

# Praktikum Rechnernetze

Protokoll zu Versuch 4 (IPv6) von Gruppe 1

---

Jakob Waibel   Daniel Hiller   Elia Wüstner   Felix Pojtinger

2021-11-09

# Einführung

---

Diese Materialien basieren auf Professor Kiefers “Praktikum Rechnernetze”-Vorlesung der HdM Stuttgart.

**Sie haben einen Fehler gefunden oder haben einen Verbesserungsvorschlag?** Bitte eröffnen Sie ein Issue auf GitHub ([github.com/pojntfx/uni-netpractice-notes](https://github.com/pojntfx/uni-netpractice-notes)):



**Abbildung 1:** QR-Code zum Quelltext auf GitHub

Dieses Dokument und der enthaltene Quelltext ist freie Kultur bzw. freie Software.



**Abbildung 2:** Badge der AGPL-3.0-Lizenz

Uni Network Practice Notes (c) 2021 Jakob Waibel, Daniel Hiller,  
Elia Wüstner, Felix Pojtinger

SPDX-License-Identifier: AGPL-3.0

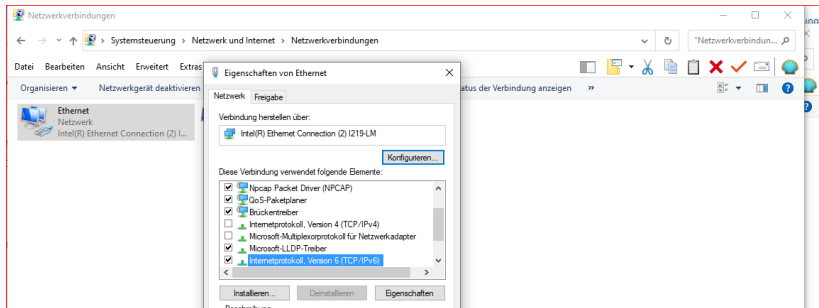
# IPv6-Adressen

---

# IPv6-Adressen

## Voreinstellung für die Aufgaben - deaktivieren von IPv4 und aktivieren von IPv6 unter Windows.

Um IPv4 zu deaktivieren und IPv6 zu aktivieren muss man in den Netzwerkeinstellungen zum jeweiligen Adapter über den Pfad Systemsteuerung > Netzwerk und Internet > Netzwerkverbindungen > Adapterstatus der Verbindung anzeigen > Eigenschaften von Ethernet gehen. Hier wurde der Haken bei IPv6 (Internetprotokoll, Version6) gesetzt und bei IPv4 (Internetprotokoll, Version4) entfernt



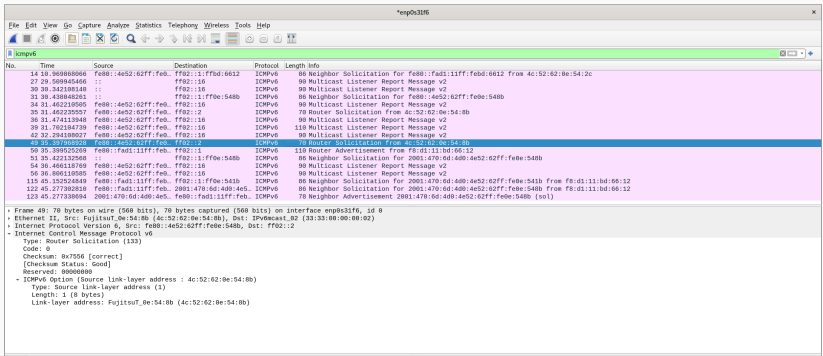
# IPv6 und DNS

---

# IPv6 und DNS

Identifizieren Sie mit Wireshark die Pakete mit denen der Router im Netz das Prefix mitteilt. Welches Protokoll wird dafür benutzt und um welchen Type handelt es sich und wie lautet die Zieladresse des Pakets?

Protokoll: ICMPv6 Type: Router Solicitation bzw. Router Advertisement



The image shows a Wireshark packet capture window titled "enp0s3196". The packet list on the left shows several ICMPv6 packets. The selected packet is packet 42, which is an ICMPv6 Router Solicitation from fe80::f0d1:11ff:febd:6612 to ff02::16. The packet details pane on the right shows the following structure:

- Frame 42: 78 bytes on wire (608 bits), 78 bytes captured (608 bits) on interface enp0s3196, id 0
- Ethernet II, Src: FujitsuT\_0e:54:0b (4c:52:02:0e:54:0b), Dst: IPv6cast\_B2 (33:33:00:00:00:02)
- Internet Protocol Version 6, Src: fe80::4e52:62ff:febe:540b, Dst: ff02::12
- Internet Control Message Protocol v6
  - Type: Router Solicitation (133)
    - Code: 0
    - Checksum: 8x7956 [correct]
    - [Checksum Status: Good]
    - Reserved: 80000000
  - ICMPv6 Option (Source Link-layer address : 4c:52:02:0e:54:0b)
    - Type: Source Link-layer address (3)
    - Length: 1 (8 bytes)
    - Link-layer address: FujitsuT\_0e:54:0b (4c:52:02:0e:54:0b)



## Neighbor Solicitation

---

# Neighbor Solicitation

Starten Sie den „Kabelhai“ und pingen Sie ihren Nachbarrechner. Welches Protokoll/Type wird anstatt ARP zur Ermittlung der MAC-Adressen verwendet?

*Windows*

The screenshot shows a Windows command prompt window on the left and a Wireshark network traffic analysis window on the right.

**Command Prompt:**

```
PS C:\WINDOWS\system32> netsh int ipv6 del neigh  
OK  
PS C:\WINDOWS\system32> ping -6 2001:470:6d:4d0:4e52:62ff:fe0e:548b  
Ping wird ausgeführt für 2001:470:6d:4d0:4e52:62ff:fe0e:548b mit 32 Bytes Daten:  
Antwort von 2001:470:6d:4d0:4e52:62ff:fe0e:548b: Zeit=1ms  
Antwort von 2001:470:6d:4d0:4e52:62ff:fe0e:548b: Zeit=1ms  
Antwort von 2001:470:6d:4d0:4e52:62ff:fe0e:548b: Zeit=1ms  
Antwort von 2001:470:6d:4d0:4e52:62ff:fe0e:548b: Zeit=1ms  
Ping-Statistik für 2001:470:6d:4d0:4e52:62ff:fe0e:548b:  
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0  
(0% Verlust)  
ca. Zeitangaben in Millisek.:  
Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms  
PS C:\WINDOWS\system32>
```

**Wireshark:**

The Wireshark window shows a packet capture on the Ethernet interface (2) 019-10A Ethernet. The packet list shows several Neighbor Solicitation (Type 135) and Neighbor Advertisement (Type 136) packets. The packet details pane shows the structure of a Neighbor Solicitation packet, including the Source MAC address (08:00:00:00:00:00) and the Destination MAC address (01:00:5E:00:00:00).

**Abbildung 13:** Solicitation und Advertisement-Pakete in Wireshark - Windows

*Linux*

```
$ sudo ip neigh flush dev enp0s31f6
```

# IPv6-Header

---

# IPv6-Header

Starten Sie Wireshark und senden sie ein ping an einen IPv6-fähigen Webserver ([www.ix.de](http://www.ix.de), <http://www.heise.de>, <http://www.kame.net>), stoppen Sie Wireshark und schauen sich den Trace an.

*Windows*

*Da der Screenshot verloren gegangen ist, wurde es nachträglich von daheim aus aufgenommen.*

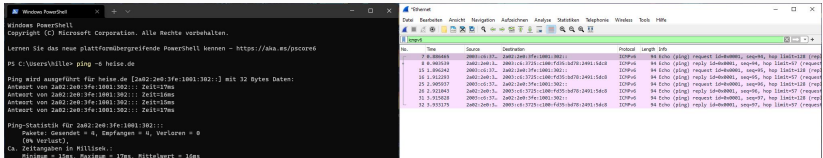


Abbildung 15: Ping Heise

*Linux*

\$ ping -6 www.kame.net

# Privacy Extension

---

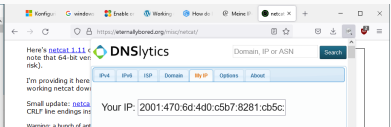
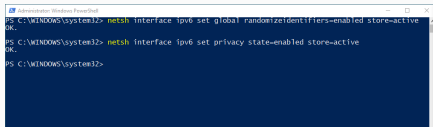
# Privacy Extension

Tragen Sie weitere Informationen zur „Privacy Extension“ (vor allem auch zur Konfiguration unter Windows und Ubuntu) zusammen und versuchen hier im Versuch die Einstellungen für die „Privacy Extension“ auf beiden Rechnern (Windows und Ubuntu) zu realisieren.

## *Windows*

Unter Windows kann die Privacy Extension mit den zwei folgenden Kommandos deaktiviert werden:

```
>netsh interface ipv6 set global randomizeidentifiers-enabled store-active  
>netsh interface ipv6 set global state=enabled store-active
```



# Feste IPv6-Adressen

---

## Feste IPv6-Adressen

Weisen Sie in dieser Aufgabe ihrem Netzwerkinterface eine feste sinnvolle (heißt: Der Prefix ist weiterhin gültig) IPv6-Adresse zu.

```
$ ip a
```

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noque
    link/loopback 00:00:00:00:00:00 brd 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: enp0s31f6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu
    link/ether 4c:52:62:0e:54:8b brd ff:ff:ff:ff:ff
    inet6 2001:470:6d:4d0:4e52:62ff:fe0e:548b/64 sc
        valid_lft 86255sec preferred_lft 14255sec
    inet6 fe80::4e52:62ff:fe0e:548b/64 scope link
```



# Lease-Zeiten

---

**Die Werte für “Maximale bevorzugte Gültigkeitsdauer” und “Maximale Gültigkeitsdauer” setzt man in Windows über die Schlüssel maxpreferredlifetime und maxvalidlifetime, die Zeitangaben in Tagen (d), Stunden (h), Minuten (m) und Sekunden (s) entgegennehmen. Wie sind diese Parameter bei Ihnen gesetzt?**

TODO: Add interpretation

**Halbieren Sie die “Maximale bevorzugte Gültigkeitsdauer” auf den Rechnern.**

TODO: Add interpretation

**Verringern Sie ebenso die Zeitspanne, in der Windows über eine temporäre IPv6-Adresse eingehende Pakete empfängt.**

TODO: Add interpretation

# OS-Updates

---

## OS-Updates

```
$ sudo ip addr del 141.62.66.5/24 dev enp0s31f6
$ sudo apt update
Hit:1 http://deb.debian.org/debian bullseye InRelease
Hit:2 http://security.debian.org bullseye-security
Get:3 http://deb.debian.org/debian bullseye-updates
Hit:4 http://ppa.launchpad.net/ansible/ansible/ubuntu
Fetched 39.4 kB in 5s (7,169 B/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1 package can be upgraded. Run 'apt list --upgradable' to see details.
$ sudo apt upgrade -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```