CloudCommand

Cyber Security

CloudCommand GmbH jens_leonhardt@outlook.de

System- und Netzwerk-administration

CloudCommand GmbH jens_leonhardt@outlook.de

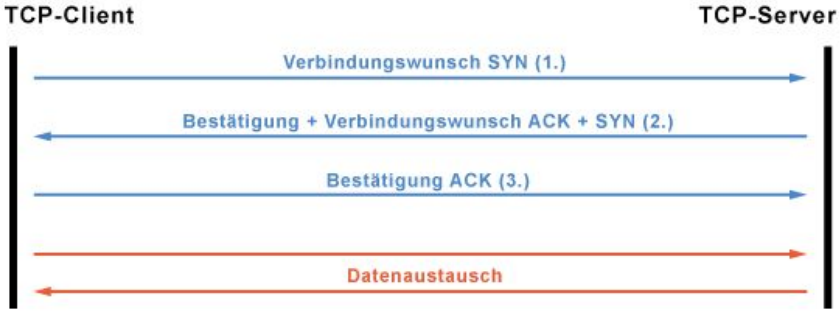
Transport-protokolle

TCP - Transmission Control Protocol

- Das im Allgemeinen zum Aufbau von Internetverbindungen verwendete Protokoll wird TCP genannt. Dabei steht TCP für Transmission Control Protocol.
- Das TCP sorgt für einen problemlosen Transport der IP-Pakete, indem Datenverluste erkannt und automatisch behoben werden.
- Eine Datenübertragung ist dabei in beide Richtungen möglich und eine Netzüberlastung wird verhindert. Dabei ist das TCP eine Implementierung der vierten OSI-Ebene, der Transportschicht.
- Im Gegensatz der IP-Pakete der dritten OSI-Schicht werden die Einheiten hier als **Segmente** bezeichnet.
- Das TCP wird als verbindungsorientiertes Protokoll bezeichnet.

TCP Handshake

Der Verbindungsaufbau läuft nach dem Three-Way-Handshake ab. Zuerst schickt der Client an den Server einen Verbindungswunsch (SYN). Der Server bestätigt den Erhalt der Nachricht (ACK) und äußert ebenfalls seinen Verbindungswunsch (SYN). Der Client bestätigt den Erhalt der Nachricht (ACK). Danach erfolgt der Datenaustausch zwischen Client und Server.

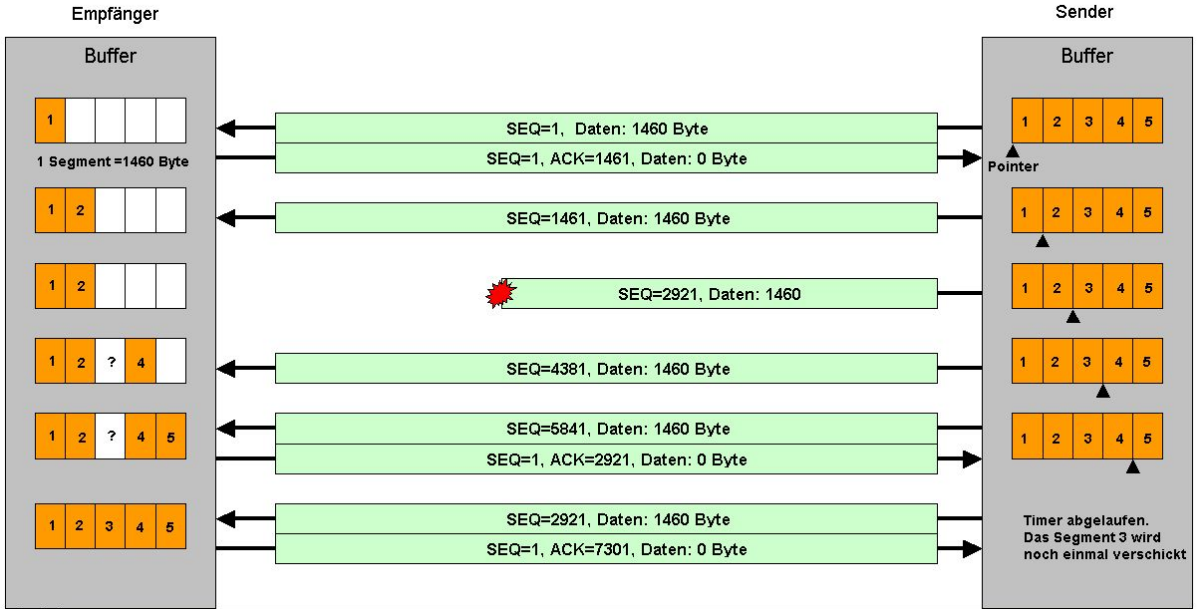


TCP Pseudo Header

TCP-Pseudo-Header (IPv4)

Bit offset	Bits 0–3	4–7	8–15	16–31
0	IP-Absenderadresse			
32	IP-Empfängeradresse			
64	00000000		6 (=TCP)	TCP-Länge
96	Quellport			Zielport
128	Sequenznummer			
160	ACK-Nummer			
192	Datenoffset	Reserviert	Flags	Window
224	Prüfsumme			Urgent pointer
256	Options (optional)			
256/288+	Daten			

Beispiel: TCP Datenübertragung



UDP – User Datagram Protocol

- Eine Alternative zum TCP stellt das UDP, oder auch User Datagram Protocol, dar. Üblicherweise wird das UDP von Verbindungen genutzt, in dem das einzelne Datenpaket von geringer Bedeutung, die Verbindungsgeschwindigkeit jedoch von hoher Bedeutung ist.
- Das UDP sorgt für einen schnelleren Datenaustausch als das TCP, ist dabei jedoch unsicherer, da 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 einmal beim Empfänger eintrifft.

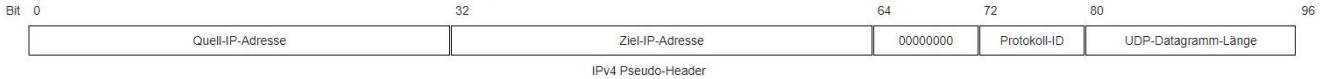
UDP – User Datagram Protocol

- UDP bietet allerdings eine Integritätsüberprüfung mittels einer Prüfsumme an, sodass Fehlerhafte Datagramme erkannt und verworfen werden können. In diesem Protokoll werden die Transporteinheiten UDP-Datagramme, oder auch User-Datagramme genannt. UDP wird auch als verbindungsloses Protokoll bezeichnet.

UDP Pseudo Header

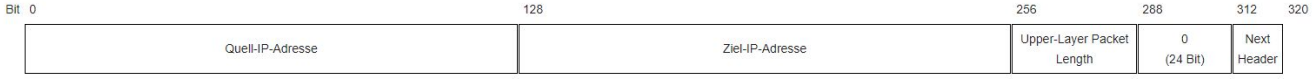
Der Pseudo-Header hat bei IPv4 eine Größe von 12 Oktetts (96 Bit) und setzt sich zusammen aus Quell-IP-Adresse (32 Bit), Ziel-IP-Adresse (32 Bit), 8 Bit Leerfeld, 8 Bit Protokoll-ID (UDP hat die ID 17) und der Länge des UDP-Datagramms (16 Bit).

- **IPv4**



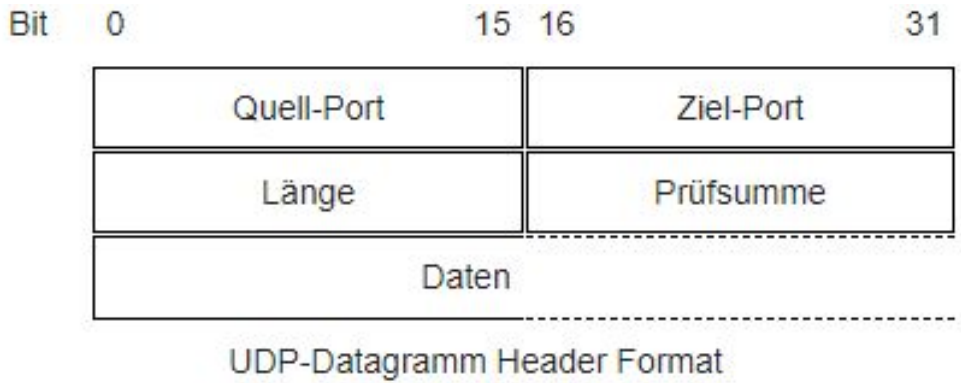
IPv4 Pseudo-Header

- **IPv6**



IPv6 Pseudo-Header

UDP-Datagramm Header



UDP-Datagramm Header Format

Ports

- Als Verbindung zwischen der vierten und der fünften OSI-Schicht existieren Ports.
- Diese werden verwendet, um ein Datenpaket einer Anwendung zuzuordnen. Diese Zuordnung erfolgt durch das Betriebssystem des Clients bzw. Servers.
- Dabei sind die ersten 1024 Ports (0 – 1023) fest vergebene Standardports wie zum Beispiel Port 21 für FTP Daten, Port 80 für http-Proxys oder 443 für HTTPS-Verbindungen.

Ports

- Die nachfolgenden Ports bis einschließlich Port 49.151 können zur Nutzung registriert werden und werden dann offiziell für die Nutzung durch einen bestimmten Dienst von der IETF (Internet Engineering Task Force) vorgesehen.
- Die Ports 49.152 bis 65.535 sind sogenannte dynamische Ports und werden vom Betriebssystem dynamisch an Clientprogramme vergeben. In Verbindung mit der IP-Adresse bildet die Portnummer dann einen sogenannten Socket. Die Schreibweise ist dann wie folgt: IP-Adresse:Port-Nr.

SMB – Server Message Block

- Zusätzlich zu diesen geläufigen Protokollen existieren noch viele weitere, welche unter Umständen auch anderen Schichten zugeordnet sein können.
- Ein weiteres bekanntes Beispiel ist der sogenannte SMB (Server Message Block). Dabei handelt es sich um ein Kommunikationsprotokoll für Datei-, Druck- und andere Serverdienste in Microsoft Netzwerken.
- Das SMB ist dabei nicht konfigurierbar und verbirgt sich meist hinter Microsoft-proprietären Diensten wie zum Beispiel „Client für Microsoft Netzwerke“, „Datei und Druckfreigabe“, „Netzwerk-Umgebung“, „Netzwerk und Freigabecenter“ usw.

SMB – Server Message Block

- Außerdem wird dieses Protokoll verwendet, um dem Open Source Dienst „Samba“ den Zugriff auf Ressourcen von Unix-basierten Systemen zu ermöglichen.
- Die aktuelle Version von SMB ist SMBv3. Die erste Version von SMB (SMBv1) gilt bereits als veraltet und unsicher und sollte daher nicht länger verwendet werden.

Was sollte ich auf jeden Fall behalten

- TCP ist ein Verbindungsorientiertes Protokoll, dass zum Verbindungsaufbau einen Drei-Wege-Handshake bestehend aus SYN, ACK+SYN und ACK durchführt
- Durch Header-Informationen und zugehörige algorithmische Implementierungen können Paketverluste in einem gewissen Maße kompensiert werden
- UDP ist minimales, verbindungsloses Protokoll, welches Vorteile in der Übertragungsgeschwindigkeit implementiert
- Als Verbindung zwischen der vierten und der fünften OSI-Schicht existieren Ports
- In Verbindung mit der IP-Adresse bildet die Portnummer dann einen sogenannten Socket: z.B. 192.168.8.1:444

CloudCommand

CloudCommand GmbH jens_leonhardt@outlook.de