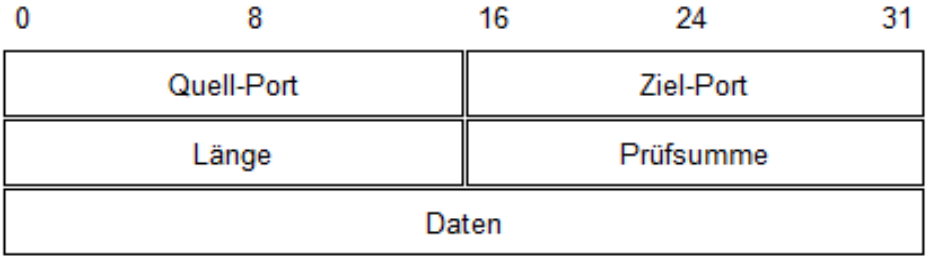
11 User Datagram Protocol (UDP)

Christian Zahler



Das *User Datagram Protocol* (Abk. UDP) ist ein **minimales, verbindungsloses Netzprotokoll**, das zur Transportschicht der Internetprotokollfamilie gehört. Aufgabe von UDP ist es, Daten, die über das Internet übertragen werden, der richtigen Anwendung zukommen zu lassen.

Die Entwicklung von UDP begann 1977, als man für die Übertragung von Sprache ein einfacheres Protokoll benötigte als das bisherige verbindungsorientierte TCP. Es wurde ein Protokoll benötigt, das nur für die Adressierung zuständig war, ohne die Datenübertragung zu sichern, da dies zu Verzögerungen bei der Sprachübertragung führen würde.

11.1 Eigenschaften

UDP stellt einen verbindungslosen, nichtzuverlässigen Übertragungsdienst bereit. Das bedeutet, dass es keine Garantie gibt, dass ein einmal gesendetes Paket auch ankommt, dass Pakete in der gleichen Reihenfolge ankommen, in der sie gesendet wurden oder dass ein Paket nur ein Mal am Empfänger eintrifft. Eine Anwendung, die UDP nutzt, muss daher gegenüber verloren gegangenen und unsortierten Paketen unempfindlich sein oder selbst entsprechende Korrekturmaßnahmen beinhalten.

Da vor Übertragungsbeginn nicht erst eine Verbindung aufgebaut werden muss, können die Hosts schneller mit dem Datenaustausch beginnen. Dies fällt vor allem bei Anwendungen ins Gewicht, bei denen nur kleine Datenmengen ausgetauscht werden müssen. Einfache Frage-Antwort-Protokolle wie das **Domain Name System** verwenden UDP um die Netzwerkbelastung gering zu halten und damit den Datendurchsatz zu erhöhen. Ein Drei-Wege-Handshake wie bei TCP für den Aufbau der Verbindung würde unnötigen Overhead erzeugen.

Daneben bietet die ungesicherte Übertragung auch den Vorteil von geringen Übertragungsverzögerungsschwankungen:
Geht bei einer TCP-Verbindung ein Paket verloren, so wird es automatisch erneut angefordert. Dies braucht Zeit, die Übertragungsdauer kann daher schwanken, was für Multimediaanwendungen schlecht ist. Bei VoIP z. B. würde es zu plötzlichen Aussetzern kommen bzw. die Wiedergabepuffer müssten größer angelegt werden. Bei verbindungslosen Kommunikationsdiensten bringen verlorengegangene Pakete dagegen nicht die gesamte Übertragung ins Stocken sondern vermindern lediglich die Qualität.

UDP übernimmt die Eigenschaften der darunterliegenden Vermittlungsschicht. Im Falle des *Internet Protocols* (IP) können Datenpakete maximal 65535 Bytes lang sein, wovon der IP-Header und UDP-Header insgesamt mindestens 28 Bytes belegen. UDP-Datagramme haben daher maximal 65507 Nutzdatenbytes. Solche Pakete werden jedoch von IP fragmentiert übertragen.

IP löscht Pakete etwa bei Übertragungsfehlern oder bei Überlast. Datagramme können daher fehlen. UDP bietet hierfür keine Erkennungs- oder Korrekturmechanismen wie etwa TCP. Im Falle von mehreren möglichen Routen zum Ziel kann IP bei Bedarf neue Wege wählen. Hierdurch ist es in seltenen Fällen möglich, dass später gesendete Daten früher gesendete überholen. Außerdem ist es möglich, dass ein einmal abgesendetes Datenpaket mehrmals beim Empfänger eintrifft.

11.2 UDP-Header

Der UDP-Header besteht aus vier Datenfeldern, die alle jeweils 16 Bit groß sind:

Der **Quell-Port** gibt die Portnummer des sendenden Prozesses an. Diese Information wird benötigt, damit der Empfänger auf das Paket antworten kann. Da UDP verbindungslos ist, ist der Quell-Port optional und kann auf den Wert "0" gesetzt werden.

Der **Zielport** gibt an, welcher Prozess das Paket empfangen soll.

Das **Längenfeld** gibt die Größe des Paketes, bestehend aus den Daten und dem Header, in Oktetten an. Der kleinstmögliche Wert sind 8 Oktette.

In dem **Prüfsummenfeld** kann eine 16 Bit große Prüfsumme mitgesendet werden. Die Prüfsumme wird über den Header, den so genannten *Pseudo-Header* und die Daten gebildet. Die Prüfsumme ist optional, wird aber in der Praxis fast immer benutzt (falls nicht, wird diese auf "0" gesetzt).

Portscanner

Franz Fiala

Im Zusammenhang mit den Protokollen der Netzwerktechnik ist es auch wichtig, sich mit Hilfe softwaregesteuerter Messtechnik Informationen über ein Netz, einen Rechner und die offenen Ports verschaffen zu können. Solche Programme, werden „Portscanner“ genannt.

Auch in einem einfachen Heimnetz sollte ein solcher Portscanner Bestandteil der eigenen Toolsammlung sein.

Die Arbeitsweise der „Portscanner“ wird in der Wikipedia unter genau diesem Begriff sehr gut beschrieben.

In gewisser Weise bedeutet ein solcher Scan schon eine Art „Angriff“ auf eine bestehende Installation. (Messtechnik hat es an sich, dass sie mit der zu messenden Größe interagieren muss.)

Ein Portscanner erkennt alle benutzten IP-Adressen in einem Netz (siehe Bild unten) und kann auch die Namen der Geräte anzeigen.

Wir haben Portscanner in Betrieb genommen und in einem Artikel auf der Homepage von ClubComputer beschrieben:

- https://clubcomputer.at/2017/11/17/portscanner/
- https://clubcomputer.at/2017/11/18/portscanner-mobil/

Die einzelnen Scanner unterscheiden sich in der Analysegenauigkeit und Benutzerfreundlichkeit. Der Portscanner „nmap“ ist schon etwas für Profis.

Windows

- SuperScan 3.0 (McAfee)
- Advanved Port Scanner (Famatech)
- Nmap (Gordon Lyon)

Mobil (Android)

- Fing

Einige Portscanner (Famatech und Fing) sind ein kostenloses Einstiegsprodukt, das mit kostenpflichtigen Produkten des Erzeugers zusammenarbeitet.

Seit ich von unserem Mitglied **Werner** den Tipp zu „Fing“ bekommen habe, schaue ich mich in jedem offenen WLAN um, wer de „unterwegs“ ist.