

# Praktikum Rechnernetze

Protokoll zu Versuch 4 (IPv6) von Gruppe 1

---

Jakob Waibel Daniel Hiller Elia Wüstner Felicitas Pajtinger

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, Felicitas Pojtinger

SPDX-License-Identifier: AGPL-3.0

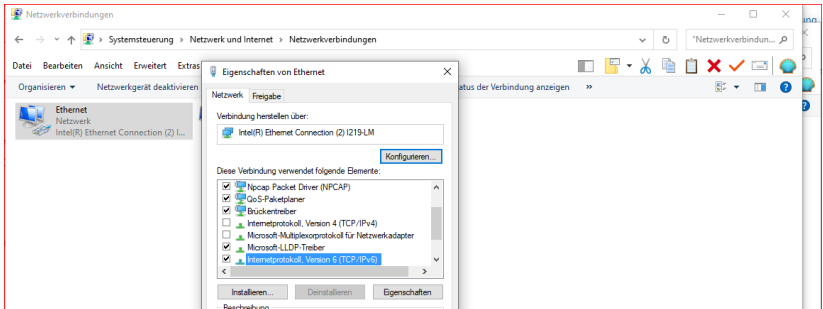
## IPv6-Adressen

---

# 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 > Adaptereinstellungen navigieren. Hier wurde der Haken bei IPv6 (Internetprotokoll, Version6) gesetzt und bei IPv4 (Internetprotokoll, Version4) entfernt.



## 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?

Das verwendete Protokoll ist wie auch in den unten stehenden Screenshots zu sehen ICMPv6. Die Types sind Router Solicitation und Router Advertisement. Die Zieladresse des Pakets ist die Multicast-Adresse ff02 ::1 .

Router Solicitation:

The screenshot shows a Wireshark capture of ICMPv6 traffic. The packet list pane displays several entries, with the selected packet (No. 49) highlighted in blue. The packet details pane shows the structure of the Router Solicitation message.

No.	Time	Source	Destination	Protocol	Length	Info
14	19.599868066	fe80::4e52:62ff:feb...	ff02::1:ffbd:6612	ICMPv6	88	Neighbor Solicitation for fe80::fad1:11ff:febd:6612 from 4c:52:62:0e:54:2c
17	19.599854066	::	ff02::1	ICMPv6	90	Multicast Listener Report Message v2
20	19.542188140	::	ff02::1	ICMPv6	90	Multicast Listener Report Message v2
31	19.438048281	::	ff02::1:ff0e:548b	ICMPv6	88	Neighbor Solicitation for fe80::4e52:62ff:febe:548b
34	19.482116595	fe80::4e52:62ff:feb...	ff02::1	ICMPv6	90	Multicast Listener Report Message v2
39	19.482235557	fe80::4e52:62ff:feb...	ff02::1	ICMPv6	78	Router Solicitation from 4c:52:62:0e:54:2b
38	19.474113948	fe80::4e52:62ff:feb...	ff02::1	ICMPv6	90	Multicast Listener Report Message v2
39	19.702184739	fe80::4e52:62ff:feb...	ff02::1	ICMPv6	118	Multicast Listener Report Message v2
42	19.294188027	fe80::4e52:62ff:feb...	ff02::1	ICMPv6	90	Multicast Listener Report Message v2
49	19.597969528	fe80::4e52:62ff:feb...	ff02::1	ICMPv6	78	Router Solicitation from 4c:52:62:0e:54:2b
50	19.599025269	fe80::fad1:11ff:feb...	ff02::1	ICMPv6	118	Router Advertisement from fe:d1:11:bd:66:12
51	19.421329568	::	ff02::1:ff0e:548b	ICMPv6	88	Neighbor Solicitation for 2001:470:6d:400:4e52:62ff:febe:548b
54	19.466187609	fe80::4e52:62ff:feb...	ff02::1	ICMPv6	90	Multicast Listener Report Message v2
56	19.806119585	fe80::4e52:62ff:feb...	ff02::1	ICMPv6	90	Multicast Listener Report Message v2
115	19.325264849	fe80::fad1:11ff:feb...	ff02::1:ff0e:541b	ICMPv6	88	Neighbor Solicitation for 2001:470:6d:400:4e52:62ff:febe:541b from fe:d1:11:bd:66:12
122	19.457738281	fe80::fad1:11ff:feb...	2001:470:6d:400:4e5...	ICMPv6	88	Neighbor Solicitation for 2001:470:6d:400:4e52:62ff:febe:548b from fe:d1:11:bd:66:12
123	19.457738694	2001:470:6d:400:4e5...	fe80::fad1:11ff:feb...	ICMPv6	78	Neighbor Advertisement 2001:470:6d:400:4e52:62ff:febe:548b (sol)

Packet details for No. 49:

- Frame 49: 78 bytes on wire (568 bits), 78 bytes captured (568 bits) on interface enp8s31f6, id 0
- Ethernet II, Src: Puj11out\_0e:54:00:4c:52:62:0e:54:2b, Dst: IPv6multicast\_32 (33:33:00:00:00:02)
- Internet Protocol Version 6, Src: fe80::4e52:62ff:febe:548b, Dst: ff02::1
- Internet Control Message Protocol v6
  - Type: Router Solicitation (133)
    - Code: 0



## 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

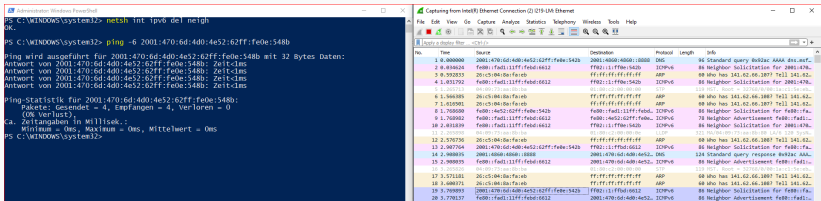


Abbildung 16: Solicitation und Advertisement-Pakete in Wireshark - Windows

## Linux

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

```
$ ping6 fe80::fad1:11ff:febd:6612
```

```
PING fe80::fad1:11ff:febd:6612 (fe80::fad1:11ff:febd:6612) 64 bytes of data: 64 bytes from fe80::fad1:11ff:febd:6612: icmp_seq=1: ttl=64: time=0.000 ms
```

## IPv6-Header

---

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

## Windows

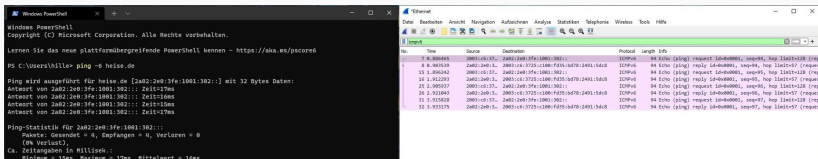


Abbildung 18: Ping Heise

## Linux

```
$ ping www.kame.net
```

```
PING www.kame.net(2001:2f0:0:8800:226:2dff:fe0b:4311 (2001:2
```

```
64 bytes from 2001:2f0:0:8800:226:2dff:fe0b:4311 (2001:2f0:0
```

```
64 bytes from 2001:2f0:0:8800:226:2dff:fe0b:4311 (2001:2f0:0
```

## 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.

Privacy Extensions sind dafür da, Rückschluss auf Nutzer:innen schwerer zu machen, indem der Hostanteil der IPv6-Adressen anonymisiert wird. Privacy Extensions entkoppeln Interface Identifier und MAC-Adresse und erzeugen diese nahezu zufällig. Mit diesen periodisch wechselnden Adressen werden dann ausgehende Verbindungen hergestellt, was den Rückschluss auf *einzelne* Nutzer:innen erschwert. Mit Hilfe der Privacy Extensions kann man also nicht mehr einzelne Nutzer:innen identifizieren. Was allerdings trotzdem möglich ist, ist das Identifizieren über den Präfix, welcher allerdings nur Informationen zum Netzwerk bereitstellt. Wenn der Provider den Präfix regelmäßig wechselt, dann kann auch die Identifikation über diesen erschwert werden.

## Feste IPv6-Adressen

---

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

*Windows*

Eigenschaften von Internetprotokoll, Version 6 (TCP/IPv6) ×

**Allgemein**

IPv6-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IPv6-Einstellungen zu beziehen.

IPv6-Adresse automatisch beziehen

Folgende IPv6-Adresse verwenden:

IPv6-Adresse:

Subnetzpräfixlänge:

Standardgateway:

DNS-Serveradresse automatisch beziehen

Folgende DNS-Serveradressen verwenden:

Bevorzugter DNS-Server:

Alternativer DNS-Server:



## 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?

*Windows*

```
netsh interface ipv6 show privacy
```

```
Parameter für temporäre Adressen
-----
Temporäre Adresse verwenden           : enabled
Versuch, doppelte Adr. zu entdecken  : 3
Maximale Gültigkeitsdauer             : 7d
Maximale bevorzugte Gültigkeitsdauer: 7d
Regenerationszeit                     : 5s
Maximale Verzögerungszeit             : 10m
Verzögerungszeit                      : 6m23s
```

## OS-Updates

---

## Lässt sich eigentlich Windows über IPv6 updaten? Was sagt Wireshark dazu?

### Windows

Unter Windows wurde das Update ohne Probleme installiert. Windows Update verfügt über vollen IPv6-Support.

(<https://sejverfault.com/questions/844107/windows-server-update-on-ipv6-network>). Dies konnte auch mittels Wireshark validiert werden:

The image shows two overlapping windows. On the left is the Wireshark network traffic analyzer, displaying a list of captured packets. The selected packet is an ICMP Echo (ping) request from 192.168.1.100 to fe80::c:ad54:7516:c09f. The packet details pane shows the Ethernet II, Internet Protocol Version 6, and ICMP Echo (ping) fields. The packet bytes pane shows the raw data in hexadecimal and ASCII.

On the right is the Windows Update settings window. It shows the status of several updates. The update '2021-11 Cumulative Update for Windows 11 for x64-based Systems (KB5007215)' is in the 'Downloading' state. The update '2021-11 Cumulative Update for .NET Frameworks 3.5 and 4.8 for Windows 11 for x64 (KB5006306)' is in the 'Installing' state. The update '2021-11 Updates for Windows 11 for x64-based Systems (KB5008295)' is in the 'Pending restart' state.