OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

Fakultät Informatik und Mathematik

COMLAB
Datenkommunikation und Netzwerke

Prof. Dr. Waas

Praktikum zum Fach

**Kommunikationssysteme/
Rechnernetze**

Übung

TCPIP 3

IP und Routing

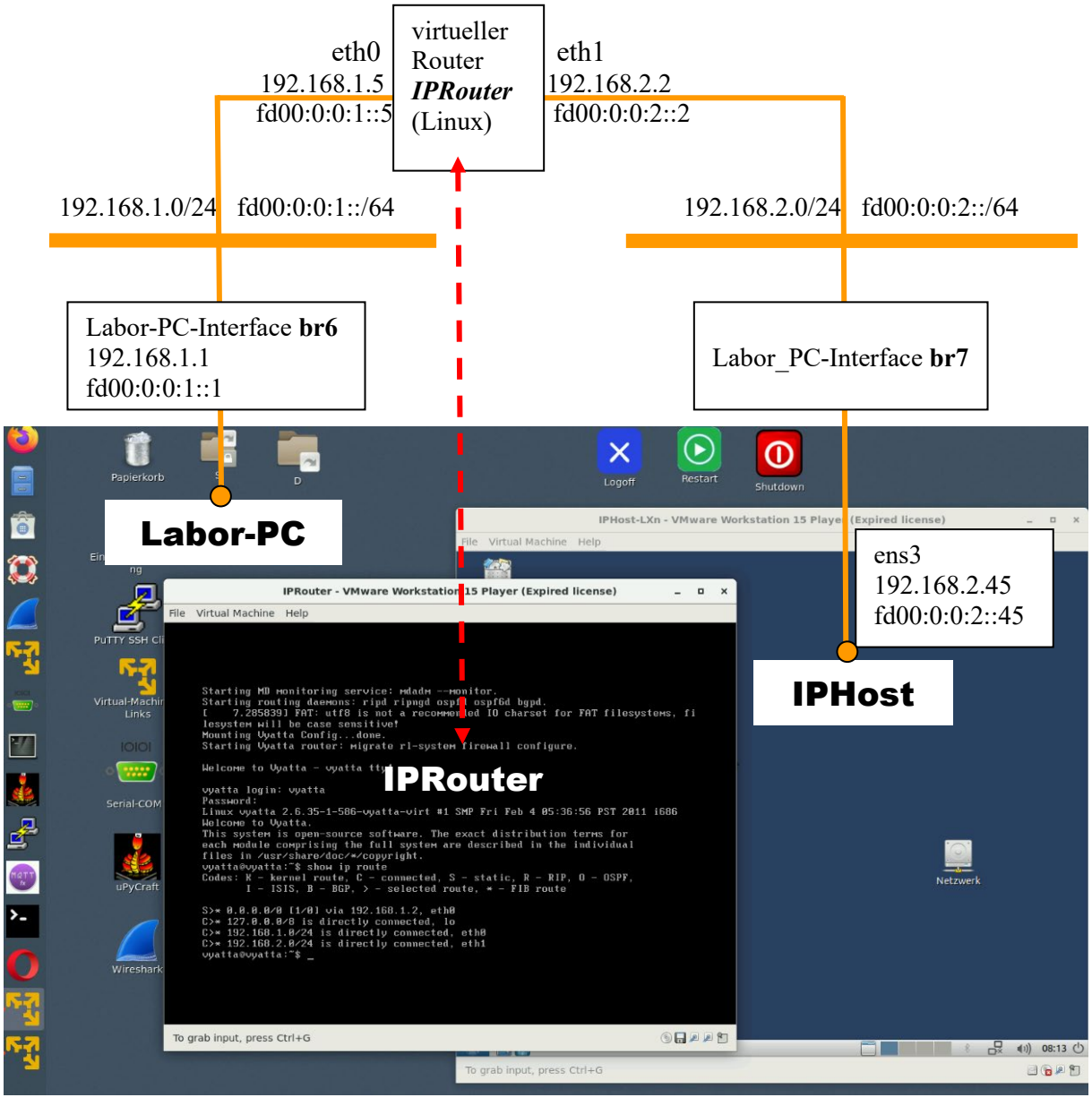
Linux

(Version 16.11.2022 KVM)

1 EINFÜHRUNG

Die folgenden Übungen der Netzwerkanalyse werden in einer virtuellen Umgebung auf dem Labor-PC durchgeführt. Dazu werden sog. virtuellen Maschinen verwendet die auf Basis von VMWare (R) mit dem VMWare Player betrieben werden.
Im Internetbetrieb ist die Dual Stack Methode der aktuelle Stand der Technik. Daher können die folgenden Übungen neben IPv4 auch mit IPv6 durchgeführt werden.

Auf dem Labor-PC sind 2 virtuelle Ethernetinterface installiert: **br6** und **br7**. Über diese Interface ist der Labor-PC mit dem Subnetz **br6 = 192.168.1.0/24 (IPv6: fd00:0:0:1::/64)** bzw. **br7 = 192.168.2.0/24 (IPv6: fd00:0:0:2::/64)** verbunden.
Der Router IPRouter soll die beiden Subnetze verbinden. Mit dem Tool „**Wireshark**“ kann auf beiden Subnetzen gleichzeitig gemessen werden. Die im Rahmen der Übung an Ihrem Arbeitsplatz erzielt Messergebnisse, dürfen Sie auf Ihrem Memorystick zur späteren Nachbearbeitung abspeichern. Sie sind am Ende des Semesters zu löschen.



2 STARTEN DER ÜBUNGSUMGEBUNG

- Öffnen Sie den Ordner **Virtual Machines Links** auf dem Desktop.
- Starten Sie die folgenden virtuellen Maschinen durch Doppelklick:
  IPRouter
  IPHost

Nun werden beide virtuelle Maschinen (=VM), gestartet. Beide VM laufen mit Linux und sind bereits voreingestellt und es braucht dort nichts verändert zu werden.

3 ROUTINGINFORMATIONEN

- Starten Sie die Eingabeaufforderung auf dem lokalen **Labor-PC und** auf dem virtuellen **IPHost**.
- Führen Sie am **Labor-PC** das Programm **routen aus** (liegt auf dem Desktop)! Damit werden die korrekten Routen der Übung und die Subnetze für br6 und br7 eingestellt.

- Geben Sie folgenden Befehle am **Labor-PC** und am **IPHost** ein, um die aktuelle Routingtabelle auszulesen:

  am Labor-PC: `route -4 -6`
  am IPHost: `route -4 -6`

  Am Labor-PC müsste u.a. folgende Route angezeigt werden:
  192.168.2.0 192.168.1.5 255.255.255.0 UG 0 0 0 br6
  Falls nicht, haben Sie **routen** nicht ausgeführt (s. oben) !

- Klicken Sie auf das Fenster in dem **IPRouter** läuft.
- Loggen Sie sich ein mit dem Benutzernamen **vyatta** und dem Passwort **vyatta** ein.
- Geben Sie folgenden Befehle ein um die aktuelle Routingtabelle auszulesen:

```
show ip route
show ipv6 route
```

- Analysieren Sie die Routingtabellen für IPv4 und IPv6 und ermitteln Sie, ob ein Weg zwischen Labor-PC und IPHost besteht und falls ja, wie dieser Weg verläuft.

Mit den Tasten **<Strg> <Alt>** schalten Sie Tastatur und Maus zurück auf den Labor-PC!

Kontrollfragen

- ☑ Wohin sendet der Labor-PC Pakete für Subnetz 192.168.2.0/24 bzw. fd00:0:0:2::/64 ?
- ☑ Wohin sendet der IPHost Pakete für Subnetz 192.168.1.0/24 bzw. fd00:0:0:1::/64 ?
- ☑ Zu welchem Interface leitet der IPRouter welche Pakete weiter?
- ☑ Wohin zeigt die Defaultroute am Labor-PC?

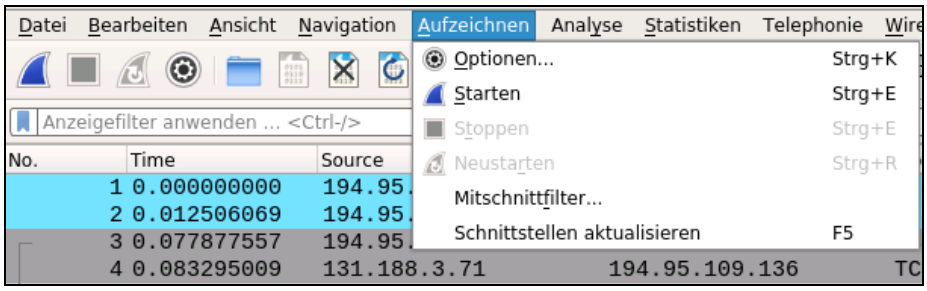
Überprüfung der Ergebnisse

- Überprüfen Sie Ihre Ergebnisse, indem Sie mit dem Programm **traceroute** die tatsächlichen Routen überprüfen.

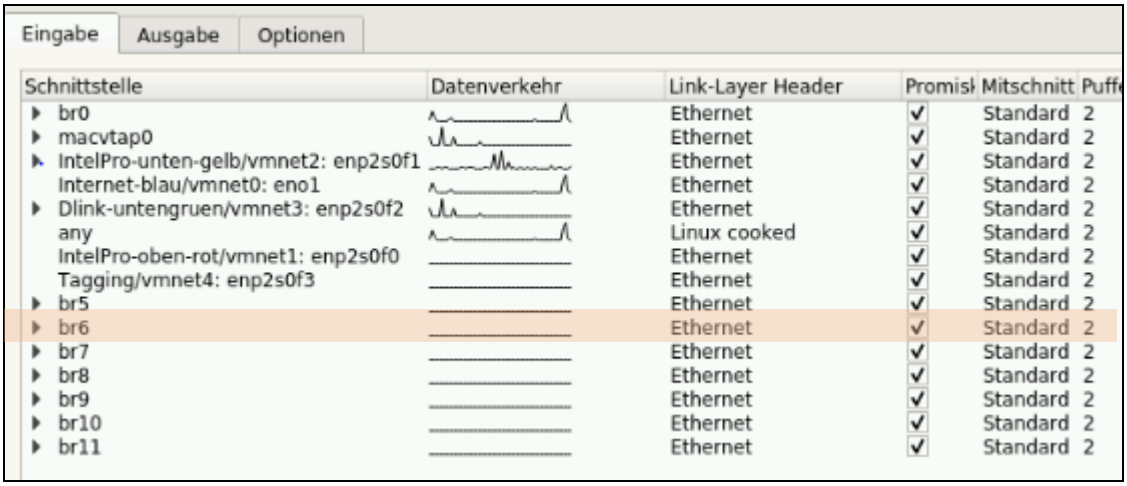
auf dem Labor-PC	auf dem IPHost
`traceroute -I 192.168.2.45` `traceroute6 fd00:0:0:2::45`	`sudo traceroute -I 192.168.1.1` `sudo traceroute6 fd00:0:0:1::1`

4 IPv4 ANALYSE MIT WIRESHARK

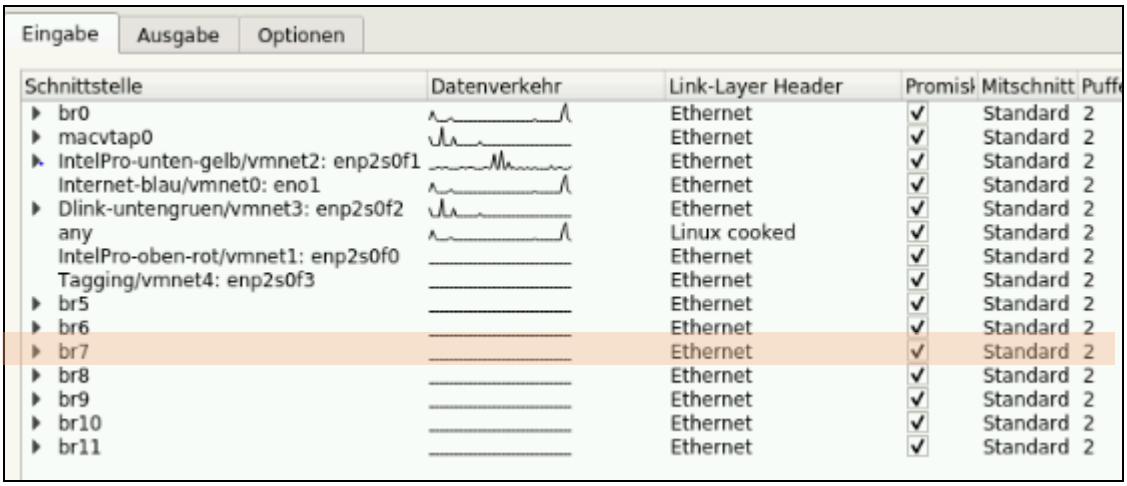
- Starten Sie auf dem lokalen Labor-PC das Programm **WireShark**
- Öffnen Sie das **Aufzeichnen Menü** und wählen Sie **Optionen...** aus.



- Wählen Sie Interface **br6** aus und klicken Sie auf den **Start**-Button (kein Mittschnittfilter). Damit kann Wireshark auf dem Subnetz br6 = 192.168.1.0 (IPv6: fd00:0:0:1::) alle Datenpakete sehen und aufzeichnen. Klicken Sie auf den **Start**-Button um die Messung zu starten.

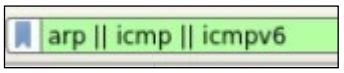


- Starten Sie das Programm Wireshark noch einmal. Öffnen Sie dort das **Aufzeichnen** Menü und klicken Sie auf **Optionen**. Wählen Sie diesmal das Interface **br7** aus und klicken auf den **Start**-Button. Damit kann der zweite Wireshark im Subnetz br7 = 192.168.2.0 (IPv6: fd00:0:0:2::) messen und aufzeichnen.



- Ordnen Sie die beiden Wireshark auf dem Desktop so an, dass Sie beide Paketfenster gleichzeitig sehen können.

- Geben Sie als Displayfilter ein: **arp || icmp || icmpv6**



- Falls noch nicht geschehen, starten Sie die Eingabeaufforderung/Terminal und geben Sie folgende Befehle ein. Zeichnen Sie mit den beiden Wireshark die übertragenen Datenpakete auf und interpretieren Sie diese. Beantworten Sie anhand der aufgezeichneten Datenmeldungen die anschließenden Kontrollfragen (-c 2 heißt 2 pings).

```
ping -c 2 192.168.1.5
ping -c 2 192.168.2.2
ping -c 2 192.168.2.45
```

Kontrollfragen:

- ☑ Warum sieht man die ersten beiden Pings im Wireshark nur an br6?
- ☑ Warum wird nur Ping zu 192.168.2.45 auch auf dem Wireshark an br7 angezeigt?
- ☑ Welches Protokoll oberhalb von IP wird für den Ping verwendet. Und welche Kommandos innerhalb dieses Protokolls werden benutzt?
- ☑ Vergleichen Sie die IP-Identifikationen (IP-Header) der Meldungen beim letzten Ping auf beiden Wireshark und finden Sie die korrespondierenden Meldungen! Welche Protokoll-Schichten hat der Router bei der Weiterleitung an den korrespondierenden Meldungen verändert und welche nicht?
- ☑ Wurde der IP-Header bzw. IP-Adressen beim Routing verändert?
- ☑ Wurden die MAC-Adressen verändert beim Routing?
- ☑ Welche MAC-Adressen waren in welchem Subnetz zu sehen?
- ☑ Wozu wird bei IPv4 das ARP Protokoll benötigt?
- ☑ Welche Adresse wird mittels ARP in br6 und welche in br7 gesucht?
- ☑ Wo werden die über ARP bezogenen MAC-Adressen später verwendet?
- ☑ Warum benutzt ARP für den Request eine Ethernet-Broadcast Adresse?
- ☑ Wird die Broadcastmeldung auch auf das andere Netz weitergeleitet?

- ☑ Welche Protokollkennung hat ICMP im IP-Header?
- ☑ Wie wird die IP-Adresse im IP-Header abgebildet. Das niederwertigste Byte zuerst oder zuletzt?
- ☑ Sind die IDs im IP-Header absteigend oder aufsteigend?
- ☑ Welcher TTL wird im IP-Header verwendet. Verändert der Router beim Weiterleiten diesen Wert und falls ja, wie und warum?
- ☑ Wurden die IP-Datenpakete fragmentiert oder nicht?

5 IPv6 ANALYSE MIT WIRESHARK

Starten Sie die Eingabeaufforderung und führen Sie die folgenden Versuche via IPv6 durch. Beobachten Sie dabei die Datenübertragung mittels Wireshark und verstehen Sie die Abläufe. Beantworten Sie anhand der aufgezeichneten Datenmeldungen die anschließenden Kontrollfragen (-c 2 heißt 2 pings).

```
ping -c 2 fd00:0:0:1::5
ping -c 2 fd00:0:0:2::2
ping -c 2 fd00:0:0:2::45
```

Kontrollfragen:

- ☑ Unterscheidet sich das ICMP von IPv4 mit dem ICMP von IPv6 bezüglich des Ping?
- ☑ Es ist kein ARP Protokoll zu erkennen. Woher weiß der Router die MAC-Adresse des jeweiligen Ziels?
- ☑ Welches Protokoll wird für die Ermittlung der MAC-Adressen der unmittelbaren Nachbarn bei IPv6 verwendet?
- ☑ Haben Sie sog. Neighbor Solicitation und Neighbor advertisement Pakete aufgezeichnet? Tauchen darin die gesuchten MAC-Adressen auf?

6 TRACEROUTE

Mit Traceroute können Routen zu bestehenden Zielen erkannt werden. Dies funktioniert jedoch nur, wenn sich die Routen während der Erkennung nicht ändern. Dieses Verfahren ist in IPv4 und IPv6 möglich.

- Geben Sie als Displayfilter **arp || icmp || icmpv6 || udp** ein, weil Traceroute auch UDP Pakete verwendet. (Parameter -I verwendet nur ICMP und nur bei IPv4)
- Starten Sie das **Aufzeichnen** auf beiden Wireshark und zeichnen Sie die Datenübertragung bei der Ausführung der folgenden Kommandos auf. Interpretieren Sie die Daten und beantworten Sie die nachfolgenden Kontrollfragen.

auf dem Labor-PC	auf dem IPHost
`traceroute -I 192.168.2.45`	`sudo traceroute -I 192.168.1.1`
`traceroute6 fd00:0:0:2::45`	`sudo traceroute6 fd00:0:0:1::1`

Kontrollfragen:

- ☑ Betrachten Sie das IP-Feld TTL bei der Sendung von ICMP-Request bzw. UDP. Es hat den Wert 1. Was wird der nächste Empfänger damit machen?
- ☑ Wer sendet eine Antwort auf die erste ICMP-Request bzw. UDP Meldung und wie sieht diese aus? Was bedeutet die Antwort und was kann der Empfänger damit anfangen?
- ☑ Was passiert bei der ICMP-Request bzw. UDP Meldung mit TTL=2. Wer sendet die Antwort und wie sieht diese aus.

7 RECORD ROUTE

Für das "Erforschen" von Routen stehen auch andere Methoden zur Verfügung. Diese sind u.U. auch besser und genauer als Traceroute. Eine, für kurze Routen geeignete Methode, ist der "Record Route". Durch ein spezielles Optionsfeld im IP-Header wird der Weg, den das IP-Paket nimmt, im Optionsfeld protokolliert. Beim Empfänger kann man dem Optionsfeld die Routen dann entnehmen. Das Ping-Programm in Windows unterstützt dieses Verfahren durch Kommandozeilenparameter.

- Starten Sie das **Aufzeichnen** auf beiden Wireshark und zeichnen Sie die Datenübertragung bei der Ausführung der folgenden Kommandos auf. Interpretieren Sie die Daten und beantworten Sie die nachfolgenden Kontrollfragen.
- Geben Sie am Labor-PC folgendes Kommando in der Eingabeaufforderung ein:

  ```
  ping -c 2 -R 192.168.2.45
  ```

  Durch den Parameter -R werden im Optionsfeld des IP-Headers mehrere Einträge reserviert, in die die Routen unterwegs eingetragen werden.
- Entnehmen Sie die gefundenen Routen der Anzeige in Wireshark.

Kontrollfragen

- ☑ Wann erfolgt der erste Eintrag in das **Optionsfeld** beim ICMP Request bzw. UDP und welche Adresse wird eingetragen?
- ☑ Wie unterscheidet sich diese Adresse vom Ergebnis durch traceroute?
- ☑ Gibt es auch einen Eintrag in das Optionsfeld beim ICMP Reply?

8 TRACEROUTE IM INTERNET

Testen Sie die Methode Traceroute im Inernet.

- Beenden Sie auf einem Wireshark die laufende Messung. Starten Sie die Messung erneut aber wählen Sie jetzt das Interface **Internet blau** aus. Das ist das Interface mit Verbindung zum Internet.
- Führen Sie am **Labor-PC** einen Traceroute zu einer beliebigen IPv4 Internetadresse aus und interpretieren Sie das Ergebnis.

  z.B. traceroute -I www.heise.de oder www.strato.de

Sternchen in der Anzeige bedeuten, dass der Router nicht auf TTL exceeded reagiert hat und keine Antwort gesendet hat.

- Betrachten Sie die Aufgezeichneten Meldungen in Wireshark. Filtern Sie alle ICMP Request Meldungen und betrachten Sie TTL im IP-Header. Dort lässt sich ein Ansteigen der TTL nachvollziehen.
  Displyfilter: icmp.type==8

- Führen Sie am Labor-PC einen Traceroute zu einer beliebigen IPv6 Internetadresse aus und interpretieren Sie das Ergebnis.
  z.B. traceroute6 -q 1 www.heise.de
  (alternativ: www.kame.net, ipv6.google.com, vmserver.ipv6.fh-regensburg.de, ftp.uni-erlangen.de). Filtern Sie alle ICMPv6 Time Exceeded Packete.
  Vergleichen Sie die IPv6-Absenderadressen mit der Auflistung der Gateways im Terminalfenster. Es müsste eine Übereinstimmung geben.
  Displyfilter: icmpv6.type==3

9 ENDE DER ÜBUNG

- Beenden Sie alle **Programme** und **virtuelle Maschinen**! Im Rahmen der Übung an Ihrem Arbeitsplatz erzielte Messergebnisse können Sie im Labor auf Ihren Memorystick zur späteren Nachbearbeitung abspeichern. Gewonnene sicherheitsrelevante Informationen insbesondere Passwörter, dürfen nicht weitergegeben oder unbefugt verwendet werden. Geht leider nicht im Remotebetrieb.
- **Loggen** Sie sich aus dem Labor-PC **aus!**
- Lassen Sie den PC weiterlaufen. Er wird automatisch ausgeschaltet.

Bitte hinterlassen Sie Ihren Arbeitsplatz in ordentlichem Zustand!
Entsorgen Sie Mitgebrachtes selbst!
Schieben Sie den Stuhl an den Tisch!