Praktikum Rechnernetze

Protokoll zu Versuch 4 (IPv6) von Gruppe 1

Jakob Waibel Daniel Hiller Elia Wüstner Felicitas Pojtinger

2021-11-09

Einführung

Mitwirken

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):

Abbildung 1: QR-Code zum Quelltext auf GitHub

Lizenz

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

Abbildung 2: Badge der AGPL-3.0-Lizenz

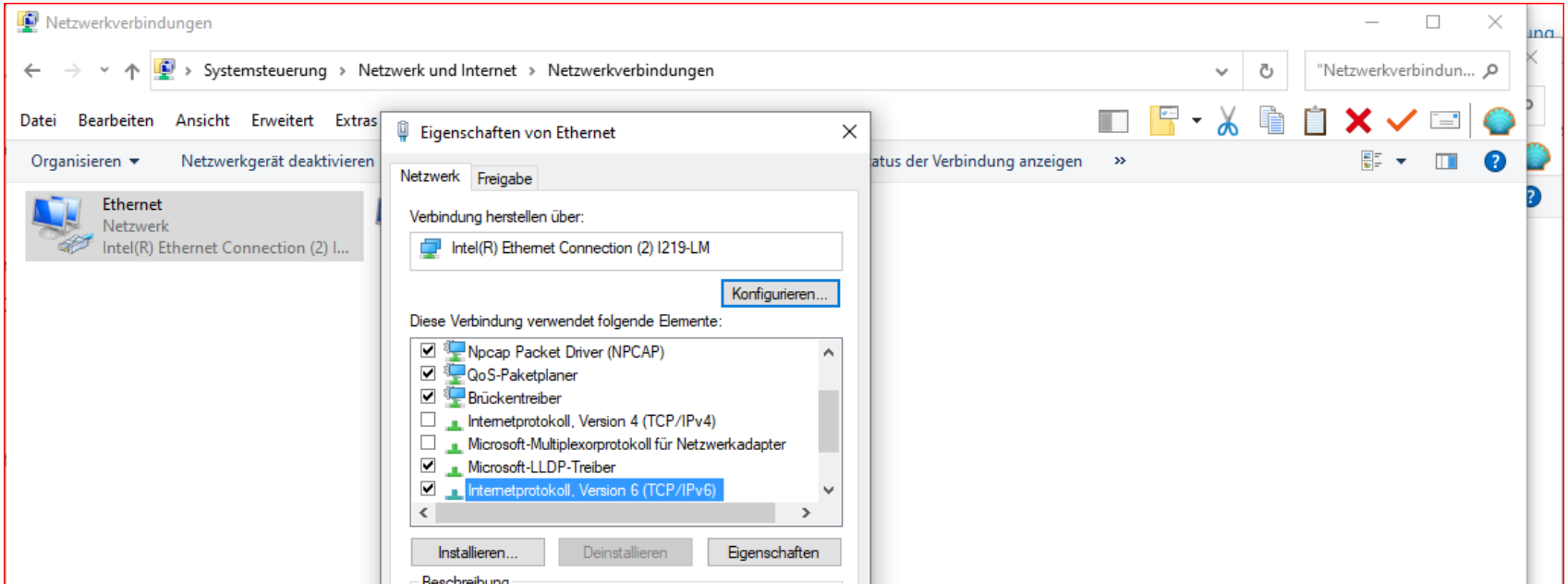
SPDX-License-Identifier: AGPL-3.0

IPv6-Addressen

IPv6-Addressen

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

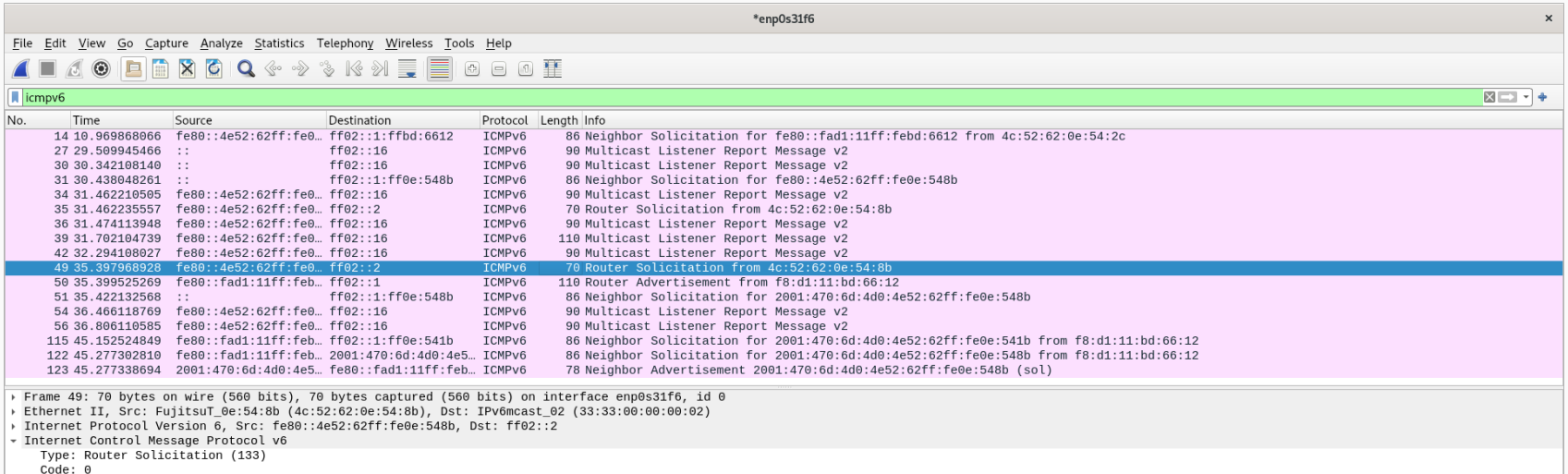


IPv6 und DNS

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 Protkoll 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:



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

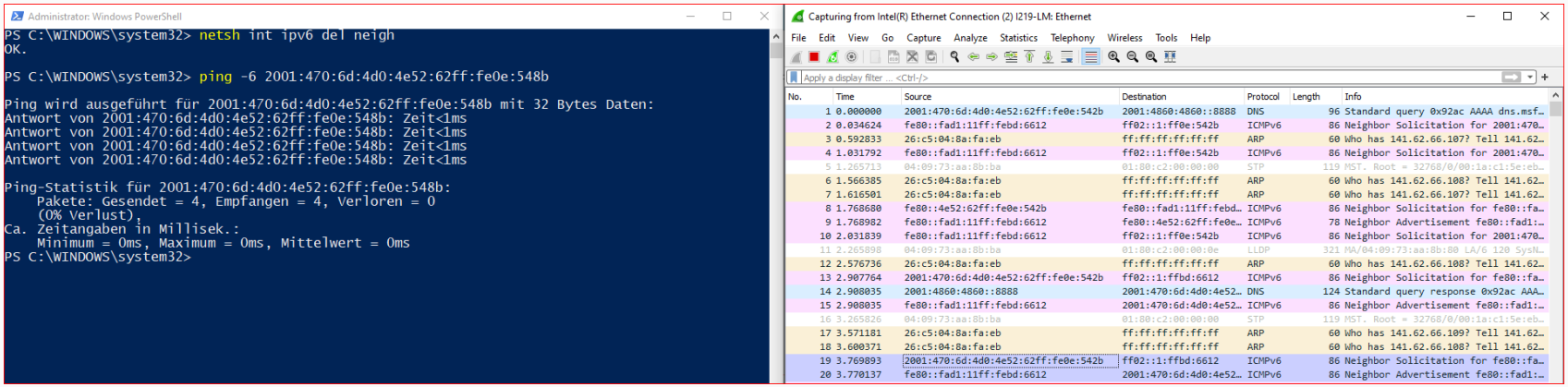


Abbildung 16: Solicitation und Advertisement-Pakete in Wireshark - Windows

Linux

```
$ sudo ip neigh flush dev enp0s31f6
$ ping6 fe80::fad1:11ff:febd:6612
PING fe80::fad1:11ff:febd:6612(fe80::fad1:11ff:febd:6612) 56
```

IPv6-Header

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

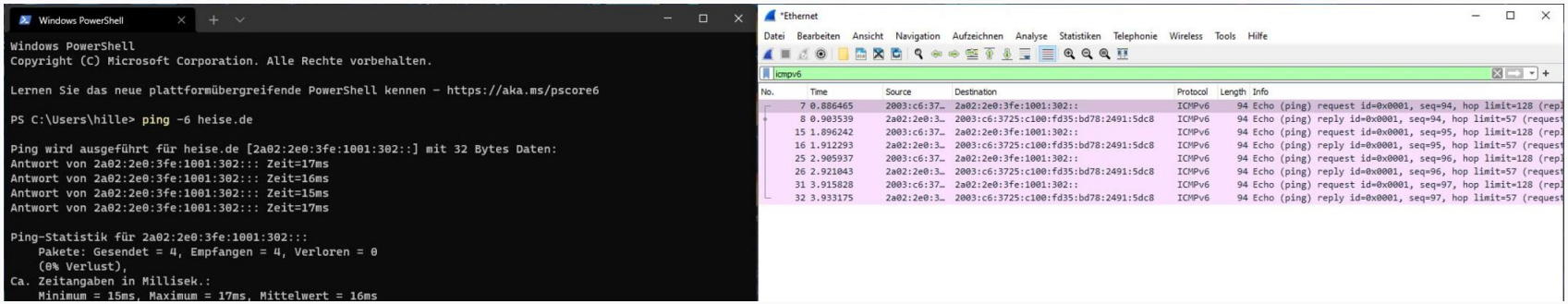


Abbildung 18: Ping Heise

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

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, Rückchluss 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-Addressen

Feste IPv6-Addressen

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

Windows

Lease-Zeiten

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

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://serverfault.com/questions/844107/windows-server-update-on-ipv6-only-network). Dies konnte auch mittels Wireshark validiert werden: