



OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

Fakultät Informatik und Mathematik



Prof. Dr. Waas

**Praktikum zum Fach
Kommunikationssysteme/
Rechnernetze**

Übung

TCPIP 2

ETHERNET

Linux

(Version 16.11.2023 KVM)

1 EINFÜHRUNG

Der Labor-PC verfügt über mehrere Ethernet Schnittstellen. Die Schnittstelle mit der Bezeichnung **Internet blau (bzw: eno1)** ist mit dem Internet verbunden. Die Internetverbindung wird über die **blauen Kabel** im Labor realisiert.

In der folgenden Übung werden zuerst Ethernet Pakete aus einer vorbereiteten Mittschnitt-Datei analysiert. Später wird dann eine eigene Messung im Internet durchgeführt. Capture wird in den folgenden Übungen synonym für Mittschnitt verwendet.

2 WIRESHARK-FILTER FÜR MAC-ADRESSEN

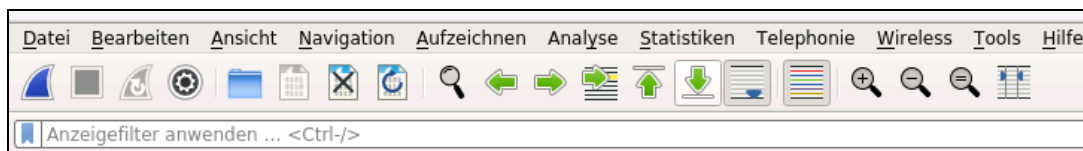
Hier wird Ihnen eine Methode vorgestellt, wie Sie Filterregeln in Wireshark erstellen, um ganz bestimmte Pakete zu finden und anzuzeigen. Es handelt sich hierbei um sog. Displayfilter. Sie wirken sich nur auf bereits aufgezeichnete Pakete aus und selektieren, welche zur Anzeige gebracht werden sollen und welche nicht.

Diese Methode ist nicht zu verwechseln mit den sog. Mittschnitt Filtern, die bereits beim Aufzeichnen greifen und filtern, welche Pakete überhaupt aufgezeichnet werden sollen.

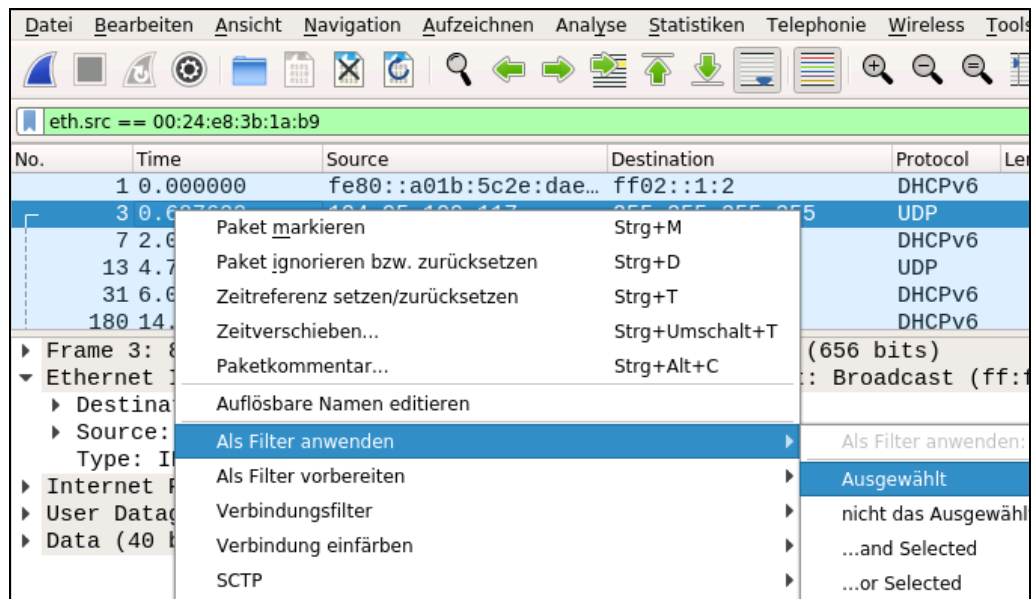
Die Methode der Displayfilter wird am Beispiel eines MAC-Adressenfilters vorgeführt. Später sollen Sie dann eigene Displayfilterregeln finden und anwenden.


Falls nicht anders angegeben erfolgen alle Eingaben am lokalen Labor-PC.

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

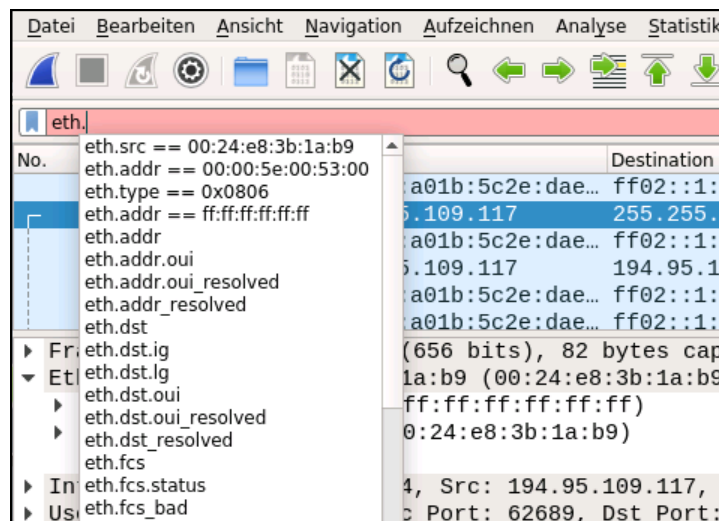


- Wählen Sie im geöffneten Dateibrowser von Wireshark die Datei **/home/kurs/D/captures/TCPIP2-Capture.pcap** (Wireshark Mittschnitt Datei) aus.
- Klicken Sie auf Paket **Nr. 3**. Im Detailfenster wird dieses Paket nun angezeigt.
- Expandieren Sie im Detailfenster das **Ethernet II**. Layer.
- Klicken Sie dann mit der rechten Maustaste auf **Source**. Wählen Sie zuerst **Als Filter Anwenden** und dann **ausgewählt**.



Die Filteranweisung wird nun automatisch als Displayfilter gesetzt und das Summary-Fenster zeigt nur noch die Pakete an, die der Filterspezifikation entsprechen. Mit  kann der Filter wieder gelöscht werden. (siehe Bild oben)

Wenn Sie die Filterregeln selbst konstruieren und eingeben wollen, werden Sie dabei von einer kleinen Hilfe in Wireshark unterstützt. Beim Eingeben der Regeln werden mögliche Vervollständigungen angezeigt. Die **grüne Hintergrundfarbe** signalisiert, dass eine syntaktisch richtige Regel eingegeben wurde. Der **Hintergrund bleibt rot**, wenn die Regel unvollständig oder falsch ist.



3 WEITERE FILTER AUF MAC-EBENE

Führen Sie nun selbständig weitere Filterversuche durch. Ermitteln Sie dabei die passende Filterregel auf Ethernet-Ebene. Entweder konstruieren Sie die Filterregel selbst oder Sie suchen ein passendes Paket und benutzen den vorher beschriebenen Weg, um die Filterregel zu erzeugen (Detailfenster ... Als Filter Anwenden...)

- Filtern Sie alle Pakete heraus, die als Zieladresse die Broadcast-Adresse haben (FF:FF:FF:FF:FF:FF). Welche höheren Protokolle verwenden diese Art der Meldungen?
- Filtern Sie alle Pakete heraus, die als Zieladresse eine Multicast Adresse haben (IG-Bit=1 und kein Broadcast). Welche höheren Protokolle verwenden diese Art der Meldungen?
- Filtern Sie alle Pakete, die IPv4 transportieren.
- Filtern Sie alle Pakete, die IPv6 transportieren.
- Filtern Sie alle Pakete heraus, die weder IPv4 noch IPv6 transportieren.
- Filtern Sie alle Pakete heraus die vom Type IPv6 sind und an eine Multicast-Adresse gesendet werden. Welche Art von Paketen ist das?
- Filtern Sie alle Pakete heraus die kürzer als die minimale Paketlänge sind. Die Filterregel dafür beginnt mit frame.len ...
- Filtern Sie alle Pakete heraus, die größer als die max. Ethernet Paketgröße sind.
- Filtern Sie alle Pakete heraus, die eine LLC haben. Filterregel: llc
- Filtern Sie alle Pakete heraus, die keine LLC haben.

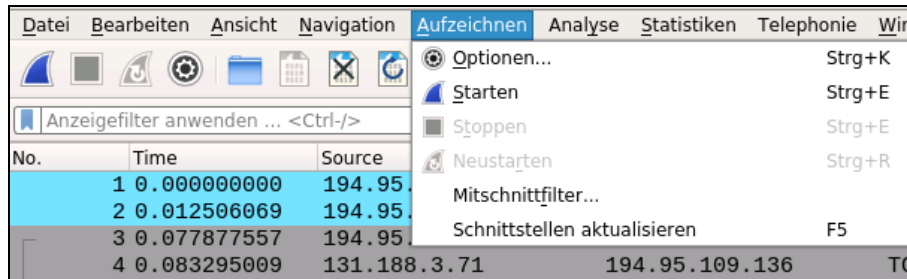
Kontrollfragen

- ☒ Mit welcher anderen Display-Filterregel könnte man LLC Ethernet Pakete noch filtern?
- ☒ Welches Bit in der Wireshark Anzeige signalisiert, dass es sich um ein Broad- oder Multicastadresse handelt?
- Löschen Sie nun alle Display Filter indem Sie in der Filterzeile auf den **Clear** Button klicken.

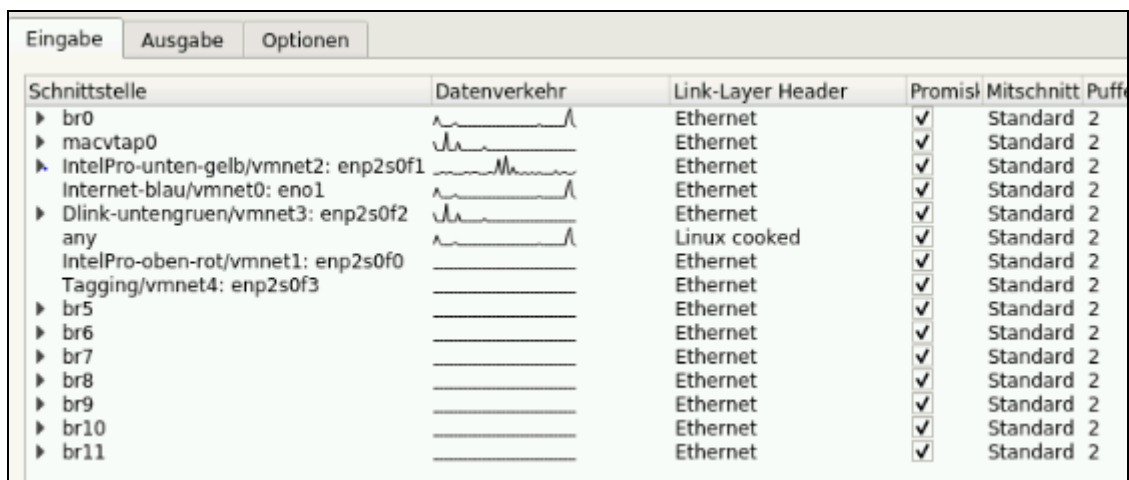
4 PAKETAUFZEICHNUNG IM NETZWERK

Nun sollen Sie eigene Messungen im Internet durchführen. Dazu muss Wireshark mit dem entsprechenden Netzwerkinterface verbunden und der sog. Aufzeichnen-Modus gestartet werden.

- Öffnen Sie das **Aufzeichnen Menü** und wählen Sie **Optionen...** aus.



- Überprüfen Sie, dass der sog. Promiskuitiv-Modus (engl. **promiscuous mode**) aktiviert ist bzw. aktivieren Sie ihn. Dieser Modus bewirkt, dass alle Pakete aufgezeichnet werden, die das Interface sieht. Ohne Promiskuitiv-Modus würden nur die Pakete aufgezeichnet, deren Zieladresse der eigenen MAC-Adresse entsprechen oder Broadcast bzw. Multicast sind.
- Wählen Sie das Interface **Internet blau** aus und klicken Sie auf den **Start**-Button.



- Sie sehen, dass alle Meldungen aufgezeichnet werden. Auch Meldungen, die man gar nicht braucht.
- Beenden Sie die Messung. Öffnen Sie dazu das **Aufzeichnen-Menü** und wählen Sie **Stoppen**.

5 AUFZEICHNUNGS FILTER

Nun sollen Aufzeichnungs-Filter angewendet werden. Zuerst soll ein Filter verwendet werden, der eine ganz bestimmte MAC-Adresse filtert:

- Im Labor: Ermitteln Sie dazu die MAC Adresse eines benachbarten Labor-PCs und tragen Sie dessen MAC-Adresse als Filterspezifikation an Ihrem Labor-PC ein.
- Bei Remotezugriff: Verwenden Sie die MAC-Adresse **9e:54:cd:0a:0d:e4**

- **Im Labor:** Ermittlung der IP- und MAC-Adresse des Nachbar-PC: Öffnen Sie auf dem Nachbar-PC die Eingabeaufforderung/Terminal und geben Sie das folgende Kommando ein:

sudo ifconfig

Es werden alle Interfaces mit IP- und MAC-Adresse ausgegeben. Notieren Sie sich beide Adressen am Interface **enol**. Tragen Sie die MAC-Adresse nachher an Ihrem Labor-PC als Wireshark-Filter ein:

- Öffnen Sie das **Aufzeichnen Menü** und wählen Sie **Mitschnittfilter...** aus.
- Klicken Sie auf + um einen neuen Filter definieren zu können.
- Geben Sie im Feld **Filter Expression** (rechte Spalte) die folgende Filterregel ein. Ersetzen Sie dabei "xx:xx:xx:xx:xx:xx" bzw. "xx-xx-xx-xx-xx-xx" mit der von Ihnen ermittelten MAC-Adresse des Nachbar-PC.

Beispiel: **ether host xx:xx:xx:xx:xx:xx**
oder: **ether host xx-xx-xx-xx-xx-xx**

Mitschnittfilter für die ausgewählte Schnittstelle: ether host 9e:54:cd:0a:0d:e4

Beispiel

- Klicken Sie auf **OK** um das *Fenster* wieder zu schließen.
- Öffnen Sie das **Aufzeichnen Menü** und wählen Sie **Options...** aus.
- Wählen Sie das Interface **Internet blau** aus.
- Klicken Sie unten bei **Mitschnittfilter für ausgewählte Schnittstelle** auf das grüne bzw. gelbe Symbol und wählen Sie aus der Liste der Mitschnittfilter den gerade von Ihnen erstellen Filter aus. Der vorherige Filter wird dann überschrieben.

Mitschnittfilter für die ausgewählte Schnittstelle: not tcp port 3389

Beispiel

```

broadcast: ether broadcast
multi and broadcast: ether broadcast or multicast
194.95.109.128/26: net 194.95.109.128/26
• Neuer Mitschnittfilter: ether host 00:0c:29:c9:a5:32
ether host 00:0c:29:c9:a5:32: ip host host.example.com
Neuer Mitschnittfilter: ether host 00:0c:29:c9:a5:32
Neuer Mitschnittfilter: net
Neuer Mitschnittfilter: ip host host.example.com
Neuer Mitschnittfilter: ip host host.example.com

```

- Klicken Sie auf **Start** um die Messung zu starten. Nun werden Sie evtl. gefragt, ob Sie die vorangegangene Messung speichern wollen. Verneinen Sie die Frage nach Speicherung!
- Veranlassen Sie am Nachbar-PC etwas Netzwerkverkehr (Web-Browser, Laufwerk S: öffnen, usw.). Im Remotebetrieb ist immer Netzwerk Traffic vom gew. Host
- Messen Sie 2 Minuten und prüfen Sie, ob Sie von dem Nachbar-PC etwas in Wireshark sehen können, außer Broadcastmeldungen. Haben Sie eine Erklärung für das Ergebnis? Warum sehen Sie nur Broadcast- und Multicast-Pakete vom Nachbar-PC?



- Pingen Sie den Nachbar-PC an. Öffnen Sie die Eingabeaufforderung und geben Sie folgendes Kommando ein:

ping x.x.x.x

Ersetzen Sie **x.x.x.x** mit der oben ermittelten IP-Adresse des Nachbar-PC oder **194.95.109.160** im Remotebetrieb.

- Jetzt müssten Sie etwas aufzeichnen können. Falls nicht, überprüfen Sie den Filter und das gewählte Mittschnitt-Interface.

Nun sollen Sie weitere Mittschnitt Filter ausprobieren. Falls nicht anders angegeben sollten nach wenigsten 1 Minute die passenden Pakete im Netz auftauchen. Verneinen Sie die Frage nach Speicherung.

Anmerkung:

Sie können neue Mitschnitt-Filter gleich im *Mitschnittstellen-Fenster* eingeben.

Schnittstelle	Datenverkehr	Link-Layer Header	Promiskuitiv	Mitschnitt
Internet-blau: eno1		Ethernet	<input type="checkbox"/>	Standard
br0		Ethernet	<input checked="" type="checkbox"/>	Standard
IntelPro-oben-rot: enp2s0f0		Ethernet	<input type="checkbox"/>	Standard
IntelPro-unten-gelb: enp2s0f1		Ethernet	<input type="checkbox"/>	Standard
Dlink-unten-gruen: enp2s0f2		Ethernet	<input type="checkbox"/>	Standard
Tagging: enp2s0f3		Ethernet	<input type="checkbox"/>	Standard
br6		Ethernet	<input checked="" type="checkbox"/>	Standard
br5		Ethernet	<input checked="" type="checkbox"/>	Standard
br11		Ethernet	<input checked="" type="checkbox"/>	Standard
br8		Ethernet	<input checked="" type="checkbox"/>	Standard
br7		Ethernet	<input checked="" type="checkbox"/>	Standard
br9		Ethernet	<input checked="" type="checkbox"/>	Standard
br10		Ethernet	<input checked="" type="checkbox"/>	Standard
br1		Ethernet	<input checked="" type="checkbox"/>	Standard
br2		Ethernet	<input checked="" type="checkbox"/>	Standard
br4		Ethernet	<input checked="" type="checkbox"/>	Standard
br3		Ethernet	<input checked="" type="checkbox"/>	Standard

☒ Promiskuitiven Modus für alle Schnittstellen aktivieren

Mitschnittfilter für die ausgewählte Schnittstelle:

- Stellen Sie die Filterregel für einen ganzen Netzbereich ein: **net 194.95.109.128/26**
- Filtern Sie nur Multicasts: **multicast**
- Filtern Sie nur Broadcast: **broadcast**
- Filtern Sie nur Multicast und Broadcast: **multicast or broadcast**
- Filtern Sie nur alle Broadcasts im Adressbereich 194.95.109.128/26. Erstellen Sie dazu selbst den geeigneten Filter.
- Filtern Sie nur ARP Pakete: **arp**

6 ARP PROTOKOLL

Jetzt soll das ARP Protokoll im Netzwerk näher untersucht werden. Das ARP Protokoll wird benötigt, um die MAC-Adressen von Nachbarstationen zu finden, von denen man nur die IP-Adresse kennt. Gelernte MAC-Adressen werden auf dem Computer im sog. ARP-Cache gespeichert um sie bei Bedarf wieder verwenden zu können.

- Öffnen Sie die Eingabeaufforderung/Terminal und sehen Sie sich den aktuellen ARP-Cache an. Geben Sie dazu folgendes Kommando ein:
`sudo arp -a` oder `sudo arp -e`
- Wählen Sie in Wireshark wieder das Interface **Internet blau** und stellen Sie einen Mittschnitt Filter ein, der nur das **ARP** Protokoll filtert.
- Löschen Sie den ganzen ARP-Cache am Labor-PC durch das Kommando:
`sudo ip -s -s neigh flush all`
- Geben sie das Kommando **ping 194.95.109.160** ein um etwas Netzwerkverkehr zu erzeugen. Alternative Adressen: 194.95.109.185, 194.95.109.129
- Analysieren Sie den ARP-Dialog zwischen Labor-PC und dem Host.



Kontrollfragen

- ☒ Warum sendet der Labor-PC den ARP Request an eine Broadcastadresse.
- ☒ Wie unterscheiden sich die Sender- und Target-Adressfelder bei ARP-Request und ARP-Reply?
- Geben Sie jetzt das Kommando **ping 194.95.104.1** ein. Hinter dieser Adresse verbirgt sich der DNS-Server. Analysieren Sie was mit Wireshark gemessen wurde.
- Beenden Sie die Aufzeichnung in Wireshark.
- Entfernen Sie den letzten Mittschnitt Filter aus der Mittschnittfilter Einstellung.

Kontrollfragen

- ☒ Sehen Sie auch einen ARP Request für 194.95.104.1?
- ☒ Und aus welchem Grund?
- ☒ Sind beide IP-Adressen im selben Subnetz?
- ☒ Wohin wird der Ping Request eigentlich gesendet. Gleichen Sie die Adresse aus Wireshark mit dem aktuellen ARP-Cache des Labor-PCs ab?
- ☒ Wer verbirgt sich hinter dieser Adresse 194.95.109.129?
- ☒ Sind unter den aufgezeichneten ARP-Request Pakete auch welche aus anderen Subnetzen? Warum ist das so?
- ☒ Wie weit breitet sich eine Broadcast-Meldung in einem Ethernet Segment aus? Wo ist die Grenze?

7 MESSUNGEN MIT IPv6

Das Gegenstück zu ARP ist in IPv6 das Neighbor Discovery (ND). Ähnlich wie bei ARP werden die MAC-Adressen von gefundenen Nachbarn in einem Neighbor-Cache gespeichert.

- Öffnen Sie die Eingabeaufforderung/Terminal und sehen Sie sich den aktuellen Neighbor-Cache an. Geben Sie dazu in der Eingabeaufforderung folgendes Kommando ein:

```
ip -6 neigh show
```

- Löschen Sie den Neighbor-Cache am Labor-PC durch das Kommando:

```
sudo ip -s -s neigh flush all
```

- Nun sollen IPv6 Pakete aufgezeichnet und analysiert werden. Das ND soll dabei etwas spezieller untersucht werden.

- Öffnen Sie das Aufzeichnen Menü und wählen Sie Optionen... aus.

- Wählen Sie das Interface Internet blau aus.

- Geben Sie im Feld **Mitschnittfilter** die folgende Filterregel ein:

```
ip6
```

- Starten Sie nun die Aufzeichnung und lassen Sie die Messung laufen, bis Sie einige DHCPv6, Router Advertisement und Neighbor Solicitation Meldungen aufgezeichnet haben. Beachten Sie, dass kein Display Filter eingestellt ist!

- Geben Sie dann in der Eingabeaufforderung das folgende Kommando ein um etwas IPv6 Traffic zu erzeugen:

```
ping -6 vmserver.oth-regensburg.de
```

- Sehen Sie sich den aktuellen Neighbor-Cache an. Geben Sie dazu in der Eingabeaufforderung folgendes Kommando ein:

```
ip -6 neigh show
```

- Beenden Sie die Aufzeichnung und analysieren Sie die aufgezeichneten Pakete. Beantworten Sie die folgenden Kontrollfragen:

Kontrollfragen:

- ☒ Betrachten Sie einen ICMPv6 Router Advertisement Paket. Welche Zieladresse hat er auf Datalink und IPv6 Ebene.
- ☒ Wie erfolgt die Abbildung der IPv6 Multicastadresse auf eine Ethernet Multicastadresse?
- ☒ Finden Sie die Neighbor Discovery Pakete für den oben "angepingten" Host. Falls Sie keine aufgezeichnet haben, löschen Sie wieder den Neighbor-Cache und wiederholen Sie den ping.
 - Welche MAC-Adresse ist beim Neighbor Solicitation im ICMPv6-Header als Link-Layer-Adresse angegeben?
 - Welche MAC-Adresse ist beim Neighbor Advertisement im ICMPv6-Header als Link-Layer-Adresse angegeben?
- ☒ Vergleichen Sie die mit Wireshark gefundene Adresse für den o. g. Host mit dem Ergebnis aus dem Neighbor-Cache.

8 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!