Übung 1

# 1.1 Download und Installation

Wireshark

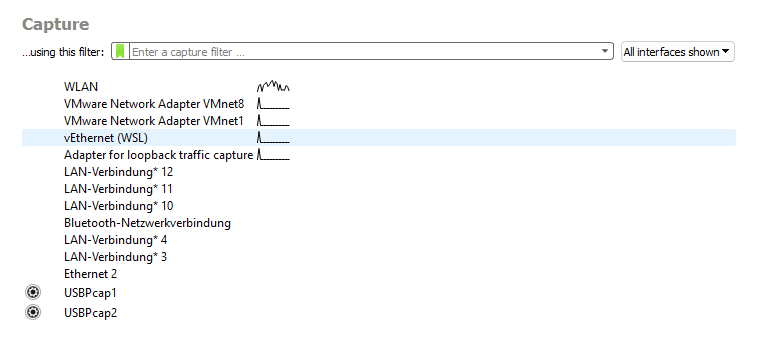
Download und Installation der .exe von folgender Website:  
<https://www.wireshark.org/download.html>

Cisco Packet Tracer

Für den Download wird ein netacad Account benötigt, welcher und id.cisco.com erstellt werden kann. Ebenfalls müssen personenbezogenen Daten unter netacad.com angegeben werden. Unter folgendem Link kann die .exe für den Cisco Packet Tracer heruntergeladen und danach installiert werden:  
<https://skillsforall.com/resources/lab-downloads>

Nach der Installation muss man sich noch mit seinem netacad Account anmelden.

# 1.2 Erstellung von Wireshark Trace File

Um ein Trace-File erstellen zu können muss zuerst eine Verbindung aufgezeichnet werden. Dafür kann wie unten gezeigt eine Netzwerkschnittstelle ausgewählt werden:  


Anschließend wird jeglicher Netzwerkverkehr, welcher über diese Schnittstelle geht, aufgezeichnet. Um nun einen Ping (ICMP-Nachricht) aufzuzeichnen kann folgender Befehl (in diesem Fall in einer WSL) verwendet werden:  
 Text

Description automatically generated

Um Pakete näher zu analysieren können sie z.B.: mit einem Doppelklick geöffnet werden:  
Graphical user interface, application

Description automatically generated

Das Trace-File ist unter „**nwt2ue1\_Jakob\_Mayr.pcapng**“ gespeichert.

# 1.3 Analyse eines existierenden Wireshark Traces

UDP

* Frage 1:
* Wenn auf udp gefiltert wird, sind 37 Frames sichtbar: Table

  Description automatically generated
* Es werden die Ports 53 (server) und 4375 (client) verwendet:

Request:

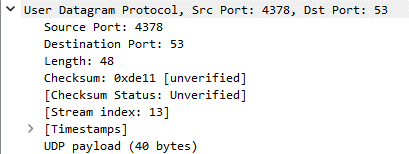
Graphical user interface, text, application

Description automatically generated

Response:

Graphical user interface, text, application

Description automatically generated

* Das Datagramm mit der Framenummer 535 besitzt **4** Header Felder:  
  

Ein UDP-Datagram besitzt immer folgende 4 Header Felder:  
**Source Port:** 4378

**Destination Port:** 53

**Length:** 48

**Checksum:** 0xde11

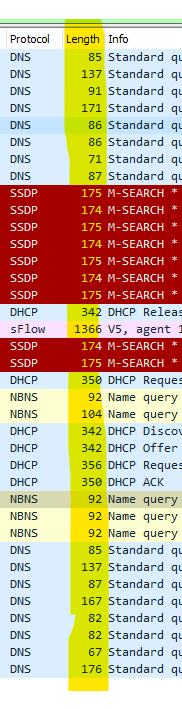
* Ein UDP-Datagram kann maximal bei IPv4 65.507 Bytes und bei IPv6 65.527 Bytes groß sein.

Table

Description automatically generated[[1]](#footnote-2)

Aus obiger Grafik ergibt sich, dass ein UDP-Datagram ohne Header 65.499 Bytes an Daten senden könnte. Jedoch wird abhängig vom Netzwerk die maximale Größe durch die MTU (maximum transmission unit) begrenzt.

* Im Trace sieht man die Größe jedes Paketes in der Spalte „Length“



TCP

* **Frage 2:**
  + Im TCP Segment in Framge 152 werden keine Nutzdaten übertragen, eine „TCP-payload“ fehlt.Graphical user interface, text, application

    Description automatically generated
  + Es sind folgende Header-Felder vorhanden:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | Source Port | 4335 | | Destination Port | 80 | | Squence Num. | 0 (raw: 4265079785) | | Acknowledgment Num. | 0 (raw: 0) | | Flags | 0x002 (SYN) | | Window | 64240 | | Checksum | 0x4d3b | | Urgent Pointer | 0 |   Die Felder DO (data offset) und RSV (reserved field), sind in wireguard nicht sichtbar. |  |

* **Frage 3:**
* Dem **3**. Tcp-stream

Graphical user interface, text, application

Description automatically generated

* Verwendete Protokolle:  
  HTTP/1.1 (Hypertext Transfer Protocol)

TCP (Transmission Control Protocol)

IP (Internet Protocol)

Ethernet

* Es werden die Ports 80 (Server) und 4335 (Client) verwendet.
* Die Übertragung ist nicht sicher, da keine Versschlüsselung der Daten bei http passiert - Die Daten werden als Klartext übertragen.
* **Frage 4:**
  + Die relative Sequenznummer ist **1686** während die absolute Sequenznummer **2437358089** ist.



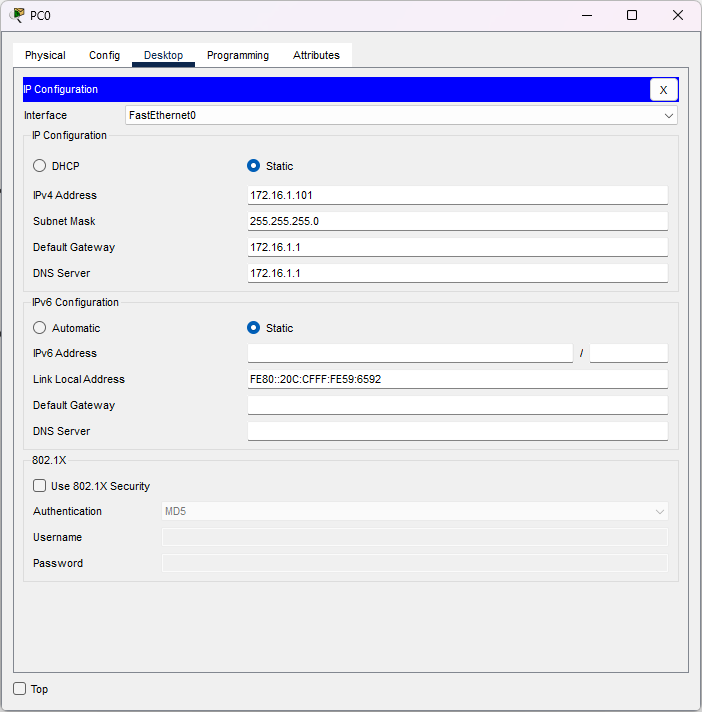
* + Die relative Bestätigungsnummer (acknowledgment number) ist **519** während die absolute Bestätigungsnummer **4265080304** ist.



* + Der Wert für die relative Bestätigungsnummer ergibt sich aus der Anzahl der vom Empfänger empfangenen Bytes, seit dem letzten Segment, das vom Sender gesendet wurde. Der Wert stellt die Differenz zwischen der nächsten erwarteten Sequenznummer (die absolute Bestätigungsnummer) und der Sequenznummer des letzten empfangenen Bytes dar.

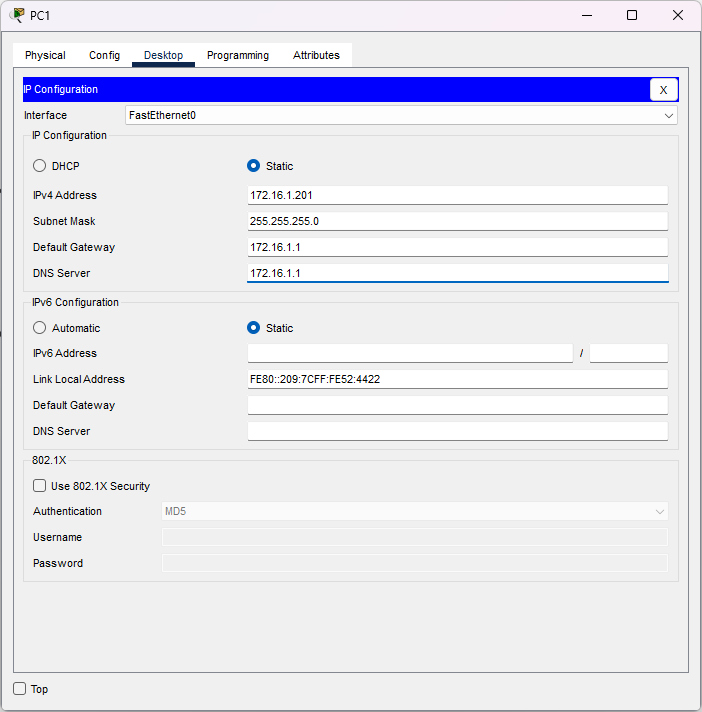
# Analyse und Verbesserung eines existierenden Packet Tracer Files

* Konfiguration PC0



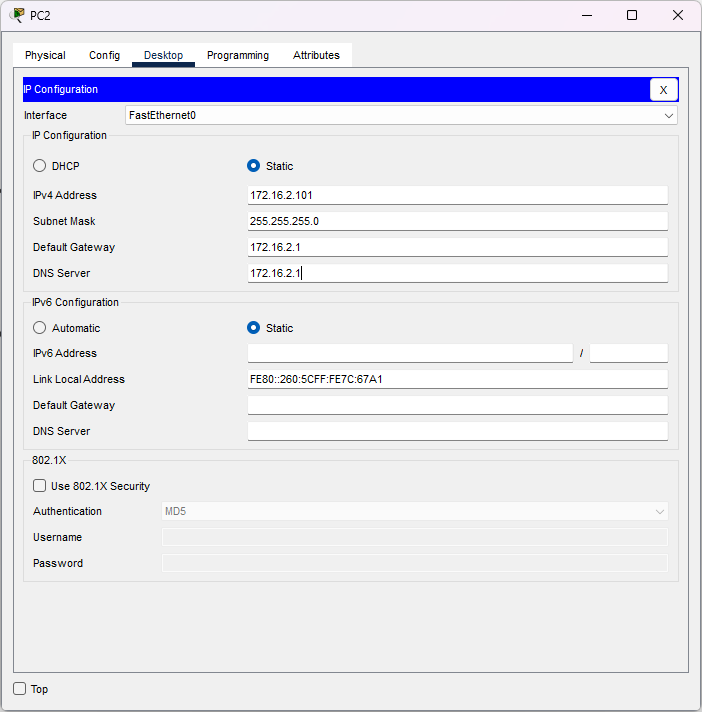
Bei PC0 müssen die Subnetzmaske (auf 255.255.255.0) und der DNS-Server (auf 172.16.1.1) angepasst werden.

* Konfiguration PC1



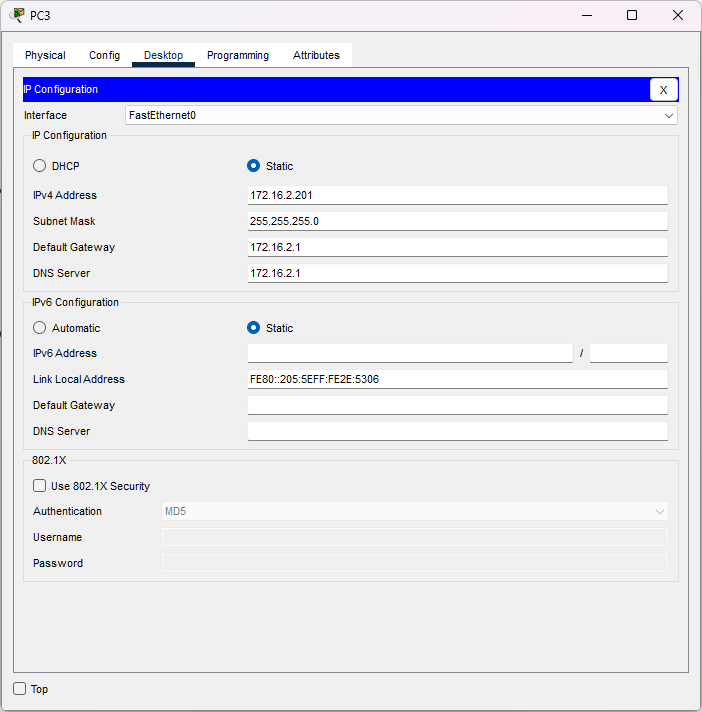
Bei PC1 müssen das Standardgateway (auf 172.16.1.1) und der DNS-Server (auf 172.16.1.1) angepasst werden.

* Konfiguration PC2



Bei PC2 muss der DNS-Server (auf 172.16.2.1) angepasst werden.

* Konfiguration PC3



Bei PC3 muss sowohl die Subnetzmaske (auf 255.255.255.0) als auch das Standardgateway (auf 172.16.2.201) und der DNS-Server (auf 172.16.2.1) angepasst werden.

|  |  |  |  |
| --- | --- | --- | --- |
| PC0  Text  Description automatically generated with medium confidence Der Grund, warum der Erste ping zu PC3 fehlschlägt ist, dass der Router zuerst einen ARP-Broadcast aussenden muss, um die MAC-Adresse des Clients zu lernen. (Wurde zuvor noch nicht gepingt) | PC1 | PC2 | PC3 |

* **PING-TEST**
* Frage 5:

Wenn ein Endsystem nicht die Gleiche Netzmaske wie das Standardgateway besitzt, so **kann** es zu Kommunikationsproblemen mit anderen Geräten kommen.   
Ist eine Adresse nicht im selben Netz wie der Client wird die Nachricht an den Router gesendet. Möchte man an die Broadcastadresse senden, kann man glück haben (Netzwerk von Client hat selbe Broadcastadresse da sich Netzwerke überlappen), es kann aber auch fehlschlagen.

1. The User Datagram Protocol (UDP), <https://erg.abdn.ac.uk/users/gorry/course/inet-pages/udp.html>, 23.03.2023. [↑](#footnote-ref-2)