ICMP

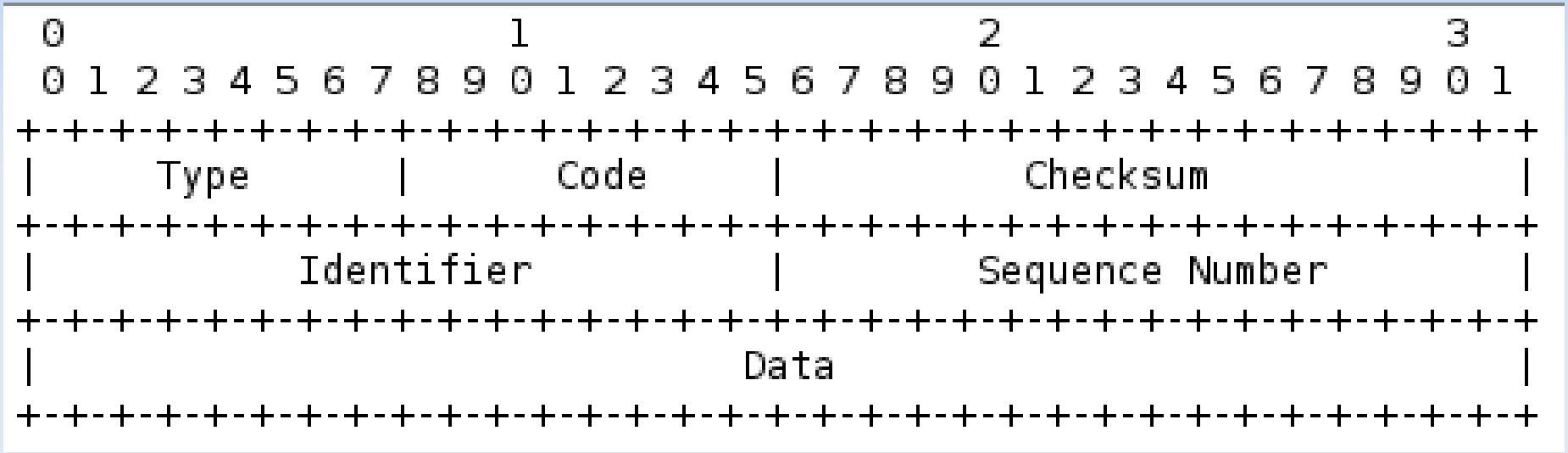
Internet Control Message Protocol

Michael Ziegler

- Situation:
  - Komplexe Rechnernetze (Internet, Firmennetze)
  - Netze sind fehlerbehaftet
  - Viele verschiedene Fehlerursachen
  - Administrator müsste zu viele Fehlerquellen prüfen

- Lösung:
  Internet Control Message Protocol (ICMP)
  - Teil des Internet Protocol (IP)
  - Informiert Absender eines Paketes über Fehler
  - Sendet Nachrichten in Form von IP-Paketen
  - Berichtet über Probleme, kann sie aber nicht lösen
  - Kommunikation der Netzteilnehmer wird erwartet

- Aufbau einer Nachricht:



Quelle: RFC 792

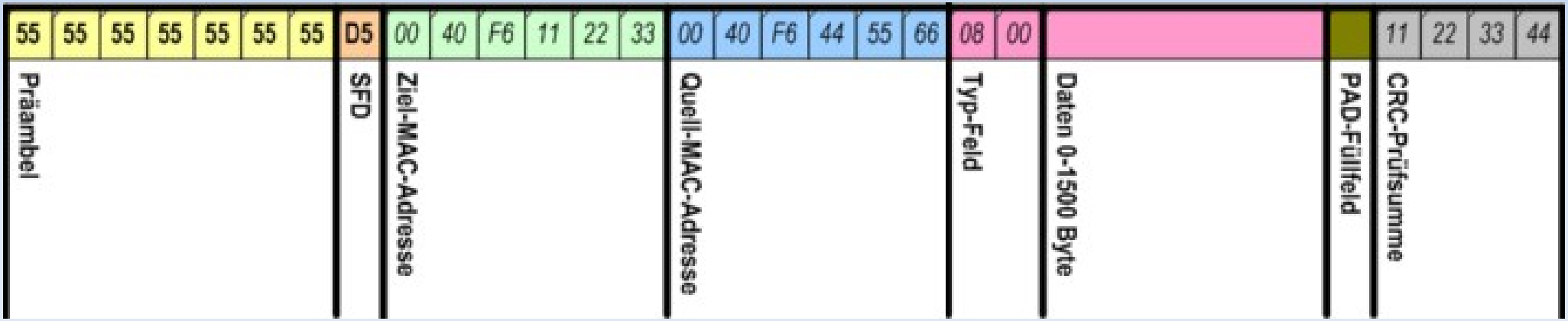
- Eingekapselt in ein IP-Paket

- Type-Feld: Gibt Art der Nachricht an
- Die wichtigsten Typen:
  - 3: Destination unreachable
  - 4: Source Quench
  - 5: Redirect
  - 8/0: Echo Request/Reply
  - 11: TTL exceeded
  - 12 : Parameter Problem

- Type 3: Destination unreachable
- Code-Feld:
  - 0: Network unreachable
  - 1: Host unreachable
  - 2: Protocol unreachable
  - 3: Port unreachable
  - 4: Fragmentation needed but DF set

- Code 4: Fragmentation needed but DF set
  - Situation:
    - meist verbreitetes Transportprotokoll ist Ethernet
    - Daten werden in Frames verschickt
    - Frames haben immer eine feste Größe
    - Maximale Datenmenge pro Frame: 1500 Bytes
    - wenn ”zu wenig” Daten im Frame, wird dieser aufgefüllt

- Aufbau eines Ethernet-Frames:



Quelle: http://de.wikipedia.org

- Maximal 1500 Bytes an Daten (MTU)
- Pad-Feld wird zum Auffüllen benutzt

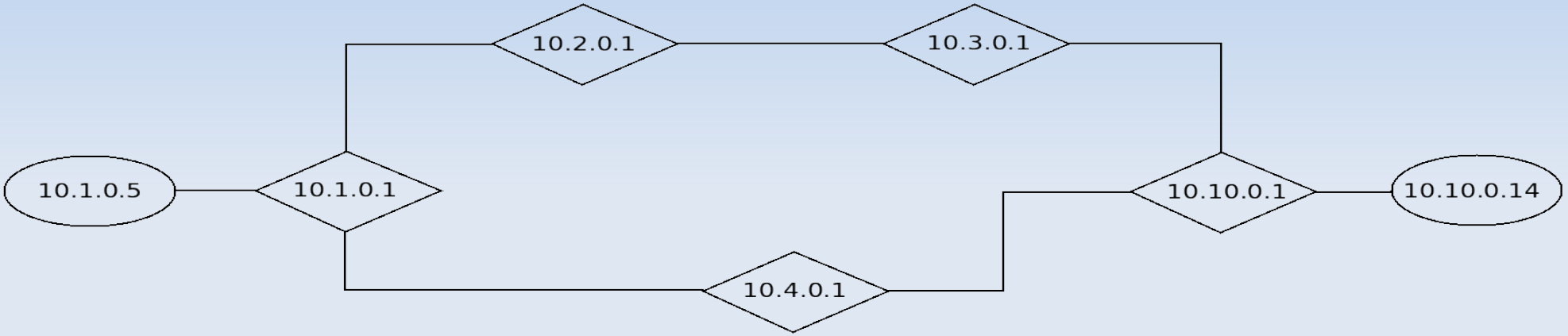
- IP-Pakete werden in Ethernet-Frames eingekapselt
- Wenn Paket größer als MTU, wird fragmentiert
- Fragmentierung verschwendet Zeit und Bandbreite
- Ziel: Fragmentierung vermeiden

- Problem: MTU-Wert kann variieren, z.B.
  - Ethernet 1500 Bytes
  - DSL (PPPoE) 1492 Bytes
- Kleinste MTU auf dem Weg zum Empfänger: Path MTU
- Methode um Path MTU herauszufinden: Path MTU Discovery (PMTUD)

- Path MTU Discovery
  - IP-Header: Don't-Fragment-Bit wird gesetzt
  - Router dürfen dieses Paket nicht fragmentieren
  - Wenn Paket zu groß ist, wird ICMP-Nachricht ”Fragmentation needed but DF set” verschickt
- Sender reduziert seine Paketgröße
- Fragmentierung wird vermieden

- Type 4: Source Quench
  - Router ist überlastet
  - Sendet Source-Quench-Nachricht an Sender
  - Sender reduziert seine Senderate
- Im Internet kaum genutzt, TCP hat eigene Methode zur Stauvermeidung

- Type 5: Redirect



- Router kann Sender über schlechte Routen informieren
- Problem: Sender meist nicht verantwortlich
- Besser: Routingprotokolle (z.B. OSPF)

- Type 8/0: Echo Request/Reply
  - Sender sendet Echo Request mit beliebigen Daten an den Empfänger
  - Empfänger antwortet mit Echo Reply und denselben Daten
- Mächtiges Hilfsmittel bei der Fehlersuche
  - testet ob ein Rechner oder Router erreichbar ist
  - erlaubt Simulation anderer Techniken, z.B. PMTUD

Einschub

Sicherheit – Firewalls

Soll man Echo Requests/Replies blocken?

Type 8/0: Echo Request/Reply - blocken?

- Nein!
- Ziel: Rechner verstecken
  - Funktioniert nicht!
  - Rechner existiert, ARP-Auflösung funktioniert
  - daher sendet der Router keine ICMP-Nachricht!
- Verzicht auf dieses mächtige Hilfsmittel lohnt sich nicht

- Type 11: Time To Live exceeded
  - Problem: Router können zirkuläre Routen nicht erkennen
  - IP-Pakete werden mit einem TTL-Wert losgeschickt, jeder Router verringert diesen um 1
  - Wenn TTL 0, schickt der Router eine ICMP-Nachricht zurück und verwirft das Paket
- Kann für Route-Tracing benutzt werden

- Type 12: Parameter Problem
  - IP-Header des Paketes enthält ungültige Werte
  - meist verursacht durch Übertragungsfehler
  - tritt beim erneuten Senden des Paketes wahrscheinlich nicht wieder auf

Sicherheit – Firewalls

Soll man ICMP blocken?

Sicherheit: Soll man ICMP blocken?

- Nein!
  - man braucht die gebotene Funktionalität
  - Sicherheit wird nicht erhöht
- Einzige Angriffsfläche bieten die Typen 4 und 5
  - DoS- und MitM-Attacken denkbar
  - werden von modernen IP-Stacks ignoriert
  - Erkennung gefälschter ICMP-Nachrichten möglich

- Weitere Nachrichtentypen
  - 9/10 Router Advertisement / Solicitation
  - 13/14 Timestamp Request / Reply
  - 15/16 Information Request / Reply
  - 17/18 Netmask Request / Reply
- in der Praxis nicht bewährt
- ersetzt durch spezielle Protokolle

Vielen Dank für Ihre Aufmerksamkeit!

- Quellen:
  - Douglas E. Comer:
    Internetworking with TCP/IP
  - RFC 792:
    Internet Control Message Protocol
  - RFC 1256:
    ICMP Router Discovery Messages