Praktikum Rechnernetze

Protokoll zu Versuch 1 (Troubleshooting TCP/IP) von Gruppe 1

Jakob Waibel Daniel Hiller Elia Wüstner Felix Pojtinger

2021-10-19

Einführung

Mitwirken

Diese Materialien basieren auf Professor Kiefers “Praktikum Rechnernetze”-Vorlesung der HdM Stuttgart.

Sie haben einen Fehler gefunden oder haben einen Verbesserungsvorschlag? Bitte eröffnen Sie ein Issue auf GitHub (github.com/pojntfx/uni-netpractice-notes):

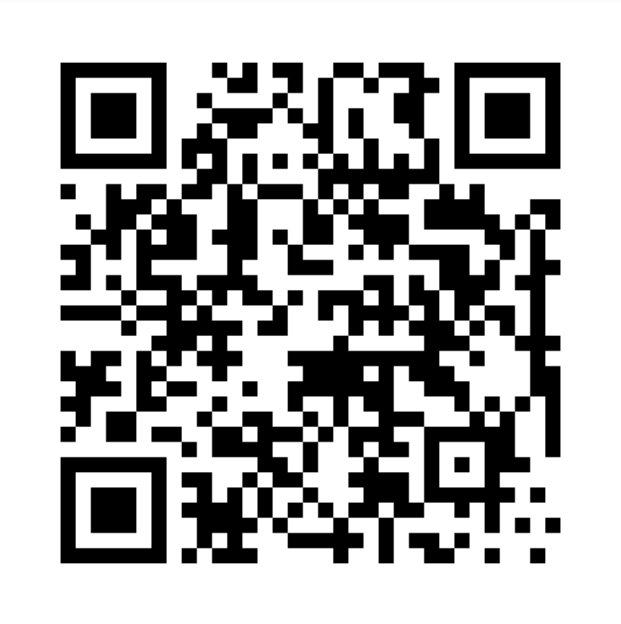


Figure 1: QR-Code zum Quelltext auf GitHub

Lizenz

Dieses Dokument und der enthaltene Quelltext ist freie Kultur bzw. freie Software.

Figure 2: Badge der AGPL-3.0-Lizenz

IP-Subnetz-Berechnung

IP-Subnetz-Berechnung

Ergänzen Sie die Tabelle

IP-Adresse	SN-Mask	Klasse	Netz-addresse	Anzahl Subnetze	Broadcast-Adresse	Anzahl Hosts	Vorheriges Netz	nachgelag. Netz
14.21.4.210	255.255.128.0	A	14.21.0.0	512	14.21.127.255	32766	14.20.128.0	14.21.128.0
184.16.12.80	255.255.255.224	B	184.16.12.64	2048	184.16.12.95	30	184.16.12.32	184.16.12.95
143.62.67.32	255.255.255.240	B	143.62.67.32	4096	143.62.67.47	14	143.62.67.16	143.62.67.80
264.12.14.81	255.255.192.0	/	/	/	/	/	/	/
192.168.1.42	255.255.255.0	C	192.168.1.0	1	192.168.1.255	254	/	/
10.15.119.237	255.255.255.252	A	10.15.119.236	4194304	10.15.119.239	2	10.15.119.232	10.15.119.240

184.16.12.80 → Class B

255.255.255.224

8 + 8 + 8 + 3 → /27 → 184.16.12.80/27 | CIDR

255.255.255.111|0 0000 } 224

184.16.12.010|1 0000 } 80

010 | 0 0000 → 64 → 184.16.12.64 | Network adress

010 | 1 1111 → 95 → 184.16.12.95 | Broadcast adress

5+3 = 11 → 2^{11} = 2048 Subnets; 5 → $2^5 - 2$ = 30 Hosts per subnets

0000 0000 010 0 + 0000 0000 001 1 = 011 | 0 0000 → 96 → 184.16.12.96/27 | Secondly network's network address

0000 0000 010 0 − 0000 0000 001 1 = 001 | 0 0000 → 32 → 184.16.12.32/27 | Primarily network's network address

Werkzeuge des Betriebssystems

IP-Konfiguration

Überprüfen Sie zunächst die Netzkonfiguration Ihres PC.
IP-Adresse, Subnetzmaske, Default-Gateway und
DNS-Server Erfragen Sie den Klartextnamen Ihres PC.

IP-Addresse: 142.62.66.5
Subnetzmaske: 255.255.255.0
Default-Gateway: 141.62.66.250
DNS-Server: 141.62.66.250
Klartextnamen: rn05

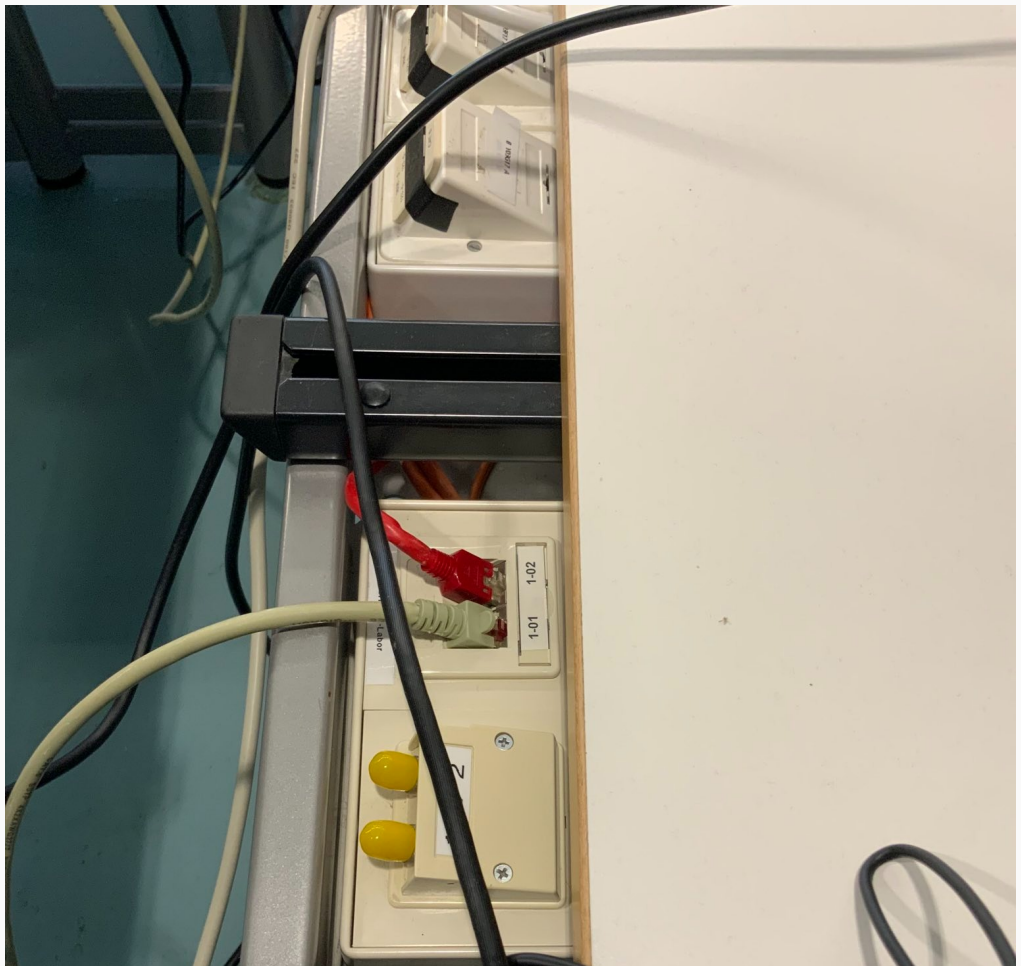
Wie können Sie die korrekte Installation der Netzwerkkarten-Treiber testen?

```
$ lspci
# ...
00:1f.6 Ethernet controller: Intel Corporation Ethe
# ...
```

Anschluss des PC an das Labornetz

Betrachten Sie die Verbindungen der Labor-Switches untereinander. Welche Wege können Sie erkennen?

Folgende Verbindungen konnten erkannt werden:



Überprüfung der korrekten Installation

Sehen Sie sich die IP-Konfiguration Ihres Rechners an durch Eingabe von ipconfig bzw. ipconfig/all in der DOS-Box.

ifconfig ist deprecated, es wird stattdessen ip verwendet.

```
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noque
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: enp0s31f6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu
    link/ether 4c:52:62:0e:54:8b brd ff:ff:ff:ff:ff
    inet 141.62.66.5/24 brd 141.62.66.255 scope glo
       valid_lft 11902sec preferred_lft 11902sec
```

Senden Sie einen ping-command an einen zweiten Rechner, der am gleichen Switch angeschlossen ist

Adress Resolution Protocol ARP

arp ist deprecated, es wird stattdessen ip neigh verwendet.

Dokumentieren Sie den Inhalt der ARP-Tabelle Ihres PC (arp-a, DOS-Box).

```
$ ip neigh show
141.62.66.186 dev enp0s31f6 lladdr 10:82:86:01:36:6
141.62.66.12 dev enp0s31f6 lladdr 4c:52:62:0e:e0:e9
141.62.66.14 dev enp0s31f6 lladdr 4c:52:62:0e:e0:ae
141.62.66.250 dev enp0s31f6 lladdr 00:0d:b9:4f:b8:14
141.62.66.4 dev enp0s31f6 lladdr 4c:52:62:0e:53:eb
141.62.66.13 dev enp0s31f6 lladdr 4c:52:62:0e:54:5d
141.62.66.22 dev enp0s31f6  FAILED
141.62.66.216 dev enp0s31f6 lladdr 44:31:92:50:6c:6
```

Nun pingen Sie einen beliebigen anderen Arbeitsplatz an und beobachten Sie evtl. Veränderungen der ARP-Tabelle

Ping

Ping-Nutzung

```
$ ping --help
Usage
   ping [options] <destination>

Options:
  <destination>      dns name or ip address
  -a                 use audible ping
  -A                 use adaptive ping
  -B                 sticky source address
  -c <count>         stop after <count> replies
  -D                 print timestamps
  -d                 use SO_DEBUG socket option
  -f                 flood ping
  -h                 print help and exit
```

Traceroute & MTR

Versuchen Sie, den zentralen Peering-Point (DE-CIX) in Deutschland geografisch anhand des Namens zu lokalisieren.

```
$ traceroute de-cix.net
traceroute to de-cix.net (46.31.121.136), 30 hops m
 1  opnsense-router.rnlabor.hdm-stuttgart.de (141.6
0.509 ms  1.566 ms  0.991 ms
 2  ciscovlgw318.hdm-stuttgart.de (141.62.31.246)
2.047 ms  1.295 ms  1.019 ms
 3  firewall-h.hdm-stuttgart.de (141.62.1.1)
1.118 ms  1.450 ms  1.120 ms
 4  * * *
 5  stu-al30-1-te0-0-0-17.belwue.net (129.143.56.53
3.625 ms  3.191 ms  3.331 ms
 6  stu-nwz-a99-hu0-3-0-5.belwue.net (129.143.56.10
3.030 ms  1.325 ms  1.440 ms
```

ss

netstat ist deprecated, es wird stattdessen dessen Nachfolger ss aus dem iproute2-Package verwendet:

```
Name         : iproute
Version      : 5.10.0
Release      : 2.fc34
Architecture : x86_64
Size         : 1.7 M
Source       : iproute-5.10.0-2.fc34.src.rpm
Repository   : @System
From repo    : anaconda
Summary      : Advanced IP routing and network devi
URL          : http://kernel.org/pub/linux/utils/ne
License      : GPLv2+ and Public Domain
Description  : The iproute package contains network
             : for example) which are designed to u
```

Route

route ist deprecated, es wird stattdessen ip route verwendet.

Interpretieren Sie die Einträge in der Routing-Tabelle Ihres Rechners.

Zu Erkennen ist, dass das Default-Gateway 141.62.66.250 ist, über das Netzwerkgerät enp0s31f6. Auf localhost wird über den Kernel geroutet, d.h. dass Traffic niemals das System verlässt. Andere Subnetze werden über das Default-Gateway gerouted.

```
$ ip route show table all
default via 141.62.66.250 dev enp0s31f6
141.62.66.0/24 dev enp0s31f6 proto kernel scope lin
broadcast 127.0.0.0 dev lo table local proto kernel
local 127.0.0.0/8 dev lo table local proto kernel s
local 127.0.0.1 dev lo table local proto kernel sco
broadcast 127.255.255.255 dev lo table local proto
```

Weitere Werkzeuge

iperf

Mittels iperf3 kann die Übertragungsrate zwischen zwei Hosts getestet werden.

```
# Host A
$ iperf3 -s
```

```
Server listening on 5201
```

```
Accepted connection from 141.62.66.4, port 54336
[  5] local 141.62.66.5 port 5201 connected to 141.
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-1.00   sec  99.4 MBytes   834 Mbits/se
[  5]   1.00-2.00   sec  99.5 MBytes   835 Mbits/se
[  5]   2.00-3.00   sec   101 MBytes   846 Mbits/se
[  5]   3.00-4.00   sec   101 MBytes   845 Mbits/se
[  5]   4.00-5.00   sec   101 MBytes   845 Mbits/se
```

Nmap

Nmap ist die Kurzform für Network Mapper. Mit diesem kann man Ports scannen, Informationen über die Services bekommen (Version, Betriebssystem etc.) und vorinstallierte als auch eigene Skripts verwenden.

Es gibt verschiedene Möglichkeiten Scans durchzuführen, der gängige (und die Standardeinstellung) ist der
TCP connect Port Scan. Es gibt noch weitere, welche situativ über Flags verwendet werden können:

```
$ nmap 10.10.247.15 -sS          # TCP SYN Por
$ nmap 10.10.247.15 -sA          # TCP ACK Por
$ nmap 10.10.247.15 -sU          # UDP Port Sc
```

Es besteht die Möglichkeit mehrere IPs zu scannen, ebenso wie ein Bereich von IPs, eine einzige IP oder eine Domain:

```
$ nmap 10.10.247.15              # Scannen ein
```