



College of Engineering, Design and Physical Science
Electronic and Computer Engineering

Assignment Java Testing and Measuring

Distributed Computing Systems Engineering Msc

Author: Christoph Gschrey

Lab-Partner: Matthias Gebert

Date: 22. September 2017

Supervisor: Prof. Dr. Peter Väterlein

ASSIGNMENT SUBMISSION FORM

Please note: that no course work will be accepted without this cover sheet.

Please ensure: that you keep a copy of work submitted and retain your receipt in case of query.

Student Number:	SPO ID Number (Office use only):	
Course:		Level:

MODULE	
Module Code:	Module Title:
Lab / Assignment:	Deadline:
Lab group (if applicable):	Date Stamp (Office use only):
Academic Responsible:	
Administrator:	

Please note: that detailed feedback will be provided on a feedback form.

✂.....

RECEIPT SECTION (Office Copy)	
Student Number:	SPO ID Number (Office use only):
Student First Name:	Student Last Name:
Module Code:	Module Title:
Lab / Assignment:	
Lab group (if applicable):	Deadline:
Academic Responsible:	Number of Days late:

DECLARATION	
I have read and I understand the guidelines on plagiarism and cheating in the Handbook and I certify that my contribution to this report fully complies with these guidelines. I confirm that I have kept a copy of my work and that I have not lent my work to any other students.	
Signed:	Date Stamp (Office use only):

✂.....

RECEIPT SECTION (Student Copy)	
Student Number:	Student Name:
Lab / Assignment:	
Lab group (if applicable):	Module Title:
Academic Responsible:	Deadline:
Module Code:	Date Stamp (Office use only):

The University penalty system will be applied to any work submitted late.

IMPORTANT: You **MUST** keep this receipt in a safe place as you may be asked to produce it at any time as proof of submission of the assignment. Please submit this form with the assignment attached to the Department of Design Education Office in the Michael Sterling Building, room MCST 055.

Contents

1	Introduction	1
2	IP/ICMP analysis	2
2.1	Node configuration	3
2.2	Subnet internal IP Destination	4
2.2.1	a) Basic PING command	5
2.2.2	b) PING command with large data package	8
2.2.3	c) PING command with 'don't fragment' flag	11
2.3	Subnet external IP Destination	11
2.3.1	d) Basic PING command with destination in another subnet	12
2.3.2	e) PING command with reduced 'time to live'	16
2.3.3	f) PING command with timestamps	19
2.4	ARP analysis	22
2.4.1	a) Deleting the ARP cache	24
2.4.2	b) Shutting down one PC	27
2.4.3	c) Reconnect after Reboot	28
2.5	IP multicast addressing	28
3	TCP analysis	31
3.1	Traffic generator handling	32
3.2	Simple TCP Communication	32
3.2.1	Connection establishment	32
3.2.2	Data transfer	34
3.2.3	Connection release	36
3.3	TCP flow control	37
3.4	TCP transmission error recovery/abort	38
3.5	TCP protocol errors (synchronization errors)	38
4	IPv6/ICMPv6 analysis	39
4.1	Node configuration	39
4.1.1	IPv4 and IPv6 configuration	39
4.1.2	interfaces for IPv6	39
4.2	PING commands	39
4.2.1	a) Basic ICMPv6 PING command	39
4.2.2	b) ICMPv6 PING command with large data package	39

4.2.3	c) Rebooting PC	39
4.2.4	d) Enforcing Neighbor discovery	39
4.2.5	e) ICMPv6 PING command with destination in another subnet	39
4.2.6	f) PING to a remote tunnel end	39
5	Conclusion	40
	Bibliography	41

1 Introduction

The following report refers to the Computer network assignment and is structured into three parts. The first part's topic is an analysis of the network protocols ICMP and IP (both v4), while the second part covers the exercises related to TCP. The final chapter describes the exercises for the new versions of ICMP and IP (v6). These exercises were done together with my lab-partner Antonio Parotta.

2 IP/ICMP analysis

In this first part of the laboratory the program Wireshark was used to capture and analyse packages of different network protocols. The traffic was generated by PING-commands to send the observable packages from one lab PC to another. The following network protocols were analyzed:

- Internet Protocol version 4 (IPv4)
- Internet Control Message Protocol version 4 (ICMPv4)
- Address Resolution Protocol (ARP)
- Carrier Sense Multiple Access/Collision Detection (CSMA/CD)

To understand how these protocols work and to be able to explain how they behave in different situations, having a look on the protocol's headers is necessary.

The PING-commands generate packages consisting of different protocol headers and transferable data. Each Ping is transformed into an Ethernet frame containing the IP and ICMP headers. Table ?? is an representation of the basic ICMP Header while Table ?? shows the header for the echo request/reply packages that can be observed via Wireshark when executing the PING-commands.

bits	0-7	8-15	16-23	24-31
bytes	1	2	3	4
offset 0	Type	Code	Checksum	
offset 32	Data			

Table 2.1: ICMP header

bits	0-7	8-15	16-23	24-31
bytes	1	2	3	4
offset 0	Type	Code	Checksum	
offset 32	Identifier		Sequence Number	
offset 64	data			

Table 2.2: ICMP type 8 echo request/reply packet

Table ?? shows the header for the Internet Protocol v4. Noteable here are the entered destination address as well as the source address of the sender. The Time to Live is also an important

segment of the header, which will be significant later on for an specific PING-Command. IP provides the possibility to specify options for the transfered packet. This will also be used in one of the PING-Commands.

bits	0-3	4-7	8-11	12-15	16-18	19-23	24-27	28-31
bytes	1		2		3		4	
offset 0	Version	IHL	Type of Service		Total Length			
offset 32	Identification				Flags	Fragment Offset		
offset 64	Time to Live		Protocol		Header Checksum			
offset 96	Source Address							
offset 128	Destination Address							
offset 160	Options							

Table 2.3: IPv4 Header

Table ?? shows the abstract Ethernet II frame. This frame contains the MAC-addresses for source and destination, a type segment as well as the checksum for the frame. Interesting here is the Payload field. This segments contains the headers for ICMP and IP as well as the transferable data. The maximal size for this segment is 1500 bytes for one packet. But because is must contain the headers for each networking protocol (ICMP and IP), it can't be fully occupied by transferable data. This is why the Maximum Transmission Unit (MTU) is smaller. It is only 1472 bytes, because the size of the headers must be subtracted from the payload field.

$$\text{MTU} = \text{Payload} - \text{IP Header} - \text{ICMP Header}$$

$$1500 \text{ byte} - 20 \text{ byte} - 8 \text{ byte} = 1472 \text{ byte}$$

Size in bit	24		24	8	184-6000	16
Size in byte	6		6	2	46 - 1500	4
Frame segments	Destination Address		Source Address	Type	Payload (Data)	FCS

Table 2.4: Ethernet II frame

2.1 Node configuration

Figure 2.1 shows the node configuration and settings for the computer used for the exercises in this workshop:

```

Ethernet-Adapter IPv4-priv:
  Verbindungsspezifisches DNS-Suffix:
  IPv4-Adresse . . . . . : 192.168.31.6
  Subnetzmaske . . . . . : 255.255.255.0
  Standardgateway . . . . . :

Ethernet-Adapter IPv4-pub:
  Verbindungsspezifisches DNS-Suffix: rznt.rzdir.fht-esslingen.de
  Verbindungslokale IPv6-Adresse . . : fe80::6051:d005:7784:47fd%11
  IPv4-Adresse . . . . . : 134.108.8.37
  Subnetzmaske . . . . . : 255.255.252.0
  Standardgateway . . . . . : 134.108.11.254

Ethernet-Adapter VMware Network Adapter VMnet1:
  Verbindungsspezifisches DNS-Suffix:
  Verbindungslokale IPv6-Adresse . . : fe80::38b3:236d:ff8:8a19%16
  IPv4-Adresse . . . . . : 192.168.110.1
  Subnetzmaske . . . . . : 255.255.255.0
  Standardgateway . . . . . :

Ethernet-Adapter VMware Network Adapter VMnet8:
  Verbindungsspezifisches DNS-Suffix:
  Verbindungslokale IPv6-Adresse . . : fe80::811e:824c:7506:61c8%17
  IPv4-Adresse . . . . . : 192.168.71.1
  Subnetzmaske . . . . . : 255.255.255.0
  Standardgateway . . . . . :

Ethernet-Adapter VirtualBox Host-Only Network:
  Verbindungsspezifisches DNS-Suffix:
  Verbindungslokale IPv6-Adresse . . : fe80::4917:2bb5:aa97:a5fa%19
  IPv4-Adresse . . . . . : 192.168.56.1
  Subnetzmaske . . . . . : 255.255.255.0
  Standardgateway . . . . . :

Ethernet-Adapter IPv6:
  Verbindungsspezifisches DNS-Suffix:
  IPv6-Adresse . . . . . : 2001:7c0:c00:19d:3c3d:b555:99e1:2a35
  Verbindungslokale IPv6-Adresse . . : fe80::3c3d:b555:99e1:2a35%12
  Standardgateway . . . . . : fe80::2e0:29ff:fe24:f2be%12

```

Figure 2.1: Node configuration for 134.108.8.37

2.2 Subnet internal IP Destination

In the first exercise we created traffic by using the PING-Command to send packets to another PC within the same subnet. Figure 2.2 shows the simplified architecture for this environment:

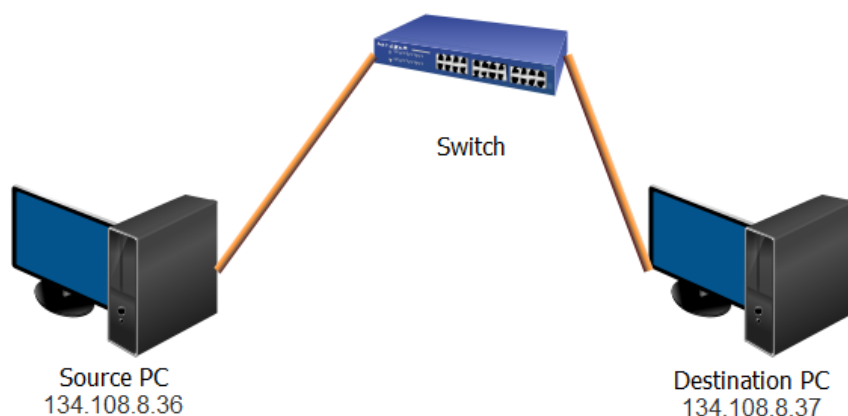


Figure 2.2: Source and Destination PC connected with a switch in the network lab

2.2.1 a) Basic PING command

The first task was sending a basic ping from one PC to another within the same subnet and capturing the sent packets using Wireshark. The PING-Command was:

```
ping -n 1 -l 64 134.108.8.37
```

Listing ?? shows the Wireshark trace for the captured packets. For this simple PING command, two ICMP packet were captured. One ICMP echo request was send from the source PC to the Destination PC and after this the Destination PC answers with an ICMP echo reqly. Both packets contain the Ethernet II frame as well as the IP and ICMP headers as discussed in chapter 2. Each packet has the source and destination address from the IP header as well as same sequence number. The total size of each packet is 106. It contains the source and target MAC-addresses from the Ethernet frame (both 6 byte), the type of the Ethernet frame (2 byte), the IP-header (20 byte), the ICMP-header (8 byte) and the transmitted data (64 byte).

No.	Time	Source	Destination	Protocol	Length	Info
445	32.125568	134.108.8.36	134.108.8.37	ICMP	106	Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (reply in 448)
Frame 445: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0						
Interface id: 0 (\Device\NPF_{55902047-E973-4FFC-B9C0-B0FAC2DA73AF})						
Interface name: \Device\NPF_{55902047-E973-4FFC-B9C0-B0FAC2DA73AF}						
Encapsulation type: Ethernet (1)						
Arrival Time: Nov 17, 2017 09:46:22.558509000 Mitteleuropäische Zeit						
[Time shift for this packet: 0.000000000 seconds]						
Epoch Time: 1510908382.558509000 seconds						
[Time delta from previous captured frame: 0.000092000 seconds]						
[Time delta from previous displayed frame: 0.000000000 seconds]						
[Time since reference or first frame: 32.125568000 seconds]						
Frame Number: 445						
Frame Length: 106 bytes (848 bits)						
Capture Length: 106 bytes (848 bits)						
[Frame is marked: True]						
[Frame is ignored: False]						
[Protocols in frame: eth:ethertype:ip:icmp:data]						
[Coloring Rule Name: ICMP]						
[Coloring Rule String: icmp icmpv6]						
Ethernet II, Src: Dell_87:b7:aa (90:b1:1c:87:b7:aa), Dst: Dell_88:97:76 (90:b1:1c:88:97:76)						
Destination: Dell_88:97:76 (90:b1:1c:88:97:76)						
Address: Dell_88:97:76 (90:b1:1c:88:97:76)						
....0. = LG bit: Globally unique address (factory default)						
....0 = IG bit: Individual address (unicast)						
Source: Dell_87:b7:aa (90:b1:1c:87:b7:aa)						

```

    Address: Dell\_87:b7:aa (90:b1:1c:87:b7:aa)
29     .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0 .... = IG bit: Individual address (unicast)
31  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 134.108.8.36, Dst: 134.108.8.37
33  0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
35  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
37  .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 92
39  Identification: 0x30fb (12539)
    Flags: 0x00
41  0... .... = Reserved bit: Not set
    .0... .... = Don't fragment: Not set
43  ..0. .... = More fragments: Not set
    Fragment offset: 0
45  Time to live: 128
    Protocol: ICMP (1)
47  Header checksum: 0xec84 [validation disabled]
    [Header checksum status: Unverified]
49  Source: 134.108.8.36
    Destination: 134.108.8.37
51  [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
53  Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
55  Code: 0
    Checksum: 0x856a [correct]
57  [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
59  Identifier (LE): 256 (0x0100)
    Sequence number (BE): 25 (0x0019)
61  Sequence number (LE): 6400 (0x1900)
    [Response frame: 448]
63  Data (64 bytes)

65  0000 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 abcdefghijklmnop
    0010 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcdefghi
67  0020 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 jklmnopqrstuvwxyzab
    0030 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 cdefghijklmnopqr
69  Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
    [Length: 64]
71
No.      Time          Source          Destination    Protocol Length Info
73  448 32.125797    134.108.8.37    134.108.8.36    ICMP      106    Echo (ping) reply id=0x0001,
    seq=25/6400, ttl=128 (request in 445)

75  Frame 448: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
    Interface id: 0 (\\Device\\NPF_{55902047-E973-4FFC-B9C0-B0FAC2DA73AF})

```

```

77      Interface name: \\Device\\NPF_{55902047-E973-4FFC-B9C0-B0FAC2DA73AF}
      Encapsulation type: Ethernet (1)
79      Arrival Time: Nov 17, 2017 09:46:22.558738000 Mitteleuropäische Zeit
      [Time shift for this packet: 0.000000000 seconds]
81      Epoch Time: 1510908382.558738000 seconds
      [Time delta from previous captured frame: 0.000005000 seconds]
83      [Time delta from previous displayed frame: 0.000229000 seconds]
      [Time since reference or first frame: 32.125797000 seconds]
85      Frame Number: 448
      Frame Length: 106 bytes (848 bits)
87      Capture Length: 106 bytes (848 bits)
      [Frame is marked: True]
89      [Frame is ignored: False]
      [Protocols in frame: eth:ethertype:ip:icmp:data]
91      [Coloring Rule Name: ICMP]
      [Coloring Rule String: icmp || icmpv6]
93      Ethernet II, Src: Dell_88:97:76 (90:b1:1c:88:97:76), Dst: Dell_87:b7:aa (90:b1:1c:87:b7:aa)
      Destination: Dell_87:b7:aa (90:b1:1c:87:b7:aa)
95          Address: Dell_87:b7:aa (90:b1:1c:87:b7:aa)
          ....0. .... = LG bit: Globally unique address (factory default)
97          ....0. .... = IG bit: Individual address (unicast)
      Source: Dell_88:97:76 (90:b1:1c:88:97:76)
99          Address: Dell_88:97:76 (90:b1:1c:88:97:76)
          ....0. .... = LG bit: Globally unique address (factory default)
101          ....0. .... = IG bit: Individual address (unicast)
      Type: IPv4 (0x0800)
103      Internet Protocol Version 4, Src: 134.108.8.37, Dst: 134.108.8.36
          0100 .... = Version: 4
105          ....0101 = Header Length: 20 bytes (5)
          Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
107          0000 00.. = Differentiated Services Codepoint: Default (0)
          ....00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
109      Total Length: 92
          Identification: 0x3021 (12321)
111      Flags: 0x00
          0... .... = Reserved bit: Not set
113          .0.. .... = Don't fragment: Not set
          ..0. .... = More fragments: Not set
115      Fragment offset: 0
          Time to live: 128
117      Protocol: ICMP (1)
          Header checksum: 0x0000 [validation disabled]
119          [Header checksum status: Unverified]
          Source: 134.108.8.37
121          Destination: 134.108.8.36
          [Source GeoIP: Unknown]
123          [Destination GeoIP: Unknown]
      Internet Control Message Protocol
125      Type: 0 (Echo (ping) reply)
          Code: 0

```

```

127    Checksum: 0x8d6a [correct]
      [Checksum Status: Good]
129    Identifier (BE): 1 (0x0001)
      Identifier (LE): 256 (0x0100)
131    Sequence number (BE): 25 (0x0019)
      Sequence number (LE): 6400 (0x1900)
133    [Request frame: 445]
      [Response time: 0.229 ms]
135    Data (64 bytes)

137 0000 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 abcdefghijklmnop
0010 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcdefghi
139 0020 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 jklmnopqrstuvwxyz
0030 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 cdefghijklmnopqr
141    Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
      [Length: 64]

```

Listing 2.1: Wireshark trace for simple PING command

2.2.2 b) PING command with large data package

For the second exercise we had to execute a PING-Command with a very large data package of 2000 byte. The PING-Command was:

```
ping -n 1 -l 2000 134.108.8.36
```

Figure 2.3 shows the console output for this ping:

```

C:\Users\rn-labor>ping -n 1 -l 2000 134.108.8.36
Ping wird ausgeführt für 134.108.8.36 mit 2000 Bytes Daten:
Antwort von 134.108.8.36: Bytes=2000 Zeit<1ms TTL=128

Ping-Statistik für 134.108.8.36:
    Pakete: Gesendet = 1, Empfangen = 1, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms

```

Figure 2.3: Console output for PING-Command with 2000 bytes data

It seems that the protocol ICMP does not have any problems with this as the console output shows no warning. IP however does have a problem with this large packet size. As the data exceeds the Maximum Transmission Unit, the packet must be fragmented and separated into two packets. The following listing is shortened, but shows the four packages sent between both lab-PCs:

,

No.	Time	Source	Destination	Protocol	Length	DestPort	Info
				Delta Time			
2	236 0.000000	134.108.8.37	134.108.8.36	ICMP	1514		Echo (ping) request id=0 x0001, seq=25/6400, ttl=128 (reply in 240) 0.000000
4	Frame 236: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0						
	Interface id: 0 (\\Device\\NPF_{55902047-E973-4FFC-B9C0-BOFAC2DA73AF})						
6	Interface name: \\Device\\NPF_{55902047-E973-4FFC-B9C0-BOFAC2DA73AF}						
	Encapsulation type: Ethernet (1)						
8	Arrival Time: Nov 17, 2017 09:58:38.374317000 Mitteleuropäische Zeit						
	[Time shift for this packet: 0.000000000 seconds]						
10	Epoch Time: 1510909118.374317000 seconds						
	[Time delta from previous captured frame: 0.000024000 seconds]						
12	[Time delta from previous displayed frame: 0.000000000 seconds]						
	[Time since reference or first frame: 36.388239000 seconds]						
14	Frame Number: 236						
	Frame Length: 1514 bytes (12112 bits)						
16	Capture Length: 1514 bytes (12112 bits)						
	[Frame is marked: True]						
18	[Frame is ignored: False]						
	[Protocols in frame: eth:ethertype:ip:icmp:data]						
20	[Coloring Rule Name: ICMP]						
	[Coloring Rule String: icmp icmpv6]						
22	Ethernet II, Src: 90:b1:1c:88:97:76, Dst: 90:b1:1c:87:b7:aa						
	Destination: 90:b1:1c:87:b7:aa						
24	Address: 90:b1:1c:87:b7:aa						
0. = LG bit: Globally unique address (factory default)						
260 = IG bit: Individual address (unicast)						
	Source: 90:b1:1c:88:97:76						
28	Address: 90:b1:1c:88:97:76						
0. = LG bit: Globally unique address (factory default)						
300 = IG bit: Individual address (unicast)						
	Type: IPv4 (0x0800)						
32	Internet Protocol Version 4, Src: 134.108.8.37, Dst: 134.108.8.36						
	0100 = Version: 4						
34 0101 = Header Length: 20 bytes (5)						
	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
36	0000 00.. = Differentiated Services Codepoint: Default (0)						
00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)						
38	Total Length: 1500						
	Identification: 0x3e7e (15998)						
40	Flags: 0x01 (More Fragments)						
	0... = Reserved bit: Not set						
42	.0.. = Don't fragment: Not set						
	..1. = More fragments: Set						
44	Fragment offset: 0						
	Time to live: 128						
46	Protocol: ICMP (1)						
	Header checksum: 0x0000 [validation disabled]						

```

48 [Header checksum status: Unverified]
Source: 134.108.8.37
50 Destination: 134.108.8.36
[Source GeoIP: Unknown]
52 [Destination GeoIP: Unknown]
Internet Control Message Protocol
54 Type: 8 (Echo (ping) request)
Code: 0
56 Checksum: 0x7b5e [unverified] [fragmented datagram]
[Checksum Status: Unverified]
58 Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
60 Sequence number (BE): 25 (0x0019)
Sequence number (LE): 6400 (0x1900)
62 [Response frame: 240]
Data (1472 bytes)
64
No.      Time      Source      Destination      Protocol Length DestPort Info
Delta Time
66 237 0.000007 134.108.8.37 134.108.8.36 IPv4 562 Fragmented IP protocol (
proto=ICMP 1, off=1480, ID=3e7e) 0.000007

68 No.      Time      Source      Destination      Protocol Length DestPort Info
Delta Time
240 0.000488 134.108.8.36 134.108.8.37 ICMP 1514 Echo (ping) reply id=0
x0001, seq=25/6400, ttl=128 (request in 236) 0.000488
70
No.      Time      Source      Destination      Protocol Length DestPort Info
Delta Time
72 241 0.000002 134.108.8.36 134.108.8.37 IPv4 562 Fragmented IP protocol (
proto=ICMP 1, off=1480, ID=332d) 0.000002

```

Listing 2.2: Wireshark trace for PING command with 2000 bytes data

It can be observed that the first packet occupies all 1514 bytes that can be sent in one ICMP packet. Subtracting the segments from the Ethernet frame (14 byte), the IP-header (20 byte) and the ICMP-header (8 byte), there is room for 1472 byte of raw data. The remaining 528 byte of data can't be transmitted in the same packet. So the data must be fragmented and sent inside another packet. As ICMP doesn't play a role in the fragmentation, it's header isn't needed anymore in the second packet. However the second packet contains the IP-header (20 byte) as it is the protocol that manages the fragmentation and transmission controlling. The segments for the Ethernet frame (14 byte) are also included, because without that there could not be any transmission at all. So summed up the second packet has a size of 562 byte.

2.2.3 c) PING command with 'don't fragment' flag

For this last exercise another PING with 2000 byte of data was executed. But this time the 'don't fragment' flag **-f** was set:

```
ping -n 1 -l 2000 134.108.8.36 -f
```

This causes a problem, because as discussed in the previous chapter this large amount of data cannot be transmitted in one single packet. So IP needs to fragment it into two separate packets. But in this case it receives the 'don't fragment' command. This contradicts the functionality of IP and it throws an error that ICMP recognizes and displays a message in the console:

```
C:\Users\rn-labor>ping -n 1 -l 2000 134.108.8.36 -f
Ping wird ausgeführt für 134.108.8.36 mit 2000 Bytes Daten:
Paket müsste fragmentiert werden, DF-Flag ist jedoch gesetzt.
Ping-Statistik für 134.108.8.36:
    Pakete: Gesendet = 1, Empfangen = 0, Verloren = 1
    (100% Verlust),
```

Figure 2.4: Console output for PING-Command with 2000 bytes data

There is no Wireshark trace for this exercise, because there were no packets sent to the destination PC.

2.3 Subnet external IP Destination

For this second part of the laboratory, we moved on to PING-commands where the destination address was located in another subnet. Both subnets were connected by a router that assigned a range of addresses to the computers inside each subnet. Each computer inside one of these subnets was connected to a switch that had a connection to the router and the router provided a host IP-address for both subnets. Figure 2.5 shows all involved network node and their IP-addresses.

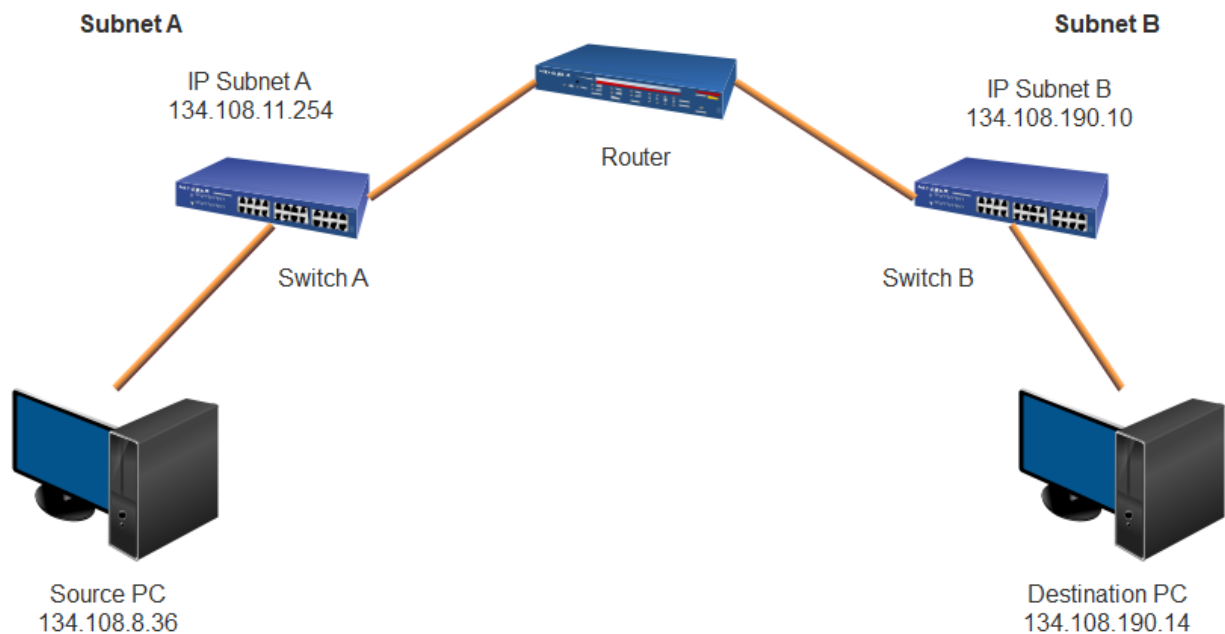


Figure 2.5: Two subnets in the network lab

2.3.1 d) Basic PING command with destination in another subnet

For this exercise the following PING-Command was used:

```
ping -n 1 -i 2 -r 4 134.108.190.10
```

The parameter **-r** activates the recoding of the route and sets the maximal number of records. **-i** indicates the 'Time to Live' in the IP-header (s. Chapter 2) and is basically nothing more than a hop-count that decrements, when the packet passes a network node (PCs or Routers in this case). When 'Time to Live' reaches zero, the packet will be abandoned. Figure 2.6 shows the output of the console command:

```
C:\Users\rn-labor>ping -n 1 -i 2 -r 4 134.108.190.10
Ping wird ausgeführt für 134.108.190.10 mit 32 Bytes Daten:
Antwort von 134.108.190.10: Bytes=32 Zeit<1ms TTL=63
Route: 134.108.190.14 ->
        134.108.190.10 ->
        134.108.190.10 ->
        134.108.11.254
Ping-Statistik für 134.108.190.10:
Pakete: Gesendet = 1, Empfangen = 1, Verloren = 0
        (0% Verlust),
Ca. Zeitangaben in Millisek.:
        Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
```

Figure 2.6: PING Command with Destination in another subnet

The output shows the recorded route, the reply packet from the destination PC took through the network. The sent packets are shown in the following listing:

No.	Time	Source	Destination	Protocol	Length	DestPort	Info
				Delta Time			
2	49 0.000000	134.108.8.37	134.108.190.10	ICMP	94		Echo (ping) request id=0 x0001, seq=37/9472, ttl=2 (reply in 50) 0.000000
4	Frame 49: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0						
	Interface id: 0 (\\Device\\NPF_{55902047-E973-4FFC-B9C0-B0FAC2DA73AF})						
6	Interface name: \\Device\\NPF_{55902047-E973-4FFC-B9C0-B0FAC2DA73AF}						
	Encapsulation type: Ethernet (1)						
8	Arrival Time: Nov 17, 2017 10:21:22.503562000 Mitteleuropäische Zeit						
	[Time shift for this packet: 0.000000000 seconds]						
10	Epoch Time: 1510910482.503562000 seconds						
	[Time delta from previous captured frame: 0.187068000 seconds]						
12	[Time delta from previous displayed frame: 0.000000000 seconds]						
	[Time since reference or first frame: 2.480985000 seconds]						
14	Frame Number: 49						
	Frame Length: 94 bytes (752 bits)						
16	Capture Length: 94 bytes (752 bits)						
	[Frame is marked: True]						
18	[Frame is ignored: False]						
	[Protocols in frame: eth:ethertype:ip:icmp:data]						
20	[Coloring Rule Name: ICMP]						
	[Coloring Rule String: icmp icmpv6]						
22	Ethernet II, Src: 90:b1:1c:88:97:76, Dst: 00:23:04:52:1c:00						
	Destination: 00:23:04:52:1c:00						
24	Address: 00:23:04:52:1c:00						
 0. = LG bit: Globally unique address (factory default)						
26 0 = IG bit: Individual address (unicast)						
	Source: 90:b1:1c:88:97:76						
28	Address: 90:b1:1c:88:97:76						
 0. = LG bit: Globally unique address (factory default)						
30 0 = IG bit: Individual address (unicast)						
	Type: IPv4 (0x0800)						
32	Internet Protocol Version 4, Src: 134.108.8.37, Dst: 134.108.190.10						
	0100 = Version: 4						
34 1010 = Header Length: 40 bytes (10)						
	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
36	0000 00.. = Differentiated Services Codepoint: Default (0)						
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)						
38	Total Length: 80						
	Identification: 0x42d5 (17109)						
40	Flags: 0x00						
	0... = Reserved bit: Not set						
42	.0.. = Don't fragment: Not set						
	..0. = More fragments: Not set						
44	Fragment offset: 0						

```

Time to live: 2
46 [Expert Info (Note/Sequence): "Time To Live" only 2]
    ["Time To Live" only 2]
48 [Severity level: Note]
    [Group: Sequence]
50 Protocol: ICMP (1)
    Header checksum: 0x0000 [validation disabled]
52 [Header checksum status: Unverified]
    Source: 134.108.8.37
54 Destination: 134.108.190.10
    [Source GeoIP: Unknown]
56 [Destination GeoIP: Unknown]
    Options: (20 bytes), Record Route
58     IP Option - Record Route (19 bytes)
        Type: 7
60         0... .... = Copy on fragmentation: No
            .00. .... = Class: Control (0)
62         ...0 0111 = Number: Record route (7)
            Length: 19
64             Pointer: 4
                Empty Route: 0.0.0.0 <- (next)
66                 Empty Route: 0.0.0.0
                    Empty Route: 0.0.0.0
68                     Empty Route: 0.0.0.0
        IP Option - End of Options List (EOL)
70         Type: 0
            0... .... = Copy on fragmentation: No
72             .00. .... = Class: Control (0)
                ...0 0000 = Number: End of Option List (EOL) (0)
74 Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
76    Code: 0
    Checksum: 0x4d36 [correct]
78    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
80    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 37 (0x0025)
82    Sequence number (LE): 9472 (0x2500)
    [Response frame: 50]
84    Data (32 bytes)

86    0000 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 abcdefghijklmnop
    0010 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcdefghi
88    Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
    Text: abcdefghijklmnopqrstuvwxyzabcdefghi
90    [Length: 32]

92 No.      Time      Source      Destination      Protocol Length DestPort Info
                                Delta Time

```

```

50 0.000692 134.108.190.10 134.108.8.37 ICMP 94 Echo (ping) reply id=0
    x0001, seq=37/9472, ttl=63 (request in 49) 0.000692
94
Frame 50: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
96   Interface id: 0 (\\Device\\NPF_{55902047-E973-4FFC-B9C0-B0FAC2DA73AF})
    Interface name: \\Device\\NPF_{55902047-E973-4FFC-B9C0-B0FAC2DA73AF}
98   Encapsulation type: Ethernet (1)
    Arrival Time: Nov 17, 2017 10:21:22.504254000 Mitteleuropäische Zeit
100   [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1510910482.504254000 seconds
102   [Time delta from previous captured frame: 0.000692000 seconds]
    [Time delta from previous displayed frame: 0.000692000 seconds]
104   [Time since reference or first frame: 2.481677000 seconds]
    Frame Number: 50
106   Frame Length: 94 bytes (752 bits)
    Capture Length: 94 bytes (752 bits)
108   [Frame is marked: True]
    [Frame is ignored: False]
110   [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
112   [Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: 00:23:04:52:1c:00, Dst: 90:b1:1c:88:97:76
114   Destination: 90:b1:1c:88:97:76
    Address: 90:b1:1c:88:97:76
116   .... 0. .... = LG bit: Globally unique address (factory default)
    .... 0. .... = IG bit: Individual address (unicast)
118   Source: 00:23:04:52:1c:00
    Address: 00:23:04:52:1c:00
120   .... 0. .... = LG bit: Globally unique address (factory default)
    .... 0. .... = IG bit: Individual address (unicast)
122   Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 134.108.190.10, Dst: 134.108.8.37
124   0100 .... = Version: 4
    .... 1010 = Header Length: 40 bytes (10)
126   Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
128   .... 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 80
130   Identification: 0x048f (1167)
    Flags: 0x00
132   0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
134   ..0. .... = More fragments: Not set
    Fragment offset: 0
136   Time to live: 63
    Protocol: ICMP (1)
138   Header checksum: 0xafa3 [validation disabled]
    [Header checksum status: Unverified]
140   Source: 134.108.190.10
    Destination: 134.108.8.37

```

```

142 [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
144 Options: (20 bytes), Record Route
    IP Option - Record Route (19 bytes)
146     Type: 7
    0... .... = Copy on fragmentation: No
148     .00. .... = Class: Control (0)
    ...0 0111 = Number: Record route (7)
150     Length: 19
    Pointer: 20
152     Recorded Route: 134.108.190.14
    Recorded Route: 134.108.190.10
154     Recorded Route: 134.108.190.10
    Recorded Route: 134.108.11.254
156     IP Option - End of Options List (EOL)
    Type: 0
158     0... .... = Copy on fragmentation: No
    .00. .... = Class: Control (0)
160     ...0 0000 = Number: End of Option List (EOL) (0)
Internet Control Message Protocol
162     Type: 0 (Echo (ping) reply)
    Code: 0
164     Checksum: 0x5536 [correct]
    [Checksum Status: Good]
166     Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
168     Sequence number (BE): 37 (0x0025)
    Sequence number (LE): 9472 (0x2500)
170     [Request frame: 49]
    [Response time: 0.692 ms]
172     Data (32 bytes)

174 0000 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 abcdefghijklmnop
    0010 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcdefghi
176 Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
    Text: abcdefghijklmnopqrstuvwxyzabcdefghi
178 [Length: 32]

```

Listing 2.3: Wireshark trace for PING command in another subnet

2.3.2 e) PING command with reduced 'time to live'

In this exercise the 'Time to Live' was reduced to 1 in the PING-Command:

```
ping -n 1 -i 1 -r 4 134.108.190.10
```

This causes a Time-To-Live-Exceeded error that was displayed in the console output:

```
C:\Users\rn-labor>ping -n 1 -i 1 -r 4 134.108.190.10

Ping wird ausgeführt für 134.108.190.10 mit 32 Bytes Daten:
Antwort von 134.108.11.254: Die Gültigkeitsdauer wurde bei der Übertragung überschritten.

Ping-Statistik für 134.108.190.10:
    Pakete: Gesendet = 1, Empfangen = 1, Verloren = 0
    (0% Verlust),
```

Figure 2.7: PING Command with reduced Time to Live

As the 'Time to Live' is reduced to 1, it cannot reach the destination PC. When bypassing the router, the TTL is decreased to zero. So the router will drop the packet and send the Time-To-Live-Exceeded error back to the source, while the destination PC never receives any traffic. The only packet sent is from the source to the router. This can be seen in the following Wireshark trace:

No.	Time	Source	Destination	Protocol	Length	DestPort	Info
				Delta Time			
2	37 0.000000	134.108.8.37	134.108.190.10	ICMP	94		Echo (ping) request id=0 x0001, seq=38/9728, ttl=1 (no response found!) 0.000000
4	Frame 37: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0						
	Interface id: 0 (\\Device\\NPF_{55902047-E973-4FFC-B9C0-B0FAC2DA73AF})						
6	Interface name: \\Device\\NPF_{55902047-E973-4FFC-B9C0-B0FAC2DA73AF}						
	Encapsulation type: Ethernet (1)						
8	Arrival Time: Nov 17, 2017 10:23:18.619066000 Mitteleuropäische Zeit						
	[Time shift for this packet: 0.000000000 seconds]						
10	Epoch Time: 1510910598.619066000 seconds						
	[Time delta from previous captured frame: 0.145036000 seconds]						
12	[Time delta from previous displayed frame: 0.000000000 seconds]						
	[Time since reference or first frame: 5.672194000 seconds]						
14	Frame Number: 37						
	Frame Length: 94 bytes (752 bits)						
16	Capture Length: 94 bytes (752 bits)						
	[Frame is marked: True]						
18	[Frame is ignored: False]						
	[Protocols in frame: eth:ethertype:ip:icmp:data]						
20	[Coloring Rule Name: ICMP]						
	[Coloring Rule String: icmp icmpv6]						
22	Ethernet II, Src: 90:b1:1c:88:97:76, Dst: 00:23:04:52:1c:00						
	Destination: 00:23:04:52:1c:00						
24	Address: 00:23:04:52:1c:00						
 0. = LG bit: Globally unique address (factory default)						
26 0 = IG bit: Individual address (unicast)						
	Source: 90:b1:1c:88:97:76						
28	Address: 90:b1:1c:88:97:76						
 0. = LG bit: Globally unique address (factory default)						

```

30      .... ..0 .... .. = IG bit: Individual address (unicast)
      Type: IPv4 (0x0800)
32 Internet Protocol Version 4, Src: 134.108.8.37, Dst: 134.108.190.10
      0100 .... = Version: 4
34      .... 1010 = Header Length: 40 bytes (10)
      Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
36      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
38      Total Length: 80
      Identification: 0x42d9 (17113)
40      Flags: 0x00
      0... .... = Reserved bit: Not set
42      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
44      Fragment offset: 0
      Time to live: 1
46      [Expert Info (Note/Sequence): "Time To Live" only 1]
      ["Time To Live" only 1]
48      [Severity level: Note]
      [Group: Sequence]
50      Protocol: ICMP (1)
      Header checksum: 0x0000 [validation disabled]
52      [Header checksum status: Unverified]
      Source: 134.108.8.37
54      Destination: 134.108.190.10
      [Source GeoIP: Unknown]
56      [Destination GeoIP: Unknown]
      Options: (20 bytes), Record Route
58      IP Option - Record Route (19 bytes)
          Type: 7
60          0... .... = Copy on fragmentation: No
          .00. .... = Class: Control (0)
62          ...0 0111 = Number: Record route (7)
          Length: 19
64          Pointer: 4
              Empty Route: 0.0.0.0 <- (next)
66              Empty Route: 0.0.0.0
              Empty Route: 0.0.0.0
68              Empty Route: 0.0.0.0
      IP Option - End of Options List (EOL)
70      Type: 0
          0... .... = Copy on fragmentation: No
72          .00. .... = Class: Control (0)
          ...0 0000 = Number: End of Option List (EOL) (0)
74 Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
76      Code: 0
      Checksum: 0x4d35 [correct]
78      [Checksum Status: Good]
      Identifier (BE): 1 (0x0001)

```

```

80 Identifier (LE): 256 (0x0100)
Sequence number (BE): 38 (0x0026)
82 Sequence number (LE): 9728 (0x2600)
[No response seen]
84 [Expert Info (Warning/Sequence): No response seen to ICMP request]
[No response seen to ICMP request]
86 [Severity level: Warning]
[Group: Sequence]
88 Data (32 bytes)

90 0000 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 abcdefghijklmnop
0010 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcdefghi
92 Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
Text: abcdefghijklmnopqrstuvwxyzabcdefghi
94 [Length: 32]

```

Listing 2.4: Wireshark trace for PING command with reduced TTL

2.3.3 f) PING command with timestamps

In this exercise the 'timestamp' option was used in the PING-Command:

```
ping -n 1 -i 2 -s 4 134.108.190.10
```

The timestamp option has the effect that a timestamp which represents the amount of time from midnight to the exact moment, the packet bypasses a network node, is recorded in milliseconds:

```

C:\Users\rn-labor>ping -n 1 -i 2 -s 4 134.108.190.10

Ping wird ausgeführt für 134.108.190.10 mit 32 Bytes Daten:
Antwort von 134.108.190.10: Bytes=32 Zeit<1ms TTL=63
    Zeitstempel: 134.108.190.14 : 34336822 ->
                  134.108.190.10 : 34336823 ->
                  134.108.190.10 : 34336823 ->
                  134.108.11.254 : 34336823

Ping-Statistik für 134.108.190.10:
    Pakete: Gesendet = 1, Empfangen = 1, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms

```

Figure 2.8: PING Command with timestamp option

The time difference between the sending from the destination PC and the bypassing of the router is only 1 ms as seen in Figure 2.8. The Options Field in the IP-header contains the timestamps as seen in the following listing: ,

```

2 No.      Time      Source      Destination      Protocol Length DestPort Info
                                     Delta Time
51 0.000778 134.108.190.10 134.108.8.37    ICMP      110          Echo (ping) reply id=0
    x0001, seq=43/11008, ttl=63 (request in 50) 0.000778
4
6 Frame 51: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
   Interface id: 0 (\\Device\\NPF_{55902047-E973-4FFC-B9C0-B0FAC2DA73AF})
   Interface name: \\Device\\NPF_{55902047-E973-4FFC-B9C0-B0FAC2DA73AF}
8   Encapsulation type: Ethernet (1)
   Arrival Time: Nov 17, 2017 10:32:16.698574000 Mitteleuropäische Zeit
10  [Time shift for this packet: 0.000000000 seconds]
   Epoch Time: 1510911136.698574000 seconds
12  [Time delta from previous captured frame: 0.000778000 seconds]
   [Time delta from previous displayed frame: 0.000778000 seconds]
14  [Time since reference or first frame: 3.015108000 seconds]
   Frame Number: 51
16  Frame Length: 110 bytes (880 bits)
   Capture Length: 110 bytes (880 bits)
18  [Frame is marked: True]
   [Frame is ignored: False]
20  [Protocols in frame: eth:ethertype:ip:icmp:data]
   [Coloring Rule Name: ICMP]
22  [Coloring Rule String: icmp || icmpv6]
   Ethernet II, Src: 00:23:04:52:1c:00, Dst: 90:b1:1c:88:97:76
24  Destination: 90:b1:1c:88:97:76
   Address: 90:b1:1c:88:97:76
26  .... ..0. .... = LG bit: Globally unique address (factory default)
   .... ..0. .... = IG bit: Individual address (unicast)
28  Source: 00:23:04:52:1c:00
   Address: 00:23:04:52:1c:00
30  .... ..0. .... = LG bit: Globally unique address (factory default)
   .... ..0. .... = IG bit: Individual address (unicast)
32  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 134.108.190.10, Dst: 134.108.8.37
34  0100 .... = Version: 4
   .... 1110 = Header Length: 56 bytes (14)
36  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   0000 00.. = Differentiated Services Codepoint: Default (0)
38  .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
   Total Length: 96
40  Identification: 0x0490 (1168)
   Flags: 0x00
42  0... .... = Reserved bit: Not set
   .0.. .... = Don't fragment: Not set
44  ..0. .... = More fragments: Not set
   Fragment offset: 0
46  Time to live: 63
   Protocol: ICMP (1)

```



```

48   Header checksum: 0x0901 [validation disabled]
    [Header checksum status: Unverified]
50   Source: 134.108.190.10
    Destination: 134.108.8.37
52   [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
54   Options: (36 bytes), Time Stamp
    IP Option - Time Stamp (36 bytes)
56     Type: 68
        0... .... = Copy on fragmentation: No
58     .10. .... = Class: Debugging and measurement (2)
        ...0 0100 = Number: Time stamp (4)
60     Length: 36
        Pointer: 37
62     0000 .... = Overflow: 0
        .... 0001 = Flag: Time stamp and address (0x1)
64     Address: 134.108.190.14
        Time stamp: 34336822
66     Address: 134.108.190.10
        Time stamp: 34336823
68     Address: 134.108.190.10
        Time stamp: 34336823
70     Address: 134.108.11.254
        Time stamp: 34336823
72 Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
74    Code: 0
    Checksum: 0x5530 [correct]
76    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
78    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 43 (0x002b)
80    Sequence number (LE): 11008 (0x2b00)
    [Request frame: 50]
82    [Response time: 0.778 ms]
Data (32 bytes)
84
    0000 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 abcdefghijklmnop
86    0010 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcdefghi
    Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
88    Text: abcdefghijklmnopqrstuvwxyzabcdefghi
    [Length: 32]

```

Listing 2.5: Wireshark trace for PING command with timestamps

2.4 ARP analysis

In the following exercises the Address Resolution Protocol was analyzed to achieve a better understanding how IP-Addresses are mapped to actual Hardware MAC-Addresses. ARP does exactly this by putting both address in relation together into a cache, also called the ARP table. Table ?? shows the header for ARP:

bits	0-7	8-15	16-23	24-31
bytes	1	2	3	4
Offset 0	Hardware-Addresstype (HTYPE)		Network Protocol Type (PTYPE)	
Offset 32	Hardware Address Length (HLEN)	Protocol Address Length (PLEN)	Operation	
Offset 64	Sender MAC-Address			
Offset 128	Sender MAC-Address		Sender IP Address	
Offset 160	Sender IP Address		Target MAC-Address	
Offset 192	Target MAC-Address			
Offset 224	Target IP-Address			

Table 2.5: Address Resolution Protocol Header

The following Figure 2.9 shows the ARP table obtained by typing 'arp -a' into the console from one of the network lab PCs before it was deleted for the next exercise:

```

C:\Users\rn-labor>arp -a

Schnittstelle: 134.108.8.37 --- 0xb
Internetadresse    Physische Adresse    Typ
134.108.8.4        b4-b5-2f-ac-d2-ed    dynamisch
134.108.8.22       90-1b-0e-66-4f-a2    dynamisch
134.108.8.32       90-b1-1c-88-98-19    dynamisch
134.108.8.34       90-b1-1c-88-99-f0    dynamisch
134.108.8.35       90-b1-1c-87-ad-47    dynamisch
134.108.8.36       90-b1-1c-87-b7-aa    dynamisch
134.108.8.48       90-b1-1c-87-b6-b9    dynamisch
134.108.8.49       90-b1-1c-88-98-75    dynamisch
134.108.8.51       90-b1-1c-87-b8-1f    dynamisch
134.108.8.168      74-46-a0-a9-e8-52    dynamisch
134.108.8.176      d8-ch-8a-7c-0a-07    dynamisch
134.108.8.177      d8-ch-8a-7c-0a-14    dynamisch
134.108.8.178      d8-ch-8a-7c-0a-78    dynamisch
134.108.8.179      d8-ch-8a-7c-09-70    dynamisch
134.108.8.180      d8-ch-8a-7c-08-cb    dynamisch
134.108.8.181      d8-ch-8a-7c-09-b6    dynamisch
134.108.8.182      d8-ch-8a-7b-fe-bf    dynamisch
134.108.8.183      d8-ch-8a-7b-ff-15    dynamisch
134.108.8.184      d8-ch-8a-7c-0a-32    dynamisch
134.108.8.185      d8-ch-8a-7c-09-61    dynamisch
134.108.8.186      d8-ch-8a-7c-09-74    dynamisch
134.108.8.187      d8-ch-8a-7c-0a-b9    dynamisch
134.108.8.188      d8-ch-8a-7c-09-7e    dynamisch
134.108.8.190      d8-ch-8a-7c-09-34    dynamisch
134.108.8.191      d8-ch-8a-7c-09-e0    dynamisch
134.108.8.213      18-03-73-3b-3e-76    dynamisch
134.108.10.227     50-26-90-17-c9-a4    dynamisch
134.108.11.254     00-23-04-52-1c-00    dynamisch
224.0.0.22         01-00-5e-00-00-16    statisch
224.0.0.251        01-00-5e-00-00-fb    statisch
224.0.0.252        01-00-5e-00-00-fc    statisch
230.0.0.1          01-00-5e-00-00-01    statisch
239.255.255.250    01-00-5e-7f-ff-fa    statisch
255.255.255.255    ff-ff-ff-ff-ff-ff    statisch

Schnittstelle: 192.168.31.6 --- 0xd
Internetadresse    Physische Adresse    Typ
224.0.0.22         01-00-5e-00-00-16    statisch
224.0.0.251        01-00-5e-00-00-fb    statisch
224.0.0.252        01-00-5e-00-00-fc    statisch
230.0.0.1          01-00-5e-00-00-01    statisch
239.255.255.250    01-00-5e-7f-ff-fa    statisch

Schnittstelle: 192.168.110.1 --- 0x10
Internetadresse    Physische Adresse    Typ
192.168.110.255    ff-ff-ff-ff-ff-ff    statisch
224.0.0.22         01-00-5e-00-00-16    statisch
224.0.0.251        01-00-5e-00-00-fb    statisch
224.0.0.252        01-00-5e-00-00-fc    statisch
230.0.0.1          01-00-5e-00-00-01    statisch
239.255.255.250    01-00-5e-7f-ff-fa    statisch

Schnittstelle: 192.168.71.1 --- 0x11
Internetadresse    Physische Adresse    Typ
192.168.71.255     ff-ff-ff-ff-ff-ff    statisch
224.0.0.22         01-00-5e-00-00-16    statisch
224.0.0.251        01-00-5e-00-00-fb    statisch
224.0.0.252        01-00-5e-00-00-fc    statisch
230.0.0.1          01-00-5e-00-00-01    statisch
239.255.255.250    01-00-5e-7f-ff-fa    statisch

Schnittstelle: 192.168.56.1 --- 0x13
Internetadresse    Physische Adresse    Typ
192.168.56.255     ff-ff-ff-ff-ff-ff    statisch
224.0.0.22         01-00-5e-00-00-16    statisch
224.0.0.251        01-00-5e-00-00-fb    statisch
224.0.0.252        01-00-5e-00-00-fc    statisch
230.0.0.1          01-00-5e-00-00-01    statisch
239.255.255.250    01-00-5e-7f-ff-fa    statisch

```

Figure 2.9: ARP table

2.4.1 a) Deleting the ARP cache

Now the ARP table on the source PC (134.108.8.37) was deleted using the console command 'arp -d'. After executing this, the ARP table was empty. After that another PING-Command was executed:

```
ping -n 2 134.108.8.36
```

The following figure shows the output of this Ping:

```
C:\Users\rn-labor>ping -n 2 134.108.8.36

Ping wird ausgeführt für 134.108.8.36 mit 32 Bytes Daten:
Antwort von 134.108.8.36: Bytes=32 Zeit<1ms TTL=128
Antwort von 134.108.8.36: Bytes=32 Zeit<1ms TTL=128

Ping-Statistik für 134.108.8.36:
    Pakete: Gesendet = 2, Empfangen = 2, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
```

Figure 2.10: PING Command Output after ARP table was deleted

Because the ARP table is now empty, IP has the problem that the target IP-Address cannot be resolved. This leads to the ARP request packet sent from the Source PC into the network via Broadcast as seen in Listing ?? asking who has the required Target IP Address. The PC inside the same subnet who owns this IP Address now answers with an ARP reply packet containing it's MAC-Address. Following this the source PC inserts a new mapping with the target PC's IP- and MAC-Address into it's ARP table. After that the two PINGs are executed as seen in the following Wireshark trace:

No.	Time	Source	Destination	Protocol	Length	DestPort	Info
					Delta Time		
2	162 0.459379	90:b1:1c:88:97:76	ff:ff:ff:ff:ff:ff	ARP	42		Who has 134.108.8.36?
		Tell 134.108.8.37	0.459379				
4	Frame 162: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0						
	Interface id: 0 (\\Device\\NPF_{55902047-E973-4FFC-B9C0-B0FAC2DA73AF})						
6	Interface name: \\Device\\NPF_{55902047-E973-4FFC-B9C0-B0FAC2DA73AF}						
	Encapsulation type: Ethernet (1)						
8	Arrival Time: Nov 17, 2017 10:50:47.561364000 Mitteleuropäische Zeit						
	[Time shift for this packet: 0.000000000 seconds]						
10	Epoch Time: 1510912247.561364000 seconds						
	[Time delta from previous captured frame: 0.397775000 seconds]						

```

12 [Time delta from previous displayed frame: 0.459379000 seconds]
   [Time since reference or first frame: 1.803262000 seconds]
14 Frame Number: 162
   Frame Length: 42 bytes (336 bits)
16 Capture Length: 42 bytes (336 bits)
   [Frame is marked: True]
18 [Frame is ignored: False]
   [Protocols in frame: eth:ethertype:arp]
20 [Coloring Rule Name: ARP]
   [Coloring Rule String: arp]
22 Ethernet II, Src: 90:b1:1c:88:97:76, Dst: ff:ff:ff:ff:ff:ff
   Destination: ff:ff:ff:ff:ff:ff
24 Address: ff:ff:ff:ff:ff:ff
   .... ..1. .... = LG bit: Locally administered address (this is NOT the
       factory default)
26 .... ..1 .... = IG bit: Group address (multicast/broadcast)
   Source: 90:b1:1c:88:97:76
28 Address: 90:b1:1c:88:97:76
   .... ..0. .... = LG bit: Globally unique address (factory default)
30 .... ..0 .... = IG bit: Individual address (unicast)
   Type: ARP (0x0806)
32 Address Resolution Protocol (request)
   Hardware type: Ethernet (1)
34 Protocol type: IPv4 (0x0800)
   Hardware size: 6
36 Protocol size: 4
   Opcode: request (1)
38 Sender MAC address: 90:b1:1c:88:97:76
   Sender IP address: 134.108.8.37
40 Target MAC address: 00:00:00:00:00:00
   Target IP address: 134.108.8.36
42
   No.      Time      Source      Destination      Protocol Length DestPort Info
                                   Delta Time
44 163 0.000164 90:b1:1c:87:b7:aa 90:b1:1c:88:97:76 ARP 60 134.108.8.36 is at 90:b1
   :1c:87:b7:aa 0.000164
46 Frame 163: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
   Interface id: 0 (\\Device\\NPF_{55902047-E973-4FFC-B9C0-B0FAC2DA73AF})
48 Interface name: \\Device\\NPF_{55902047-E973-4FFC-B9C0-B0FAC2DA73AF}
   Encapsulation type: Ethernet (1)
50 Arrival Time: Nov 17, 2017 10:50:47.561528000 Mitteleuropäische Zeit
   [Time shift for this packet: 0.000000000 seconds]
52 Epoch Time: 1510912247.561528000 seconds
   [Time delta from previous captured frame: 0.000164000 seconds]
54 [Time delta from previous displayed frame: 0.000164000 seconds]
   [Time since reference or first frame: 1.803426000 seconds]
56 Frame Number: 163
   Frame Length: 60 bytes (480 bits)
58 Capture Length: 60 bytes (480 bits)

```

```

[Frame is marked: True]
60 [Frame is ignored: False]
[Protocols in frame: eth:ethertype:arp]
62 [Coloring Rule Name: ARP]
[Coloring Rule String: arp]
64 Ethernet II, Src: 90:b1:1c:87:b7:aa, Dst: 90:b1:1c:88:97:76
    Destination: 90:b1:1c:88:97:76
66     Address: 90:b1:1c:88:97:76
        .... ..0. .... = LG bit: Globally unique address (factory default)
68     .... ..0 .... = IG bit: Individual address (unicast)
    Source: 90:b1:1c:87:b7:aa
70     Address: 90:b1:1c:87:b7:aa
        .... ..0. .... = LG bit: Globally unique address (factory default)
72     .... ..0 .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
74     Padding: 00000000000000000000000000000000
Address Resolution Protocol (reply)
76     Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
78     Hardware size: 6
    Protocol size: 4
80     Opcode: reply (2)
    Sender MAC address: 90:b1:1c:87:b7:aa
82     Sender IP address: 134.108.8.36
    Target MAC address: 90:b1:1c:88:97:76
84     Target IP address: 134.108.8.37

86 No.      Time      Source      Destination      Protocol Length DestPort Info
                                Delta Time
    164 0.000018 134.108.8.37 134.108.8.36    ICMP      74          Echo (ping) request id=0
        x0001, seq=52/13312, ttl=128 (reply in 165) 0.000018
88

90 No.      Time      Source      Destination      Protocol Length DestPort Info
                                Delta Time
    165 0.000168 134.108.8.36 134.108.8.37    ICMP      74          Echo (ping) reply id=0
        x0001, seq=52/13312, ttl=128 (request in 164) 0.000168
92

94 No.      Time      Source      Destination      Protocol Length DestPort Info
                                Delta Time
    176 1.005949 134.108.8.37 134.108.8.36    ICMP      74          Echo (ping) request id=0
        x0001, seq=53/13568, ttl=128 (reply in 177) 1.005949
96

98 No.      Time      Source      Destination      Protocol Length DestPort Info
                                Delta Time
    177 0.000271 134.108.8.36 134.108.8.37    ICMP      74          Echo (ping) reply id=0
        x0001, seq=53/13568, ttl=128 (request in 176) 0.000271

```

Listing 2.6: Wireshark trace for PING command after deleting the ARP table

2.4.2 b) Shutting down one PC

For this second exercise the ARP-table on the source PC was deleted again. But this time, the target PC was shut down before the same Ping command as in ?? was executed. The following figure 2.11 shows the console output for the Ping-Command:

```
C:\Users\rn-labor>ping -n 2 134.108.8.36

Ping wird ausgeführt für 134.108.8.36 mit 32 Bytes Daten:
Antwort von 134.108.8.37: Zielhost nicht erreichbar.
Antwort von 134.108.8.37: Zielhost nicht erreichbar.

Ping-Statistik für 134.108.8.36:
    Pakete: Gesendet = 2, Empfangen = 2, Verloren = 0
    (0% Verlust),
```

Figure 2.11: PING Command Output after ARP table was deleted and target PC was shut down

Because the ARP table is empty, the source PC has to send another ARP request packet. But this time he receives no answer because the PC owning the required IP address is not reachable. The console output shows that the source PC tries to reach the target PC with another ARP request, but again there is no answer. So the communication is canceled after this. Listing ?? shows the two ARP request packet that were sent from the source PC via Broadcast.

No.	Time	Source	Destination	Protocol	Length	Info
21	2.895675	Dell_88:97:76	Broadcast	ARP	42	Who has 134.108.8.36? Tell 134.108.8.37
Frame 21: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0						
Ethernet II, Src: Dell_88:97:76 (90:b1:1c:88:97:76), Dst: Broadcast (ff:ff:ff:ff:ff:ff)						
Address Resolution Protocol (request)						
No.	Time	Source	Destination	Protocol	Length	Info
31	3.798686	Dell_88:97:76	Broadcast	ARP	42	Who has 134.108.8.36? Tell 134.108.8.37
Frame 31: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0						
Ethernet II, Src: Dell_88:97:76 (90:b1:1c:88:97:76), Dst: Broadcast (ff:ff:ff:ff:ff:ff)						
Address Resolution Protocol (request)						

Listing 2.7: Wireshark trace for PING command after deleting the ARP table and shutting down target PC

2.4.3 c) Reconnect after Reboot

After rebooting the target PC and reconnecting it to the network, the same PING-Command as in 2.4.1 was sent again from the source PC. Because now the target PC was reachable, the process and the outcome was exactly the same as in exercise 2.4.1.

2.5 IP multicast addressing

IP multicast addressing is used to send packets to groups of different IP addresses without broadcasting into the network. There are different protocols that are able to do this such as the Virtual Router Redundancy Protocol (VRRP), the Internet Group Management Protocol (IGMP), the routing protocol OSPF, the Network Time Protocol (NTP), the Simple Service Discovery Protocol (SSDP) and the Spanning Tree Protocol (STP).

The range for IP-Multicast Addresses is from 224.0.0.0 to 239.255.255.255. This can be seen when observing the intranet traffic of the Hochschule Esslingen. As a multicast packet contains a range of target IP-addresses, they cannot be exclusively mapped to a single MAC-address. So a trick is used here. The 23 lowest bits from the IP-address are put into the MAC-address. This leads to a range of MAC-addresses from 01-00-5e-00-00-00 to 01-00-5e-7f-ff-ff. The Downside is, that it is possible, that a single MAC-address can be referenced by multiple IP-Addresses. The following listing shows an SSDP packet captured from the traffic of the Hochschule Esslingen:

```

1  No.      Time      Source      Destination      Protocol Length Info
4  0.461068  134.108.8.33  239.255.255.250  SSDP      175      M-SEARCH * HTTP/1.1
3
Frame 4: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface 0
5      Interface id: 0 (\\Device\\NPF_{55902047-E973-4FFC-B9C0-B0FAC2DA73AF})
      Interface name: \\Device\\NPF_{55902047-E973-4FFC-B9C0-B0FAC2DA73AF}
7      Encapsulation type: Ethernet (1)
      Arrival Time: Nov 17, 2017 11:09:15.825997000 Mitteleuropäische Zeit
9      [Time shift for this packet: 0.000000000 seconds]
      Epoch Time: 1510913355.825997000 seconds
11     [Time delta from previous captured frame: 0.115495000 seconds]
      [Time delta from previous displayed frame: 0.115495000 seconds]
13     [Time since reference or first frame: 0.461068000 seconds]
      Frame Number: 4
15     Frame Length: 175 bytes (1400 bits)
      Capture Length: 175 bytes (1400 bits)
17     [Frame is marked: False]
      [Frame is ignored: False]
19     [Protocols in frame: eth:ethertype:ip:udp:ssdp]

```



```

[Coloring Rule Name: UDP]
21 [Coloring Rule String: udp]
Ethernet II, Src: Dell\_87:b4:26 (90:b1:1c:87:b4:26), Dst: IPv4mcast\_7f:ff:fa (01:00:5e:7f:ff:
fa)
23 Destination: IPv4mcast\_7f:ff:fa (01:00:5e:7f:ff:fa)
Address: IPv4mcast\_7f:ff:fa (01:00:5e:7f:ff:fa)
25 .... ..0. .... = LG bit: Globally unique address (factory default)
.... ...1 .... = IG bit: Group address (multicast/broadcast)
27 Source: Dell\_87:b4:26 (90:b1:1c:87:b4:26)
Address: Dell\_87:b4:26 (90:b1:1c:87:b4:26)
29 .... ..0. .... = LG bit: Globally unique address (factory default)
.... ...0 .... = IG bit: Individual address (unicast)
31 Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 134.108.8.33, Dst: 239.255.255.250
33 0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
35 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
37 .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 161
39 Identification: 0x2fc2 (12226)
Flags: 0x00
41 0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
43 ..0. .... = More fragments: Not set
Fragment offset: 0
45 Time to live: 1
Protocol: UDP (17)
47 Header checksum: 0x0b03 [validation disabled]
[Header checksum status: Unverified]
49 Source: 134.108.8.33
Destination: 239.255.255.250
51 [Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
53 User Datagram Protocol, Src Port: 53552, Dst Port: 1900
Source Port: 53552
55 Destination Port: 1900
Length: 141
57 Checksum: 0x01c6 [unverified]
[Checksum Status: Unverified]
59 [Stream index: 0]
Simple Service Discovery Protocol
61 M-SEARCH * HTTP/1.1\r\n
[Expert Info (Chat/Sequence): M-SEARCH * HTTP/1.1\r\n]
63 [M-SEARCH * HTTP/1.1\r\n]
[Severity level: Chat]
65 [Group: Sequence]
Request Method: M-SEARCH
67 Request URI: *
Request Version: HTTP/1.1

```

```
69  Host:239.255.255.250:1900\r\\n
    ST:urn:schemas-upnp-org:device:InternetGatewayDevice:1\r\\n
71  Man:"ssdp:discover"\r\\n
    MX:3\r\\n
73  \r\\n
    [Full request URI: http://239.255.255.250:1900*]
75  [HTTP request 1/19]
    [Next request in frame: 206]
```

Listing 2.8: A single SSDP packet

3 TCP analysis

In this second part of the laboratory the Transmission Control Protocol (TCP) was examined through various exercises showing its functionality.

TCP is one layer above the protocols ICMP and IP in the transport layer of the OSI-model. Its main goal is to establish a stable connection between two hosts to ensure transmission of information without data loss. Other than the protocols one layer down in the Network Layer such as ICMP or IP, TCP provides enhanced functionality for transmission control, error recovery and handling for protocol errors. These functionalities will be shown in the exercises of this laboratory. Table ?? shows the TCP Header.

bits	0-3	4-7	8	9	10	11	12	13	14	15	16-23	24-31
bytes	1		2								3	4
Offset 0	source port										destination port	
Offset 32	sequence number											
Offset 64	acknowledgment number											
Offset 96	data offset	reserved	C W R	E C E	U R G	A C K	P S H	R S T	S S Y	F I N	window	
Offset 128	checksum										urgent pointer	
Offset 160	options											

Table 3.1: Transmission Control Protocol Header

TCP does not handle the networking part of the communication. This task is still handled by IP, which is one layer below TCP in the protocol stack. This is why there are no source- or target address fields in the TCP header. Instead it has segments for source- and target ports. These are necessary because a program such as *Traffic*¹ is needed for the TCP communication and these programs run on a port on both hosts. Sequence and acknowledgment numbers are used for the synchronization and error recovery between server and client. These will be important for the exercises. The control flags (each of them is only one bit) are used for traffic handling. The protocol decides how to interpret the sent data based on the set flags. They are also used for connection establishment, connection reset and for terminating a connection.

¹bla

3.1 Traffic generator handling

As mentioned above, simple PING-commands weren't enough for generating traffic using the Transmission Control Protocol. A program which occupies ports on both PCs (server and client) is needed to establish a TCP connection. For this exercise a tool named *Traffic* was used. The tool provides the functionality of a socket and can perform simple socket routines such as *socket*, *bind()*, *listen()*, *accept()*. It also provides a simple user interface where all functionalities are accessible for a user.

3.2 Simple TCP Communication

The first task in this laboratory was to establish a simple TCP-connection between a Server PC and a Client PC, sending multiple messages from client to server and vice versa, and finally releasing the connection.

3.2.1 Connection establishment

To establish a connection between server and client, TCP performs a routine known as the Three-Way-Handshake. The Three-Way-Handshake consists of three packets being transmitted between client and server. First, the client sends a TCP packet with the SYN-Flag containing a random number x as sequence number (s. header in chapter 3) to the server. If the server is reachable, it replies with a TCP packet with the SYN and ACK-flags being enabled. Furthermore this packet contains the incremented sequence number $x+1$ from the client as acknowledgment number and a newly generated random number y as sequence number. Finally the client performs the last step of the Three-Way-Handshake by replying with another ACK-flagged TCP-packet, containing the incremented sequence number from the server $y+1$ as acknowledgment number.

After these steps were successful, a stable connection is established and both client and server can begin to send data to each other. The following figure 3.1 shows the steps of the Three-Way-Handshake.

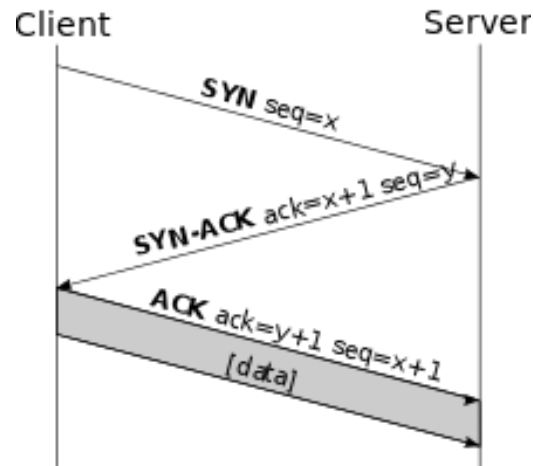


Figure 3.1: Three-Way-Handshake

The Wireshark-trace reveals some more details about the Three-Way-Handshake. As seen in listing ?? client and server also exchange information about the Maximum Segment Size (MSS). Furthermore both parties, the client and the server, set their window size which corresponds to the size of the buffer. When the buffer is completely occupied with data, no more data can be transferred until the buffer is cleaned by the receiver.

7

1	No.	Time	Source	Destination	Protocol	Length	Info
129	14.773660	134.108.8.37	134.108.8.36	TCP	66	51444 -> 6777 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
3	Frame 129: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0						
5	Ethernet II, Src: Dell_88:97:76 (90:b1:1c:88:97:76), Dst: Dell_87:b7:aa (90:b1:1c:87:b7:aa)						
	Internet Protocol Version 4, Src: 134.108.8.37, Dst: 134.108.8.36						
7	Transmission Control Protocol, Src Port: 51444, Dst Port: 6777, Seq: 0, Len: 0						
9	No.	Time	Source	Destination	Protocol	Length	Info
130	14.773711	134.108.8.36	134.108.8.37	TCP	66	6777 -> 51444 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
11	Frame 130: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0						
13	Ethernet II, Src: Dell_87:b7:aa (90:b1:1c:87:b7:aa), Dst: Dell_88:97:76 (90:b1:1c:88:97:76)						
	Internet Protocol Version 4, Src: 134.108.8.36, Dst: 134.108.8.37						
15	Transmission Control Protocol, Src Port: 6777, Dst Port: 51444, Seq: 0, Ack: 1, Len: 0						
17	No.	Time	Source	Destination	Protocol	Length	Info
131	14.773828	134.108.8.37	134.108.8.36	TCP	60	51444 -> 6777 [ACK] Seq=1 Ack=1 Win=65536 Len=0	
19	Frame 131: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0						
21	Ethernet II, Src: Dell_88:97:76 (90:b1:1c:88:97:76), Dst: Dell_87:b7:aa (90:b1:1c:87:b7:aa)						
	Internet Protocol Version 4, Src: 134.108.8.37, Dst: 134.108.8.36						

23 Transmission Control Protocol, Src Port: 51444, Dst Port: 6777, Seq: 1, Ack: 1, Len: 0

Listing 3.1: Wireshark trace for Three-Way-Handshake

3.2.2 Data transfer

After the successful establishment of the TCP connection, multiple messages were transmitted between client and server. the Wireshark trace ?? shows all the packets in chronological order. All packets have in common that the PSH and ACK flags are enabled.

The first message was sent from client to server and contained 100 bytes of data. Because this was the first packet after the Three-Way-Handshake, both acknowledgment and sequence numbers are 1. The server answers with an ACK-packet, where the acknowledgment number is now 101. This is because the data size of the previous packet sent from client to server is added to the acknowledgment number. Also the data size is subtracted from the buffer size.

The second message sent from client to server is much larger, containing 1000 bytes of data. The procedure is the same as for the first message. The only difference is, that the sequence number of the packet is now 101 because of the previous ACK-Packet from the server. The server answers with an ACK-packet where the acknowledgment number is now 1101. Again the data size was added here and subtracted from the buffer size of the server. The sequence number is still 1, because the server hasn't sent any data to the client yet. The window-size of the server however is now reduced to 252, because the data has not been read from the buffer yet.

The third message follows the same procedure as message 1, but of cause this time the acknowledgment number in the server's reply packet is 1201, because there were again 100 bytes transmitted. The window size of the server is now reduced to 251.

The last message was sent from server to client. Here the sequence number is still 1 while the acknowledgment number is already 1201. The client replies with a ACK-packet containing a acknowledgment number increased to 101, because the previous packet was the first data packet it received since the Three-Way-Handshake.

,

No.	Time	Source	Destination	Protocol	Length	Info
41	7.691788	134.108.8.37	134.108.8.36	TCP	154	51444 -> 6777 [PSH, ACK] Seq=1 Ack=1 Win=256 Len=100

3

Frame 41: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on [interface 0](#)

```

5 Ethernet II, Src: Dell\_88:97:76 (90:b1:1c:88:97:76), Dst: Dell\_87:b7:aa (90:b1:1c:87:b7:aa)
  Internet Protocol Version 4, Src: 134.108.8.37, Dst: 134.108.8.36
7 Transmission Control Protocol, Src Port: 51444, Dst Port: 6777, Seq: 1, Ack: 1, Len: 100
  Data (100 bytes)
9
11 No.      Time           Source           Destination      Protocol Length Info
    46 7.892984      134.108.8.36      134.108.8.37      TCP           54      6777 -> 51444 [ACK] Seq=1 Ack
      =101 Win=256 Len=0

13 Frame 46: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
  Ethernet II, Src: Dell\_87:b7:aa (90:b1:1c:87:b7:aa), Dst: Dell\_88:97:76 (90:b1:1c:88:97:76)
15 Internet Protocol Version 4, Src: 134.108.8.36, Dst: 134.108.8.37
  Transmission Control Protocol, Src Port: 6777, Dst Port: 51444, Seq: 1, Ack: 101, Len: 0
17
19 No.      Time           Source           Destination      Protocol Length Info
    90 19.684399      134.108.8.37      134.108.8.36      TCP           1054     51444 -> 6777 [PSH, ACK] Seq
      =101 Ack=1 Win=256 Len=1000

21 Frame 90: 1054 bytes on wire (8432 bits), 1054 bytes captured (8432 bits) on interface 0
  Ethernet II, Src: Dell\_88:97:76 (90:b1:1c:88:97:76), Dst: Dell\_87:b7:aa (90:b1:1c:87:b7:aa)
23 Internet Protocol Version 4, Src: 134.108.8.37, Dst: 134.108.8.36
  Transmission Control Protocol, Src Port: 51444, Dst Port: 6777, Seq: 101, Ack: 1, Len: 1000
25 Data (1000 bytes)

27 No.      Time           Source           Destination      Protocol Length Info
    92 19.889133      134.108.8.36      134.108.8.37      TCP           54      6777 -> 51444 [ACK] Seq=1 Ack
      =1101 Win=252 Len=0

29
31 Frame 92: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
  Ethernet II, Src: Dell\_87:b7:aa (90:b1:1c:87:b7:aa), Dst: Dell\_88:97:76 (90:b1:1c:88:97:76)
  Internet Protocol Version 4, Src: 134.108.8.36, Dst: 134.108.8.37
33 Transmission Control Protocol, Src Port: 6777, Dst Port: 51444, Seq: 1, Ack: 1101, Len: 0

35 No.      Time           Source           Destination      Protocol Length Info
   1875 165.393174      134.108.8.37      134.108.8.36      TCP           154     51444 -> 6777 [PSH, ACK] Seq
      =1101 Ack=1 Win=256 Len=100

37
39 Frame 1875: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface 0
  Ethernet II, Src: Dell\_88:97:76 (90:b1:1c:88:97:76), Dst: Dell\_87:b7:aa (90:b1:1c:87:b7:aa)
  Internet Protocol Version 4, Src: 134.108.8.37, Dst: 134.108.8.36
41 Transmission Control Protocol, Src Port: 51444, Dst Port: 6777, Seq: 1101, Ack: 1, Len: 100
  Data (100 bytes)
43
45 No.      Time           Source           Destination      Protocol Length Info
   1879 165.608164      134.108.8.36      134.108.8.37      TCP           54      6777 -> 51444 [ACK] Seq=1
      Ack=1201 Win=251 Len=0

47 Frame 1879: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
  Ethernet II, Src: Dell\_87:b7:aa (90:b1:1c:87:b7:aa), Dst: Dell\_88:97:76 (90:b1:1c:88:97:76)
49 Internet Protocol Version 4, Src: 134.108.8.36, Dst: 134.108.8.37

```

```

Transmission Control Protocol, Src Port: 6777, Dst Port: 51444, Seq: 1, Ack: 1201, Len: 0
51
No.      Time            Source            Destination        Protocol Length Info
53 2086 201.626400    134.108.8.36      134.108.8.37      TCP        154      6777 -> 51444 [PSH, ACK] Seq
      =1 Ack=1201 Win=251 Len=100

55 Frame 2086: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface 0
Ethernet II, Src: Dell\_87:b7:aa (90:b1:1c:87:b7:aa), Dst: Dell\_88:97:76 (90:b1:1c:88:97:76)
57 Internet Protocol Version 4, Src: 134.108.8.36, Dst: 134.108.8.37
Transmission Control Protocol, Src Port: 6777, Dst Port: 51444, Seq: 1, Ack: 1201, Len: 100
59 Data (100 bytes)

61 No.      Time            Source            Destination        Protocol Length Info
      2088 201.832292    134.108.8.37      134.108.8.36      TCP        60      51444 -> 6777 [ACK] Seq=1201
      Ack=101 Win=256 Len=0

63
Frame 2088: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
65 Ethernet II, Src: Dell\_88:97:76 (90:b1:1c:88:97:76), Dst: Dell\_87:b7:aa (90:b1:1c:87:b7:aa)
Internet Protocol Version 4, Src: 134.108.8.37, Dst: 134.108.8.36
67 Transmission Control Protocol, Src Port: 51444, Dst Port: 6777, Seq: 1201, Ack: 101, Len: 0

```

Listing 3.2: Wireshark trace for TCP messages

3.2.3 Connection release

To terminate an active connection, one of the two connected nodes sends a TCP-packet with the FIN-Flag enabled to the other node. In this case the client releases the connection first. The server answers with an ACK-packet where the acknowledgment number is increased to 102 because of the FIN-Flag. At this point, the connection is half-closed. The server can still send data to the client, but the client cannot send any data to the server, because it already released the connection. Now the server sends a FIN-enabled TCP packet to the client to terminated it's side of the connection. The client answers with an ACK-packet where the sequence number is 102 as before and the acknowledgment number is increased from 1201 to 1202 because of the server's FIN-flag in the previous packet. Now the connection is fully terminated. The following Wireshark-trace shows the captured packets:

```

,
1 No.      Time            Source            Destination        Protocol Length Info
  3752 554.875797    134.108.8.36      134.108.8.37      TCP        54      6777 -> 51444 [FIN, ACK] Seq
      =101 Ack=1201 Win=251 Len=0
3
Frame 3752: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
5 Ethernet II, Src: Dell\_87:b7:aa (90:b1:1c:87:b7:aa), Dst: Dell\_88:97:76 (90:b1:1c:88:97:76)
Internet Protocol Version 4, Src: 134.108.8.36, Dst: 134.108.8.37

```



```

7 Transmission Control Protocol, Src Port: 6777, Dst Port: 51444, Seq: 101, Ack: 1201, Len: 0

9 No.      Time            Source            Destination      Protocol Length Info
  3755 554.876001    134.108.8.37      134.108.8.36     TCP           60      51444 -> 6777 [ACK] Seq=1201
      Ack=102 Win=256 Len=0

11
12 Frame 3755: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
13 Ethernet II, Src: Dell_88:97:76 (90:b1:1c:88:97:76), Dst: Dell_87:b7:aa (90:b1:1c:87:b7:aa)
14 Internet Protocol Version 4, Src: 134.108.8.37, Dst: 134.108.8.36
15 Transmission Control Protocol, Src Port: 51444, Dst Port: 6777, Seq: 1201, Ack: 102, Len: 0

17 No.      Time            Source            Destination      Protocol Length Info
  3869 569.922788    134.108.8.37      134.108.8.36     TCP           60      51444 -> 6777 [FIN, ACK] Seq
      =1201 Ack=102 Win=256 Len=0

19
20 Frame 3869: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
21 Ethernet II, Src: Dell_88:97:76 (90:b1:1c:88:97:76), Dst: Dell_87:b7:aa (90:b1:1c:87:b7:aa)
22 Internet Protocol Version 4, Src: 134.108.8.37, Dst: 134.108.8.36
23 Transmission Control Protocol, Src Port: 51444, Dst Port: 6777, Seq: 1201, Ack: 102, Len: 0

25 No.      Time            Source            Destination      Protocol Length Info
  3870 569.922807    134.108.8.36      134.108.8.37     TCP           54      6777 -> 51444 [ACK] Seq=102
      Ack=1202 Win=251 Len=0

27
28 Frame 3870: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
29 Ethernet II, Src: Dell_87:b7:aa (90:b1:1c:87:b7:aa), Dst: Dell_88:97:76 (90:b1:1c:88:97:76)
30 Internet Protocol Version 4, Src: 134.108.8.36, Dst: 134.108.8.37
31 Transmission Control Protocol, Src Port: 6777, Dst Port: 51444, Seq: 102, Ack: 1202, Len: 0

```

Listing 3.3: Wireshark trace for Connection Release

3.3 TCP flow control

For this exercise another connection between server and client was established the same way as before. Now the task was to send a burst of 100 message from one host to another, while each message contained 1000 bytes of data. The intention behind this is to completely occupy the server's receive buffer with data and to observe what happens next. As seen in the Wireshark-trace, the client sends packet after packet to the server until the Window-size in the Servers corresponding ACK-packet is decreased to a value beneath 1000 bytes. When the client now tries to send the next packet, the server answers with a **TCP Zero Window** packet, where the window-size is decreased to 0, so the client cannot send another packet, no matter how small it is. This causes the client to stop sending the data packets. Instead it asks the server regularly if the receiver-buffer was cleared using a **TCP Zero Window Probe** packet. While the buffer is still occupied, the server answers with another TCP Zero Window packet. When the buffer

is cleared by the server, it sends a **Zero Window Update** packet with the new buffer size to the client. As soon as the client receives this packet, it answers with an ACK-packet and continues to send the data packets. The following Wireshark trace shows an example for each of the packets mentioned above.

No.	Time	Source	Destination	Protocol	Length	Info
711	94.044149	134.108.8.37	134.108.8.36	TCP	60	[TCP ZeroWindowProbe] 51484 -> 6777 [ACK] Seq=73467 Ack=1 Win=256 Len=1
Frame 711: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0						
Ethernet II, Src: Dell_88:97:76 (90:b1:1c:88:97:76), Dst: Dell_87:b7:aa (90:b1:1c:87:b7:aa)						
Internet Protocol Version 4, Src: 134.108.8.37, Dst: 134.108.8.36						
Transmission Control Protocol, Src Port: 51484, Dst Port: 6777, Seq: 73467, Ack: 1, Len: 1						
Data (1 byte)						
0000	53		S			
714	94.255811	134.108.8.36	134.108.8.37	TCP	54	[TCP ZeroWindow] [TCP ACKed unseen segment] 6777 -> 51484 [ACK] Seq=1 Ack=73468 Win=0 Len=0
Frame 714: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0						
Ethernet II, Src: Dell_87:b7:aa (90:b1:1c:87:b7:aa), Dst: Dell_88:97:76 (90:b1:1c:88:97:76)						
Internet Protocol Version 4, Src: 134.108.8.36, Dst: 134.108.8.37						
Transmission Control Protocol, Src Port: 6777, Dst Port: 51484, Seq: 1, Ack: 73468, Len: 0						
1795	204.639823	134.108.8.36	134.108.8.37	TCP	54	[TCP Window Update] 6777 -> 51484 [ACK] Seq=1 Ack=73469 Win=18 Len=0
Frame 1795: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0						
Ethernet II, Src: Dell_87:b7:aa (90:b1:1c:87:b7:aa), Dst: Dell_88:97:76 (90:b1:1c:88:97:76)						
Internet Protocol Version 4, Src: 134.108.8.36, Dst: 134.108.8.37						
Transmission Control Protocol, Src Port: 6777, Dst Port: 51484, Seq: 1, Ack: 73469, Len: 0						

Listing 3.4: Wireshark trace example for Zero Window packets

3.4 TCP transmission error recovery/abort

3.5 TCP protocol errors (synchronization errors)

4 IPv6/ICMPv6 analysis

4.1 Node configuration

4.1.1 IPv4 and IPv6 configuration

4.1.2 interfaces for IPv6

4.2 PING commands

4.2.1 a) Basic ICMPv6 PING command

4.2.2 b) ICMPv6 PING command with large data package

4.2.3 c) Rebooting PC

4.2.4 d) Enforcing Neighbor discovery

4.2.5 e) ICMPv6 PING command with destination in another subnet

4.2.6 f) PING to a remote tunnel end

5 Conclusion

Bibliography

- [Bec04] Kent Beck. *Test-Driven development by Example*. Pearson, 2004. ISBN: 8131715957.
- [WMV03] Laurie Williams, E. Michael Maximilien, and Mladen Vouk. “Test-Driven Development as a Defect-Reduction Practice”. In: *14th IEEE International Symposium on Software Reliability Engineering ISSRE 2003*. Denver, Colorado: IEEE, 2003. URL: <http://ieeexplore.ieee.org/document/1251029/> (visited on 10/01/2016).