Adding trust and consent to path signals

What's the problem?

There's a growing disconnect between directions in **privacy** and **network management**, and we're lacking an architectural approach to reconcile them

Applications and networks can benefit from coordination, but existing mechanisms use insecure and untrusted information that can't be distinguished from attacks

Proposal: work on defining how trust and coordination can be added into protocols that do path signaling

Recent and upcoming trends

Encryption & Privacy

- Content — More ubiquitous TLS
- Control — QUIC, Encrypted DNS, Encrypted Hello (ECH)
- Traffic flow control — Privacy proxying (MASQUE), flow mobility and multihoming (MPTCP, QUIC)

Higher flexibility in evolving transports, congestion control, etc.

Increasing deployment of services in cloud platforms & CDNs

Increasing distribution of local instances, often in ISP networks

Existing practices

- Debugging
- Network performance analysis (transport characteristics, destinations)
- Filtering services (often via looking up DNS or TLS SNI)
- Various attack prevention mechanisms (traffic signature, destination, domain)
- Zero rating
- Optimizations (finding the closest server, transport “enhancements”)

These features may or may not be desired by endpoints and users

Implementation techniques were chosen because inspecting packets was often the easiest and fastest option

Documents on Path Signals

IAB stream has multiple documents on this topic already

- The Wire Image of a Network Protocol, RFC 8546
- Transport Protocol Path Signals, RFC 8558

There are also well-behaved (though not always universally deployed) standard designs

- ECN
- Spin

Some more controversial ones:

- SPUD, PLUS
- More bits (see QUIC and IPPM)
- APN BOF
- Network tokens
- Re-implementing every feature ever used

Danger of inaction

Deployments and users are left with an either/or choice between privacy and network functions

Solutions will be found for required functions, but they may not be standards across different networks, and may not meet the goals of the IETF

What can we do?

Highlight the need for solutions in standards

Define a framework for thinking about trust and consent between clients and paths, including aspects of consent, preventing misuse, information flows, addressing, etc.

Start conversations from a place of problem statements, not solutions

Some initial principles

Information should be distributed intentionally, not accidentally

Consent, type of information, and trust must determine what information can be shared and with whom

Information should be specific, not general.

- Identify what you need instead of who you are

Unlikely that there is a single framework that supports all information sharing

- Network to app and app to network are different, tweaking some bits on a packet (ECN) is different from establishing a full connection and signaling channel with someone (MASQUE)

Guiding questions

Any new network path functions should consider:

- What is the **minimum set of entities** that need to be involved in order to perform this function?

- What is the **minimum information** each entity in this set needs to perform its part of the function correctly and reliably?

- Which entities must **consent** to each piece of information that is shared?

Ideas?