OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

Fakultät Informatik und Mathematik

COMLAB
Datenkommunikation und Netzwerke

Prof. Dr. Waas

Praktikum zum Fach

**Kommunikationssysteme/
Rechnernetze**

Übung

DHCP / DHCPv6

Linux

(Version 27.02.2022 KVM)

1 EINFÜHRUNG

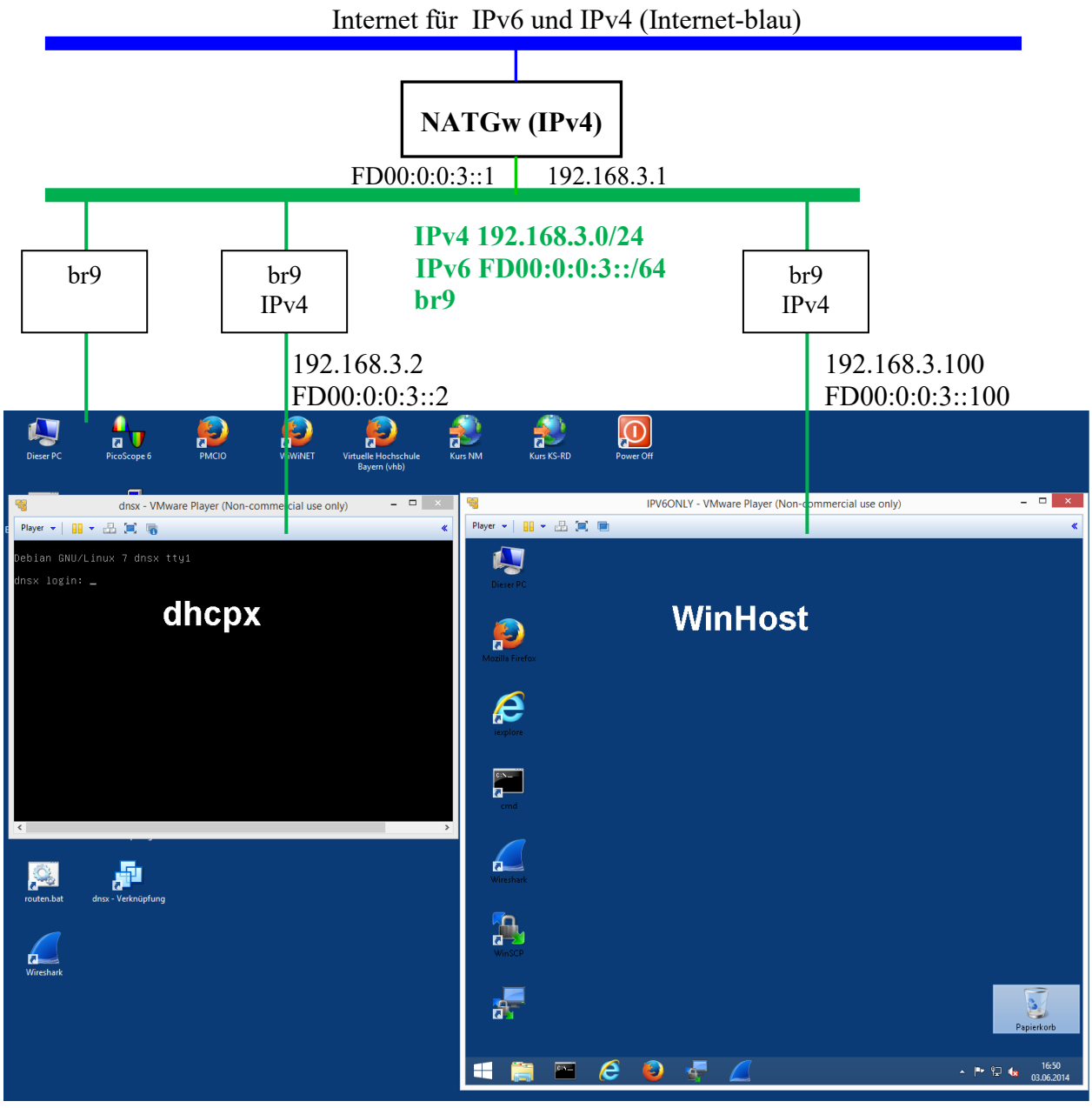
Die folgenden Übungen für DHCP werden in einer virtuellen Umgebung auf dem Labor-PC durchgeführt. Dazu werden virtuellen Maschinen auf Basis von KVM / QEMU betrieben.

Im Internetbetrieb ist die Dual Stack Methode der aktuelle Stand der Technik. Daher können die folgenden Übungen neben IPv4 auch mit IPv6 durchgeführt werden.

Damit die in der Übung betriebenen DHCP-Server im Labornetz kein Chaos anrichten, wird die Übung ausschließlich in einer virtuellen Netzwerkumgebung durchgeführt.

Die Verbindung zwischen dem PC und dem DHCP-Server erfolgt auf dem virtuellen Netz VMnet9. Zusätzlich verbindet ein NAT-Gateway das virtuelle Netz mit dem Labornetz.

Mit dem Tool Wireshark kann auf dem virtuellen Netzwerk das DHCP Protokoll aufgezeichnet und analysiert werden.



2 STARTEN DER ÜBUNGSUMGEBUNG

- Öffnen Sie den Ordner **Virtual Machines Links** auf dem Desktop.
- Starten Sie die virtuelle Maschine **NATGw** durch Doppelklick und minimisieren Sie die VM-Anzeige in die Taskleiste.
- Starten Sie die beiden virt. Maschinen **WinHost** und **dhcpx** durch Doppelklick.

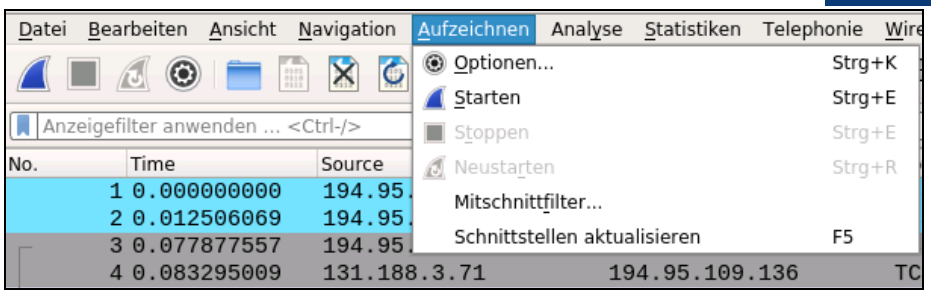
Der dhcpx ist ein virtueller Linux-PC. Auf dem dhcpx ist der ISC-DHCP-SERVER installiert worden. Die Installation erfolgte mit dem Kommando: `apt-get install isc-dhcp-server`
Der DHCP-Server kann IPv4 und IPv6 bedienen.

- Minimieren Sie **dhcpx** in die Taskleiste! Nur **WinHost** bleibt am Desktop offen.

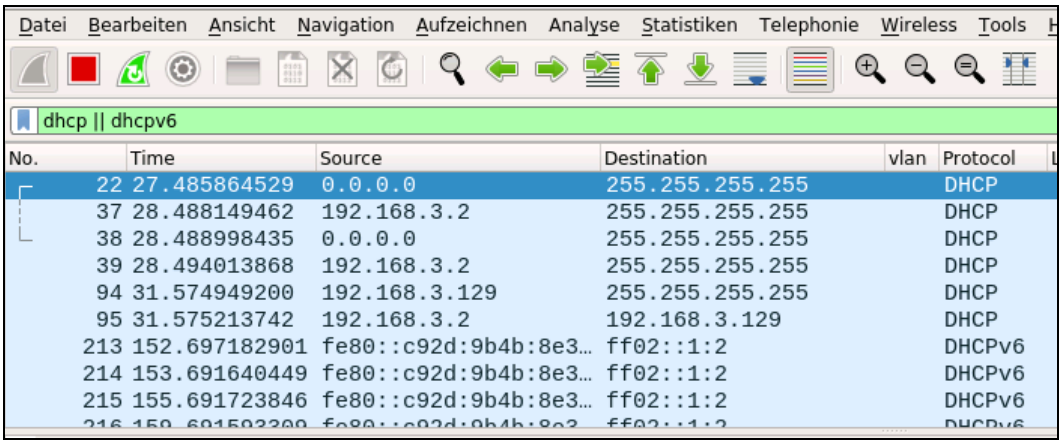
3 TEST UND ANALYSE MIT WIRESHARK

Der DHCP-Server ist nur minimal konfiguriert und soll von Ihnen im Zuge der Übung erweitert werden. Verfolgen Sie mit Wireshark den DHCP-Ablauf und ermitteln Sie, welche Optionen und Parameter im DHCP-Server noch eingetragen werden müssen.

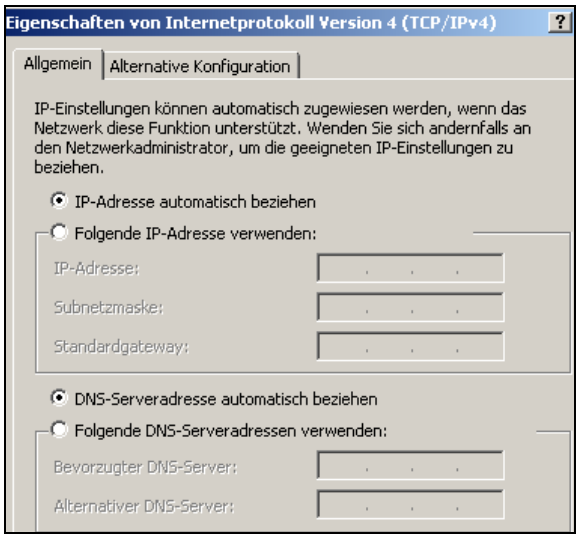
- Starten Sie auf **dem lokalen Labor-PC** das Programm **WireShark**
- Öffnen Sie das **Aufzeichnen** Menü und wählen Sie **Optionen...** aus.



- Wählen Sie das Mittschnitt Interface **br9** aus und klicken Sie auf den **Start**-Button (keine Mittschnitt Filter). Damit kann Wireshark auf dem Subnetz VMnet9 = 192.168.3.0 (IPv6: fd00:0:0:3::) alle Datenpakete aufzeichnen.
- Betrachten Sie im Wireshark die aufgezeichneten DHCP-Pakete. Stellen Sie dafür den Display-Filter in Wireshark auf **dhcp || dhcpv6**



- Überprüfen Sie im **WinHost,** dass der Netzwerkadapter auf **„IP-Adresse automatisch beziehen“** und **„DNS -Serveradresse automatisch beziehen“** gestellt ist. Stellen Sie dies ggf. selbst ein.



Hinweis: Jetzt sollten Sie in Wireshark DHCP bzw. DHCPv6 Meldungen sehen. Falls nicht, starten Sie entweder den WinHost neu oder deaktivieren Sie den Netzwerkadapter am **WinHost** und aktivieren Sie ihn anschließend wieder.

Wie funktioniert DHCP?

(1) Mit dem **DHCP DISCOVER** sucht der Client nach mind. einem DHCP Server und fordert die nötigen IP-Parameter an, z.B.: IP-Adresse, Subnetzmaske, Bootimage-Server, Hostnamen, Router, usw.

(2) Die DHCP-Server (falls mehrere aktiv sind) liefern mit **DHCP OFFER** die angeforderten Parameter, soweit möglich, d.h. soweit sie am Server konfiguriert wurden. Falls der Client mehrere Angebote bekommt, nimmt er eines an.

(3) Mit **DHCP REQUEST** kann der Client weitere, für seine Wahl spezifische Parameter nachfordern,

(4) die vom ausgewählten DHCP-Server mit **DHCP ACK** beantwortet werden.

```
Bootstrap Protocol

    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xa30ea49e
    Seconds elapsed: 0
    Bootp flags: 0x8000 (Broadcast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: 00:0c:29:83:88:7a (00:0c:29:83:88:7a)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type
    Option: (61) Client identifier
    Option: (12) Host Name
    Option: (60) Vendor class identifier
    Option: (55) Parameter Request List
        Length: 12
        Parameter Request List Item: (1) Subnet Mask
        Parameter Request List Item: (15) Domain Name
        Parameter Request List Item: (3) Router
        Parameter Request List Item: (6) Domain Name Server
        Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
        Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
        Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
        Parameter Request List Item: (31) Perform Router Discover
        Parameter Request List Item: (33) Static Route
        Parameter Request List Item: (121) Classless Static Route
        Parameter Request List Item: (249) Private/Classless Static Route
        Parameter Request List Item: (43) Vendor-Specific Information
    Option: (255) End
```

```
Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xa30ea49e
    Seconds elapsed: 0
    Bootp flags: 0x8000 (Broadcast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.3.128 (192.168.3.128)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: 00:0c:29:83:88:7a (00:0c:29:83:88:7a)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type
    Option: (54) DHCP Server Identifier
        DHCP Server Identifier: 192.168.3.2 (192.168.3.2)
    Option: (51) IP Address Lease Time
        IP Address Lease Time: (600s) 10 minutes
    Option: (1) Subnet Mask
        Subnet Mask: 255.255.255.0 (255.255.255.0)
    Option: (255) End
```

- Öffnen Sie am **WinHost** die **Eingabeaufforderung** und führen Sie folgenden Befehl aus:


```
ipconfig /all
```

Vergleichen Sie die mit DHCP gelieferten IP-Parameter mit der Anzeige am WinHosts.

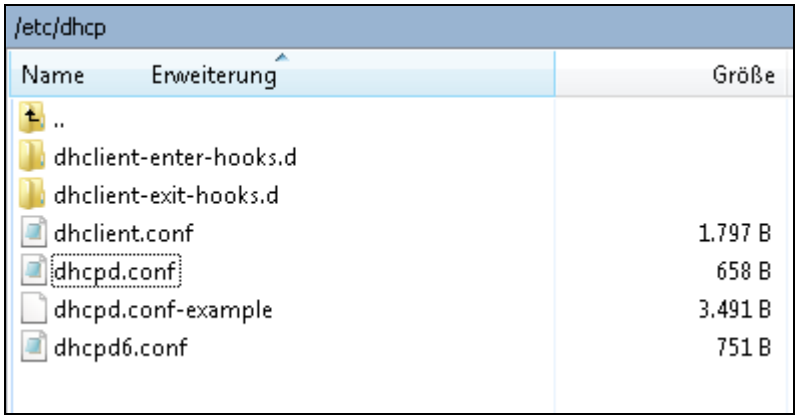
Kontrollfragen:

- ☑ Welche IP-Parameter wurden vom Client angefordert?
- ☑ Welche IP-Parameter wurden vom DHCP-Server zugewiesen?
- ☑ Welche IP-Parameter hat der Host eingestellt:
  DNS-Suffix Suchliste ?
  IPv4-Adresse ?
  DHCP-Server ?
  Standartgateway ?
  DNS-Server ?
- ☑ Wie lange ist die Zuweisung (=Lease) gültig?

4 ERWEITERN DER KONFIGURATION DES DHCP-SERVERS

- Erstellen Sie eine SSH-Verbindung zu dnsx. Dazu ist auf dem Desktop von WinHost ein Shortcut **„dhcpx“** vorhanden, das mit WinSCP die Verbindung aufbaut. (Zum Einloggen: User: root, Passwort: comlab)

- Verzweigen Sie am **dhcpx** ins Verzeichnis **/etc/dhcp** und öffnen Sie die Datei **dhcpd.conf** mit dem built-in Editor von WinSCP (Doppelklick auf Datei oder Rechtsklick->Bearbeiten).



- Erweitern Sie die Konfiguration des DHCP-Servers um folgende Optionen. Die Optionen sind schon vorbereitet, aber auskommentiert. Entfernen Sie nur die entsprechenden Kommentarzeichen „#“.

Default Gateway	`option routers 192.168.3.1;`
Domain Name	`option domain-name "imtest.hs-regensburg.de";`
DNS	`option domain-name-servers 194.95.109.185;`

Hinweis: Der WinHost hat bisher eine Adresse aus dem Pool des Subnetzes 192.168.3.0 bezogen (Adressen 128 bis 191). Nun soll aber für den Host eine IP-Adresse fest eingestellt werden, die er bei jedem neuen DHCP-Vorgang erhält. Diese IP-Adresse ist statisch an die Ethernet-Adresse des Hosts gebunden.

- Ermitteln Sie am **WinHost** die **Ethernet-Adresse** für Interface **LAN-Adapter.** (Eingabeaufforderung: **ipconfig /all**)

- Tragen Sie die Ethernet-Adresse in die Datei **/etc/dhcp/dhcpd.conf** ein. Überschreiben Sie nur den vorbereiteten Eintrag mit der tatsächlichen Ethernet Adresse. Beachten Sie, dass die Bytes der Ethernet-Adresse mit Doppelpunkt (:) getrennt werden. und dass am Zeilenende ein Strichpunkt (;) stehen muss.

```
host WinHost {
   hardware ethernet 00:0C:29:00:00:00;
   fixed-address 192.168.3.100;
}
```

- Speichern Sie die Änderungen an der Datei und schließen Sie sie wieder (Klick auf Diskettensymbol oben links).

- Öffnen Sie eine Terminal-Verbindung zum **dhcpx**. Klicken Sie dazu auf das **Terminal-Symbol** in der Menüzeile von WinSCP. Loggen Sie sich am dhcpx als Benutzer **root** und Passwort **comlab** ein.

- Damit die neue Konfiguration in den Server übernommen wird, restarten Sie den DHCP-Server auf dem dhcpx mit dem folgenden Kommando: Achten Sie auf Fehlermeldungen!

```
/etc/init.d/isc-dhcp-server restart
```

- Loggen Sie sich mit **exit** am Terminal aus und schließen Sie ggf. das Terminalfenster. Die Terminalverbindung wird jetzt nicht mehr benötigt.

```
exit
```

- **Deaktivieren** Sie den Netzwerkadapter am **WinHost**.

- Der **Display**-Filter in Wireshark steht immer noch auch **DHCP || DHCPv6.**

- Starten Sie das **Aufzeichnen** von Ethernetpaketen neu.

- **Aktivieren** Sie den Netzwerkadapter auf **WinHost** wieder.

- Überprüfen Sie in Wireshark und am WinHost (mit ipconfig/all) ob der WinHost die neuen Optionen über DHCP bekommen hat!

Kontrollfragen:

- ☑ Wurden die neuen IP-Parameter zugewiesen?
- ☑ Welche IP-Parameter hat der Host eingestellt:
  DNS-Suffix bzw. Suchliste ?
  IPv4-Adresse ?
  Standartgateway?
  DNS-Server ?
- ☑ Finden Sie die Parameter im Wireshark Listing?

```
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
▸ Option: (53) DHCP Message Type (ACK)
▸ Option: (54) DHCP Server Identifier (192.168.3.2)
▸ Option: (51) IP Address Lease Time
▸ Option: (1) Subnet Mask (255.255.255.0)
▸ Option: (15) Domain Name
▸ Option: (3) Router
▸ Option: (6) Domain Name Server
▸ Option: (255) End
```

5 EINRICHTEN DES DHCP-SERVERS FÜR IPV6

Der ISC-DHCP-SERVER unterstützt auch IPv6, doch muss er dafür ein zweites Mal gestartet werden. (kein gemeinsamer Prozess für beide Protokolle). Doch vor dem Start muss die Konfigurationsdatei für IPv6 eingerichtet werden.

- Editieren Sie die Datei **/etc/dhcp/dhcpd6.conf** auf dem dhcpx.

- Erweitern Sie die Konfiguration des DHCP-Servers um folgende Optionen. Eine Übersicht aller Optionen des ISC-DHCP-SERVER finden Sie im Anhang. Die Optionen sind schon vorbereitet, aber auskommentiert. Entfernen Sie die entspr. Kommentarzeichen „#“.

Domain Name	`option dhcp6.domain-search "ipv6-regensburg.de";`
DNS	`option dhcp6.name-servers 2001:638:a01:3f09::8185;`

Der WinHost soll eine fest eingestellte IPv6-Adresse erhalten. Diese IPv6-Adresse ist an die DHCPv6 Client DUID des Hosts gebunden, eine 14 Byte lange ID.

- Ermitteln Sie die die **DHCPv6 Client DUID** des WinHosts. (**ipconfig /all**)

- Nehmen Sie den entsprechenden Eintrag in **der /etc/dhcp/dhcpd6.conf** vor. Überschreiben Sie nur den vorbereiteten Eintrag mit der tatsächlichen DUID. Beachten Sie, dass zwischen den Bytes ein Doppelpunkt (:) und am Zeilenende ein Strichpunkt (;) stehen muss.

```
host WinHost {
    host-identifier option dhcp6.client-id
                    00:01:00:01:1B:DB:BC:67:00:0C:29:00:00:00;
    fixed-address6 fd00:0:0:3::100;
    }
```

- Speichern Sie die Änderungen an der Datei und schließen Sie sie wieder (Klick auf Diskettensymbol oben links).

- Öffnen Sie eine Terminal-Verbindung zum **dhcpx**. Klicken Sie dazu auf das **Terminal-Symbol** in der Menüzeile von WinSCP. Loggen Sie sich am dhcpx als Benutzer **root** und Passwort **comlab** ein.

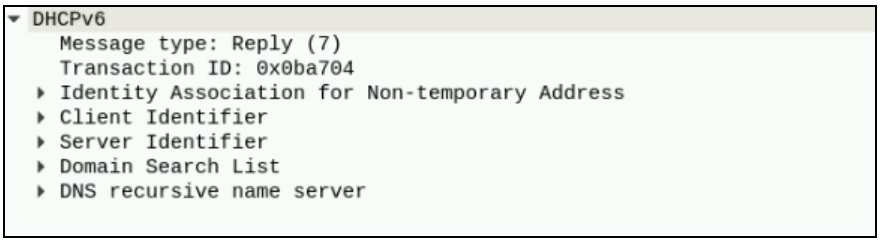
- Starten Sie den DHCP-Server für IPv6 mit dem folgenden Kommando und achten Sie auf Fehlermeldungen beim Start.

```
/usr/sbin/dhcpd -6 -cf /etc/dhcp/dhcpd6.conf eth0 &
```

Hinweis: Drücken Sie nach ein paar Sekunden ggf. ein zweites Mal auf die Enter-Taste, sodass das Befehls-prompt wieder erscheint. Sollte der DHCPv6-Server einen Restart benötigen, so muss der Prozess vorher beendet werden. Dies ist über den Befehl: **kill <PID>** möglich. Die PID (Process ID) aller Prozesse erhält man über den Befehl **ps –A** . Um nach einem bestimmten Prozess zu suchen kann man eingeben: **ps –A | grep dhcp** .

Es werden zwei Prozesse mit demselben Namen angezeigt. Der erstere gehört wahrscheinlich zum DHCPv4-Prozess (wurde ja auch vorher gestartet), der zweite wahrscheinlich dem DHCPv6 Prozess.

- Loggen Sie sich mit **exit** am Terminal aus und schließen Sie ggf. das Terminalfenster. Die Terminalverbindung wird jetzt nicht mehr benötigt.
- Überprüfen Sie im **WinHost**, dass der Netzwerkadapter auch für das IPv6 auf **„IPv6-Adresse automatisch beziehen“** und **„DNS -Serveradresse automatisch beziehen“** gestellt ist. Stellen Sie dies ggf. selbst ein.
- **Deaktivieren** Sie den Netzwerkadapter am **WinHost**.
- Stellen Sie in Wireshark den **Display-Filter** auf **dhcpv6** und starten Sie **Aufzeichnen** neu.
- **Aktivieren** Sie den Netzwerkadapter auf **WinHost** wieder.
- Überprüfen Sie in Wireshark und am **WinHost** (mit ipconfig/all) ob der WinHost die neuen Optionen über DHCP bekommen hat! Schauen Sie sich in Wireshark besonders die DHCPv6 Reply Meldungen an.



Falls Sie die DHCP-Messung mit Wireshark wiederholen wollen, deaktivieren und reaktivieren Sie den Ethernet-Adapter auf dem WinHost. Vorher muss aber im Wireshark das Aufzeichnen von Paketen gestartet sein.

Kontrollfragen:

- ☑ Welche IPv6 Adresse wurde in der DHCPv6-Meldung vergeben?
- ☑ Welche IPv6-Adresse wurde in der DHCPv6-Meldung als DNS gesendet?
- ☑ Welche Lifetime für die Adresse wurde gesendet? Rechnen Sie diese in Stunden um und vergleichen Sie sie mit der Leasedauer am WinHost. Passen beide Werte zusammen?
- ☑ Finden Sie die DHCPv6-Client-DUID im dhcpv6-Paket wieder?
- ☑ Hat der IPHost auch lokale IPv6-Adressen die mit fe80… beginnen? Darf er eine haben?

6 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!