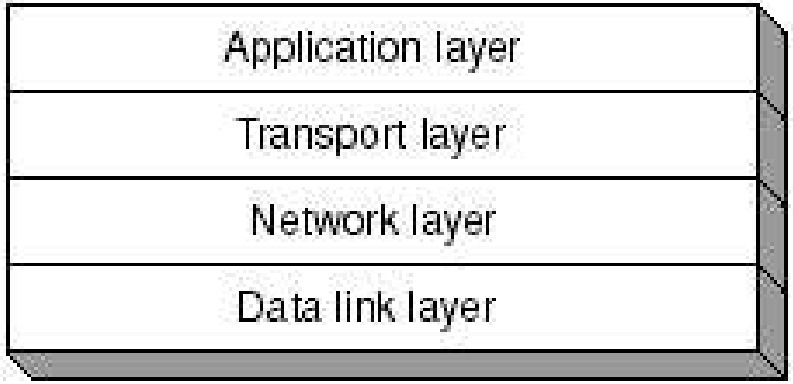
ARP, ICMP, ping

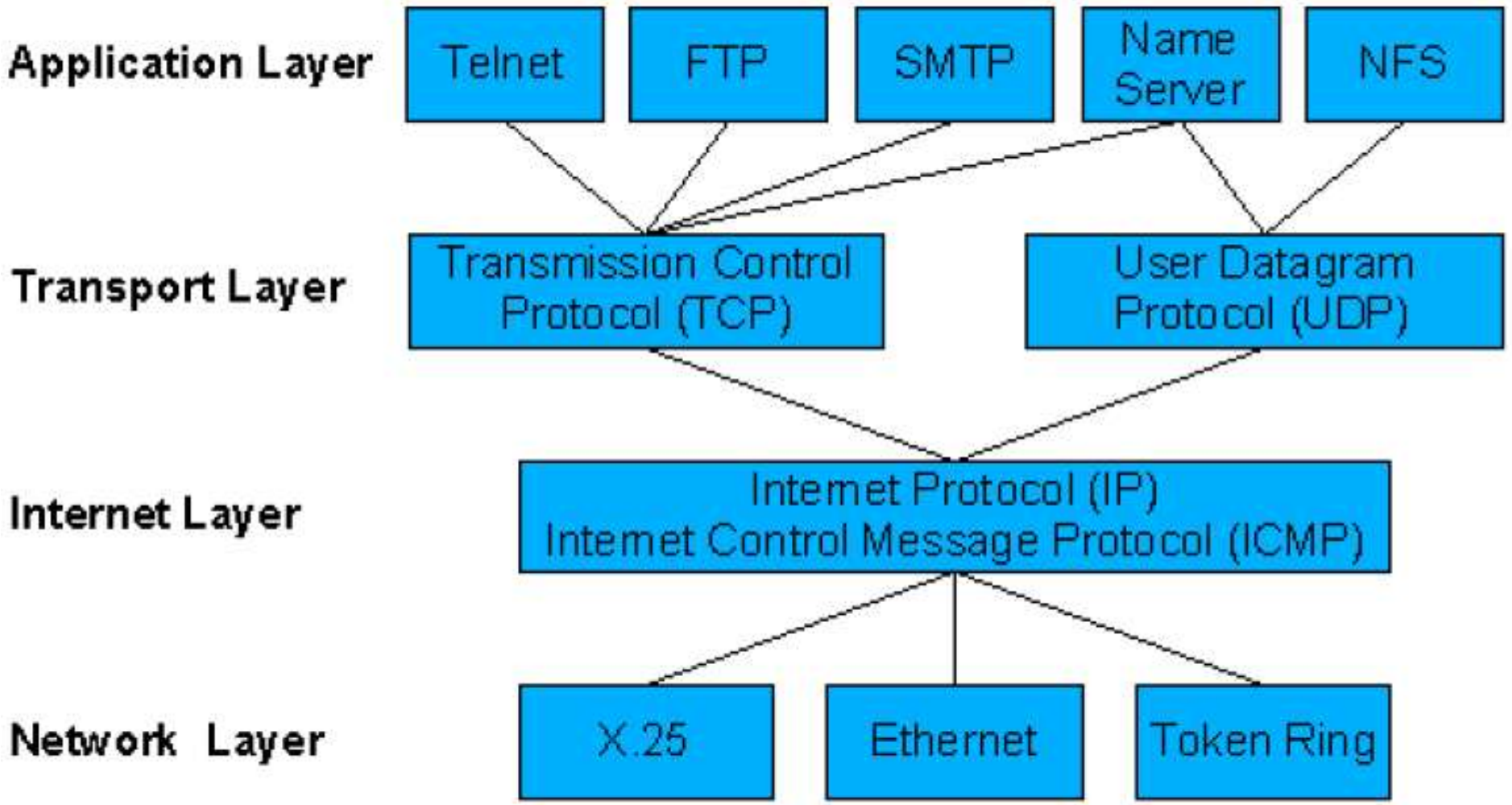
Jörn Stuphorn
stuphorn@rvs.uni-bielefeld.de

- Data Link Layer
  - Aufgabe: Zuverlässige Übertragung von Rahmen über Verbindung
  - Funktionen: Synchronisation, Fehlerkorrektur, Datenflusskontrolle

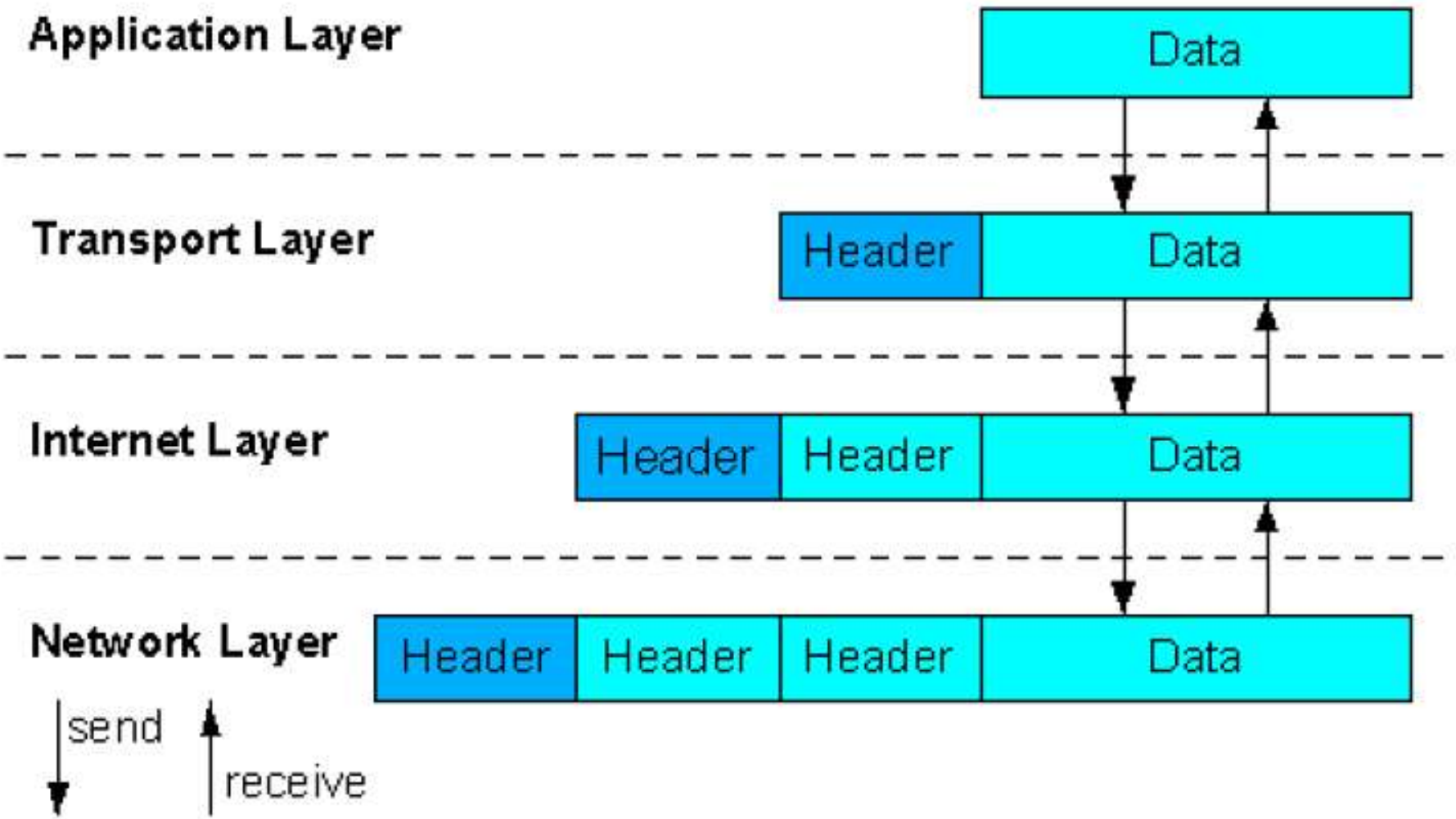


- Network Layer
  - Aufgabe: Paketübertragung innerhalb des Netzes
  - Funktionen: Routing, Addressierung, Switching, Kollisionsbehandlung
- Transport Layer
  - Aufgabe: Steuerung der Kommunikation zwischen zwei Rechnern
  - Funktionen: Verbindungsaufbau, Fehlerkorrektur, Flußkontrolle
- Application Layer
  - Aufgabe: Details von Anwendungsprogrammen
  - Funktionen: Alle Funktionen anwendungsspezifisch

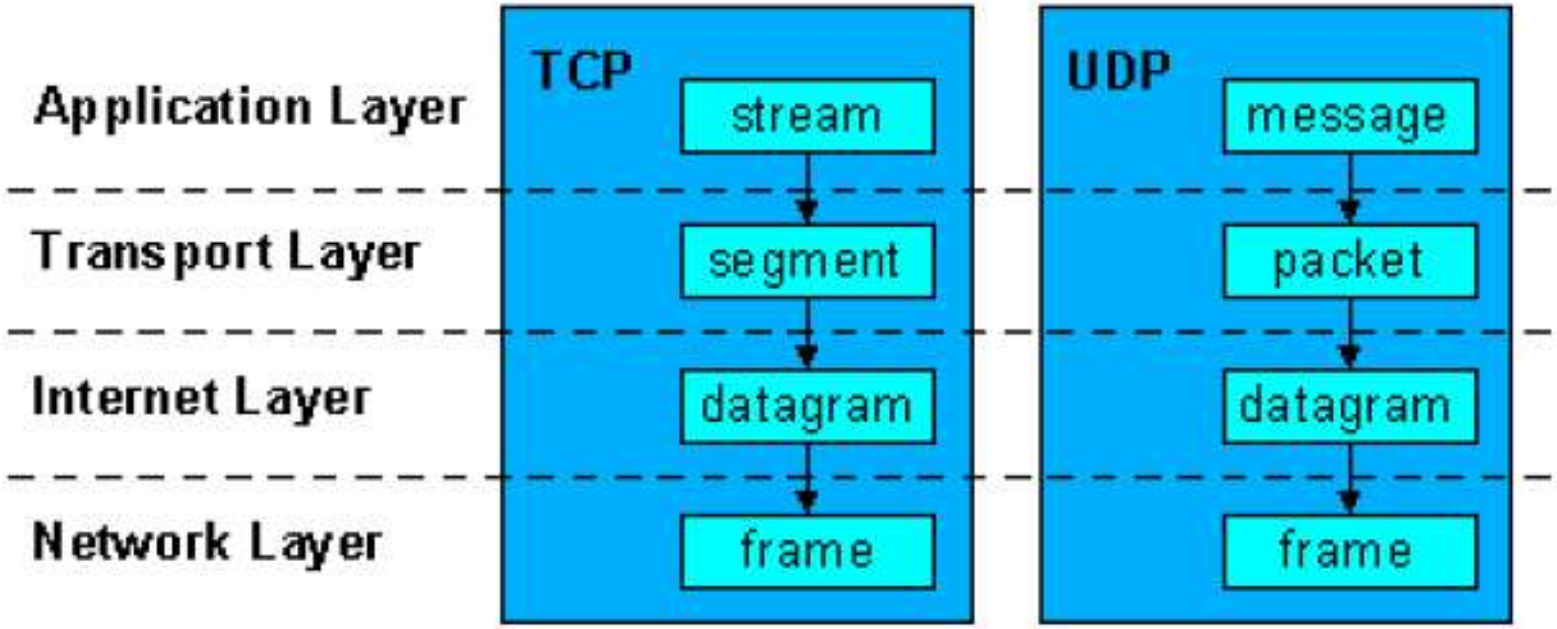
Protokolle nach Schichten



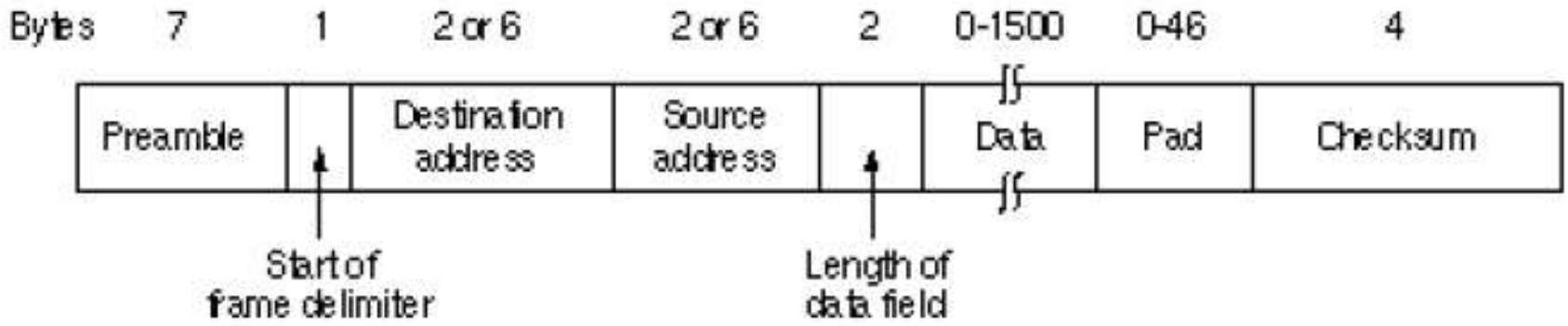
Kapselung


Application Layer
Data
Transport Layer
Header
Data
Internet Layer
Header
Header
Data
Network Layer
Header
Header
Header
Data
send
receive

Bezeichnungen



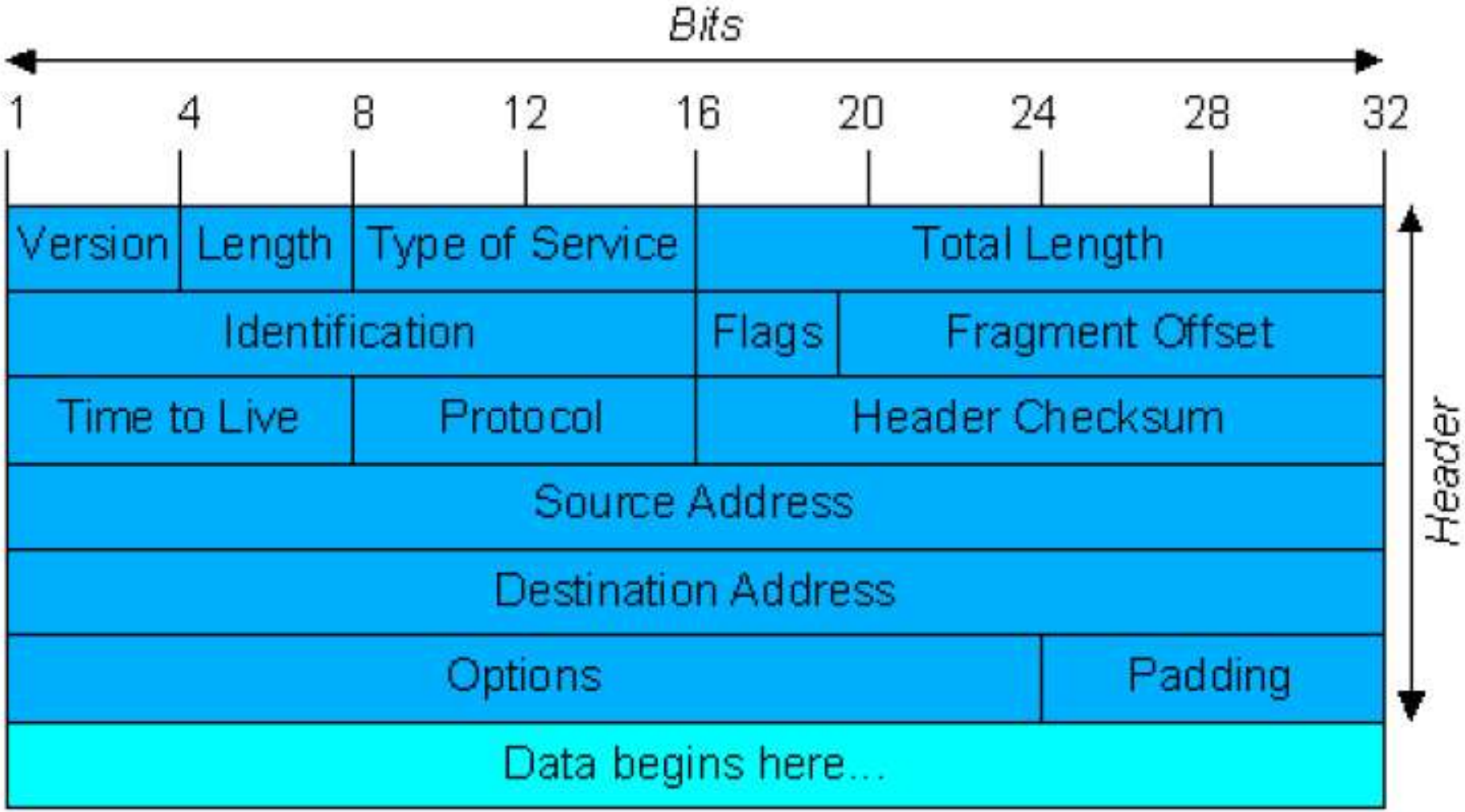
Ethernet Rahmen



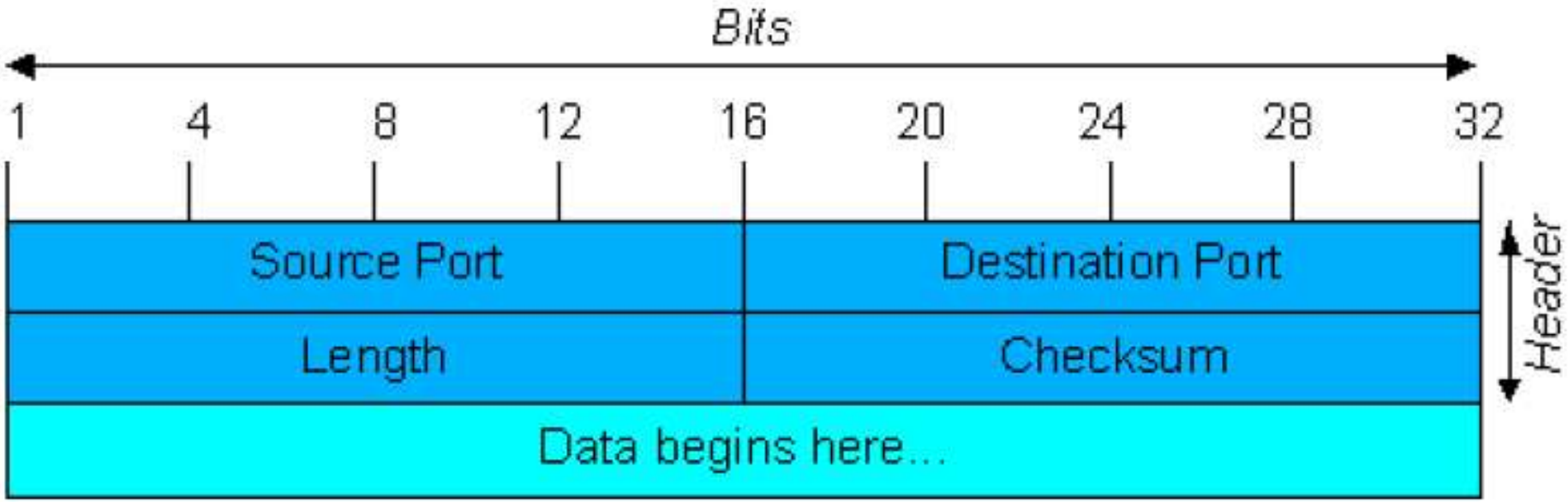
- Data Link Layer
  - Aufgabe: Zuverlässige Übertragung von Rahmen über Verbindung
  - Funktionen: Synchronisation, Fehlerkorrektur, Datenflusskontrolle

- Source: Ethernet (MAC) Adresse des Senders
- Destination: MAC Adresse des Empföngers
- Frame Type: Identification der folgenden Daten
- CRC: Fehlerkontrolle

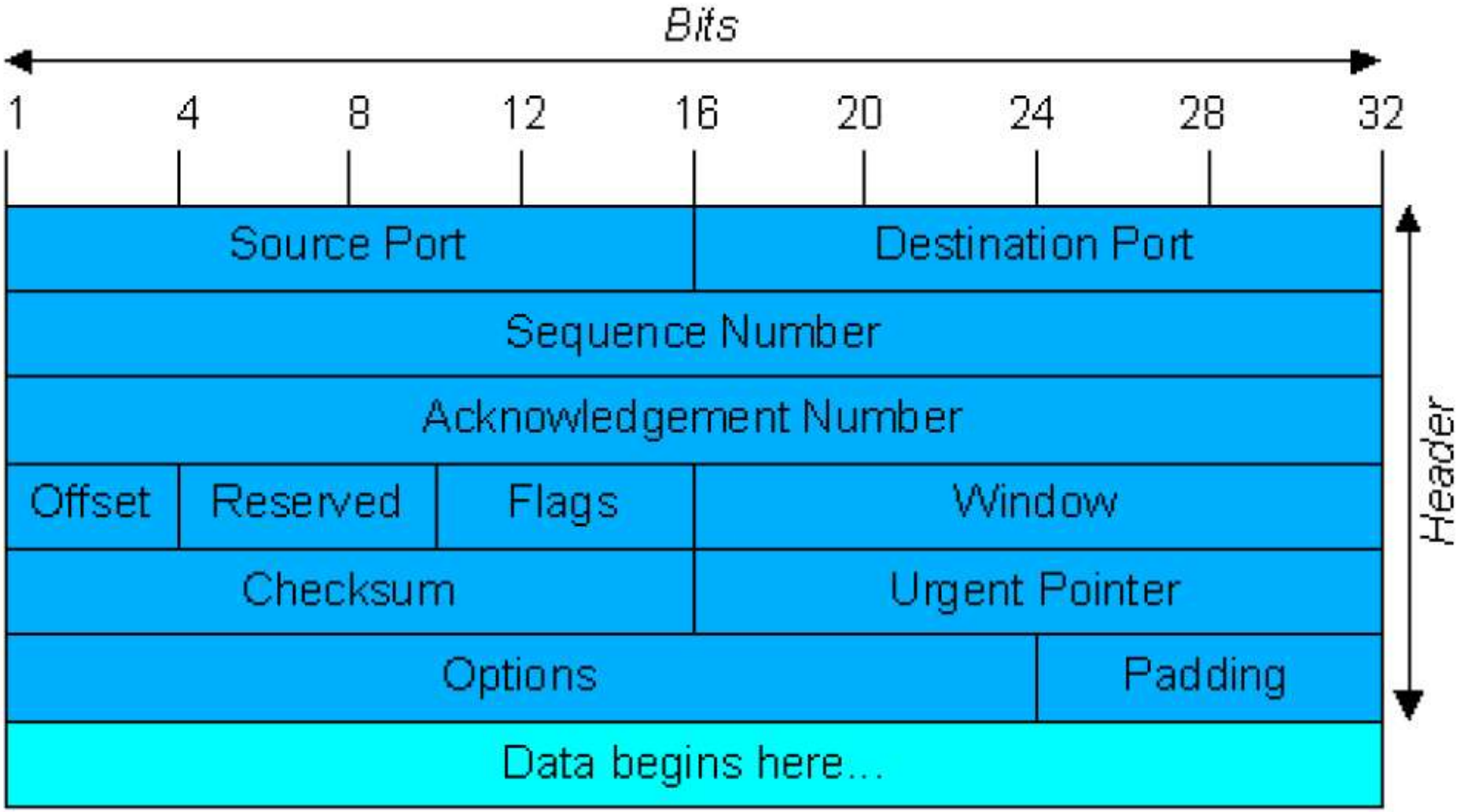
IP Header


Bits
1
4
8
12
16
20
24
28
32
Version
Length
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding
Data begins here...
Header

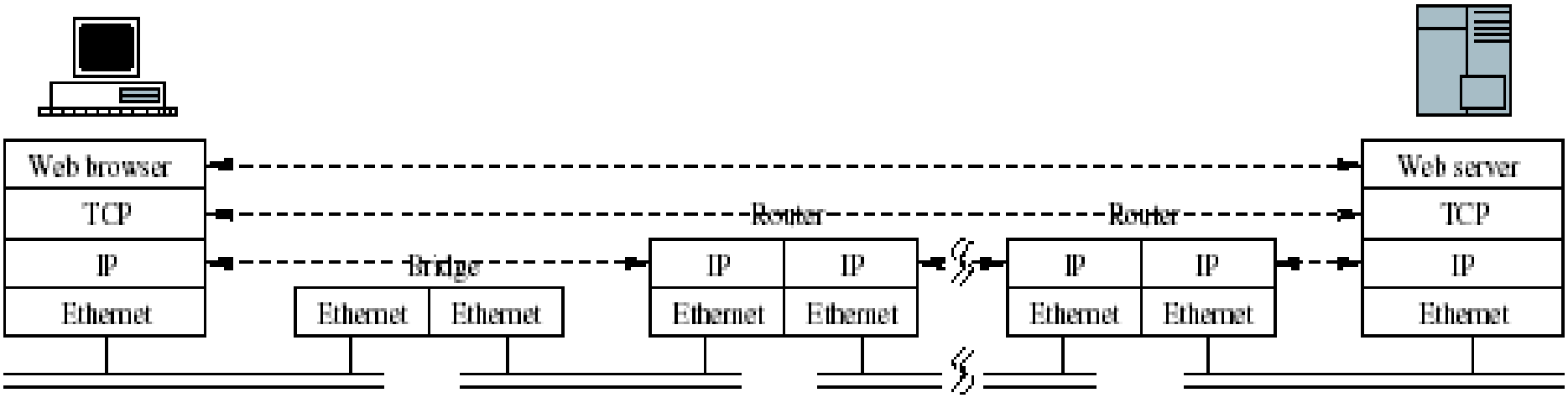
UDP Header


Bits
1
4
8
12
16
20
24
28
32
Source Port
Destination Port
Length
Checksum
Data begins here...
Header

TCP Header


Bits
1
4
8
12
16
20
24
28
32
Source Port
Destination Port
Sequence Number
Acknowledgement Number
Offset
Reserved
Flags
Window
Checksum
Urgent Pointer
Options
Padding
Data begins here...
Header

Verbindung über TCP/IP

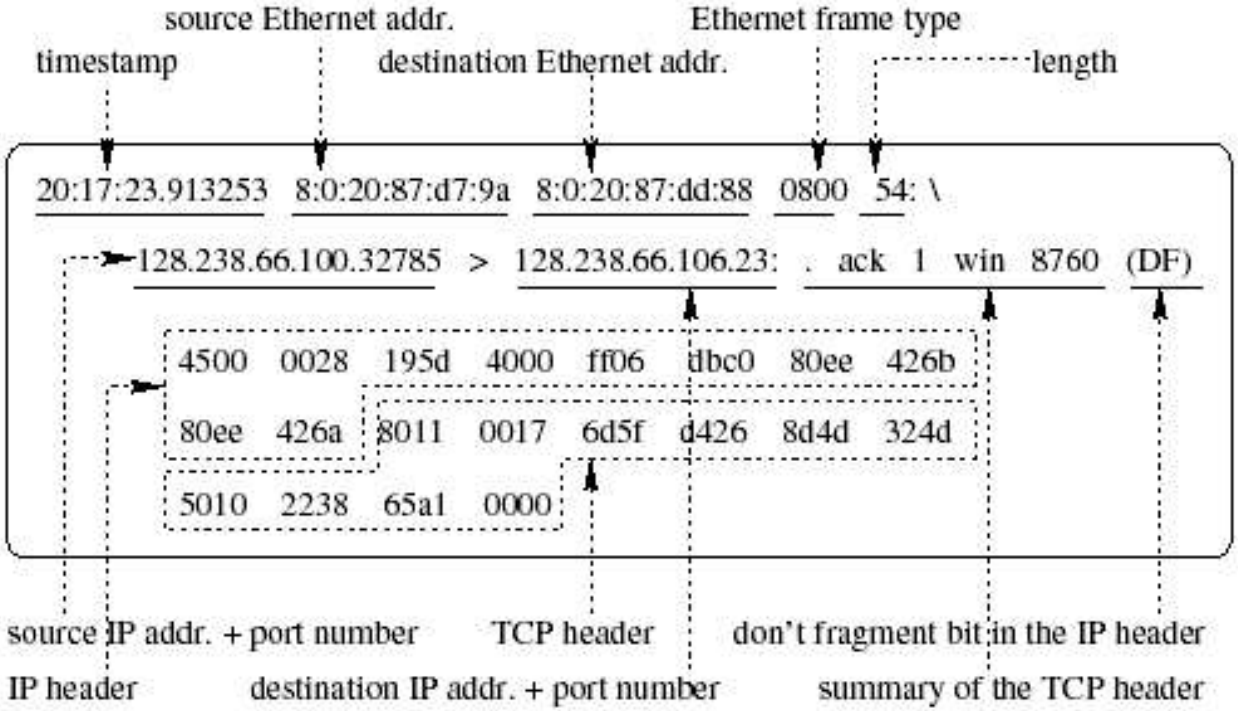


Quelle: Panwar, Mao, Ryoo, Li, „TCP/IP Essentials“, Lecture Slides

Netzwerk Konfiguration

- Übung 1:
  - Rufe ***ifconfig -a*** auf
- Fragen:
  - Wie viele Interfaces hat der Host?
  - Welche MTUs benutzen die Interfaces?
  - Existiert ein Subnetz?

tcpdump



Quelle: Panwar, Mao, Ryoo, Li, „TCP/IP Essentials“, Lecture Slides

Netzwerk Konfiguration

- Übung 2:
  - Host: Rufe ***tcpdump host [****hostIP****]*** auf
  - Host: Wechsel Kommandofenster
  - Host: Rufe dort ***ping 127.0.0.1*** auf
- Fragen:
  - Ist das Interface 127.0.0.1 aktiv?
  - Erscheinen ICMP Nachrichten im Output?
  - Warum?

Netzwerk Konfiguration

- Übung 3:
  - Host: Rufe ***netstat -in*** auf
  - Um Traffic zu erzeugen:
  - Host: ***sock -u -i -n200 [remoteHost]*** aufrufen
- Fragen:
  - Wie groß ist die durchschnittliche Kollisonsrate?

ARP

- Ethernet Frame muss an das Interface eines entfernten Routers gesendet werden
- MAC Adresse des Zielrechners ist in der Regel unbekannt
- Auflösung der MAC-Adresse nach der IP-Adresse wird benötigt

- ARP Tabellen werden dynamisch aufgebaut
- Neue Zuordnungen werden bei Bedarf ergänzt
- Einträge altern und laufen nach festgesetzter Zeit aus

ARP Übungen

- Übung 4:
  - Rufe ***arp -a*** auf
  - Wenn Server vorhanden ist
    - Lösche mit ***arp -d [remoteHost]*** ARP-Eintrag
  - Notiere ARP-Tabelle
  - Rufe ***tcpdump -enx -w exe4.out*** auf
  - Rufe ***ping [remoteHost]*** auf.

  - Kontrolliere die ARP-Tabelle
  - Werte exe4.out mit *ethereal* aus.

- Fragen:
  - Beschreibe, wie ARP funktioniert anhand der tcpdump Ausgabe

ARP Übungen

- Übung 5:
  - Rufe ***tcpdump host [localHost]*** auf
  - Rufe ***telnet 192.168.254.100*** auf

- Fragen:
  - Werte tcpdump Ausgabe aus
  - Beschreibe, wie ARP-Timeout und Retransmission ausgeführt wurden
  - Wie viele Versuche wurden unternommen, die nicht vorhandene IP-Adresse aufzulösen?

ARP Übungen

- Übung 6:
  - Rufe ***tcpdump -ex -w exe6.out*** auf
  - Starte Server neu
- Fragen:
  - Werte tcpdump Ausgabe aus
  - Beschreibe, gratuitous ARP

ICMP

- Internet Control Message Protocol
- Bestandteil jeder IP Implementierung
- Aufgabe:
  Fehler- und Diagnoseinformationen für IP zu transportieren
- ICMP wird oft auch für Testzwecke verwendet
  - Ermittlung, ob ein Host derzeit empfangsbereit ist

ICMP Übungen

- Übung 7:
  - ***tcpdump -enx host [****localHost****] and [****remoteHost****]***
  - ***ping -sv [****remoteHost****]***
- Fragen:
  - Welche ICMP Nachrichten werden von ping verwendet?

ICMP Übungen

- Übung 8:
  - ***tcpdump -x -s 70***
    host [*localHost****] and [****remoteHost****]***
  - ***sock -i -u -n1 -w1000 [****remoteHost****] 88888***

- Fragen:
  - Wie sieht die ICMP port unreachable Fehlermeldung aus?
  - Warum sind die ersten 8 Byte der original IP datagram payload in der ICMP Nachricht enthalten?

ICMP Übungen

- Übung 9:
  - ***tcpdump***
  - ***ping 192.168.254.100***
- Fragen:
  - Entsteht Traffic auf dem Netzwerk?
  - Begründe anhand der ping Ausgabe.