

zu Aufgabe 1

IPv4 Header

No.	Time	Source	Destination	Protocol	Length	Info
451	0.744488	18.64.119.2	192.168.178.60	TCP	66	443 → 50150 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 SACK_PERM WS=512
> Frame 451: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{16891839-8155-4D1F-B382-8AD9123C73AA}, id 0 > Ethernet II, Src: AVMAudiovisu_3d:2a:ca (f0:b0:14:3d:2a:ca), Dst: ASUSTekCOMPU_6e:6b:72 (c8:7f:54:6e:6b:72) > Internet Protocol Version 4, Src: 18.64.119.2, Dst: 192.168.178.60 > 0100 = Version: 4 > 0101 = Header Length: 20 bytes (5) > > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) > 0000 00.. = Differentiated Services Codepoint: Default (0) >00 = Explicit Congestion Notification: Not ECN-Capable Transport (0) > Total Length: 52 > Identification: 0x0000 (0) > > 010. = Flags: 0x2, Don't fragment > 0... = Reserved bit: Not set > .1.. = Don't fragment: Set > ..0. = More fragments: Not set > ...0 0000 0000 0000 = Fragment Offset: 0 > Time to Live: 250 > Protocol: TCP (6) > Header Checksum: 0x849c [validation disabled] > [Header checksum status: Unverified] > Source Address: 18.64.119.2 > Destination Address: 192.168.178.60 > [Stream index: 2] > > Transmission Control Protocol, Src Port: 443, Dst Port: 50150, Seq: 0, Ack: 1, Len: 0 > Source Port: 443 > Destination Port: 50150 > [Stream index: 2] > [Stream Packet Number: 1] > [Conversation completeness: Incomplete (2)] > [TCP Segment Len: 0] > Sequence Number: 0 (relative sequence number) > Sequence Number (raw): 2129801078 > [Next Sequence Number: 1 (relative sequence number)] > Acknowledgment Number: 1 (relative ack number) > Acknowledgment number (raw): 3624477885 > 1000 = Header Length: 32 bytes (8) > > Flags: 0x012 (SYN, ACK) > Window: 65535 > [Calculated window size: 65535] > Checksum: 0x021b [unverified] > [Checksum Status: Unverified] > Urgent Pointer: 0 > > Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale > > TCP Option - Maximum segment size: 1440 bytes > > TCP Option - No-Operation (NOP) > > TCP Option - No-Operation (NOP) > > TCP Option - SACK permitted > > TCP Option - No-Operation (NOP) > > TCP Option - Window scale: 9 (multiply by 512) > > [Timestamps]						

Version	0100 (Version: 4)
Header Length	0101 (20 bytes)
Type of Service	0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length	52
Identification	0x0000 (0)
ID Flags	010. (0x2, Don't Fragment) 0... =Reserved bit: Not set .1.. =Don't fragment: set ..0. =More fragments: Not set
Fragment Offset	...0 0000 0000 0000 = Fragment Offset: 0

Time to Live	250
Protocol	TCP (6)
Header Checksum	0x849 [validation disabled]
Source Address	18.64.119.2
Destination Address	192.168.178.60

TCP Header

No.	Time	Source	Destination	Protocol	Length	Info
451	0.744488	18.64.119.2	192.168.178.60	TCP	66	443 → 50150 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 SACK_PERM WS=512


```

...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 250
Protocol: TCP (6)
Header Checksum: 0x849c [validation disabled]
[Header checksum status: Unverified]
Source Address: 18.64.119.2
Destination Address: 192.168.178.60
[Stream index: 2]
▼ Transmission Control Protocol, Src Port: 443, Dst Port: 50150, Seq: 0, Ack: 1, Len: 0
  Source Port: 443
  Destination Port: 50150
  [Stream index: 2]
  [Stream Packet Number: 1]
  > [Conversation completeness: Incomplete (2)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 2129801078
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 3624477885
  1000 .... = Header Length: 32 bytes (8)
  ▼ Flags: 0x012 (SYN, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Accurate ECN: Not set
    .... 0... = Congestion Window Reduced: Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 = Acknowledgment: Set
    .... ....0 = Push: Not set
    .... .....0 = Reset: Not set
    ▼ .... ....1 = Syn: Set
      ▼ [Expert Info (Chat/Sequence): Connection establish acknowledge (SYN+ACK): server port 443]
        [Connection establish acknowledge (SYN+ACK): server port 443]
        [Severity level: Chat]
        [Group: Sequence]
        .... ....0 = Fin: Not set
        [TCP Flags: .....A..S.]
        Window: 65535
        [Calculated window size: 65535]
        Checksum: 0x021b [unverified]
        [Checksum Status: Unverified]
        Urgent Pointer: 0
      ▼ Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
        > TCP Option - Maximum segment size: 1440 bytes
        > TCP Option - No-Operation (NOP)
        > TCP Option - No-Operation (NOP)
        > TCP Option - SACK permitted
        > TCP Option - No-Operation (NOP)
        > TCP Option - Window scale: 9 (multiply by 512)
      > [Timestamps]

```

Source Port 443
 Destination Port 65535
 Sequence Number 0 (relative sequence number)
 Acknowledgement Number 1 (relative ACK number)
 Header length 32 bytes (8) Data Offset

Reserved 000. Not set
 Cingestion Window Reduced
 0... Not set
 ECN-Echo0.. Not set
 Urgent0. Not set

Acknowledgement1 Set
Push 0... Not set
Reset0.. Not set
Syn1. Not set
Fin0 Set
Window	65535
Checksum	0x021b [unverified]
Urgent Pointer	0
Options	(12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale

```

35072 31.627210      192.168.1.142      192.168.1.255      UDP      371 50178  → 20002 Len=329

```

```

> Frame 35072: 371 bytes on wire (2968 bits), 371 bytes captured (2968 bits) on interface \Device\NPF_{16891839-8155-4D1F-B382-8AD9123C73AA}, id 0
> Ethernet II, Src: TPLink_44:f7:74 (ac:15:a2:44:f7:74), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
√ Internet Protocol Version 4, Src: 192.168.1.42, Dst: 192.168.1.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    √ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... 00.. = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 357
    Identification: 0x6a5e (27230)
    √ 010. .... = Flags: 0x2, Don't fragment
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
        ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x4ab0 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.42
    Destination Address: 192.168.1.255
    [Stream index: 2]
√ User Datagram Protocol, Src Port: 50178, Dst Port: 20002
    Source Port: 50178
    Destination Port: 20002
    Length: 337
    Checksum: 0xfa62 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 8]
    [Stream Packet Number: 1]
    > [Timestamps]
    UDP payload (329 bytes)
√ Data (329 bytes)
    [Data ...: 01f00000139110000000003480eadf81a3ceabdf7d8bc9ea486f684eb89ecce2c0a4c5b1d0f2c8b391f684eb9eeeb1d8bc9ea486be86b188bd8cb486ab93ac3f0dde9dd...
    [Length: 329]

```

Source Port	50178
Destination Port	20002
Length	337
Checksum	0xfa62 [unverified]

zu Aufgabe 2

103.161.122.83/18 ist classless inter-domain routing Notation, um die IPv4 Adresse 103.161.122.83 mit ihrer zugehörigen Netzmaske darzustellen. Dabei stellen die ersten 18 Bits der IPv4 Adresse die Netzadresse und die letzten 14 Bits die Host-Adresse dar.

Die Netzadresse erhält man, indem man alle Bits der Host-Adresse auf 0 setzt. Die Netzadresse für das Beispiel ist 103.161.64.0, d.i. in binär

01100111.10100001.01000000.00000000

Entsprechend umfasst der Hostbereich für das Beispiel die Host-Adressen 103.161.64.1 bis 103.161.127.254, d.i. in binär

01100111.10100001.01000000.00000001

bis

01100111.10100001.01111111.11111110

Die Letzte Adresse im Netzwerk ist die Broadcastadresse. Diese erhält man die alle Bits der Host-Adresse auf 1 setzt. Für das Beispiel ist das die Adresse 103.161.127.255, d.i. in binär

01100111.10100001.01111111.11111111

Die Subnetzmaske erhält man, indem man alle Bits der Netzwerkadresse auf 1 setzt. Für das Beispiel ist die Subnetzmaske somit 255.255.192.0, d.i. in binär

11111111.11111111.11000000.00000000

Die beiden Adressen 103.161.122.83/18 und 103.161.193.83/18 liegen nicht im selben Netzwerk, da 103.161.122.83/18 im Netzwerk 103.161.64.0 und 103.161.193.83/18 im Netzwerk 103.161.192.0, d.i. in binär

01100111.10100001.01000000.00000000 (103.161.64.0)

im Unterschied zu

01100111.10100001.11000000.00000000 (103.161.192.0)

zu Aufgabe 3

UDP- Probleme

- Es kam nur eine einseitige Verbindung zustande, da nur ein client die Registrierung des anderen parsen konnte
- Es kam keine Verbindung zustande, da keiner der clients die Registrierung des anderen parsen konnte
- Es konnten von einem client keine gesendeten Nachrichten empfangen werden, da die send Nachrichten nicht geparkt werden konnten
- Es traten Fragmente wie *send username* in übermittelten Nachrichten auf, da die Nachrichten vom Empfänger fehlerhaft geparkt wurden

TCP-Probleme

- Es kam keine Verbindung zum Server zustande, da der Server die Nachrichten nicht parsen konnte
- Es kam zu einem Deadlock, da Client und Server nach dem Verbindungsaufbau in einen blockierenden read übergegangen sind
- Einzelne Befehle funktionierten nicht, da diese vom Server / einem anderen Client nicht geparkt werden konnten
- Es traten Fragmente wie *send username* in übermittelten Nachrichten auf, da die Nachrichten vom Empfänger fehlerhaft geparkt wurden

Lösungsansätze

- UDP & TCP: eine einheitliche Syntax für den Aufbau der Nachrichten festlegen
- TCP: Die Kommunikation zwischen Server und Client vereinheitlichen, um zu verhindern das client und server beide in einem *blockierenden read* stecken bleiben
- UDP & TCP: die Anzahl der Annahmen, die über die Implementierung von client und server gemacht werden, reduzieren