



Dirk
Jarzyna

TCP/IP

Grundlagen, Adressierung, Subnetting



Verlagsgruppe
Hüthig Jehle Rehm

Hinweis des Verlages zum Urheberrecht und Digitalen Rechtemanagement (DRM)

Der Verlag räumt Ihnen mit dem Kauf des ebooks das Recht ein, die Inhalte im Rahmen des geltenden Urheberrechts zu nutzen. Dieses Werk, einschließlich aller seiner Teile, ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und Einspeicherung und Verarbeitung in elektronischen Systemen.

Der Verlag schützt seine ebooks vor Missbrauch des Urheberrechts durch ein digitales Rechtemanagement. Bei Kauf im Webshop des Verlages werden die ebooks mit einem nicht sichtbaren digitalen Wasserzeichen individuell pro Nutzer signiert.

Bei Kauf in anderen ebook-Webshops erfolgt die Signatur durch die Shopbetreiber. Angaben zu diesem DRM finden Sie auf den Seiten der jeweiligen Anbieter.

Dirk Jarzyna

TCP/IP – Grundlagen, Adressierung, Subnetting



mitp

Bibliografische Information der Deutschen Nationalbibliothek

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

ISBN 978-3-8266-9553-7

I. Auflage 2013

www.mitp.de

E-Mail: kundenbetreuung@hjr-verlag.de

Telefon: +49 6221 / 489 -555

Telefax: +49 6221 / 489 -410

© 2013 mitp, eine Marke der Verlagsgruppe Hüthig Jehle Rehm GmbH Heidelberg, München, Landsberg, Frechen, Hamburg

Dieses Werk, einschließlich aller seiner Teile, ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Lektorat: Ernst Heinrich Profener

Sprachkorrektur: Jürgen Dubau

Satz: III-satz, Husby, www.drei-satz.de

Inhaltsverzeichnis

	Einführung	11
Teil I	TCP/IP-Grundlagen	15
1	Das TCP/IP- und OSI-Netzwerkmodell	17
1.1	Die TCP/IP-Architektur	18
1.1.1	Die TCP/IP-Anwendungsschicht	20
1.1.2	Die TCP/IP-Transportschicht	22
1.1.3	Die TCP/IP-Internetschicht	24
1.1.4	Die TCP/IP-Netzzugangsschicht	25
1.2	Das OSI-Referenzmodell	27
1.2.1	Einordnung der Komponenten und Protokolle ins OSI-Referenzmodell	30
1.2.2	OSI und TCP/IP	31
1.2.3	OSI-Einkapselung	33
1.3	Das weiß ich nun	33
2	Routing und IP-Adressierung	35
2.1	Funktionen der Vermittlungsschicht	35
2.1.1	Routing	36
2.1.2	Das Zusammenspiel von Vermittlungs- und Sicherungsschicht	37
2.1.3	IP-Paket und IP-Header	38
2.1.4	Adressierung auf Ebene der Vermittlungsschicht	40
2.1.5	Routing-Protokolle	40

2.2	IPv4-Adressierung	41
2.2.1	Ein paar IP-Adressbegriffe	41
2.2.2	Wie IP-Adressen gruppiert werden	42
2.2.3	Netzwerkklassen	43
2.3	IP-Routing	50
2.3.1	Routing-Logik der Hosts	51
2.3.2	Routing-Entscheidungen und IP-Routing-Tabellen.	51
2.4	IP-Routing-Protokolle	52
2.5	Utilities der Vermittlungsschicht.	53
2.5.1	DNS und ARP	54
2.5.2	Adresszuweisung und DHCP	57
2.5.3	ICMP Echo und Ping	61
2.6	Das weiß ich nun	63
3	TCP/IP-Transport	65
3.1	Das Transmission Control Protocol.	65
3.1.1	Multiplexing über Port-Nummern	69
3.1.2	Flusssteuerung.	71
3.1.3	Verbindungsauf- und -abbau	72
3.1.4	Geordnete Datenübertragung und Segmentierung.	73
3.2	Das User Datagram Protocol	74
3.3	Das weiß ich nun	75
4	IP-Adressierung und Subnetting	77
4.1	IP-Adressierung	77
4.1.1	Öffentliche und private Adressen	79
4.1.2	IPv6-Adressierung.	80
4.2	Subnetting	81
4.2.1	Präfixnotation.	82
4.2.2	Subnetzmasken analysieren und auswählen.	85
4.2.3	Existierende Subnetze analysieren	92
4.2.4	Die Subnetze eines klassenbezogenen Netzwerks.	97

4.3	Variable-Length Subnet Masking (VLSM)	101
4.3.1	Klassenbezogene und klassenlose Routing-Protokolle	102
4.3.2	Überlappende VLSM-Subnetze	103
4.3.3	Ein Subnetzschemata mit VLSM entwerfen.	104
4.4	Das weiß ich nun	107
5	Routing	109
5.1	Direkt verbundene und statische Routen	109
5.1.1	Direkt verbundene Routen	109
5.1.2	Statische Routen	111
5.2	Routing-Protokolle	112
5.2.1	Interior- und Exterior-Routing-Protokolle	113
5.2.2	Klassenloses und klassenbezogenes Routing	114
5.2.3	Automatische und manuelle Routen-Zusammenfassung	115
5.2.4	Algorithmen	115
5.2.5	Routing-Metrik.	116
5.2.6	Konvergenz	116
5.3	Default- oder Standardrouten	118
5.4	Das weiß ich nun	119
6	Network Address Translation	121
6.1	Das NAT-Konzept	122
6.2	Ein (NAT-)Problem	124
6.3	Mögliche Probleme	124
6.4	Nachteile von NAT	125
Teil II	IP Version 6	127
7	IPv6-Adressen	129
7.1	Der Aufbau einer IPv6-Adresse	130
7.1.1	IPv6-Präfixe	131
7.1.2	Subnetting im Unternehmen	132

7.2	Global-Unicast-Adressen	135
7.2.1	Effizientes Routing	137
7.2.2	Adresszuweisung	139
7.3	Weitere IPv6-Adressen	140
7.3.1	Unicast-IPv6-Adressen	141
7.3.2	Multicast und spezielle IPv6-Adressen	143
7.4	Das weiß ich nun	145
8	Adresskonfiguration	147
8.1	Interface-ID und das EUI-64-Format	148
8.2	Statische Konfiguration	150
8.3	Autokonfiguration	153
8.3.1	DHCPv6	154
8.3.2	Stateless Autokonfiguration	155
8.4	Das weiß ich nun	163
9	IPv6-Routing	165
9.1	Routing-Protokolle für IPv6	166
9.1.1	RIPng	167
9.1.2	OSPFv3	168
9.2	Zusammenfassung	170
10	IPv6-Optionen für den Übergang	171
10.1	Dual-Stacks	172
10.2	Tunneling	174
10.2.1	Manually Configured Tunnel (MCT)	175
10.2.2	Dynamischer 6to4-Tunnel	177
10.2.3	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)	178
10.2.4	Teredo-Tunneling	183
10.3	Übersetzung zwischen IPv4 und IPv6	188
10.4	Fazit	190
11	IPv6-Campus-Deployment	193
11.1	Deployment-Strategie	193
11.1.1	Deployment-Plan	194

II.2	Adressierung	195
	II.2.1 Adresszuweisung	198
II.3	Deployment-Optionen	199
	II.3.1 Routing-Protokolle	202
II.4	DNS-Überlegungen	202
	II.4.1 DNS mit IPv6	203
II.5	Kleinere Szenarios	204
	II.5.1 IPv6-Connectivity für Heimanwender	204
	II.5.2 IPv6-Testumgebung	205
	II.5.3 Verteilte IPv6-Hosts	205
12	Netzwerkmanagement	207
12.1	Basisanforderungen	207
12.2	Standards	208
	12.2.1 SNMP für IPv6	208
	12.2.2 Andere Standards	210
	12.2.3 Netflow und IPFIX	210
12.3	Managementwerkzeuge	211
	12.3.1 Managementwerkzeuge für das Core-Netzwerk	212
	12.3.2 Managementwerkzeuge für das lokale Netzwerk	215
	12.3.3 Managementwerkzeuge für jedes Netzwerk	218
	12.3.4 Empfehlungen für den Administrator	220
13	Sicherheit	223
13.1	Sicherheitsbedrohungen	223
	13.1.1 Reconnaissance oder Informations- beschaffung	223
	13.1.2 Unautorisierter Zugriff	225
	13.1.3 Spoofing	225
	13.1.4 Stören der Host-Initialisierung	226
	13.1.5 Broadcast-Storms	226
	13.1.6 Angriffe gegen die Routing-Infrastruktur	227

13.1.7	Sniffing oder Abfangen von Daten.....	228
13.1.8	Man-in-the-Middle-Angriffe	228
13.1.9	Angriffe auf die Anwendungsschicht.....	228
13.1.10	Denial-of-Service-Angriffe.....	228
13.2	IPSec	229
13.3	Sichere Autokonfiguration	230
13.3.1	Privacy-Extensions	230
13.3.2	DHCPv6.....	231
13.3.3	Statische Adresskonfiguration	231
13.3.4	Falsche Router-Advertisements	231
A	Das weiß ich nun – Auflösung.....	233
B	Der IPv6-Header.....	237
	Stichwortverzeichnis.....	241

Einführung

Über TCP/IP sind schon viele Bücher geschrieben worden, dicke und dünne, leicht verständliche, schwer verdauliche, rote und blaue. Kein origineller Einfall also, ein weiteres hinzuzufügen. So war ursprünglich auch geplant, ein Buch ausschließlich über IPv6-Grundlagen zu schreiben. Doch schon zu Beginn der Arbeit wurde klar, dass es kaum möglich ist, einfach bei IPv6 einzusteigen, ohne zuvor über IP in der Version 4 oder TCP/IP allgemein geschrieben zu haben. Denn IPv6 baut in vielerlei Hinsicht auf IPv4 auf, und es ist deutlich einfacher, IPv6 zu verstehen, wenn IPv4 verstanden ist. Da man nicht unbedingt bei jedem an IPv6 interessierten Leser ein solides Grundverständnis von IPv4 voraussetzen kann, erschien es mir notwendig, in den ersten Kapiteln dieses Buchs ein solches Grundverständnis aufzubauen. Entstanden ist so schließlich ein Buch, das Grundwissen über IPv4 bzw. TCP/IP und IPv6 zu gleichen Teilen vermittelt. Tatsächlich nimmt sich dieses Buch bestimmte IPv4-Themen sehr gründlich vor. Das betrifft beispielsweise die mit IPv4-Adressen verbundene Mathematik. Ich habe die Erfahrung gemacht, dass zwar viel über IP-Adressen und Subnetting geschrieben wird, aber der Interessierte kaum eine gründliche Anleitung findet, die ihm dabei hilft, Subnetting in der Praxis durchzuführen.

In diesem Buch geht es also generell um TCP/IP. Deshalb war der für die erste Auflage dieses Buchs genutzte Titel »IPv6 – Das Praxisbuch« unglücklich gewählt. Ich bin zwar der Auffassung, dass das Buch tatsächlich alle für die Praxis relevanten Aspekte von IPv6 behandelt, aber der Titel war definitiv irreführend. Der Titel »TCP/IP – Grundlagen, Adressierung, Subnetting trifft den Inhalt genauer. Aber natürlich befasst sich ein großer Teil des Buches mit IPv6. Und das aus gutem Grund:

Die Netzwerk- und Internetwelt hat sich im Laufe der letzten Jahre dramatisch verändert: Ethernet feierte im Mai 2013 seinen vierzigsten Geburtstag! Das Internet ist riesig geworden und gereift, die Netzwerktechnik hat sich weiterentwickelt, und neue Technologien, die vor zehn, zwanzig Jahren noch unbekannt waren, sind heute allgegenwärtig und erlauben es den Menschen, miteinander zu kommunizieren, Dokumente, Bilder, Musik, Videos und Gummibärchen auszutauschen und von fast jedem Ort der Erde aus auf Daten zuzugreifen, die an irgendeinem anderen Ort auf der Erde gespeichert sind. Noch vor zwanzig Jahren gab es kein globales Netzwerk, mit dem sich interessierte Zeitgenossen einfach so verbinden konnten. Erst vor rund zehn, zwölf Jahren war das öffentliche Internet an dem Punkt angelangt, wo sich Menschen in den meisten Teilen der Welt mit ihm verbinden konnten. Selbst zur Jahrtausendwende waren die typischen Internetbenutzer überwiegend Menschen mit einem Faible für Computertechnik oder Benutzer, die das Internet beruflich nutzten. Heute scheint praktisch jeder aufs Internet zuzugreifen – über PCs, mobile Geräte, Telefone, Fernsehgeräte, Radios und sogar Kühlschränke. Und das mit dem Kühlschrank ist ernst gemeint.

So gut wie jedes Mobiltelefon unterstützt Internetverkehr und benötigt deshalb eine IP-Adresse. Dies gilt auch für moderne TV-Geräte, für Internet-Radios sowieso. Viele neue Autos können eine IP-Adresse beziehen und nutzen. Einige Hardwarehersteller sind der Meinung, wirklich jede ihrer Appliances benötige unbedingt die Fähigkeit, sich mit dem Internet zu verbinden. Selbst Nintendo hat den Gameboy zum IP-Adressen-Konsumenten weiterentwickelt, indem das Unternehmen ihm einen kleinen Web-Browser und ein paar weitere Funktionen eingepflanzt hat. Die riesige Zahl der Internetbenutzer und fast explosionsartig zunehmende Anzahl internetfähiger Endgeräte hat Auswirkungen: Die verfügbaren IP-Adressen (IPv4) sind so gut wie erschöpft. Das bedeutet nicht, dass sich Netzwerkfachleute nicht mehr mit IPv4 beschäftigen müssen, denn die riesige Zahl IPv4 nutzender Geräte will ja nach wie vor gemanagt werden, sondern es bedeutet, dass nun zusätzlich IPv6-Kenntnisse erforderlich sind.

»Irgendwann innerhalb der nächsten sechs Jahre wird die Menge der noch zuteilbaren IPv4-Adressen verbraucht sein.« Dies schrieb in ähnlicher Form die *Information Week*, und zwar bereits am 21. Mai 2007 (www.informationweek.com, »The Impending Internet Address Shortage«). Diese Situation ist inzwischen eingetreten.

Das bedeutet, dass die Migration zum neuen Internet-Protokoll IPv6 beschleunigt werden muss, um die sich abzeichnende Katastrophe ein für alle Mal zu stoppen.

Die Migration zu IPv6 wird durch den Bedarf nach immer mehr Adressen getrieben werden. Außerdem steigt die Nachfrage nach IPv6 durch den Druck der Behörden: Die US-Regierung setzte bereits ein Datum im Jahr 2008, bis zu dem sämtliche Einrichtungen, Behörden, Ämter und Agenturen der Regierung ihre Core-IP-Netzwerke auf IPv6 umgestellt haben sollten. Inzwischen haben wir 2013, die Sache dürfte also längst erledigt sein. Ob dies tatsächlich so ist, war mir nicht wichtig genug, um es zu recherchieren. Als Signal taugt diese Regierungsinitiative auf jeden Fall.

Die Frage, die sich IT-Verantwortlichen stellt, lautet nicht mehr, ob sie zu IPv6 migrieren, sondern *wann* sie dies tun.

Die zwei wichtigsten Gründe für die Migration zu IPv6 wurden genannt: der Bedarf nach mehr Adressen und die Vorgaben durch Behörden. Daneben gibt es aber noch viele weitere Gründe, die IP-Verantwortliche eine Migration in Angriff nehmen lassen sollten, darunter folgende:

- Adresszuweisungsfunktionen: Die IPv6-Adresszuweisung erlaubt dynamische Zuteilung, leichtere Änderung und die Wiederherstellung von Adressen.
- Kein Bedarf für NAT und PAT: Durch Nutzung öffentlich registrierter eindeutiger Adressen auf allen Geräten entfällt die Notwendigkeit von Netzwerkadress- und Port-Übersetzungen. Ein angenehmer Nebeneffekt ist die Beseitigung einiger Anwendungsschicht- und VPN-Tunneling-Probleme, die NAT sonst bereitet.

- **Aggregation:** Der riesige Adressbereich von IPv6 erlaubt eine viel leichtere Zusammenfassung von Adressblöcken im Internet.
- **IPSec:** IPSec funktioniert natürlich sowohl mit IPv4 als auch mit IPv6, ist auf IPv6-Hosts jedoch zwingend erforderlich. Man kann also darauf vertrauen, dass IPSec vorhanden ist, beispielsweise für VPN-Tunneling.
- **Header-Verbesserungen:** Router müssen nicht mehr für jedes Paket eine Header-Prüfsumme berechnen, was natürlich den Overhead pro Paket reduziert. Außerdem enthält der Header ein Flow-Label, das die leichte Identifizierung von Paketen erlaubt, die über dieselbe einzelne TCP- oder UDP-Verbindung gesendet werden.

Selbstverständlich wird die weltweite Migration von IPv4 zu IPv6 kein einmaliges Ereignis sein. Ja selbst innerhalb von ein, zwei Jahren wird sie nicht erledigt sein. Stattdessen wird sie ein sehr langfristiger Prozess sein, der – siehe die Regierung der USA – bereits begonnen hat. IT-Verantwortliche, Netzwerkadministratoren und System Engineers werden zunehmend mehr über IPv6 lernen müssen. Dieses Buch ist eine Informationsquelle dafür.

IPv6 wurde nicht von Grund auf neu erfunden, sondern bedient sich bei einigen Konzepten, Methoden und Strategien durchaus bei IPv4. Andererseits unterscheidet es sich in vielen Punkten signifikant von IPv4. Um IPv6 zu verstehen, bietet es sich deshalb an, beide Protokollfamilien miteinander zu vergleichen. Dieses Buch tut genau dies an vielen Stellen. Im ersten Teil des Buchs findet der Leser alles wirklich Wissenswerte zu TCP/IP und IPv4, im zweiten Teil geht es dann ausschließlich um IPv6.

Dieses Buch erhebt keinen Anspruch auf Vollständigkeit; es beschreibt Dinge, die für die Praxis relevant sind. Sie finden hier also beispielsweise keine Listen, die jedes einzelne Bit einer DHCP-Acknowledgment-Nachricht beschreiben, sondern Sie erfahren hier, wozu DHCP dient, wie es grundsätzlich funktioniert und wo Sie es bei Bedarf herbekommen.

Teil I

TCP/IP- Grundlagen

Das TCP/IP- und OSI-Netzwerkmodell

Es existiert heute kaum ein Computer, der die TCP/IP genannte Netzwerkprotokollsammlung nicht unterstützt. Das liegt daran, dass heute so gut wie jeder Computer mit dem Internet verbunden ist und deshalb gar nicht darum herum kommt. Jedes Betriebssystem, ob Windows, Linux oder Unix, unterstützt TCP/IP. Selbst die sogenannten digitalen Assistenten (PDAs) und neueren Mobiltelefone unterstützen TCP/IP. Netzwerk-Switches unterstützen TCP/IP und Router natürlich ebenfalls, denn sonst könnten sie ihre Aufgabe, Daten über lokale Netzwerke und das Internet an den richtigen Adressaten weiterzuleiten, gar nicht erledigen.

So einfach war es nicht immer. Es ist noch nicht besonders lange her, da gab es keine Netzwerkprotokolle – auch kein TCP/IP. Computerhersteller erfanden die ersten Netzwerkprotokolle, die aber zunächst nur die Systeme genau dieses Herstellers unterstützten. Die Details der Implementierung wurden als Geheimnis gehütet. Irgendwann erkannten die Hersteller aber die Notwendigkeit, ihre Computer auch mit Computern und Geräten anderer Hersteller kommunizieren zu lassen, und veröffentlichten ihre Netzwerkprotokolle. IBM veröffentlichte beispielsweise 1974 ihr Netzwerkmodell *Systems Network Architecture* (SNA). Daraufhin entwickelten andere Hersteller Produkte, mit deren Hilfe ihre Computer über SNA mit den Computern von IBM kommunizieren konnten. Das funktionierte tadellos, hatte aber unter anderem den Nachteil, dass die großen Hersteller sagen konnten, wo es im Netzwerkmarkt langgeht. Dieses Problem ist noch immer nicht so ganz gelöst ...

Eine bessere Lösung war es jedenfalls, ein offenes standardisiertes Netzwerkmodell zu schaffen, das alle Hersteller unterstützen. In den später 1970er Jahren nahm sich die *International Organization for Standardiza-*

tion (ISO) dieser Aufgabe an und begann, an etwas zu arbeiten, das wir heute als *Open-Systems-Interconnection-* oder *OSI-Netzwerkmodell* kennen. Das Ziel des OSI-Modells war von Anfang an, Netzwerkprotokolle zu standardisieren, um die Kommunikation zwischen allen Computern auf der Welt zu ermöglichen.

Dem US-Verteidigungsministerium verdanken wir nicht nur Patriot-Raketen sondern auch ein zweites standardisiertes offenes Netzwerkmodell. Verschiedene amerikanische Universitäten entwickelten (freiwillig) im Auftrag des Ministeriums Netzwerkprotokolle. Diese Arbeit resultierte in ein konkurrierendes Netzwerkmodell mit dem Namen TCP/IP.

Ende der 1980er Jahre gab es viele konkurrierende proprietäre Netzwerkmodelle, darunter beispielsweise auch Novells IPX/SPX, und zwei konkurrierende standardisierte Netzwerkmodelle (OSI und TCP/IP). Was passierte, wissen wir: Am Ende setzte sich TCP/IP durch, nicht nur unter den zwei standardisierten Modellen, sondern es verdrängte auch viele der proprietären Protokolle.

Dieses Kapitel liefert die Grundlagen zu TCP/IP. Es beschreibt, was das TCP/IP-Netzwerkmodell ist und wie es funktioniert. Da in Verbindung mit TCP/IP immer wieder Begriffe auftauchen, die sich auf OSI beziehen, ist es notwendig, auch kurz auf das OSI-Modell einzugehen.

1.1 Die TCP/IP-Architektur

TCP/IP definiert eine große Anzahl von Protokollen, die Computern erlauben, miteinander zu kommunizieren. Allerdings sind es nur einige wenige Protokolle, die tatsächlich als »Hauptprotokolle« betrachtet werden. Von diesen wenigen Schlüsselprotokollen gelten zwei Protokolle als die wichtigsten: Das *Internet Protocol* (IP) übernimmt die Adressierung, das Datagram-Routing und weitere Funktionen in einem Internetzwerk. Das *Transmission Control Protocol* (TCP) ist das primäre Protokoll der Transportschicht; es ist verantwortlich für den Verbindungsaufbau und das Verbindungsmanagement und sorgt für einen zuverlässigen Datentransport zwischen Softwareprozessen auf Geräten. Die Details aller Protokolle der TCP/IP-Suite sind in Dokumenten beschrieben, die *Request*

for Comments (RFCs) genannt werden. Wer die in den TCP/IP-RFCs beschriebenen Protokolle in einen Computer implementiert, kann relativ sicher sein, dass dieser Computer mit anderen Computern kommunizieren kann, die ebenfalls TCP/IP implementiert haben.

Wie andere Netzwerkarchitekturen verteilt TCP/IP die verschiedenen Protokolle auf unterschiedliche Schichten oder Layers eines Architektur- oder Schichtenmodells. Ein solches Modell hilft, die einzelnen Komponenten und deren Funktionen zu beschreiben. Als klassisches Schichtenmodell wird zwar das 1979 definierte OSI-Modell angesehen. *Protokollschichtenkonzepte* existierten allerdings schon lange, bevor sie durch das OSI-Modell formalisiert wurden. Ein Beispiel dafür ist eben die TCP/IP-Protokollarchitektur. Da TCP/IP historisch eng mit dem *Department of Defence* (US-Verteidigungsministerium) verknüpft ist, wird das TCP/IP-Schichtenmodell auch als *DoD-Modell* bezeichnet.

Tabelle 1.1 zeigt die Hauptkategorien des TCP/IP-Architekturmodells.

TCP/IP-Layer (Schicht)	Beispielprotokolle
Application (Anwendungsschicht)	HTTP, POP3, SMTP, FTP, Telnet
Transport (Transportschicht)	TCP, UDP
Internet (Internetschicht)	IP (IPv4 und IPv6)
Network Access (Netzzugangsschicht)	Ethernet, Token-Ring, FDDI

Tabelle 1.1: Das TCP/IP-Architekturmodell

Hinweis

Für die Bezeichnungen der einzelnen Schichten sowohl im TCP/IP- als auch im OSI-Schichtenmodell gibt es deutsche Begriffe. In Tabelle 1.1 sehen Sie die deutschen Begriffe in Klammern hinter den englischen Originalbegriffen. Es empfiehlt sich, beide Begriffe zu lernen, weil der größte Teil der Dokumentation zu TCP/IP und anderen Netzwerkthemen in englischer Sprache vorliegt und IT-Profis selbst in Deutschland häufig die englischen Originalbegriffe bevorzugen (und die deutschen Begriffe manchmal noch nicht einmal kennen – ich selbst muss sie auch immer wieder nachschlagen).

Tabelle 1.1 zeigt die vier Schichten des TCP/IP-Modells und nennt für jede Schicht beispielhaft ein paar populäre Protokolle, die eben auf der jeweiligen Schicht angesiedelt sind. Die folgenden Abschnitte beschreiben jede der vier Schichten und ihr Zusammenspiel genauer.

1.1.1 Die TCP/IP-Anwendungsschicht

Gleich das Wichtigste vorweg: Die *TCP/IP-Anwendungsschicht* definiert nicht die Anwendung selbst, sondern Dienste, die von Anwendungen benötigt werden. Das kann im Fall von HTTP beispielsweise die Fähigkeit sein, eine Datei zu übertragen. Die TCP/IP-Anwendungsschicht bietet also der auf einem Computer laufenden Anwendungssoftware Dienste. Sie bildet die Schnittstelle zwischen der Software auf dem Computer und dem Netzwerk.

Die heute populärste TCP/IP-Anwendung ist ohne Zweifel der Web-Browser. Einen Web-Browser zu benutzen ist so einfach wie Kaugummi kauen: Sie starten den Web-Browser auf Ihrem Computer und tippen den Namen der gewünschten Website ein, die daraufhin – falls nichts schiefliegt – erscheint. Hinter den Kulissen läuft dabei natürlich einiges ab.

Nehmen wir einmal an, Peter öffnet seinen Browser, der bequemerweise so konfiguriert ist, dass er automatisch die Homepage des Web-Servers Webby lädt.

Um die Webseite von Webby zu bekommen, sendet Peter einen *HTTP-Header* zu Webby. Dieser *Header* enthält den Befehl »get«, um eine Datei abzurufen. Normalerweise enthält diese Anfrage auch noch den Namen der Datei. Wird kein Name angegeben, nimmt der Web-Server an, dass die Default-Webseite gewünscht ist. Damit liegt er in der Regel richtig.

Hinweis

In deutschsprachiger Literatur über Netzwerkprotokolle liest man statt Header gelegentlich Kopf, beispielsweise statt Nachrichten-Header Nachrichtenkopf. Obwohl dies ein Buch in deutscher Sprache ist, möchte ich doch lieber beim englischen Originalbegriff Header bleiben.

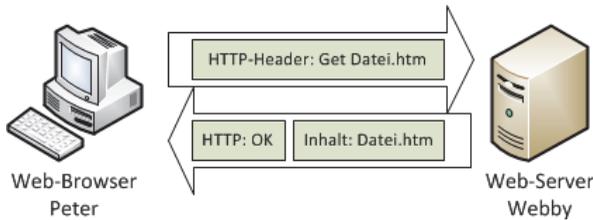


Abb. 1.1: Eine HTTP-Get-Anfrage und die HTTP-Antwort

Die Antwort des Web-Servers enthält ebenfalls einen HTTP-Header, der aber gerade mal ein »OK« zurück liefert. In der Realität enthält der Header natürlich einen HTTP-Return-Code, der sagt, ob die Anfrage bedient werden kann. Kann der Web-Server die gewünschte Datei nicht finden, sendet er einen HTTP-404-Fehler, »not found«. Findet er die Datei, dann sendet er den Return-Code 200: »Alles klar, ich bearbeite die Anfrage.«

Dieses einfache Beispiel zeigt eines der wichtigsten Konzepte von Netzwerkmodellen: Wenn eine bestimmte Schicht auf einem Computer mit derselben Schicht auf einem anderen Computer kommuniziert, dann nutzen die beiden Computer *Header*, welche die zu kommunizierenden Informationen enthalten. Die Header sind ein Teil dessen, was zwischen den Computern übertragen wird. Dieser Prozess wird »*same-layer interaction*« genannt, übersetzt etwa »Interaktion gleicher Schichten«.

Das Anwendungsschichtprotokoll (HTTP in unserem Beispiel) auf Peters Computer kommuniziert mit der Anwendungsschicht auf dem Web-Server Webby. Diese Kommunikation erfolgt durch das Erzeugen und Senden von Anwendungsschicht-Headern. Egal um welches Anwendungsschichtprotokoll es sich handelt, sie alle nutzen dasselbe Konzept der Kommunikation.

Neben HTTP umfassen die Protokolle dieser Schicht u.a. noch die Applikationsprotokolle FTP und SMTP sowie die administrativen Protokolle SNMP, DHCP und DNS.

1.1.2 Die TCP/IP-Transportschicht

Während zur TCP/IP-Anwendungsschicht relativ viele Protokolle zählen – HTTP ist ja nur eines davon –, gibt es auf der *TCP/IP-Transportschicht* eigentlich nur zwei Hauptprotokolle, die der Rede wert sind: das *Transmission Control Protocol* (TCP) und das *User Datagram Protocol* (UDP). Eine detaillierte Beschreibung der Transportprotokolle erfolgt später, und in diesem Abschnitt konzentrieren wir uns auf eine Schlüsselfunktion von TCP, die gut geeignet ist, etwas mehr über das generelle Konzept von Netzwerkmodellen zu erklären.

Um zu verstehen, was *Transportprotokolle* leisten, müssen wir an die Schicht direkt oberhalb der Transportschicht denken, die Anwendungsschicht. Jede Schicht stellt der direkt oberhalb liegenden Schicht einen Dienst zur Verfügung. Kehren wir noch einmal zurück zu unserem Beispiel mit Peter und Webby. Was wäre passiert, wenn Peters HTTP-Anfrage oder die Antwort des Web-Servers während der Übertragung irgendwo im TCP/IP-Netzwerk verloren gegangen wäre? Klar, die Seite wäre nicht im Browser erschienen.

TCP/IP benötigt also einen Mechanismus, der die Lieferung von Daten über ein Netzwerk garantiert. Da natürlich sehr viele Anwendungsschichtprotokolle eine garantierte, also zuverlässige Datenübertragung über ein Netzwerk wünschen, bietet TCP ihnen eine Error-Recovery-, also Fehlerbehebungsfunktion, die sich Acknowledgments (Bestätigungsnummern) bedient.

Betrachten Sie Abbildung 1.2: Der Web-Browser beauftragt TCP, die HTTP-Get-Anfrage zuverlässig auszuliefern. TCP sendet die Daten von Peter zum Web-Server – die Daten treffen fehlerfrei beim Web-Server ein, was dieser umgehend durch ein Acknowledgment bestätigt. Außerdem reicht der Web-Server die Daten an die Web-Server-Software weiter, die sie verarbeitet. Dasselbe geschieht in umgekehrter Richtung mit der Antwort des Web-Servers, die ebenso erfolgreich bei Peter eintrifft.

Welche Vorteile die TCP-Fehlerbehebung bietet, stellt man natürlich erst dann fest, wenn die Daten unterwegs verloren gehen. Gehen wir einstweilen davon aus, dass bei einem Datenverlust nicht etwa HTTP

eingreift, sondern TCP die Daten erneut sendet und gewährleistet, dass sie erfolgreich empfangen werden.

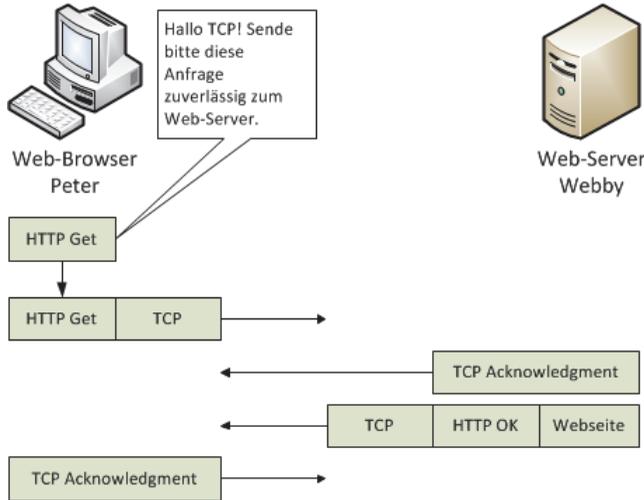


Abb. 1.2: TCP stellt HTTP seine Dienste zur Verfügung.

Dieses zweite Beispiel veranschaulicht ein Konzept, das »*adjacent-layer interaction*« genannt wird, übersetzt etwa »Interaktion benachbarter oder angrenzender Schichten«. Dieses Konzept beschreibt, wie die benachbarten Schichten eines Netzwerkmodells auf demselben Computer zusammenarbeiten. Das Protokoll der höheren Schicht, in diesem Fall HTTP, muss etwas tun, was es nicht kann (Fehlerbehebung). Also beauftragt das Protokoll der höheren Schicht das Protokoll der eine Stufe tiefer liegenden Schicht (TCP) damit, diese Aufgabe zu übernehmen. Das Protokoll der tieferen Schicht bietet dem Protokoll der höheren Schicht also einen Dienst.

Die beiden Beispiele zur Anwendungs- und Transportschicht ignorieren viele Details des physischen Netzwerks. Beide Schichten funktionieren immer genau gleich, unabhängig davon, ob sich die involvierten Endpunkt-Computer im selben LAN befinden oder ob sie durch das komplette Internet voneinander getrennt sind. Die zwei verbleibenden

Schichten aber, die Internet- und die Netzzugangsschicht, müssen das zugrunde liegende physische Netzwerk verstehen, denn sie definieren die Protokolle, die benutzt werden, um die Daten von einem Host zum anderen zu liefern.

1.1.3 Die TCP/IP-Internetschicht

Die *Internetschicht* ist zuständig für die logische Adressierung der physischen Netzwerkschnittstelle. Das klingt kompliziert, ist aber ganz einfach. Sehen wir uns noch einmal die Anfrage an, die Peter zum Web-Server sendet, diesmal mit einigen Details über das *Internetprotokoll* (IP). Die Linien bei Peters Arbeitsstation und dem Web-Server repräsentieren einfach zwei LANs, deren Details nicht wichtig sind. Wenn Peter die Daten sendet, dann sendet er tatsächlich ein IP-Paket. Dieses IP-Paket enthält einen IP-Header, den Transportschicht-Header (in diesem Fall einen TCP-Header), den Anwendungsschicht-Header (HTTP) und Anwendungsdaten (in diesem Fall keine). Der IP-Header enthält jeweils ein Quell- und ein Ziel-IP-Adressfeld. Das Quell-IP-Adressfeld enthält Peters IP-Adresse (1.1.1.1), das Ziel-IP-Adressfeld die IP-Adresse des Web-Servers (2.2.2.2).

Peter sendet das Paket zum Router R₁. R₁ untersucht die Ziel-IP-Adresse (2.2.2.2) und fällt die Routing-Entscheidung, das Paket zum Router R₂ zu senden. Das funktioniert, weil R₁ genug von der Netzwerktopologie kennt, um zu wissen, dass der Web-Server (2.2.2.2) auf der anderen Seite von R₂ liegt. Wenn R₂ das Paket empfängt, leitet dieser Router es über das Ethernet an den Web-Server weiter. Sollte die Verbindung zwischen R₁ und R₂ ausfallen, dann erlaubt IP R₁, eine neue Route zu lernen, die den Web-Server über R₃ erreicht.

IP definiert also IP-Adressen für jedes TCP/IP-fähige Gerät (IP-Host genannt). Diese Adressen erlauben IP-Hosts zu kommunizieren. Außerdem definiert IP *Routing*. Routing beschreibt, wie ein Router Datenpakete weiterleiten oder *rouuten* sollte.

Auf dieser Schicht finden wir also IP, außerdem unterstützende Protokolle wie ICMP und diverse Routing-Protokolle wie OSPF, RIP oder BGP.

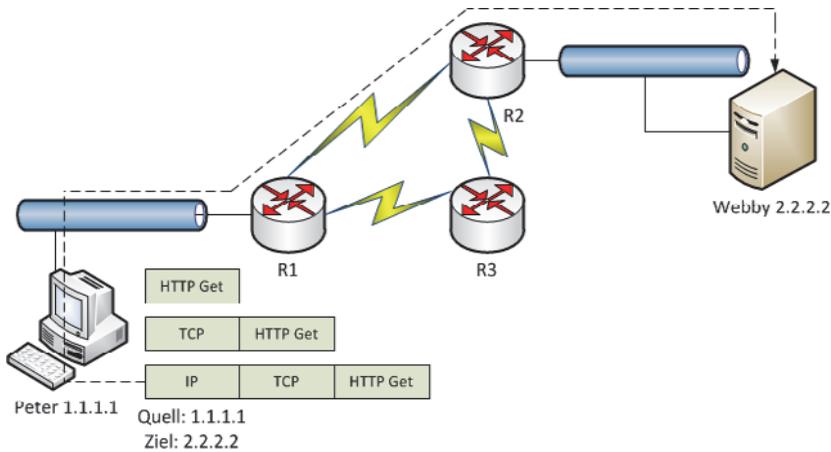


Abb. 1.3: IP-Dienste

1.1.4 Die TCP/IP-Netzzugangsschicht

Die *Netzzugangsschicht* definiert die für die Lieferung von Daten über ein physisches Netzwerk notwendigen Protokolle und Geräte. Der Begriff *Netzzugang* oder *Network Access* lässt bereits daran denken, dass diese Schicht definiert, wie ein Host-Computer zu verbinden ist mit dem physischen Medium, über das Daten transportiert werden können. Ethernet ist beispielsweise ein Protokoll, das auf der Netzzugangsschicht angesiedelt ist. Es definiert die notwendige Verkabelung, die Adressierung und Protokolle für ein Ethernet-LAN. Andere Protokolle der Netzzugangsschicht definieren Stecker, Kabel und Stromstärken für Protokolle, die Daten über WAN-Verbindungen übertragen.

Hier ist anzumerken, dass auf dieser Schicht sehr häufig überhaupt kein Protokoll läuft, das zur TCP/IP-Familie gehört. Wird TCP/IP zum Beispiel über ein Ethernet ausgeführt, dann ist es Ethernet, das sich um die Funktionen dieser Schicht kümmert. Trotzdem definiert der TCP/IP-Standard natürlich Protokolle für TCP/IP-Netzwerke, die keine eigenen Netzzugangsschichtprotokolle haben. Diese Protokolle sind das *Serial Line Internet Protocol (SLIP)* und das *Point-to-Point Protocol (PPP)*.