptsächlich Ethernet zum Einsatz kommt. Ohne Ethernet und seine vielen Erweiterungen geht es praktisch nicht mehr. Andere Netzwerkstandards spielen nur in Randbereichen eine Rolle.
Neben der Standardisierung neuer Übertragungstechniken hat das IEEE 802 die Aufgabe bestehende Techniken weiter zu entwickeln und für neue Anwendungen zu optimieren. Einige Standards bauen deshalb aufeinander auf oder hängen voneinander ab.

IEEE - Institute of Electrical and Electronics Engineers

Das IEEE (Institute of Electrical and Elektronics Engineers) ist eine internationale Organisation von Fachleuten und Experten aus der Elektrotechnik und dem Ingenieurwesen, ähnlich dem deutschen VDE (Verband der Elektrotechnik, Elektronik und Informationstechnik e. V.).
Das IEEE wurde offiziell am 1.1.1963 gegründet. Damals fusionierten zwei Gremien, die sich mit ähnlichen Aufgabenstellungen beschäftigen.
Das IEEE umfasst über 430.000 Mitglieder in über 160 Ländern und ist damit die weltweit führende Organisation für die Standardisierung im Bereich Elektronik und Informationstechnik. Das Spektrum der Aktivitäten ist extrem breit und unübersichtlich. Nicht alles, was das IEEE entwickelt und standardisiert bringt es zur Marktreife. Die Entwicklung neuer Standards läuft der Entwicklung im Markt meist hinterher. So kommt es vor, dass ein Standard verabschiedet wird, der sich wenig später als überflüssig herausstellt. Trotzdem werden in der Regel nur die Standards genormt, die technisch umsetzbar sind und auch wirtschaftliche Chancen haben.
Das IEEE kennt man vor allem durch Standardisierungen im Bereich Local Area Network (LAN) und Schnittstellen. Die bekanntesten Standards sind 1394 für FireWire, 1284 für die Centronics-Druckerschnittstelle und 802 für Übertragungssysteme im LAN und WAN. Eine vollständige Projektliste ist auf der Webseite des IEEE zu finden.

IEEE 802

Mit der Notwendigkeit Ende der 70er Jahre Standards im Bereich der lokalen Netze einzuführen, wurde das Projekt 802 gegründet. Später wurden auch Standards für Weitverkehrsnetze (WAN) hinzugefügt, die aber nur teilweise so erfolgreich sind, wie das sehr bekannte Ethernet.

2		**802.2** Logical Link Control				
	802.1 Internet-Working	**802.1** Media Access Control				
1		**802.3** Ethernet	**802.4** Token-Bus	**802.5** Token-Ring	**802.11** Wireless LAN	**802.12** AnyLAN

Die Standards der 802-Familie umfassen die physikalische Übertragungsschicht (Physical Layer) bzw. Bitübertragungsschicht (OSI-Schicht 1) und die Verbindungsschicht (Data Link Layer) bzw. die Sicherungsschicht (OSI-Schicht 2). Die Sicherungsschicht (Schicht 2) wird noch einmal in einen Logical-Link-Control (LLC) und einen Medium-Access-Control-Layer (MAC) unterteilt. Das LLC ist für die Übertragung und den Zugriff auf die logische Schnittstelle zuständig. Die MAC-Schicht umfasst die Steuerung des Zugriffs auf das Übertragungsmedium und ist somit für den fehlerfreien Transport der Daten verantwortlich.

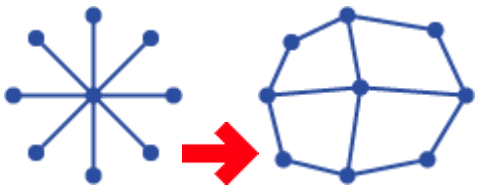
Projekte des IEEE 802

Die folgende Liste ist unvollständig. Sie bildet nur die wichtigsten Standards und Arbeitsgruppen des IEEE ab. Unterstandards und weitere nahezu unbedeutende Standards wurden hier nicht berücksichtigt.

- 802.1: Internet-Working und Media Access Control (MAC)
- 802.2: Logical Link Control (LLC
- 802.3: Ethernet (10Base5) und das CSMA/CD-Zugriffsverfahren
- 802.3i: 10BaseT
- 802.3u: Fast Ethernet (100BaseT)
- 802.3z: Gigabit-Ethernet (1GBaseT)
- 802.3an: 10-Gigabit-Ethernet
- 802.4: Token-Bus-Zugriffsverfahren
- 802.5: Token-Ring-Zugriffsverfahren
- 802.11: Wireless LAN / WiFi
- 802.14: Breitband-Cable-TV (CATV)
- 802.15.1: Bluetooth
- 802.15.3a: UWB - Ultra Wideband Wireless
- 802.16: BWA - Broadband Wireless Access (WiMAX)
- 802.20: Mobile Broadband Wirless Access (MBWA)

Besonders die Projekte 802.3 und 802.11 sind sehr aktiv.

TCP/IP



Die Abkürzung TCP/IP steht für die beiden Protokolle Transmission Control Protocol (TCP) und Internet Protocol (IP). Zusammen mit vielen weiteren Protokollen ist TCP/IP eine Protokoll-Familie für die Vermittlung und den Transport von Datenpaketen in einem dezentral organisierten und globalen Netzwerk. Um hier eine durchgängige Kommunikation von Host zu Host über Netzgrenzen hinweg zu ermöglichen, bedarf es Kommunikationsprotokolle, die im LAN (Local Area Network) und im WAN (Wide Area Network) angewendet werden.
Der Erfolg des Internets, als ein weltweit verfügbares Kommunikationsnetz, ist zum großen Teil auch die Protokolle rund um TCP/IP zu verdanken.

TCP/IP im DoD- und OSI-Schichtenmodell

DoD	Schichtenmodelle	OSI
4. Anwendung	HTTP, FTP, SMTP, POP, IMAP, ...	**7. Anwendung**
		6. Darstellung
		5. Kommunikation
3. Transport	TCP / UDP	**4. Transport**
2. Vermittlung	IPv4 / IPv6	**3. Vermittlung**
1. Netzzugang	IEEE 802.3 (Ethernet), IEEE 802.11 (WLAN), ...	**2. Sicherung**
		1. Bitübertragung

Innerhalb des DoD- und OSI-Schichtmodells bildet TCP/IP das Rückgrat für alle Kommunikationsverbindungen.

Aufgaben und Funktionen von TCP/IP

Die zentrale Aufgabe von TCP/IP ist dafür Sorgen zu tragen, dass Datenpakete innerhalb eines dezentralen Netzwerks beim Empfänger ankommen. Dafür stellt TCP/IP die folgenden zentralen Funktionen bereit.

- Logische Adressierung / Logical Addressing (IP)
- Wegfindung / Routing (IP)
- Fehlerbehandlung und Flussteuerung / Error Control and Flow Control (TCP)
- Anwendungsunterstützung / Application Support (TCP/UDP)
- Namensauflösung / Name Resolution (DNS)

Die Besonderheiten und Probleme der paketorientierten Datenübertragung sind sehr vielfältig und erfordern deshalb spezielle Lösungen und Funktionen, die an dieser Stelle nicht alle berücksichtigt werden. Die folgende Darstellung und Beschreibung ist also nur eine Auswahl der wichtigsten Funktionen.

Logische Adressierung / Logical Addressing (IP)

In einem einfachen, lokalen Netzwerk empfängt jeder Netzwerk-Adapter jedes Datenpaket. Das ist dann der Fall, wenn sich prinzipbedingt alle Netzwerk-Teilnehmer das Übertragungsmedium teilen müssen (z. B. bei WLAN oder Ethernet). Bei Netzwerken mit wenigen Teilnehmern ist das eine praktikable Lösung. Doch in einem Netzwerk mit vielen Tausend oder sogar Millionen Teilnehmern ist es wenig sinnvoll, wenn Datenpakete in Teile des Netzwerks gelangen, in denen nicht das Ziel liegt. Ob ein Datenpaket seinen richtigen Empfänger erreicht, wäre dann dem Zufall überlassen. Deshalb bedarf es einer Möglichkeit das Netzwerk physikalisch (Topologie) und auch logisch (Adressierung) zu strukturieren. Innerhalb von TCP/IP übernimmt das Internet Protocol (IP) die logische Adressierung von Netzwerken und deren Teilnehmern. Dabei gelangen Datenpakete nur in das Netz, in dem sich das Ziel befindet. Die Verfahren der Adressierung sind zum Beispiel fest definierte Netzklassen, Subnetting und CIDR.

Wegfindung / Routing (IP)

Während die logische Adressierung durch IP dafür sorgt, dass ein großes Netzwerk in Segmente geteilt wird, sorgt Routing als eine Art Wegfindung dafür, dass ein Datenpaket sein Ziel über die einzelnen Netzwerk-Segmente erreicht. Für jedes einzelne Datenpaket wird in jedem Netzknoten auf dem Weg vom Sender zum Empfänger, der nächste Netzknoten ermittelt. Auf diese Weise findet ein Datenpaket den Weg zu seinem Empfänger, auch wenn der in einem unbekannten Netzwerk-Segment liegt.

Fehlerbehandlung und Flussteuerung / Error and Flow Control (TCP)

Durch TCP stehen Sender und Empfänger ständig in Kontakt zueinander (Verbindungsmanagement). Obwohl es sich eher um eine virtuelle Verbindung handelt, werden während der Datenübertragung ständig Kontrollmeldungen ausgetauscht, weshalb man von einer verbindungsorientierten Kommunikation spricht. Wird ein Fehler festgestellt, wird das betreffende Datenpaket erneut übertragen. Zusätzlich ist eine Daten-Flusssteuerung notwendig, um die verfügbare Übertragungsgeschwindigkeit auszunutzen. Weil es im Internet für eine Ende-zu-Ende-Verbindung keinen exklusiven Kanal mit fester Übertragungsgeschwindigkeit gibt, bedarf es hier einer automatischen Anpassung.

Anwendungsunterstützung / Application Support (TCP/UDP)

Ähnlich wie Rechner mit IP-Adressen in Netzwerken adressiert werden, bedarf es einer Unterscheidung der Kommunikationsverbindungen zwischen spezifischen Anwendungen, die gemeinsam auf einem Rechner laufen. TCP- und UDP-Ports (Nummern) bilden eine Software-Abstraktion, um spezifische Anwendungen und deren Kommunikationsverbindungen voneinander unterscheiden zu können.

Namensauflösung / Name Resolution (DNS)

In einem TCP/IP-Netzwerk werden Verbindungen zwischen den Netzwerk-Teilnehmern mit IP-Adressen aufgebaut. Eine IP-Adresse hat ursprünglich die binären Form bzw. Schreibweise und ist damit eine Folge von 1en und 0en, mit denen elektronische Schaltungen und digitale Programme arbeiten. Zur besseren Lesbarkeit werden IP-Adressen in der dezimalen (IPv4) oder hexadezimalen (IPv6) Schreibweise dargestellt. Doch weder die Bitfolge, noch eine andere Schreibweise sind für das menschliche Gehirn einfach zu erfassen und zu merken. Der Mensch verwendet lieber Namen um eine Sache zu benennen und zu identifizieren. Deshalb werden statt IP-Adressen eher Namen zur Adressierung auf der Anwendungsebene verwendet. Damit eine Verbindung auf IP-Ebene möglich ist, ist eine Namensauflösung notwendig. Gemeint ist, dass zu einem Computer- oder Domain-Namen eine zugehörige IP-Adresse ermittelt werden muss. Man bezeichnet das als Namensauflösung.

Vorteile von TCP/IP

TCP/IP hat mehrere entscheidende Vorteile. Jede Anwendung ist mit TCP/IP in der Lage über jedes Netzwerk Daten zu übertragen und auszutauschen. Dabei ist es egal, wo sich die Kommunikationspartner befinden. Das Internet Protocol (IP) sorgt dafür, dass das Datenpaket sein Ziel erreicht und das Transmission Control Protocol (TCP) steuert die Datenübertragung und sorgt für die Zuordnung von Datenstrom und Anwendung.

Für die Anwendungen soll die Art und Weise der physikalischen und logischen Datenübertragung keine Rolle spielen. Der Anwender soll sich auch nicht um Verbindungsaufbau und -abbau kümmern müssen. So lange der Anwender eine korrekte Adresse kennt, wird sich TCP/IP um den Verbindungsaufbau, -abbau und die Übertragung zum Ziel kümmern. Ganz egal welche Anwendung oder welcher Übertragungsweg verwendet wird.

- TCP/IP ist ein weltweit gültiger Standard und an keinen Hersteller gebunden.
- TCP/IP kann auf einfachen Computern und auf Supercomputern implementiert werden.
- TCP/IP ist in LANs und WANs nutzbar.
- TCP/IP macht die Anwendung vom Übertragungssystem unabhängig.

Nachteile von TCP/IP

Allerdings ist TCP/IP alles andere als eine effiziente Methode um Daten zu übertragen.

Die Daten werden in kleine Datenpakete aufgeteilt. Damit der Empfänger eines Datenpakets weiß, was er damit machen soll, wird dem Datenpaket ein Kopfdatensatz, der als Header bezeichnet wird, vorangestellt. Pro Datenpaket ergibt sich ein Verwaltungsanteil von mindestens 40 Byte pro TCP/IP-Datenpaket. Nur wenn Datenpakete von mehreren kByte gebildet werden, bleibt der Verwaltungsanteil im Vergleich zu den Nutzdaten (Payload) gering.

Wenn die Anwendung bestimmte Anforderungen an das Übertragungssystem stellt, dann lässt sich das nur sehr schwer realisieren. Die systeminterne Kommunikation zwischen Anwendung und Übertragungssystem über TCP/IP hinweg ist nicht vorgesehen.
Auch lässt sich ein koordinierten Austausch von Verbindungsqualität und -anforderungen zwischen Netzknoten nur sehr schwer netzüberbreifend realisieren. Es gibt zwar Quality of Service (QoS). Doch das ist optional und erfordert die Kontrolle über das Netzwerk, was in einem dezentral organisierten Netzwerk, wie dem Internet, nicht vorgesehen ist.

Man spricht in diesem Zusammenhang auch von Netzneutralität. Die Netzneutralität fordert, dass jedes Paket gleich behandelt wird. Das hat den Nachteil, dass bestimmte Datenpakete nicht priorisiert werden können. Das hat wiederum die Konsequenz, dass bestimmte Anwendungen im Internet mit TCP/IP nicht gut funktionieren.

IP - Internet Protocol

Das Internet Protocol, kurz IP, hat maßgeblich die Aufgabe, Datenpakete zu adressieren und in einem verbindungslosen paketorientierten Netzwerk zu vermitteln (Routing). Dazu haben alle Hosts und Endgeräte eine eigene IP-Adresse. Die IP-Adresse dient nicht nur zur Adressierung einzelner Hosts, sondern ganzer Netze. Beim IP-Routing geht es nicht darum, Datenpakete an bestimmte Hosts zu schicken, sondern die Pakete ins richtige Netzwerk zu leiten.
Man unterscheidet zwischen IPv4 und dem Nachfolger IPv6.

TCP - Transmission Control Protocol

In der TCP/IP-Protokollfamilie übernimmt TCP, als verbindungsorientiertes Protokoll, die Aufgabe der Anwendungszuordnung, der Daten-Flusssteuerung und ergreift Maßnahmen bei einem Paketverlust. Die Funktionsweise von TCP besteht darin, die Dateien oder den Datenstrom von den Anwendungen entgegen zu nehmen, aufzuteilen, mit einem Header zu versehen und an das Internet Protocol (IP) zu übergeben.
Beim Empfänger werden die Datenpakete in die richtige Reihenfolge wieder zusammengesetzt und der richtigen Anwendung übergeben. Die Zuordnung erfolgt über eine Port-Nummer. Durch die Ports ist es möglich, dass mehrere Anwendungen gleichzeitig Verbindungen zu unterschiedlichen Kommunikationspartnern aufbauen können.
Der kleine Bruder von TCP ist UDP, das ein abgespecktes Transport-Protokoll ist.