Titel: NSCS Labor 1

AufgabeNr: 1

Klasse: 3AHIF

Name: Ertl Maximilian

Gruppe: 1

Abgabetermin: 09.11.2022

Abgabedatum: 06.11.2022

Kurzbeschreibung:

Übung mit IP, ARP und ICMP in der Linux Kommandozeile

Inhaltsverzeichnis

1 IP 1
1.1 IP-Adresse abrufen 1
2 ARP 1
2.1 ARP-Cache 1
3 ICMP 2
3.1 Neuer Ping 2
3.2 ICMP Payload 3

1 IP

1.1 IP-Adresse abrufen

Mit dem Befehl ***ip adress*** kann man sich seine eigene IP-Adresse ansehen, welche in diesem Fall 10.140.0.92 ist.

```
schueler@debian11:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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 08:00:27:79:2d:c5 brd ff:ff:ff:ff:ff:ff
    inet 10.140.0.92/16 brd 10.140.255.255 scope global dynamic noprefixroute en
p0s3
       valid_lft 2114sec preferred_lft 2114sec
    inet6 fe80::a00:27ff:fe79:2dc5/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOW
N group default
    link/ether 02:42:d1:69:b4:8d brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
```

2 ARP

2.1 ARP-Cache

Man kann sich den ARP-Cache mit dem Befehl ***sudo arp –a*** ausgeben lassen.

```
schueler@debian11:~$ sudo arp -a
[sudo] Passwort für schueler:
? (10.140.0.96) auf 08:00:27:6d:65:e8 [ether] auf enp0s3
? (10.140.0.94) auf 08:00:27:26:01:bd [ether] auf enp0s3
? (10.140.255.254) auf b0:8b:cf:03:e7:07 [ether] auf enp0s3
schueler@debian11:~$
```

Nach dem ich den Rechner meines Nachbars gepingt habe wurde dieser im ARP-Cache angezeigt.

```
schueler@debian11:~$ sudo arp -a
[sudo] Passwort für schueler:
? (10.140.0.96) auf 08:00:27:6d:65:e8 [ether] auf enp0s3
? (10.140.0.94) auf 08:00:27:26:01:bd [ether] auf enp0s3
? (10.140.255.254) auf b0:8b:cf:03:e7:07 [ether] auf enp0s3
schueler@debian11:~$ ping 10.140.0.97
PING 10.140.0.97 (10.140.0.97) 56(84) bytes of data.
64 bytes from 10.140.0.97: icmp_seq=1 ttl=64 time=1.97 ms
64 bytes from 10.140.0.97: icmp_seq=2 ttl=64 time=1.99 ms
^C
--- 10.140.0.97 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.972/1.983/1.994/0.011 ms
schueler@debian11:~$ sudo arp -a
? (10.140.255.254) auf b0:8b:cf:03:e7:07 [ether] auf enp0s3
? (10.140.0.97) auf 08:00:27:f9:9d:d8 [ether] auf enp0s3
? (10.140.0.94) auf 08:00:27:26:01:bd [ether] auf enp0s3
? (10.140.0.96) auf 08:00:27:6d:65:e8 [ether] auf enp0s3
schueler@debian11:~$
```

Mit ***man arp*** kann man sich die “man” Seiten ansehen, welche eine genauere Beschreibung bieten als z.B. sudo arp –h

```
schueler@debian11:~$ sudo arp -h
Benutzung:
  arp [-vn]  [<HW>] [-i <if>] [-a] [<Hostname>]
  arp [-v]          [-i <if>] -d  <host> [pub]              <-Delete ARP entry
  arp [-vnD] [<HW>] [-i <if>] -f  [<filename>]            <-Add entry from file
  arp [-v]   [<HW>] [-i <if>] -s  <host> <hwaddr> [temp]            <-Add entry
  arp [-v]   [<HW>] [-i <if>] -Ds <host> <if> [netmask <nm>] pub          <-''-

        -a                      Alle Hosts im BSD-Format anzeigen
        -e                      display (all) hosts in default (Linux) style
        -s, --set               Neuen ARP-Eintrag setzen
        -d, --delete            Einen bestimmten Eintrag löschen
        -v, --verbose           Ausführliche Ausgaben
        -n, --numeric           don't resolve names
        -i, --device            Netzwerkgerät (z.B. eth0) angeben
        -D, --use-device        <hwaddr> von gegebenem Gerät lesen
        -A, -p, --protocol              Routentabelle anzeigen
        -f, --file              Neue Einträge aus Datei lesen

  <HW>='-H <hw>' um Hardwareadresstyp anzugeben.  Standard: ether
  Liste möglicher Hardwaretypen, die ARP unterstützen:
    ash (Ash) ether (Ethernet) ax25 (AMPR AX.25)
    netrom (AMPR NET/ROM) rose (AMPR ROSE) arcnet (ARCnet)
    dlci (Frame Relay DLCI) fddi (Fiber Distributed Data Interface) hippi (HIPPI)
    irda (IrLAP) x25 (generic X.25) eui64 (Generic EUI-64)
```

man arp

```
OPTIONEN
       -v, --verbose
              Ausführlichere Ausgaben.

       -n, --numeric
              Numerische  Adressausgaben  anstatt zu versuchen, den symbolischen
              Rechner-, Port- oder Benutzernamen zu ermitteln.

       -H Typ, --hw-type Typ
              Beim Setzen oder Auslesen des  ARP-Caches  schränkt  diese  Option
              ein,  auf  welcher  Klasse  von  Einträgen arp operieren soll. Der
              Standardwert dieses Arguments ist ether  (d.h.  Hardwarecode  0x01
              für  IEEE 802.3 10Mbps Ethernet). Andere mögliche Werte sind Netz-
              werkstechnologien so wie z.B. ARCnet  (arcnet),  PROnet  (pronet),
              AX.25 (ax25) und NET/ROM (netrom).

       -a [Rechnername], --display [Rechnername]
              Zeigt die Einträge der angegebenen Rechner an. Wird kein hostname-
              Argument verwendet, so werden alle Einträge aufgelistet.

       -d Rechnername, --delete Rechnername
              Alle Einträge für den angegebenen Host entfernen. Dies  kann  z.B.
              benutzt werden, wenn ein System angehalten wird.
```

Mit dem Befehl ***sudo arp –s*** kann man einen neuen ARP-Eintrag setzen.

3 ICMP

3.1 Neuer Ping

Zuerst muss man mit ***sudo apt install wireshark*** installieren um die Pakete die gesendet und empfangen werden zu sehen.

Es wird mit einem Broadcast begonnen in dem gefragt "Who has this “IP-Adress”“ gefragt wird.

Mit einem ARP-Reply wird dann mit der gesuchten Mac- und IP-Adresse geantwortet und diese Adressen werden dann im ARP-Chache gespeichert und bleit dort für eine unbestimmte Zeit meistens 5 bis 10 Minuten.

Dann kommt das Internet Control Message Protocol (ICMP) zum Einsatz, um zu kommunizieren.

3.2 ICMP Payload

Zuerst werden nur Fragmented IPv4 Pakete gesendet und am Ende wird erst ein ICMP-Paket gesendet.

Am Ende sind keine Screenshots mehr vorhanden da es bei mir zuhause einen Fehler in der Virtuellen Maschine gab und ich trotz dem installieren des net-tools Pakets keinen ARP Befehl ausführen konnte.