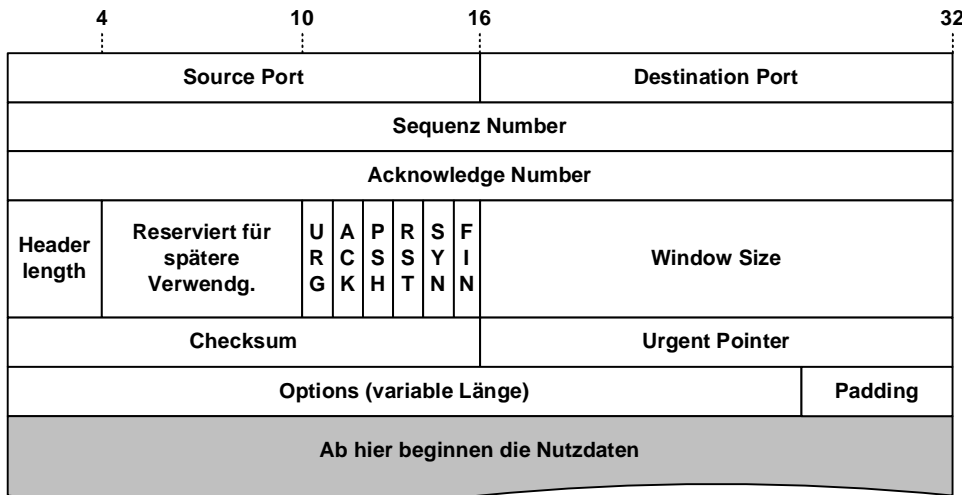


TCP-Paket-Header

Wichtige Ports	
Port-Nr.:	Anwendung
20	FTP - Verbindung
21	FTP - Dateitransfer
22	ssh
23	Telnet
25	SMTP
53	DNS
80	http
110	POP3
143	IMAP
443	HTTPS / SSL

Bedeutung der Felder:

Source / Destination Port (Absender- / Empfänger-Port): Adressieren die Portnummern der Absender-Anwendung bzw. die Portnummer der Empfänger-Anwendung. (Im TCP-IP-Modell werden alle Anwendungen über eine festgelegte Portnummer angesprochen.)

Sequence Number / Acknowledge Number: Die Sequenznummer und die Bestätigungsnummer geben jeweils die Stellung der jeweiligen Daten des aktuellen Paketes innerhalb des in der Verbindung ausgetauschten gesamten Datenstroms an. Die Sequenznummer bezieht sich auf das aktuelle Paket. Die Acknowledge Number gibt die Nummer an, unter welcher der Absender die nächste Nachricht vom Absender erwartet.

TCP Header Length: Die Länge des TCP-Headers in 32-Bit-Wörtern. Dies entspricht dem Anfang der Daten im TCP-Paket. (Dieses Feld ist notwendig, da die Länge des Options-Feldes variabel ist.)

Flags: Mit den sechs 1-Bit-Flags werden bestimmte Aktionen im TCP-Protokoll ausgelöst.

- **URG:** Das Feld Urgent-Pointer soll ausgewertet werden.
- **ACK:** Das Feld Acknowledgement-Number soll ausgewertet werden.
- **PSH:** Push - Ist dieses Bit gesetzt, sollen die Daten sofort an die Empfänger-Anwendung weitergeleitet werden. Sie sollen keinesfalls, z.B. aus Effizienzgründen, zwischengespeichert werden.
- **RST:** Das Reset-Flag dient dazu, eine Verbindung zurückzusetzen falls ein Fehler bei der Übertragung aufgetreten ist.
- **SYN:** (Synchronize Sequence Numbers) Ist dieses Flag gesetzt, soll mit dieser Anfrage eine Verbindung aufgebaut werden.
- **FIN:** Das Fin-Flag zeigt an, dass die aktuelle Verbindung beendet werden soll.

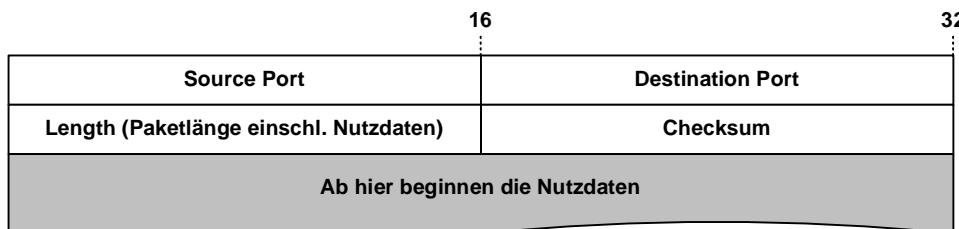
Window Size: Anzahl der Bytes, die der Sender problemlos in einem Segment empfangen kann.

Checksum: Prüfsumme über Header und Daten des TCP-Pakets.

Urgent Pointer: Sind Daten als urgent (dringend) gekennzeichnet, so werden sie bevorzugt befördert.

Options: Zur Angabe von zusätzlichen Optionen beim Verbindungsaufbau, wie zum Beispiel der maximalen Paketgröße. (Standard sind 536 Byte Nutzdaten)

Padding: Mit Hilfe dieses Feldes werden gegebenenfalls die Optionsangaben auf 32-Bit-Werte aufgefüllt.

UDP-Paket-Header

Während TCP-Pakete quasi als Einschreiben mit Rückschein verschickt werden, ist das UDP-Protokoll ein sog. verbindungsloses Protokoll. Das heißt im Gegensatz zu TCP wird von diesem Protokoll nicht überprüft, ob die jeweiligen Datenpakete auch tatsächlich beim Empfänger ankommen. Das Protokoll ist dadurch sehr effizient und eignet sich vor allem für Anwendungen bei denen es in erster Linie auf Geschwindigkeit der Datenübertragung ankommt und bei denen die Vollständigkeit der Datenübertragung von der Anwendungsebene kontrolliert wird.

Quellen:

- Heiko Holtkamp; Einführung in TCP/IP; Technische Fakultät Universität Bielefeld, Febr. 2002
- Linux Systemsicherheit; foobar GmbH Chemnitz 2002; http://www.foobar-cpa.de/documents/admin_-_security/script.html#scriptch2.html