

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	14.21.255.255	32.768	14.20.255.0	14.21.255.0
184.16.12.80	255.255.255.224	B	184.16.12.64	2.048	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	4.096	143.62.67.47	6	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	254	/	/
10.15.119.237	255.255.255.252	A	10.15.119.232	4.194.304	10.15.119.239	2	10.15.119.232	10.15.119.240

184. 11. 12. 80 → Chu B

255, 255, 255, 224

$$P + P + P + 3 \rightarrow 12 \rightarrow 184, 11, 12, 80/12 \rightarrow 1600$$

255, 255, 255, 11110 0000 } 224

184. 11. 12. 0101 0000 } 80

$010 \mid 00000 \rightarrow 64 \rightarrow A16, A1, A2, 64 \mid \text{Network address}$
 $010 \mid 11111 \rightarrow 95 \rightarrow A16, A1, A2, 95 \mid \text{Broadcast address}$
 $\underbrace{\hspace{1.5cm}}_{\text{64-95}} \quad \underbrace{\hspace{1.5cm}}_{\text{5}} \quad \underbrace{\hspace{1.5cm}}_{\text{2}^{10} - 2 = 10 \text{ hosts per subnets}}$
 $2^{10} = 2048 \text{ subnets}$

$\begin{array}{r} \text{+} \\ \text{+} \end{array} \begin{array}{r} \text{Dist Dfns} \\ \text{Dist Dfns} \end{array} \begin{array}{r} 0/0 \\ \text{+/-} \\ \text{+/-} \end{array}$
 $0 \ 0000 \rightarrow 98 \rightarrow 114, 11, 12, 8/12 \mid \text{simultaneous network address}$

$\begin{array}{r} \text{Dist Dfns} \\ \text{- Dist Dfns} \end{array} \begin{array}{r} 0/0 \\ \text{+/-} \\ \text{+/-} \end{array}$
 $0 \ 0000 \rightarrow 32 \rightarrow 114, 11, 12, 8/12 \mid \text{Primary network's network address}$

Werkzeuge des Betriebssystems

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 Ethernet Conn
```

```
# ...
```


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 noqueue state U  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
2: enp0s31f6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state U  
    link/ether 4c:52:62:0e:54:8b brd ff:ff:ff:ff:ff:ff  
    inet 141.62.66.5/24 brd 141.62.66.255 scope global dynamic enp0s31f6  
        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 10:82:86:01:36:6d STALE
141.62.66.12 dev enp0s31f6 lladdr 4c:52:62:0e:e0:e9 STALE
141.62.66.14 dev enp0s31f6 lladdr 4c:52:62:0e:e0:ae STALE
141.62.66.250 dev enp0s31f6 lladdr 00:0d:b9:4f:b8:14 REACHAB
141.62.66.4 dev enp0s31f6 lladdr 4c:52:62:0e:53:eb STALE
141.62.66.13 dev enp0s31f6 lladdr 4c:52:62:0e:54:5d STALE
141.62.66.22 dev enp0s31f6 FAILED
141.62.66.216 dev enp0s31f6 lladdr 44:31:92:50:6c:61 STALE
```

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

```
$ ping 141.62.66.226
```

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 max, 60 bytes
 1  opnsense-router.rnlabor.hdm-stuttgart.de (141.62.66.250)
   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 (129.143.56.106)
   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 configuration
URL            : http://kernel.org/pub/linux/utils/net/iproute2/
License        : GPLv2+ and Public Domain
Description    : The iproute package contains networking utilities
                  (for example) which are designed to use the 11ad
```

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 src 141.62.66.1
```

```
broadcast 127.0.0.0 dev lo table local proto kernel scope link
```

```
local 127.0.0.0/8 dev lo table local proto kernel scope host
```

```
local 127.0.0.1 dev lo table local proto kernel scope host
```

```
broadcast 127.255.255.255 dev lo table local proto kernel scope
```

```
broadcast 141.62.66.0 dev enp0s31f6 table local proto kernel
```

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 141.62.66.4 p
```

[ID]	Interval		Transfer	Bitrate
[5]	0.00 - 1.00	sec	99.4 MBytes	834 Mbits/sec
[5]	1.00 - 2.00	sec	99.5 MBytes	835 Mbits/sec
[5]	2.00 - 3.00	sec	101 MBytes	846 Mbits/sec
[5]	3.00 - 4.00	sec	101 MBytes	845 Mbits/sec
[5]	4.00 - 5.00	sec	101 MBytes	845 Mbits/sec

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 einer einzigen IP
$ nmap 10.10.247.15 10.10.247.240 # Scannen mehrerer IPs
```