

# Implementierung eines multithreaded TCP/IP Stacks für einen auf AMIDAR basierten Java Prozessor

Bachelorarbeit  
Robert Wiesner  
31. Mai 2017



TECHNISCHE  
UNIVERSITÄT  
DARMSTADT



---

Erklärung gemäß § 22 Abs. 7 APB

---

Hiermit erkläre ich gemäß § 22 Abs. 7 der Allgemeinen Prüfungsbestimmungen (APB) der Technischen Universität Darmstadt in der Fassung der 4. Novelle vom 18. Juli 2012, dass ich die Arbeit selbstständig verfasst und alle genutzten Quellen angegeben habe und bestätige die Übereinstimmung von schriftlicher und elektronischer Fassung.

Darmstadt, den 31. Mai 2017

Ort, Datum

Robert Wiesner

**Fachbereich Elektro- und Informationstechnik**

Institut für Datentechnik

Fachgebiet Rechnersysteme

Prüfer: Prof. Dr.-Ing. Christian Hochberger

Betreuer: Dipl.-Inform. Changgong Li

---

## Inhaltsverzeichnis

---

1	Einleitung	3
1.1	Motivation . . . . .	3
1.2	Aufgabenstellung . . . . .	3
2	Grundlagen	4
2.1	Netzwerk Schichtenmodell . . . . .	4
2.2	Ethernet . . . . .	4
2.2.1	Verfahren . . . . .	4
2.2.2	Ethernet Frame . . . . .	5
2.3	Internet Protocol Version 4 (IPv4) . . . . .	5
2.3.1	Paket Aufbau . . . . .	5
2.3.2	Adressierung . . . . .	6
2.3.3	Fragmentierung . . . . .	7
2.4	Transmission Control Protocol (TCP) . . . . .	8
2.4.1	Paketaufbau . . . . .	8
2.4.2	Zustände . . . . .	9
2.4.3	Sequenznummern . . . . .	9
2.4.4	Verbindungsaufbau . . . . .	10
2.4.5	Datenübertragung . . . . .	10
2.4.6	Überlastkontrolle . . . . .	10
2.4.7	Verbindungsabbau . . . . .	10
2.5	Dynamic Host Control Protocol (DHCP) . . . . .	10
2.5.1	Paket Format DHCP (Bootstrap) . . . . .	10
2.6	AMIDAR . . . . .	12
3	Implementierung	13
3.1	Überblick . . . . .	13
3.2	TCP Stack . . . . .	13
3.3	IP Stack . . . . .	13
3.4	DHCP . . . . .	13
3.5	Stream Sockets . . . . .	13
4	Evaluation	14
4.1	Testaufbau . . . . .	14
4.2	Funktionen . . . . .	14
4.3	Performanz . . . . .	14
5	Zusammenfassung	15
5.1	Fazit . . . . .	15
5.2	Ausblick . . . . .	15

---

## 1 Einleitung

---

### 1.1 Motivation

---

Diese Arbeit basiert auf den im Fachgebiet Rechnersystem entwickelten AMIDAR Prozessor und der dafür angepassten Java API. Zum Zeitpunkt der Arbeit verfügt AMIDAR mit der dazugehörigen API über grundlegende Netzwerk Funktionalitäten. Dazu gehören die Unterstützung für die Protokolle Ethernet, ARP, begrenzt IPv4 und UDP. Mit UDP kann keine korrekte und verlustfreie Datenübertragung garantiert werden, welche für viele Netzerkanwendungen vorausgesetzt wird. Im Rahmen dieses Projektes wird TCP Stack entwickelt, sowie der IP Stack erweitert um eine geordnete und verlustfreie Datenübertragung zu realisieren.

---

### 1.2 Aufgabenstellung

---

---

## 2 Grundlagen

---

### 2.1 Netzwerk Schichtenmodell

---

Netzwerk Kommunikation zwischen Anwendungen wird üblicherweise als Schichtenmodell beschrieben. Die unterste Schicht stellt dabei das physical layer. Das beschreibt die Physische Übertragung von Daten. Darüber sorgt die Sicherungsschicht für eine funktionierende Verbindung zwischen Endgeräten und den Übertragungsmedium. Auf dieser Schicht wird zum Beispiel das Ethernet Protokoll eingesetzt, das die übertragenen Daten auf Fehler überprüft und im Zweifel verwirft. Darunter kommt die Vermittlungsschicht, in der die Endgeräte Adressiert werden und Routing und Datenflusskontrolle gesteuert werden. Ein wichtiges Protokoll dieser Schicht ist das IP Protokoll. 5blabla

Bei einer Datenübertragung von einer Anwendung zu einer auf einen anderen Endgerät laufenden werden die Daten in durch die Schichten nach unten gereicht, wobei in jeder Schicht ein neuer Header erzeugt wird, der für die jeweilige Schicht wichtige Informationen enthält. Zum Beispiel werden die Daten von der Anwendung mit betriebsystemsabhängigen Systemaufrufen an den TCPStack übergeben. Dieser erzeugt ein TCP Paket, das außer den Daten einen Header enthält, welcher Information bereitstellt, die unter anderen für das richtige Zusammensetzen der einzelnen Datenpakete beim Empfänger, als auch für die Zuordnung der übertragen Daten zu der jeweiligen Anwendung benötigt werden. Bei der anschließenden Erzeugung des IP Pakets bilden das TCP Paket bestehend aus Daten und TCP-Header die zu übertragenden Daten. Der IP Header enthält unter anderen die IP-Adressen des Ziel und Quell Geräts. Das IP Paket bleibt im Normalfall unverändert, bis das Zielgerät erreicht ist. An der nächst unteren Ebene steht das Ethernet Datagramm. Es enthält neben dem IP Paket die Physischen Adressen von des Quell Endgeräts und der nächsten Zwischenstation auf dem Weg zum Ziel. Bei Zwischenstation wird anhand der der Daten des IP Pakets der nächste Wegpunkt ermittelt und ein neues Datagramm erzeugt.

Wenn ein Datagramm das Ziel erreicht wird das IP Paket extrahiert und daraus das TCP Paket. Anhand der Port Nummer kann das TCP Paket der Anwendung zugeordnet werden.

---

### 2.2 Ethernet

---

Ethernet nach der IEEE Norm 802.3 ist seit den 90ern der am weitesten verbreitete Standard für Lokale Netzwerke und beschreibt sowohl die Bitübertragungs als auch die Sicherungsschicht.

---

#### 2.2.1 Verfahren

---

Um zu ermöglichen das mehrere Endgeräte auf den selben Physischen Medium kommunizieren können wurde früher ein Zeitmultiplexverfahren eingesetzt, das durch den CSMA/CD Algo-

---

rhythmus gesteuert wird. Wenn eine Stelle Daten zum senden bereithält, wartet diese bis das Medium ungenutzt ist und fängt dann an die Daten zu übertragen. Wenn 2 Stellen gleichzeitig beginnen zu senden wechseln beide auf ein SStörung-ErkantSSignalmuster und beenden die Übertragung. Nach einer zufällig langen Pause wird jeweils ein erneuter Übertragungsversuch gestartet.

Mittlerweile werden Kollisionen durch die Einführung von Switches verhindert. In diesen können Ethernet Pakete zwischengespeichert werden bis diese gesendet werden können. Dadurch wird eine Vollduplex Übertragung zwischen Switches und anderen Endgeräten ermöglicht. Es kann jedoch vorkommen, das Switches bei zu großen Datenaufkommen überlastet werden weswegen die Ethernet Flow Control Datenpakete verwerfen kann. Deswegen ist es wichtig, das Protokolle auf den darüber liegenden Schichten verworfene Datenpakete erkennen und erneut senden können um eine zuverlässige Datenübertragung zu gewährleisten.

---

### 2.2.2 Ethernet Frame

---

Ein Ethernet Paket beginnt mit einer sieben Bit langen Präambel die aus einer alternierenden Folge von Einsen und Nullen besteht. Diese wird für die Synchronisation der Verbindung benötigt und ermöglicht es die Folgen Daten von Hintergrundrauschen zu unterscheiden. Unterbrochen wird die Präambel durch das auf Eins gesetzte SStart of Frame"Bit was mit den letzten Bit der Präambel 2 aufeinander Folgende Einsen ergibt. Der eigentliche Ethernet Frame beginnt mit der aus Sechs Byte bestehenden Ziel MAC-Adresse gefolgt von der Quell MAC-Adresse. Dazu kommen 2 Byte die den Typ des darüber liegenden Protokolls angeben. Zum Beispiel 0x0800 gibt IPv4 an. Dahinter kommen 46-1500 Bytes an Daten, gefolgt von 4 Bytes Frame Check Sequence. Diese besteht aus einer CRC Checksumme.

---

## 2.3 Internet Protocol Version 4 (IPv4)

---

Das IP Protokoll ist das für die Datenübertragung wichtigste Protokoll, auf der Vermittlungsschicht. Es wurde Entwickelt um eine paketvermittelte Kommunikation über mehrere Computernetzwerke hinweg zu ermöglichen. Quellen und Ziele der Übertragungen werden jeweils als Adressen mit fester 32 Bit Länge angegeben. Es gibt keine Mechanismen für Zuverlässige Übertragung, Flusskontrolle und Sequenzierung, weswegen das darüber liegen Protokoll dies sicher stellen muss. Es gibt jedoch Möglichkeiten zur Paketfragmentierung, falls Datenpakete die Maximale Segment Größe für Pakete der darunter liegenden Schicht überschreiten sollten.

---

### 2.3.1 Paket Aufbau

---

Version: Gibt in an welche Version des IP Protokolls verwendet wird. (4Bit)

IHL: Steht für Internet Header Length und gibt an wie 32Bit Wörter von dem IP-Header belegt werden.

ToS: Type of Service beinhaltet abstrakte Parameter zur Bestimmung der Qualität des gewünschten Services. Dabei geben die Bits Null bis Zwei die Priorität der Daten an. Die Bits Drei, Vier und

---

Fünf stehen für niedrige Latenz, hohen Durchsatz und hohe Zuverlässigkeit. Die letztgenannten Parameter werden von Netzwerkgeräten von unterschiedlich interpretiert, in dem meisten ruft bessere Performance für einen der Parameter eine Verschlechterung bei einen anderen herbei.

Paketlänge: Gesamtlänge eines Pakets in Bytes einschließlich des Headers. Die 16Bit ergeben eine theoretische Gesamtlänge von 65.535 Bytes, was für viele Netzwerke jedoch nicht geeignet ist. Als Mindestgröße die alle Hosts unterstützen müssen wurde 576 Bytes festgelegt. Das ermöglicht es 512 Byte Daten und 64 Byte Header in einen Paket zu übertragen. Da der IP Header selber nur 20 Byte benötigt bleibt noch ein Puffer von 44 Byte für den Header des darüber liegenden Protokolls.

Kennung: Ein Identifikationswert, der benötigt wird um fragmentierte Pakete wieder zusammen zu setzen. (16Bit)

Flags: 3 Bits von denen das erste reserviert ist und dauerhaft auf Null gesetzt wird. Das zweite Bit gibt an, ob das Paket fragmentiert werden darf. Das letzte Bit wird gesetzt, wenn nach dem Paket noch weiter Fragmente folgen.

Fragment-Offset: Besteht aus 13 Bit und gibt an, an welche Stelle des Datagramms die Daten dieses Fragments gehören.

TTL (Time-to-live): Gibt die maximale Zeit in Sekunden an, die ein Paket im Netzwerk unterwegs sein darf. Sobald die TTL den Wert Null erreicht muss das Paket gelöscht werden. Da der Wert bei jeder Zwischenstation, unabhängig von der eigentlichen Verarbeitungszeit ebenfalls um eins Reduziert werden muss ist die übliche Lebensdauer eines Pakets deutlich kürzer als in der TTL angegeben.

Protokoll: Gibt an welches Protokoll im nächst höheren Level verwendet wird.

Header Checksumme: Checksumme nur über den Header. Da sich der Header beim Weg Zwischenstationen verändern kann, zum Beispiel wegen der Time to Life , muss die Checksumme nach jeder Verarbeitung des Headers an den Zwischenstationen neu berechnet werden.

Quell-IP-Adresse: IP Adresse des Hosts, der das Paket ursprünglich versendet hat.(4 Byte)

Ziel-IP-Adresse:IP Adresse des Zielendgeräts. (4 Byte)

Optionen/Füllbits

---

### 2.3.2 Adressierung

---

Um mehrere Netzwerke innerhalb eines großen zu ermöglichen, werden IP Adressen interpretiert, in dem eine bestimmte Menge der höherwertigen Bits das Netzwerk spezifiziert und die restlichen Bits den genauen Hosts des gewählten Netzwerks adressieren. Dabei soll Flexibili-

---

tät bei der Unterteilung von kleineren Teilnetzwerken ermöglicht werden. Daher wurde das Adressfeld entsprechend in bestimmte Klassen unterteilt. Es wurden 3 Klassen A,B,C angelegt. Die Klassen unterscheiden sich jeweils durch die Aufteilung des Adressbereichs zwischen Netzwerk Adresse und Host Adresse innerhalb des Netzwerks. Die ersten 1-3 Bits der Adresse geben jeweils Ausschluss darüber zu welcher Netzwerkkategorie die jeweilige IP-Adresse gehört. Um innerhalb dieser starren Netzwerke feiner Aufgeteilte Subnetze zu erzeugen kann die Subnetmask genutzt werden. Die Subnetmask ist ebenfalls eine 4 Byte Zahl, deren niederwertige Bits auf Null gesetzt werden und damit den Variablen Teil innerhalb des subnetz angeben. Der Rest der Maske wird dabei auf Eins gesetzt.

---

### 2.3.3 Fragmentierung

---

Paketfragmentierung wird nötig, wenn ein Paket aus einem Netzwerk kommt das eine große maximale Segmentgröße erlaubt und durch eines geleitet wird, das nur eine kleinere Segmentgröße erlaubt. Dabei können die Pakete in eine theoretisch nahezu endlose Anzahl von kleinen Paketen zerlegt werden. Dabei müssen die Datenblöcke alle Fragmente bis auf das letzte ein vielfaches von 64 Byte an Daten beinhalten. Damit fragmentierte Pakete richtig zusammen gesetzt werden können, haben alle Fragmente, eines Pakets, die selbe Identifikationsnummer. Für das Zusammensetzen des Datenblock wird der Fragmentoffset benötigt der angibt, an welcher Stelle des ursprünglichen Datenblocks die Daten des Fragments stehen. Wobei das fragmented-flag angibt, ob noch weitere Fragmente folgen, oder ob dies das letzte Teil ist. Sobald alle Fragmente eines Pakets beim Ziel eingetroffen sind, kann das ursprüngliche Paket wiederhergestellt werden.



---

## 2.4 Transmission Control Protocol (TCP)

---

Da die Protokolle der unteren Schichten, IP und Ethernet keine fehlerfreie und Verlustlose Übertragung der Daten garantieren können, wird ein Protokoll auf der Transportschicht benötigt, das eine zuverlässige Übertragung von Daten zwischen Anwendungen auf entfernten Hosts sicherstellen kann, auch wenn auf jeden Hosts eine große Anzahl an Anwendungen läuft, die TCP verwenden. Für diesen Zweck wurde das TCP-Protokoll erschaffen. Um dabei die Datenpakete jeweils der richtigen Anwendung zuordnen zu können werden Port-nummern verwendet.

Es handelt sich bei TCP um ein verbindungsorientiertes Protokoll, das bedeutet, dass es zu Beginn einer Übertragung einen klar definierten Verbindungsaufbau gibt. Nachdem die Verbindung etabliert es können Daten Vollduplex in beide Richtungen übertragen werden. Wobei durch Sequenznummern und Acknowledge Nummern die richtige Reihenfolge und Vollständigkeit der Datenpakete sichergestellt wird. Pakete deren Erhalt nicht bestätigt wurde werden automatisch neu übertragen. Desweiteren verfügt TCP über Mechanismen um eine Überlast auf dem Übertragungsweg rechtzeitig zu erkennen und zu beheben.

---

### 2.4.1 Paketaufbau

---

Quell Port (16Bit): Gibt die Portnummer der Anwendung auf Senderseite an

Ziel Port (16Bit): Gibt die Portnummer der Anwendung auf Empfängerseite an

Sequence Number (32Bit):

Acknowledge Number (32Bit):

Data Offset (4Bit): Anzahl von 32Bit Wörtern aus denen der Header besteht.

Reserved (6Bit): reserviert für zukünftige Nutzung

Steuerungsbits (6Bit): 6 Flags die für die Ablauf Steuerung der Übertragung genutzt werden:

URG: Urgent Pointer, wird in moderner Software nicht mehr genutzt und wird von vielen Implementierungen ignoriert.

ACK: Acknowledgment gibt an, ob das Paket eine gültige Bestätigung für empfangene Pakete enthält.

PSH: Push, ist dieses Flag gesetzt, werden die empfangenen Daten sofort an die Hostsoftware weitergereicht. RST: Resetet die Verbindung. Wird im Fehlerfall gesendet und bricht die Verbindung ab. FIN: Signalisiert das Ende der Verbindung, wenn es keine zu übertragenden Daten gibt.

Window (16Bits): Gibt die Größe des Empfangswindows des Absenders an. Gilt für den Empfänger als obere Grenze des Congestion Windows

Checksum (16Bits): Für die Berechnung der Checksumme über das TCP Paket wird vorher ein Pseudoheader bestehend aus den Quell- und Ziel IP-Adresse, des IP-Codes für das verwendete Protokoll und die Gesamtlänge des eigentlichen TCP Pakets. Die Checksumme wird daraufhin über den Pseudoheader, den Header und die Payload berechnet. Dafür werden diese in 16 Bit große Blöcke aufgeteilt und im einer Komplement die Summe über diese gebildet.

UrgentPointer (16Bits): Gibt den Urgentpointer als Offset zu der Sequenznummer an. Wird nur interpretiert, wenn das URG Flag gesetzt ist.

Options: (Variabel): Optionale Informationen, die von TCP Implementierungen unterstützt werden können um Sicherheit und Performance zu verbessern. Optionen bestehen entweder nur aus einem Optionsbyte oder haben zusätzlich ein weiteres Byte das die Länge der jeweiligen Op-

---

tionen angibt. Padding: Falls der TCP Header mit den Optionen einen teilweise genutzten 32Bit Block hat, wird dieser mit Nullen aufgefüllt.

---

#### 2.4.2 Zustände

---

TCP ist im Gegensatz zu den bisher genannten Protokollen Zustandsorientiert, was bedeutet, dass es je nach Zustand anders auf Nutzeraktionen und ankommende Pakete reagiert. Zu den Zuständen gehören:

- Closed**: Das ist der Startzustand einer TCP Instanz. Die Verbindung ist geschlossen. Usercalls außer "Open" werden mit Fehlermeldungen quittiert und ankommende Pakete werden verworfen und mit einem Reset-Paket beantwortet.

**SYN-sent**: Nachdem eine Verbindung initiiert wurde, wird auf eine Antwort des "remote Hosts" gewartet.

**SYN-received**: Nachdem ein SYN Paket erhalten und ein SYN-ACK gesendet wurde wird auf das ACK gewartet, um den 3-Wege-Handschlag abzuschließen.

**ESTABLISHED**: Nach dem der Verbindungsaufbau erfolgreich abgeschlossen wurde befinden sich beide Hosts im ESTABLISHED Zustand, in dem die eine Vollduplex Kommunikation möglich ist.

**FIN-WAIT-1**: Wenn ein Verbindungsabbau initiiert wurde wird ein FIN Paket gesendet und in den Zustand FIN-WAIT-1 gewechselt und auf die Bestätigung des Erhalts gewartet.

**FIN-WAIT-2**: In dem Fall dass die Gegenstelle noch Daten zu übertragen hat, bleibt die Verbindung einseitig offen um die letzten Pakete zu empfangen.

**CLOSING**:

**TIME-WAIT**:

Zu den Zuständen kommen noch eine Reihe von Ereignissen auf, auf die, abhängig von den jeweiligen Zuständen entsprechend reagiert werden muss. Dazu gehören neben eintreffenden Paketen und Timeouts die Usercalls.

**Active OPEN**: Öffnet einen Port und initiiert den Verbindungsaufbau zu einem Remote Host.

**Passive OPEN**: Öffnet einen Port ohne eine Verbindung zu initiieren und wartet auf einen Verbindungsaufbau,

**SEND**: Fügt dem Sendepuffer Daten hinzu und sendet gegebenenfalls ein Datenpaket.

**RECEIVE**: Überprüft, ob genug Daten vorhanden sind und gibt diese an die Anwendung zurück.

**CLOSE**: Initiiert den Abbau der Verbindung, wenn es keine Daten mehr zu übertragen gibt.

**ABORT**: Bricht die Verbindung ab. In den meisten Zuständen wird in dem Fall ein Reset Paket gesendet.

---

#### 2.4.3 Sequenznummern

---

Ein wichtiges Grundprinzip von TCP dass jedes Byte an Daten eine eigene Sequenznummer zugewiesen werden kann, dadurch ist es möglich, dass jedes Byte einzeln bestätigt werden kann. Der in TCP dazu verwendete Mechanismus arbeitet kumulativ. Das bedeutet dass wenn eine Sequenznummer bestätigt wird, alle Sequenznummern kleiner als die Bestätigungsnummer als angekommen gelten. Dadurch wird es einfach den Verlust einzelner Pakete zu erkennen und die-

---

se nochmal zu senden. Das erste Byte eines Datenpaketes entspricht dabei der Sequenznummer des Pakets.

---

#### 2.4.4 Verbindungsaufbau

---

Um zuverlässig einen sicheren Verbindungsaufbau zu gewährleisten verwendet TCP einen Drei Wege Handshake. Soll eine neue Verbindung aufgebaut werden wird die Initiale Sequenznummer zuverlässig generiert. Das SYN Paket enthält nur den HEADER mit der um eins inkrementierten Initialen Sequenznummer und den SYN bit auf eins gesetzt. Nach dem Sendevorgang wird in den Zustand SYN-SENT gewechselt. Wenn die Empfängerseite sich im Zustand LISTEN befindet kann die Verbindungsanfrage bestätigt werden. Dafür wird ebenfalls eine Initiale Sequenznummer generiert. Zur Antwort wird ein Paket erzeugt, das die neue initiale Sequenznummer verwendet und als Acknummer die um eins erhöhte Sequenznummer des SYN Pakets verwendet. Die Flags für SYN und ACK werden gesetzt. Nach dem senden wird in den Zustand SYN-RECEIVED gewechselt.

Nach dem Erhalt des SYN-ACK Pakets sendet die initiiierende Seite ein leeres ACK Paket und wechselt in den ESTABLISHED Zustand.

---

#### 2.4.5 Datenübertragung

---

---

#### 2.4.6 Überlastkontrolle

---

---

#### 2.4.7 Verbindungsabbau

---

---

### 2.5 Dynamic Host Control Protocol (DHCP)

---

Mit größeren lokalen Netzwerken mit wechselnden Teilnehmer kam der bedarf nach einer Zentralen Einrichtung, die die Verteilung der IP-Adressen innerhalb eines Netzwerkes verwaltet. Dafür wurde aufbauend auf den älteren Bootstrap Protokoll DHCP entwickelt. Um dies zu realisieren wird das Optionsfeld des Bootstrap Protocols genutzt. Um ein Bootstrap Paket als DHCP Paket zu identifizieren werden die ersten 32 Bit des Optionsfeldes durch den "Magic Cookie" 99.130.83.99 belegt.

---

#### 2.5.1 Paket Format DHCP (Bootstrap)

---

Op: Gibt den generellen Typ der Nachricht an. Ein Wert von 1 signalisiert eine Anfrage, wobei eine 2 eine Antwort signalisiert.

HType: Spezifiziert die Art der dem Netzwerk zugrunde liegende Hardware. Der Code 1 steht dabei für Ethernet.

HLen: Bezeichnet die Länge der physischen Adressen im Netzwerk. Im Falle von Ethernet Netzwerken sind dies 6 Byte.

---

Hops: Wird beim Absenden auf 0 gesetzt und von jedem Relay Agentüm eins erhöht.

XID: Eine Identifikationsnummer mit der Server Antworten den Anfragen zugeordnet werden können.

Secs: Dieses Feld ist für das Bootstrap Protokoll ungenau definiert und wird oft nicht verwendet. Für DHCP wird es für die Zeit in Sekunden genutzt die vergangen ist, seit der Client damit begonnen hat nach einen neuen "Lease" zu fragen.

Flags: 8 Bits die für als Flags genutzt werden können. Das erste Bit wird gesetzt, falls die Nachricht als Broadcast gesendet wird, was den DHCP Server signalisiert, das dieser über keine gültige IP Adresse verfügt.

CIAddr: Steht für "Client IP Adresse" Der Client schreibt seine eigene IP-Adresse in dieses Feld. Im Falle von DHCP kann dieses nur in den Zuständen BOUND, RENEWING oder REBINDING genutzt werden. In allen anderen Fällen bleibt dieses Feld auf Null.

YIAddr: Abkürzung für "Your IP Address". Wird vom Server gesetzt um den Client eine IP Adresse zuzuweisen.

SIAddr: Der Server gibt hier die Adresse des Servers an, dem der Client seine nächste Anfrage schicken soll.

GIAddr: Wird nur im Bootstrap Protokoll für die Kommunikation zwischen Client und Server verwendet, wenn diese nicht im selben Netzwerk oder Subnetz liegen. Wird im DHCP nicht dafür verwendet das Standardgateway anzugeben.

CHAddr: Hardware Adresse des Clients. Bei Nutzung von Ethernet die Mac-Adresse.

SName: Der DHCP Server kann hier optional seinen Namen angeben. Alternativ kann dieses Feld durch die Option overload" Funktion auch für Optionen genutzt werden.

File: Kann genutzt werden um bei einen DHCPDISCOVER oder OFFER eine Bootdatei anzugeben.

Options: Für das Bootstrap Protokoll gibt es eine große Menge an Optionen, einige davon werden exklusiv für DHCP genutzt.

Die Anzahl und Art der verwendeten Optionen ist variabel. Der Aufbau von diesen folgt jedoch einen definierten Format. Die ersten 8 Bit eines Optionsblock enthalten den Code der Option, weitere 8 Bit geben die Länge des folgenden Datenfeldes an. Das Optionfeld beginnt im Falle von DHCP mit der "Magic Number" 99.130.83.99 nur dann können die exklusiven DHCP Optionen genutzt werden. Dazu gehören:

---

**Requested IP Address** Diese Option kann während eines dhcp Discovers gesetzt werden um die Verfügbarkeit einer bestimmten IP-Adresse anzufragen.

Code: 50; Länge: 4 Byte;

**IPAddress Lease Time** Kann in einer DHCP-Request oder DHCP-Offer Nachricht gesetzt werden. Der Client kann dabei eine bestimmte Lease Time in Sekunden angeben.

Code: 51; Länge 4 Byte;

**Option Overload** Diese option signalisiert, das Option Overload genutzt wird. Das bedeutet das weitere Optionen anstelle der Felder SNAME oder FILE geschrieben werden.

Code 52; Länge 1; Es gibt 3 mögliche Werte die geschrieben werden können.

- 1: Optionen stehen im File Feld.
- 2: Optionen stehen im SNAME Feld.
- 3: Optionen stehen in beiden Feldern.

**DHCP Message Type** dieses Feld ist bei DHCP Nachrichten immer vorhanden und gibt die Art der DHCP Nachricht an.

Code 53; Länge 1;

- 1 DHCPDISCOVER
- 2 DHCPOFFER
- 3 DHCPREQUEST
- 4 DHCPDECLINE
- 5 DHCPACK
- 6 DHCPNAK
- 7 DHCPRELEASE
- 8 DHCPINFORM

**Server Identifier** Die Option kann von einem Client bei einer DHCPREQUEST gesetzt werden, um bei Unicast Nachrichten die Adresse von einen bestimmter Server anzugeben. Ein DHCP-Server kann dieses Feld setzten, damit ein Client mehrere DHCP Offer unterscheiden kann.

Code 54; Länge 4;

**Parameter Request List** Es kann eine Liste von Parametern übergeben werden um die Werte von diesen bei einen Server anzufragen. Dazu kann eine beliebig Lange Folge aus DHCP/Bootstrap Optioncodes genutzt werden

Code 54; Länge n;

---

### 2.5.2 Ablauf

---

Zu Beginn eines DHCP-Vorgangs, wenn zum Beispiel ein Client hochgefahren wird, verfügt dieser weder über eine IP-Adresse, noch über andere Information die Netzertopologie betreffend. Als erstes sendet der Client ein Discover Paket. Dafür wird der Operationscode auf 1 gesetzt um

---

eine request Paket zu signalisieren, die MAC-Adresse wird für die Physische Client Adresse verwendet, das Broadcast-Flag wird gesetzt und der DHCP-Message-Type wird auf Discover gesetzt. Aus diesen DHCP-Paket wird ein UDP-Paket erzeugt, mit den Quellport 68 und dem Zielpport 67. Die Nachricht wird als Broadcast gesendet.

Auf diese Anfrage können einer oder mehrere DHCP Server antworten. Wenn kein bestimmter in der DISCOVER-Nachricht spezifiziert wurde, schicken alle Server in den jeweiligen Netzwerk ein OFFER". Diese Nachricht wird ebenfalls als Broadcast gesendet, da der Client noch keine eigene IP zugewiesen hat. Das OFFER enthält einen Vorschlag mit einer IP Adresse in dem Feld "Your IP Address". Anhand der "Transaction ID" und dem Feld CHADDR kann der Client die Offer eindeutig seiner Anfrage zuordnen. Der Client antwortet auf das OFFER" mit einer "REQUEST" Nachricht. Dafür wird die Option "Requested IP Address" gesetzt.

---

## 2.6 AMIDAR

---

---

## 3 Implementierung

---

### 3.1 Überblick

---

### 3.2 TCP Stack

---

### 3.3 IP Stack

---

### 3.4 DHCP

---

### 3.5 Stream Sockets

---

---

## 4 Evaluation

---

### 4.1 Testaufbau

---

### 4.2 Funktionen

---

### 4.3 Performanz

---



---

## 5 Zusammenfassung

---

### 5.1 Fazit

---

### 5.2 Ausblick

---

---

## Abkürzungsverzeichnis

---

CLB Configurable Logic Block

CPU central processing unit

ELF Executable and Linking Format

FPGA Field Programmable Gate Array

MC Microcontroller

CPU central processing unit

NCD Native Circuit Description Format

SoC System on Chip

Sph SpartanMC Hex Dateiformat

XDL Xilinx Design Language Format

---

## Abbildungsverzeichnis

---

---

## Literaturverzeichnis

---

- [BUG] *BUG Xilinx XDL Programm*. <http://forums.xilinx.com/t5/Spartan-Family-FPGAs/A-bug-for-Spartan-6/td-p/271026>
- [ELF] *Executable and linkable Format*. <http://www.linux-kernel.de/appendix/ap05.pdf>
- [GNU] *GNU - make*. <http://www.gnu.org/software/make/manual/make.html>
- [OSE] *Open Source ELF-Library*. <https://www.hpi.uni-potsdam.de/hirschfeld/trac/SqueakMaxine/browser/com.oracle.max.elf?rev=1d81ff0c9a2a8a101fe33f4ac1495decc6147517#src/com/oracle/max/elf>
- [UCS] *XDL Use Case Senarios*. [http://www.cs.indiana.edu/hmg/le/project-home/xilinx/ise\\_5.2/help/data/xdl/xdl-ucs-ext.html](http://www.cs.indiana.edu/hmg/le/project-home/xilinx/ise_5.2/help/data/xdl/xdl-ucs-ext.html)
- [XDL] *Xilinx Design Language*. [http://www.cs.indiana.edu/hmg/le/project-home/xilinx/ise\\_5.2/help/data/xdl/xdl.html](http://www.cs.indiana.edu/hmg/le/project-home/xilinx/ise_5.2/help/data/xdl/xdl.html)