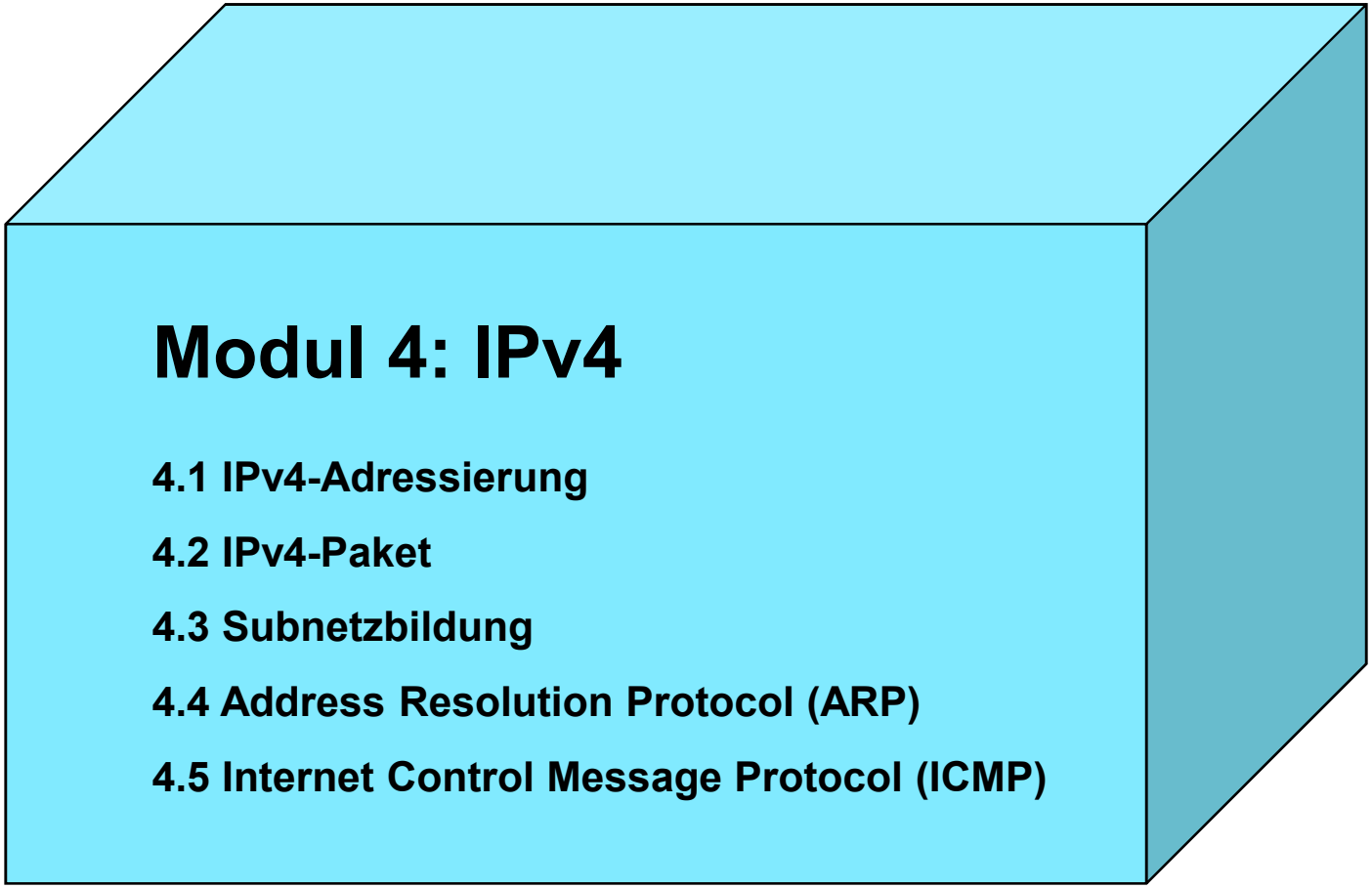


Modul 4: IPv4

4.1 IPv4-Adressierung

4.2 IPv4-Paket

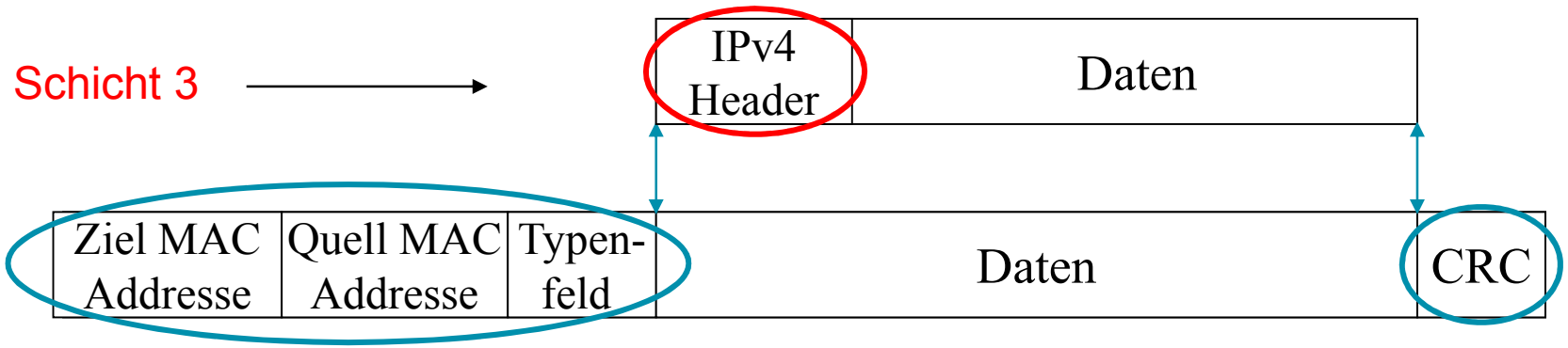
4.3 Subnetzbildung

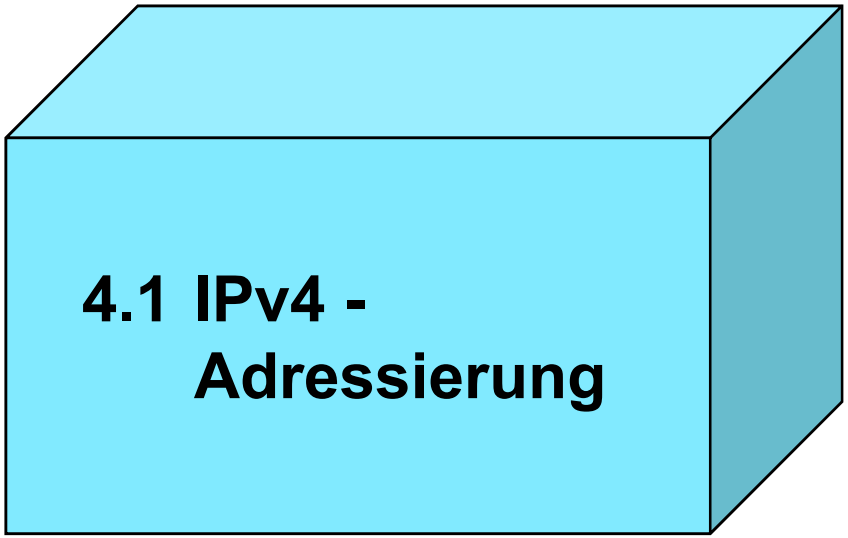
4.4 Address Resolution Protocol (ARP)

4.5 Internet Control Message Protocol (ICMP)

Allgemeines

- IP ist ein verbindungsloser Nachrichtentransportdienst
  (ohne Fehlerkorrektur, ohne Empfangsbestätigung, ohne Sicherung der Reihenfolge der übertragenen Datenpakete und ohne eine „spezielle Route“ festzulegen)
- Das IP Protokoll ist OSI Schicht 3 zuzuordnen, es definiert die IP Adressen und den Aufbau von IP Datenpaketen (Datagrammen)




4.1 IPv4 -
Adressierung

Darstellung von IPv4 Adressen

- **Adresslänge bei IPv4: 4 Byte bzw. 32 Bit**
- **Darstellung der 32 Bit IP-Adresse durch 4 durch Punkte getrennte Dezimalzahlen (eine für jedes Byte)**

  z.B. 01100101 . 00011110 . 00000110 . 00010100

  = 101.30.6.20

Aufbau der IPv4-Internetadressen

- **Anzahl der Adressen bei IPv4**
  - Es gibt 2^{32} = 4.294.967.296 IPv4-Adressen;
    das ist zu wenig!
  - IPv6: 128 Bit = 2^{128} = $3{,}4*10^{38}$ IP-Adressen;
    das sollte ausreichen
- **Ursprüngliche Aufteilung der IP-Adresse in drei Teile:**
  - Klasse
  - Netzadresse und
  - Rechneradresse oder Hostadresse

  Beachte: Oft wird auch die Kombination aus
  Klasse + Netzadresse + Hostadresse 0
  als Netzwerkadresse oder Netzwerk-Id bezeichnet.

  mit den Netzklassen A, B, C, D oder E.
- **Frage:**
  Wie könnte eine IP-Adresse (=32-Bit) in verschiedene Netzklassen aufgeteilt werden?

Klassen von IPv4-Netzen

Adressen der Klasse A:

- **1.Bit: "0" <Netzadresse (7 Bit)> <Rechneradresse (24 Bit)>**

Adressen der Klasse B:

- **1. und 2.Bit: "10" <Netzadresse (14 Bit)> <Rechneradresse (16 Bit)>**

Adressen der Klasse C

- **1. - 3. Bit: "110" <Netzadresse (21 Bit)> < Rechneradresse (8 Bit)>**

Adressen der Klasse D:

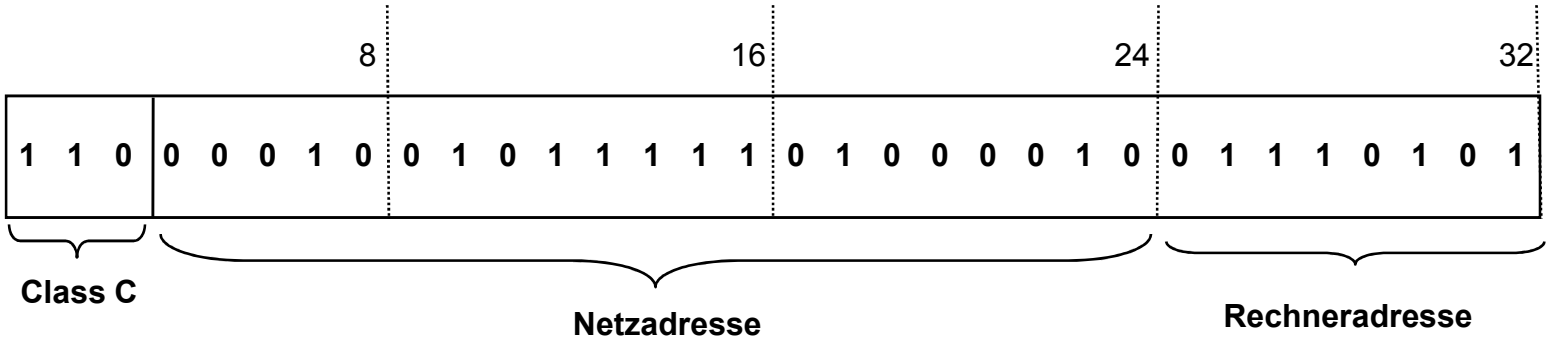
- **1. - 4. Bit: "1110" <Multicastadresse (28 Bit)>, nur lokal gültig**

Adressen der Klasse E:

- **1. - 4. Bit: "1111" + (28 Bit)**
  reservierter Adressbereich (28 Bit)

=> Diese Einteilung erlaubt im Grunde nur 3 verschiedene Netzgrößen und ist sehr unflexibel

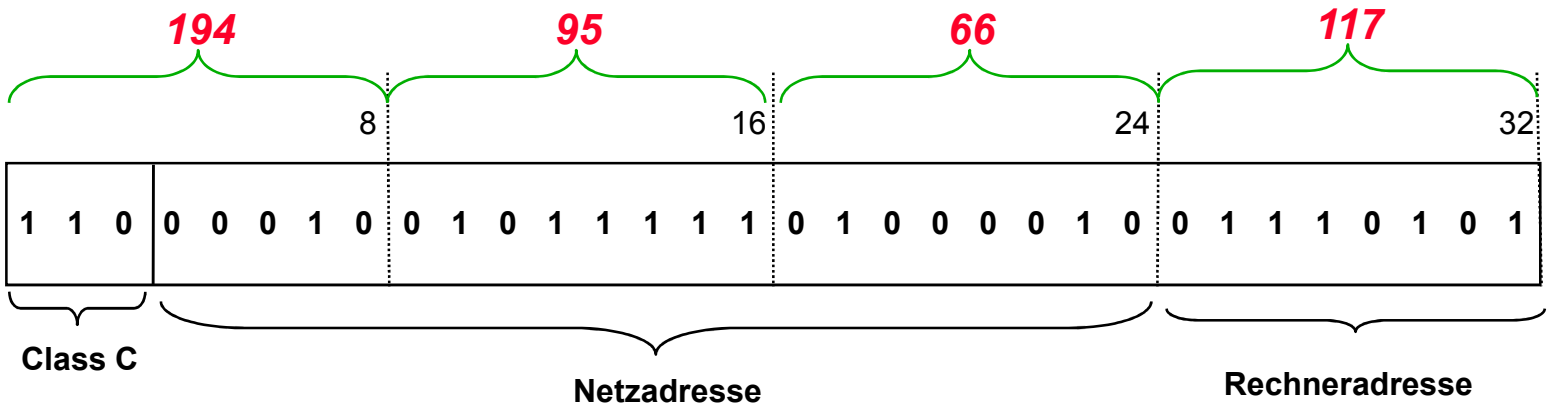
Beispiel einer IP-Adresse der Klasse C



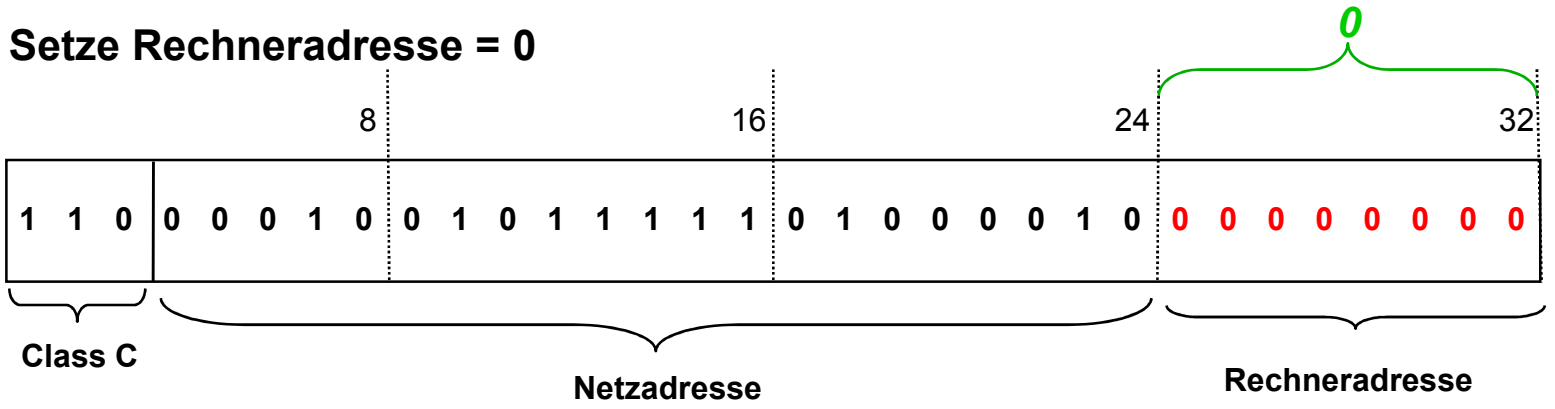
Schreibweisen:

- in Bit-Schreibweise:
  1100 0010 / 0101 1111 / 0100 0010 / 0111 0101 (unüblich!)
- in HexSchreibweise:
  C2 5F 42 75 (unüblich!)
- **übliche Schreibweise: 194.95.66.117**
- **Die „Netzmaske“ gibt den Bereich der Netzadresse plus Klassenangabe an, dieser Bereich wird durch „111 ...“ markiert
  (für das obige Beispiel ergibt sich dann: 255.255.255.0)**

Frage: zu welchem Netz gehört die folgende IP-Adresse ?



Setze Rechneradresse = 0



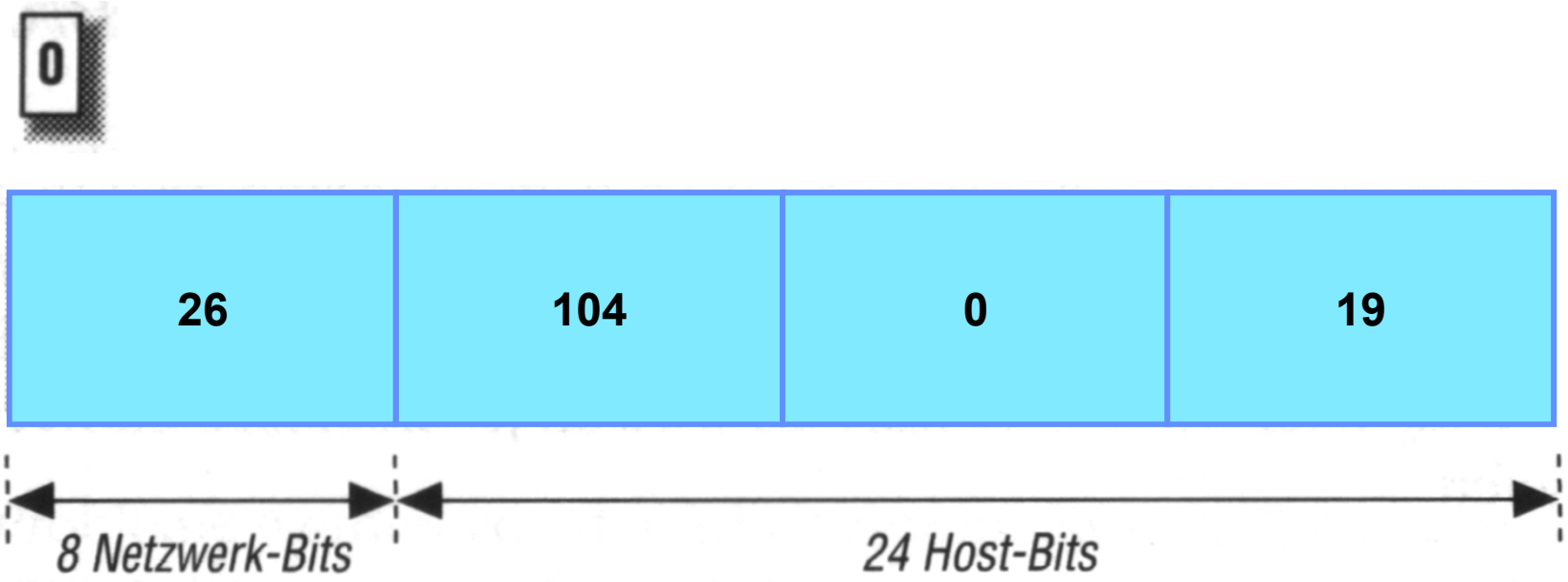
Lösung: diese genannte IP-Adresse gehört zum Netz 194.95.66.0

Ursprüngliche Einteilung der IP-Adressen in Klasse (1)

- Beispiel: **Klasse A**

Netzmaske: 255.0.0.0

Netzadresse: 26.0.0.0



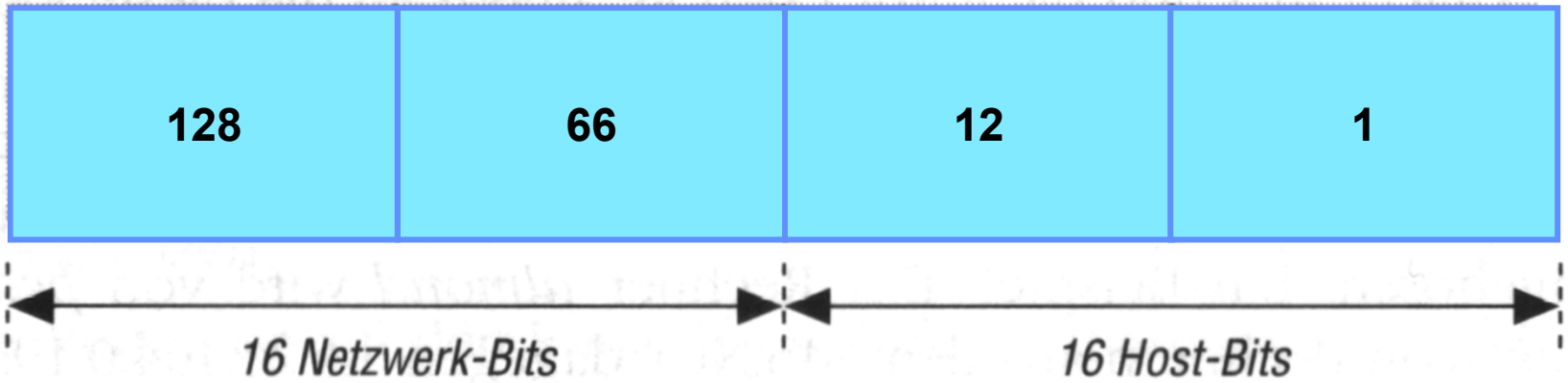
0 0011010 . 01101000 . 00000000 . 00010011

Ursprüngliche Einteilung der IP-Adressen in Klasse (2)

- Beispiel: **Klasse B**

Netzmaske: 255.255.0.0

Netzadresse: 128.66.0.0



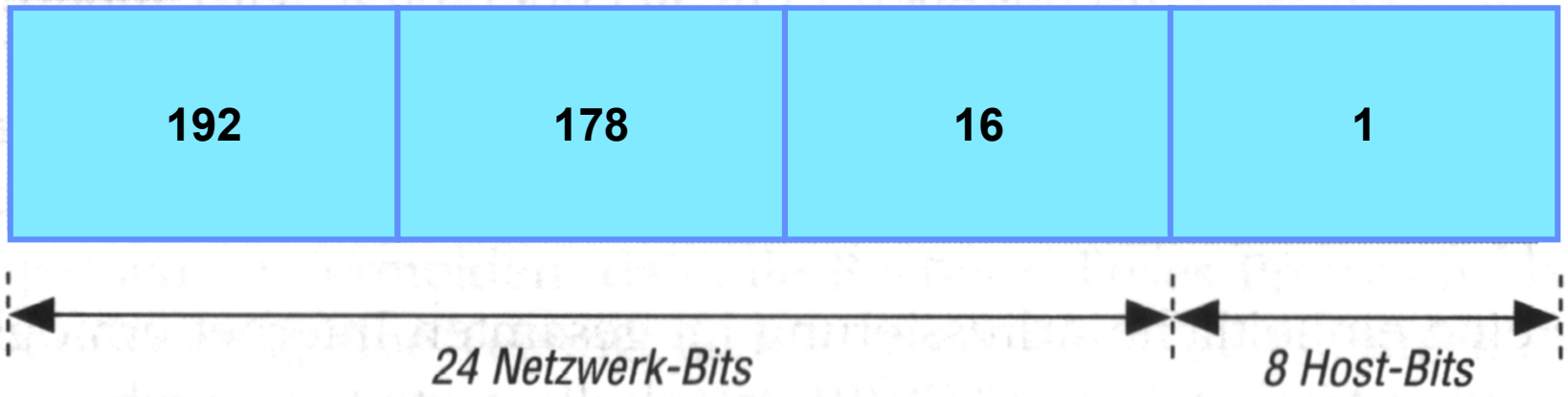
10000000 . 01000010 . 00001100 . 00000001

Ursprüngliche Einteilung der IP-Adressen in Klasse (3)

- Beispiel: **Klasse C**

Netzmaske: 255.255.255.0

Netzadresse: 192.178.16.0



11000000 . 10110010 . 00010000 . 00000001

Spezielle IPv4-Adressen

- **Netzwerkadresse: Hostteil =0**
  (Bezeichnung eines bestimmten Netzes)

  Beispiel: 194.95.66.0 *"Das Netz 194.95.66.0"*
- **gerichtete Broadcast-Adresse: Hostteil = „1“ Bits**

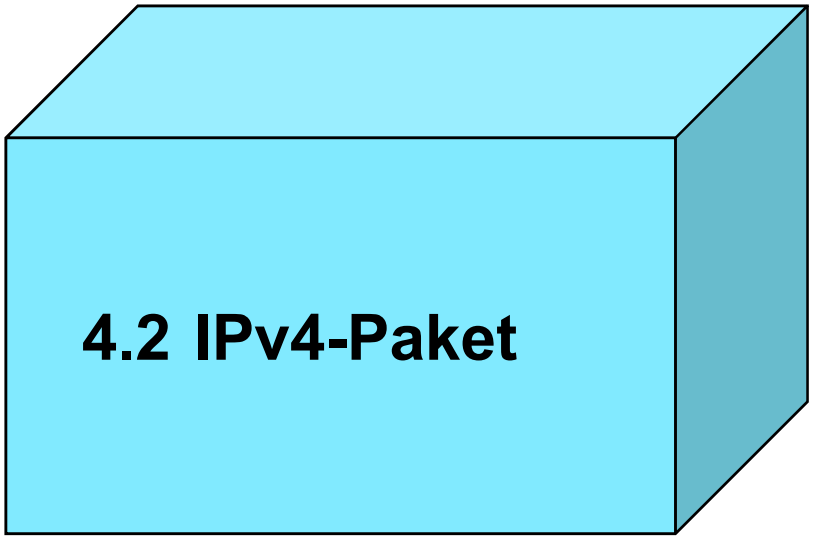
  Beispiel: 194.95.66.255 *"Broadcast an alle Rechner im Netz 194.95.66.0"*
- **begrenzte Broadcast-Adresse: nur „1“ Bits**

  Beispiel: 255.255.255.255 *"Broadcast an alle Rechner im lokalen Netz"*
- **Loopback-Adresse: Netz-Präfix = 127**
  (üblicherweise mit Hostteil 1, für Testzwecke)

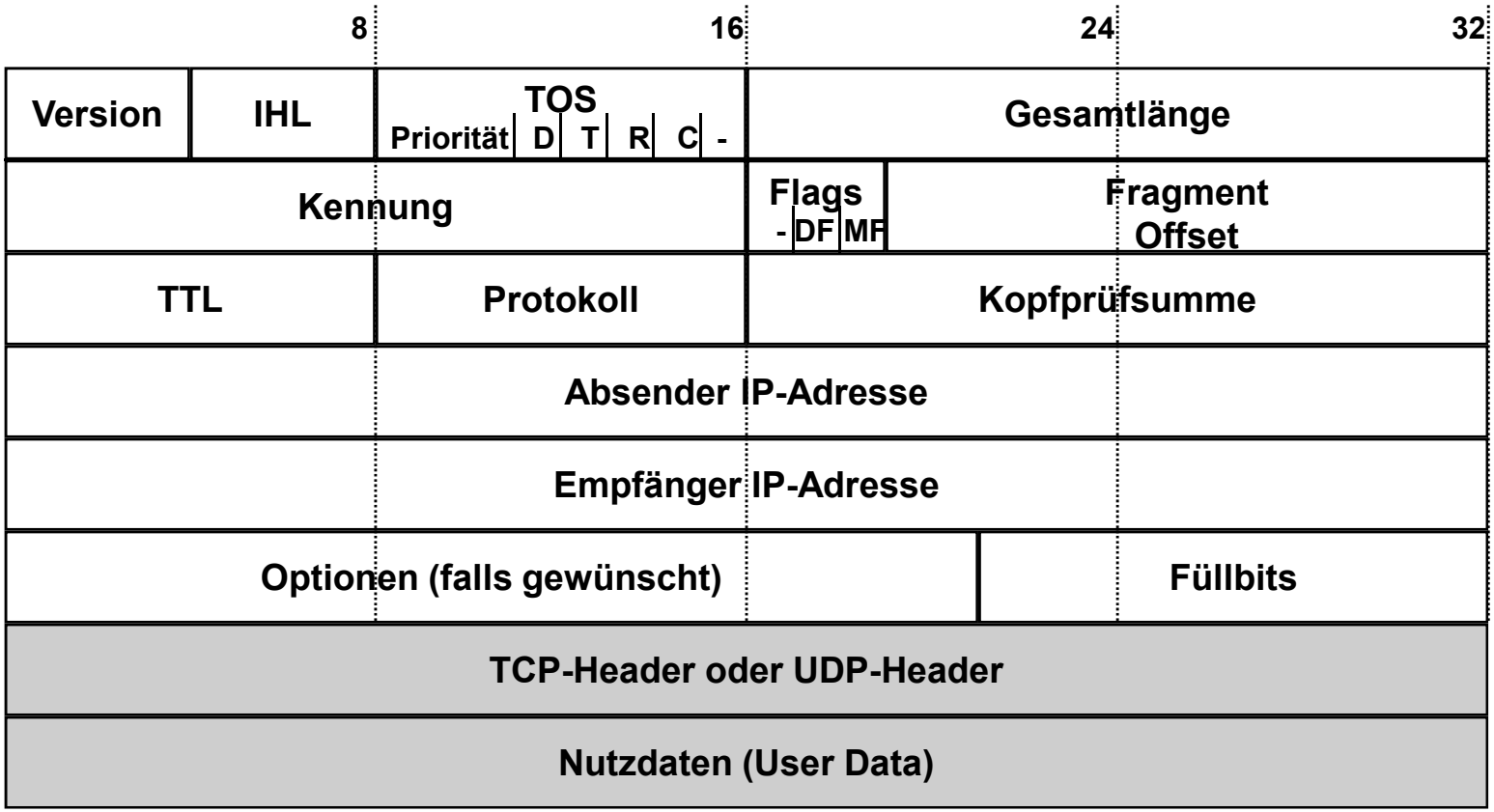
  Beispiel: 127.0.0.1 *"an den eigenen Rechner"*
- **Konvention: Router erhalten als Hostteil die Adresse 1**
- **Private IP-Netze**
  - **10.0.0.0 - 10.255.255.255** **priv. Netz der Klasse A**
  - **172.16.0.0 - 172.31.255.255** **priv. Netz der Klasse B (16 mögl.)**
  - **192.168.0.0 - 192.168.255.255** **priv. Netz der Klasse C (256 mögl.)**

CIDR Classless Inter-Domain Routing

- **Die Adressen wurden immer knapper und der verbleibende Adressraum sollte besser genutzt werden (siehe RFC 1518 und 1519)**
  - **Der Adressraum sollte flexibler aufgeteilt werden; es sollten mehr als 3 Netzgrößen möglich sein.**
  - **Nach wie vor besteht jede Adresse aus Netzadresse und Rechneradresse, wobei die Netzgröße d.h. Länge des Netzadressbereichs an die jeweiligen Randbedingungen angepasst wird.**
  - **Angegeben werden immer die IP-Adresse und die Netzmaske (mit Anzahl der Netzadressenbits).**
  - **Beispiel: 12.10.1.64 /26**
  - **Eigentlich bezeichnet diese Adresse die Adresse eines Klasse A Netzes, aber mit CIDR enthält die Adresse selbst keinen Anhaltspunkt mehr auf die Größe des Netzadressbereichs! Daher ist zusätzlich die Angabe der Netzmaske notwendig. In diesem Beispiel hat die Netzadresse eine Länge von 26 Bit. Für die Adressierung der Rechner bleiben nur 6 Bit!**


4.2 IPv4-Paket

Aufbau IP-Header



Aufbau des IP-Headers

- **Version:** **zur Zeit 4, Version 6 wird eingeführt/ existiert parallel** (4 Bit)
- **IHL:** **Internet-Header-Length, Länge in Einheiten zu 32 Bit-Oktetts (also 4 Bytes), normalerweise ist die IHL=5 (keine Optionen)** (4 Bit)
- **ToS: Type of Service** (8 Bit)
  - **die ersten drei Bits geben den Prioritäten-Level an (0-7)**
  - **-D: Anforderung low delay**
  - **-T: Anforderung high throughput**
  - **-R: Anforderung high reliability**
  - **-C: Anforderung low cost**

  Dieses Feld wird praktisch nicht mehr in dieser Weise benutzt, sondern dient der Definition von Quality-of-Service-Klassen bei Differentiated-Services
- **Gesamtlänge:** **maximal 2^{16} - 1 = 65535 Bytes** (16 Bit)

Aufbau des IP-Headers (Fortsetzung)

- **Kennung:** **Integerwert zur Identifizierung (Nummerierung) der einzelnen Fragmente eines Datagramms** (16 Bit)
- **Flags:** **Steuerung der Fragmentierung** (3 Bit)

  DF=1 “do-not-fragment”

  MF=1 “more-fragments-exist”
- **Fragment-Offset:** **Position des Fragments im ursprünglichen Datagramm (modulo 8)** (13 Bit)
- **TTL:** **wird vom Router dekrementiert; ist die vorgegebene Zeit abgelaufen, dann wird das Paket weggeworfen** (8 Bit).

  Anmerkung:
  Historisch in Sekunden, daher TTL = Time-To-Live,
  heute *keine* Zeitangabe, sondern Hop-Zähler,
  d.h. Anzahl der Router auf dem Weg.
  (Standardstartwert= z.B. 64)

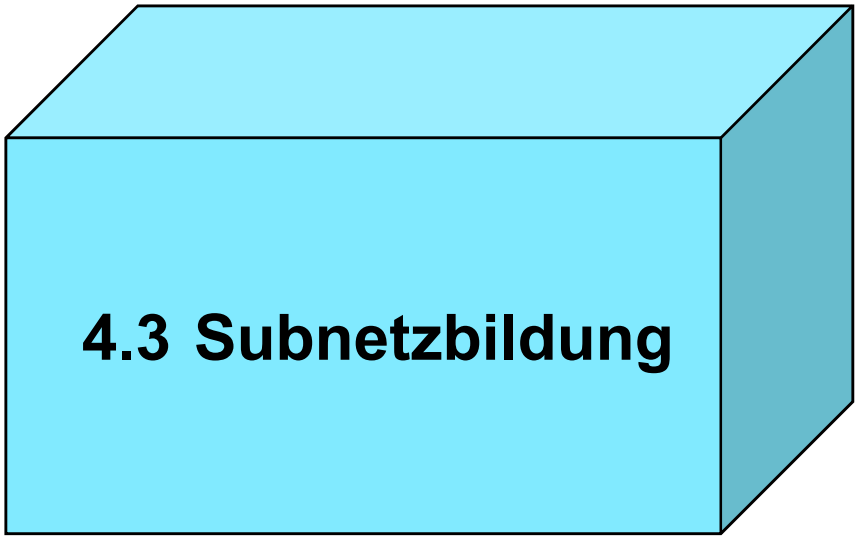
Aufbau des IP-Headers (Fortsetzung)

- **Protokoll:** **Wert zur Identifizierung des darüberliegenden Transportprotokolls** (8 Bit)

  z.B. 6 = TCP
  17 = UDP

- **Kopfprüfsumme:** **Einfachstverfahren, nur für Kopffelder, um für den Router unnötig lange Bearbeitungszeiten zu vermeiden** (16 Bit).

- **Optionen:** **Zur Unterstützung von Debugging-, Mess- und Sicherheitsfunktionen.**
  z.B. Option 7: Router werden aufgefordert, ihre IP-Adresse im Optionsfeld zu hinterlegen.


4.3 Subnetzbildung

Aufgabenstellung:

- **Eine Firma, die eine IPv4 Adresse hat, kann entsprechend der Netzklasse eine bestimmte Anzahl von Benutzern mit IPv4 Adressen versorgen**

  => Die IP Adressen aller Benutzer (und damit auch aller Abteilungen) liegen in einem Netz

  => Alle Broadcasts gehen an alle Benutzer!!! (= Broadcastdomäne)

- **Ein Router benötigt pro Interface eine eigene Netzadresse, sonst können die Daten nicht richtig zugestellt werden d.h. das Netz einer Firma (= die Broadcastdomäne) kann nicht mit Hilfe von Routern aufgeteilt werden, wenn es nur eine einzige Netzadresse gibt ...**

  Oder doch ?

  Ist es also sinnvoll, wenn eine Firma mehrere kleinere Adressbereiche also z.B. die Adressen mehrerer Klasse C-Netze erhält?

  Oder gibt es andere Möglichkeiten ???

Konkretes Beispiel:

Eine Firma mit 1000 Mitarbeitern hat eine „Klasse B“ Netzadresse.

Wie kann eine Broadcastdomäne mit 1000 Endgeräten vermieden werden?

Was kann diese Firma tun, um ihr internes Netz zu strukturieren?

Beispiel:

- Ein Klasse B Netz mit hat die IPv4 Adresse: 140.64.0.0
- Die ursprüngliche Netzmaske dafür lautet: 255.255.0.0
- 4 Bits werden für die Subnetzadressierung verwendet d.h. es können bis zu 16 Subnetze gebildet werden
- Die Subnetzmaske lautet dann 255.255.240.0 = /20

  (= 11111111 . 11111111. 1111 0000.00000000)
- IP-Adresse: 140.64.32.4

  (= 11000010. 01000000. 0010 0000. 0000100)
- Lokale Interpretation:

  Rechner Nr. 4 im Subnetz 140.64.32.0

Lösung: IP Subnetz-Bildung (1)

- **Grundsätzliche Funktionsweise: Lokale Erweiterung der Netzadresse**

  Bits, die zur Kodierung der Rechneradresse vorgesehen sind, werden lokal zur Adressierung von Teilnetzen verwendet

  => innerhalb eines großen Netzes können mehrere kleine Netze adressiert werden

  Andererseits: Die Anzahl der anschließbaren Rechner wird reduziert

- **Die Teilnetze werden „Subnetze“ genannt und haben verschiedene Sub-Netzadressen**

- **Die Interfaces der Router erhalten dadurch unterschiedliche Sub-Netzadressen und die Daten können eindeutig weitergeleitet werden**

- **Die organisatorischen Einheiten innerhalb einer Firma (z.B. entsprechend den verschiedenen Abteilungen) können auf die Subnetze abgebildet werden (d.h. jede Abteilung kann ein Subnetz mit eigener Subnetzadresse erhalten)**

Lösung: IP Subnetz-Bildung (2)

- Definition eines Subnetzes durch eine „Subnetz-Maske“, wobei die Subnetzmaske die Bits der Netzadresse inklusive der Erweiterung anzeigt
- Die Subnetzmaske entspricht in Ihrer Funktionsweise der ursprünglichen Netzmaske
- **Hinweis:** Rechner, die direkt oder über Schicht 1 oder über Schicht 2 Komponenten verbunden werden, müssen im selben Subnetz liegen!

Weiteres Anwendungsbeispiel (1)

- **Firma XYZ hat eine Klasse C Adresse mit der Netzadresse:** **196.32.8.0**

  (11000100.00100000.00001000.00000000)

- **Die ursprüngliche Netzmaske lautet:** **255.255.255.0**

  (11111111.11111111.11111111.00000000)

- **Dazu gehört die Broadcast-Adresse:** **196.32.8.255**

  (11000100.00100000.00001000.11111111)

- **Der 1. Rechner hat die Adresse:** **196.32.8.1**

  und der letzte Rechner hat die Adresse: **196.32.8.254**

Anwendungsbeispiel (2)

- In der Firma XYZ gibt es 5 Abteilungen:

  (z.B. Entwicklung, Marketing, Produktion,Vertrieb und Verwaltung ...)

  Die IP-Adressen jeder Abteilung sollen ein gemeinsames Merkmal haben d.h. irgendwie gekennzeichnet sein.
- Lösung: Jede Abteilung erhält eine eigene Subnetzadresse. Für die Adressierung von 5 Netzen werden 3 Bit benötigt
- Welche Subnetzmaske ergibt sich bei dieser Subnetzbildung?

Anwendungsbeispiel (3)

- **Die Subnetzmaske lautet: 255.255.255.224**

  11111111 . 11111111 . 11111111. 111 00000

⇨ **3 Bit des Rechneradresseraums werden für eine Erweiterung der Netzadresse verwendet**

- **Wie lauten die Subnetzadressen der Abteilungen?**
- **Die Abteilungen erhalten die folgenden Adressen:**

11000100.00100000.00001000.	001 00000	=	196.32.8.32
11000100.00100000.00001000.	010 00000	=	196.32.8.64
11000100.00100000.00001000.	011 00000	=	196.32.8.96
11000100.00100000.00001000.	100 00000	=	196.32.8.128
11000100.00100000.00001000.	101 00000	=	196.32.8.160

Anwendungsbeispiel (4)

- Alle Subnetze haben die gleiche Subnetzmaske
- Jedes Subnetz hat eine eigene Subnetzadresse

  UND eine eigene Broadcastadresse
- Pro Abteilung bleiben 5 Bits für die Adressierung der Rechner => $2^5 = 32$ Zustände

  Aber: der Zustand 00000 ist bereits für die Netzadresse verwendet und der Zustand 11111 für die Broadcast- Adresse

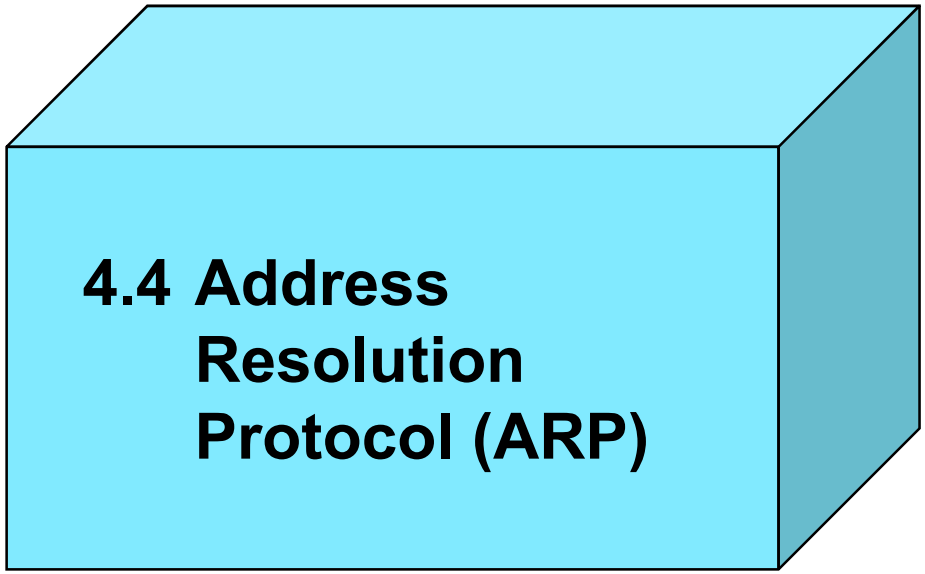
  => es können $2^5 - 2 = 30$ Rechner pro Abteilung adressiert werden.

Welche beiden Randbedingungen sind grundsätzlich bei einer Subnetzbildung zu beachten?

Die Anzahl der benötigen Subnetze UND die Anzahl der Rechner im größten Subnetz!

Anwendungsbeispiel (5)

• IP-Adresse der 1. Abteilung:	11000100.00100000.00001000.	001 00000	= 196.32.8.32
mit der Broadcast-Adresse:	11000100.00100000.00001000.	001 11111	= 196.32.8.63
• IP-Adresse der 2. Abteilung:	11000100.00100000.00001000.	010 00000	= 196.32.8.64
mit der Broadcast-Adresse:	11000100.00100000.00001000.	010 11111	= 196.32.8.95
• IP-Adresse der 3. Abteilung:	11000100.00100000.00001000.	011 00000	= 196.32.8.96
mit der Broadcast-Adresse:	11000100.00100000.00001000.	011 11111	= 196.32.8.127
• IP-Adresse der 4. Abteilung:	11000100.00100000.00001000.	100 00000	= 196.32.8.128
mit der Broadcast-Adresse:	11000100.00100000.00001000.	100 11111	= 196.32.8.159
• IP-Adresse der 5. Abteilung:	11000100.00100000.00001000.	101 00000	= 196.32.8.160
mit der Broadcast-Adresse:	11000100.00100000.00001000.	101 11111	= 196.32.8.191


4.4 Address
Resolution
Protocol (ARP)

Adressauflösung (1)

Kleine Wiederholung:

Welche verschiedenen Adressentypen kennen Sie?

Wo bzw. von welchen Komponenten werden diese Adressen benutzt?

Adressauflösung (2)

- Grundsätzlich 3 verschiedene Arten von Adressen:
  - MAC-Adressen/ Hardware-Adressen (48-Bit-Adressen benutzt von der MAC-Schicht d.h. von Switches)
  - IP-Adressen/ Netzadressen (32-Bit-Adressen benutzt von der IP-Schicht d.h. von Routern)
  - Namen (benutzt von der Anwendungsschicht z.B. h-bonn-rhein-sieg.de)

Adressauflösung (3)

- Um ein Datenpaket zu versenden, müssen die Ziel IP-Adresse und auch die Ziel MAC-Adresse des Empfängers bekannt sein
- Auflösung der Adressen der Anwendungsschicht in IP-Adressen mit Domain Name Service (DNS)
- Auflösung der IP-Adressen in MAC-Adressen mit dem Address Resolution Protocol (ARP)
- Die Ziel IP Adresse entspricht dem (entfernten) Empfänger
- Die Ziel MAC Adresse hat immer nur Gültigkeit im lokalen Netz

Adressauflösung (4)

- Wie werden diese Adressen aufeinander abgebildet?

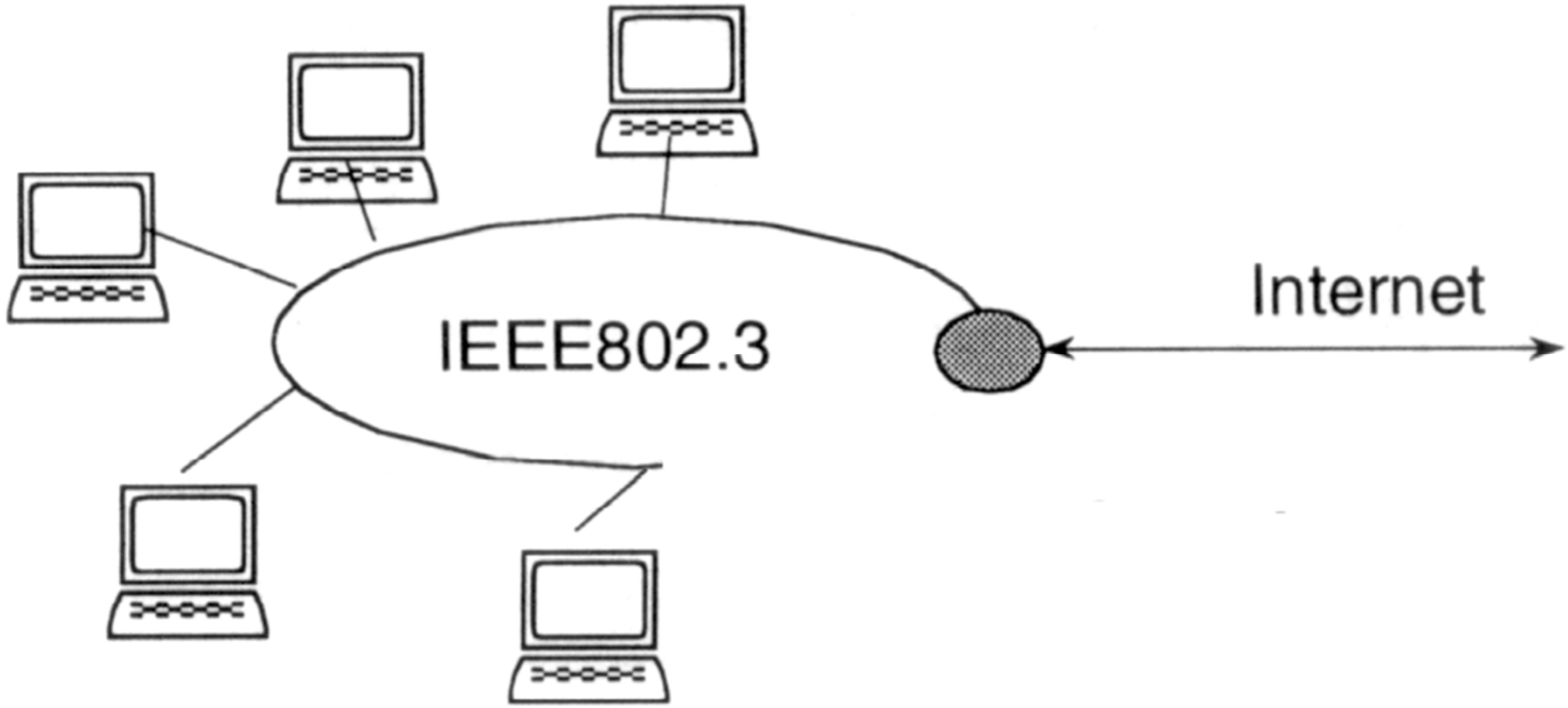
- MAC-Adressen/ Hardware-Adressen
  (48-Bit-Adressen
  benutzt von der MAC-Schicht)

- IP-Adressen/ Netzadressen (32-Bit-Adressen
  benutzt von der IP-Schicht)
- Namen (benutzt von der Anwendungsschicht,
  z.B. h-bonn-rhein-sieg.de)

Ablauf von ARP

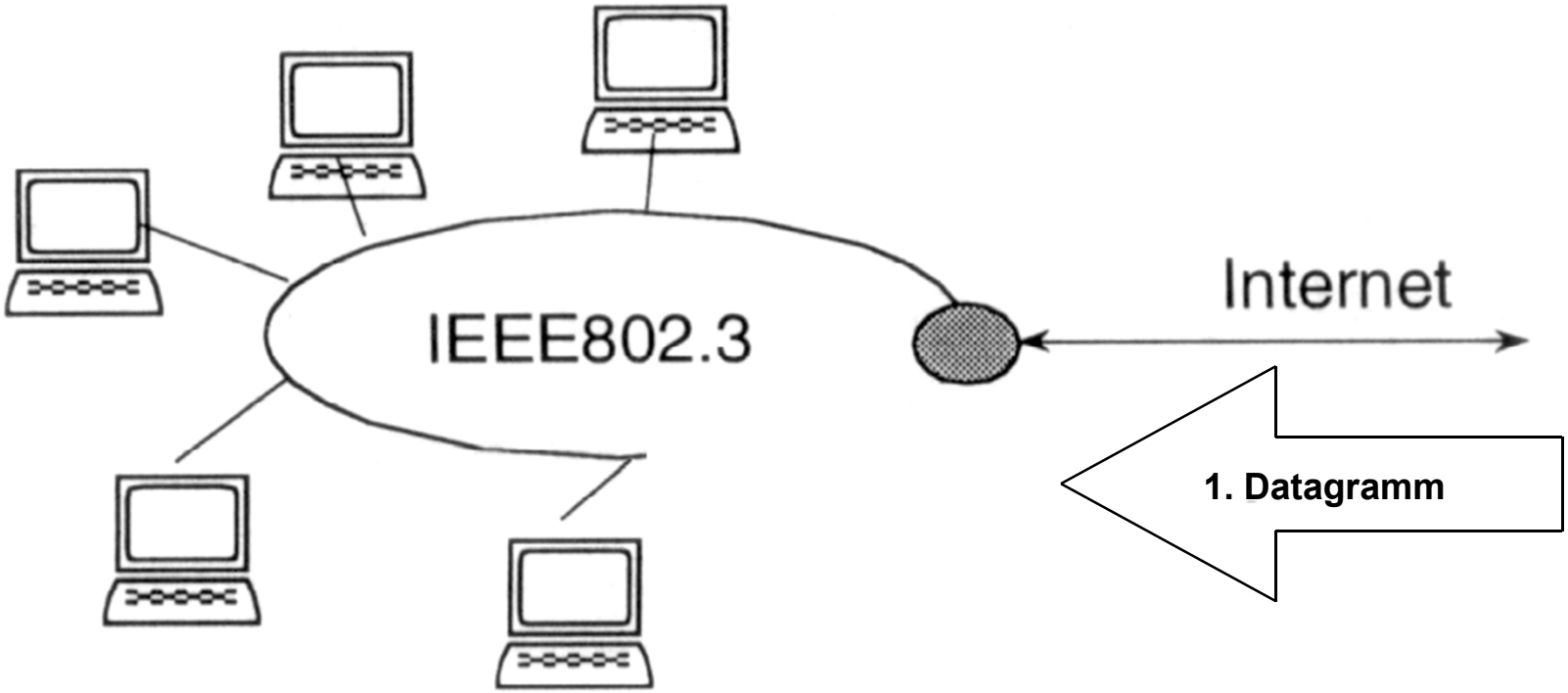
- Überprüfung, ob sich die aktuelle Ziel IP im lokalen Netz befindet. Wenn sich der Zielrechner nicht im lokalen Netz befindet, wird die IP-Adresse des „Standard Gateways“ für die folgenden Schritte verwendet
- Überprüfung, ob das benötigte IP-MAC-Adresspaar bereits im ARP Cache des sendewilligen Rechners gespeichert ist
- Falls nicht, wird ein ARP Request an alle Rechner im lokalen Netz gesendet d.h. mit Broadcast-Ethernet Adresse und Ziel IP Adresse
- Alle Rechner prüfen, ob sie Besitzer der Ziel IP Adresse sind. Nur der Besitzer der gesuchten IP Adresse antwortet mit ARP Reply und sendet seine MAC Adresse an den Absender des ARP Requests
- Absender des ARP Requests speichert das erhaltene IP-MAC-Adressen-paar in seinem ARP Cache und sendet das Datenpaket los

- **ARP - Address Resolution Protocol - übernimmt die Umwandlung der IP Adressen in MAC Adressen**



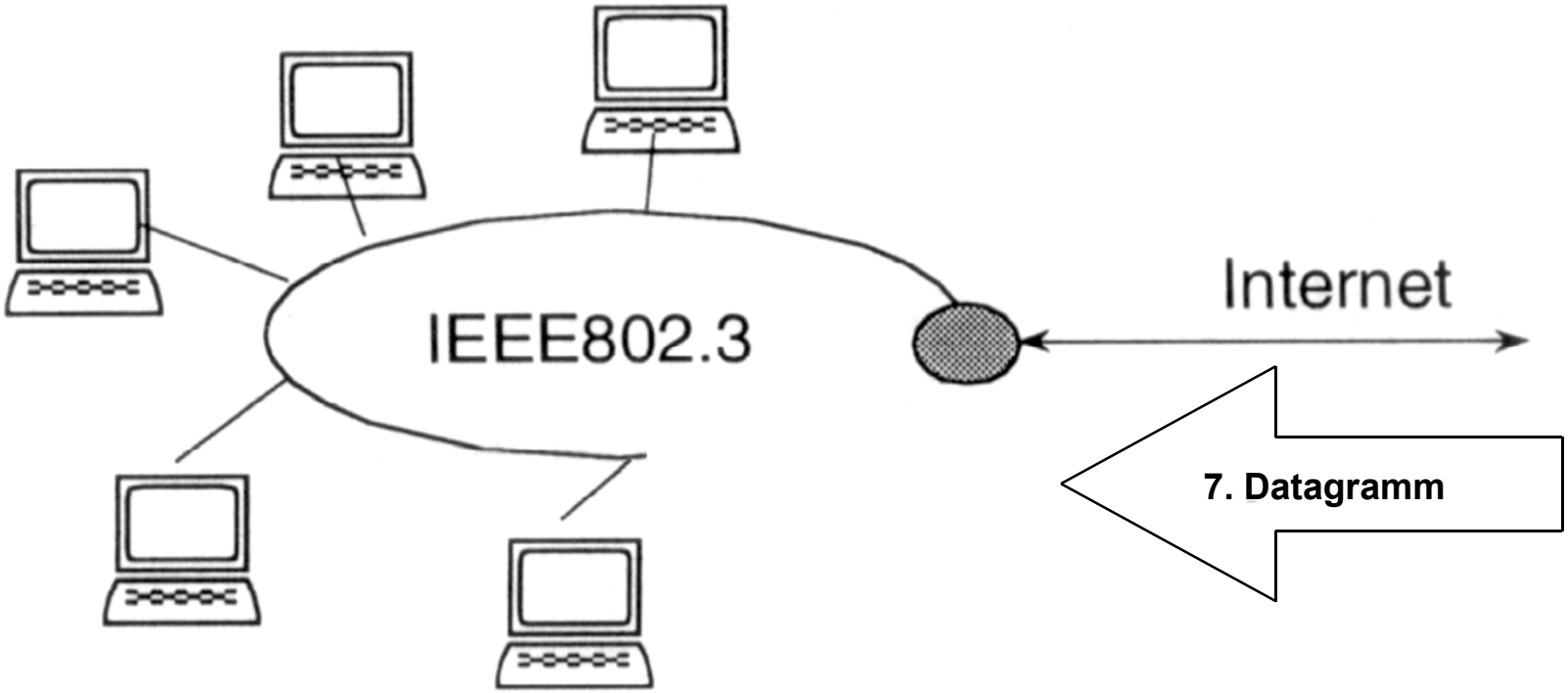
- Zuordnungstabellen in allen Rechnern (ARP Cache)
- Falls gesuchtes Adressenpaar (noch) nicht vorhanden => Verwendung von ARP

ARP - Address Resolution Protocol



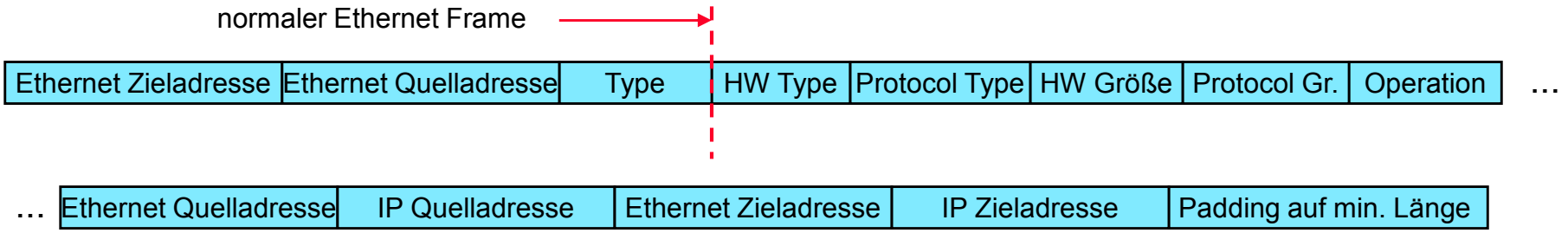
2. Broadcast der gewünschten IP-Adresse mit ARP Request
3. Vergleich in allen Rechnern
4. Antwort eines Rechners mit seiner MAC-Adresse mit ARP Reply
5. Datagramm als Ethernet-Frame an Rechner
6. IP-MAC Adressenpaar wird im ARP-Cache gespeichert

ARP - Address Resolution Protocol

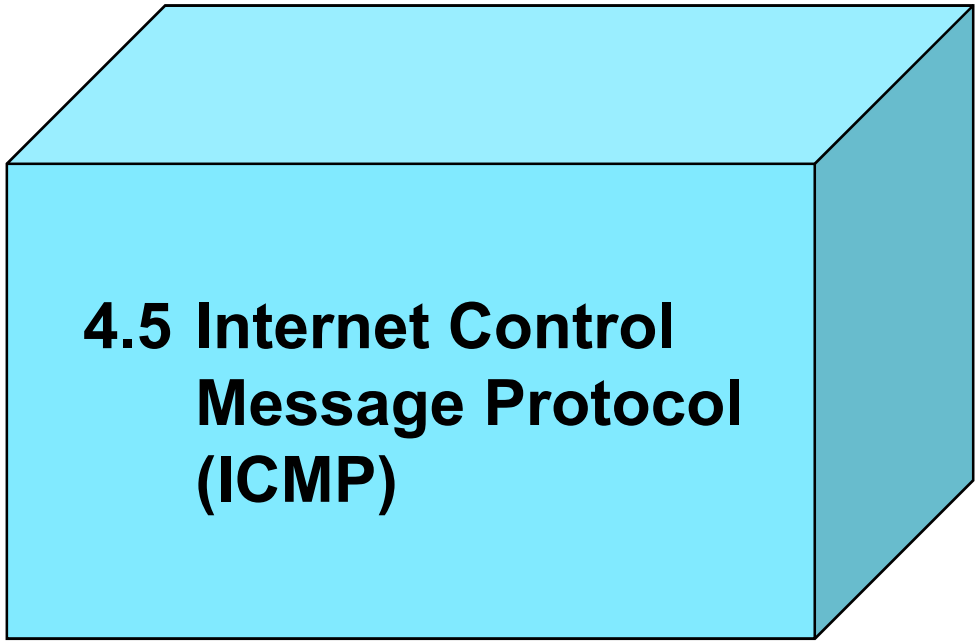


8. Bei den nächsten Daten: Ethernet-Adresse wird aus ARP Cache entnommen, danach Datagramm als Ethernet-Frame an Rechner

Format eines ARP Request- oder ARP Reply- Pakets



- Normaler Ethernet Frame mit Broadcast Zieladresse und Type Nummer 2054
- Danach:
  - HW Type (Ethernet = 1), Länge: 2 Byte
  - Protocol Type (IP = 0x0800), Länge: 2 Byte
  - HW address Größe (Länge der HW Adresse = 6), Länge: 1 Byte
  - Protocol address Größe (Länge der IP Adresse = 4), Länge: 1 Byte
  - Operation (ARP Request = 1 oder ARP Reply = 2), Länge: 2 Byte
  - Ethernet Adresse des Senders, Länge: 6 Byte
  - IP Adresse des Senders, Länge: 4 Byte
  - Ethernet Adresse des Empfängers, Länge: 6 Byte (ist bei ARP Request nicht gesetzt)
  - IP Adresse des Empfängers, Länge: 4 Byte


4.5 Internet Control
Message Protocol
(ICMP)

Internet Control Message Protocol (ICMP)

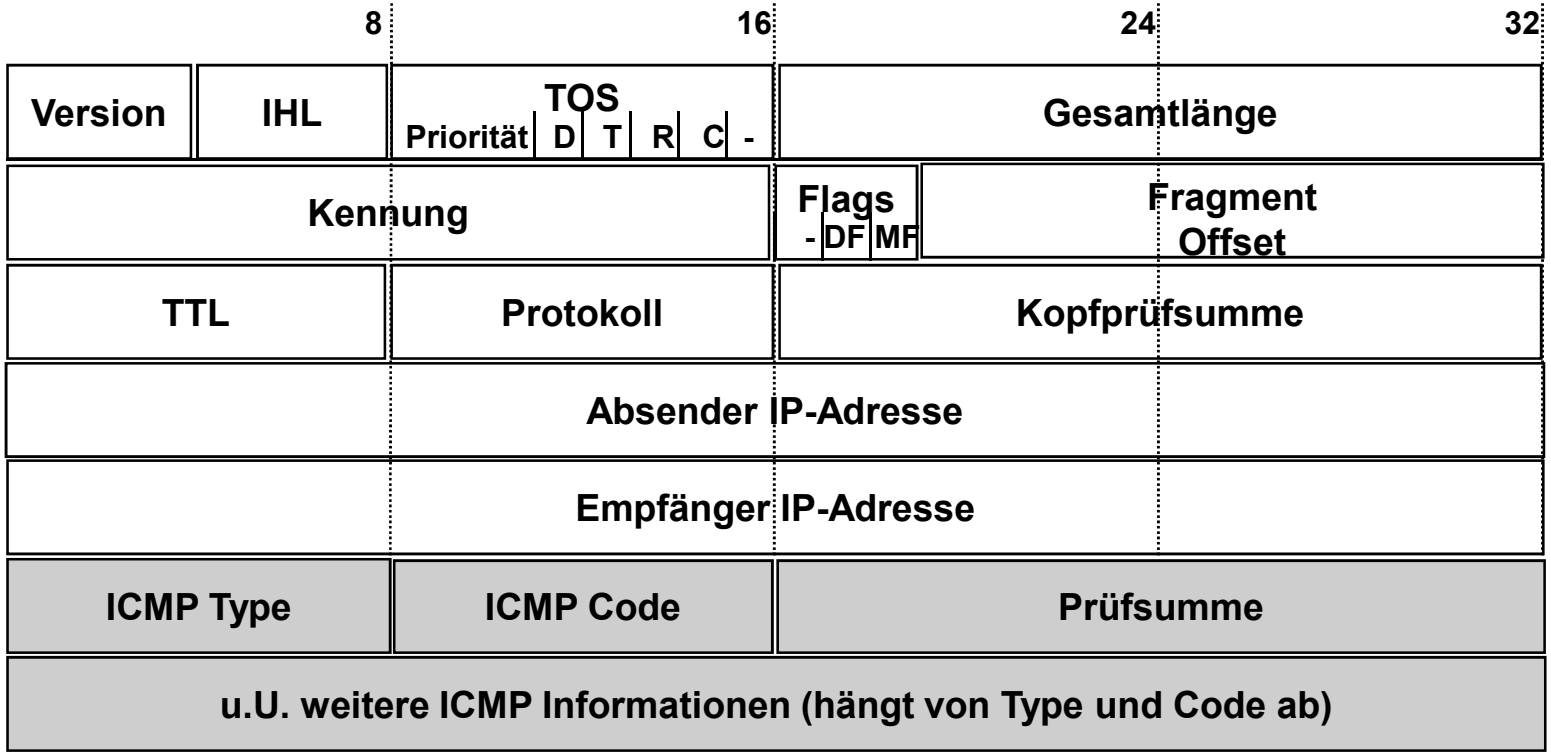
- Genaue Spezifikation in RFC 792
- ICMP dient zur Übermittlung von Fehler- und Statusmeldungen und wird zur IP Schicht gerechnet
- Die ICMP Protokoll Informationen folgen direkt dem IP Header und sind durch eine Prüfsumme geschützt
- Wichtige ICMP Nachrichtentypen:
  - Ziel nicht erreichbar (der Code gibt dann genauere Informationen z.B. Netzwerk nicht erreichbar, Host nicht erreichbar, Port nicht erreichbar ...)
  - Echo Request und Echo Reply (werden bei „Ping“ verwendet)
  - Zeitüberschreitung (bei TTL =0)
  - Parameter Probleme etc.

Allgemeines zu ICMP

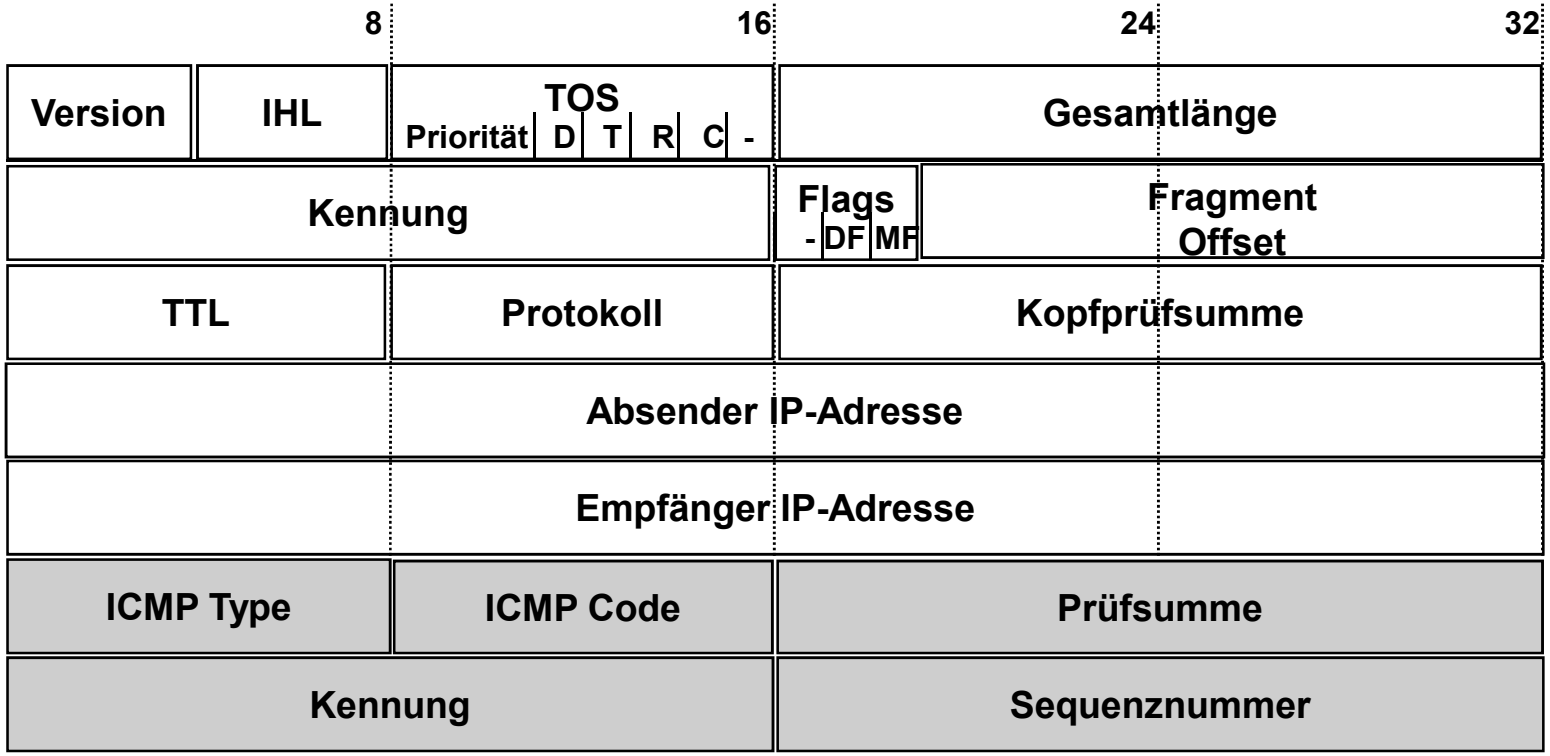
- ICMP Nachrichten zur Anzeige von Fehlern oder zur Übermittlung von Informationen
- ICMP Fehlernachrichten werden niemals erzeugt als Reaktion auf
  - eine ICMP Fehlermeldung (wohl aber auf eine ICMP Information)
  - eine IP Broadcast Nachricht
  - eine Schicht 2 Broadcast Nachricht
  - IP Fragmente
  - eine IP Nachricht, die mit einer IP Quelladresse aus „Nullen“, einer Loopback-, Broad- oder Multicast-Adresse

Warum gibt es diese Einschränkungen???

Aufbau einer ICMP Nachricht



Aufbau einer ICMP Nachricht für Echo Request (Type = 8) und Echo Reply (Type = 0)



PING

- Basiert auf den ICMP Typen Echo Request (8) und Echo Response (0) jeweils mit Code = 0
- Kann für grundlegende Verbindungstests verwendet werden
- Kennung und Sequenznummer können von Absender des Echo Request auf einen beliebigen Wert gesetzt werden. Diese Werte werden im Echo Reply zurückgesendet.
- Bei mehrfachen Ping wird die Sequenznummer hochgezählt.

Übersicht über verschiedene ICMP Typen

ICMP Type	Bedeutung
0	Echo Reply (verwendet von Ping)
3	Ziel unerreichbar
8	Echo Request (verwendet von Ping)
11	Zeitlimitüberschreitung
12	Parameterproblem
13	Zeitstempel Anforderung
14	Zeitstempel senden

ICMP Type	Code	Bedeutung
3	0	Netzwerk unerreichbar
	1	Rechner unerreichbar
	2	Protokoll unerreichbar
	3	Port unerreichbar
	4	Fragmentierung erforderlich
	6	Zielnetzwerk unbekannt