

Grundlagen Rechnernetze und Verteilte Systeme (IN0010)

Übungsblatt 8

27. Juni – 1. Juli 2022

Aufgabe 1 Neighbor Discovery Protocol und IP-Fragmentierung bei IPv6

In Abbildung 1.1 ist eine Anordnung von Netzkomponenten mit ihren MAC-Adressen dargestellt. PC1 und PC2 seien mittels SLAAC sowohl Link-Local (LL) als auch Global-Unique (GU) Adressen zugewiesen. Für letztere werde das Präfix $2001:db8:1::/64$ (PC1/R1) bzw. $2001:db8:2::/64$ (PC2/R2) verwendet. PC1 sendet ein IP-Paket mit 1400 B Nutzdaten an PC2. Die MTU auf dem WAN-Link zwischen R1 und R2 betrage $1280 B^1$. Innerhalb der lokalen Netzwerke gelte die für Ethernet übliche MTU von $1500 B$.

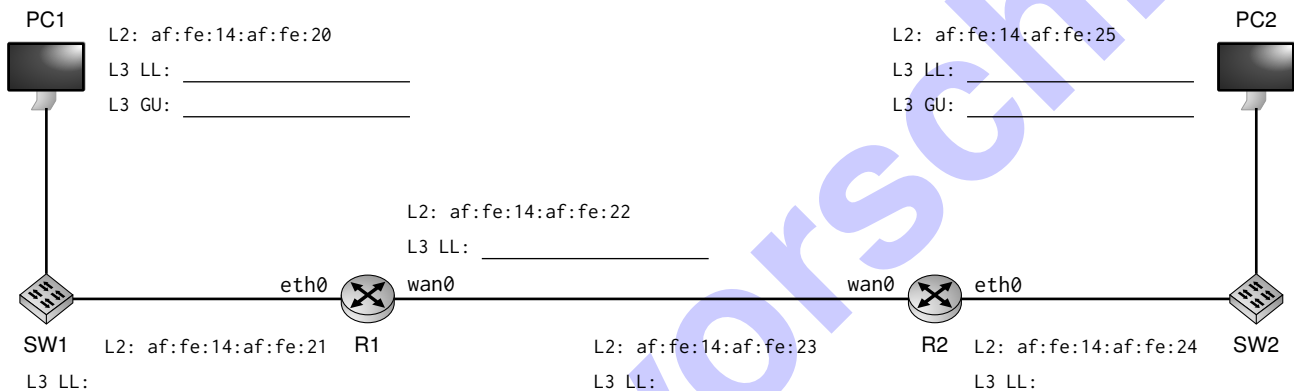


Abbildung 1.1: Netztopologie

Zunächst soll die Adressvergabe mittels SLAAC nachvollzogen werden.

a)* Bestimmen Sie die Link-Local Adressen aller Interfaces.

Siehe Vorlesung:

- PC1: af:fe:14:af:fe:20 → fe80::adfe:14ff:feaf:fe20
- R1.eth0: af:fe:14:af:fe:21 → fe80::adfe:14ff:feaf:fe21
- R1.eth1: af:fe:14:af:fe:22 → fe80::adfe:14ff:feaf:fe22
- R2.eth1: af:fe:14:af:fe:23 → fe80::adfe:14ff:feaf:fe23
- R2.eth0: af:fe:14:af:fe:24 → fe80::adfe:14ff:feaf:fe24
- PC2: af:fe:14:af:fe:25 → fe80::adfe:14ff:feaf:fe25

Hinweis: Das zweite Bit des ersten Oktetts jeder MAC-Adresse wird invertiert.

Grund: Manuell vergebene IPv6-Adressen haben häufig einen Interface-Identifizier der Form $::abcd$, d. h. die ersten 48 Bit sind 0. Schließt man nun von einer solchen IPv6-Adresse auf die zugrundeliegende MAC-Adresse, wäre das vorletzte Bit deren ersten Oktetts 0, was auf eine global eindeutige MAC-Adresse hinweisen würde – was offensichtlich falsch ist, da diese ja von einer manuell vergebenen IPv6-Adresse stammt.

Würde man dieses Bit nicht invertieren, müssten alle manuell vergebenen Interface-Identifizier von der Form $2001:db8:1:0:200::1$ sein (oder, falls die einmalige Abkürzung mehrerer Nullgruppen bereits im Subnet-Identifizier lag, von der Form $2001:db8::200:0:0:1$).

¹ Dies entspricht der minimalen MTU, die laut RFC 2460 Schicht 2 für IPv6 unterstützen muss.

b) Bestimmen Sie die Global-Unique Adressen von PC1 und PC2. Nehmen Sie dazu an, dass Router R1 mit dem Präfix $2001:db8:1::/64$ und Router R2 mit $2001:db8:2::/64$ konfiguriert sind.

Die Herleitung geschieht analog zu den Link-Local-Adressen, allerdings mit dem Präfix des jeweiligen Routers, welche über Router Advertisements PC1 und PC2 bekannt gemacht werden.

- $af:fe:14:af:fe:20 \rightarrow 2001:db8:1:0:adfe:14ff:feaf:fe20$
- $af:fe:14:af:fe:25 \rightarrow 2001:db8:2:0:adfe:14ff:feaf:fe25$

c)* An welcher Stelle im Netzwerk wird die Fragmentierung stattfinden?

Direkt an PC1, da bei IPv6 keine Fragmentierung an Routern stattfindet.

d)* In wie viele Fragmente muss das Paket mindestens aufgeteilt werden?

Die MTU (Maximum Transmission Unit) ist die maximale Größe eines Pakets auf Schicht 3 inkl. Header. Sie entspricht also genau der maximalen Größe der Payload auf Schicht 2. Im Falle von Fragmentierung werden die einzelnen Fragmente jeweils einen IPv6-Header der Länge 40 B sowie einen Fragment Header der Länge 8 B tragen. Sofern keine weiteren Extension Header zum Einsatz kommen, erhalten wir demnach:

$$N = \left\lceil \frac{1400 \text{ B}}{1280 \text{ B} - 40 \text{ B} - 8 \text{ B}} \right\rceil = 2$$

e) Bestimmen Sie die Größe der L3-SDU für jedes Fragment.

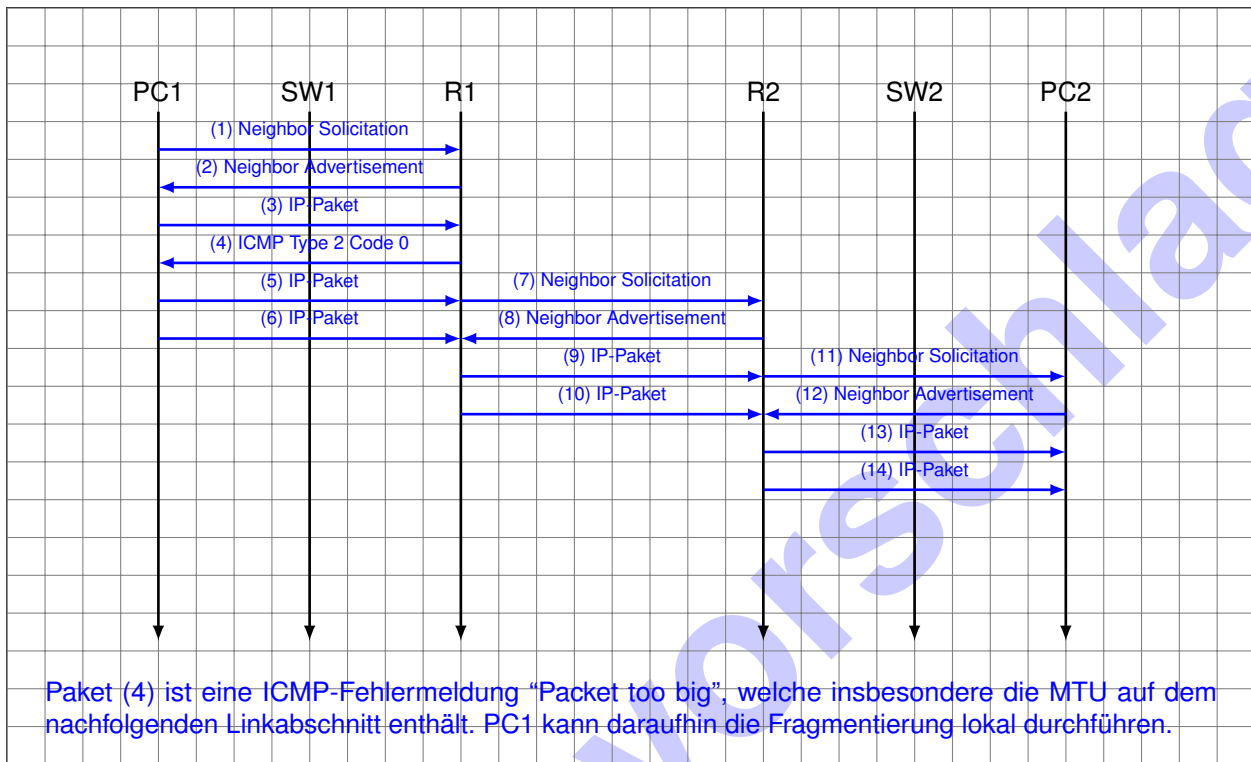
Pro Fragment können $1280 \text{ B} - 40 \text{ B} - 8 \text{ B} = 1232 \text{ B}$ Nutzdaten übertragen werden. Da es sich dabei auch um ein Vielfaches von acht handelt (Fragment Offset ist in Vielfachen von 8 B angegeben), entspricht dies auch der tatsächlich übertragbaren Nutzdatenmenge. Das erste Fragment hat daher eine Payload von 1232 B und das zweite eine Payload von 168 B.

f)* Begründen Sie, an welcher Stelle im Netzwerk werden die Fragmente reassembliert werden.

Erst der Empfänger, hier also PC2, reassembliert die Fragmente wieder. Tatsächlich kann i. A. kein anderer Knoten die Reassemblierung durchführen, da die Fragmente jeweils einzelne und voneinander unabhängige Pakete darstellen. Dies bedeutet insbesondere, dass sie unabhängig voneinander geroutet werden und daher u. U. verschiedene Wege zum Ziel nehmen können – das sieht man aus dem einfachen Beispiel in Abbildung 1.1 natürlich nicht, da es hier nur einen Pfad zwischen PC1 und PC2 gibt.

g) Skizzieren Sie ein einfaches Weg-Zeit-Diagramm, welches **alle Rahmen** berücksichtigt, die auf den jeweiligen Verbindungen übertragen werden müssen. **Nennen Sie die Art der ausgetauschten Rahmen und geben Sie den Rahmen Nummern (1,2,3,...).** (Das Diagramm muss nicht maßstabsgetreu sein. Serialisierungszeiten und Ausbreitungsverzögerungen sind zu vernachlässigen.) **Gehen Sie davon aus, dass derzeit keinerlei Mappings zwischen IP- und MAC-Adressen gecached sind.**

Nummerieren Sie die einzelnen Pakete spaltenweise (Spalte $\hat{=}$ Bereich z. B. zwischen R1 und R2).



h) Bestimmen Sie die Destination-MAC-Adresse des ersten übertragenen Rahmens.

Der Rahmen enthält ein IPv6 Neighbor Solicitation Paket. Diese werden laut Vorlesung an die entsprechende Solicited-Node Adresse geschickt. Da diese Multicast Adressen sind, berechnet sich die Destination-MAC-Adresse aus der Solicited-Node Adresse.

Es soll die MAC Adresse für R1 mit der IP `fe80::adfe:14ff:feaf:fe21` erfragt werden. Mit dem Solicited-Node Prefix `ff02::1:ff00:0/104` und den letzten 24 bit der Ziel Adresse ergibt sich die Solicited-Node Adresse `ff02::1:ffaf:fe21`. Diese liegt im Prefix `ff00::/8` und ist somit eine Multicast Adresse. Deshalb wird die zugehörige MAC aus dem Prefix `33:33` und den letzten 32 bit der Ziel Adresse `ff02::1:ffaf:fe21` berechnet und es ergibt sich `33:33:ff:af:fe:21`.

Am Ende dieses Übungsblatts finden Sie Vordrucke für Ethernet-Header, ICMPv6 und IP-Header (mehr als benötigt). Es ist nicht notwendig, den Header binär auszufüllen. Achten Sie lediglich darauf, dass Sie die Zahlenbasis deutlich kennzeichnen, z. B. $0x10$ für hexadezimal oder $63_{(10)}$ für dezimal.

i) Füllen Sie für die ersten beiden Rahmen aus Teilaufgabe g) jeweils einen Ethernet- und einen IP-Header sowie die passende Payload aus. Beschriften Sie die gestrichelte Box neben dem jeweiligen Header/Paket mit der jeweiligen Rahmennummer.

Hinweis: Nutzen Sie den Cheatsheet zum bestimmen der Werte (z. B. Next Header). Sollte ein Wert nicht eindeutig bestimmt sein, treffen Sie eine sinnvolle Wahl.

j) Füllen Sie pro Pfadabschnitt (z. B. zwischen R1 und R2) für das jeweils erste fragmentierte Paket jeweils einen Ethernet- und einen IP-Header aus. Beschriften Sie die gestrichelte Box neben dem jeweiligen Header/Paket mit der jeweiligen Rahmennummer.

Hinweis: Nutzen Sie den Cheatsheet zum bestimmen der Werte (z. B. Next Header). Sollte ein Wert nicht eindeutig bestimmt sein, treffen Sie eine sinnvolle Wahl.

f) Benennen und beschreiben Sie die drei kleinsten Headerfelder von Schicht 3. Geben Sie zudem die Größe der beschriebenen Headerfelder an.

Die drei kleinsten Headerfelder alle eine Größe von 1 bit.

RES reserved, reserviert um unter Umständen in Zukunft verwendet werden zu können

DF do not fragment, weißt den Verarbeitenden an, dass dieses Paket nicht fragmentiert werden darf

MF more fragments, informiert, dass — aufgrund einer vorangegangenen Fragmentierung — zu diesem IPv4 Paket weitere Fragmente gehören.

g) Falls es eine L3-SDU gibt, geben Sie ihren Typ an und begründen Sie die Angabe. Andernfalls, legen Sie Ihren Gedankengang dar und erörtern wie es zu dieser Situation kommen konnte.

Der Wert des IPv4 Headerfelds Protocol ist 0x06. Demnach ist die L3-SDU TCP.

h) Die Bytes 0x0042 und Folgende sind Payload von Schicht 4. Geben Sie die ASCII Darstellung der ersten 7 B der Payload an.

Die ASCII Darstellung von 0x53 53 48 2d 32 2e 30 ist SSH-2.0.

i) Um welches Protokoll der Anwendungsschicht handelt es sich also vermutlich und wozu wird dieses Protokoll verwendet?

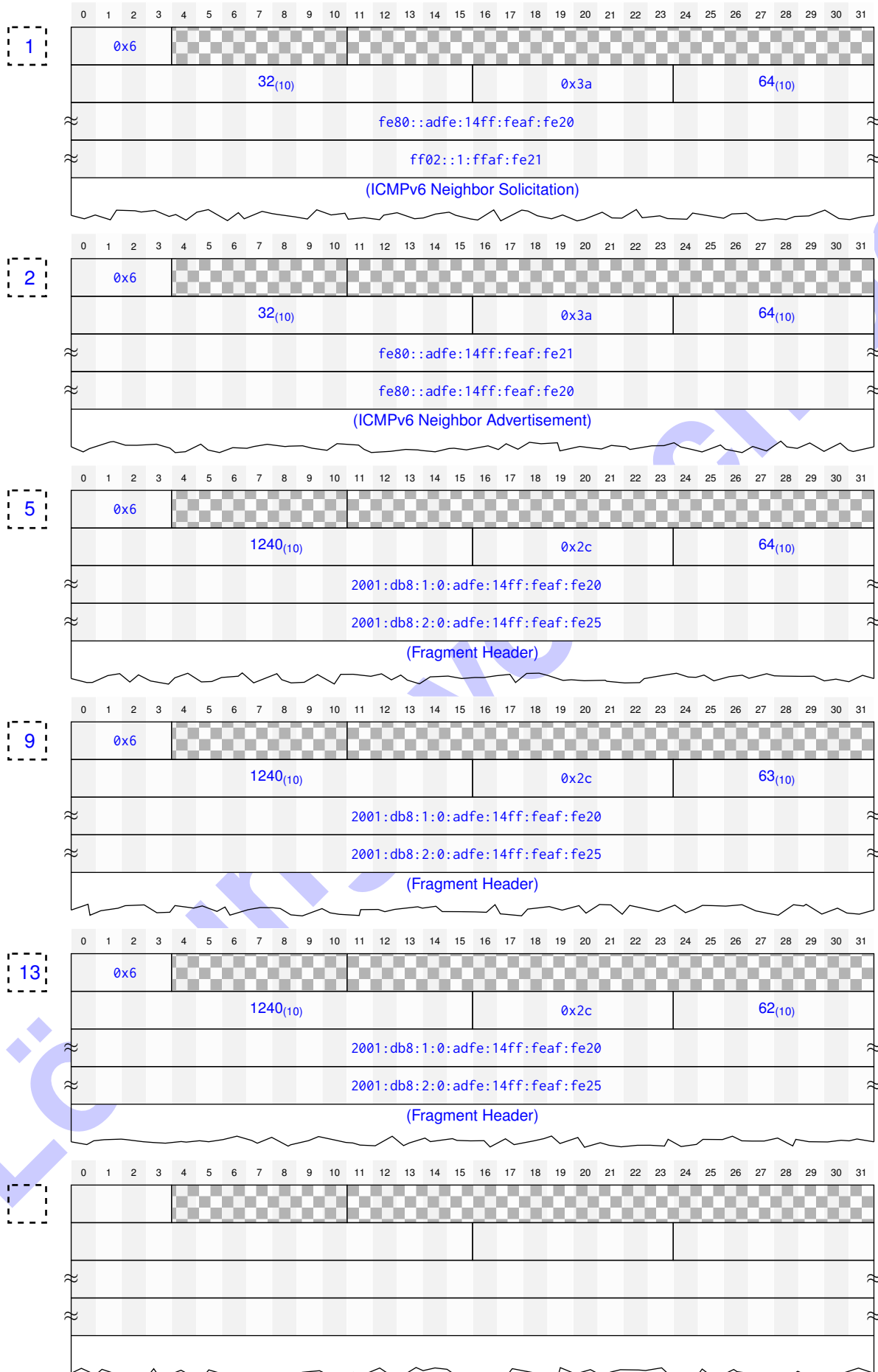
Es handelt sich um SSH (Version 2.0), das für eine verschlüsselte Konsolensitzung unter Linux/Unix und neuerdings auch unter Windows verwendet wird.

Vordrucke für Protokoll-Header:

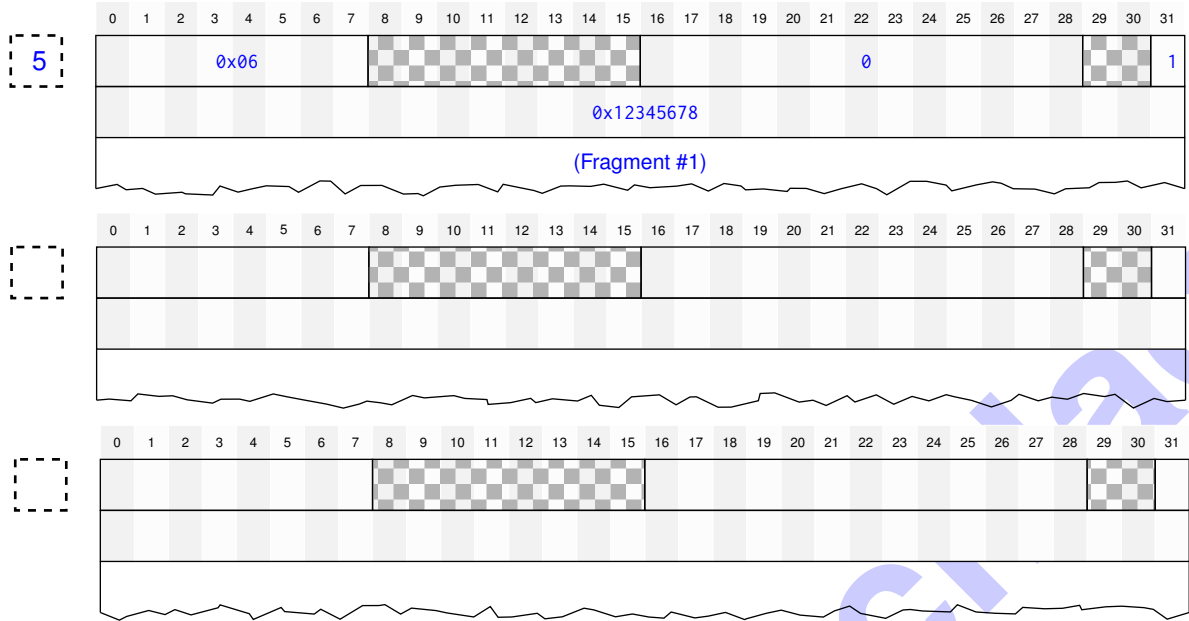
Ethernet-Frames

1	33:33:ff:af:fe:21	af:fe:14:af:fe:20	0x86dd	Payload	FCS
2	af:fe:14:af:fe:20	af:fe:14:af:fe:21	0x86dd	Payload	FCS
5	af:fe:14:af:fe:21	af:fe:14:af:fe:20	0x86dd	Payload	FCS
9	af:fe:14:af:fe:23	af:fe:14:af:fe:22	0x86dd	Payload	FCS
13	af:fe:14:af:fe:25	af:fe:14:af:fe:24	0x86dd	Payload	FCS
				Payload	FCS
				Payload	FCS
				Payload	FCS
				Payload	FCS
				Payload	FCS
				Payload	FCS
				Payload	FCS
				Payload	FCS
				Payload	FCS
				Payload	FCS
				Payload	FCS

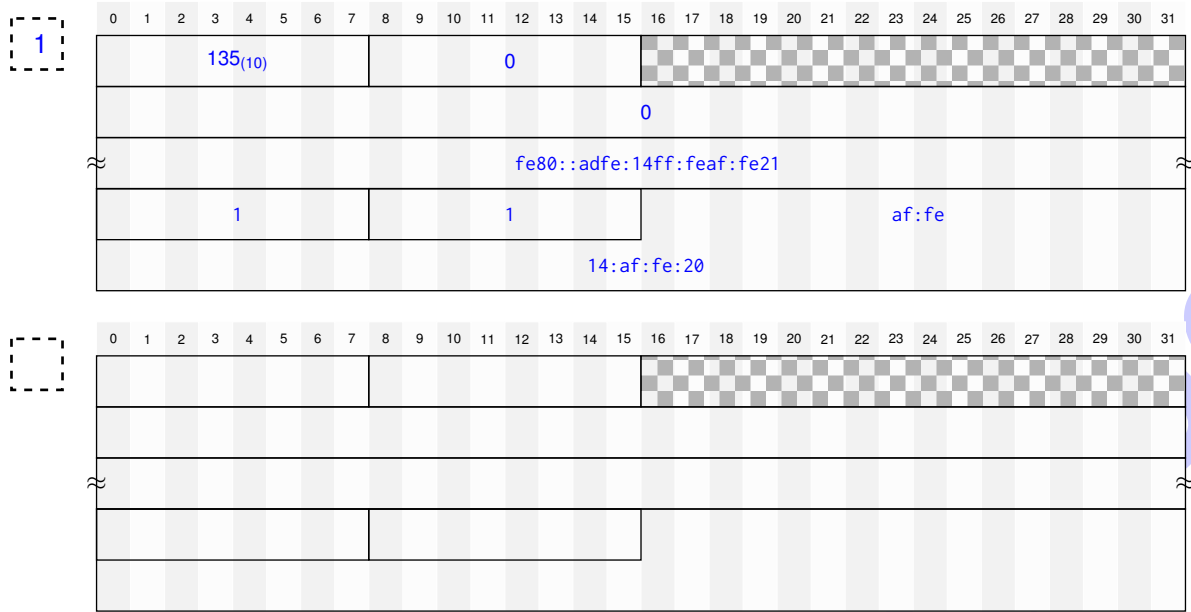
IPv6 Header



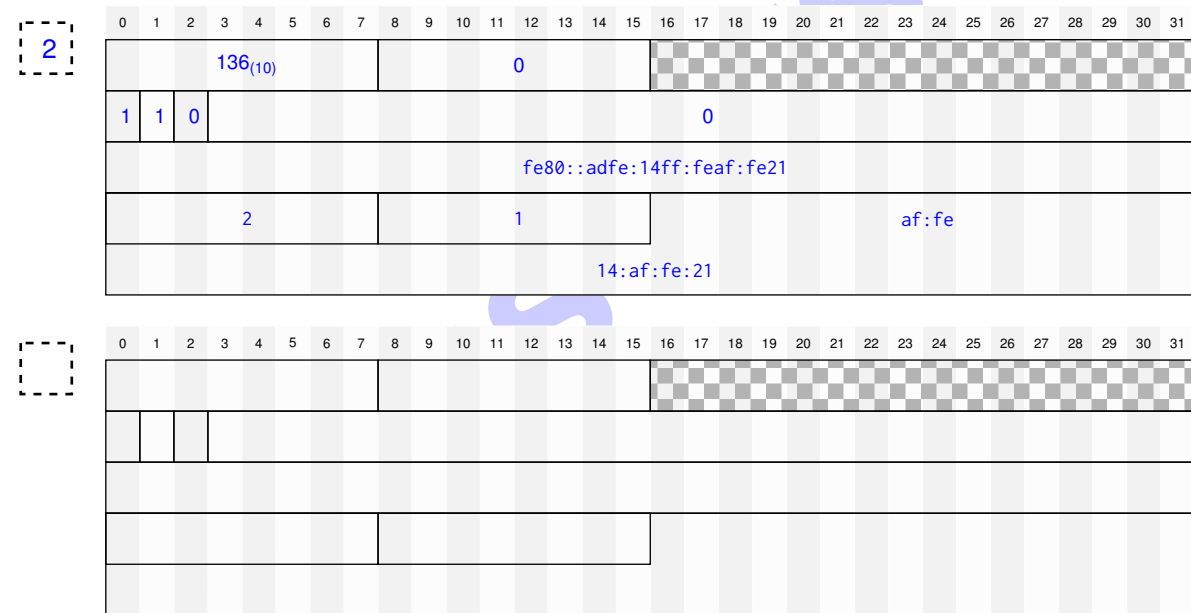
IPv6 Fragment Header

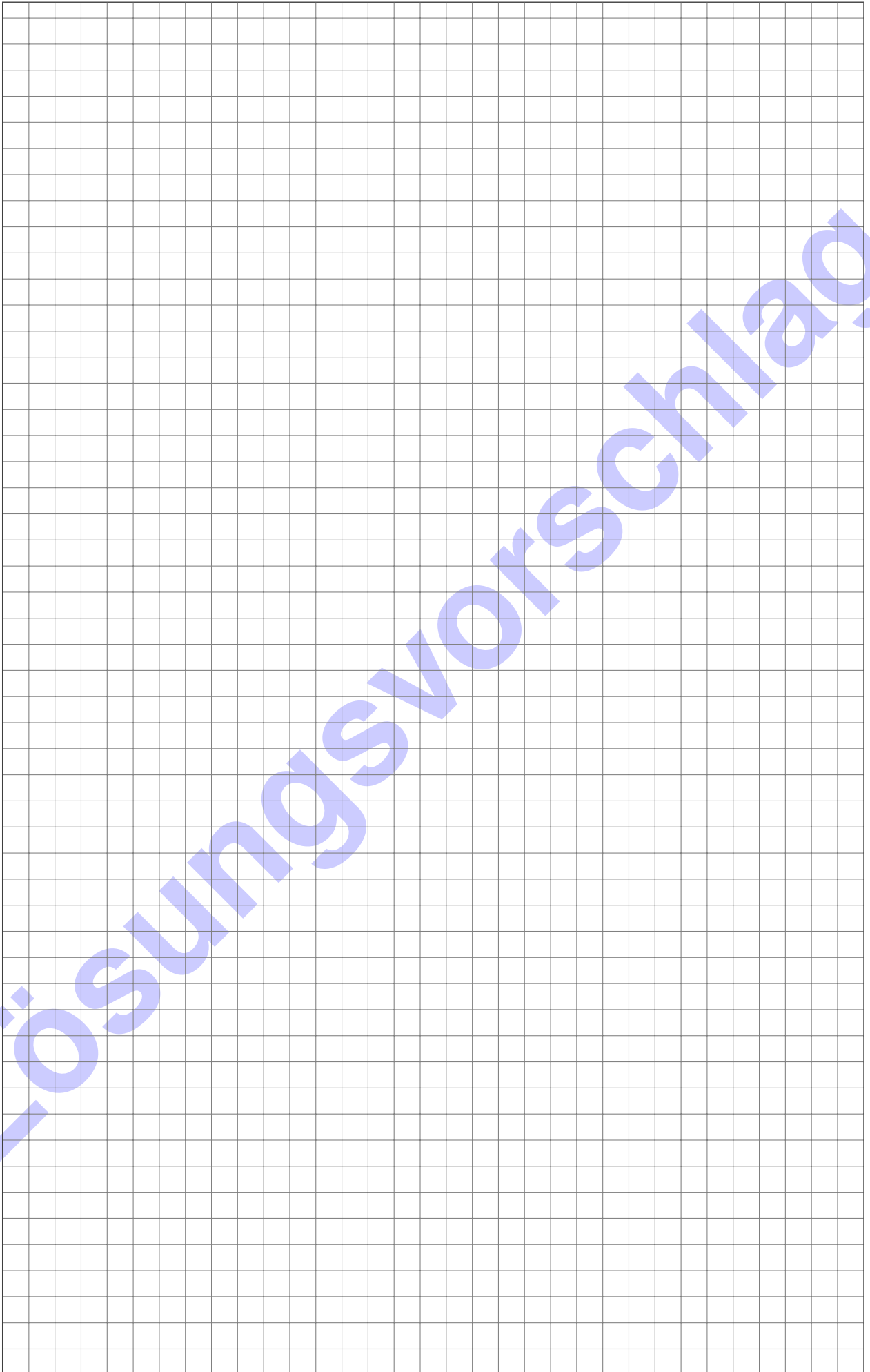


ICMPv6 Neighbor Solicitation



ICMPv6 Neighbor Advertisement





Lösungsvorschlag