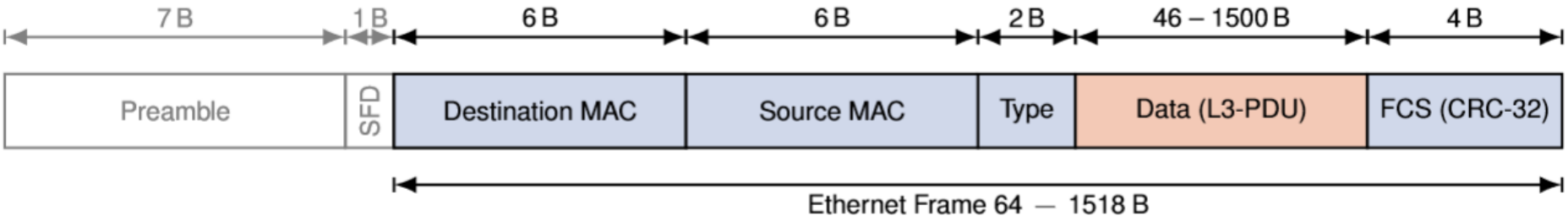
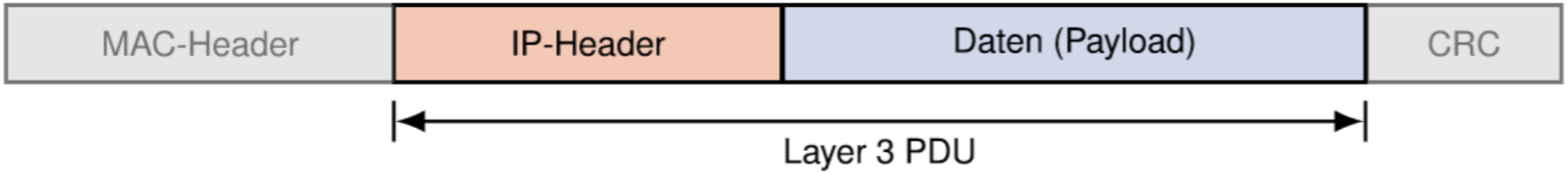
Repetitorium Grundlagen Rechnernetze und Verteilte Systeme

Niels Mündler

Garching, 21.9.2018



Quelle: https://grnvs.net



Quelle: https://grnvs.net

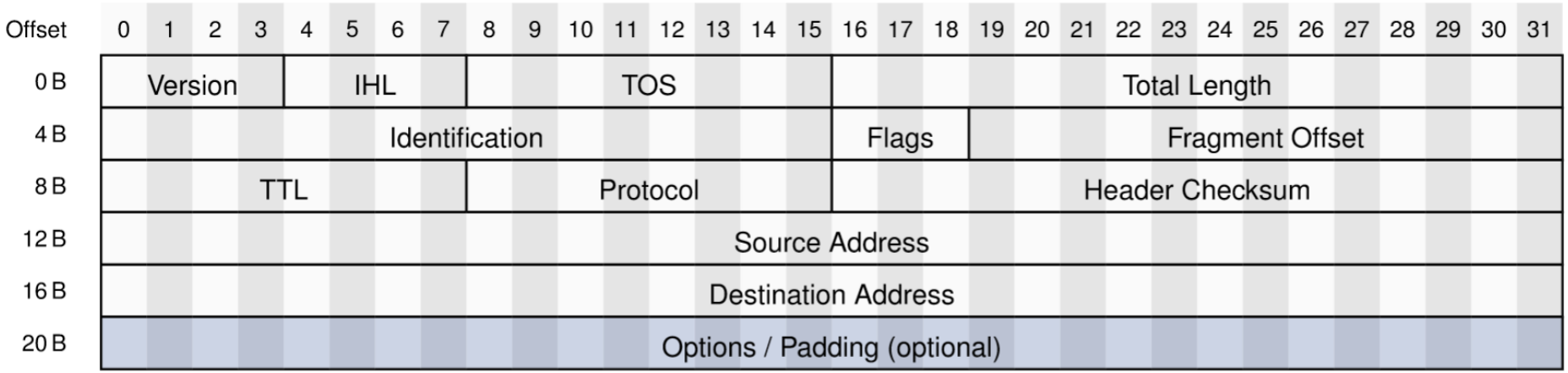


Abbildung 1: IPv4-Header (minimale Länge: 20 B)

Quelle: https://grnvs.net

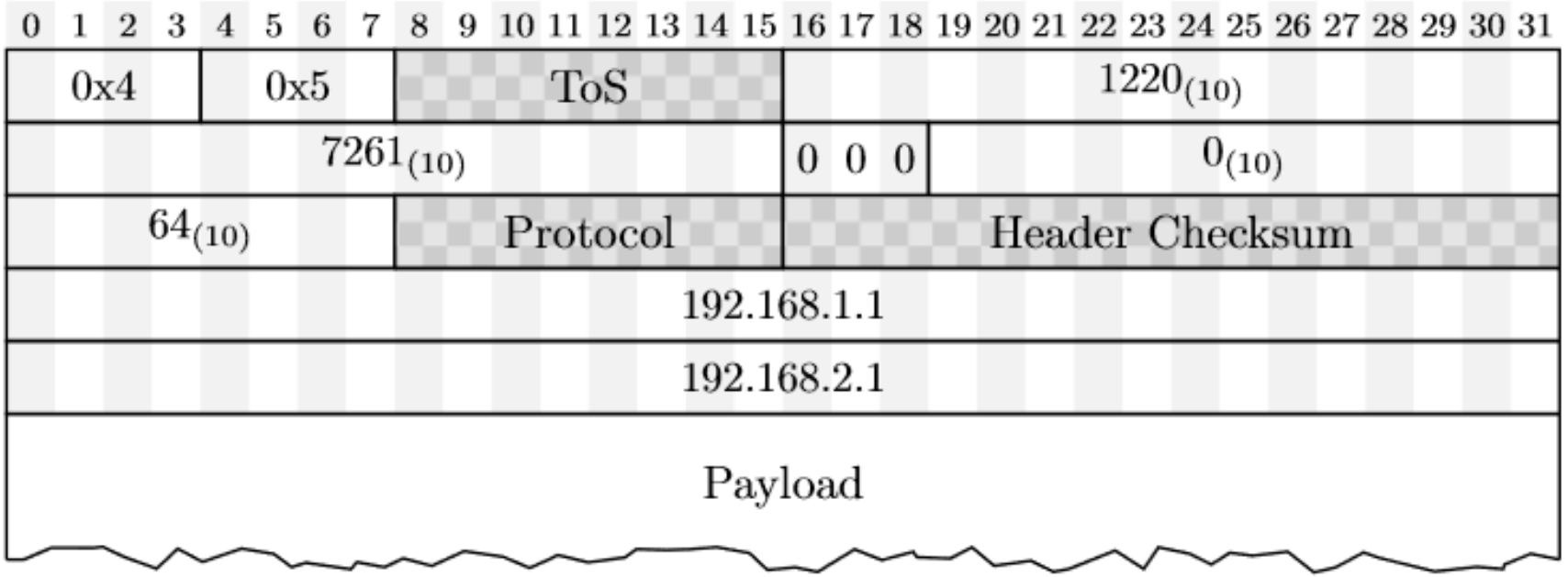


Abbildung 3.2: Schematische Darstellung des von PC1 gesendeten IP-Pakets

e)* Welche Größe besitzt der IP-Header des in Abbildung 3.2 dargestellten Pakets?

f)* Wie groß ist die Payload des in Abbildung 3.2 dargestellten Pakets?

Quelle: https://grnvs.net

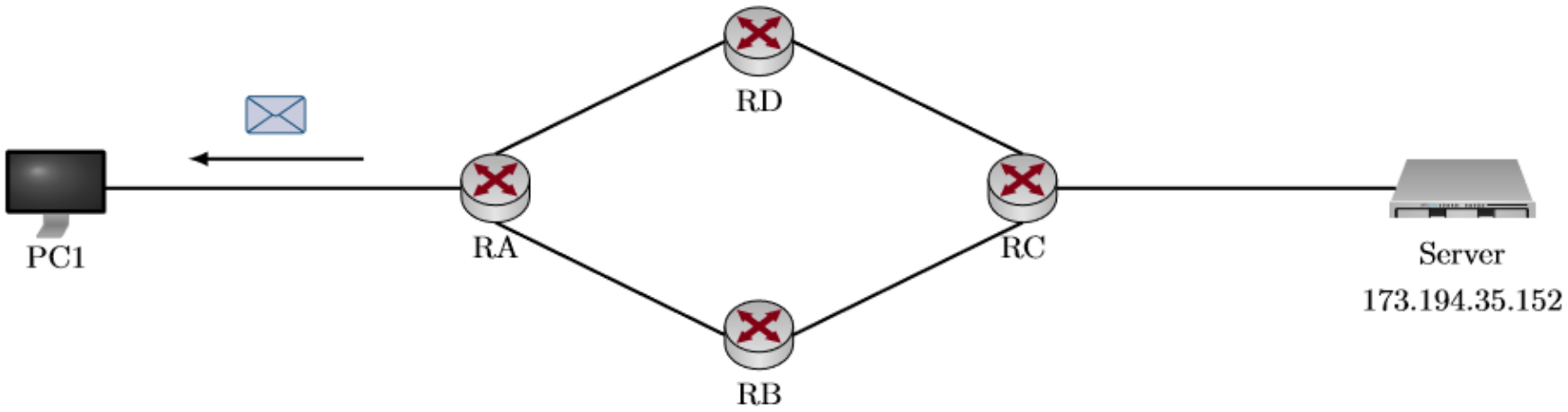


Abbildung 4.1: Vereinfachte Netztopologie (Switches zwischen den Geräten sind der Übersichtlichkeit wegen nicht eingezeichnet)

Quelle: https://grnvs.net

Retake 2012 Aufgabe 4

Sie beschließen deshalb, den Netzwerkverkehr an PC1 mit einem Sniffer[1] zu überprüfen, während Sie erneut versuchen, eine Verbindung zum Server aufzubauen. Dabei zeichnen sie die in Abbildung 4.1 eingezeichnete Nachricht auf, welche an PC1 adressiert ist. Diese Nachricht ist als Hexdump in Abbildung 4.2 abgedruckt. Die linke Spalte gibt den Offset (hexadezimal) in Vielfachen von Bytes an. Die beiden nachfolgenden Spalten repräsentierten die Daten (hexadezimal) in Blöcken zu je 8 Byte in Network-Byte-Order.

```
0000    28 37 37 02 32 41 00 25    90 57 1f dc 08 00 45 00
0010    00 38 b2 40 00 00 3f 01    b1 57 83 9f fc 95 83 9f
0020    14 59 0b 00 5e a4 00 00    00 00 45 00 00 40 16 17
0030    40 00 01 06 fa 4e 83 9f    14 59 ad c2 23 98 e8 fc
0040    01 bb 22 67 a5 d2
```

Abbildung 4.2: Hexdump der in Abbildung 4.1 dargestellten Nachricht (inkl. L2-Header) in Network-Byte-Order.

Im Folgenden werden wir diese Nachricht schrittweise untersuchen und herausfinden, aus welchem Grund der Server nicht erreichbar ist. **Nutzen Sie zur Lösung die auf dem Beiblatt abgegebildeten Protokoll-Header und Zusatzinformationen.**

Quelle: https://grnvs.net

Gegeben sei die Netztopologie aus Abbildung 3.1. PC1 und PC2 sind über ein gewöhnliches Ethernet-Switch SW1 mit Router R1 verbunden, welches Zugang zum Internet ermöglicht.

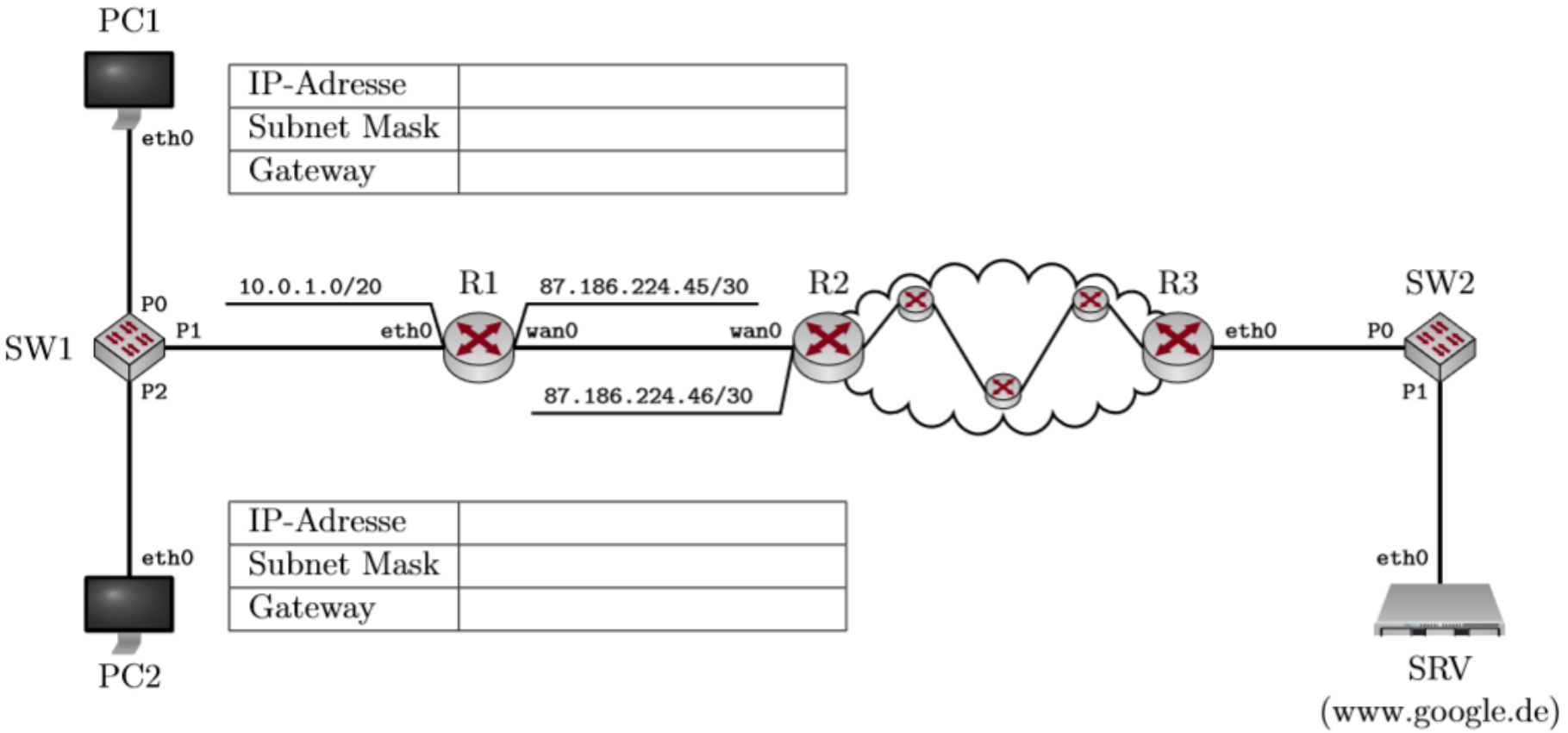


Abbildung 3.1: Netztopologie

a)* Begründen Sie, ob die Adresse 10.0.1.0 für das gegebene Präfix nutzbar ist. Falls nein, vergeben Sie an R1 eine sinnvolle Adresse im selben Netz.

Quelle: https://grnvs.net

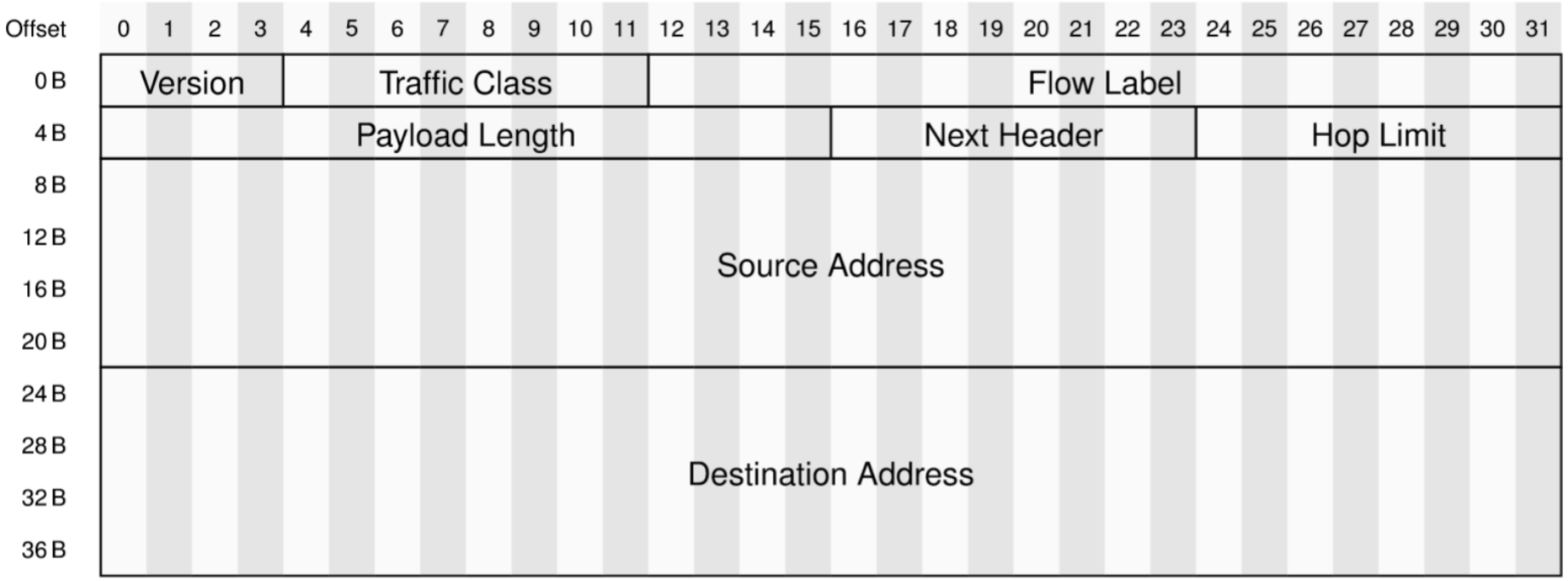


Abbildung 5: IPv4-Header (oben) und IPv6-Header (unten) im Vergleich

IPv6 verfügt zu diesem Zweck über einen eigenen Extension Header, den Fragment Header:

Abbildung 7: Fragment Header

Quelle: https://grnvs.net

Retake 2014 Aufgabe 3

Aufgabe 3 Hexfun (21 Punkte)

Gegeben sei der Hexdump aus Abbildung 3.1, welcher einen 86 B langen Rahmen (Ethernet ohne FCS) darstellt. Die linke Spalte gibt den Offset (hexadezimal) in Vielfachen von Bytes an. Die beiden nachfolgenden Spalten repräsentieren die Daten (hexadezimal) in Blöcken zu je 8 Byte in Network-Byte-Order.

```
0x0000:  08 60 6e 45 dc e6 00 1c   14 01 4e 18 86 dd 60 00
0x0010:  00 00 00 20 06 40 2a 01   04 f8 0d 16 19 43 00 00
0x0020:  00 00 00 00 00 02 2a 02   02 e0 03 fe 10 01 77 77
0x0030:  77 2e 00 02 00 85 ce 44   00 50 9b 94 59 c9 2f e7
0x0040:  5d 10 50 10 65 00 85 88   00 00 47 45 54 20 2f 68
0x0050:  65 78 0d 0a 0d 0a
```

Abbildung 3.1: Hexdump eines Ethernet-Rahmens (inkl. L2-Header) in Network-Byte-Order.

Im Folgenden werden wir diese Nachricht schrittweise untersuchen. **Nutzen Sie zur Lösung die auf dem Beiblatt abgebildeten Protokoll-Header und Zusatzinformationen.**

Quelle: https://grnvs.net

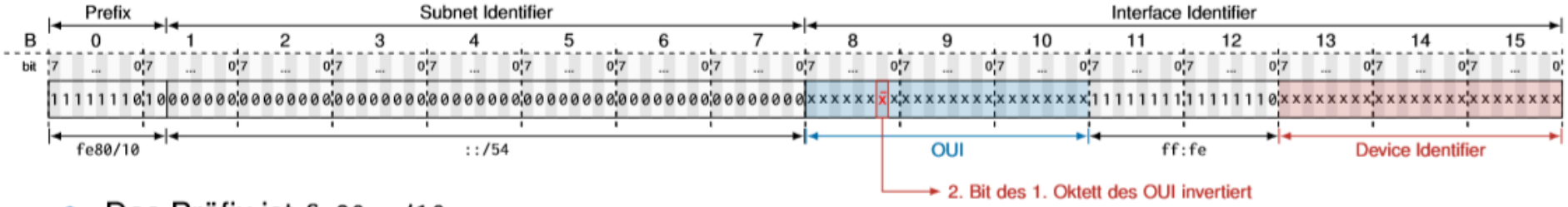
d)* Gegeben sei `fe80::222:b0ff:febc:1fe2/64`. Zu welchem Protokoll gehört diese Adresse?

Quelle: https://grnvs.net

Stateless Address Autoconfiguration (SLAAC) [17]

IPv6 erlaubt eine automatische Konfiguration von Hosts innerhalb eines einzelnen Subnetzes.

Ein Host generiert sich die für ein Interface benötigte link-local IPv6-Adresse wie folgt:



- Das Präfix ist `fe80::/10`.
- Der Subnet Identifier (die folgenden 54 bit) werden auf `0` gesetzt.
- Die verbleibenden 64 bit stellen den Interface Identifier dar, welcher aus der MAC-Adresse des jeweiligen Interfaces als modifizierter EUI-64 Identifier generiert wird:
  - Die ersten 24 bit sind der OUI der MAC-Adresse.
  - Die nachfolgenden 16 bit werden mit `ff:fe` „gestopft“.
  - Die restlichen 24 bit werden mit dem Device Identifier der MAC-Adresse aufgefüllt.
- Dabei das vorletzte Bit des ersten Oktett des OUI (global/local-Bit) invertiert:
  - Bei MAC-Adressen bedeutet eine `0` an dieser Bitstelle eine global eindeutige und eine `1` eine lokal administrierte Adresse (siehe Kapitel 2).
  - Bei IPv6 ist es genau andersrum: Durch die Invertierung wird erreicht, dass eine manuell konfigurierte IPv6-Adresse wie `2001:db8::1` nicht einen Interface Identfier enthält, der auf eine global eindeutige MAC- Adresse hinweist.
  - Andernfalls müsste man von Hand Adressen wie `2001:db8::200:0:0:1` vergeben ...

Quelle: https://grnvs.net

`ff02::1:ff00:0/104` – Solicited-Node Address

- Die Solicited-Node Adresse wird im Neighbor Discovery Protocol (mehr dazu gleich) verwendet, welches u.a. zur Adressauflösung dient.
- Die Solicited-Node Adresse zu einer IPv6 Adresse wird aus dem Präfix `ff02::1:ff00:0/104` und den letzten 24 bit der ursprünglichen IPv6 Adresse generiert.
- Die Solicited-Node Adresse für `2001:0db8:1ee7:2ea2:0921:2e11:d2c6:938b` ist somit `ff02::1:ffc6:938b`.
- IPv6-Multicasts werden auch auf Schicht 2 mittels Multicast-Adressen versendet.
  - Switches müssen Multicast-Rahmen nur an diejenigen Ports weiterleiten, an denen ein Mitglied der entsprechenden Multicast-Gruppe angeschlossen ist.
  - In großen L2-Netzen können so unnötige Broadcasts vermieden werden.
  - Knoten, für die eine Nachricht nicht von Interesse ist, bekommen diese somit erst gar nicht.

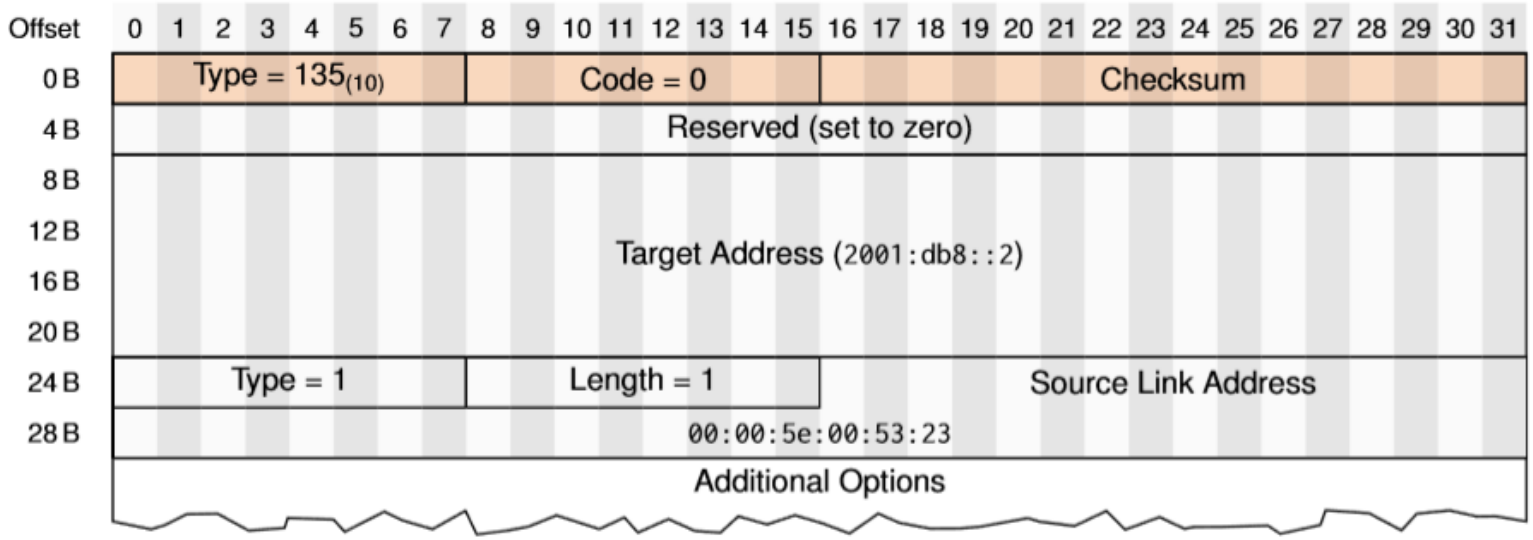
Quelle: https://grnvs.net

Mapping von Multicast IPv6 Adressen auf MAC-Adressen [5]

- IPv6-Pakete mit einer Zieladresse aus dem Präfix `ff00::/8` werden mit der zugehörigen Multicast-Adresse auf Schicht 2 (Ethernet) versendet.
- Um Multicasts auf Schicht 3 auch auf Schicht 2 abbilden zu können, muss es einen Zusammenhang zwischen den verwendeten Adressen beider Schichten geben.
- Die ersten 2 Oktette der MAC-Adresse werden auf `33:33` gesetzt.
  - letztes Bit des ersten Oktetts ist gesetzt → Multicast
  - vorletztes Bit des ersten Oktetts ist gesetzt → locally administered
  - siehe Kapitel 2
- Die letzten 4 Oktette der Ethernetadresse werden die letzten 4 Oktette der IPv6 Multicastadresse.

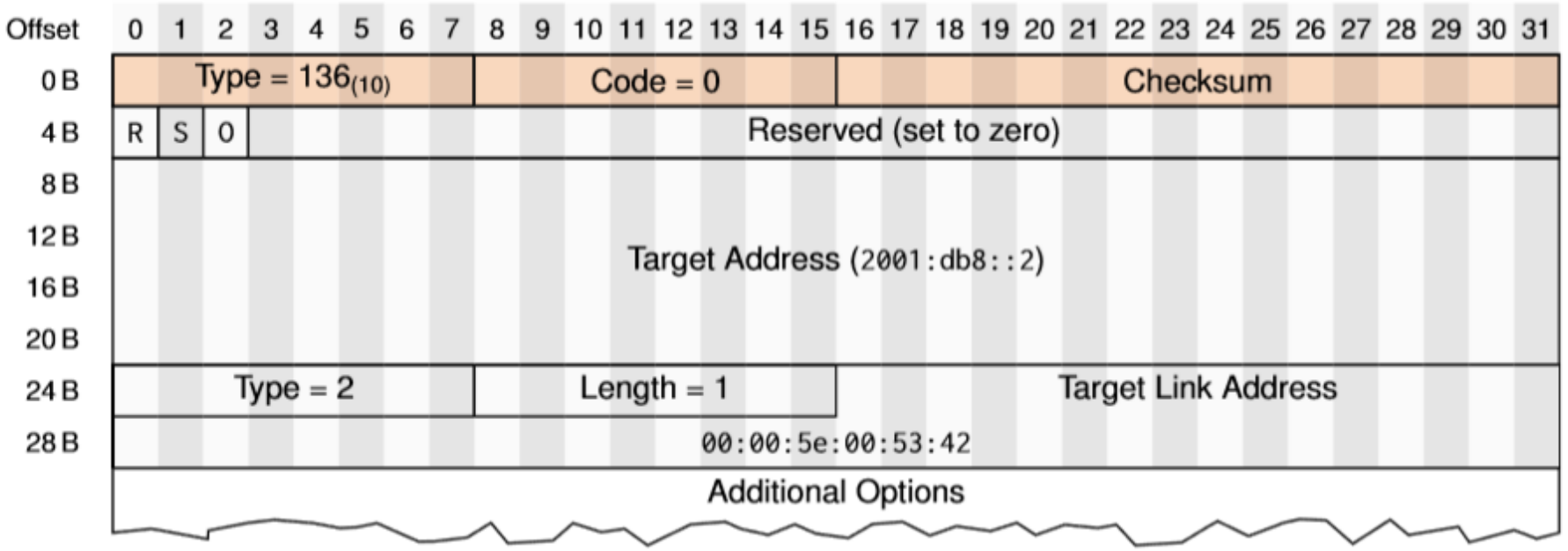
Quelle: https://grnvs.net

Neighbor Discovery Protocol (NDP) [13] – Neighbor Solicitation (Request)



Quelle: https://grnvs.net

Neighbour Advertisement (Reply)



Quelle: https://grnvs.net

Übungsblatt 8 Aufgabe 1

Quelle: https://grnvs.net

Übungsblatt 8 Aufgabe 2

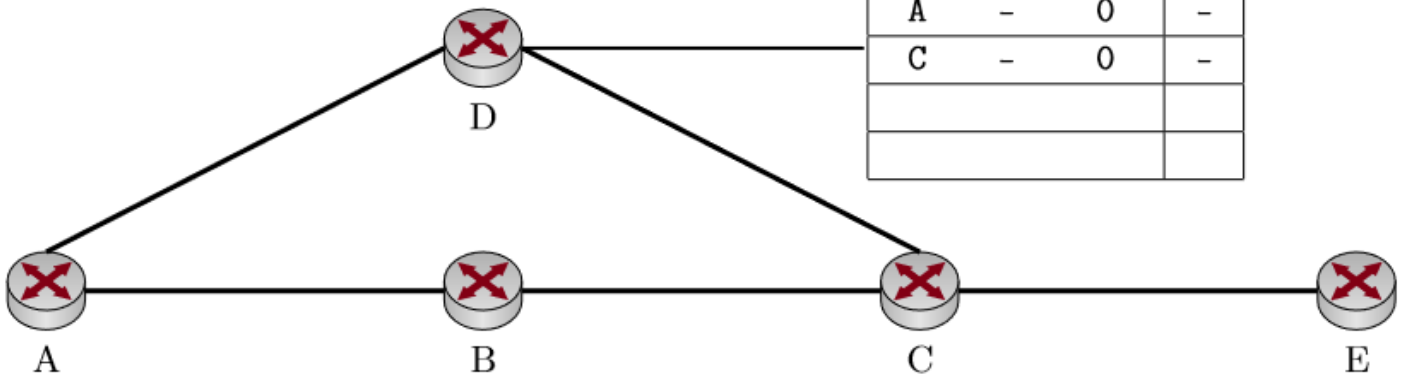
Quelle: https://grnvs.net

Endterm 2012

Aufgabe 4 Dynamisches Routing (15 Punkte)

15

Gegeben sei das in Abbildung 4.1 vereinfacht dargestellte Netzwerk. Alle Router verwenden RIP als Routingprotokoll. Die Tabellen unterhalb der Router A – E in Abbildung 4.1 stellen die Routingtabelle des jeweiligen Routers dar, bevor RIP gestartet wird.



Dst	GW	Cost	TA
A	-	0	-
C	-	0	-

Dst	GW	Cost	TA
B	-	0	-
D	-	0	-

Dst	GW	Cost	TA
A	-	0	-
C	-	0	-

Dst	GW	Cost	TA
B	-	0	-
D	-	0	-
E	-	0	-

Dst	GW	Cost	TA
C	-	0	-

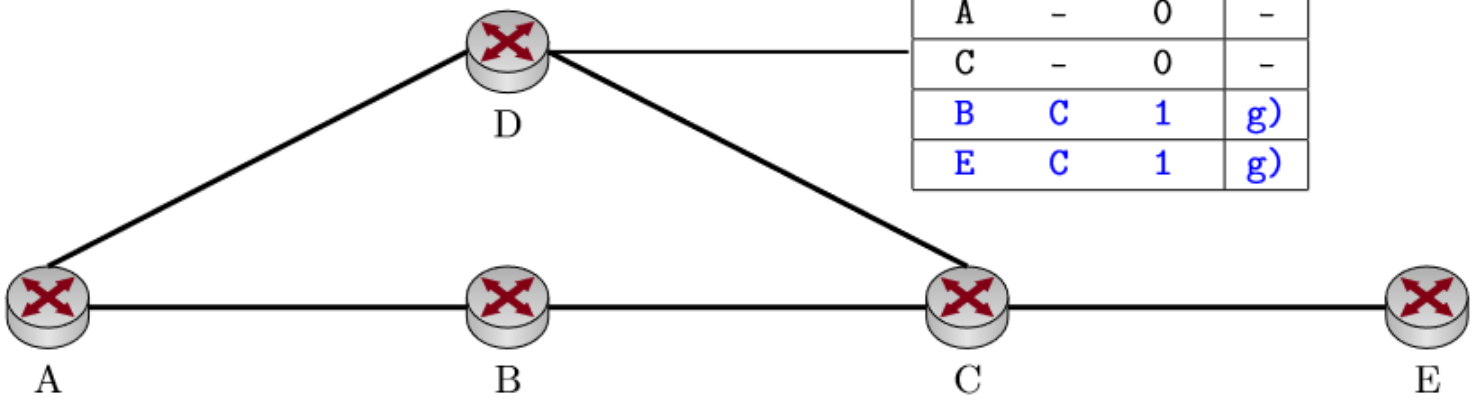
Abbildung 4.1: Netztopologie

Quelle: https://grnvs.net

Endterm 2012

Aufgabe 4 Dynamisches Routing (15 Punkte)

Gegeben sei das in Abbildung 4.1 vereinfacht dargestellte Netzwerk. Alle Router verwenden RIP als Routingprotokoll. Die Tabellen unterhalb der Router A – E in Abbildung 4.1 stellen die Routingtabelle des jeweiligen Routers dar, bevor RIP gestartet wird.



Dst	GW	Cost	TA
A	-	0	-
C	-	0	-
B	C	1	g)
E	C	1	g)

Dst	GW	Cost	TA
B	-	0	-
D	-	0	-
C	B	1	f)
E	D	2	h)

Dst	GW	Cost	TA
A	-	0	-
C	-	0	-
D	C	1	g)
E	C	1	g)

Dst	GW	Cost	TA
B	-	0	-
D	-	0	-
E	-	0	-
A	B	1	f)

Dst	GW	Cost	TA
C	-	0	-
A	C	2	g)
B	C	1	g)
D	C	1	g)

Abbildung 4.1: Netztopologie

Quelle: https://grnvs.net

Endterm 2015 Aufgabe 4

Quelle: https://grnvs.net