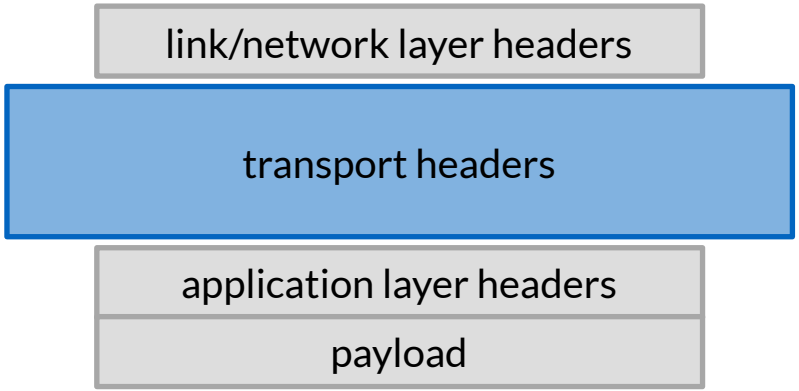
The Wire Image of a Network Protocol

Brian Trammell
Mirja Kühlewind
OPSEC — IETF 102 Montréal — Friday 20 July 2018

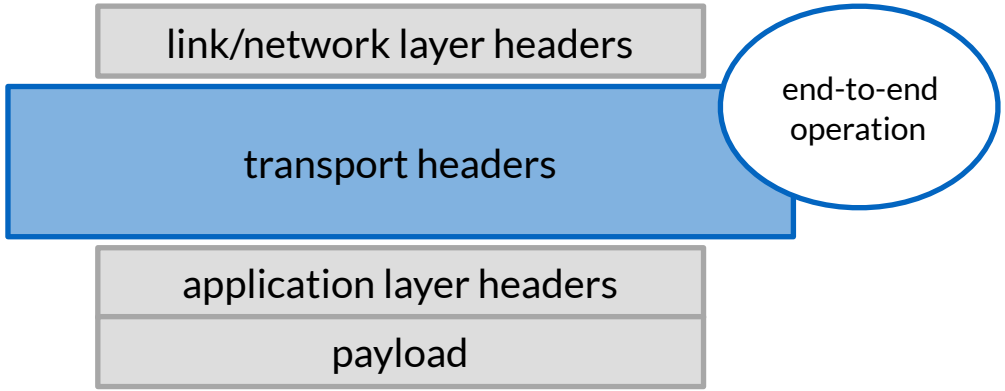
Transport protocol design:

1990s style



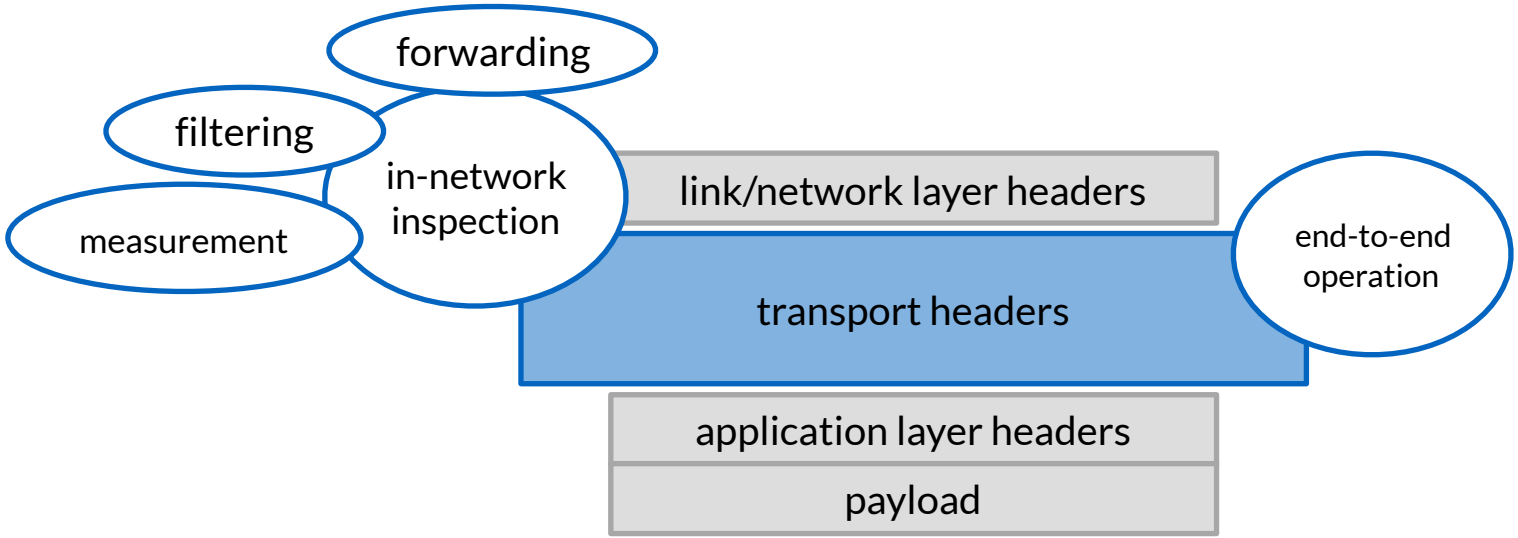
Transport protocol design:

1990s style



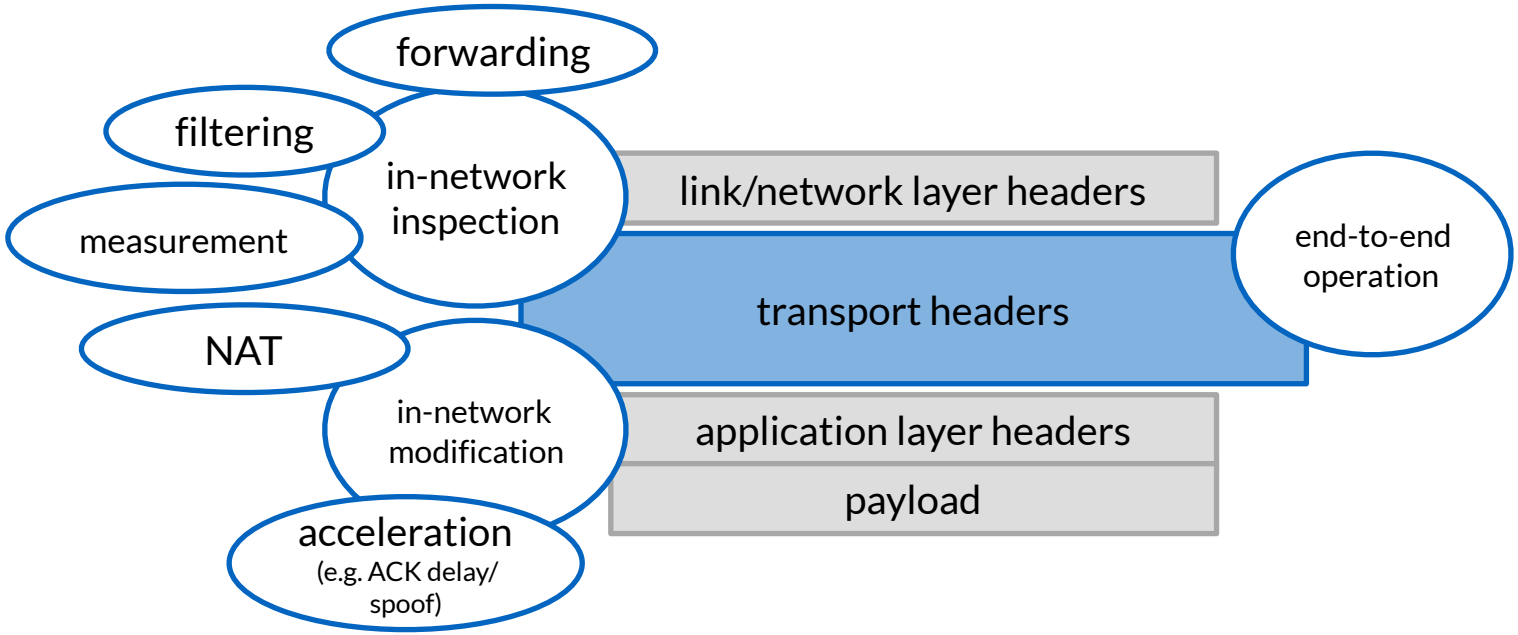
Transport protocol design:

1990s style

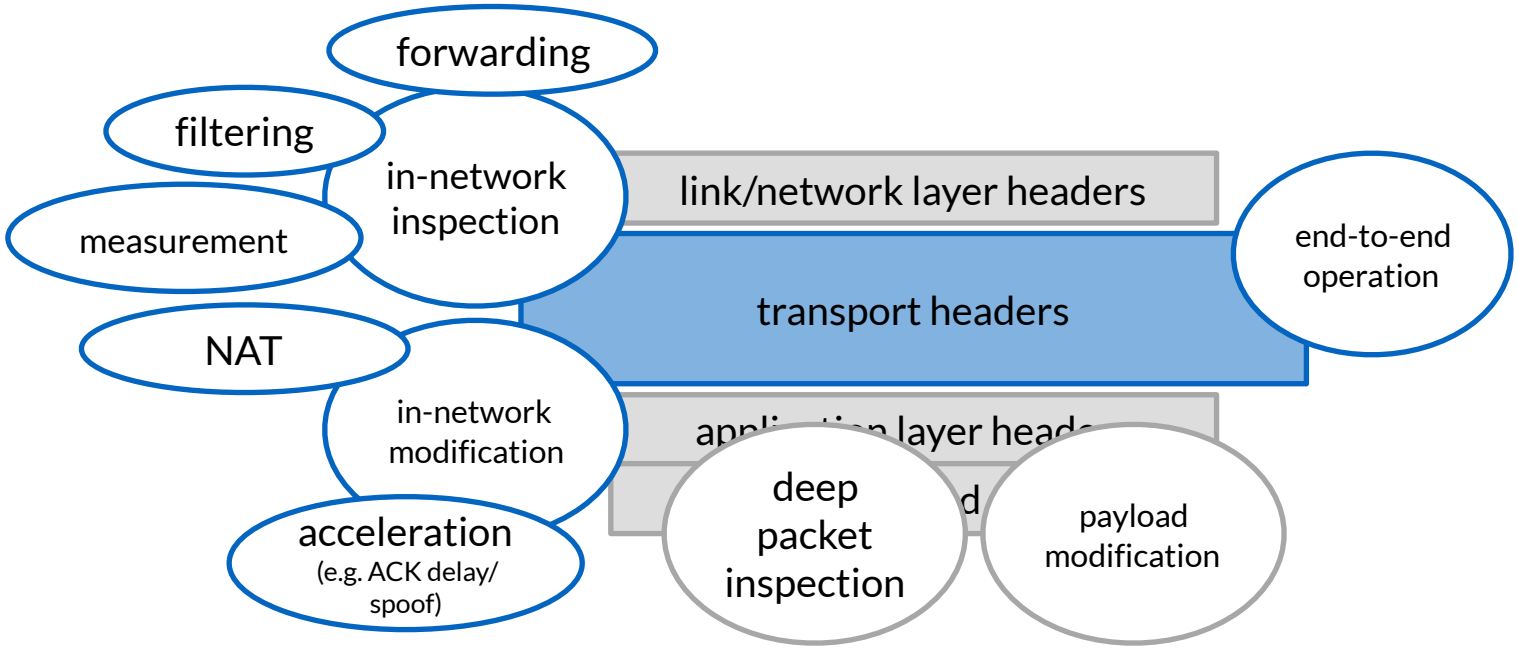


Transport protocol design:

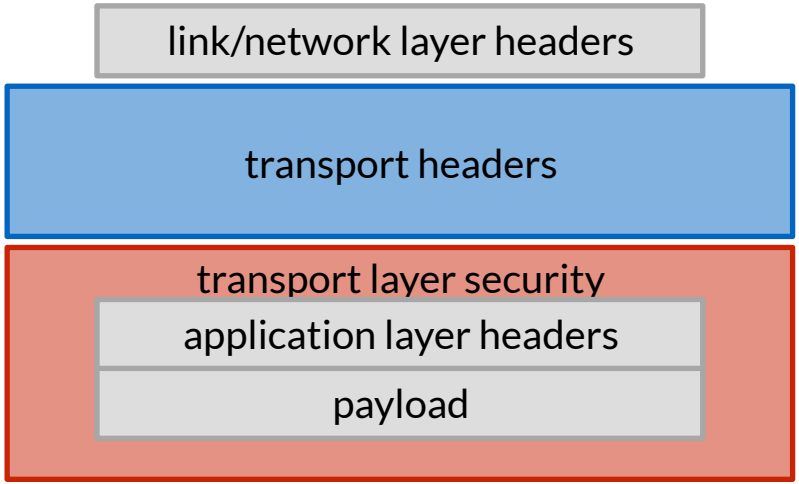
1990s style



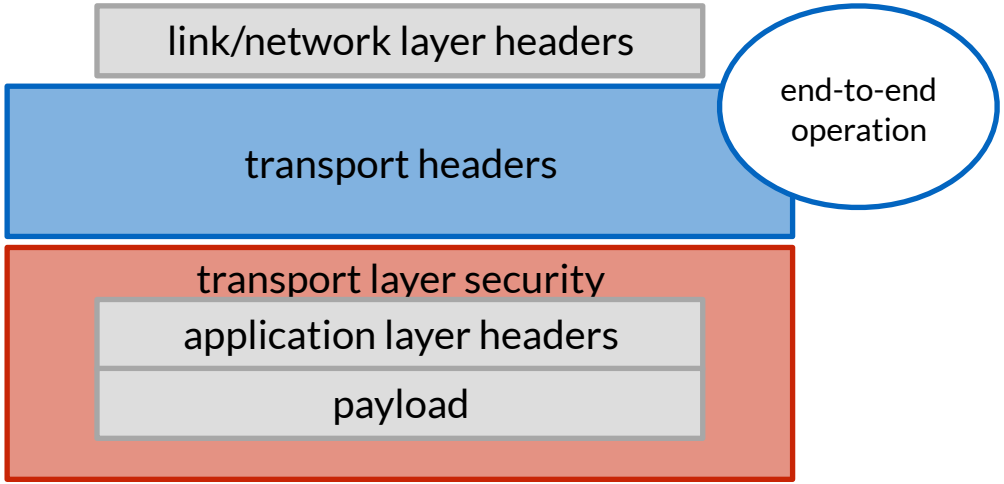
Transport protocol design:
1990s style



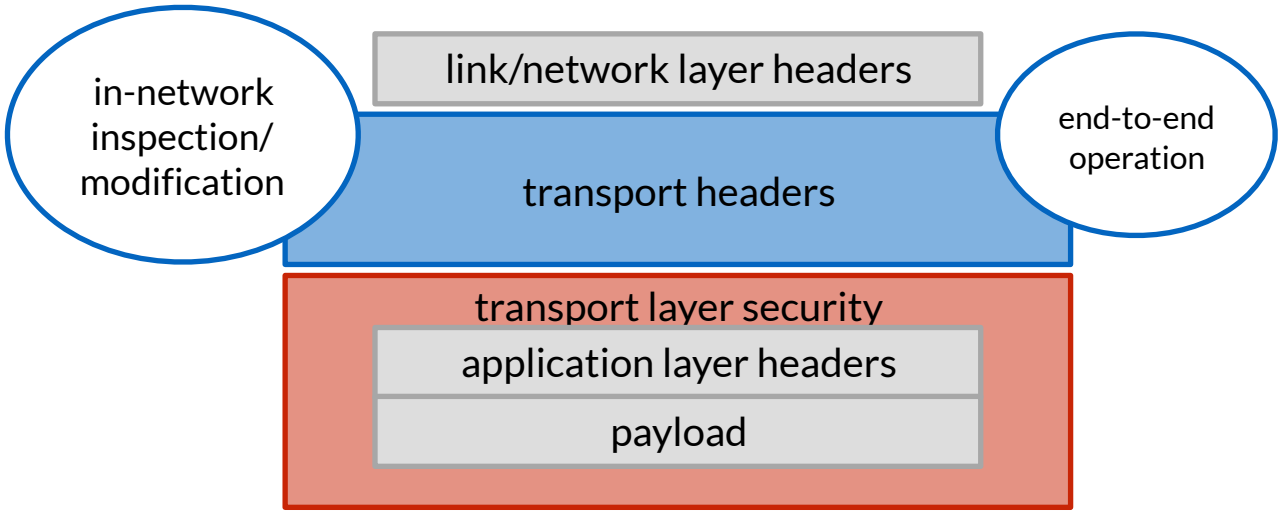
Transport protocol design:
now with security!



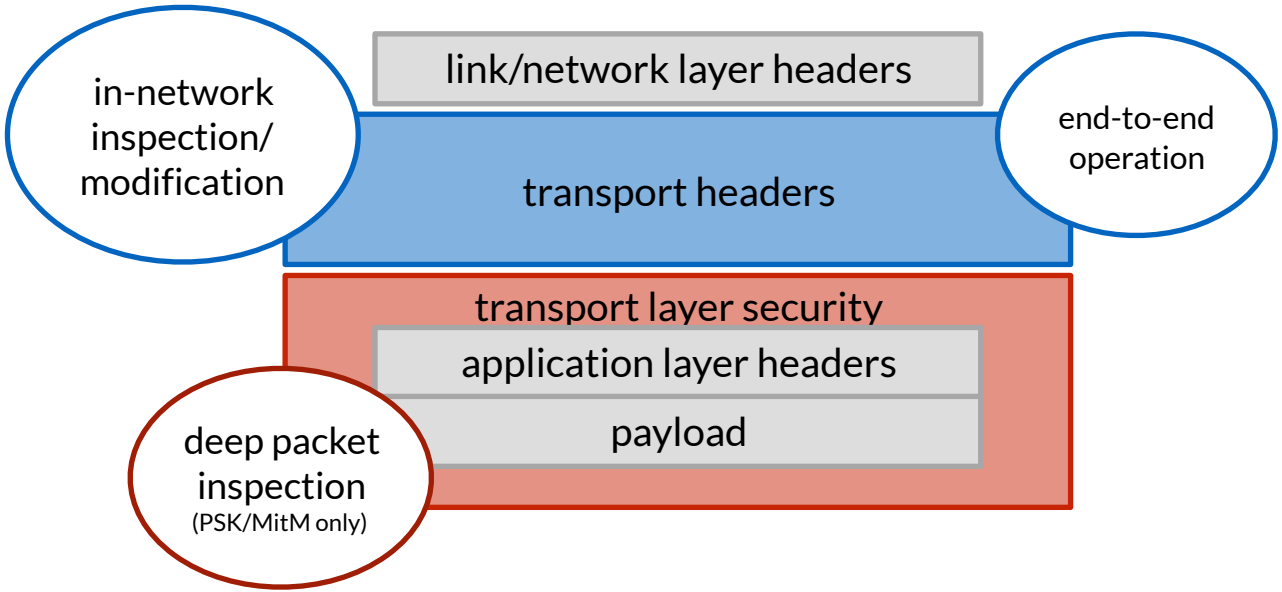
Transport protocol design:
now with security!



Transport protocol design:
now with security!

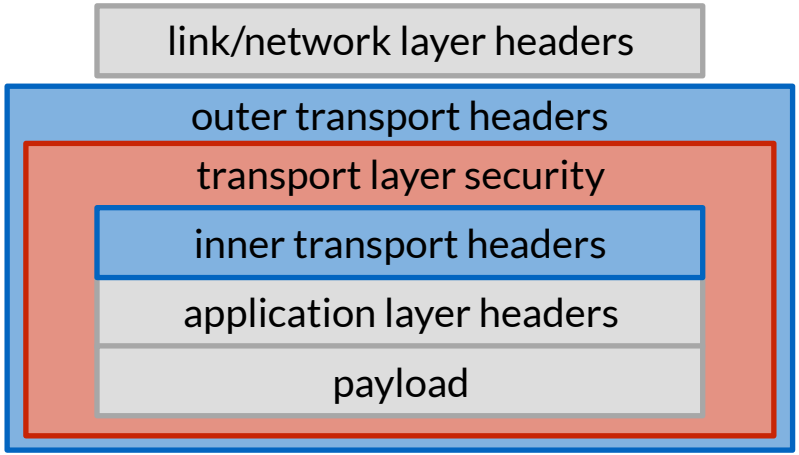


Transport protocol design:
now with security!



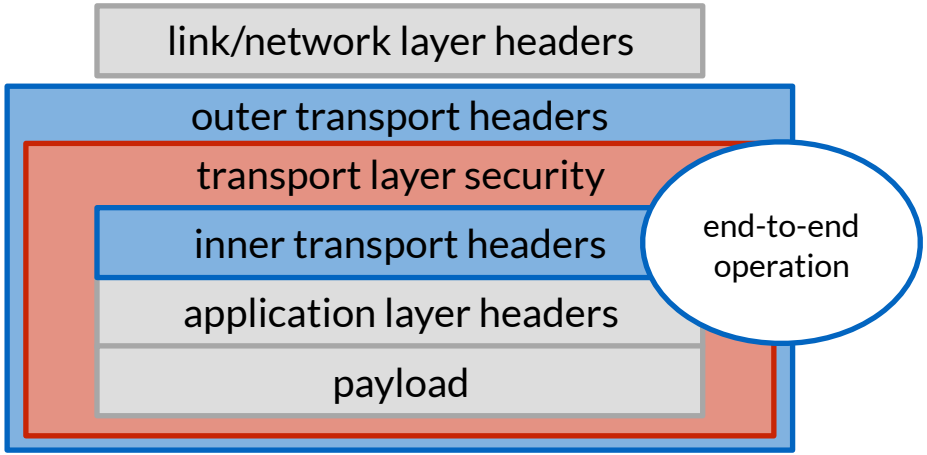
Encrypted transport protocol design:

introducing the wire image



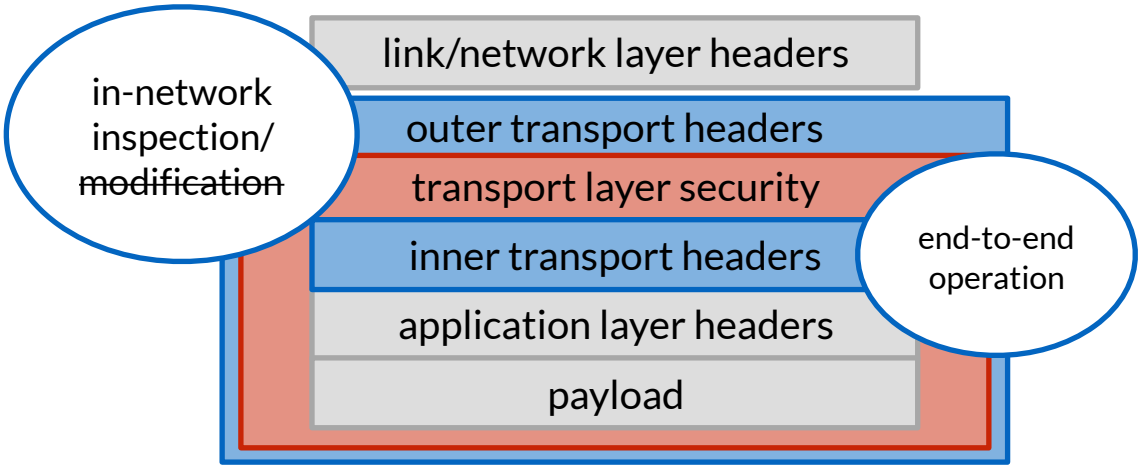
Encrypted transport protocol design:

introducing the wire image

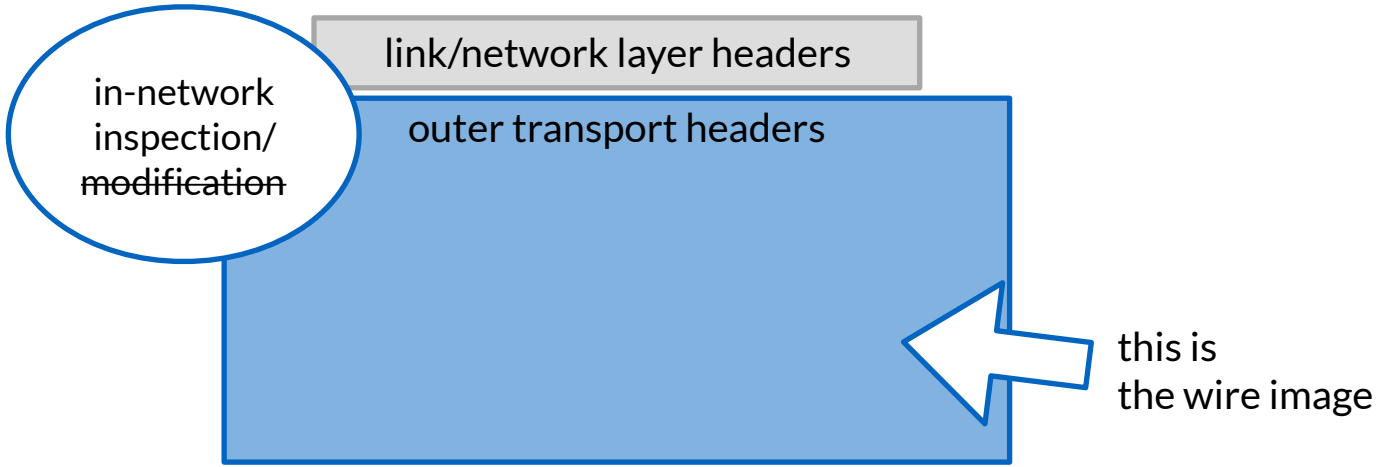


Encrypted transport protocol design:

introducing the wire image



Encrypted transport protocol design:
introducing the wire image



What's in the wire image?

Information in unencrypted bits in the protocol headers.
(this is the obvious part)

Length and entropy of all bits in the packet.
(provides an upper bound on information content,
even for the encrypted bits)

Timing of packet observation (transmission, arrival)
(information about the sender's behavior)

Why does this matter?

The advent of encrypted transport protocols means that a protocol's end-to-end operation is separate from its appearance on the wire, and how intermediate devices interact with it.

This is new.

Design goal: every bit needs to be designated and considered

There's no default for determining what signals to send; it needs to be determined per transport.

And it needs to be optional; if a client or server don't want to send that signal, it can't be needed for session state.

Ops impact: less (but hopefully, eventually) better visibility

Encryption of transport protocols (e.g. QUIC) will reduce the size of the wire image, and the set of things that can be done with it.

The opportunity to explicitly engineer the wire image can make new and more useful information available in the future.

Further Reading

please read and comment on IAB drafts on this topic:

draft-trammell-wire-image

draft-iab-path-signals