Implementierung von UDP Options

RFC 9868 in Zig mit eBPF-Monitoring

Alan Bernstein

FernUniversität in Hagen

Problemstellung: UDP heute

Limitierungen von UDP (RFC 768, 1980):

- Keine native Integritätsprüfung der Payload
- Fehlende Authentifizierung auf Transportebene
- Keine Path MTU Discovery
- Keine Timestamps für RTT-Messung

Minimalistisch, aber unflexibel für moderne Anforderungen.

UDP Header (8 Bytes)

Source Port	Dest Port
Length	Checksum
16 bits	16 bits

Seit 45 Jahren unverändert

Warum werden UDP Options benötigt?

Drei zentrale Gründe:

- **Legacy-Kompatibilität**
  Bestehende UDP-Anwendungen können nicht einfach auf DTLS migriert werden.
  Options werden von Legacy-Empfängern ignoriert.
- **Performance-Anforderungen**
  Echtzeit-Anwendungen benötigen minimale Latenz.
  UDP Options arbeiten direkt auf Transportebene – ohne zusätzliche Schicht.
- **Middlebox-Traversal**
  NATs und Firewalls müssen UDP-Pakete korrekt weiterleiten.
  RFC 9868 definiert dafür die Options Checksum (OCS).

Prominente UDP-basierte Protokolle: QUIC (HTTP/3) | WebRTC | DNS

RFC 9868: Transport Options for UDP

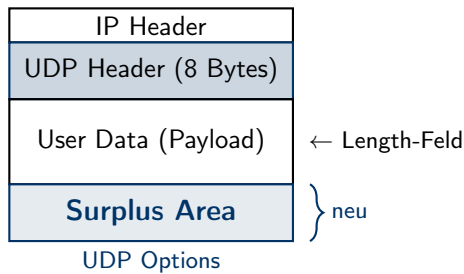
Definition (Oktober 2025):

- Erste Erweiterung von RFC 768 nach 45 Jahren
- Options im *Surplus Area* zwischen UDP-Payload und IP-Ende
- Abwärtskompatibel zu Legacy-Empfängern

Kernprinzipien:

- UDP bleibt zustandslos
- UDP bleibt unidirektional
- Options sind ein Framework

UDP Datagram mit Options



UDP Options Architektur

Definierte Option-Typen:

- **OCS** – Options Checksum
  Sichert Middlebox-Traversal
- **FRAG** – Fragmentation
  UDP-Level Fragmentierung, unabhängig von IP
- **TIME** – Timestamps
  RTT-Messung und Rate Limiting
- **AUTH** – Authentication
  Source-Validierung und Integritätsschutz

Zusätzlich: EOL (End of List), NOP (Alignment)

Option Format (TLV)

Type-Length-Value Schema

Anwendungsfälle für UDP Options

Sicherheit & Integrität:

- Authentifizierung und Integritätsschutz (AUTH)
- Path MTU Discovery ohne Payload-Beeinflussung

Echtzeit & Performance:

- Präzise RTT-Messung mit Timestamps (TIME)
- UDP-Level Fragmentierung statt IP (FRAG)

Einsatzgebiete: VoIP | IoT | Gaming | Streaming

Zusammenfassung

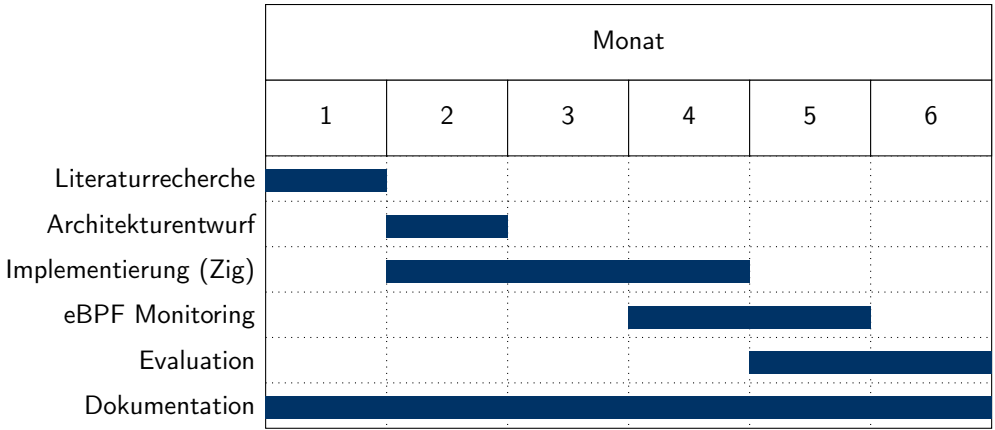
RFC 9868 erweitert UDP um:

- Sicherheitsfunktionen (Authentifizierung, Integrität)
- Path MTU Discovery
- Timestamps für RTT-Messung
- Fragmentierung auf UDP-Ebene

Vorteile:

- Abwärtskompatibel – Legacy-Empfänger ignorieren Options
- Kein zusätzlicher Protokoll-Overhead wie bei DTLS
- Erweiterbar durch neue Option-Typen

Zeitplan


Monat
1
2
3
4
5
6
Literaturrecherche
Architekturentwurf
Implementierung (Zig)
eBPF Monitoring
Evaluation
Dokumentation