Oliver Kreipl, Dorian Karnbaum, Marc Remolt, Thorsten Schneider

Einführung in TCP/IP-Networking

Ein Webmasters Press Lernbuch

Version 1.2.0 vom 29.01.2019

Autorisiertes Curriculum für das Webmasters Europe Ausbildungs- und Zertifizierungsprogramm

Inhaltsverzeichnis

Internetschicht

7

In dieser Lektion lernen Sie

- was die Aufgaben der Internetschicht sind.
- welche Protokolle in dieser Schicht ihre Arbeit verrichten.
- welche Netzwerkhardware dort ihren Dienst verrichtet.

7.1 Aufgaben der Internetschicht

Die Internetschicht ist für die eigentliche Zustellung der Datenpakete über Netzwerke hinweg zuständig. Durch die weltweit eindeutigen IP-Adressen kann ein Zielhost erreicht werden, egal wo er sich physikalisch befindet solange er am Internet angeschlossen ist.

Die TCP/IP-Internetschicht entspricht im ISO/OSI-Modell der Netzwerkschicht, also Layer 3.

7.2 Protokolle der Internetschicht

7.2.1 IP

Das wichtigste Protokoll der Internetschicht ist ***IP***, das ***Internet Protocol***. Es ist für den Transport der Datenpakete (sog. IP-Datagramme) über IP-Netze hinweg zuständig. Dank IP können wir im Internet mit Hosts kommunizieren, auch wenn sich diese am anderen Ende der Welt befinden.

Dem IP-Protokoll habe ich eine eigene Lektion, nämlich Lektion 8, gewidmet. Daher werde ich hier nicht näher auf das Protokoll eingehen.

7.2.2 ICMP

ICMP, das ***Internet Control Message Protocol***, ist der kleine Helfer von IP. Es ist für den Austausch von Nachrichten, Statusmeldungen und Fehlern zuständig, rüstet also die in IP fehlenden Möglichkeiten zum Informationsaustausch zwischen Routern und Hosts nach.

Auch ICMP hat eine eigene Lektion erhalten, nämlich Lektion 10.

7.3 Router und Routing

7.3.1 Router

Ein ***Router*** ist eine Netzwerkhardware, die mehrere Netzwerke miteinander verbindet. Dabei ist der Router in jedem dieser Netzwerke mit einem eigenen Netzwerkinterface vertreten. Er hat also mindestens für jedes Netz, in dem er präsent ist, eine Netzwerkkarte.

Dabei kann ein Router auch Netze mit unterschiedlicher Technologie verbinden. So kann ein Router zum Beispiel an zwei Ethernet-Netzen angeschlossen sein und zusätzlich noch eine Verbindung zu einem dritten Netz per Modem verwalten. Er muss nur über die passende Hardware verfügen.

Da ein Router auf Layer 3 des OSI-Modells arbeitet, wird er auch oft als ***Layer-3-Switch*** bezeichnet.

7.3.2 Vorgang

Das eigentliche ***Routing*** ist die wichtigste Aufgabe, die Router durchführen müssen, daher auch ihr Name. Unter Routing verstehen wir die Weiterleitung von IP-Paketen von einem Netzwerk zum nächsten. Wie Sie bereits wissen, bilden Router die Übergänge zwischen verschiedenen Netzwerken und verbinden diese. Daher werden Sie auch oft als ***Gateways*** bezeichnet.

Sobald ein IP-Paket ein Netzwerk verlassen muss, wird es an einen der in diesem Netz vorhandenen Router gesendet. Dieser entscheidet dann, an welches an ihn angeschlossene Netz das Paket weitergeleitet werden soll.

Dort nimmt der nächste Router das Paket entgegen und entscheidet wieder, wohin das Paket weiter versendet werden soll. Dieser Vorgang wiederholt sich so lange, bis das Paket das Zielnetzwerk erreicht hat. Der letzte Router weiß, dass das Paket für ein Netzwerk bestimmt ist, das direkt an ihn angeschlossen ist. Daher leitet er es nicht mehr an einen weiteren Router, sondern sendet es direkt an den Empfänger.

Die einzelnen Stationen eines IP-Pakets werden auch als ***Hops***, also Hüpfer, bezeichnet, da das Paket von Netz zu Netz *springt*.

7.3.3 Routingtabellen und Standardroute

Woher weiß ein Router aber, wohin er ein Paket weiterleiten muss? Jeder Router verwaltet sogenannte ***Routingtabellen***, das sind Konfigurationen, welche IP-Pakete er wohin weiterleiten muss.

Beispiel

Auf einem Linux-basierten Router wird die Routingtabelle mit dem Kommando `route` ausgegeben. Die Option `-n` sorgt dafür, dass IP-Adressen statt Hostnamen ausgegeben werden. Der Befehl benötigt unter Debian wieder Root-Rechte.

```
oliver@gollum:~$ sudo route -n
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref Use Iface
0.0.0.0        192.168.255.14  0.0.0.0         UG    0      0   0   eth4
192.168.255.8  0.0.0.0         255.255.255.248 U     0      0   0   eth4
192.168.3.0    0.0.0.0         255.255.255.0   U     0      0   0   eth3
192.168.2.0    0.0.0.0         255.255.255.0   U     0      0   0   eth2
192.168.1.0    0.0.0.0         255.255.255.0   U     0      0   0   eth1
192.168.0.0    0.0.0.0         255.255.255.0   U     0      0   0   eth0
```

Dieser Beispiel-Router hat sechs Einträge in der Routingtabelle. Lassen Sie uns die Einträge als Beispiel durchgehen.

Die *Destination* ist das Ziel der IP-Pakete. Wenn also ein IP-Paket das Netz mit der Adresse `192.168.255.8` als Ziel hat, werden die Einstellungen dieser Zeile aktiv. Hat ein IP-Paket das Netz `192.168.2.0` als Ziel, gelten die Einträge der entsprechenden Zeile. Welche IP-Adresse zu welchem Netz gehört, werden wir in der Lektion 9 »IP-Adressierung und Subnetting« durchsprechen. Akzeptieren Sie momentan einfach, dass die IP-Adressen `192.168.2.1`, `192.168.2.2` bis `192.168.2.254` zum Netz `192.168.2.0` gehören.

Die Spalte *Gateway* legt fest, über welchen Router die Pakete weitergeleitet werden. Steht hier `0.0.0.0`, ist kein Gateway notwendig, da sich das Ziel direkt im angrenzenden Netz befindet. In der letzten Zeile der Ausgabe ist ein Gateway eingetragen. Alle Pakete, die das Netz `0.0.0.0` als Ziel haben, werden über das Gateway mit der IP-Adresse `192.168.255.14` weitergeleitet. Was es mit dem komischen Netz `0.0.0.0` auf sich hat, klären wir gleich.

Die dritte Spalte *Genmask* legt die Subnetzmaske des Zielnetzes fest. Dieses Thema besprechen wir im Abschnitt 9.5.2 »Subnetting«.

Die Spalten *Flags*, *Metric* und *Ref* sind für uns erst einmal nicht von Bedeutung.

Die letzte Spalte *Iface* gibt das Netzwerk-Interface an, also die Netzwerkkarte, über die die Pakete weitergeleitet werden. Hat ein IP-Paket also das Zielnetz 192.168.2.0, wird dieses Paket über die Netzwerkkarte `eth2`, was für *Ethernet-Karte Nummer 2* steht, weitergeleitet. Da die Karten mit 0 beginnend durchnummeriert werden, handelt es sich also um die dritte Netzwerkkarte dieses Routers.

Jeder Router und sogar jeder Host, der an ein Netzwerk angeschlossen ist, hat zumindest einen Eintrag in seiner Routingtabelle. Es handelt sich dabei um die sogenannte Standardroute. Dabei handelt es sich um die Route, die verwendet wird, wenn der Router selbst nichts mehr mit dem IP-Paket anfangen kann. Wenn ein Router für ein Paket keinen passenden Eintrag in seiner Tabelle hat, wird diese Standardroute aktiv.

In unserem Beispiel handelt es sich bei dem letzten Eintrag um die Standardroute:

```
0.0.0.0    192.168.255.14    0.0.0.0    UG    0    0    0    eth4
```

Diese besondere Route erkennen Sie an der *Destination* von `0.0.0.0`. Das Zielnetzwerk steht stellvertretend für jedes beliebige Netz, also im Prinzip das gesamte Internet. Der Eintrag greift also immer, egal welche IP-Adresse als Ziel angegeben ist. Die Standardroute wird immer dann aktiv, wenn kein anderer Eintrag in der Routingtabelle auf das Zielnetzwerk des IP-Pakets verweist.

Als Gateway der Standardroute wird meistens der nächst höhere Router im Netzwerk eingetragen. Im Prinzip steht in der Standardroute also Folgendes: Wenn du selbst nicht mehr weiter weißt, leite das Paket an deinen Vorgesetzten weiter. Dieser nächsthöhere Router hat selbst wieder eine Standardroute, die auf einen Router verweist, der noch höher in der Hierarchie steht, und so weiter.

Die Hauptrouter der Internet-Provider verfügen über sehr umfangreiche Routingtabellen. Das bedeutet, spätestens diese Router können mit dem Paket etwas anfangen und leiten es in die richtige Richtung (z.B. den richtigen Kontinent) weiter.

7.3.4 Routingprotokolle

Ein Router, der einen Knotenpunkt des Internet verwaltet, zum Beispiel einen Übergang zwischen Kontinenten oder Backbones, benötigt oft tausende Einträge in seiner Routingtabelle, um effektiv arbeiten zu können. Je mehr Netze er kennt, umso bessere Entscheidungen kann er treffen, wohin ein Paket geleitet werden muss.

Diese sich ständig ändernden Einträge von Hand zu verwalten, wäre ein nicht zu leistender Aufwand. Daher werden viele dieser Einträge automatisch verwaltet. Einträge, die von Hand gepflegt werden, nennt man ***statische Routen***, die automatisch angelegten ***dynamische Routen***.

Dynamische Routen werden generiert, indem Router untereinander Informationen austauschen. Verfügt ein Router über eine neue Route, zum Beispiel eine statische, leitet er diese Information an seine benachbarten Router weiter. Diese tragen die Daten bei sich als dynamische Route ein und leiten die Information ebenfalls weiter. So können sich Routing-Einträge mit sehr wenig manuellem Aufwand sehr schnell verbreiten.

Dieser Austausch findet über ***Routingprotokolle*** statt. Die bekanntesten sind:

- ***BGP***, das *Border Gateway Protocol*
- ***RIP***, das *Routing Information Protocol*
- ***OSPF***, *Open Shortest Path First*
- ***EIGRP***, das *Enhanced Interior Gateway Routing Protocol*

Die Arbeitsweise der einzelnen Protokolle ist teilweise sehr unterschiedlich und ich erspare Ihnen die technischen Details. Für den Betrieb einiger weniger Server im Internet sind diese Kenntnisse noch nicht nötig. Wenn Sie allerdings eine Karriere bei einem Internet-Provider oder einem Rechenzentrum anstreben, werden Sie tiefgehende Freundschaft mit diesen Routingprotokollen schließen müssen.

7.4 Zusammenfassung

Die Protokolle der Internetschicht sind für den Transport der Datenpakete durch TCP/IP-Netzwerke zuständig. Anhand der IP-Adresse kann das IP-Protokoll Zielhosts weltweit finden und Pakete zustellen. Es wird von ICMP[45] in seiner Aufgabe unterstützt.

Den Vorgang, ein Datenpaket von einem Netzwerk zum nächsten zu transportieren, nennt man Routing. Anhand ihrer Routingtabellen entscheiden Router, wohin sie ein Datenpaket weiterleiten. Ein statischer Eintrag in der Routingtabelle ist ein manuell gepflegter Eintrag, unter einer dynamischen Route versteht man einen Eintrag, die ein Router von benachbarten Routern erhalten hat. Dieser Austausch von Routen findet über Routingprotokolle wie OSPF oder BGP statt.

7.5 Testen Sie Ihr Wissen

1. Beschreiben Sie kurz die Aufgabe der Internetschicht.
2. Auf welcher Ebene des OSI-Modells arbeiten Router?
3. Wie werden sie deshalb auch oft genannt?
4. Was versteht man in der Netzwerktechnik unter einem Hop?
5. Was ist eine Routingtabelle?
6. Warum benötigt ein Router (fast) immer eine Standardroute?
7. Nennen Sie drei Routingprotokolle.

45. Siehe Lektion 10 »ICMP«

IP

8

In dieser Lektion lernen Sie

- das IP-Protokoll näher kennen.
- den Aufbau des IP-Headers.
- den Vorgang, wie IP-Pakete im Internet ihren Weg finden.

8.1 IP Internet Protocol

Das Internet-Protokoll IP deckt Schicht 3 des ISO/OSI-Referenzmodells (Netzwerkschicht) ab. Seine Aufgabe besteht darin, die Datenpakete des Absenders innerhalb eines Netzwerkes oder über mehrere Netzwerke hinweg zum Empfänger zu transportieren. In diesem Sinne kann es mit einem Logistik-Unternehmen, z.B. der Post, verglichen werden. IP-Pakete werden auch als ***Datagramme***[46] bezeichnet, um sie von den Paketen anderer Netzwerkprotokolle bzw. darunterliegender Schichten (z.B. Ethernet-Pakete) zu unterscheiden. Der Adresskopf (Header) des IP-Pakets enthält die Absender- und Empfänger-IP-Adresse der miteinander kommunizierenden Computer (diese werden auch Netzwerkknoten oder Netzknoten genannt).

IP ist ein ***verbindungsloses*** Protokoll[47], d.h. vor der Datenübertragung werden zwischen Sender und Empfänger keinerlei Kontrollinformationen ausgetauscht. IP kümmert sich nicht darum, ob der Zielhost erreichbar ist oder ob es ihn überhaupt gibt. IP ist nur für den eigentlichen Transport zuständig.

IP ist ein ***unzuverlässiges*** Protokoll, da es selbst keinerlei Mechanismen zur Fehlererkennung und Korrektur besitzt und keine Empfangsquittungen anfordert. Wie gesagt, IP kümmert sich nur um den eigentlichen Transport.

Dies bedeutet aber nicht, dass man sich auf IP nicht verlassen könnte, ganz im Gegenteil: Wenn das Netzwerk funktionstüchtig ist, liefert IP die Pakete auch korrekt aus. Es ist ähnlich wie mit Ihren Briefen: Die meisten Briefe senden Sie nicht per Einschreiben, und trotzdem wissen Sie, dass die Briefe in aller Regel auch beim Empfänger ankommen. Ohne Einschreiben jedoch können Sie sich nicht zu 100 Prozent sicher sein. Wirklich wichtige Post werden Sie daher wohl via Einschreiben versenden. Ähnlich ist es bei TCP/IP. Protokolle in anderen Schichten, vor allem TCP, können diese Art von Prüfung übernehmen.

8.2 Header

Der Header eines IP-Pakets umfasst normalerweise 20 Byte, wobei bis zu 40 Byte weitere optionale Felder hinzukommen können. Das Maximum liegt also bei 60 Byte. Lassen Sie mich Ihnen den IP-Header zuerst in der Übersicht vorstellen.

46. Ich ziehe es vor, die Pakete aller Schichten auch als Paket zu bezeichnen. Wo eine Verwechslung auftreten könnte, setze ich das Protokoll als Präfix vor den Begriff Paket, also zum Beispiel TCP-Paket oder IP-Paket.

47. Als verbindungsorientiert werden Protokolle bezeichnet, die vor dem Datenaustausch zu Kontrollzwecken bereits eine Kommunikation mit dem Empfänger aufbauen, z.B. um zu checken, ob der Empfänger überhaupt bereit ist, Daten entgegenzunehmen.

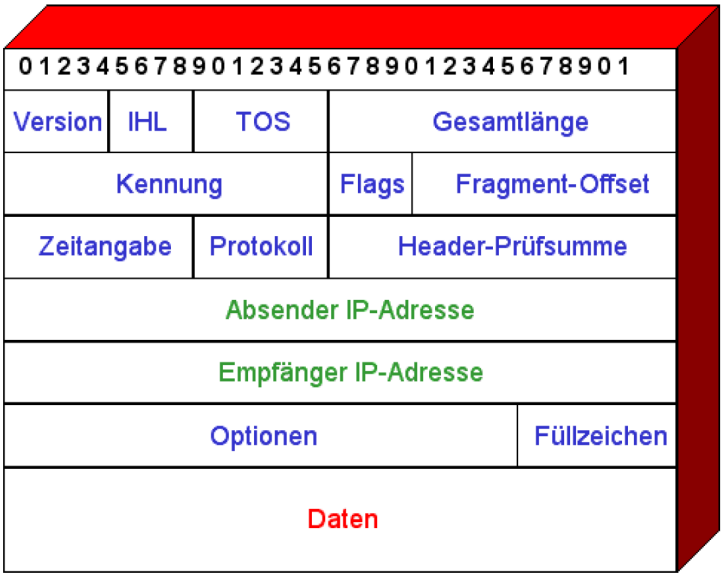

Abb. 15 *Format eines IP-Datagramms*

Feldbezeichnung	**Länge des Feldes(Bits)**	**Beschreibung**
Version	4	Gibt die IP-Versionsnummer an. Zur Zeit wird noch überwiegend IPv4 eingesetzt.
IHL	4	*Internet Header Length* - gibt die Länge des IP-Headers an. Da dieser zwischen 20 und 60 Byte lang sein kann, ist es nötig, im Header die tatsächliche Länge festzuhalten.
TOS	8	*Type of Service* - dient zur Festlegung, wie das Datenpaket behandelt wird (z.B. Priorität, Verzögerung, Durchsatz).
Gesamtlänge	16	Gibt die Gesamtlänge des IP-Pakets, d.h. Header und Daten, an.
Kennung	16	Router sind in der Lage, bei Bedarf IP-Pakete weiter zu zerlegen (fragmentieren), wenn diese für die Datenleitung zu groß sind. Dieses Feld dient zur Erkennung der einzelnen Fragmente eines Pakets, um diese beim Empfänger wieder korrekt zusammenzusetzen. Alle Fragmente eines Original-Pakets weisen dieselbe *Kennung* auf.
Flags	3	Zeigt an, ob ein Datagramm fragmentiert werden darf und welches das letzte Fragment ist.
Fragment-Offset	13	Legt die Position eines Fragmentes fest. Dies ist notwendig, um die IP-Fragmente beim Empfänger wieder in die richtige Reihenfolge zu bringen.
TTL	8	*Time-to-Live* Gibt die maximale Lebensdauer eines Datagramms in *Hops* an. Der Maximalwert beträgt 255.
Protokoll	8	In diesem Feld wird das Protokoll für die Transportschicht verschlüsselt, z.B. TCP, UDP, OSPF.
Kopf-Prüfsumme	16	Über die Felder des IP-Headers wird eine Prüfsumme gebildet und in diesem Feld abgelegt. Damit kann ein Router prüfen, ob der Header beim Transport beschädigt wurde, und das Paket verwerfen.
Absender-IP-Adresse	32	Enthält die IP-Adresse des Absenders. Die IP-Adressierung wird im nächsten Kapitel beschrieben.
Empfänger-IP-Adresse	32	Enthält die IP-Adresse des Empfängers.

Tabelle 8.1 *Felder des IP-Datagramms gemäß RFC 791.*

Feldbezeichnung	Länge des Feldes(Bits)	Beschreibung
Optionen	max. 32	IP kann durch verschiedene Optionen an die Protokolle der höheren Schichten angepasst werden. Die Feldlänge wird durch die Art und die Anzahl der Optionen bestimmt.
Füllzeichen	variabel	Dieses Feld dient zum Auffüllen der leeren Bits, falls das Feld Optionen nicht vollständig genutzt wird.
Daten	variabel	Enthält die eigentlichen Dateninformationen.

Tabelle 8.1 *Felder des IP-Datagramms gemäß RFC 791.*

8.3 IP-Adressen

Das wichtigste Merkmal des IP-Protokolls sind wohl die IP-Adressen. Diese werden im IP-Header zwar binär (also mit 0 und 1) abgelegt, wir kennen jedoch eher die dezimale Schreibweise. Eine IP-Adresse der Version 4 des Protokolls besteht aus vier Zahlen zwischen 0 und 255, die jeweils mit einem Punkt getrennt sind, also zum Beispiel 192.168.3.8 oder 12.17.100.0.

IP-Adressen werden im Internet zur eindeutigen Identifizierung von Hosts verwendet. Jede IP-Adresse darf weltweit nur ein einziges Mal verwendet werden.[48] Die Router verwenden die Empfänger-IP-Adresse eines Pakets, um es weltweit zu seinem Zielhost zu bringen.

Da dem Thema IP-Adressen eine eigene Lektion gewidmet ist (Lektion 9 »IP-Adressierung und Subnetting«), möchte ich an dieser Stelle nicht weiter auf das Thema eingehen.

8.4 Aufgaben von IP

Den weltweiten Versand von Datenpaketen zu organisieren und zu verwalten ist eine enorme Aufgabe. Sehen wir uns doch einige Funktionen von IP an, die den Routern bei der Aufgabe helfen, IP-Pakete möglichst sicher ans Ziel zu bringen.

Bedenken Sie dabei, dass diese Funktionen von jedem Router auf dem Weg durchgeführt werden.

8.4.1 Validierung der IP-Headers

Wenn ein Router ein IP-Paket erhält, prüft er zuerst, ob das Paket auch nicht auf dem Transport beschädigt wurde. Dabei interessiert ihn nicht die Nutzlast des Pakets, sondern nur die Header-Informationen.

Wenn ein IP-Paket beim Absender erzeugt wird, berechnet dieser aus den Feldern des IP-Headers eine Prüfsumme und legt sie im Header ab. Jeder Router, der dieses Paket erhält, führt diese Berechnung ebenfalls durch und vergleicht sein Ergebnis mit dem im Header eingetragenen Wert. Weicht dieser ab, wurde der Header offensichtlich beschädigt und der Router verwirft das Paket sofort.

Wenn Sie sich jetzt fragen, warum IP nur den Header auf Beschädigungen prüft, nicht aber das ganze Paket, ist die Antwort ganz einfach. IP interessiert sich nicht dafür, was es transportiert, nur dass die Lieferung ankommt. Erst auf dem Zielrechner wird auch der Inhalt auf Beschädigungen geprüft, was aber die Transportschicht übernimmt.

Den Header auf jedem Router zu prüfen, ist eine sehr wichtige Aufgabe von IP. Stellen Sie sich vor, durch die Beschädigung würde das Feld mit der Absender-Adresse verändert. Das Paket wird korrekt zuge-

48. Ausgenommen die privaten IP-Adressen. Siehe Abschnitt 9.7 »Private IP-Adressen«.

stellt, doch die Antwort des Servers wird an den falschen Host versendet. Der ursprüngliche Absender wird die Antwort niemals erhalten.

8.4.2 Prüfen der TTL

Eine weitere wichtige Aufgabe von IP ist, den Müll wegzuräumen. Durch verschiedene Umstände, zum Beispiel falsch konfigurierte Router, kann es vorkommen, dass IP-Pakete ihr Ziel nicht erreichen können.

Beispiel

Der Router mit der IP-Adresse 12.14.5.1 erhält ein IP-Paket für den Empfänger 80.45.2.9. Gemäß seiner Konfiguration leitet er das Paket an einen weiteren Router (IP 12.25.2.255). Dieser prüft den Empfänger und leitet das Paket an einen dritten Router (IP 12.26.7.1) weiter.

So weit an sich nichts Besonderes. Doch Router Nummer 3 ist falsch konfiguriert. Er leitet das Paket an den Router mit der IP-Adresse 12.14.5.1, also unseren ersten Router weiter. Dieser erhält das Paket, leitet es an Router 2, dieser leitet es an Router 3

Sie sehen das Problem. Dieses IP-Paket wird bis in alle Ewigkeit[49] zwischen diesen Routern kreisen. Bei einem Paket ist dies kein Problem, aber stellen Sie sich vor, was passiert, wenn mit der Zeit tausende Pakete in dieser Schleife hängen.

Um Pakete auszufiltern, die ihr Ziel nie erreichen werden, bedient sich IP eines einfachen Mechanismus. Im Header-Feld TTL, also Time To Live (Lebenszeit), wird beim Absender eine Zahl eingetragen. Jeder Router, der dieses Paket nun erhält und weiterschickt, öffnet den Header und verringert die Zahl um 1. Wenn ein Router ein IP-Paket mit einer TTL von 0 erhält, wirft er es sofort weg.

Damit werden Pakete, die niemals ihr Ziel erreichen, zwar nicht sofort, aber zumindest nach einigen Sekunden aus dem Datenstrom entfernt.

In der Original-IP-Spezifikation wurde die TTL als Wert in Sekunden festgelegt, wobei der Wert bei jedem Hop um mindestens 1 verringert wird. Hat ein Hop länger gedauert, musste die TTL auch um mehr als 1 verringert werden.

Da heutzutage kein Router auch nur annähernd eine Sekunde für einen Hop benötigt, betrachtet man die TTL inzwischen als einen reinen Hop-Zähler. Jeder Router verringert den Wert um 1 und ignoriert die tatsächlich benötigte Zeit.

8.4.3 Fragmentierung

Darüber hinaus übernimmt IP auch die ***Fragmentierung*** eines Datenpakets und die Zusammensetzung der fragmentierten Pakete in der richtigen Reihenfolge beim Empfänger. Dies ist wichtig, da die maximale Paketgröße ***(Maximum Transfer Unit, MTU)***, die über ein Netzwerk transportiert werden kann, von dem zugrunde liegenden Netzwerkstandard abhängt.

Die MTU eines Ethernet ist anders als die von *ISDN* oder *ATM*. Da das Internet sich aus den unterschiedlichsten Netzwerken zusammensetzt, muss die Paketgröße an jedem Übergang von einem zum anderen Netzwerktyp angepasst werden.

Um das zu illustrieren, stellen Sie sich Folgendes vor: Sie sind Erdöl-Verkäufer und müssen den Transport des Öls von den Ölfeldern im persischen Golf bis zum Endabnehmer, dem Besitzer eines Einfamilienhauses in Berlin, organisieren. Hierbei kommen verschiedene Verkehrswege ins Spiel: Ein Tanker trans-

49. Oder zumindest, bis einer der Router resettet, umkonfiguriert oder ersetzt wird.

portiert das Öl auf dem Meer in den Hamburger Hafen. Dort muss es in viele Eisenbahnwagons umgeladen werden, da die MTU auf der Schiene kleiner ist als auf dem Meer. Im Berliner Bahnhof muss jeder Eisenbahnwagon auf mehrere Tanklaster aufgeteilt werden, da die MTU des Transportwegs Straße noch kleiner ist als auf der Schiene. Am Ziel angekommen, wird das Öl aus den vielen einzelnen Lastern in ein einzelnes großes Silo geladen.

Die Paketgröße muss also bei jedem Übergang von einem zu einem anderen Transportmedium angepasst werden. Am Ende wird die Nutzlast aus den vielen Teilen wieder zu einem großen Ganzen zusammengefügt.

Genauso verhält es sich auch im Internet. Wenn ein Router ein Paket erhält und über eine Route weiterleiten soll, für die das Paket zu groß ist, fragmentiert der Router das Paket. Dabei wird die Nutzlast des IP-Pakets in ausreichend kleine Teile aufgespalten und auf mehrere einzelne IP-Pakete verteilt.

Diese Fragment-Pakete weisen einige Besonderheiten auf, die Sie im Header sehen können:

- Das *Kennung*-Feld ist bei allen Fragment-Paketen identisch. Hierüber erkennt der Zielhost, welche Pakete zusammengehören.
- In dem Feld *Flags* gibt es ein Bit *More Fragments* (weitere Fragmente), das festlegt, ob nach diesem Fragment noch weitere folgen. Bei jedem Fragment, bis auf das letzte, ist dieser Wert auf 1 gesetzt. Das letzte Fragment (oder ein nicht fragmentiertes Paket) hat hier den Wert 0. Damit erkennt der Empfänger, wann er alle Pakete erhalten hat.
- Im Feld *Fragment-Offset* wird die Position des Frements im Originalpaket festgehalten. Dies ist notwendig, um die Fragmente später auch in der richtigen Reihenfolge zusammenzusetzen.

Mit diesen drei Informationen kann der Zielhost Fragmente wieder zum Original-IP-Paket zusammensetzen. Wenn das Feld *Fragment Offset* gesetzt ist, weiß der Host, dass er ein Fragment vor sich hat. Dann sammelt er alle Fragmente mit derselben *Kennung* ein, bis zum letzten, das *More Fragments* auf 0 gesetzt hat. Sobald er alle hat, baut er aus den Teilen wieder das alte Paket zusammen.

8.5 Zusammenfassung

Das IP-Protokoll ist das Transportmedium, das die Datenpakete vom Absender zum Zielhost transportiert. Durch die weltweit eindeutigen IP-Adressen kann IP den Empfänger eines IP-Pakets im Internet finden und ihm das Paket zustellen.

Dabei verfügt IP über einige nützliche Funktionen, die ihm die Aufgabe erst ermöglichen:

- Validierung des Headers über Prüfsummen
- Verwerfen alter Pakete mit Hilfe der TTL
- Fragmentierung von Paketen

8.6 Testen Sie Ihr Wissen

1. Warum wird IP als verbindungsloses Protokoll bezeichnet?
2. Warum wird IP als unzuverlässig bezeichnet?
3. Wie und warum prüft jeder Router ein IP-Paket auf Beschädigungen?
4. Was ist die Aufgabe des TTL-Felds im IP-Header?
5. Was versteht man unter der Fragmentierung eines IP-Pakets?
6. Warum muss IP Fragmentierung beherrschen?