IN DIESEM KAPITEL

- Wie kommen Informationen in ein Datenpaket?
- Wie werden Datenpakete in Netzwerken übertragen?
- Datenzuverlässigkeit, -sicherheit und -priorisierung: ein Überblick

Kapitel 1
Ein Sprachpaket geht auf Reisen

In unserer digital vernetzten Welt gehen jeden Moment Unmengen an Informationen auf Reisen. Fast alle nutzen den Transportweg des Internets und halten sich dabei an die Regeln des Internet-Protokolls (IP) und all seiner »Helfer«. Das Internet wird dabei nicht nur für E-Mails, Webseitenabfragen, Dateitransfers oder Ähnliches verwendet, sondern auch für das Telefonieren, also die direkte Sprachkommunikation. Gehen Sie in diesem Kapitel mit einem Sprachpaket auf Reisen, um einen digitalen Datentrip grundsätzlich zu verstehen. Genauso gut könnten wir auch das Fragment einer Webseite in die Ferien schicken oder ein Stück einer E-Mail. Die grundlegenden Konzepte sind die gleichen. Sie müssen nur einsteigen und können sich in diesem Kapitel noch auf die Hilfe eines Reisebüros verlassen, das Ihnen die allzu technischen Details des Transports zunächst erspart. Startpunkt ist Ihr Heim-PC, Ziel der Reise ein Weit-Weg-Notebook. Suchen Sie sich aus, in welchem Land dessen Besitzer oder Besitzerin gerade Urlaub macht. Abbildung 1.1 hilft Ihnen hoffentlich dabei, in Urlaubs- und Lesestimmung zu kommen.

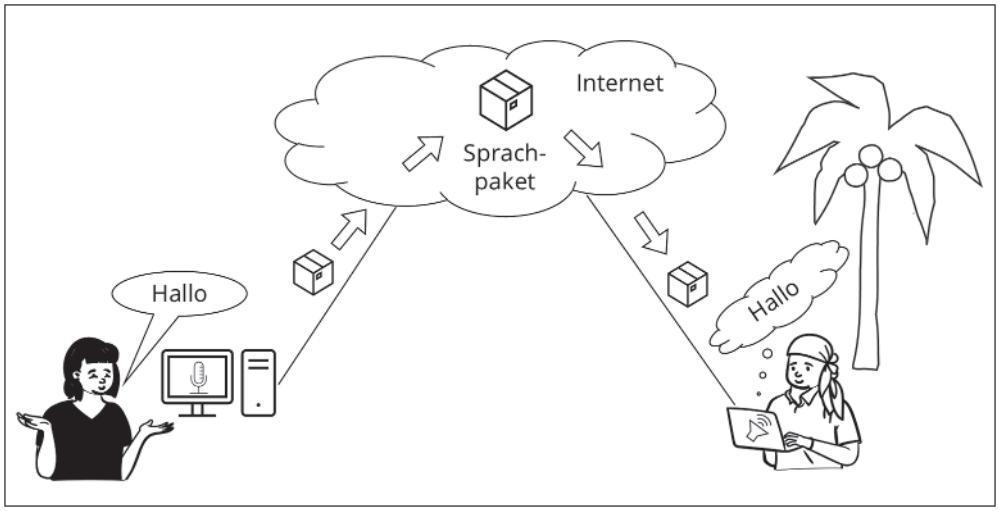

Abbildung 1.1: Reisendes Sprachpaket

Worte, gut verpackt

Wer verreist, trifft üblicherweise bereits im Vorfeld gewisse Vorkehrungen: Wie viele Koffer werden gepackt? Was ist wichtig, was kann zu Hause bleiben? Wie sind die Reisebedingungen? Gibt es Staumeldungen, Streiks im Flugverkehr? Auch der Heim-PC bereitet die Sprachdaten auf ihre Reise vor. Dieser Abschnitt beschäftigt sich daher mit den Fragen:

- ✔ In welcher Form werden die Daten übertragen? Welche Bedeutung haben die Nullen und Einsen?
- ✔ Warum werden Daten überhaupt in Pakete verpackt? Ginge es auch anders?
- ✔ Wie kommt das gesprochene Wort in ein IP-Paket?

Die Welt der Nullen und Einsen

Wie alles in der Welt der digitalen Technologien, arbeiten Computer in ihrer Logik ausschließlich mit Nullen und Einsen. Der Grund hierfür ist ganz einfach: Elektronische Schaltkreise kennen nur den Zustand »an« oder »aus«. Im sogenannten binären System stehen diese Zustände für »1« bzw. »0« und repräsentieren die kleinste Informationseinheit, das **Bit**. Durch die Kombination von Nullen und Einsen können nach bestimmten Regeln verschiedene Muster dargestellt werden, die dann Texte, Bilder, Videos oder eben auch Sprache für den Computer repräsentieren. Den Vorgang des Umwandelns eines solchen Signals in eine Bitfolge nennt man **Binärcodierung.** Sie findet nach klar definierten Regeln im sogenannten **Encoder** statt (siehe Abbildung 1.2). Auf der Empfängerseite kennt der Gegenspieler des Encoders, der **Decoder**, diese Regeln und erzeugt aus dem 0-1-Muster im

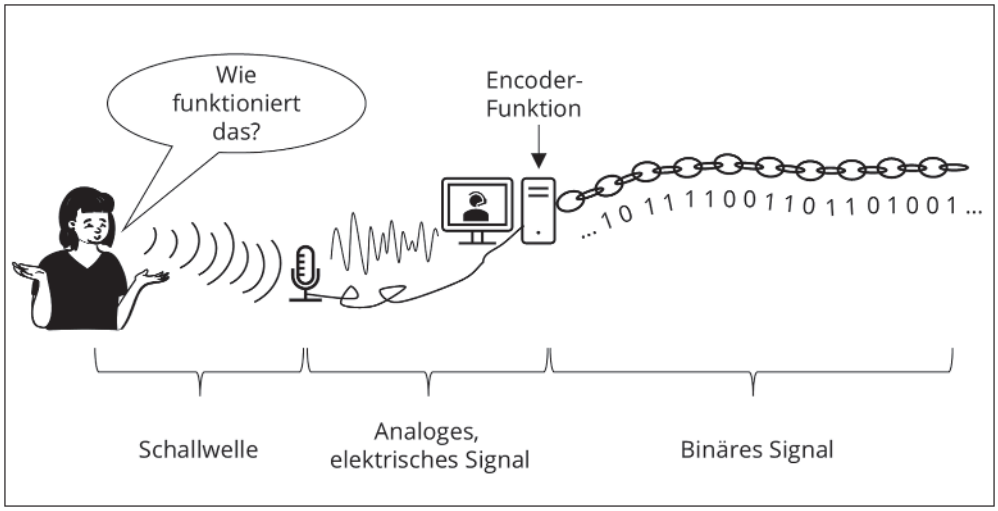

Abbildung 1.2: Vorgang der Binärcodierung

Fall unseres Sprachsignals wieder genau das Wort, das ursprünglich gesprochen wurde. Auch Informationen zum Tonfall, der Stimmhöhe und der Lautstärke verstecken sich in den Nullen und Einsen. Im Fall des Telefonierens wüsste man sonst kaum, mit wem man es am anderen Ende der Leitung zu tun hat.

Grundprinzip der Paketvermittlung

Während wir sprechen, produziert der Encoder unseres PCs eine lange Kette aus Nullen und Einsen. Damit diese zu ihrem Zielort gelangen können, müssen sie verpackt und adressiert werden. Die Informationen werden dafür in kleine Stücke zerlegt und als einzelne Datenpakete wie digitale Postkarten verschickt. Man nennt dieses Prinzip des Datenversands daher auch Paketvermittlung. Zu den eigentlichen, nun schon portionierten Sprachdaten kommt vor dem Versand noch einiges an Bits dazu. Die Zieladresse ist eine der wichtigsten Zusatzinformationen und wann immer Daten mit Hilfe des Internet-Protokolls versendet werden, steht im Adresslabel des Pakets die IP-Adresse des Zielgeräts. Sie dient an den verschiedenen Knotenpunkten des Internets der bestmöglichen Routenfindung. Nicht umsonst heißen diese Knotenpunkte auch Router. Aber dazu später mehr. Alle Informationen, die zu den eigentlichen Sprachdaten hinzukommen, bezeichnet man als **Overhead**. Das ist in manchen Fällen auch mal mehr als der eigentliche Inhalt des Pakets. Aber nur dank dieser zusätzlichen Informationen kann es autonom und unabhängig durch das Internet gelotst werden. Alles, was das Paket braucht, hat es selbst dabei und so kann es sein, dass die einzelnen Bestandteile eines Satzes, den wir sprechen, ganz unterschiedliche Wege im Netz nehmen. Genauso wie Postkarten, die wir hin und wieder noch aus dem Urlaub verschicken: Der Overhead-Bereich für Adresse und Briefmarke nimmt schnell mal die Hälfte der Fläche in Anspruch und Karten an Oma und Tante, die im gleichen Haus wohnen, sind nicht selten unterschiedlich lange auf dem Weg.

Wenn die Datenpakete, die wir in unserem Telefonier-Beispiel auch als »Sprachpakete« bezeichnen, ihr Ziel erreichen, werden sie wieder zusammengefügt. Ähnlich wie beim Zusammensetzen von Puzzlestücken entsteht so die ursprüngliche Kette aus Nullen und Einsen. Und diese kann vom Decoder in den gesprochenen Satz zurückgewandelt werden. Zum Grundprinzip der Paketvermittlung siehe auch Abbildung 1.3.

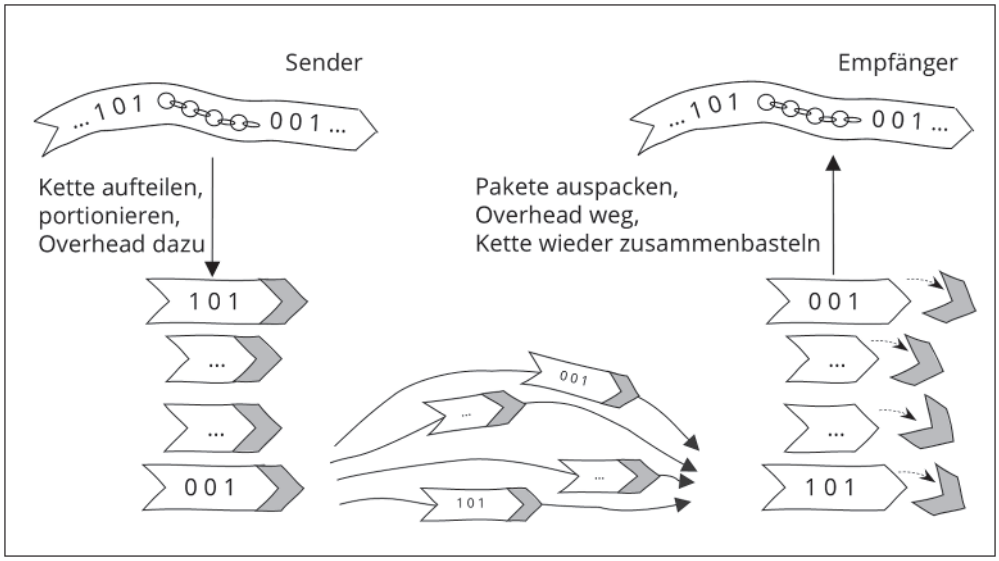

Abbildung 1.3: Grundprinzip der Paketvermittlung

Historisches: Das Fräulein vom Amt

Speziell für Sprachdaten war es nicht immer so, dass Gesprächsfetzen in einzelne Pakete verpackt und getrennt durch das Netzwerk geschickt wurden. In den Anfängen der Telekommunikation Ende des 19. Jahrhunderts wurde eine Telefonleitung noch im klassischen Sinne vermittelt, indem tatsächlich Telefonapparate mit Hilfe einzelner Kabel über Steckplätze miteinander verbunden wurden. Diese manuelle Vermittlung wurde überwiegend von Frauen übernommen, da sie im Allgemeinen bessere Umgangsformen hatten und ihnen für diese Aufgabe auch weniger bezahlt werden musste als Männern. Das »Fräulein vom Amt« war dennoch ein begehrter Beruf für Frauen auf der Suche nach finanzieller Unabhängigkeit.

Historische Aufnahme eines »Fräuleins vom Amt«, © everettovrk - stock.adobe.com

Es geht auch ohne Pakete: Das Prinzip der Leitungsvermittlung

Aus den Anfängen der Telefonie ist der Begriff der **Leitungsvermittlung** als Gegenstück zur eingangs beschriebenen Paketvermittlung geblieben. Von Leitungsvermittlung spricht man immer dann, wenn vor der eigentlichen Datenübertragung eine exklusive Übertragungsressource vom Sender bis zum Empfänger eingerichtet wird. Wenn die »Leitung einmal steht«, ist sie wie ein Gartenschlauch, in den die Daten nur noch reintröpfeln müssen. Sie brauchen keine Adressierung mehr und auch sonstiger Overhead hält sich in Grenzen. Solange die Verbindung besteht, kann niemand anderes diese Leitung nutzen, auch wenn gerade keine Daten übertragen werden.

In Zeiten des Internets spielt die klassische Leitungsvermittlung, wie wir sie aus den Anfängen der Telefonie kennen, kaum noch eine Rolle. Insbesondere nicht für eine vollständige Datenübertragung vom Sender bis zum endgültigen Empfänger. Als veraltet sollte das Konzept dennoch nicht angesehen werden. Auf ihrem Weg durchs Netz durchlaufen Daten

ganz unterschiedliche Teilstrecken; je nach Auslastung und Beschaffenheit des Übertragungsmediums macht es da schon mal Sinn, eine Ressource zu reservieren, beispielsweise auf Funkstrecken. In heutigen Netzen spielen sich die Reservierungen daher eher auf der Ebene der tatsächlichen Übertragung und meist nur auf einzelnen »Reiseabschnitten« ab. Ein Datenpaket bekommt davon gar nicht viel mit. Es ist wie ein »All-inclusive-Reisender«: Hauptsache ankommen – da wo es nötig ist, übernehmen andere die Reservierung. In Abbildung 1.4 ist ein solches »All-inclusive-Paket« unterwegs.

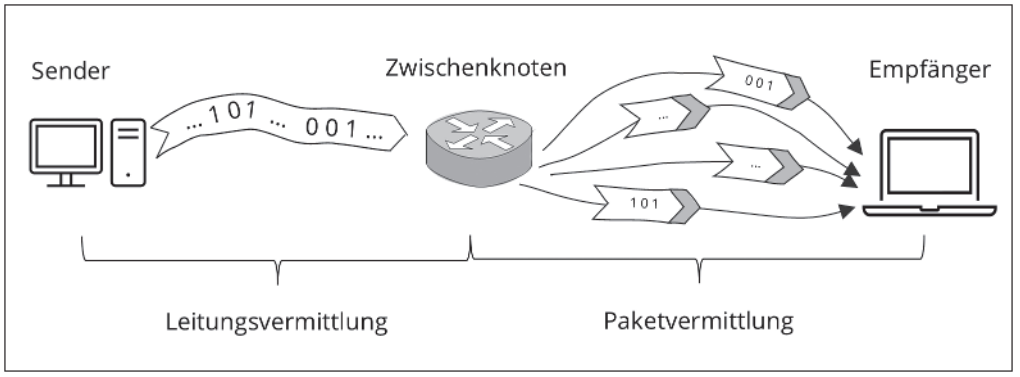

Abbildung 1.4: Paket- und Leitungsvermittlung innerhalb einer Datenübertragung

Schlauch verlegen oder jeden Tag gießen?

Die Frage, ob für eine Datenübertragung die Leitungs- oder Paketvermittlung sinnvoller ist, kann man auch daran festmachen, wie die Daten eigentlich genutzt werden bzw. wie oft es zu einer Übertragung kommt.

Stellen Sie sich ein bepflanztes Blumenbeet in Ihrem Garten vor. Um es zu bewässern, können Sie regelmäßig einzelne Gießkannen befüllen, durch den Garten tragen und gießen (paketvermittelt) oder Sie verlegen einmal einen Schlauch und den Blumen geht es gut (leitungsvermittelt). Betreiben wir also mit unseren Gießkannen immer wieder ein bisschen Aufwand oder akzeptieren einmal viel Aufwand beim Verlegen des Gartenschlauchs? Entschieden wird das nicht nur anhand des Wasserbedarfs der Blumen. Wenn die Gießkannen billig sind, wir aber niemanden finden, der uns den Schlauch verlegt, dann entscheiden wir uns eher für das aufwendige Gießen, noch dazu, wenn die Gießkanne ohnehin schon gekauft ist.

Und so ist es auch mit der Paketvermittlung im Internet. Diese Form der Datenübertragung als IP-Paket hat sich etabliert. Unsere Notebooks, Smartphones und sonstige Geräte wissen, wie sie diese Pakete packen und adressieren müssen. Es wäre mehr als aufwändig, ihnen die Leitungsvermittlung beizubringen und von allen Netzen zu erwarten, dass sie beides können. Also bringen wir möglichst all unseren Datenanwendungen bei, mit der paketvermittelten Übertragung zurechtzukommen, auch wenn es manchmal etwas ineffizient ist, wie wir im nächsten Abschnitt noch sehen werden.

Klein aber fein: Ein Sprachpaket im Internet

Ein IP-Paket kann bis zu 1500 Byte groß sein (also 8 * 1500 Bit, denn es gilt 1 Byte = 8 Bit). Je nach Übertragungsweg geht auch mehr. Zieht man den minimal notwendigen Overhead für Adressen und andere logistisch relevante Informationen ab, bleiben immer noch bis zu 1460 Byte für die Sprachdaten. Sollten Sie diese Paketgröße für ein Telefonat voll ausnutzen, wird Ihr Gesprächspartner schnell auflegen. Denn es dauert allein fast 1,5 Sekunden, bis ein solches Paket voll ist und überhaupt losgeschickt werden kann. So viel Geduld hat niemand am Telefon. Sie würden sich gegenseitig permanent ins Wort fallen. Bereits eine Verzögerung von 200 Millisekunden wird in einer direkten Sprachkommunikation als störend empfunden.

Wieviel Sprache passt in ein vollgepacktes Standard-IP-Paket?

Die Fakten:

- ✔ Maximale Kapazität in einem IP-Paket auf einem Standardübertragungsweg:

  1460 Byte = 1460 * 8 Bit = 11680 Bit

- ✔ Datenrate eines typischen Sprachsignals, sozusagen die »Paketfüllrate«:

  Beispiel 8 kbit/s = 8000 Bit/s (also entspricht 1 Sekunde Sprache 8000 Bit)

Wie lange dauert es, bis das ganze Paket voll ist?

- ✔ Paketfüllzeit = maximale Kapazität / Füllrate

  11680 Bit / 8000 Bit/s = 1,46 s

Fazit: Ein Paket mit Platz für 11680 Bit braucht also fast 1,5 Sekunden Sprache, bis es voll ist. Das ist bereits ein kurzer, vollständiger Satz.

Die volle Größe eines IP-Pakets auszunutzen, macht für Sprachdaten also wenig Sinn. Die Pakete werden eher minimal bestückt, um den Zeitverlust durch diese Paketierung in Grenzen zu halten. Üblich ist beispielsweise, ein Sprachpaket nach 20 Millisekunden, mit oft nicht mehr als 20 Byte Sprachdaten, auf die Reise zu schicken. Das geht schnell, bringt aber viel Overhead ins Netzwerk, wie in Abbildung 1.5 zu erkennen ist.

Ob ein Paket bis zur maximal möglichen Anzahl an Bits vollgepackt wird, hängt von der konkreten Anwendung ab.

Mehr zur internetbasierten Sprachübertragung, auch bekannt als **Voice over IP (VoIP),** finden Sie in Kapitel 14.

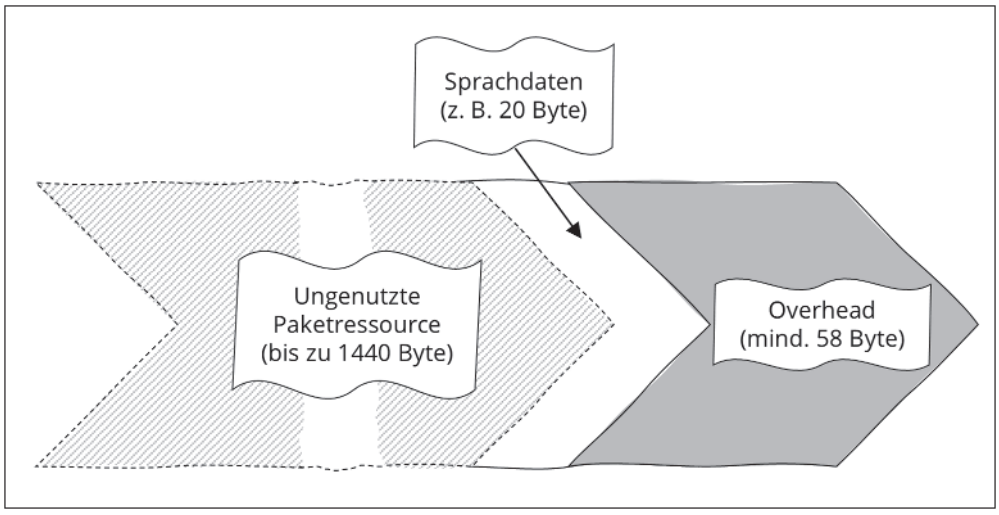

Abbildung 1.5: Overhead und Ressourcenverschwendung bei einem Sprachpaket

Die Reise kann beginnen

Die Koffer sind gepackt und die Reise für unsere Sprachpakete kann beginnen. Auch ohne Detailwissen zu den unterwegs relevanten Netzwerkprotokollen, die wir in den folgenden Kapiteln noch kennenlernen werden, begleiten wir unsere Sprachdaten nun auf ihrem Weg durch das Internet. Um die wichtigsten Abläufe dabei zu verstehen, betrachten wir in diesem Abschnitt:

- ✔ Wichtige Adressen im Internet und deren Zusammenspiel
- ✔ Grundlagen des Routings

Der erste Schritt ins Netz

Jedes IP-Paket enthält in seinem Header die IP-Adresse des Zielrechners, in unserem Fall das Weit-Weg-Notebook. IP-Adressen bilden die Grundlage sämtlicher Routing-Entscheidungen, die Hop-by-Hop in den Knotenpunkten des Internets getroffen werden. Etwas genauer wird der Ablauf des Routings im nächsten Abschnitt *Hop-by-Hop durchs Internet* bzw. in Kapitel 7 behandelt. Spannend ist aber bereits der Weg raus aus dem Heim-PC bis zum ersten Router.

Der Weg zum nächsten Briefkasten

In den üblichen Strukturen des Internets, speziell der lokalen Netze, die meist Ausgangspunkt der Datenübertragungen sind, reicht es nicht, die IP-Adresse auf das Paket zu

schreiben. Das wäre wie ein fertig adressierter Brief, der nicht zur Post gebracht wird, weil keiner weiß, wo die Post oder zumindest ein Briefkasten ist. Also geben wir diese Information noch dazu und zwar in Form der sogenannten **MAC-Adresse**. MAC steht für Medium Access Control, ein Begriff, der mit Adressierung zwar wenig zu tun hat, aber mit der Hardware, die die Daten verschickt oder empfängt. Und diese Hardware möchte in den Netzwerkabläufen konkret adressiert werden. Jedes Gerät bzw. jeder Netzwerkadapter hat demnach eine fixe Hardwareadresse, die bereits vom Hersteller vorgegeben wird. Eine typische MAC-Adresse sieht beispielsweise so aus: *00-1A-2B-3C-4D-5E*.

Ein IP-Paket wird daher für die lokale Zustellung noch einmal in einen extra Karton verpackt, der als Ziel die MAC-Adresse des nächsten Routers enthält. Der kümmert sich dann um die weitere Zustellung und gewährleistet generell den Zugang zu anderen Netzen. Jedes Endgerät kennt seinen Ansprechpartner für den »ersten Hop nach draußen« als sogenanntes **Standardgateway** (siehe Abbildung 1.6).

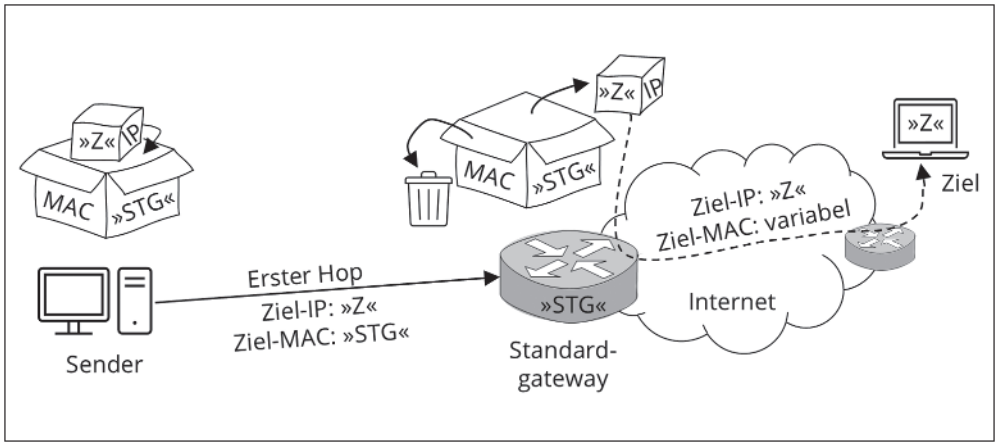

Abbildung 1.6: Erster Hop einer Datenübertragung

Der Unterschied zwischen MAC- und IP-Adressen

Den Unterschied zwischen MAC- und IP-Adressen kann man sich auch anders verdeutlichen. Mit unseren Endgeräten, speziell Notebooks oder Smartphones, gehen wir an unterschiedlichsten Standorten ins Internet, ziehen also immer wieder um und sind demnach auch unter unterschiedlichen Adressen erreichbar. Das sind die IP-Adressen, die wir bei jedem »Wohnsitzwechsel« neu zugewiesen bekommen. Das Internet-Protokoll arbeitet in seiner globalen Zustellung mit diesen Adressen. Vor Ort braucht das System dann aber doch eine fix zugewiesene, physische Adresse, die immer gleichbleibt. Geräte haben im Netzwerk also ihre fixe MAC-Adresse und eine variable, logisch zugeordnete IP-Adresse (siehe Abbildung 1.7). In dem Postbeispiel prüft der Postbote oder die Postbotin zum Schluss als

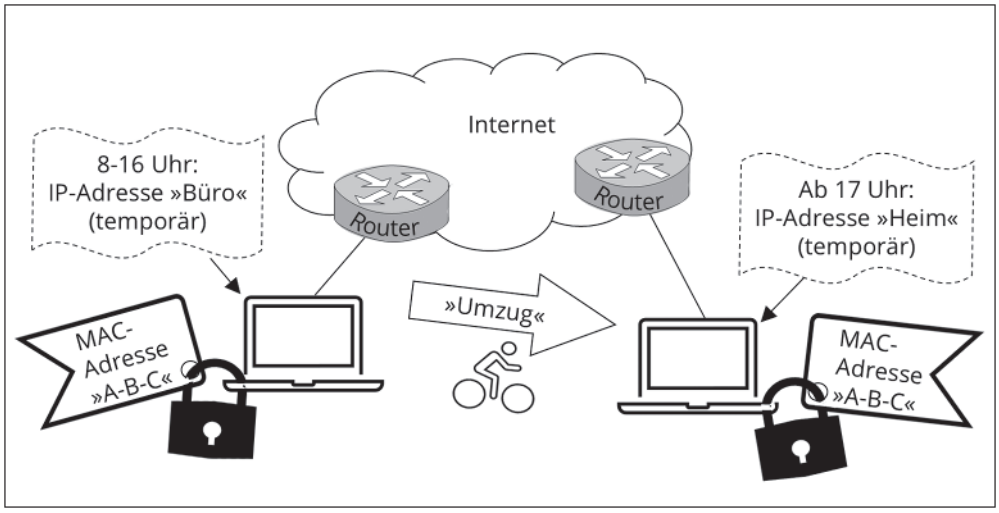

Abbildung 1.7: MAC- und IP-Adressen

Hardware-Kennung also vielleicht so etwas wie unseren Fingerabdruck, um das Paket tatsächlich zuzustellen. Und der ist immer gleich, egal, wo auf der Welt wir gerade sind.

Für das Auslesen der eigenen logischen und physischen Adressen gibt es je nach verwendetem Gerät und Betriebssystem mehrere Möglichkeiten. Auf einem Windowsrechner sind es beispielsweise folgende:

Prüfen der Windows-Netzwerkeinstellungen

- ✔ Klicken Sie mit der rechten Maustaste auf das Windows-Startmenü und wählen Sie im Menü »Netzwerkverbindungen«.
- ✔ Klicken Sie im nächsten Fenster auf die Verbindung, die Sie interessiert.
- ✔ Alle relevanten Informationen werden angezeigt; manches davon wird erst einige Kapitel später behandelt.

Auslesen über die Eingabeaufforderung:

- ✔ Öffnen der Eingabeaufforderung: [Windows]-Taste drücken, »cmd« eingeben, anschließend [Enter] drücken.
- ✔ Die Windows-Eingabeaufforderung ist offen.
- ✔ Eingabe »ipconfig /all« und [Enter].
- ✔ Alle relevanten Informationen werden angezeigt.

Hop-by-Hop durchs Internet

Hat das Paket den ersten Schritt vor die Tür geschafft, kümmern sich nun verschiedene Netzwerkkomponenten um dessen Weiterleitung. Der Begriff des Routers wurde bereits genannt. Ein Router ist wie ein Postverteilzentrum: Er kennt sich mit der logischen IP-Adressierung der Datenpakete aus. Sobald er ein Paket empfängt, wertet er diese Adresse aus und trifft eine Entscheidung für den nächsten Hop, also definiert den Weg zum nächsten Router oder vielleicht auch schon an das Zielgerät. Grundlage für diese Entscheidung ist die sogenannte Routingtabelle, die in jedem Router enthalten ist und sich üblicherweise auch kontinuierlich aktualisiert.

Aufgrund seiner großen Bedeutung in der Welt des Internets ist dem Router das gesamte Kapitel 7 gewidmet.

Für die Wege zwischen den Routern wird das Paket immer wieder neu eingepackt und auf dem »Außenumschlag« mit der Hardware(MAC-)adresse des nächsten Hops versehen. In lokalen Netzen spielt auf den Pfaden zwischen den Routern der **Switch** – als weitere Netzwerkkomponente – eine wichtige Rolle. Er versteht zwar nichts von der großen, weiten Welt des Internets, prüft aber sehr genau den »Außenumschlag« und kann basierend auf der MAC-Adresse dafür sorgen, dass die Daten hier effizient weitergeleitet werden.

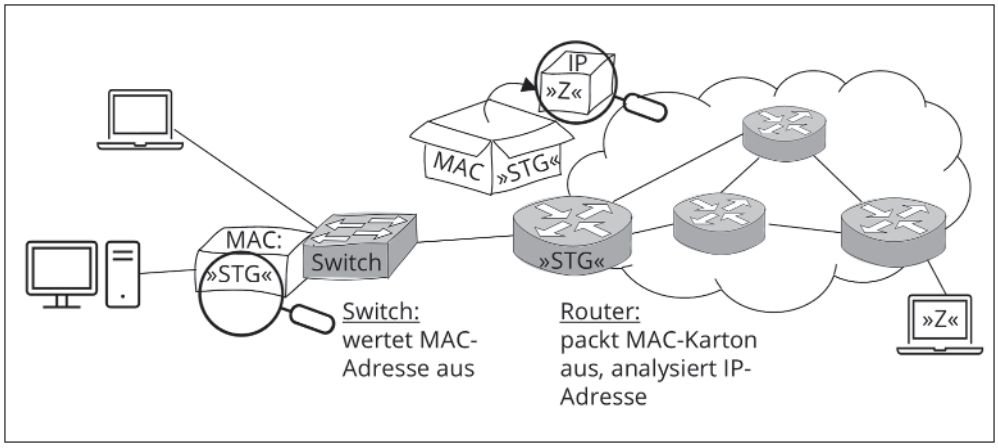

Abbildung 1.8: Die Rolle von Router und Switch bei der Paketzustellung

Mehr zu den Abläufen in einem lokalen Netzwerk ist in Kapitel 3 im Abschnitt *Adressierung und Zuständigkeiten* zu finden.

Sicher, zuverlässig, überpünktlich: Die Extras im Internet

Für eine Reise lassen sich üblicherweise verschiedene Zusatzangebote dazu buchen, sei es für mehr Sicherheit, mehr Komfort, schnelleren Transport oder Ähnliches. So ist es auch im Internet. Je nach Art der Daten, die übertragen werden, »kümmert« sich das Netzwerk sehr unterschiedlich um sie. Von größter Fürsorge bis zu »einfach vor die Tür setzen« ist alles dabei. Einige dieser Optionen werden im folgenden Abschnitt kurz vorgestellt und in späteren Kapiteln genauer betrachtet:

- ✔ Kontrollierte Verbindungen und Quittierung der Daten
- ✔ Schutz von Daten und Netzwerken vor Missbrauch und Schädigung
- ✔ Priorisierungsoptionen

Unterwegs im Internet: Frei oder kontrolliert?

Verbindungsaufbau: Erst mal schauen, ob jemand zuhört

Für einen Datenversand werden bezüglich der Zuverlässigkeit grundsätzlich zwei Strategien unterschieden: die verbindungslose Variante und die verbindungsorientierte. Das Internet-Protokoll beispielsweise bietet lediglich einen verbindungslosen Dienst an. Das heißt, analog zu der Post, bei der Briefe einfach in einen Briefkasten geworfen werden, schickt ein sendender Rechner die Daten mit dem Internet-Protokoll einfach los und kümmert sich dann nicht mehr darum. Bei einem verbindungsorientierten Dienst würde der Sender das Zielgerät zunächst kontaktieren, auf Erreichbarkeit prüfen und eine Verbindung aufbauen. In der menschlichen Kommunikation ist das vergleichbar mit dem Austausch höflicher Grußfloskeln, bevor man im Gespräch »zur Sache« kommt. Natürlich gehört auch eine Verabschiedung, also ein Verbindungsabbau zu diesem Zusatzdienst.

Ein verbindungsorientierter Dienst baut lediglich eine *logische* Verbindung auf. Manchmal wird diese auch *virtuell* genannt. Die bereits beschriebene Leitungsvermittlung geht einen Schritt weiter: Hier wird beim Verbindungsaufbau zusätzlich eine fixe Übertragungsressource (also eine Art Leitung) reserviert. Ein verbindungsorientierter Datendienst ist mit einem leitungsvermittelten also nicht gleichzusetzen.

Bestätigungen: Alles angekommen?

Ob mit oder ohne einleitende Grußformel und Verabschiedung stehen wir in einer Kommunikation auch vor der Wahl, ob wir für das, was wir sagen, eine Bestätigung bekommen möchten oder nicht. Ein Kopfnicken oder ein »Ja« nach jedem Satz mag manchmal wichtig sein, könnte aber auch den Gesprächsfluss stören und verzögern. Ähnlich ist es in der Welt des Datentransfers. Es gibt Anwendungen und Szenarien, in denen ein Datenempfang bestätigt werden sollte und solche, in denen eine Quittung nicht notwendig, nicht sinnvoll

oder vielleicht auch gar nicht möglich ist. Denken Sie nur an ihr TV-Gerät, das sicherlich nicht den Empfang jedes einzelnen empfangenen Bildpunkts oder Tonfetzens an den Fernsehsender zurückmeldet.

Das Kopfnicken des Datentransfers ist das **Acknowledgement**, kurz **ACK**, das von einem Empfänger an den Sender zurückgeschickt wird. Wenn etwas schief geht, gibt es ein **negative Acknowledgement (NACK)**. Sollte beides ausbleiben, merkt der Sender anhand eines Timers, dass bei der Kommunikation irgendetwas nicht geklappt hat.

Grundsätzlich lässt sich für jeden Datentransfer eine Aussage darüber treffen, ob er

- ✔ verbindungslos ist oder verbindungsorientiert
- ✔ als bestätigter oder unbestätigter Dienst arbeitet

Abbildung 1.9 zeigt beispielhaft eine verbindungslose, dafür aber bestätigte Datenübertragung sowie eine verbindungsorientierte, die auf Bestätigung des Datenempfangs verzichtet.

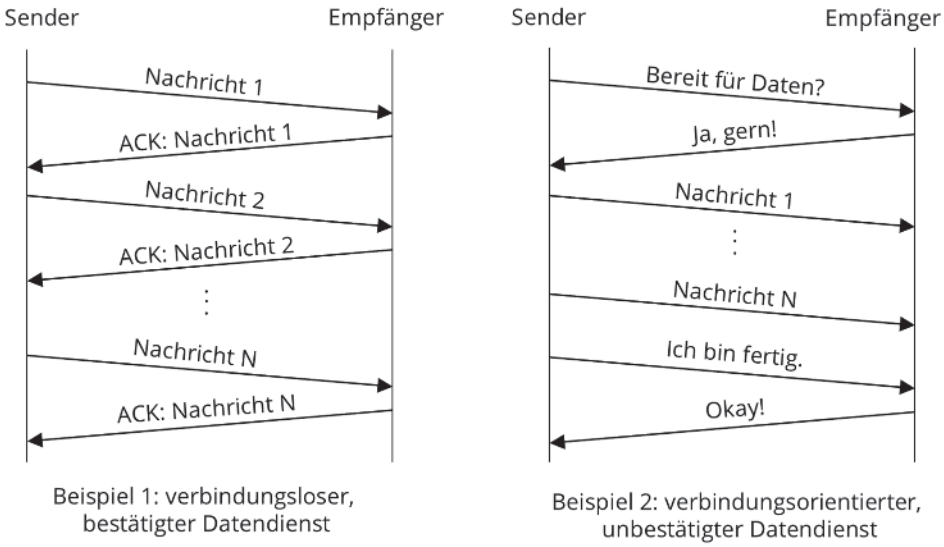

Abbildung 1.9: Optionen der Datenübertragung

Die Frage, ob Daten verbindungslos oder verbindungsorientiert, mit oder ohne Bestätigung im Netz verschickt werden, stellt sich auf unterschiedlichen Ebenen. Mal will man nur auf einem Teilstück der Übertragungsstrecke auf Nummer sicher gehen, ein anderes Mal soll von Anfang bis Ende eine Kontrollinstanz über den Datentransfer wachen. Diese Ende-zu-Ende-Kontrollinstanz im Internet ist das sogenannte Transmission Control Protocol (TCP), das zum einen eine logische Verbindung zwischen Sender und Empfänger aufbaut, sich zum anderen aber auch um die Bestätigung der Datenpakete kümmert.

TCP und sein »Gegenspieler«, das User Datagram Protocol (UDP), werden in Kapitel 8 genauer behandelt. In Kapitel 9, im Abschnitt *Daten in Watte packen*, widmen wir uns generell noch einmal dem Thema, wie Übertragungsfehler im Netzwerk verhindert bzw. erkannt und gegebenenfalls korrigiert werden.

Security im Internet: Hört da jemand mit?

Das globale Internet ist für unsere Daten eine Art öffentlicher Raum, in dem gewisse Bereiche oder Inhalte vor unerwünschten Zugriffen geschützt werden sollten. Vergleichbar ist dies mit einem Park, der zwar frei oder gegen ein kleines Entgelt für alle Menschen zugänglich ist, aber eventuell auch abgegrenzte Bereiche enthält, die nicht jede Person nutzen kann. Außerdem möchte ich plaudernd durch diesen Park spazieren, ohne dass andere mein Gespräch belauschen. Das Schlagwort Cyber Security steht in diesem Kontext generell für den Schutz von Computersystemen, Netzwerken und Daten vor böswilligen Angriffen und unerlaubtem Zugriff. Verschiedene Mechanismen und Algorithmen dienen letztendlich folgenden Grundfunktionen bezüglich Datensicherheit im Netzwerk:

- ✔ **Authentifizierung:** stellt sicher, dass nur autorisierte Personen Zugriff auf ein bestimmtes System oder eine bestimmte Anwendung haben, indem sie ihre Identität bestätigen, beispielsweise durch Eingabe eines Benutzernamens und eines Passworts.
- ✔ **Vertraulichkeit:** bedeutet, dass Informationen nur von berechtigten Personen oder Systemen eingesehen oder genutzt werden können. Zum Beispiel, wenn eine Nachricht verschlüsselt wird, können sie nur Personen oder Systeme mit dem richtigen Schlüssel lesen (siehe Abbildung 1.10).
- ✔ **Zugriffskontrolle:** regelt, wer auf bestimmte Informationen oder Ressourcen zugreifen kann und wer nicht. So kann eine Zugriffskontrolle festlegen, dass nur ausgewählte Benutzerinnen und Benutzer auf bestimmte Dateien oder Ordner zugreifen dürfen. Die Zugriffskontrolle ist eng an die Authentifizierung gekoppelt.
- ✔ **Datenintegrität:** bedeutet, dass die Daten bei ihrem Weg durch das Netzwerk korrekt und unverändert bleiben. Datenintegritätsmechanismen kontrollieren, ob Informationen während der Übertragung verändert oder beschädigt wurden.

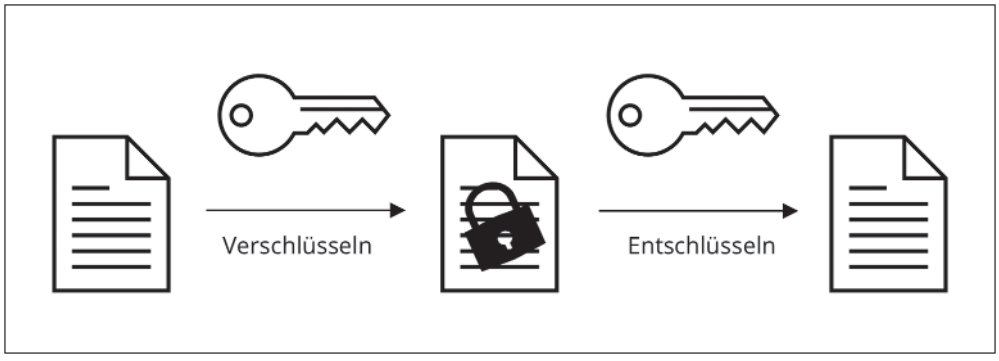

Abbildung 1.10: Vertraulichkeit im Kontext einer Datenübertragung

Diese Sicherheitsfunktionen kommen je nach Netzbereich und Art der Daten in unterschiedlicher Ausprägung zum Einsatz. Mehr dazu ist in Kapitel 12 zu finden. Aber auch dort wird es nur bei einem Überblick bleiben, da das Thema Cyber Security und IT-Sicherheit bereits das ein oder andere Dummie-Buch füllt.

Wenn es schnell gehen soll: Fast Lane gefällig?

So wie es bei Reisenden neben den gemütlichen auch die hektischen gibt, die unter ständigem Zeitdruck und ohne unnötige Wartezeiten versuchen, schnellstmöglich ans Ziel zu gelangen, unterliegen auch Daten in den Übertragungsnetzwerken sehr unterschiedlichen Anforderungen bezüglich Verzögerungszeiten zwischen Sender und Empfänger. Während es eine E-Mail sehr entspannt angehen kann, sollte unser reisendes Sprachpaket, wie schon erwähnt, nach spätestens 200 Millisekunden am Ziel sein, damit das Telefonat noch als angenehm empfunden wird. In Abläufen der Industrieautomatisierung, in denen beispielsweise Steuerbefehle für Maschinen durch ein Netzwerk verschickt werden, muss es noch um einiges schneller gehen. Einen Stau können sich diese Daten nicht leisten. Hier zählt jede Mikro- bzw. sogar Nanosekunde. Mit diesen Anforderungen können Netzwerke sehr unterschiedlich umgehen. Datenpakete mit einem Prioritätslabel zu versehen, damit sie unterwegs bevorzugt behandelt werden, ist eine Möglichkeit. Sie reisen sozusagen mit Blaulicht durchs Netzwerk (siehe Abbildung 1.11). Es kann aber auch schon von vornherein eine Strecke für besonders wichtige Daten freigehalten werden. Dann ist die Kreuzung bereits geräumt, bevor das Blaulichtfahrzeug kommt, das dadurch freie Fahrt hat.

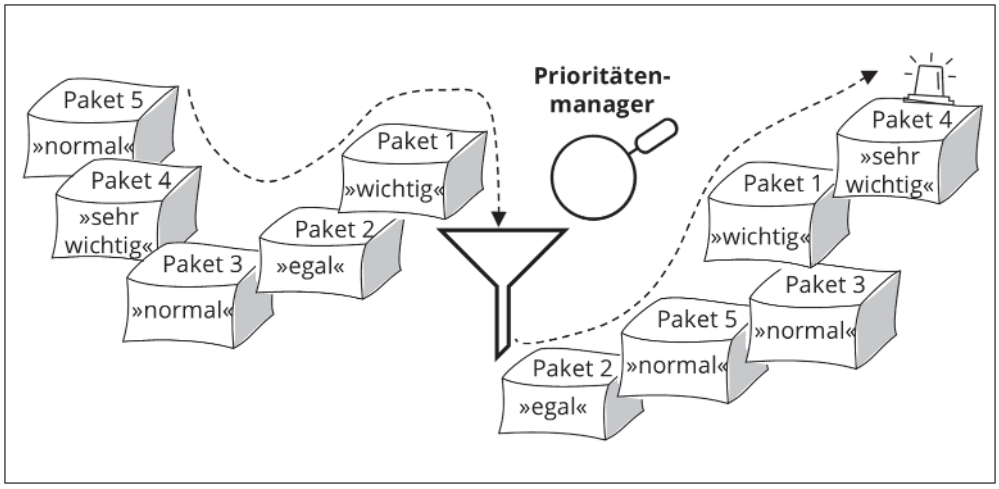

Abbildung 1.11: Priorisierung von Daten

Auch möglichen Datenverlusten kann prophylaktisch entgegengewirkt werden. Ein wirklich wichtiges Datenpaket wird beispielsweise in Industrienetzwerken vor dem Versand dupliziert und gleich zwei Mal auf unterschiedlichen Wegen verschickt. Auf der Empfängerseite wird dann das erste der beiden Pakete weitergegeben, das zweite verworfen.

Mehr zu den Möglichkeiten, wie besonders wichtige bzw. eilige Daten im Internet behandelt werden können, sind in Kapitel 13 zu finden.