Encrypted Transport Protocol Path Explicit Signals

draft-reddy-tsvwg-explicit-signal-01
IETF117, July 2023

T. Reddy (Nokia)
Dan Wing (Citrix)
M. Boucadair (Orange)
Problem

• Cellular needs to manage radio resources
  – Network congestion/noise/distance
  – Mobile device changes towers: drop or transmit?

• IAB discussions explicit signals
  – Transport Protocol Path Signals, RFC8558
  – Considerations on Application - Network Collaboration Using Path Signals, RFC9419

• Improving radio management can improve user experience
Network-Layer verses Transport-Layer signal

• IPv6 hop-by-hop headers limitations:
  – IPv4
  – Routers drop hop-by-hop options (to avoid slow path)
  – 90% loss rate in transit ASs for packets with HBH options
  – Years until network adoption of draft-ietf-6man-hbh-processing
Solution overview

• *Sender* obtains keys
• *Sender* signals “tag” in the packet
  – As new UDP option (“trailer”)
• Necessary network elements understand the signal
  – ~Always near the subscriber (“last hop”)
• IPv6 and IPv4
Design Principles

• Explicit signal is *encrypted or obfuscated*
• Explicit signals are shared intentionally, not accidentally
  – Authentication and trust between the endpoint and network path elements
• Endpoint constrains data shared with network
• Explicit signal is *integrity-protected*
• Explicit signals decoupled from endpoint protocol state
  – Reduces network interference opportunities
System Diagram

- **client**
- **Edge router**
- **Access network**
- **server**

Connect

Obfuscation/encryption key

- **IP** 
  - UDP 
  - tag=0xe53f

Obfuscation/encryption key

- **IP** 
  - UDP 
  - tag=0xe53f

- **IP** 
  - UDP 
  - tag=0xc679

Scope of draft-reddy-tsvwg-explicit-signal
• Comments and suggestions are welcome