# M129 Labornetz: 5. Erste Netzwerkanalyse mit Wireshark

**Lernziele**

- Netzwerkkonfiguration in Windows und Linux kennenlernen

- Netzwerkprotokolle und Umschlagsprinzip durch Netzwerkanalyse verstehen.

**Voraussetzungen (Windowsrechner )**

- Schliessen Sie Ihren Rechner per Kabel ans Labornetz an.

- Installieren Sie Wireshark auf Ihrem Rechner.

- Starten Sie Ihre Linux-VM.

**Art:** Selbstständige Einzelarbeit, man darf zusammen diskutieren.

**Hilfsmittel**

- Lehrmittel: Kapitel 1.4

- Wireshark-Video und ev. weitere Quellen

**Zeit** ca. 60 Min.

**Abgabe**

Dokumentieren Sie Ihre Resultate mit einem Printscreen. Pasten Sie die Printscreens in Ihr Abgabedokument und laden Sie das Dokument **im PDF-Format** auf die Lernplattform hoch.

Die Datei soll **kuerzel-wireshark1.pdf** heissen.

**Termine**

- Bis zum Ende des Unterrichts sollten Sie mindestens ca. die Hälfte der Aufgaben gelöst haben. Laden Sie den Zwischenstand beim entsprechenden Link auf Moodle hoch.

- Laden Sie bis Anfang nächstes Mal das Dokument mit der vollständig gelösten Aufgabe hoch.

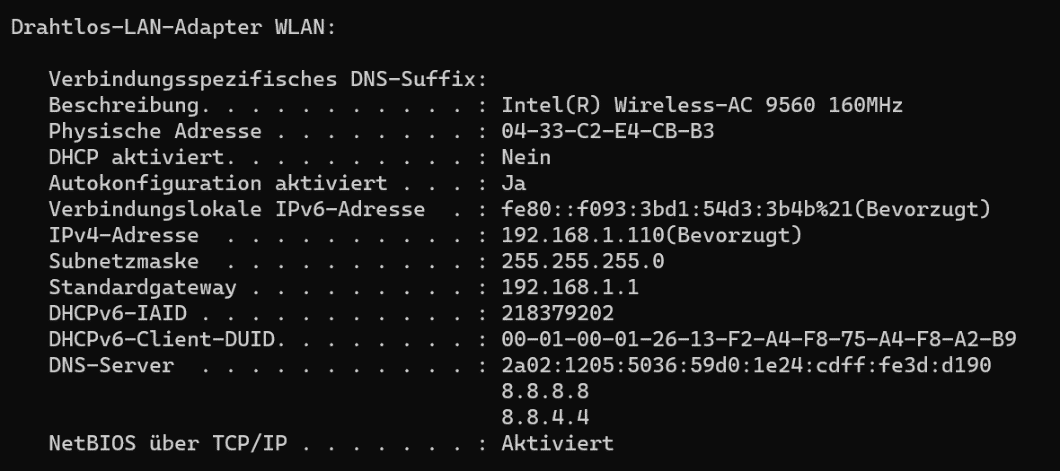
### Aufgabe 1: Netzwerkumgebung konfigurieren

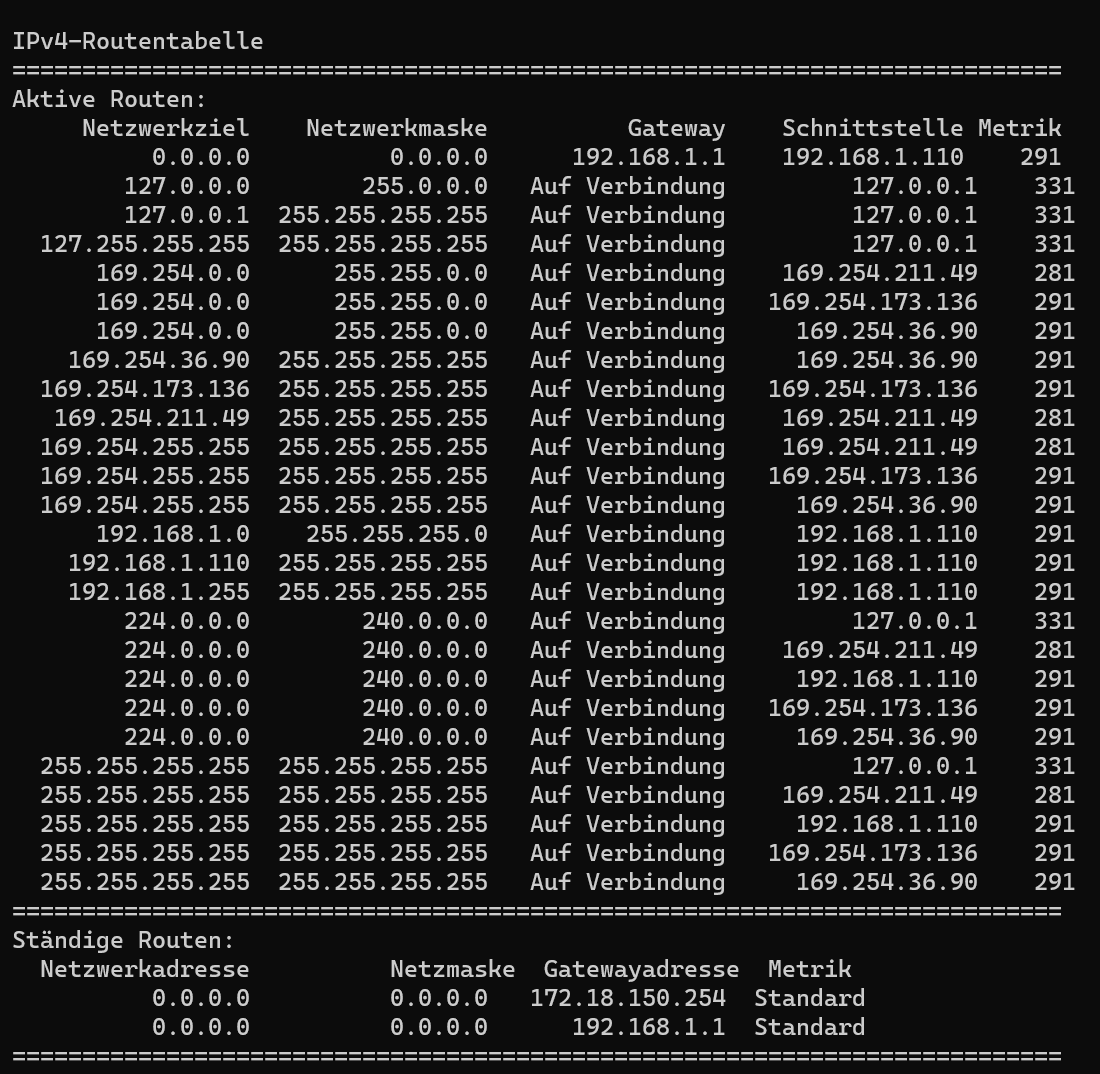
#### 1.1 Windows-Host auf fixe IP umstellen

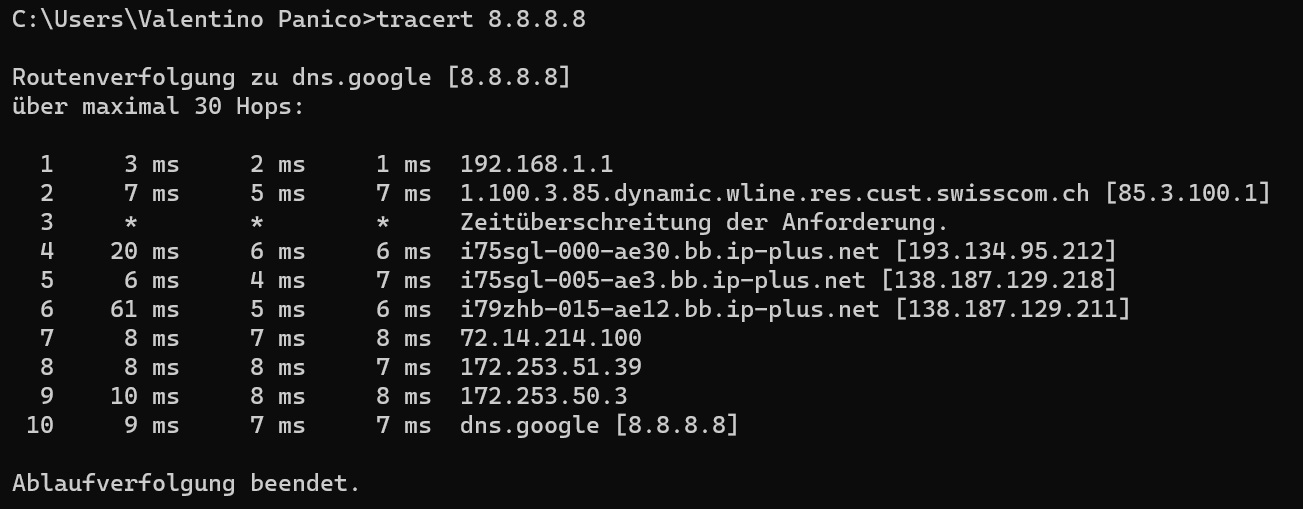
Schliessen Sie Ihren Rechner ans Ethernet.

a) Tragen Sie eine feste IP-Adresse Default Gateway und DNS gemäss Liste ein. DNS z.B. Nr. 1 gleich wie Gateway, Nr. 2 = 1.1.1.1 oder 8.8.8.8 (auch eigene funktionierende Konfigurationen sind erlaubt)

Belegen Sie mit den folgenden Screenshots, dass es geklappt hat:

i) **ipconfig /all**   
ii) **route print**iii) **tracert 8.8.8.8**





#### 1.2 Linux-VM auf fixe IP umstellen

Bridgen sie die Netzwerkschnittstelle zum Ethernet-Anschluss des Hosts.

Stellen Sie die Netzwerkkonfiguration auf die Werte in der IP-Liste um.

Hinweis: Sie können die grafische Oberfläche benützen oder die Datei „interfaces“ editieren: die Datei */etc/network/interfaces* können Sie mit „sudo nano ….“ editieren. Schreiben Sie den Inhalt nach dem folgenden Muster um. Lassen Sie danach **service networking restart** oder **dhclient -r + dhclient** laufen.

auto lo enp0s3

iface lo inet loopback

iface enp0s3 inet static

address a.b.c.d

netmask a.b.c.d

gateway a.b.c.d

Belegen Sie die geänderte Konfiguration mit den folgenden Screenshots:   
a) **ip a**  
b) **ping 1.1.1.1**  
c) **traceroute 1.1.1.1**

#### 1.3 Installieren Sie die klassischen Netzwerkwerkzeuge (falls noch nicht gemacht)

- Die Paketlisten synchronisieren mit **apt-get update**

- Das Paket net-tools mit den Tools ifconfig, route, arp usw. installieren:   
 **apt install net-tools**

- Installieren Sie auch gleich andere wichtige Tools wie **tcpdump** und **nmap**.

Belegen Sie die Lösung mit folgenden Screenshots:  
a) **ifconfig enp0s3**   
b) **route -n**   
c) **tcpdump -i enp0s3** (bzw. Ihr Adaptername  
d) **nmap -sP 172.18.150.30-60** (sP = skip port scan, gibt nur erreichbare Hosts aus. Auch genannt „ping scan“)

### Aufgabe 2: Untersuchen der Kapselung

Schauen Sie das kurze Einführungsvideo auf https://www.youtube.com/watch?v=yn3yzFDub1E

Finden Sie sich auf der Oberfläche zurecht, insbesondere den Einstellungen (Menu Bearbeiten -> Einstellungen), den Aufzeichnungsoptionen (schwarzes Zahnrad) und den Anzeigefiltern (obere weisse Leiste).

Starten Sie Wireshark auf Ihrem Host. Machen Sie dann folgendes:

1. Starten Sie eine Aufzeichnung (Capture).
2. Sprechen Sie den Labor-Router mit den Protokollen ICMP (ping), FTP, SSH und HTTP an.
3. Stoppen Sie die Erfassung und untersuchen Sie die einzelnen Pakete.
4. Suchen Sie Einträge für folgende Protokolle: ARP, ICMP, TCP und UDP.
5. Erklären Sie anhand eines solchen Beispiels, wie das Umschlagsprinzip (Kapselung) funktioniert.

### Aufgabe 3: Protokollverteilung (Statistik)

1. Starten Sie die Aufzeichnung wieder und lassen Sie sie einige Minuten lang laufen.
2. Führen Sie auf Ihrem Computer viele verschiedene Transaktionen durch.
3. Stoppen Sie die Aufzeichnung und wählen Sie aus dem Menu „Statistiken“ „Protokollhierarchie“.
4. Listen Sie im Lösungsdokument einige verwendete Protokolle auf und versuchen Sie ihre relative Häufigkeit zu ermitteln. Welches ist das gebräuchlichste Protokoll auf der oberen Schicht?

TCP, UDP und TLS sind die meist verwendeten Protokolle. Auch wenn nichts gemacht wird, passiert im Hintergrund einiges.

### 