Die Transportschicht

Zwischen der Anwendungsschicht und der Netzwerkschicht befindet sich die Transportschicht, die im Rahmen der TCP/IP-Protokollfamilie aus lediglich zwei Protokollen besteht

- das verbindungsorientierte und zuverlässige Transmission Control Protocol (TCP)
- das verbindungslose und unsichere User Datagram Protocol (UDP)

TCP „baut“ im Gegensatz zu UDP eine Verbindung zwischen genau zwei Systemen auf, überträgt die Daten und „baut“ anschließend die Verbindung wieder ab. Hierbei werden für den Auf- und Abbau der Verbindung sowie bei der Datenübertragung Bestätigungen übermittelt, die TCP als zuverlässig kennzeichnen.

UDP hingegen verzichtet auf diese Maßnahmen, wodurch UDP (aufgrund der dadurch geringeren Protokolldaten) etwas schneller ist. Durch den Verzicht ist nicht sicher gestellt, dass versendete Daten auch wirklich beim Empfänger angekommen sind. Empfangene Daten sind jedoch garantiert fehlerfrei! Dies wird durch die dem ISO/OSI-RM vergleichbare Sicherungsschicht in der Netzzugangsschicht vom TCP/IP-RM übernommen.

Transmission Control Protocol

im Wesentlichen hat TCP die Aufgabe. eine sichere Ende-zu-Ende-Datenübertragung zu gewährleisten. Die Kommunikation erfolgt zwischen zwei Applikationen (z.B. Browser und Webserver oder FTP-Client und FTP-Server).

Hierzu wird eine Software-Schnittstelle verwendet, die man als Socket bezeichnet. Ein Socket ist ein Kommunikationsendpunkt, der durch eine IP-Adresse und eine so genannte Portnummer eindeutig bestimmt ist. Die IP-Adresse bezeichnet hierbei eindeutig das Rechnersystem, mit dem kommuniziert wird; die Portnummer hingegen ist eine 16 Bit Integer-Zahl (0...65535), durch die die jeweilige Anwendung auf dem vorgenannten Rechnersystem identifiziert wird.

Sobald eine Anwendung eine Kommunikationsverbindung per TCP öffnet, wird dieser Anwendung vom Betriebssystem für die Kommunikation eine freie Portnummer zugeteilt.

Die Portnummern[1] lassen sich grob unterscheiden:

- „Well known“ Ports (0...1023)
- „Registered“ Ports (1024...49151
- „Dynamische“ bzw. „Private“ Ports (49152...65535)

Die so genannten „Well Known“ Ports sind von der IANA fest zugeordnete Nummern. Die „Registered“ Ports sind von Herstellern bei der IANA registrierte Portnummern. Der letzte Bereich hingegen kann von eigenen (Server-) Anwendungen bzw. von Anwendungen, die mit Servern kommunizieren wollen, verwendet werden.

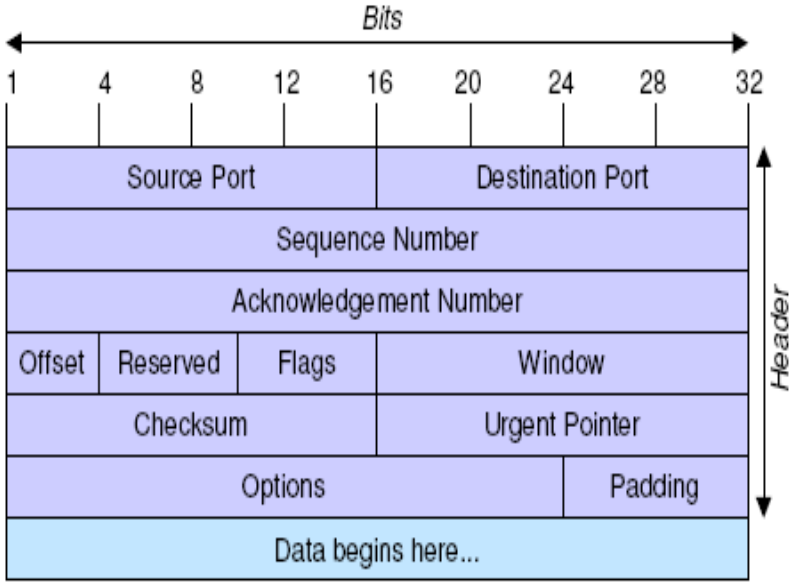
Übung

1. Auf welchen Portnummern „lauschen“ folgende Dienste: ECHO, DAYTIME, QUOTE OF THE DAY, WWW, SMTP, POP3, IMAP, NNTP, DNS.
2. Beschreiben Sie kurz, um welchen Dienst es sich jeweils handelt.
3. Bauen Sie eine Verbindung per Kommandozeile auf: **`telnet gerau1 Portnummer`** wobei `Portnummer`, die Nummer von DAYTIME und QUOTE OF THE DAY ist.

1 http://www.iana.org/assignments/port-numbers

Aufbau des TCP-Headers

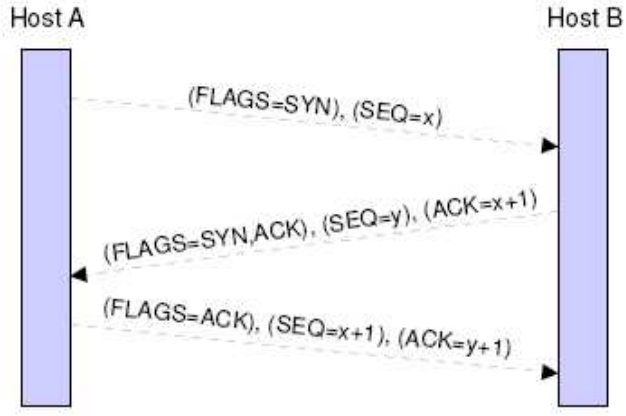
Der Aufbau des TCP-Header ist in der nachfolgenden Grafik dargestellt: Zu Beginn findet man den *Quell-* und *Ziel*-Port des Datenstroms (jeweils 16 Bit). Die TCP-Schicht versendet einen Strom von Bytes, die i.d.R. nicht mit einem Paket übermittelt werden können. In dem Feld *Sequenznummer* übermittelt der Sender daher die Position der angehängten Daten im gesamten Datenstrom. Im Feld *Quittungsnummer* übermittelt der Empfänger die Nummer der bereits übermittelten Datenbytes. Mit *Offset* wird die wirkliche, weil variable, Länge des Headers angegeben, damit der Beginn der Anwendungsschichtdaten bestimmt werden kann. Mittels sechs Bits, die als *Flag* fungieren, werden bestimmte Aktionen wie z.B. der Auf- und Abbau einer Verbindung markiert. Mit *Windows* wird die Zahl der Bytes bestimmt, die ohne eine Quittung abzuwarten, gesendet werden dürfen. Im Feld *Prüfsumme* wird ein 16 Bit Wert eingetragen, der die einwandfreie Übermittlung des TCP-Segments sicherstellt. Mit dem Feld *Optionen* wird u.a. die maximale Bytezahl, die ohne Quittung gesendet werden darf, ausgehandelt. Mit dem Füll-Feld *Padding* wird der Header erweitert, damit er ein Vielfaches von 32 Bit groß ist.



Aus "Einführung in TCP/IP" von Heiko Holtkamp

Auf- und Abbau einer TCP-Verbindung

Wie bereits dargestellt, TCP ist ein verbindungsorientiertes Protokoll. Bevor also Daten zwischen *Sender Host A* und *Empfänger Host B* ausgetauscht werden, nimmt A mit B Kontakt auf und äußert einen Verbindungswunsch durch Senden eines TCP-Headers ohne Nutzdaten.



Aus "Einführung in TCP/IP" von Heiko Holtkamp

Hierzu setzt A das Flag SYN und erzeugt eine Sequenznummer. Wenn B dem Verbindungswunsch nachkommen kann, sendet dieser ebenfalls einen TCP-Header zurück, in dem nun zusätzlich das ACK-Flag gesetzt ist und das Feld Sequenznummer durch eine von B generierte Zahl gefüllt ist. Das Feld ACK-Nummer enthält die von A erzeugte Nummer +1.

Im letzten und dritten Schritt des Verbindungsaufbaus sendet A nun einen TCP-Header mit gesetztem ACK-Bit und der angegebenen Sequenz- und Acknowledmentnummer.

Dieses Verfahren wird als **Drei-Wege-Handskake** (Three-Way-Handshake) bezeichnet.

Beim Verbindungsabbau sendet A einen TCP-Header mit gesetztem FIN-Flag. B bestätigt den

Erhalt des Abbauwunsches mit einem ACK-Flag in seinem Header. Es wird dann noch ein weiterer Header von B versendet, der ebenfalls ein gesetztes FIN-Flag und eine Sequenznummer enthält. Im letzten Schritt bestätigt A den Erhalt des zweiten Headers von B.

Übung

1. Skizzieren Sie den Verbindungsabbau in der für den Aufbau dargestellten Weise
2. Ermitteln Sie alle sechs Bezeichnungen der Flags sowie in einem stichwortartigen Satz deren Bedeutung

Abbau einer TCP-Verbindung

Flag 1: _____

_____

Flag 2: _____

_____

Flag 3: _____

_____

Flag 4: _____

_____

Flag 5: _____

_____

Flag 6: _____

TCP-Segmente

Da die TCP-Segmente in Form von IP-Datagrammen durch ein Netz gesendet werden, ist die Reihenfolge des Eingangs beim Empfänger nicht unbedingt die Reihenfolge des Senders. Die TCP-Schicht hat also u.a. noch die Aufgabe, den Bytestrom, der vom Sender verschickt wurde, anhand der TCP-Segmente zusammen zu setzen. Dies erledigt TCP mittels der Sequenznummer im TCP-Header.

Die Größe eines TCP-Segmentes richtet sich nach der so genannten MTU (***M***aximum ***T***ransfer ***U***nit). Diese ist bei IP in Verbindung mit Ethernet typischerweise 1500 Bytes. In einem IP-Paket können daher 1460 Bytes an Nutzdaten enthalten sein (20 Byte IP-Header sowie 20 Byte TCP-Header). Werden Pakete >1500 Byte erzeugt, müssen diese fragmentiert werden. Die MTU hängt vom jeweiligen Medium ab! Dies kann bei einem Mediumwechsel bei Routern auftreten.

Frage: Wie groß ist die MTU bei PPPoE und warum? _____

Ein Sender darf mehrere TCP-Segmente ohne eingegangene Quittung verschicken; die Anzahl dieser TCP-Segmente richtet sich nach der Größe des freien Pufferspeichers beim Empfänger.

Diese Technik wird als ***Sliding-Window*** bezeichnet.