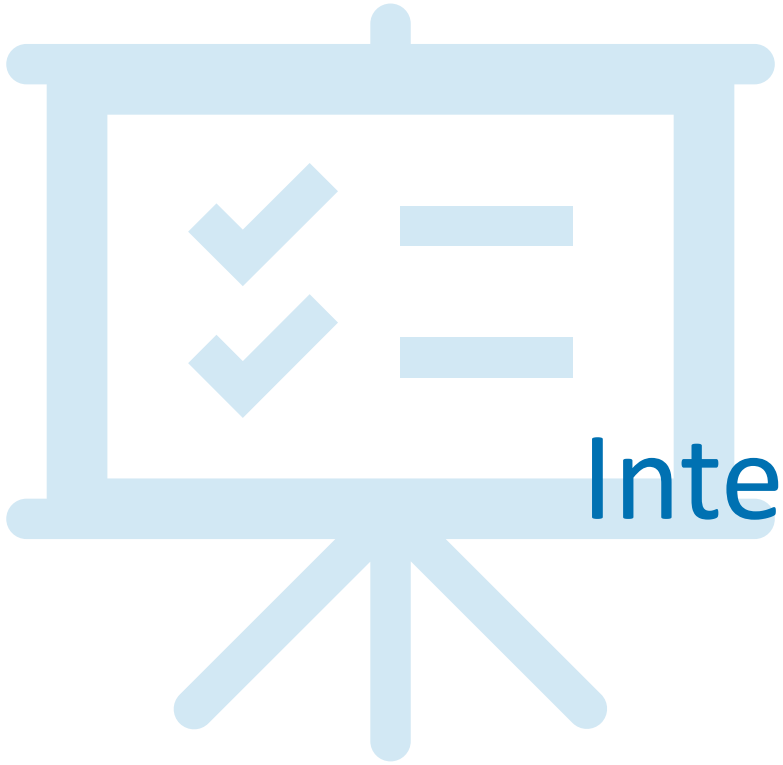

Netzwerke und Internettechnologien 1

ICMP, IGMP, TPC und UDP

Netzwerke und Internettechnologien 1

Lernziele

1. Protokolle der Internetschicht IGMP, ICMP

2. Protokolle der Transportschicht TCP, UDP

3. Socket-Kommunikation

Protokolle der Internetschicht
ICMP und IGMP

ICMP (Internet Control Message Protocol)

- ICMP ist ein Protokoll der Internetschicht, das zur Übermittlung von Meldungen über IP dient.
- Aufgaben sind die Übertragung von Statusinformationen und Fehlermeldungen der Protokolle IP, TCP und UDP.
- Die ICMP-Meldungen werden von Netzwerkknoten wie Routern benutzt, um sich gegenseitig Probleme mitzuteilen. Ziel der ICMP-Kommunikation ist, die Qualität der Datenübertragung zu verbessern.
- Hinweis: ICMP verwendet das unsichere Internet Protocol. Gehen Meldungen von ICMP verloren, dann löst das keine Fehlermeldung aus.
- Für den Betrieb mit IPv6 wurde ICMPv6 entwickelt, welches als Hilfsprotokoll dient. IPv6-Kommunikation ist ohne ICMPv6 nicht möglich.

ICMP (Internet Control Message Protocol)

- ICMP hat keine eigene Header-Struktur, sondern nutzt den Standard-IP-Header
- Die Felder Type-of-Service und Protokoll des IP-Headers werden angepasst.
- Alle ICMP-Nachrichten beinhalten drei Felder:
  - Das Typfeld, um den Typ der Nachricht anzugeben.
  - Das Codefeld, um den Typ der Fehler- oder Statusinformation zu beschreiben.
  - Ein Prüfsummenfeld.

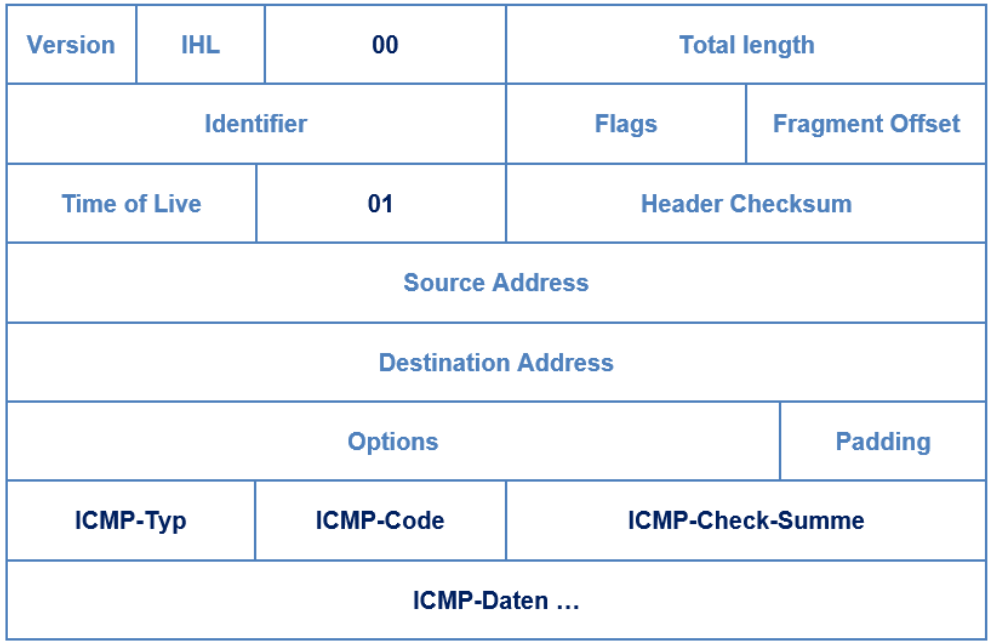

Abbildung 1: ICMP (Quelle RFC 792, Eigene Darstellung)

ICMP (Internet Control Message Protocol)

Fehler- und Statusmeldungen (Auszug)

Typ	Typname	Code	Bedeutung
0	Echo-Antwort	0	Echo-Antwort
3	Ziel nicht erreichbar	0	Netzwerk nicht erreichbar
		1	Host (Zielstation) nicht erreichbar
		2	Protokoll nicht erreichbar
		3	Port nicht erreichbar
		4	Fragmentierung nötig, **D**on't **F**ragment aber gesetzt
		5	Route nicht möglich (die Richtung in IP-Header-Feld Option falsch angegeben)
		13	Communication administratively prohibited (Paket wird von der Firewall des Empfängers geblockt)
4	Entlasten der Quelle	0	Datagramm verworfen, da Warteschlange voll
8	Echo-Anfrage	0	Echo-Anfrage (besser bekannt als „Ping“)
11	Zeitlimit überschritten	0	TTL (Time To Live, Lebensdauer) abgelaufen
		1	Zeitlimit während der Defragmentierung überschritten

Abbildung 2: ICMP-Meldungen (Quelle Wikipedia, Eigene Darstellung)

ICMP (Internet Control Message Protocol)

- Anwendung von ICMP
  - ICMP-Meldungen werden häufig von Hosts im Netzwerk verursacht, die Probleme mit IP-Paketen des sendenden Hosts mitteilen wollen.
  - Jedes Betriebssystem, das mit TCP/IP arbeitet, hat Tools, welche ICMP nutzen. Die beiden bekanntesten Tools sind Ping und Trace Route. Diese sind für die Analyse von Netzwerk-Problemen gedacht und können bei der Behebung von Problemen helfen.
    - Ping
    - Trace Route (traceroute, tracert)
  - Zur Problemlösung können auch der Datenverkehr und die ICMP-Meldungen mit einem Netzwerkmonitor überwacht werden.

ICMP (Internet Control Message Protocol)

- Es kommt zum Einsatz, wenn
  - ein Gateway das Datagramm nicht weiterleiten kann.
  - ein Gateway Datenverkehr über eine kürzere Route leitet.
  - ein Gateway nicht genügend Pufferkapazität besitzt, um ein Datenpaket zwischenzuspeichern und weiterzuleiten.
  - ein Empfänger nicht erreichbar ist.
  - die Lebensdauer eines Datagramms ausläuft.

ICMP (Internet Control Message Protocol)

- Sicherheitsbedrohungen:
  - ICMP als verbindungsloses Protokoll kann für eine Reihe von Angriffsmethoden mißbraucht werden, wie Denial-of-Service- (DoS) oder Distributed-Denial-of-Service-Angriff (DDoS).
  - Typische Angriffe sind der Smurf-Angriff, das Flooding oder der Ping of Death.
  - Das ICMP-Protokoll kann zur unberechtigten Datenübertragung verwendet werden, um so den Schutz von Paketfilter-Firewalls auszuhebeln.

IGMP (Internet Group Management Protocol)

- Das Internet Group Management Protocol (IGMP) ist eine Erweiterung des Internet Protokolls (IPv4).
- Mit IGMP ist IP-Multicasting (Gruppenkommunikation) im LAN und im Internet möglich.
- Für IPv6 wurde MLD (Multicast Listener Discovery) entwickelt, das die Funktionen von IGMP übernimmt.
  MLD ist kein eigenständiges Protokoll, sondern in ICMPv6 eingebettet.

IGMP (Internet Group Management Protocol)

- IGMP dient zur dynamischen Gruppenverwaltung.
- Die Verwaltung erfolgt über die Routern, an denen die Empfänger einer Multicast-Gruppe direkt angeschlossen sind. Eine Station teilt einem Router mit, dass sie Multicast-IP-Pakete einer bestimmten Multicast-Gruppe empfangen will.
- Der Sender verschickt ein einziges Datenpaket an seinen übergeordneten Router. Dieser dupliziert das IP-Paket bei Bedarf, wenn er mehrere angeschlossene Netze mit Empfängern hat.

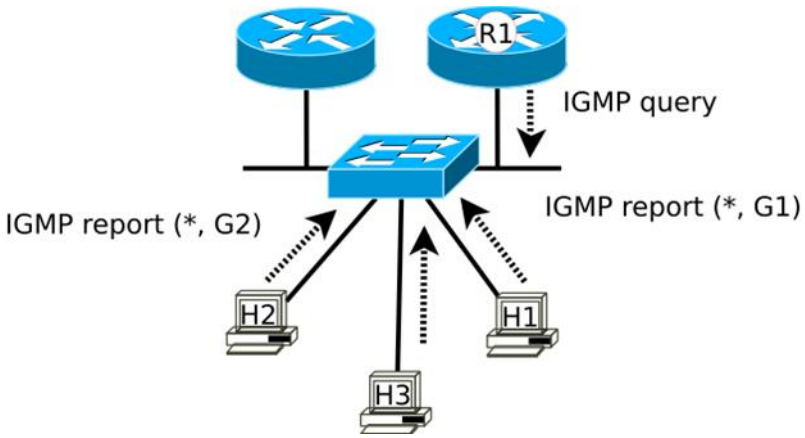

Abbildung 3: IGMP-Struktur (Quelle Wikipedia)

IGMP (Internet Group Management Protocol)

IGMP-Snooping

- IGMP-Snooping ist ein Abhörverfahren für Multicast-Datenverkehr und soll diesen auf die anfordernden Hosts beschränken .
- Die beteiligten Router oder Switches müssen dieses Verfahren beherrschen.
- Die Geräte überwachen den Multicast-Datenverkehr und erkennen, wenn ein Empfänger einer Multicast-Gruppe beitritt oder sie verlässt. Dazu führen Sie eine entsprechende Adresstabelle.
- Bei Verwendung von IPv6 gibt es für Multicast Listener Discovery (MLD) die Möglichkeit MLD-Snooping zu aktivieren.

IGMP (Internet Group Management Protocol)

- ICMP hat keine eigene Header-Struktur, sondern nutzt den Standard-IP-Header.
- Die Felder Type-of-Service und Protokoll des IP-Headers werden angepasst und das TTL-Feld auf 1 gesetzt. IGMP-Meldungen werden nur zwischen direkt ausgetauscht.
- Alle IGMP-Nachrichten beinhalten die Felder:
  - IGMP-Typ (Meldungstyp)
  - Max. Response Time (maximale Antwortzeit)
  - IGMP-Check-Summe Multicast-IP-Adresse (Gruppenadresse)

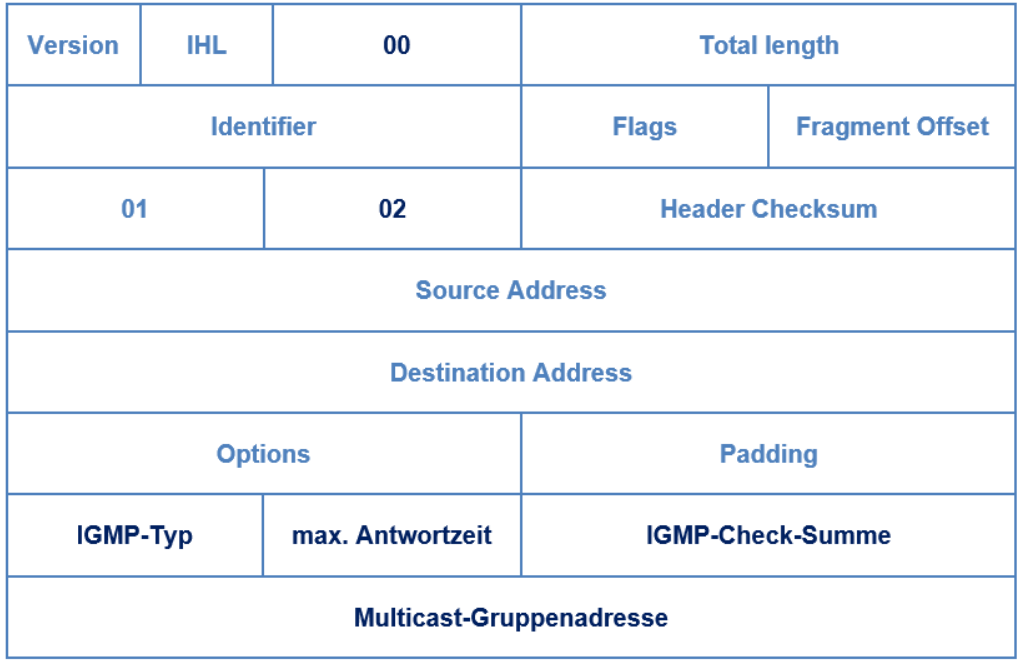

Abbildung 4: IGMP (Quelle Wikipedia, Eigene Darstellung)

Protokolle der Transportschicht

TCP (Transmission Control Protocol)

- TCP ist ein verbindungsorientiertes Protokoll.
- TCP arbeitet streamorientiert, da es seine Daten als Datenstrom ansieht. Durch die Verwendung von Sequenznummern kann die Empfängerseite die Segmente wieder in richtiger Reihenfolge zusammenbauen und wieder zu Datenstrom formieren.
- TCP bietet einen verlässlichen Datentransfer durch einen Mechanismus, der Datenpakete solange an den Empfänger schickt, bis dieser eine Bestätigung des Empfangs schickt.
- Nachteilig ist der recht große Overhead.

Vergleich UDP- und TCP-Header

TCP Header

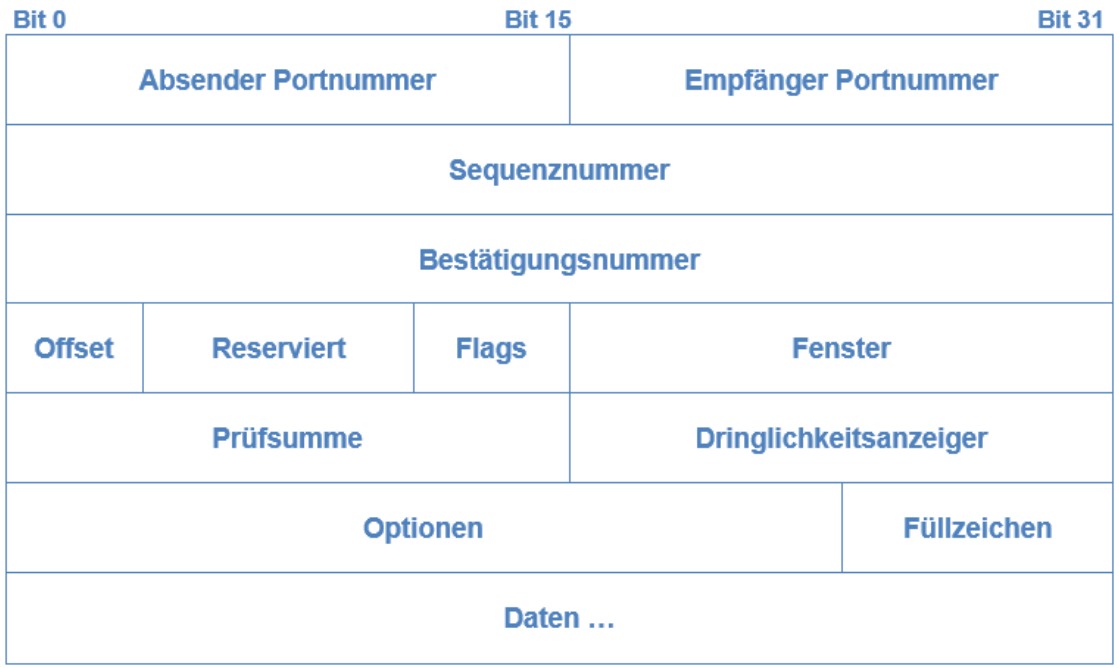

Abbildung 5: TCP-Header (Quelle RFC 793 Eigene Darstellung)

UDP Header

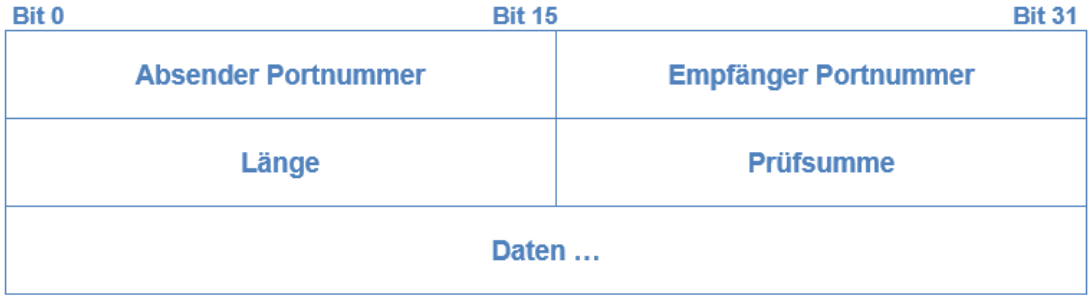

Abbildung 6: UDP-Header (Quelle RFC 768 Eigene Darstellung)

UDP

- Ist ein einfaches Protokoll, welches die Übermittlung von Daten mit einem Minimum an Protokollinformationen ermöglicht.
- UDP ist verbindungslos, die Sicherstellung des Empfangs ist Sache der Anwendungsprotokolle.
- UDP arbeitet mit Datagrammen fester Größe, es ist nicht in der Lage einen Datenstrom aufzuteilen und wieder zusammenzusetzen.
- Die Verwendung erfolgt immer dann, wenn es:
  - mehr auf die Geschwindigkeit, als auf die Sicherheit in der Übertragung ankommt.
  - wenn die Datenmenge so klein ist, dass ein großer Header nicht lohnt.

Port

- Ein Port ist innerhalb des TCP/IP-Modells ein Prozess der oberen Schicht (Anwendung), der seine Daten an die darunterliegende Schicht übergibt bzw. von dieser erhält.
- Ist in der Transportschicht definiert.
- Ports sind mit einem 16 Bit Wert nummeriert, getrennt für TCP und UDP, dabei hat jeder Prozess hat seine eigene Portnummer.
- Port-Zustände können sei: offen, geschlossen und gefiltert.
- Port-Bereiche:

Well Known Ports	0 - 1.023	Diese Ports sind fest einer Anwendung oder einem Protokoll zugeordnet. Diese Ports dürfen nur von root (Administrator) gebunden werden.
Registered Ports	1.024 - 49.151	Diese Ports sind für Dienste vorgesehen.
Dynamically Allocated Ports	49.152 - 65.535	Jeder Client kann diese Ports nutzen, sie werden dynamisch zugewiesen.

Socket

- Socket ist eine Adressen-Struktur, die einen Kommunikationsendpunkt darstellt.
- Ein solcher Socket bezeichnet den logischen Endpunkt einer Verbindung und ist über die Datenstruktur, den Port, die IP-Adresse und das Transportprotokoll definiert.
- Als Socket wird die Adressenkombination aus IP-Adresse und Portnummer bezeichnet mit der eine bestimmte Anwendung auf einem bestimmten Rechner angesprochen werden kann. Mit der IP-Adresse wird das Netzwerk und der Rechner bestimmt und mit der Portnummer die Anwendung ausgewählt.
- Ein Socket existiert jeweils auf Sender- und auf Empfängerseite.
- Anwendungen auf den Kommunikationspartnern kommunizieren mittels der Sockets.

Socket-Kommunikation

- Sockets bilden eine standardisierte Schnittstelle (API) zwischen dem Netzwerkprotokoll und der Anwendung.
- Die Socket API stellt dabei Funktionen, wie socket(), bind(), listen(), connect(), accept(), end(), receive() und close() bereit.
- Der Client / die Clientanwendung fordert meist vom Betriebssystem ein Socket mit Portnummer an. Serveranwendungen wählen den Port selbst.
- Es muß zwischen TCP- und UDP-Kommunikation unterschieden werden.

Socket-Kommunikation

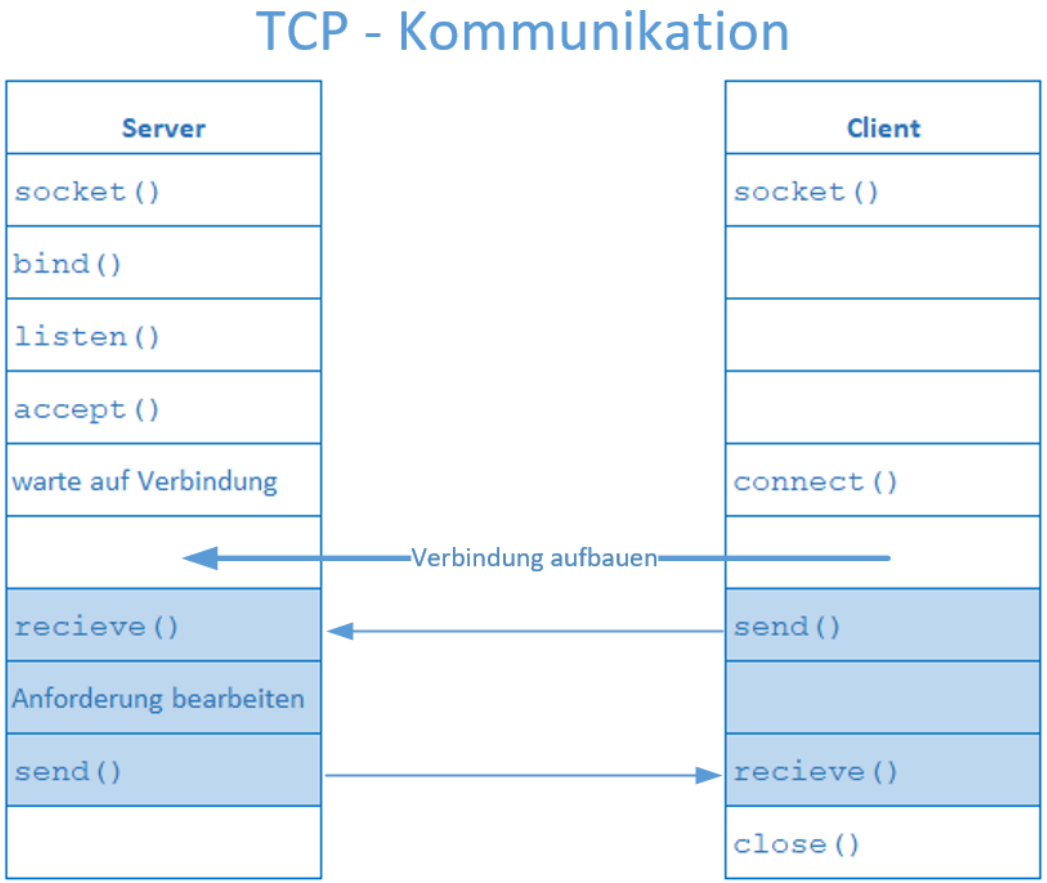

Abbildung 7:TCP-Socket (Quelle Socket Programming HOWTO, Eigene Darstellung)

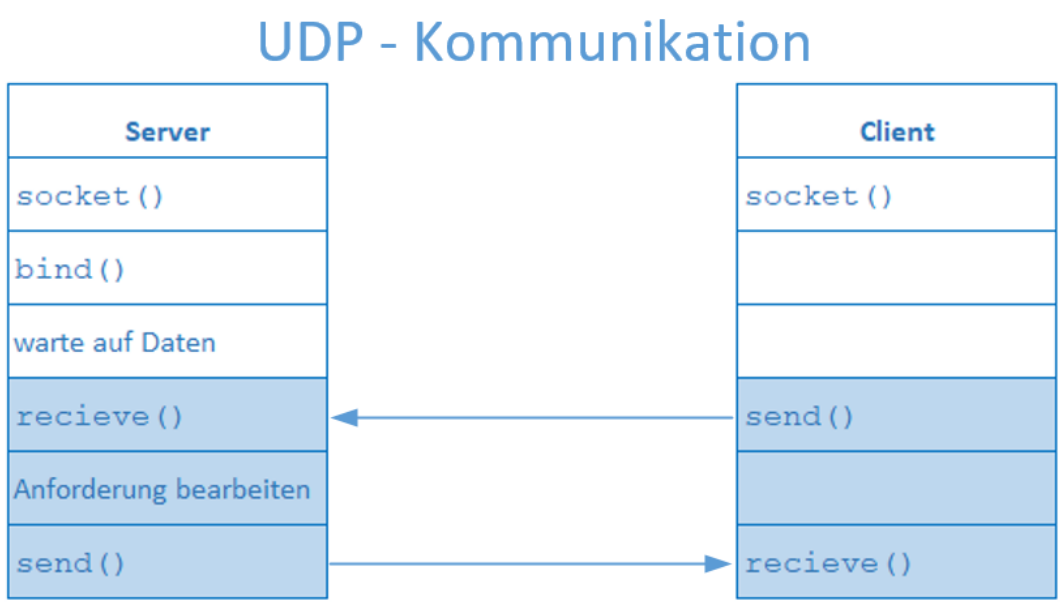

Abbildung 8: UDP-Socket (Quelle Socket Programming HOWTO, Eigene Darstellung)

Quellen

Buchquellen

Socket Programming HOWTO — Python 3.9.5 documentation (2021). Online verfügbar unter https://docs.python.org/3/howto/sockets.html, zuletzt aktualisiert am 07.05.2021, zuletzt geprüft am 07.05.2021.

IONOS Hilfe (2021): IPv6: Grundlagen - IONOS Hilfe. Online verfügbar unter https://www.ionos.de/hilfe/server-cloud-infrastructure/ip-adressen/ipv6-grundlagen/#c21567, zuletzt aktualisiert am 03.05.2021, zuletzt geprüft am 03.05.2021.

Kersken, Sascha (2017): IT-Handbuch für Fachinformatiker. Der Ausbildungsbegleiter. 8. Auflage, revidierte Ausgabe. Bonn: Rheinwerk Verlag; Rheinwerk Computing.

Schreiner, Rüdiger (2014): Computernetzwerke. Von den Grundlagen zur Funktion und Anwendung. 5., erw. Aufl. München: Hanser.

Tools.ietf.org, Rfcmarkup Version 1.129d On (2021): RFC 768 - User Datagram Protocol. Online verfügbar unter https://tools.ietf.org/html/rfc768, zuletzt aktualisiert am 25.04.2021, zuletzt geprüft am 07.05.2021.

Tools.ietf.org, Rfcmarkup Version 1.129d On (2021): RFC 792 - Internet Control Message Protocol. Online verfügbar unter https://tools.ietf.org/html/rfc792, zuletzt aktualisiert am 02.05.2021, zuletzt geprüft am 06.05.2021.

Tools.ietf.org, Rfcmarkup Version 1.129d On (2021): RFC 793 - Transmission Control Protocol. Online verfügbar unter https://tools.ietf.org/html/rfc793, zuletzt aktualisiert am 02.05.2021, zuletzt geprüft am 07.05.2021.

Wikipedia (Hg.) (2019): Internet Control Message Protocol, zuletzt aktualisiert am 13.12.2019, zuletzt geprüft am 06.05.2021.

Wikipedia (Hg.) (2019): Internet Group Management Protocol, zuletzt aktualisiert am 09.02.2019, zuletzt geprüft am 07.05.2021.

Cisco (2020): Konfigurieren von IGMP-Snooping (Internet Group Management Protocol) auf den Managed Switches der Serien 200 und 300, zuletzt aktualisiert am 08.07.2021, zuletzt geprüft am 08.07.2021.

IONOS Digitalguide (2021): IGMP-Snooping: Das Abhörverfahren für Multicast-Traffic. Online verfügbar unter https://www.ionos.de/digitalguide/server/knowhow/igmp-snooping/, zuletzt aktualisiert am 08.07.2021, zuletzt geprüft am 08.07.2021.

Quellen

Abbildungen

3 „Struktur von IGMP“ Lizenz: Mro (https://commons.wikimedia.org/wiki/File:IGMP_LAN.svg), „IGMP LAN“, https://creativecommons.org/licenses/by-sa/3.0/legalcode

VIELEN DANK!