

Praktikum Rechnernetze

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

Jakob Waibel Daniel Hiller Elia Wüstner Felix Pojtinger

2021-10-19

Einführung

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/poijntfx/uni-netpractice-notes):



Abbildung 1: QR-Code zum Quelltext auf GitHub

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



Abbildung 2: Badge der AGPL-3.0-Lizenz

Uni Network Practice Notes (c) 2021 Jakob Waibel, Daniel Hiller,
Elia Wüstner, Felix Pojtinger

SPDX-License-Identifier: AGPL-3.0

IP-Subnetz-Berechnung

IP-Subnetz-Berechnung

Ergänzen Sie die Tabelle

IP-Adresse	SN-Mask	Klasse	Netz- adresse	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	32.768	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	16	143.62.67.16	143.62.67.50
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	256	/	/
10.15.119.237	255.255.255.252	A	10.15.119.236	4.096.104	10.15.119.239	2	10.15.119.232	10.15.119.240

184.16.12.80 → Class B

255.255.255.224

$8 + 8 + 8 + 7 \rightarrow 127 \rightarrow 184.16.12.127$ 1.128

255.255.255.224 → 11111000 → 224

184.16.12.01010000 → 80

01010000 → 64 → 184.16.12.64 1.128

01011111 → 95 → 184.16.12.95 1.128

$2^8 - 1 = 255$
 $2^7 - 1 = 127$ → 128 Hosts pro Netzwerk

00000000 → 0
 00000001 → 1
 00000010 → 2
 00000011 → 3
 00000100 → 4
 00000101 → 5
 00000110 → 6
 00000111 → 7
 00001000 → 8
 00001001 → 9
 00001010 → 10
 00001011 → 11
 00001100 → 12
 00001101 → 13
 00001110 → 14
 00001111 → 15
 00010000 → 16
 00010001 → 17
 00010010 → 18
 00010011 → 19
 00010100 → 20
 00010101 → 21
 00010110 → 22
 00010111 → 23
 00011000 → 24
 00011001 → 25
 00011010 → 26
 00011011 → 27
 00011100 → 28
 00011101 → 29
 00011110 → 30
 00011111 → 31
 00100000 → 32
 00100001 → 33
 00100010 → 34
 00100011 → 35
 00100100 → 36
 00100101 → 37
 00100110 → 38
 00100111 → 39
 00101000 → 40
 00101001 → 41
 00101010 → 42
 00101011 → 43
 00101100 → 44
 00101101 → 45
 00101110 → 46
 00101111 → 47
 00110000 → 48
 00110001 → 49
 00110010 → 50
 00110011 → 51
 00110100 → 52
 00110101 → 53
 00110110 → 54
 00110111 → 55
 00111000 → 56
 00111001 → 57
 00111010 → 58
 00111011 → 59
 00111100 → 60
 00111101 → 61
 00111110 → 62
 00111111 → 63
 01000000 → 64
 01000001 → 65
 01000010 → 66
 01000011 → 67
 01000100 → 68
 01000101 → 69
 01000110 → 70
 01000111 → 71
 01001000 → 72
 01001001 → 73
 01001010 → 74
 01001011 → 75
 01001100 → 76
 01001101 → 77
 01001110 → 78
 01001111 → 79
 01010000 → 80
 01010001 → 81
 01010010 → 82
 01010011 → 83
 01010100 → 84
 01010101 → 85
 01010110 → 86
 01010111 → 87
 01011000 → 88
 01011001 → 89
 01011010 → 90
 01011011 → 91
 01011100 → 92
 01011101 → 93
 01011110 → 94
 01011111 → 95
 01100000 → 96
 01100001 → 97
 01100010 → 98
 01100011 → 99
 01100100 → 100
 01100101 → 101
 01100110 → 102
 01100111 → 103
 01101000 → 104
 01101001 → 105
 01101010 → 106
 01101011 → 107
 01101100 → 108
 01101101 → 109
 01101110 → 110
 01101111 → 111
 01110000 → 112
 01110001 → 113
 01110010 → 114
 01110011 → 115
 01110100 → 116
 01110101 → 117
 01110110 → 118
 01110111 → 119
 01111000 → 120
 01111001 → 121
 01111010 → 122
 01111011 → 123
 01111100 → 124
 01111101 → 125
 01111110 → 126
 01111111 → 127
 10000000 → 128
 10000001 → 129
 10000010 → 130
 10000011 → 131
 10000100 → 132
 10000101 → 133
 10000110 → 134
 10000111 → 135
 10001000 → 136
 10001001 → 137
 10001010 → 138
 10001011 → 139
 10001100 → 140
 10001101 → 141
 10001110 → 142
 10001111 → 143
 10010000 → 144
 10010001 → 145
 10010010 → 146
 10010011 → 147
 10010100 → 148
 10010101 → 149
 10010110 → 150
 10010111 → 151
 10011000 → 152
 10011001 → 153
 10011010 → 154
 10011011 → 155
 10011100 → 156
 10011101 → 157
 10011110 → 158
 10011111 → 159
 10100000 → 160
 10100001 → 161
 10100010 → 162
 10100011 → 163
 10100100 → 164
 10100101 → 165
 10100110 → 166
 10100111 → 167
 10101000 → 168
 10101001 → 169
 10101010 → 170
 10101011 → 171
 10101100 → 172
 10101101 → 173
 10101110 → 174
 10101111 → 175
 10110000 → 176
 10110001 → 177
 10110010 → 178
 10110011 → 179
 10110100 → 180
 10110101 → 181
 10110110 → 182
 10110111 → 183
 10111000 → 184
 10111001 → 185
 10111010 → 186
 10111011 → 187
 10111100 → 188
 10111101 → 189
 10111110 → 190
 10111111 → 191
 11000000 → 192
 11000001 → 193
 11000010 → 194
 11000011 → 195
 11000100 → 196
 11000101 → 197
 11000110 → 198
 11000111 → 199
 11001000 → 200
 11001001 → 201
 11001010 → 202
 11001011 → 203
 11001100 → 204
 11001101 → 205
 11001110 → 206
 11001111 → 207
 11010000 → 208
 11010001 → 209
 11010010 → 210
 11010011 → 211
 11010100 → 212
 11010101 → 213
 11010110 → 214
 11010111 → 215
 11011000 → 216
 11011001 → 217
 11011010 → 218
 11011011 → 219
 11011100 → 220
 11011101 → 221
 11011110 → 222
 11011111 → 223
 11100000 → 224
 11100001 → 225
 11100010 → 226
 11100011 → 227
 11100100 → 228
 11100101 → 229
 11100110 → 230
 11100111 → 231
 11101000 → 232
 11101001 → 233
 11101010 → 234
 11101011 → 235
 11101100 → 236
 11101101 → 237
 11101110 → 238
 11101111 → 239
 11110000 → 240
 11110001 → 241
 11110010 → 242
 11110011 → 243
 11110100 → 244
 11110101 → 245
 11110110 → 246
 11110111 → 247
 11111000 → 248
 11111001 → 249
 11111010 → 250
 11111011 → 251
 11111100 → 252
 11111101 → 253
 11111110 → 254
 11111111 → 255

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-Adresse: 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
```

```
# ...
```

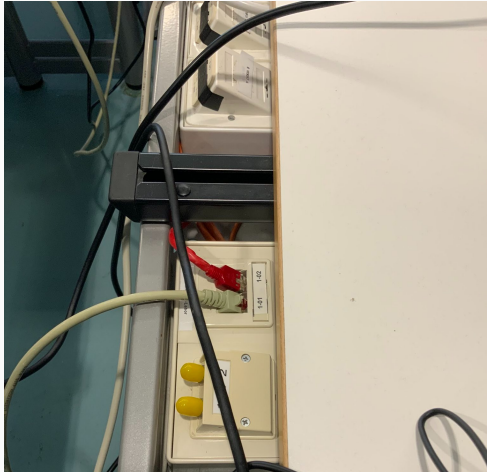
```
00:1f.6 Ethernet controller: Intel Corporation Ethe
```

```
# ...
```


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-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
```

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 device
URL            : http://kernel.org/pub/linux/utils/net
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 link
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 proto12
```

Weitere Werkzeuge

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 ¹³

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 Port Scan
$ nmap 10.10.247.15 -sA          # TCP ACK Port Scan
$ nmap 10.10.247.15 -sU          # UDP Port Scan
```

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
```