

Der TCP/IP – Protokollstapel

Inhaltsverzeichnis

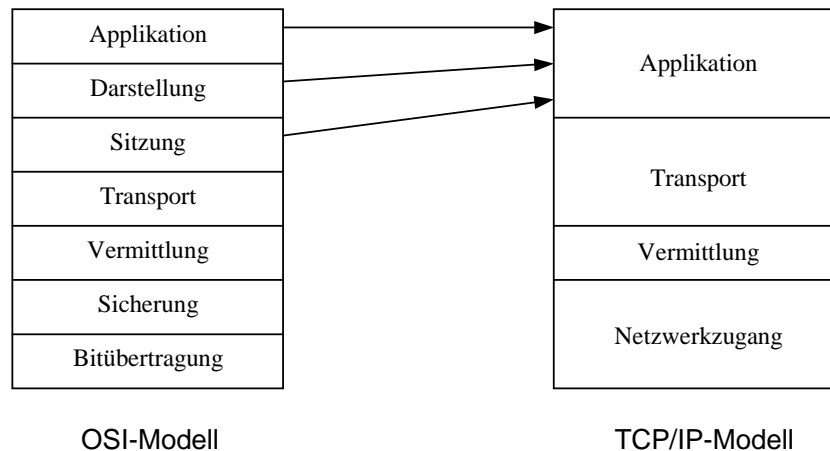
1. EINFÜHRUNG	2
2. VERGLEICH OSI-MODELL – TCP/IP-SCHICHTENMODELL	2
3. PHYSISCHES NETZWERK – TCP/IP – DATENFLUß	3
3.1 ARP	3
3.2 DATENFLUß IM TCP/IP – MODELL	3
4. DIE VERMITTLUNGSSCHICHT	4
4.1 ALLGEMEINES	4
4.2 IP (INTERNET PROTOCOL)	4
IP-ADRESSEN	6
4.3 ICMP (INTERNET CONTROL MESSAGE PROTOCOL)	6
DESTINATION UNREACHABLE	6
TIME EXCEEDED	6
PARAMETER PROBLEM	6
SOURCE QUENCH	6
REDIRECT	6
ECHO REQUEST, ECHO REPLY	6
TIMESTAMP REQUEST, TIMESTAMP REPLY	6
4.4 ROUTING	7
4.5 MULTICASTING	7
4.6 FRAGMENTIERUNG	7
5. TRANSPORTSCHICHT	7
5.1 ALLGEMEINES	8
5.2 UDP (USER DATAGRAM PROTOCOL)	8
5.3 TCP (TRANSMISSION CONTROL PROTOCOL)	8

1. Einführung

Die Entwicklung des TCP/IP – Protokollstapels, welcher durch sein **offenes und flexibles Design** zum raschen Wachstum des Internets beigetragen hat, begann Mitte der 60er Jahre und wurde vom amerikanischen Department of Defense in Auftrag gegeben. Das Ziel war es, ein **offenes Netzwerk** zu schaffen, welches imstande war, unterschiedlichste Hard- u. Softwaresysteme zu verbinden und auch noch funktionsfähig zu sein, wenn große bzw. wichtige Teile des Netzes ausfallen. Nach der Einbindung von TCP/IP ins **Berkley UNIX** war die Grundlage für die erfolgreiche Verbreitung geschaffen.

2. Vergleich OSI-Modell – TCP/IP-Schichtenmodell

Das TCP/IP – Modell basiert auf dem OSI-Schichtmodell, konzentriert sich aber eher auf die unteren Schichten und lässt relativ viel Spielraum in den oberen Schichten.



Kurz beschrieben, bieten die Schichten des TCP/IP-Modells folgende Funktionen:

Netzwerkzugangsschicht: In dieser Schicht gibt es kein Protokoll des TCP/IP-Modells, sondern diese wird von bereits bestehender Implementierung realisiert wie z.B.: Ethernet, Token Ring, ATM, FDDI, ...

Vermittlungsschicht: Sie entspricht in etwa der Vermittlungsschicht im OSI-Referenzmodell. Diese Schicht umfaßt unter anderem die TCP/IP-Protokolle **IP**, **ICMP**, **IGMP** (Internet Group Management Protocol). Das **ARP-Protokoll ist zwischen der Vermittlungsschicht und der Netzwerkzugangsschicht angesiedelt.**

Transportschicht: Diese Schicht umfaßt die Protokolle **TCP** und **UDP** und entspricht in etwa der Transportschicht im OSI-Referenzmodell.

Applikationsschicht: Umfaßt die Sitzungs-, Darstellungs- und Applikationsschicht des OSI-Referenzmodells. In dieser Schicht existieren eine Vielzahl von Protokollen, wie zum Beispiel **HTTP**, **FTP**, **SMTP** und **NNTP**.

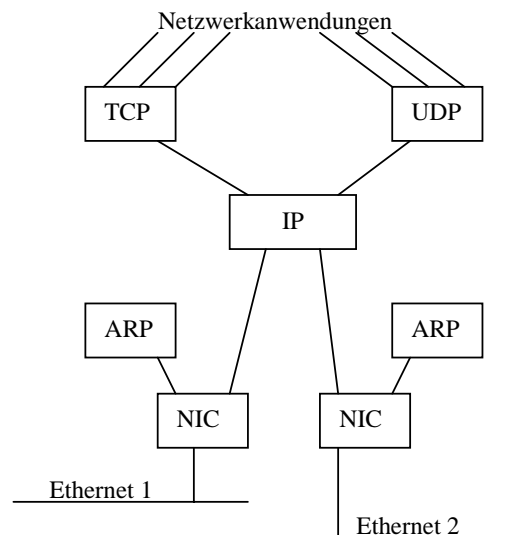
3. Physisches Netzwerk – TCP/IP – Datenfluß

3.1 ARP

ARP (Address Resolution Protocol) wird benutzt, um die **IP-Adressen**, die unabhängig von der Art des physischen Netzwerkes sind, in **physische Netzwerkadressen umzuwandeln**. Das bedeutet, daß für **jede Netzwerkschnittstelle** in einem Rechner **genau eine zugehörige ARP-Schnittstelle** existieren muß.

ARP arbeitet mit einer Adreßtabelle, die durch Broadcast-Techniken um noch nicht bekannte, aber benötigte physische Adressen ergänzt wird. Genauer wird hier auf ARP nicht eingegangen. → siehe Referat "Adreßumsetzungsverfahren" (Gumpinger)

3.2 Datenfluß im TCP/IP – Modell



Wenn wir als Beispielanwendung FTP verwenden, welches wiederum TCP verwendet, ergibt sich also folgender Datenfluß: **FTP → TCP → IP → NIC**

Das TCP-Modul, das UDP-Modul und das NIC-Modul können als **n-zu-1 Multiplexer** betrachtet werden. Sie besitzen **mehrere Eingänge aber nur einen Ausgang**. Weiters sind sie aber auch **1-zu-n Demultiplexer**, d.h. sie leiten Pakete vom **einzigen Eingang** anhand einer Kennung im Protokollheader an das passende **übergeordnete Modul** weiter.

Der Datenfluß von der Anwendung zum Netzwerk hin ist einfach zu durchzuführen, da ohnehin nur ein Weg gegangen werden kann.

Der umgekehrte Weg wird mit Hilfe der schon genannten Kennung im jeweiligen Protokollheader durchgeführt.

Bei nur einer Netzwerkschnittstelle in einem Rechner ist dies relativ einfach, da auch das IP-Model ein n-zu-1 Multiplexer bzw. ein 1-zu-n Demultiplexer ist. Komplizierter wird es da schon bei **mehreren Netzwerkschnittstellen**, da hier das **IP-Modul als n-zu-m Multiplexer bzw. m-zu-n Demultiplexer** fungiert.

Diese Tatsache führt auch dazu, daß Daten von einer Schnittstelle direkt zur nächsten Schnittstelle weitergeleitet werden können. Dieser Vorgang wird "**IP-Forwarding**" genannt.

Zusammenfassend und vereinfacht kann man sagen, daß ein Protokoll die Daten der übergeordneten Schicht übernimmt, seinen Header hinzufügt und dem untergeordneten Protokoll übergibt. Dies geht so lange, bis die Daten bei der Empfängerschnittstelle angekommen sind. Hier wird genau der umgekehrte Weg gegangen.

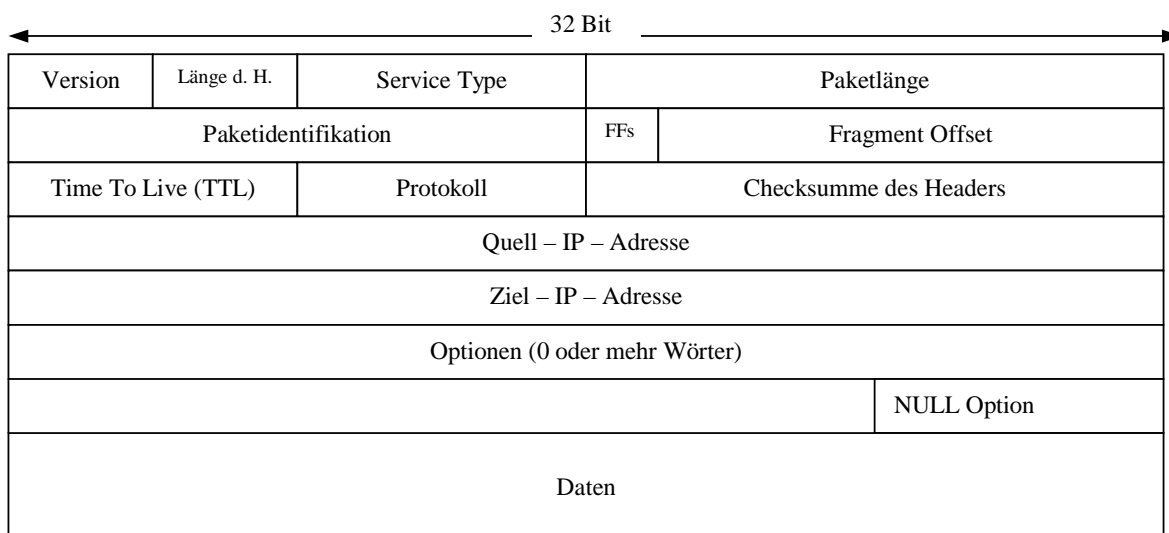
4. Die Vermittlungsschicht

4.1 Allgemeines

Die Aufgabe der Vermittlungsschicht ist es, Daten vom Ursprung zum Ziel zu bringen, auch wenn der Weg über mehrere zwischenliegende Rechner führt. Weitere Ziele sind die Erkennung und Ausgleichung von Lastunterschieden und das Auswählen einer optimalen Route.

4.2 IP (Internet Protocol)

Das Layout eines IP-Paketes sieht folgendermaßen aus:



Erklärung der einzelnen Felder:

Bezeichnung	Länge (Bit)	Beschreibung
Version	4	Versionsnummer, derzeit 4
Länge d. H.	4	Header-Länge in 32-Bit-Wörtern, mind. 5, max. 15
Service Type	8	gewünschter Dienst, Kombination aus Zuverlässigkeit und Geschwindigkeit. hohe Zuverlässigkeit: Bei Pufferüberlauf werden diese Pakete als letzte verworfen (bei Netzen mit unterschiedlicher Übertragungsrate) Durchsatz vs Verzögerung: (De-)Fragmentierung Durchsatz: Defragmentieren so weit wie möglich Verzögerung: Jedes Fragment sofort übertragen
Paketlänge	16	Länge des Pakets inkl. Header (in Bytes → max. Paketgröße für IP: 64 kB)
Paket-ID	16	Durch den Sender (durch Inkrement) gesetzte Paket-ID. Im Falle einer Fragmentierung tragen alle Fragmente die gleiche Paket-ID (Angabe in Bytes)
FFs	3	Fragment-Flags Bit 1: "Don't Fragment": Ist das Paket zu fragmentieren, wird es verworfen, Fehlermeldung an Sender Bit 2: "More Fragments": Bei allen Fragmenten außer dem letzten eines Paketes gesetzt
Fragment Offset	13	rel. Adresse d. Daten des Paketes im Gesamtpaket. In 8-Byte-Schritten
Time To Live	8	Jeder Router dekrementiert diesen Wert, der vom Sender bestimmt wird. Wird der Wert 0, so verwirft der Router das Paket und ein ICMP-Paket wird dem Sender zurückgeschickt
Protokoll	8	Protokoll, an das die Daten weitergegeben werden. z.B.: 6: TCP; 1: ICMP; 17: UDP
Checksumme	16	Prüfsumme des Heades
Quell-IP-Adr.	32	4-Byte lange IP-Adresse des Senders
Ziel-IP-Adr.	32	4-Byte lange IP-Adresse des Empfängers
Optionen	32 * x	5 Möglichkeiten: - Security - Strict Source Routing - Loose Source Routing - Record Route - Time Stamp

Weitere Infos zu den Optionen:

Security: Bezeichnet, wie geheim ein Paket ist

Strict Source Routing: Bestimmt den Pfad, den das Paket gehen muß. Es dürfen nur die angegebenen Stationen ohne Zwischenstationen und in der richtigen Reihenfolge verwendet werden.

Loose Source Routing: ähnlich wie Strict Source Routing, nur dürfen zwischen zwei vorgegebenen Stationen noch andere Stationen liegen.

Record Route: Veranlaßt jeden Router, seine IP-Adresse in das Paket zu schreiben, um so den Pfad verfolgen zu können. Da die Optionen maximal nur 40 Byte umfassen können, kann diese Option heute meist nicht mehr genutzt werden.

Time Stamp: Ähnlich wie Record Route, nur wird neben der IP-Adresse auch ein Zeitstempel von jedem Router eingetragen.

IP-Adressen

Jedes Gerät in einem Internet muß eine eindeutige IP-Adresse haben, welche in einen Netz- und einen Hostanteil zerfällt. Genauere Informationen zu IP-Adressen findet man im Referat "Routing" → Spitzbart.

4.3 ICMP (Internet Control Message Protocol)

Dieses Protokoll kommt dann zum Einsatz, wenn ein unvorgesehenes Ereignis eintritt. ICMP-Nachrichten, von denen es mehrere Typen gibt, werden mit einem IP-Header gesendet.

DESTINATION UNREACHABLE

Wird benutzt, wenn ein Teilnetz oder ein Router das Ziel nicht finden kann

TIME EXCEEDED

Wird benutzt, wenn ein Paket weggeworfen wird, wenn sein Zähler (Time To Live) 0 erreicht hat. Ist ein Anzeichen dafür, daß eine **hohe Überlastung** vorliegt, oder die Pakete kreisen in einer Schleife, weil eine Fehlkonfiguration auf einem Router herrscht

PARAMETER PROBLEM

Zeigt einen unzulässigen Wert im IP-Header an. Dies deutet auf einen Fehler in der Software des Quellrechners bzw. eines Routers hin

SOURCE QUENCH

Wird heute kaum mehr benutzt. Diente früher dazu, um einem Host mitzuteilen, daß er seine Aktivitäten drosseln soll.

REDIRECT

Wird benutzt, wenn ein Router festgestellt hat, daß ein Paket falsch weitergeleitet wurde.

ECHO REQUEST, ECHO REPLY

Wird benutzt, um festzustellen, ob ein Ziel noch erreichbar ist. Von jedem Ziel wird erwartet, auf einen ECHO-REQUEST mit einem ECHO-REPLY zu antworten.

TIMESTAMP REQUEST, TIMESTAMP REPLY

Ähnlich wie ECHO-x, nur wird zusätzlich die Zeit mitgesendet. Die Optionen ECHO-x und TIMESTAMP-x werden auch zum Messen der Netzleistung verwendet.

4.4 Routing

Das Routing ist eine der wichtigsten Aufgaben der Vermittlungsschicht und somit auch des IP-Protokolls. Meist wird diese Aufgabe von **eigenen Geräten** erfüllt, die auf diese Anforderungen optimiert sind. Es kann jedoch auch ein beliebiger Rechner mit **mindestens zwei Netzwerkschnittstellen als Router** fungieren.

Wenn ein IP-Paket von einem Router empfangen wird, stellt dieser anhand seiner Routing-Tabellen fest, in welche Richtung (auf welche Schnittstelle) er dieses Paket weiterleiten soll. Weiters können hier auch Fakten wie die Verfügbarkeit und Netzwerkauslastung auch einen Rolle für die Auswahl der Route eine Rolle spielen.

Der Inhalt der Routing-Tabellen kann entweder statisch eingetragen werden oder dynamisch von Routing-Protokollen erstellt werden. Näheres zu diesem Thema gibt es in den Referaten "Routing" und "Routing Protokolle".

4.5 Multicasting

Überlicherweise findet die Kommunikation in der Vermittlungsschicht zwischen Sender und Empfänger statt (Ende-zu-Ende-Kommunikation). Es wäre aber nützlich, ein IP-Paket gleichzeitig an mehrere Rechner zuzustellen. Dies wird in IP durch die Klasse-D-Adressen (224.0.0.0 – 239.255.255.255) möglich.

Jede Adresse der Klasse D identifiziert eine **Hostgruppe**. Sendet nun ein Prozeß ein Paket an eine Adresse der Klasse D, dann wird es allen Mitgliedern der adressierten Gruppe zugestellt, was aber nicht garantiert ist.

Es gibt 2 Gruppen von Klasse-D-Adressen: permanente und temporäre. Jede permanente Gruppe hat auch eine permanente Gruppenadresse.

Temporäre Gruppen müssen vor der Nutzung erstellt werden, wobei jeder Host die Mitgliedschaft einer bestimmten Gruppe beantragen kann.

Multicasting wird durch spezielle **Multicast-Router** implementiert, welche auch neben "normalen" Routern existieren können. Dieser Multicast-Router sendet einmal pro Minute einen **Broadcast** an die Rechner in seinem LAN, welche ihm dann mitteilen, **in welcher Gruppe sie Mitglied** sind. Diese Kommunikation erfolgt über **IGMP (Internet Group Management Protocol)**, welches grob ICMP entspricht.

4.6 Fragmentierung

Jedes Netzwerk gibt Höchstwerte für Paketgrößen vor, die von mehreren Faktoren abhängen (z.B.: Hardware, Standards, Protokolle, Betriebssysteme,...).

Daher kommt es zu Problemen wenn großes IP-Paket auf ein Netz trifft, wo es die physische Maximalgröße überschreitet. Aus diesem Grund wird den Routern erlaubt, das Paket in mehrere Fragmente zu unterteilen. Schwierigkeiten entstehen hier natürlich bei der Zusammensetzung des Paketes am anderen Ende. Weiteres zu diesem Thema ist im Referat "Fragmentierung" zu finden.

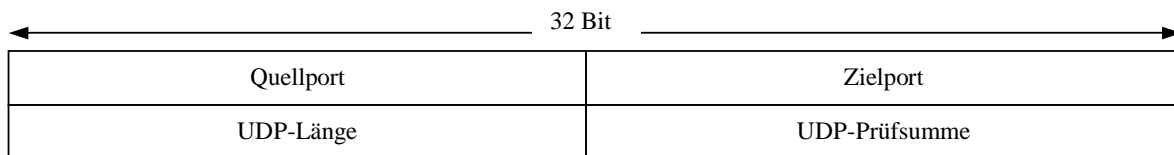
5. Transportschicht

5.1 Allgemeines

Das Ziel der Transportschicht ist es, die **Qualität der Übertragung zu verbessern**. Ein weiteres Merkmal sind **Ports**, welche in etwa Nebenstellennummern einer Telefonanlage entsprechen. Eine Verbindung auf Ebene der Transportschicht wird durch die **Adresse und die gewünschte Portnummer eindeutig identifiziert**.

5.2 UDP (User Datagram Protocol)

UDP ist die **verbindungslose** Variante der Transportschicht in der TCP/IP-Suite. Ein UDP-Header hat folgenden Aufbau:



Wie man leicht erkennen kann ist der Header ziemlich klein und somit ist UDP ein **sehr schnelles** Protokoll. Der Nachteil von UDP ist, daß **keine Sicherung** gegen

- Übertragungsfehler
- Paketverlust
- Paketverdoppelung
- Sequenzfehler

gegeben ist, dies ist bei UDP ein Problem der Anwendung.

UDP wird dort eingesetzt, wo nicht die Qualität der Verbindung eine Rolle spielt, sondern **wo Schnelligkeit gefragt** ist. Beispiele dafür sind DNS und TFTP.

5.3 TCP (Transmission Control Protocol)

TCP ist die **verbindungsorientierte** Implementierung in der Transportschicht der TCP/IP-Protokollsuite.

Es bietet eine **Ende-zu-Ende-Verbindung und sichert gegen**:

- Übertragungsfehler
- Paketverlust
- Paketverdopplung
- Sequenzfehler
- Überlastung des Empfängers

Wie auch bei UDP wird eine TCP-Verbindung durch die Adressen und die Portnummer gekennzeichnet. Eine TCP-Verbindung ist eine **Voll-Duplex-Verbindung** und ein **Datenstrom**, deshalb kann man auch **nicht von TCP-Paketen**

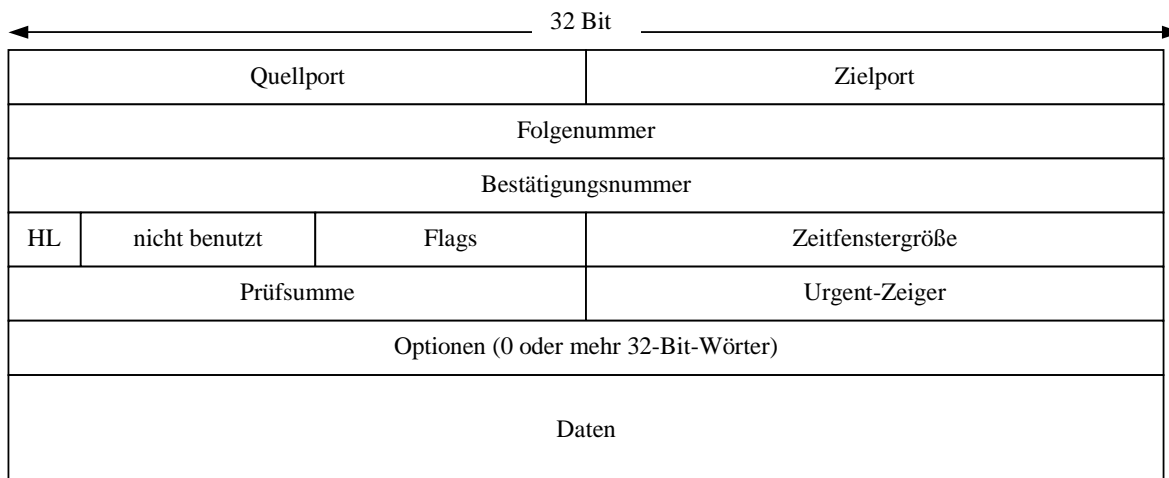
sprechen, sondern von **TCP-Segmenten**. Weiters hat die Größe eines gesendeten Segments nichts mit der Größe des empfangenen Segments zu tun.

TCP wird von Applikationen verwendet, die diese Vorteile den Vorteilen von UDP (Schnelligkeit) vorziehen (z.B.: FTP, Telnet, ...). Aufgrund des großen Overheads ist TCP auch merkbar langsamer als UDP und belastet das Netz viel mehr.

Der Grund dieser Belastung liegt auch in der komplizierten Kommunikationsform, da zuerst eine Verbindungsanfrage geschickt, die von der Gegenstelle bestätigt werden muß,... Näheres dazu erfährt man beim Referat "Sockets".

TCP führt **für jede Verbindung einen eigenen Puffer** und muß die **Daten für IP in Pakete umwandeln**.

Ein TCP-Segment sieht folgendermaßen aus:



Beschreibung der einzelnen Felder:

Bezeichnung	Länge (Bit)	Beschreibung
Quellport	16	Quellport der Verbindung
Zielport	16	Zielport der Verbindung
Folgenummer	32	Zeiger auf die Stelle des Datenstromes, wo dieses Paket hingehört. Falls das SYN-Flag gesetzt ist, befindet sich hier die anfängliche Folgenummer.
Bestätigungsnr.	32	Gibt das als nächstes zu erwartende Datenbyte an
HL	4	Länge des Headers in 32-Bit-Wörtern
nicht benutzt	6	Derzeit keine Verwendung
Flags	6	Bit 10 (URG): Urgent Pointer ist gültig Bit 11 (ACK): Bestätigungsnummer ist gültig Bit 12 (PSH): Empfänger wird aufgefordert, die Daten ohne Pufferung der Anwendung zuzustellen Bit 13 (RST): zum Rücksetzen einer Verbindung Bit 14 (SYN): Daten dienen der Synchronisation Bit 15 (FIN): zum Abbau einer Verbindung
Zeitfenstergröße	16	Angabe über die Fenstergröße

Prüfsumme	16	Prüfsumme inkl. Daten aus IP-Kopf
Urgent-Zeiger	16	Zeiger auf vorrangige Daten
Optionen	32 * x	z.B. max. Segmentgröße, NAK-Option, NOOP, End of Options

Bemerkungen:

Flags: Diese Flags dienen der Flußsteuerung, was ein kompliziertes Verfahren bei TCP ist.

Zeitfenstergröße: Diese Angabe ist sehr wichtig für die Steuerung der Übertragungsrate, falls zwei kapazitiv unterschiedliche Netze verbunden werden. Hier kommt die "Sliding Window Technik" zum Tragen.