**Aufgabenstellung:** ICMP und ARP Pakete mittels einem Paketsniffer zu analysieren.

**Übung 3**

Analyse von ARP und ICMP Paketen

Gruppe: 1

Klasse: 2AHIT

Abgegeben am: \_\_\_\_\_\_\_\_\_

Leonard bunea & Konrad guntendorfer

December 14, 2021

# Inhaltsverzeichnis

[1 Inhaltsverzeichnis 1](#_Toc90384510)

[2 Abbildungsverzeichnis 2](#_Toc90384511)

[3 ARP/ICMP in Packet-Tracer 3](#_Toc90384512)

[3.1.1 Simulationsmodus 4](#_Toc90384513)

[3.1.2 Ausführung eines Pings 5](#_Toc90384514)

[4 ARP-Cache 8](#_Toc90384515)

[4.1.1 Vergleich 9](#_Toc90384516)

[4.2 ARP Cache löschen 11](#_Toc90384517)

[5 ARP/ICMP in Wireshark 12](#_Toc90384518)

[5.1 Nur ARP-Aufzeichnungen anzeigen 13](#_Toc90384519)

[5.2 Datenverkehr von einem Ping-Kommando 14](#_Toc90384520)

# Abbildungsverzeichnis

[Abbildung 1: Ping Zwischen PC1 und PC2 und auch das arp -a Kommando 3](https://d.docs.live.net/082dcf85f8043c6a/School/Netzwerktechnik/Protokolle/Übung3.docx#_Toc90384521)

[Abbildung 2: arp -a Kommando von PC2 3](https://d.docs.live.net/082dcf85f8043c6a/School/Netzwerktechnik/Protokolle/Übung3.docx#_Toc90384522)

[Abbildung 3: ipconfig /all PC2 4](https://d.docs.live.net/082dcf85f8043c6a/School/Netzwerktechnik/Protokolle/Übung3.docx#_Toc90384523)

[Abbildung 4: ipcofig /all PC1 4](https://d.docs.live.net/082dcf85f8043c6a/School/Netzwerktechnik/Protokolle/Übung3.docx#_Toc90384524)

[Abbildung 5: Alle Protokolle außer ARP und ICMP werden raus gefiltert 4](#_Toc90384525)

[Abbildung 6: Visualisierung eines Ping Kommandos 5](https://d.docs.live.net/082dcf85f8043c6a/School/Netzwerktechnik/Protokolle/Übung3.docx#_Toc90384526)

[Abbildung 7: Gesamter Netzverlauf von einem Ping 5](#_Toc90384527)

[Abbildung 8: PDU Information ARP 6](#_Toc90384528)

[Abbildung 9: Netzaktivität von einem ARP-Broadcast 6](#_Toc90384529)

[Abbildung 10: Ping Erfolgreich 7](https://d.docs.live.net/082dcf85f8043c6a/School/Netzwerktechnik/Protokolle/Übung3.docx#_Toc90384530)

[Abbildung 11: Ping Kommando und ARP Cache von PC2 8](#_Toc90384531)

[Abbildung 12: Ping Kommando und ARP Cache von PC1 9](https://d.docs.live.net/082dcf85f8043c6a/School/Netzwerktechnik/Protokolle/Übung3.docx#_Toc90384532)

[Abbildung 13: ipconfig /all PC1 10](https://d.docs.live.net/082dcf85f8043c6a/School/Netzwerktechnik/Protokolle/Übung3.docx#_Toc90384533)

[Abbildung 14: ipconfig /all PC2 10](https://d.docs.live.net/082dcf85f8043c6a/School/Netzwerktechnik/Protokolle/Übung3.docx#_Toc90384534)

[Abbildung 15: ARP Cache löschen 11](#_Toc90384535)

[Abbildung 16: Wireshark ARP Anfrage 12](https://d.docs.live.net/082dcf85f8043c6a/School/Netzwerktechnik/Protokolle/Übung3.docx#_Toc90384536)

[Abbildung 17: ARP Antwork in Wireshark 13](https://d.docs.live.net/082dcf85f8043c6a/School/Netzwerktechnik/Protokolle/Übung3.docx#_Toc90384537)

[Abbildung 18: Nur ARP-Aufzeichnungen zu sehen 13](https://d.docs.live.net/082dcf85f8043c6a/School/Netzwerktechnik/Protokolle/Übung3.docx#_Toc90384538)

[Abbildung 19: Alle Protokolle außer ARP filtrieren 13](https://d.docs.live.net/082dcf85f8043c6a/School/Netzwerktechnik/Protokolle/Übung3.docx#_Toc90384539)

[Abbildung 20: Datenverkehr von einem Ping Kommando 14](https://d.docs.live.net/082dcf85f8043c6a/School/Netzwerktechnik/Protokolle/Übung3.docx#_Toc90384540)

# ARP/ICMP in Packet-Tracer

Hier wird ein Netzwerk mit einem Switch und zwei PCs simuliert.

Graphical user interface

Description automatically generatedIn Abbildung 1 sieht den erfolgreichen Ping zwischen den zwei virtuellen Computern. Man sieht, dass PC1 sich die MAC-Adresse von PC2 im ARP-Cache gespeichert hat.

Abbildung 1: Ping Zwischen PC1 und PC2 und auch das arp -a Kommando

Graphical user interface, application

Description automatically generatedIn Abbildung 2 sieht man die Ausgabe von arp -a von PC2. PC2 hat auch die MAC-Adresse von PC1 gespeichert.

Abbildung 2: arp -a Kommando von PC2

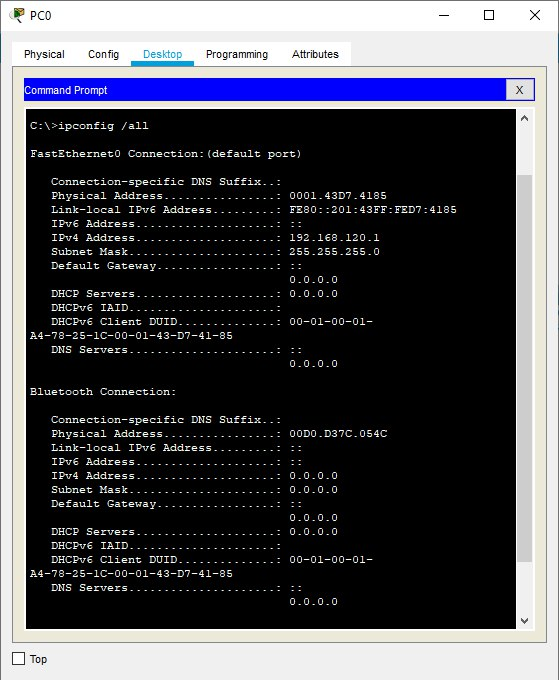
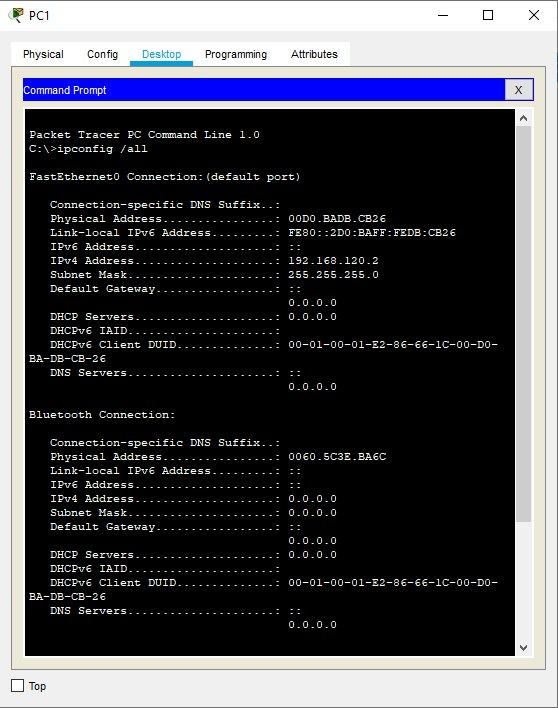


Abbildung 3: ipconfig /all PC2

Abbildung 4: ipcofig /all PC1

### Simulationsmodus

Im Simulationsmodus kann man alle Netzwerkaktivität Schritt für Schritt verfolgen.

Graphical user interface, application, Word

Description automatically generated

Abbildung 5: Alle Protokolle außer ARP und ICMP werden raus gefiltert

### Chart, line chart Description automatically generatedAusführung eines Pings

Abbildung 6: Visualisierung eines Ping Kommandos

Graphical user interface, application

Description automatically generated

Abbildung 7: Gesamter Netzverlauf von einem Ping

In Abbildung 6 kann den ARP Broadcast mitsamt den Inhalten sehen.

Graphical user interface, application, Word

Description automatically generated

Abbildung 8: PDU Information ARP

In der nächsten Abbildung ist der komplette Verlauf von einem ARP-Broadcast dargestellt. Man sieht, dass sich die zwei PCs gemeinsam mit ARP verständigen um ihre MAC-Adressen herauszufinden.

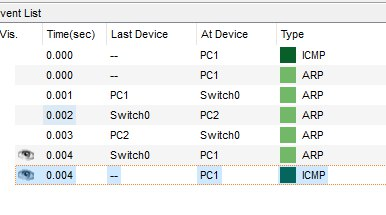


Abbildung 9: Netzaktivität von einem ARP-Broadcast

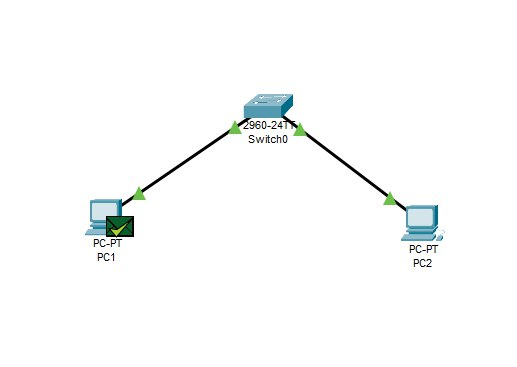


Abbildung 10: Ping Erfolgreich

# ARP-Cache

Graphical user interface, text

Description automatically generatedIn den nächsten zwei Screenshots wird die Verbindung zwischen den 2 PCs kontrolliert und der ARP Cache überprüft.

Abbildung 11: Ping Kommando und ARP Cache von PC2

### A screenshot of a computer Description automatically generated with medium confidenceVergleich

Abbildung 12: Ping Kommando und ARP Cache von PC1

In Abbildung 13 und 14 erkennt man, dass die beiden PCs ihre IP- und MAC-Adressen in ihren ARP Cache gespeichert haben.

Text

Description automatically generatedA picture containing text, indoor, computer, screenshot

Description automatically generated

Abbildung 13: ipconfig /all PC1

Abbildung 14: ipconfig /all PC2

## ARP Cache löschen

Um den ARP Cache zu löschen benutzt man das Kommando:

arp -d \*

Text

Description automatically generated

Abbildung 15: ARP Cache löschen

# ARP/ICMP in Wireshark

Auf PC2 wurde das Programm Wireshark installiert.

In Abbildung 16 sieht man eine ARP-Anfrage, sowohl auch die restlichen Protokolle die zurzeit im Netz verwendet werden. in Wireshark. Ein ARP-Broadcast hat die Zieladresse FF:FF:FF:FF:FF:FF.

Graphical user interface, text, application, email

Description automatically generatedDie ARP-Antwort beinhaltet die Ziel MAC-Adresse und wird zurück zum originalen Sender geschickt.

Abbildung 16: Wireshark ARP Anfrage

## Text, application, table Description automatically generatedNur ARP-Aufzeichnungen anzeigen

Abbildung 17: ARP Antwork in Wireshark

Table

Description automatically generatedGraphical user interface

Description automatically generatedUm in Wireshark nur bestimmte Protokolle anzeigen zu lassen, kann man sie in der Suchleiste eingeben.

Abbildung 18: Nur ARP-Aufzeichnungen zu sehen

Abbildung 19: Alle Protokolle außer ARP filtrieren

## Graphical user interface, text Description automatically generatedDatenverkehr von einem Ping-Kommando

Abbildung 20: Datenverkehr von einem Ping Kommando

Ein Ping-Kommando sendet zuerst einen „ICMP echo (ping) request“ zur Ziel IP-Adresse. Falls die MAC-Adresse nicht vorhanden ist, wird auch ein ARP-Broadcast gesendet. Der Ziel Computer sendet dann ein „ICMP echo (ping) reply“ zurück. Dies geschieht 4 mal.