Abteilung für INFORMATIK

HTL ST. PÖLTEN

Titel: Labor 8

Klasse: 3BHIF

Name: Haiden

Gruppe: 01

Aufgabe: 04.03.2020 Abgabe: 18.03.2020

Inhaltsverzeichnis

1 Netzwerk – Labor 9

1.1 Geben Sie die aktuelle Netzwerkkonfiguration an. Stellen sie die Netzwerkeinstellung der Virtualbox auf Bridged um. Was bedeutet das?

Um sich Informationen zum Netzwerk-Interface anzeigen zu lassen, kann man den Befehl `ip a` ausführen. Dieser Befehl ersetzt in aktuellen Linux-Versionen den Befehl ifconfig, mit dem man sich vorher Informationen über die Netzwerkkarte geholt hat.

Bridged bedeutet, dass der virtuelle Netzwerkadapter der Virtualbox über den echten in den PC eingebauten Netzwerkadapter geleitet wird und im Netzwerk quasi als eigener PC erscheint. Dabei wird der gesamte Traffic über die Netzwerkkarte des echten PCs geroutet.

```
: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
group default qlen 1000

    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

    inet6 ::1/128 scope host

       valid_lft forever preferred_lft forever

2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast state UP group default qlen 1000

    link/ether 08:00:27:24:ec:96 brd ff:ff:ff:ff:ff:ff

    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic
noprefixroute enp0s3

       valid_lft 82325sec preferred_lft 82325sec

    inet 10.140.0.34/16 brd 10.140.255.255 scope global dynamic
noprefixroute enp0s3

       valid_lft 86392sec preferred_lft 86392sec

    inet6 fe80::a00:27ff:fe24:ec96/64 scope link noprefixroute

       valid_lft forever preferred_lft forever
```

1.2 Stoppen Sie den Network-Manager Dienst

Um den Network-Manager Dienst zu stoppen, muss man einfach folgenden Befehl eingeben:

```
sudo systemctl stop network-manager
```

Netzwerk – Labor 9

1.3 Konfigurieren Sie folgende Netzwerkparameter (Befehl ip):

IP-Adresse 192.168.100.KNR und 192.168.101.KNR

Netzmaske 255.255.255.0

Gateway: 192.168.100.254

IP-Adressen ändern:

```
schueler@Debian10nvs:~$ sudo ip a change 192.168.100.6 dev enp0s3

schueler@Debian10nvs:~$ sudo ip a add 192.168.101.6 dev enp0s3

schueler@Debian10nvs:~$ ip addr

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
group default qlen 1000

    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

    inet6 ::1/128 scope host

       valid_lft forever preferred_lft forever

2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast state UP group default qlen 1000

    link/ether 08:00:27:24:ec:96 brd ff:ff:ff:ff:ff:ff

    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic
noprefixroute enp0s3

       valid_lft 81549sec preferred_lft 81549sec

    inet 10.140.0.34/16 brd 10.140.255.255 scope global dynamic
noprefixroute enp0s3

       valid_lft 85906sec preferred_lft 85906sec

    inet 192.168.100.6/32 scope global enp0s3

       valid_lft forever preferred_lft forever

    inet 192.168.101.6/32 scope global enp0s3

       valid_lft forever preferred_lft forever

    inet6 fe80::a00:27ff:fe24:ec96/64 scope link noprefixroute

       valid_lft forever preferred_lft forever
```

Netzmaske ändern:

```
sudo ip a change 192.168.100.6/255.255.255.0 dev enp0s3

sudo ip a change 192.168.101.6/255.255.255.0 dev enp0s3
```

Netzwerk – Labor 9

Standard-Gateway ändern:

```
schueler@Debian10nvs:~$ sudo ip route replace 192.168.100.254 dev
enp0s3

schueler@Debian10nvs:~$ sudo ip route replace 192.168.100.254 dev
enp0s3

schueler@Debian10nvs:~$ ip route

default via 10.0.2.2 dev enp0s3 proto dhcp metric 100

default via 10.140.255.254 dev enp0s3 proto dhcp metric 100

10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric
100

10.140.0.0/16 dev enp0s3 proto kernel scope link src 10.140.0.34
metric 100

192.168.100.0/24 dev enp0s3 proto kernel scope link src
192.168.100.106

192.168.100.254 dev enp0s3 scope link

192.168.101.0/24 dev enp0s3 proto kernel scope link src
192.168.101.7
```

1.4 Tragen Sie die IP-Einstellungen fix ein. Welche Datei kommt dabei zum Einsatz? Welcher Dienst muss neu gestartet werden?

Um die IP-Einstellungen fix in die Dateien einzutragen, öffnet man in Debian's Fall die Datei `/etc/network/interfaces` eintragen. Damit diese Einstellungen aktiv werden, muss der Network-Manager neugestartet werden.

Syntax für einen Eintrag in der `interfaces` – Datei:

```
iface <INTERFACE> inet static

address <ADRESSE>

netmask <NETZMASKE>

gateway <GATEWAY_IP>
```

Wenn man nun die Beispiele von oben nimmt, sehen die Einträge dann so aus:

```
auto enp0s3

iface enp0s3 inet static

address 192.168.100.7

netmask 255.255.255.0

gateway 192.168.100.254
```

```
auto enp0s3
```

Netzwerk – Labor 9

```
iface enp0s3 inet static
address 192.168.101.7
netmask 255.255.255.0
gateway 192.168.100.254
```

Um die Einstellungen zu bekommen, muss der `networking` – Dienst neugestartet werden.

1.5 Ändern Sie die Konfiguration auf DHCP. Welche Einstellungen ergeben sich?

Um die Konfiguration auf DHCP zu ändern, einfach alle anderen Zeilen auskommentieren und diese Zeile einfügen:

```
iface enp0s3 inet dhcp
```

Danach muss wie beim vorherigen Beispiel der `networking` – Dienst neugestartet werden.

Nach dem der Networking Dienst neugestartet wurde, ergeben sich folgende Einstellungen:

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
group default qlen 1000
    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
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:24:ec:96 brd ff:ff:ff:ff:ff:ff
    inet 10.140.0.44/16 brd 10.140.255.255 scope global dynamic
enp0s3
       valid_lft 86387sec preferred_lft 86387sec
```

1.6 Welche Aufgabe hat der Befehl arp (ip neighbor). Geben Sie die wichtigsten Parameter an. Welche Einträge sehen Sie im Arp-Cache? Senden Sie einen Ping an einen Nachbarrechner. Was ändert sich?

Der ARP-Befehl, oder auch in modernen Versionen `ip neighbour`, listet von den IP-Adressen die dazugehörigen MAC-Adressen auf. Dabei werden diese in einer ARP-Tabelle (Address Resolution Protocol) gespeichert. Mit dem Befehl kann man diese auflisten.

Die wichtigsten Parameter:

Add | del | change | replace: Einträge in die ARP-Tabelle hinzufügen / löschen / ändern / ersetzen

Show: Um die ARP-Tabelle aufzulisten, kann aber weggelassen werden.

Flush: Mit diesem Befehl wird die gesamte ARP-Tabelle gecleared und ist danach leer.

Ausgabe des derzeitigen ARP-Cache / Tabelle:

Netzwerk – Labor 9

```
schueler@Debian10nvs:~$ ip n
10.140.0.43 dev enp0s3 lladdr 08:00:27:7d:1b:13 STALE
10.140.255.254 dev enp0s3 lladdr b0:8b:cf:03:e7:07 STALE
10.140.255.253 dev enp0s3 lladdr 2c:44:fd:25:29:20 STALE
```

Nach einem Ping-Versuch wird der angepingte Computer in die ARP-Tabelle hinzugefügt, der hinzugefügte Computer, der im ARP-Cache gelandet ist, hat die IP-Adresse 10.140.0.57.

```
schueler@Debian10nvs:~$ ping 10.140.0.57
PING 10.140.0.57 (10.140.0.57) 56(84) bytes of data.
64 bytes from 10.140.0.57: icmp_seq=1 ttl=64 time=2.18 ms
64 bytes from 10.140.0.57: icmp_seq=2 ttl=64 time=1.04 ms
64 bytes from 10.140.0.57: icmp_seq=3 ttl=64 time=1.04 ms
^C
--- 10.140.0.57 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 5ms
rtt min/avg/max/mdev = 1.040/1.422/2.184/0.540 ms
schueler@Debian10nvs:~$ ip neighbor
10.140.0.57 dev enp0s3 lladdr 08:00:27:74:45:67 REACHABLE
10.140.0.43 dev enp0s3 lladdr 08:00:27:7d:1b:13 STALE
10.140.255.254 dev enp0s3 lladdr b0:8b:cf:03:e7:07 STALE
10.140.255.253 dev enp0s3 lladdr 2c:44:fd:25:29:20 STALE
```

Die ARP-Tabelle hat folgenden Aufbau:

Zuerst die IP-Adresse des betroffenen Computers, danach das Interface wovon darauf zugegriffen wurde, gefolgt von der physischen MAC-Adresse welche aufgelöst wurde und danach der Status.

1.7 Welche Aufgabe hat der Befehl ping. Schicken Sie einen Ping an das Gateway (ip route). Wie können Sie die Größe des Payloads angeben?

Mit dem Befehl `ping` wird eine ICMP (Echo) – Nachricht versendet, die dafür verwendet wird, um festzustellen, ob ein Computer / Gerät noch aktiv oder inaktiv ist. Ist das Gerät aktiv und werden Ping-Befehle von der Firewall nicht geblockt, antwortet das Gerät mit einer Echo-Nachricht zurück.

Ping an den Gateway:

```
schueler@Debian10nvs:~$ ping 10.140.255.254
PING 10.140.255.254 (10.140.255.254) 56(84) bytes of data.
64 bytes from 10.140.255.254: icmp_seq=1 ttl=255 time=0.746 ms
64 bytes from 10.140.255.254: icmp_seq=2 ttl=255 time=0.973 ms
64 bytes from 10.140.255.254: icmp_seq=3 ttl=255 time=0.943 ms
```

```
^C
--- 10.140.255.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 12ms
rtt min/avg/max/mdev = 0.746/0.887/0.973/0.103 ms
```

Mit dem Parameter `-s` kann man die Paketgröße angeben:

```
schueler@Debian10nvs:~$ ping -s 256 10.140.0.44
PING 10.140.0.44 (10.140.0.44) 256(284) bytes of data.
264 bytes from 10.140.0.44: icmp_seq=1 ttl=64 time=0.031 ms
264 bytes from 10.140.0.44: icmp_seq=2 ttl=64 time=0.063 ms
264 bytes from 10.140.0.44: icmp_seq=3 ttl=64 time=0.063 ms
264 bytes from 10.140.0.44: icmp_seq=4 ttl=64 time=0.062 ms
^C
--- 10.140.0.44 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 73ms
rtt min/avg/max/mdev = 0.031/0.054/0.063/0.016 ms
```

1.8 Welche Aufgabe hat der Befehl traceroute. Geben Sie die wichtigsten Parameter an.

Mit dem Befehl traceroute sieht man die Stationen, an denen das Paket vorbeikommt bzw. durch welche Knoten es geroutet wird.

Die wichtigsten Parameter:

Mit den `-4 / -6` kann man angeben ob Traceroute im IPv4 bzw. IPv6 Modus arbeiten soll.

Mit `-g` kann man den Gateway, über den das Paket geroutet werden soll, laufen soll.

Mit `-i` kann man das Interface bestimmen, über den das Paket laufen soll. Hat man z.B. eine zweite Netzwerkkarte, so kann man diese hier angeben.

1.9 Welche Aufgabe hat der Befehl netstat.(ss) Geben Sie die wichtigsten Parameter an. Welche Ports sind auf Ihrem PC geöffnet?

Mit netstat sieht man alle offenen Verbindungen, über welche Adressen und Ports diese jeweiligen Verbindungen gehen. Man sieht welche Ports für Anfragen offen sind (LISTENING).

Wichtigste Parameter:

Mit `-4` kann man sich die geöffneten IPv4 Sockets anzeigen lassen.

Mit `-6` kann man sich die geöffneten IPv6 Sockets anzeigen lassen.

Mit `-t` kann man sich geöffnete TCP Sockets anzeigen lassen.

Mit `-u` kann man sich nur die UDP Sockets anzeigen lassen.

Netzwerk – Labor 9

Um seine offenen Ports zu sehen, kann man einfach ss eingeben:

```
Peer Address:Port

u_str                       ESTAB                       0
0
* 5796111
* 5796110

u_str                       ESTAB                       0
0
* 21800
* 21121

u_str                       ESTAB                       0
0
/var/run/dbus/system_bus_socket 13645
* 13644

u_str                       ESTAB                       0
0                             @/containerd-
shim/moby/f3ffc83e1d76d3a66eeba7aae282d3d851f5a1ea74a77ed1d6cc2ffa53
a44463/shim.sock@ 20948
* 21651

u_str                       ESTAB                       0
0
* 13644
* 13645

u_str                       ESTAB                       0
0
/run/containerd/containerd.sock 16385
* 15360

u_str                       ESTAB                       0
0                             @/containerd-
shim/moby/6c9bd27176636c7886529a125d2900d386687bb6fd8cc014e302537f45
bea86f/shim.sock@ 21121
* 21800
```