Protokolle

Inhalt

Zu diesem Paper

Was Sie hier lesen, ist eine Einführung in die Welt der (Netzwerk)Protokolle. Ich hoffe, dass es so geschrieben ist, dass es für jeden oder einfach für möglichst viele tauglich ist, egal ob man sich nun schon lange mit dem Thema befasst oder gerade erst in diese spannende Welt eintaucht.

Ich wünsche Ihnen viel Spass beim lesen und hoffe, Sie können durch dieses Paper Ihr Wissen um das ein oder andere erweitern.

Sven Vetsch

Der Begriff Protokoll(e)

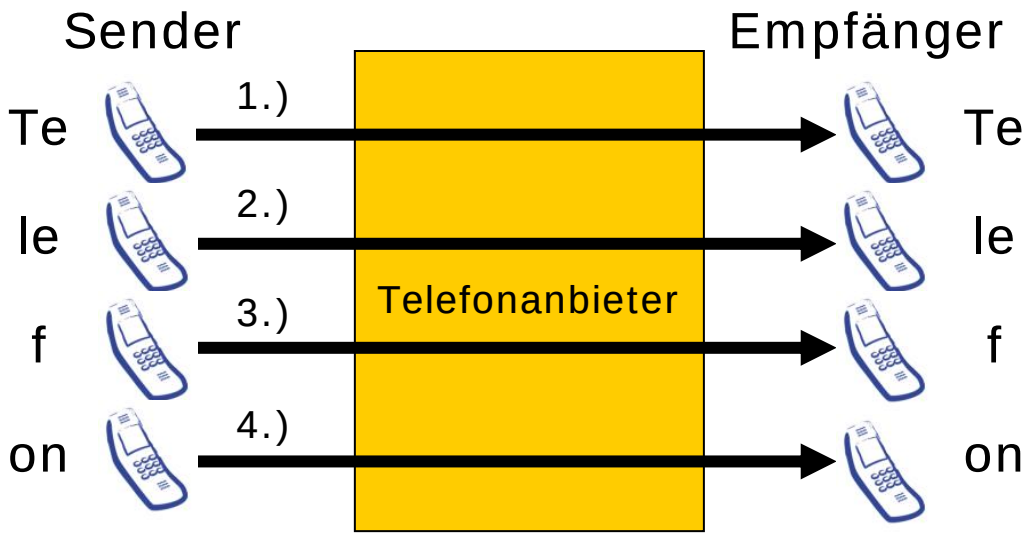
Protokolle dienen in Computernetzwerken dazu, die Kommunikation zwischen den einzelnen Komponenten zu regeln, seien dies nun Workstations, PDAs oder Switches.

Routing-Fähigkeit

Eine der wichtigsten Eigenschaften eines Protokolls ist die Routing-Fähigkeit beziehungsweise, ob das Protokoll verbindungsorientiert ist oder nich.

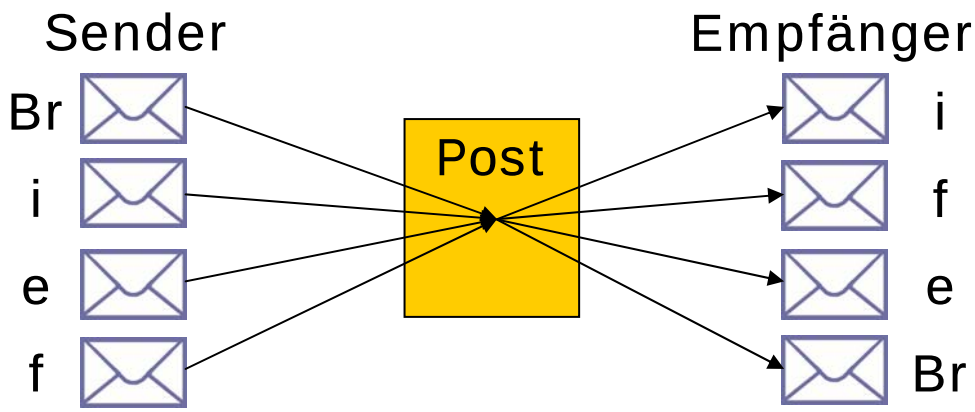
Verbindungsorientiert
Bei dieser Art von Protokollen muss zuerst eine Route zum Ziel gesucht werden. Diese Route wird während der Datenübertragung nicht verändert, dass heisst die einmal festgelegte Route gilt für alle weiteren Pakete. Dies hat den grossen Vorteil, dass die Pakete in der gleichen Reihenfolge beim Zielsystem ankommen, in der sie versendet wurden.
Bestes Beispiel für ein verbindungsorientiertes Protokoll ist TCP.

Eine Kommunikation mit einem verbindungsorientierten Protokoll kann man sich etwa wie folgt vorstellen.



Verbindungslos
Bei einem Verbindungslosen Protokoll, ist keine ständige Verbindung zum Kommunikationspartner nötig. Die Daten-Pakete, suchen sich einen beliebigen Weg zum Empfänger, dies gilt für jedes Packet einzeln. So kann es sein, dass ein Packet, das später als ein anderes abgeschickt wurde, dennoch später am Ziel ankommt.
Das wohl bekannteste Protokoll dieser Art ist IP.

Auch hier eine kleine Vorstellungshilfe zum besseren Verständnis.



TCP / IP

Kurzinfos zu TCP
- ISO Layer 4 Protokoll
- TCP bedeutet „**T**ransmission **C**ontrol **P**rotocol“
- Die zwei Hauptaufgaben von TCP sind eine zuverlässige Nachrichtenübertragung sowie das Porthandling
- TCP ist verbindungsorientiert

Kurzinfos zu IP
- ISO Layer 3 Protokoll
- IP bedeutet soviel wie „**I**nternet **P**rotokoll“
- Hauptaufgaben von IP ist routen und adressieren
- IP ist wie schon erwähnt verbindungslos

Aufbau eines Datenpakets

Auch wenn es nicht direkt mit dem Thema Protokolle zu tun hat, denke ich, ist es dennoch wichtig, kurz den Aufbau von Datenpaketen zu erklären.

Hier eine Grafik zum Aufbau:

Legende:

Header:	Begin des Pakets, Protokollinfos, Version → Adresse, Empfänger etc.
Daten:	Die zu übermittelnden Daten
Trailer:	Ende des Pakets, oft Prüfsumme

Diese Header und Trailer werden immer wieder in jeder Schicht des OSI-Modells angefügt. Dass heisst jede Schicht, die vom Datenpaket durchlaufen wird, übergibt diesem weitere Header- bzw. Trailerinformationen.

Diese Informationen von Header und Trailer werden immer von „aussen“ an das Datenpaket angefügt (wie im Bild oben gezeigt) und vom Zielsystem in umgekehrter Reihenfolge wieder gelesen und verarbeitet.

Wichtige Protokolle

Die wichtigsten Protokolle sind wohl unbestritten TCP und IP doch es gib eine rechte Anzahl an weiteren Protokollen, die man kennen sollte.

FTP
Das FTP-Protokoll wir fast ausschliesslich zur Übertragung von Daten in Netzwerken verwendet. Die Abkürzung FTP steht für „**F**ile **T**ransfer **P**rotocol“.

Telnet
Über das Telnet-Protokoll werden meist entfernte Rechner zum Beispiel über das Internet ferngesteuert. Telnet wird meist über eine so genannte Shell gesteuert, dies ist ein Fenster, in welches über Textkommandos Befehle ausgeführt werden können. Unter Unix-Systemen wird dies noch heute recht viel gebraucht, auch wenn es langsam durch SSH „**S**ecure **Sh**ell“ ersetzt wird. Auf Windows-Systemen kommt Telnet dagegen kaum noch zum Einsatz, was sicher auch dem RemoteDesktop-Dienst von Microsoft zuzuschreiben ist.

SMTP
Eines der wohl wichtigsten Protokolle neben TCP und IP ist wohl das „**S**imple **M**ail **T**ransfer **P**rotocol“, kurz SMTP. Es findet Verwendung beim versenden von E-Mails.

HTTP
Auch ein in der heutigen Zeit nicht wegzudenkendes Protokoll ist das so genannte „**H**yper**t**ext **T**ransfer **P**rotocol“. Dieses Protokoll wird hauptsächlich zur Übertragung von Webseiten vom Webserver zum Client verwendet. Auch der Name des Protokolls kommt davon, den Webseiten sind meist in HTML geschrieben, was soviel bedeutet wie „**H**yper**t**ext **M**arkup **L**anguage“.

POP
Das „**P**ost **O**ffice **P**rotocol“ ist das Gegenstück zum oben schon erwähnten SMTP. Im Gegensatz zu SMTP wird POP aber zum empfangen von E-Mails und nicht zum versenden solcher benötigt.

UDP
Das UDP-Protokoll ist eigentlich ein Pendant von TCP jedoch mit dem Unterschied, dass das „**U**ser **D**atagram **P**rotocol“ nicht verbindungsorientiert sondern verbindungslos ist. Es ist somit ein wenig schneller als TCP aber auch um ein rechtes Stück weniger sicher.

IPSec
Diese Protokoll ist eigentlich identisch mit IP ausser, dass es noch ein ganzes Packet mit zusätzlichen Sicherheitsmechanismen beinhaltet.

ARP
Das „Adress Resolution Protocol“ dient dazu, die logische IP-Adresse einer Netzwerkkomponente nach dessen physikalischer Adresse (MAC-Adresse) aufzulösen.

NetBIOS
Dieses Protokoll wurde als Anwenderschnittstelle von IBM entwickelt und gehört der OSI Layer 5 an, somit lässt es sich nicht als eigentliches Netzwerkprotokoll bezeichen. Der Name NetBIOS kommt von „**Net**work **B**asic **I**nput **O**utput **S**ystem“.

Apple-Talk
Bei der Entwicklung von Apple-Talk ging es hauptsächlich darum, verschiedene Apple Macintoshs miteinander zu vernetzen. Mittlerweilen, hat aber auch Apple auf TCP/IP umgestellt.

Ports

Da ein modernes System, welches in einem Netzwerk integriert ist, eine Unmenge verschiedener Dienste zu erfüllen hat, ist es unumgänglich, etwas Weiteres zur exakteren Bestimmung von Daten beziehungsweise deren Funktion zu haben. Diese Zusätze nennt man Ports.
Durch die Ports kann schon beim ansteuern eines Gerätes im Netzwerk, durch den Port, deutlich gemacht werden, in welcher Form die Daten ankommen, beziehungsweise, wie sie interpretiert werden müssen. Somit sind Ports eigentlich nichts anderes als eine genauere Beschreibung eines Zielortes. Als vergleich könnte man sagen, wenn ich nur die IP eines Systems habe, dann wüsste ich im richtigen leben vielleicht, das ich meinen Freund in Zürich abholen soll, wenn aber noch ein Port angegeben ist, ist das im Beispiel so, als wenn ich nicht nur wüsste, dass ich meinen

Freund in Zürich abholen soll, sondern weiss ich auch noch genau, an welcher Adresse er wohnt.

Portnummern
Man sollte auch die Grundlagen über die Verwendung von Portnummern kennen, darum möchte ich diese hier in einer kleinen Tabelle kurz aufzeigen.

Bereich	Beschreibung
0 bis 255	Well-Known-Ports
256 bis 1023	Registriert
1024 bis 5000	Dynamisch
Alle Anderen	Frei verwendbar

IP-Adressierung

Im Zeitalter des Internets, ist die Adressierung von Netzwerk-Komponenten über eine IP-Adresse nicht mehr wegzudenken.

Was ist eine IP-Adresse?
Eine IP-Adresse lässt sich wohl am besten mit einer Telefonnummer vergleichen. Jede Komponente im Netzwerk, die direkt angesprochen werden können möchte, besitzt eine Telefonnummer, doch diese nennt sich einfach IP-Adresse. Wir können also unserem System sagen, ruf die Komponente xy unter der Nummer 123 an und sag ihr dies und das. Das System nimmt über die IP-Adresse Kontakt zur Zielkomponente auf, dann beginnt der Datenaustausch zwischen den Geräten. Somit passiert tatsächlich nichts, was wirklich anders wäre als bei einem normalen Telefonanruf.

Aufbau einer IP-Adresse
Der Aufbau einer IP-Adresse zurzeit besteht aus vier Oktetten mit Dezimalzahlen also zum Beispiel 192.168.1.45, dies ändert sich allerdings mit IPv6. Bei IPv6 sind nicht nur dezimale sondern auch hexadezimale Zahlen erlaubt, was es ermöglicht viel mehr IPs vergeben zu können.

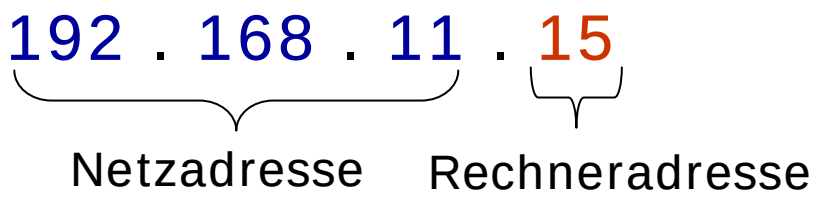
Subnetmaske
Um das nächste Thema (IP-Klassen) zu verstehen, ist es erforderlich, kurz den Begriff „Subnetmaske“ zu erläutern, damit dieser dann vorausgesetzt werden kann.
Eine Subnetmaske ist ein Bitmuster, welches Teile einer IP-Adresse „maskiert“, damit wird der Übergang von Netzadresse zu Rechneradresse gekennzeichnet (siehe Bild bei IP-Klassen). Binär betrachtet, besteht eine Subnetmaske aus einer Folge von Einsen und Nullen. Der Wechsel zwischen den Nullen und den Einsen gibt an, wie viele Bits zur Netzadresse (Einsen) und wie viele zur Rechneradresse (Nullen) gehören.

Hier ein kleines Beispiel:

	Netzadresse		Rechneradresse	
IP-Adresse (dezimal) Binär	192 1100 0000	168 1010 1000	10 0000 1010	1 0000 0001
Subnetmaske (dezimal) Binär	255 1111 1111	255 1111 1111	255 1111 1111	0 0000 0000

IP-Klassen

Es gibt beim Protokoll IP sogenannte Klassen (A, B und C). Diese werden durch die Subnetmaske sowie einer bestimmte IP-Range (ein Bereich von IP-Adressen zum Beispiel 143.23.12.1 bis 147.142.87.12) bestimmt. Um nun die Unterteilungen sowie die Beschreibungen zu verstehen, ist es wichtig innerhalb einer IP-Adresse zwischen Netzadresse und Rechneradresse zu Unterscheiden. Am besten kann dies durch eine kleine Illustration gezeigt werden.



So nun aber zu den verschiedenen IP-Adressklassen.

Klasse A:

- 1 Oktett Netzadresse, 3 Oktett Rechneradresse
- Netzadresse: 1 – 126
- 126 Klasse A-Netze
- 1 Klasse A Netz → über 16Mio Rechneradressen
- Subnetmaske: 255.0.0.0
- Heute sind alle Klasse A Netze vergeben

Beispiel: **34.211.98.155**

Klasse B:

- 2 Oktett Netzadresse, 2 Oktett Rechneradresse
- erste Netzadresse: 128 – 192
- Über 16‘000 Klasse B-Netze
- 1 Klasse B Netz → über 16‘000 Rechneradressen
- Subnetmaske: 255.255.0.0

Beispiel: **145.167.65.178**

Klasse C:
- 3 Oktett Netzadresse, 1 Oktett Rechneradresse
- erste Netzadresse: 193 – 223
- 16Mio Klasse C-Netze
- 1 Klasse C Netz → 255 Rechneradressen
- Subnetmaske: 255.255.255.0

Beispiel: **201.0.113.155**

Hier noch eine Kurzübersicht über die IP-Adressklassen:

Klasse	Netzwerkadresse	Subnetmaske	Anzahl Netzwerke	Anzahl Netzwerkknoten
A	0 bis 126	255.0.0.0	126	(2^24)-2
B	128.0 bis 191.255	255.255.0.0	16'348	(2^16)-2
C	192.0.0 bis 223.255.255	255.255.255.0	2'097'152	(2^8)-2

Dank

An dieser Stelle möchte ich mich noch bei der SBW Neue Medien AG bedanken, die einen Teil der Informationen zur Verfügung gestellt hat, auf denen dieses Dokument aufbaut.

Abschluss

Zu guter Letzt, möchte ich mich bei Ihnen bedanken, dass sie sich die Zeit genommen haben, dieses Paper zu lesen. Ich hoffe es hat Ihnen Spass gemacht und Sie können von Ihrem neuen Wissen profitieren.

Sollten Sie Fragen oder Anregungen haben, stehe ich Ihnen gerne zur Verfügung.

admin@disenchant.ch
http://www.disenchant.ch

Mit freundlichen Grüssen
Sven Vetsch