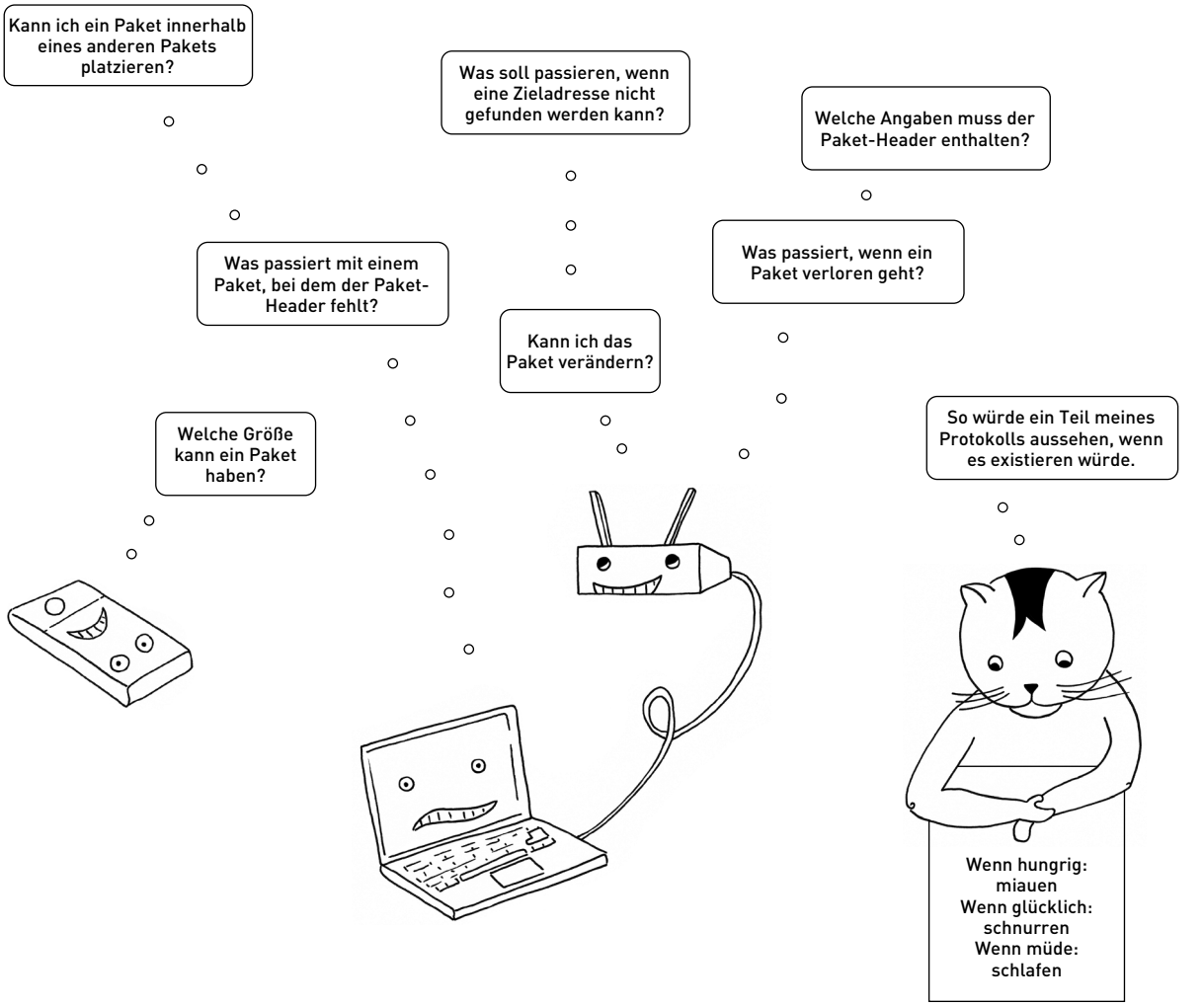
3

WIE KOMMUNIZIEREN GERÄTE IM INTERNET?

Protokolle

Wenn Geräte miteinander kommunizieren, brauchen sie eine Sprache, die beide verstehen. Wir nennen diese Sprache ein **Protokoll**, ein System von Regeln mit einer bestimmten Syntax, das definiert, wie Geräte im Internet miteinander kommunizieren und was zu tun ist, wenn Fehler auftreten. Fragen, die ein Protokoll beantworten kann:



Manchmal gibt es verschiedene Protokolle für dieselbe Kommunikation. Zum Beispiel definieren mehrere Protokolle, wie Pakete von Knoten zu Knoten transportiert werden sollen:

Das **Transmission Control Protocol (TCP)** wird verwendet, um Pakete genau und vollständig, aber nicht unbedingt zeitnah zu senden.

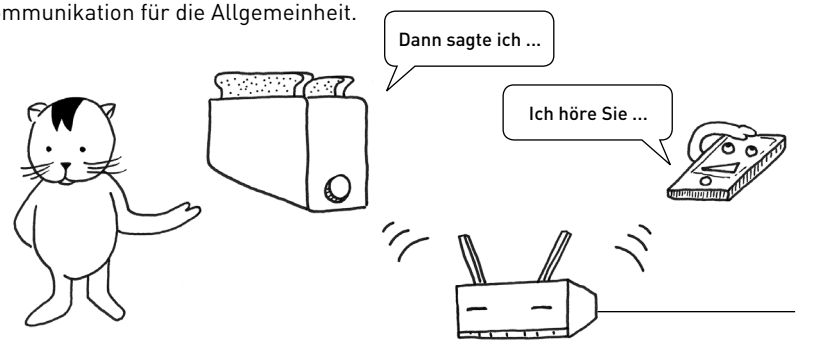
Das **User Datagram Protocol (UDP)** priorisiert die Geschwindigkeit, indem es sich nicht um die Reihenfolge oder die Zustellung der Pakete kümmert.

Quick UDP Internet Connections (QUIC) nutzt mehrere, schnelle UDP-Verbindungen, aber auf eine Art und Weise, die zuverlässig und präzise ist, wie TCP...

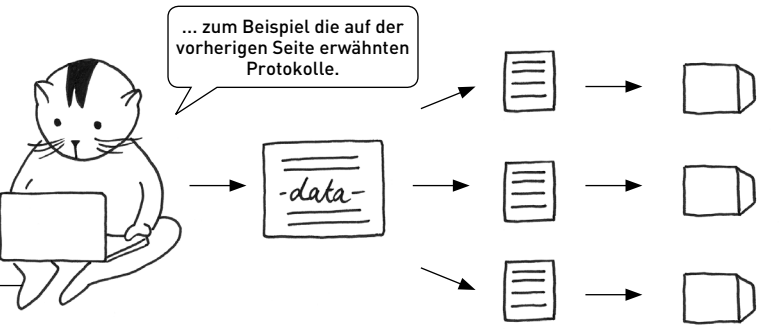
Die internationalen Organisationen für Protokolle und Standards

Internationale technische Organisationen und Institutionen definieren und verbessern Standards für Protokolle und Kommunikation für die Allgemeinheit. Im Folgenden finden Sie Beispiele:

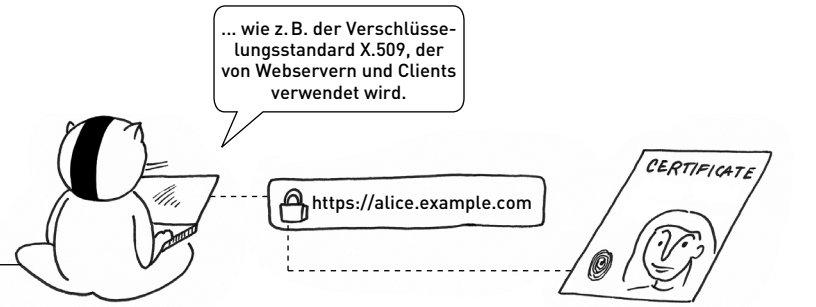
Das **Institute of Electrical and Electronics Engineers (IEEE)** befasst sich mit Protokollen für drahtgebundene und drahtlose Netzwerke.



Die **Internet Engineering Task Force (IETF)** erstellt und veröffentlicht Internet-Kommunikationsprotokolle.



Die **Standardisierungssektion der Internationalen Telekommunikations-Union (ITU-T)** kümmert sich um Telekommunikationsprotokolle.



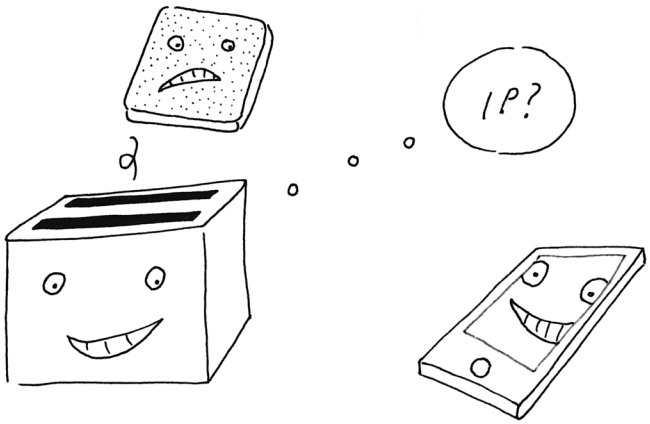
Die **International Organization for Standardization (ISO)** definiert Standards für Anwendungen in einer Vielzahl von Bereichen: Technologie, Wirtschaft, Regierung und Gesellschaft.

Das Internetprotokoll (IP)

Schauen wir uns ein wichtiges Protokoll genauer an: das **Internetprotokoll**, das das Format von IP-Adressen und IP-Paketen definiert.

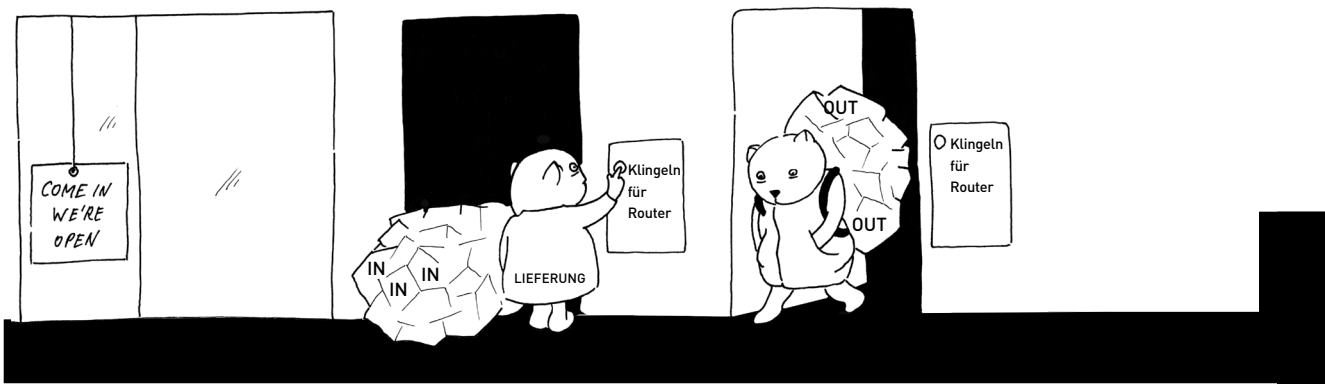
Das Internetprotokoll (IP) normiert, wie Pakete strukturiert sind und wie Adressen im Internet formatiert sein müssen, damit Pakete an ihr Ziel gelangen.

Sobald ein Gerät eine Verbindung zu einem Netzwerk herstellt, erhält es eine Netzwerkadresse. Um mit anderen Geräten im Internet zu kommunizieren, muss diese Adresse dem Internetprotokoll-Standard folgen. Schauen wir uns diesen speziellen Typ von Netzwerkadresse, genannt IP-Adresse, genauer an.



Jedes Gerät, das im »Internetprotokoll« spricht, kann mit anderen Geräten kommunizieren, die das gleiche Protokoll sprechen, seien es Computer, Telefone oder sogar Toaster.

Öffentliche und private IP-Adressen

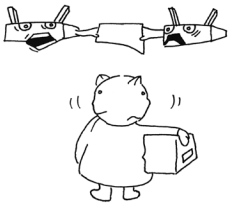


Das Internetprotokoll bezeichnet Adressen als:

Öffentlich, wenn sie direkten Zugang zum Internet haben, wie die, die Ihrem heimischen Router von Ihrem Internet-Service-Provider (ISP) zugewiesen wurde.

Privat, wenn sie keinen direkten Zugang zum Internet haben, sondern über einen Vermittler verbunden sind, wie die, die den an Ihren Router zu Hause angeschlossenen Geräten gegeben wurden. Private Adressen sind nur innerhalb von privaten Netzwerken wie lokalen Netzwerken (LAN) oder virtuellen privaten Netzwerken (VPN) zugänglich.

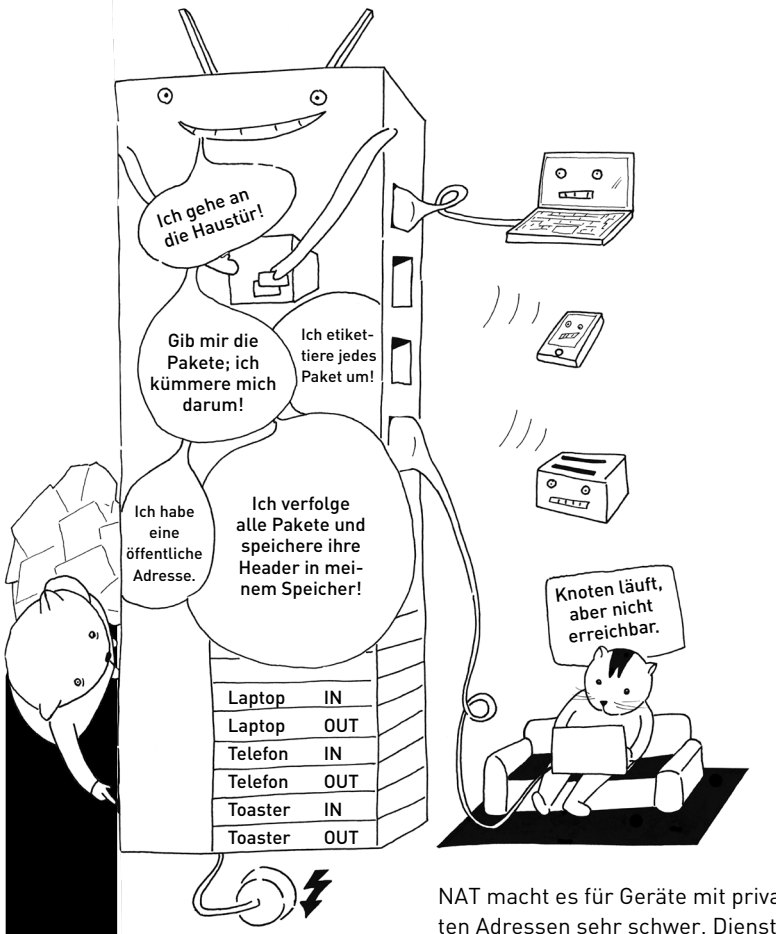
Ihr Router zu Hause hat eine öffentliche Adresse, aber da er die Paketzustellung innerhalb des Haushalts übernimmt, fungiert er auch als Vermittler für Geräte mit privaten Adressen innerhalb des privaten Netzwerks Ihres Hauses.



In einem Netzwerk kann immer nur ein Gerät eine bestimmte Adresse benutzen, daher muss eine öffentliche IP-Adresse für den ganzen Erdball eindeutig sein.

Adressübersetzung

Wenn sich ein privates Netzwerk mit dem Internet verbindet und Pakete über einen Router versendet, verwendet der Router eine Technik namens **Network Address Translation (NAT)**, um die Adress-Tags der Pakete umzuschreiben.
Bei der Verwendung von NAT behält der Router alle Informationen darüber, wer welche Pakete gesendet hat, in seinem Speicher. Wenn das Netzwerk eine Antwort aus dem Internet erhält, schreibt der Router die Tags der eingehenden Pakete um und sendet die Pakete an die private Adresse, die laut seinem Speicher für den Empfang vorgesehen ist. Wenn sich der Router ausschaltet, gehen alle diese Informationen verloren.



NAT macht es für Geräte mit privaten Adressen sehr schwer, Dienste im Internet anzubieten, da sie von außen nicht ohne Weiteres zu erreichen sind.

IPv4-Adressen

NAT kommt nur in der vierten Version des Internetprotokolls vor, die als **IP-Version 4 (IPv4)** bekannt ist. Dies ist die Version, die wir am häufigsten verwenden.

Eine IPv4-Adresse besteht aus vier Zahlenblöcken im Bereich von 0 bis 255, die durch Punkte getrennt sind: 198.51.100.7.

Diese vier Zahlen sind eigentlich vier Gruppen von **acht Binärziffern (Bits)**. Ein Satz von acht Binärziffern wird oft als ein **Byte** oder ein **Oktett** bezeichnet. IPv4 stellt diese binären Ziffern als Dezimalzahlen dar, um die Lesbarkeit zu verbessern:

Binärdarstellung:	11000110.	00110011.	01100100.	00000111
Dezimaldarstellung:	198	.51	.100	.7

Private Adressen beginnen mit:

192.168.xxx.xxx
10.xxx.xxx.xxx
172.16.xxx.xxx - 172.31.xxx.xxx

Andere Adressen sind reserviert und können nicht für das Routing von Datenverkehr über ein Netzwerk verwendet werden:

0.0.0.0 - 0.0.0.31

127.xxx.xxx.xxx

Alle anderen Adressen sind öffentlich.

IPv6-Adressen

Das Problem mit dem IPv4-Adressformat ist, dass es nur etwa 4,3 Milliarden Adressen bereitstellt. Das mag viel erscheinen, aber mit mehr und mehr Geräten, die sich mit dem Internet vernetzen, sind uns die möglichen Adressen ausgegangen! Deshalb haben wir eine neuere Version von IP erfunden – **IP Version 6 (IPv6).**

Eine IPv6-Adresse besteht aus acht Blöcken von 16-Bit-Zahlen, die durch Doppelpunkte getrennt sind. Die 16-Bit-Zahlen werden oft als Hexadezimalzahlen dargestellt, um die Lesbarkeit zu verbessern.

Binärdarstellung	0010000000000001:0000110110111000:0000000000000000:0000000000000001: 0000000000000000:0000000000000000:0000000000010000:0000000111111111
Hexadezimaldarstellung	2001:0DB8:0000:0001:0000:0000:0010:01FF
Verkürzte Hexadezimaldarstellung Aufeinanderfolgende Blöcke von Nullen können durch einen Doppelpunkt dargestellt werden.	2001:0DB8:0000:0001::0010:01FF

IPv6 verwendet 128 Bit für jede Adresse, was uns 2^{128} oder 340.282.366.920.938.463.463.374.607.431.768.211.456 (mehr als 340 Undezillionen) mögliche Adressen gibt.

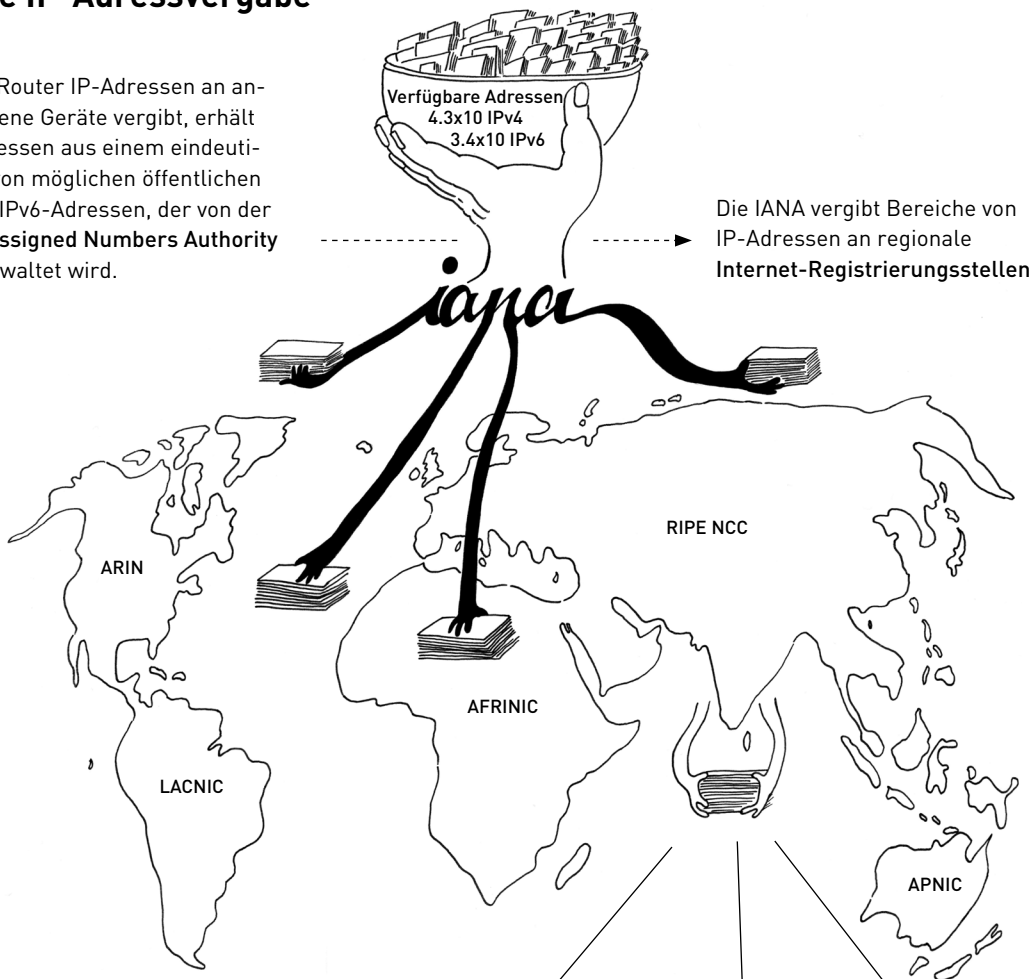
Das ist genug, um 667.126.144.800.000.000 Adressen für jeden Quadratmillimeter der Erdoberfläche bereitzustellen.

IPv6 ermöglicht auch die Verwendung von **Unique Local Addresses (ULA)** – das sind private IP-Adressen innerhalb von Netzwerken, die keinen Zugang zur Außenwelt haben. Allerdings können Pakete zu und von diesen Adressen nur innerhalb privater Netzwerke zugestellt werden und können nicht mit dem globalen IPv6-Internet kommunizieren.

IPv6 hat einen weiteren Vorteil gegenüber IPv4. Immer wenn sich ein Gerät mit einem heimischen Router verbindet, der IPv6 spricht, erhält das Gerät nicht nur eine private, durch NAT umgeschriebene Adresse, die von der Außenwelt nicht erreichbar ist, sondern eine ganze Reihe von Adressen, die alle öffentlich erreichbar sind. Dies ermöglicht es den Geräten, Dienste anzubieten und aktiv am Internet teilzunehmen.

Globale IP-Adressvergabe

Wenn ein Router IP-Adressen an angeschlossene Geräte vergibt, erhält er die Adressen aus einem eindeutigen Pool von möglichen öffentlichen IPv4- und IPv6-Adressen, der von der **Internet Assigned Numbers Authority (IANA)** verwaltet wird.

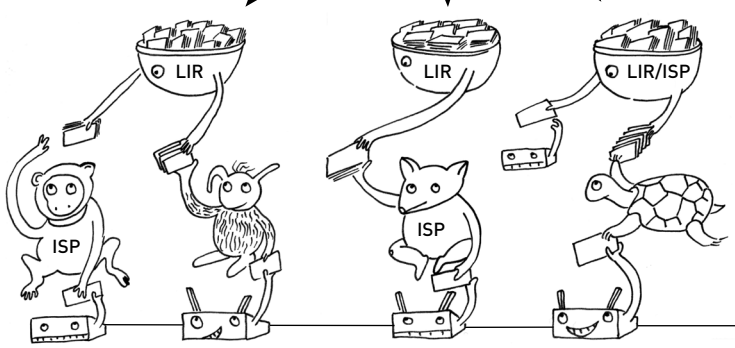


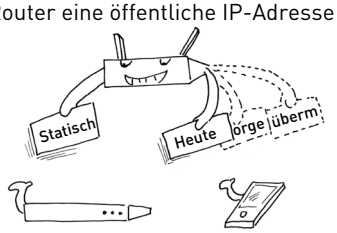
Die IANA vergibt Bereiche von IP-Adressen an regionale **Internet-Registrierungsstellen (RIR)**.

Die RIR geben die IP-Bereiche dann an **lokale Internet-Registrierungsstellen (LIR)** weiter.

Die LIR geben die Bereiche entweder an weitere Subunternehmer weiter oder sind selbst **Internet-Service-Provider (ISP)**.

Schließlich weisen die ISP jedem Router eine öffentliche IP-Adresse zu.





Es ist wichtig zu wissen, dass eine IP-Adresse **statisch** zugewiesen werden kann, sodass sie für ein bestimmtes Gerät immer dieselbe ist, oder **dynamisch**, sodass sie sich regelmäßig ändert.

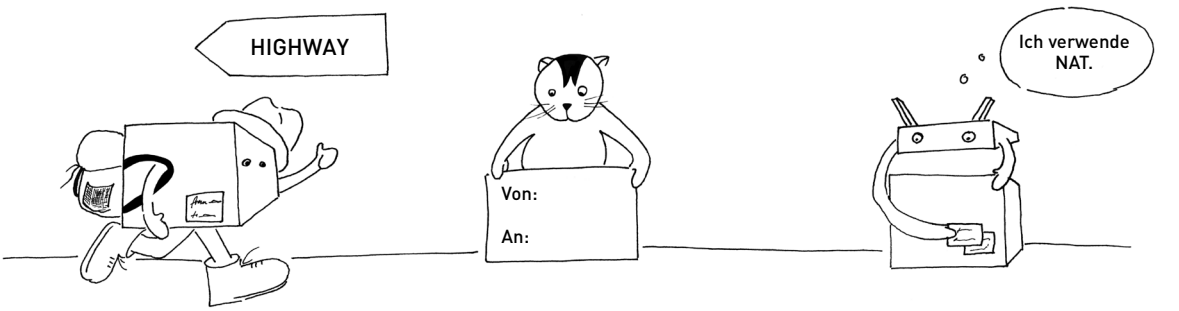
Wir verwenden statische IP-Adressen meist für Server: Sie sollten immer unter der gleichen Adresse erreichbar sein.

IP-Routing

Nachdem wir nun wissen, wie Adressen im Internet aussehen und woher wir sie bekommen, wollen wir uns ansehen, wie Pakete reisen.

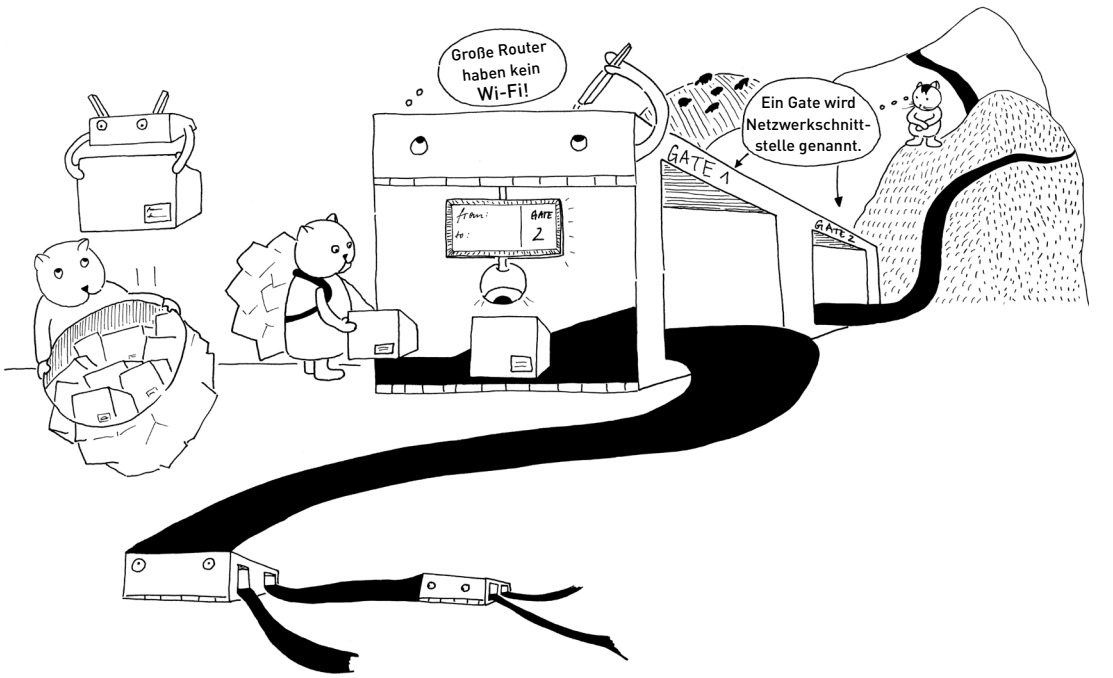
Wie bereits erwähnt, enthalten Pakete Informationen, sogenannte Paket-Header, die Absender- und Empfängeradressen umfassen und die angeben, woher ein Paket kommt und wohin es geht.

Wir haben gesehen, dass in einem Netzwerk, das NAT verwendet, ein IPv4-Router Pakete so kennzeichnet, dass Knoten mit privaten Adressen, die Pakete ins Internet senden, eine Antwort erhalten können. In Netzwerken, die kein NAT verwenden, z. B. in Netzwerken, die IPv6 verwenden, ist das Neukennzeichnen nicht notwendig.



Was passiert an dieser Stelle? Wenn ein Router Pakete an eine andere IP-Adresse im Internet sendet, sendet er die Pakete zuerst an den nächsten Router, den er kennt. Dies ist in der Regel der große Router unseres ISP, der wie ein Postamt fungiert.

Im großen Router werden die Paket-Header gelesen und an das Ziel im gleichen Netzwerk oder an einen anderen Router in Richtung des Ziels gesendet. Der erste Teil einer IP-Adresse zeigt an, ob das Paket auf ein Zielgerät im gleichen Netzwerk des Routers adressiert ist, sodass der Router weiß, ob er die Pakete an sein eigenes Netzwerk oder weiter an den nächsten ihm bekannten Router senden muss. Jeder Router auf dem Pfad tut dies, bis die Pakete an ihrem Ziel ankommen.



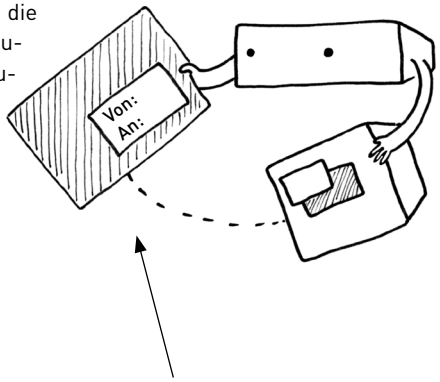
Internetprotokoll-Sicherheit (IPsec)

Im Internet werden Pakete durch mehrere Router geschickt, bevor sie an ihrem Ziel ankommen. Router können Paket-Tags lesen und verändern, aber auch den Inhalt von Paketen kopieren, verlieren, verwerfen, untersuchen oder verändern.

Dies gibt Angreifern die Möglichkeit, Datenpakete zu senden und dabei vorzugeben, ein anderer Computer zu sein, indem sie eine gefälschte Absender-IP-Adresse in das Paket-Tag schreiben. Dies wird als IP-Spoofing bezeichnet.

Durch das Ändern der Absender-IP-Adresse eines Paket-Tags kann ein Angreifer seine wahre Herkunft verbergen und anonym bleiben oder Ihnen vorgaukeln, dass diese Pakete von irgendwoher kommen, wo sie nicht herstammen.

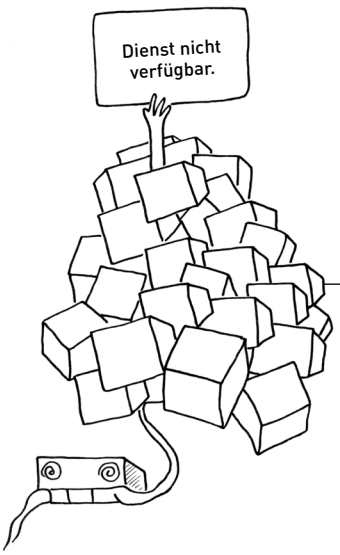
Es gibt eine Lösung für IP-Spoofing: **Internet Protocol Security (IPsec)**, ein Protokoll, das mit einer Vielzahl von Mechanismen ausgestattet ist, um die Integrität, Authentizität und Vertraulichkeit von Datenpaketen sicherzustellen.



Kryptografische Funktionen liefern Informationen über den Paket-Header.

Authentizität und Integrität werden durch kryptografische Funktionen gewährleistet, die überprüfen, dass das Paket, der Paket-Header und die Absenderadresse nicht verändert oder manipuliert wurden. Die Vertraulichkeit wird durch die Verschlüsselung des Paketinhalts gewährleistet.

Während Pakete in normalem IP ungehindert übertragen werden, verwerfen Geräte und Router, die IPsec verwenden, jedes Paket, das nicht vertrauenswürdig oder anderweitig falsch zu sein scheint.



Auf diese Weise kann IPsec auch vor **Denial-of-Service-Angriffen (DoS)** schützen, bei denen eine ungewöhnlich große Menge an Paketen an eine Ziel-IP-Adresse gesendet wird, in der Regel von vielen verschiedenen Absenderadressen gleichzeitig, bis das Zielgerät überlastet ist und nicht mehr auf Anfragen reagieren kann IPsec bietet Mittel zur Lösung von Problemen mit der Integrität, Authentizität und Vertraulichkeit von Datenpaketen, ist aber aufgrund seiner Komplexität nicht weit verbreitet.