Praktikum Rechnernetze: Versuch 1: Troubleshooting TCP/IP

Gruppe 1 (Jakob Waibel, Daniel Hiller, Elia Wüstner und Felix Pojtinger)

Durchführung 2021-10-19, letzte Änderung October 20, 2021

Introduction

Contributing

Contributing

These study materials are heavily based on professor Kiefer's "Praktikum Rechnernetze" lecture at HdM Stuttgart.

Found an error or have a suggestion? Please open an issue on GitHub (github.com/pojntfx/uni-netpractice-notes):

Figure 1: QR code to source repository

If you like the study materials, a GitHub star is always appreciated :)

License

License

Figure 2: AGPL-3.0 license badge

SPDX-License-Identifier: AGPL-3.0

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	143.62.67.50
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	10.15.119.236	4 194 304	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 address

010|1 1111 → 95 → 184.16.12.95 | Broadcast adress

(11 + 11) 5

2^{11} = 2048 subnets

$2^5 - 2$ = 30 Hosts per subnets

0000 0000 010|0 + 0000 0000 00|1 = 010|1

0|0000 → 96 → 184.16.12.96/27 | Security network's network address

0000 0000 010|0 − 0000 0000 00|1 = 001|1

0|0000 → 32 → 184.16.12.32/27 | Private network's network address

Tools des OS

IP-Konfiguration

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?

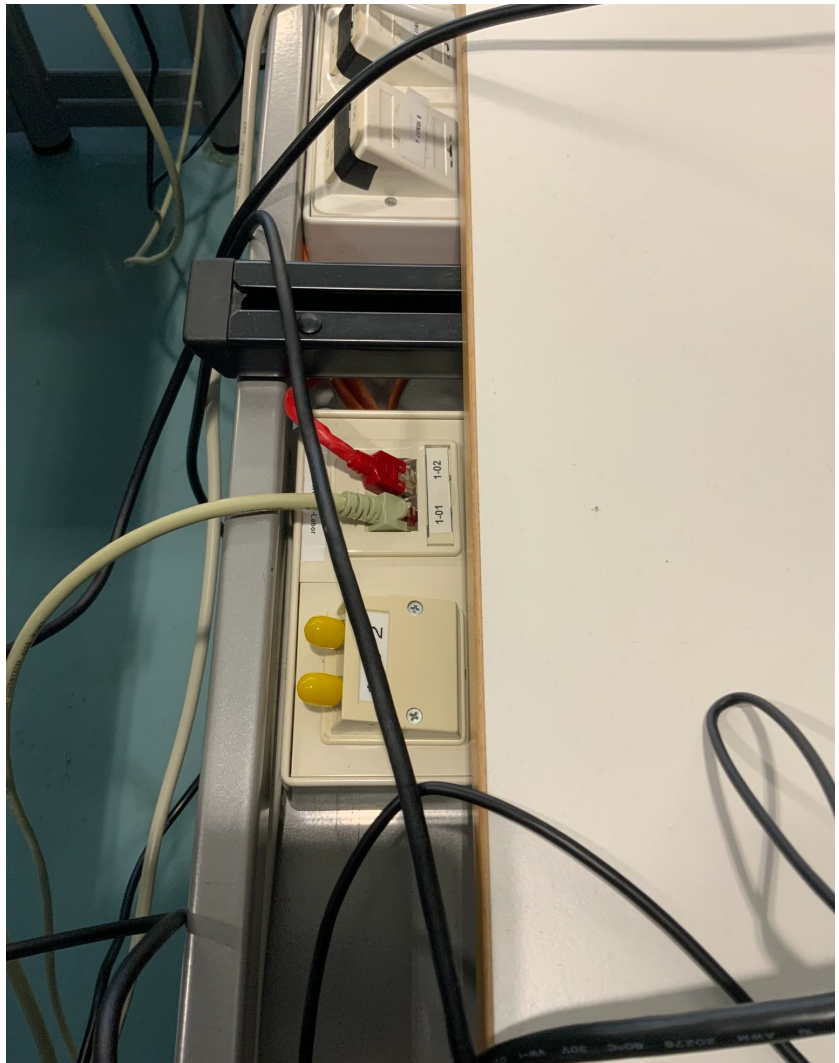
```
$ lspci
# ...
00:1f.6 Ethernet controller: Intel Corporation Ethernet Co
# ...
$ find /sys | grep drivers.*00:1f.6
# ...
/sys/bus/pci/drivers/e1000e/0000:00:1f.6
```

Anschluss des PC an das Labornetz

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

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
    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 qd
    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 dyna
       valid_lft 11902sec preferred_lft 11902sec
```

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

Hier wird ein anderer Laborrechner, `141.62.66.4`, angepingt.

```
$ ping 141.62.66.4
```

Adress Resolution Protocol ARP

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 REACHA
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 141.62.66.236
PING 141.62.66.236 (141.62.66.236) 56(84) bytes of data.
```

Ping

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
  -I <interface>     either interface name or address
  -i <interval>      seconds between sending each packet
  -L                 suppress loopback of multicast packets
```

Traceroute & MTR

Traceroute & MTR

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

```
$ traceroute de-cix.net
traceroute to de-cix.net (46.31.121.136), 30 hops max, 60 b
 1  opnsense-router.rnlabor.hdm-stuttgart.de (141.62.66.250
 2  ciscovlgw318.hdm-stuttgart.de (141.62.31.246)  2.047 ms
 3  firewall-h.hdm-stuttgart.de (141.62.1.1)  1.118 ms  1.4
 4  * * *
 5  stu-al30-1-te0-0-0-17.belwue.net (129.143.56.53)  3.625
 6  stu-nwz-a99-hu0-3-0-5.belwue.net (129.143.56.106)  3.03
 7  fra-decix-1-hu0-0-0-4.belwue.net (129.143.60.113)  5.14
 8  sgw2-te-0-0-2-3-ixp.fra.de-cix.net (80.81.194.116)  7.2
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
```

SS

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 device confi
URL          : http://kernel.org/pub/linux/utils/net/iprout
License      : GPLv2+ and Public Domain
Description  : The iproute package contains networking util
             : for example) which are designed to use the a
             : capabilities of the Linux kernel.
```

Gehen Sie ins www und beobachten Sie die Veränderungen

Route

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 src 14
broadcast 127.0.0.0 dev lo table local proto kernel scope l
local 127.0.0.0/8 dev lo table local proto kernel scope hos
local 127.0.0.1 dev lo table local proto kernel scope host
broadcast 127.255.255.255 dev lo table local proto kernel s
broadcast 141.62.66.0 dev enp0s31f6 table local proto kerne
local 141.62.66.5 dev enp0s31f6 table local proto kernel sc
broadcast 141.62.66.255 dev enp0s31f6 table local proto ker
```

Nmap

Nmap

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

Es gibt verschiedene Möglichkeiten Scans durchzuführen, der gängige (auch default) ist der `TCP Connect Port Scan`. Es gibt noch weitere, welche situativ über Flags verwendet werden können:

```
-sS   TCP SYN Port Scan
-sA   TCP ACK Port Scan
-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 einz
$ nmap 10.10.247.15 10.10.247.240      # Scannen mehrerer I
$ nmap 10.10.247.15-240                # Scannen des Bereic
$ nmap scanme.nmap.org                 # Scannen der Domain
```