

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 Screenshots 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**

Drahtlos-LAN-Adapter WLAN:

```

Verbindungsspezifisches DNS-Suffix:
Beschreibung. . . . . : Intel(R) Wireless-AC 9560 160MHz
Physische Adresse . . . . . : 04-33-C2-E4-CB-B3
DHCP aktiviert. . . . . : Nein
Autokonfiguration aktiviert . . . : Ja
Verbindungslokale IPv6-Adresse . . : fe80::f093:3bd1:54d3:3b4b%21(Bevorzugt)
IPv4-Adresse . . . . . : 192.168.1.110(Bevorzugt)
Subnetzmaske . . . . . : 255.255.255.0
Standardgateway . . . . . : 192.168.1.1
DHCPv6-IAID . . . . . : 218379202
DHCPv6-Client-DUID. . . . . : 00-01-00-01-26-13-F2-A4-F8-75-A4-F8-A2-B9
DNS-Server . . . . . : 2a02:1205:5036:59d0:1e24:cdff:fe3d:d190
                        8.8.8.8
                        8.8.4.4
NetBIOS über TCP/IP . . . . . : Aktiviert
  
```

IPv4-Routentabelle

Aktive Routen:

Netzwerkziel	Netzwerkmaske	Gateway	Schnittstelle	Metrik
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.110	291
127.0.0.0	255.0.0.0	Auf Verbindung	127.0.0.1	331
127.0.0.1	255.255.255.255	Auf Verbindung	127.0.0.1	331
127.255.255.255	255.255.255.255	Auf Verbindung	127.0.0.1	331
169.254.0.0	255.255.0.0	Auf Verbindung	169.254.211.49	281
169.254.0.0	255.255.0.0	Auf Verbindung	169.254.173.136	291
169.254.0.0	255.255.0.0	Auf Verbindung	169.254.36.90	291
169.254.36.90	255.255.255.255	Auf Verbindung	169.254.36.90	291
169.254.173.136	255.255.255.255	Auf Verbindung	169.254.173.136	291
169.254.211.49	255.255.255.255	Auf Verbindung	169.254.211.49	281
169.254.255.255	255.255.255.255	Auf Verbindung	169.254.211.49	281
169.254.255.255	255.255.255.255	Auf Verbindung	169.254.173.136	291
169.254.255.255	255.255.255.255	Auf Verbindung	169.254.36.90	291
192.168.1.0	255.255.255.0	Auf Verbindung	192.168.1.110	291
192.168.1.110	255.255.255.255	Auf Verbindung	192.168.1.110	291
192.168.1.255	255.255.255.255	Auf Verbindung	192.168.1.110	291
224.0.0.0	240.0.0.0	Auf Verbindung	127.0.0.1	331
224.0.0.0	240.0.0.0	Auf Verbindung	169.254.211.49	281
224.0.0.0	240.0.0.0	Auf Verbindung	192.168.1.110	291
224.0.0.0	240.0.0.0	Auf Verbindung	169.254.173.136	291
224.0.0.0	240.0.0.0	Auf Verbindung	169.254.36.90	291
255.255.255.255	255.255.255.255	Auf Verbindung	127.0.0.1	331
255.255.255.255	255.255.255.255	Auf Verbindung	169.254.211.49	281
255.255.255.255	255.255.255.255	Auf Verbindung	192.168.1.110	291
255.255.255.255	255.255.255.255	Auf Verbindung	169.254.173.136	291
255.255.255.255	255.255.255.255	Auf Verbindung	169.254.36.90	291

Ständige Routen:

Netzwerkadresse	Netzmaske	Gatewayadresse	Metrik
0.0.0.0	0.0.0.0	172.18.150.254	Standard
0.0.0.0	0.0.0.0	192.168.1.1	Standard

```
C:\Users\Valentino Panico>tracert 8.8.8.8
```

```
Routenverfolgung zu dns.google [8.8.8.8]
über maximal 30 Hops:
```

```
 1      3 ms      2 ms      1 ms  192.168.1.1
 2      7 ms      5 ms      7 ms  1.100.3.85.dynamic.wline.res.cust.swisscom.ch [85.3.100.1]
 3      *          *          *    Zeitüberschreitung der Anforderung.
 4     20 ms      6 ms      6 ms  i75sgl-000-ae30.bb.ip-plus.net [193.134.95.212]
 5      6 ms      4 ms      7 ms  i75sgl-005-ae3.bb.ip-plus.net [138.187.129.218]
 6     61 ms      5 ms      6 ms  i79zhh-015-ae12.bb.ip-plus.net [138.187.129.211]
 7      8 ms      7 ms      8 ms  72.14.214.100
 8      8 ms      8 ms      7 ms  172.253.51.39
 9     10 ms      8 ms      8 ms  172.253.50.3
10      9 ms      7 ms      7 ms  dns.google [8.8.8.8]
```

```
Ablaufverfolgung beendet.
```

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 benutzen 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:

- `ip a`**
- `ping 1.1.1.1`**
- `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:

- `ifconfig enp0s3`**
- `route -n`**
- `tcpdump -i enp0s3`** (bzw. Ihr Adaptername)
- `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.

Protokoll	Prozentualer Anteil bei den Paketen	Pakete	Prozentualer Anteil der Bytes	Bytes	Bits/s	Pakete (bei denen das Protokoll vorkommt)
▼ Frame	100.0	3539	100.0	1848104	235k	0
▼ Ethernet	100.0	3539	2.7	49546	6321	0
> Internet Protocol Version 6	0.7	24	0.1	960	122	0
▼ Internet Protocol Version 4	99.0	3502	3.8	70040	8935	0
▼ User Datagram Protocol	46.1	1631	0.7	13048	1664	0
Simple Service Discovery Protocol	0.5	17	0.2	3193	407	17
QUIC IETF	40.9	1446	59.0	1089707	139k	1435
Network Time Protocol	0.4	14	0.0	672	85	14
NetBIOS Name Service	0.3	9	0.0	450	57	9
Multicast Domain Name System	0.4	14	0.0	513	65	14
Link-local Multicast Name Resolution	0.2	6	0.0	176	22	6
Domain Name System	1.4	50	0.2	3264	416	50
Data	2.4	86	1.2	22276	2842	86
▼ Transmission Control Protocol	52.9	1871	32.0	591352	75k	1062
Transport Layer Security	22.5	797	30.9	570350	72k	778
SSH Protocol	0.8	29	0.3	5534	706	28
Malformed Packet	0.0	1	0.0	0	0	1
▼ Hypertext Transfer Protocol	0.1	2	0.0	742	94	1
eXtensible Markup Language	0.0	1	0.0	413	52	1
HomePlug protocol	0.1	2	0.0	92	11	2
HomePlug AV protocol	0.0	1	0.0	46	5	1
Address Resolution Protocol	0.3	10	0.0	406	51	10