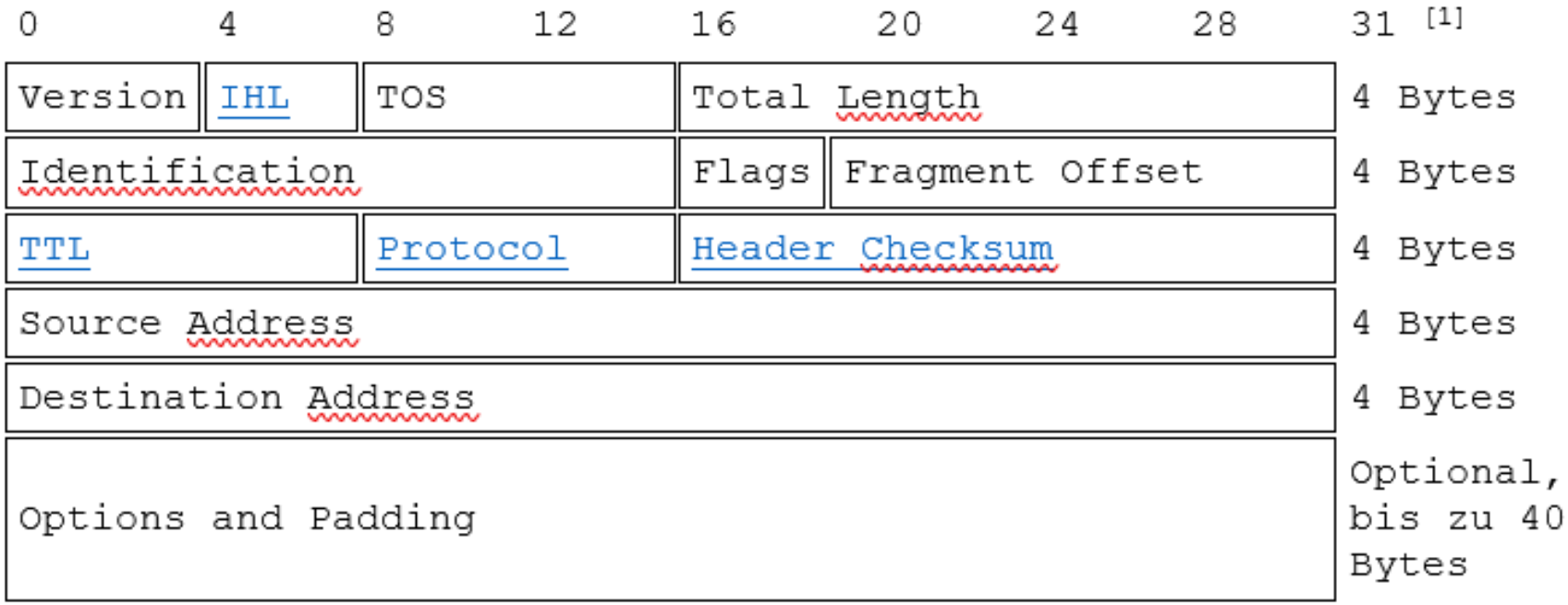
IPv4



Aufbau des Kopfdatenbereiches (IP-Header)

Der IPv4-Kopfdatenbereich umfasst 20 Byte plus bis zu 40 Byte optionale Felder, die Länge des Kopfes darf 60 Byte nicht überschreiten. Der IPv6-Header ist 40 Byte lang; Optionen werden hier in eigenen Erweiterungsheadern dargestellt.

Entnommen aus https://de.wikipedia.org/wiki/IP-Paket

Erläuterung für IPv4

- **Version**
- 4 Bit groß. Die IP-Version. Hierbei sind Version 4 und Version 6 zurzeit möglich, wobei Version 4 die im Internet meistgenutzte ist.
- **IHL (Internet Header Length)**
- 4 Bit groß. Die gesamte Länge des IP-Kopfdatenbereiches wird in Vielfachen von 32 Bit angegeben. Steht hier also eine 5, so ist der Kopfdatenbereich 5 mal 32 Bit gleich 160 Bit oder 20 Byte lang, was auch die Minimallänge für den IP-Kopfdatenbereich ist (das Options-Feld ist optional) und dadurch anzeigt, wo die Nutzdaten beginnen.
- n1 bis nx sind Optionen
- Gesamtlänge des Headers = $(5 \cdot 32)$ + (Länge(n1) + … + Länge(nx) + Padding auf 32 Bit)

TOS (Type of Service)

- 8 Bit groß. Das Feld kann für die Priorisierung von IP-Datenpaketen gesetzt und ausgewertet werden (Quality of Service).
- Seit September 2001 (RFC 3168[3]) gilt folgende Aufteilung:
- Bits 0-5: DSCP (Differentiated Services Code Point)
- Bits 6-7: ECN (Explicit Congestion Notification – IP-Staukontrolle)

Total Length & Identification

- **Total Length**
- 16 Bit groß. Gibt die Länge des gesamten Pakets (inkl. Kopfdaten) in Byte an. Daraus ergibt sich eine maximale Paketlänge von 65535 Byte (64 KiB − 1 B). Alle Hosts müssen Datagramme mit einer Länge von mindestens 576 Byte verarbeiten können.
- **Identification**
- 16 Bit groß. Dieses und die beiden folgenden Felder *Flags* und *Fragment Offset* steuern die Reassembly (Zusammensetzen von zuvor fragmentierten IP-Datenpaketen). Eindeutige Kennung eines Datagramms. Anhand dieses Feldes und der 'Source Address' kann der Empfänger die Zusammengehörigkeit von Fragmenten detektieren und sie mit Hilfe des *Fragment Offset* wieder reassemblieren.

Flags

- 3 Bit groß. Die Bits haben folgende Bedeutung:
- Bit 0
- reserviert, muss 0 sein
- Bit 1 – DF (Don’t Fragment)
- Wenn auf 1, zeigt es an, dass das Paket nicht in Fragmente zerlegt (fragmentiert) werden darf
- Bit 2 – MF (More Fragments)
- Wenn auf 1, zeigt es an, dass weitere Fragmente folgen. Wenn auf 0, ist dieses Paket das letzte (bzw. einzige) Fragment.

Fragment Offset

- 13 Bit groß. Eine Nummer, die bei fragmentierten Paketen besagt, ab welcher Position innerhalb des Paketes das Fragment anfängt. Die Nummerierung bezieht sich auf Daten-Blöcke von 64 Bit bzw. 8 Byte Größe und ist unabhängig von der Fragmentierung. Ein Paket kann daher falls notwendig mehrmals hintereinander in immer kleinere Fragmente zerteilt werden. Dabei muss nur die Nummer des ersten enthaltenen Datenblocks (Offset) und das Total-Length-Feld an die Länge des Fragments angepasst werden. Das erste Fragment, oder ein nicht fragmentiertes Paket, enthält als Offset den Wert Null. Ist ein Paket mit 800 Byte Nutzdaten (Offset-Nummerierung von 0 bis 99) in zwei Fragmente zerteilt, ist der Offset des zweiten Fragments die Nummer 50. Da der Offset keinerlei Hinweis enthält, wie groß das ursprüngliche Paket ist, muss das allerletzte Fragment das MF-Flag auf Null setzen.

Time to Live (Lebenszeit)

- 8 Bit groß. Ein Wert, der die Lebensdauer des Pakets angibt. Hat dieses Feld den Wert null, so wird das Paket verworfen. Jede Station (Router) auf dem Weg des Pakets verringert diesen Wert um eins. Dies soll verhindern, dass Pakete ewig weitergeleitet werden (beispielsweise wenn das Paket fälschlicherweise im Kreis geleitet wird und somit das Netz überlasten würde).
- Der Standard von 1981 sieht vor, dass jede Station den TTL-Wert um die Anzahl der Sekunden verringert, die das Paket an der Station verweilt, mindestens jedoch um eins. Heute wird es de facto als Hop-Count implementiert.

Protocol

- 8 Bit groß. Dieses Feld bezeichnet das Folgeprotokoll, zu dem die im betreffenden IPv4-Paket transportierten Nutzdaten gehören. Enthält das IP-Paket zum Beispiel ein TCP-Paket, steht hier der Wert 6, für ein UDP-Paket 17. Diese Werte werden seit RFC 3232[5] von der IANA in einer Online-Datenbank für Protokoll-Nummern definiert.[6]
- Im IPv6-Header gibt es dieses Feld ebenfalls, allerdings heißt es dort *Next Header*. Die zulässigen Werte sind die gleichen wie bei IPv4.

Header Checksum

- 16 Bit groß. Eine Prüfsumme sichert ausschließlich den Kopfdatenbereich. IP selbst hat keine Mechanismen zur Prüfung der Nutzlast auf Korrektheit, dies wird im TCP/IP-Referenzmodell durch die Transportschicht sichergestellt. Dieser Wert wird bei jeder Station neu verifiziert und – weil sich die TTL pro Hop verändert – neu berechnet. Dabei werden alle 16-Bit-Halbwörter des Kopfdatenbereichs nach den Regeln des Einerkomplements addiert (Übertrag auf das LSB addieren) und von der Summe das Einerkomplement gebildet. Das Ergebnis sollte 1111 1111 1111 1111 (Hex: 0xFFFF) sein, denn sonst ist ein Fehler im Header. Vorteil dabei ist, dass sich die Prüfsumme pro Hop nur um eins erhöht. Die Berechnung kann daher schnell in der Hardware ausgeführt werden. Bei einem zuverlässigeren Prüfverfahren wie CRC müsste dagegen die Prüfsumme bei jedem Hop neu berechnet werden. Trotzdem kostet das Prüfen der Prüfsumme verhältnismäßig viel Zeit. Moderne Router überprüfen die Prüfsumme aus Gründen der Verarbeitungsgeschwindigkeit nicht und inkrementieren sie nur. Diese Umstände haben dazu geführt, dass dieses Feld bei IPv6 nicht mehr existiert.

Source & Destination Address

- **Source Address**
- 32 Bit groß. Enthält die Quelladresse des IP-Pakets in *network byte order* (Byte Order, erstes Byte ist das *most significant Byte*).
- **Destination Address**
- Enthält die Zieladresse im gleichen Format wie die Quelladresse.

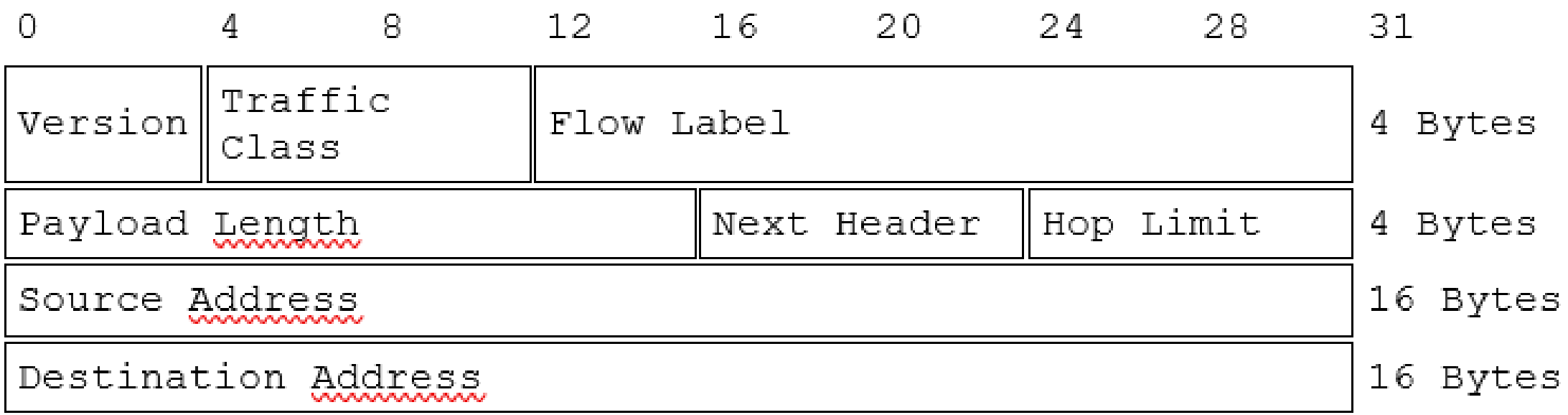
Options und Padding -1-

- Zusatzinformationen für das konkrete Paket. Die Optionen sind nur im Header optional, sie müssen aber von allen IP-Modulen unterstützt werden. Das Format der Optionen ist im RFC 791[1] beschrieben. Die maximale Anzahl der mit Optionen belegbaren Byte im konkreten Paket ergibt sich aus (IHL*4)-20. Da mit den 4 Bits in IHL ein Wertebereich von 0 bis 15 kodiert wird, können somit bis zu 40 Byte durch Optionen belegt werden. Die einzelnen Optionen selbst können unterschiedliche Länge haben, es gibt sowohl Optionen fester Länge als auch Optionen mit variabler Länge. Da die Gesamtlänge des IP-Headers durch das Feld IHL nur in Vielfachen von 4 Byte festgelegt wird, werden unbenutzte Byte mit Nullen aufgefüllt (Padding).

Options und Padding -2-

- Strict Routing
  - Option gibt den gesamten Pfad an, welchen das Paket durchlaufen muss
- Free Routing
  - Option gibt eine Liste von Routern an, die vom Paket nicht verfehlt werden dürfen
- Record Route
  - Lässt die gesamte Route aufzeichnen (Heute reicht die Größe des Option-Feldes meist nicht mehr dafür aus)
- Time Stamp
  - Zeitstempel
- Security
  - Bezeichnet, wie geheim das Paket ist

IPv6


0
4
8
12
16
20
24
28
31
Version
Traffic Class
Flow Label
4 Bytes
Payload Length
Next Header
Hop Limit
4 Bytes
Source Address
16 Bytes
Destination Address
16 Bytes