Path Layer Substrate Protocol (PLUS)

Side Meeting - IETF97 Seoul - 15 November 2016

PLUS, new and shiny

- New mailing list: plus@ietf.org ***(pending)***
- New drafts:
  - draft-hardie-path-signals-00: Problem statement
  - draft-trammell-plus-statefulness-00: middle-point view on state management
  - draft-trammell-plus-abstract-mech-00: BoF slides in draft format
- New charter proposal
  - Smaller initial scope in response to feedback in Berlin

draft-hardie-path-signals

- TCP's state mechanics uses a series of well-known messages that are exchanged in the clear.
- Often used as signals by network elements.
- In transports that do not exchange these messages in the clear, on-path network elements lack those signals.

Currently Implicit Signals

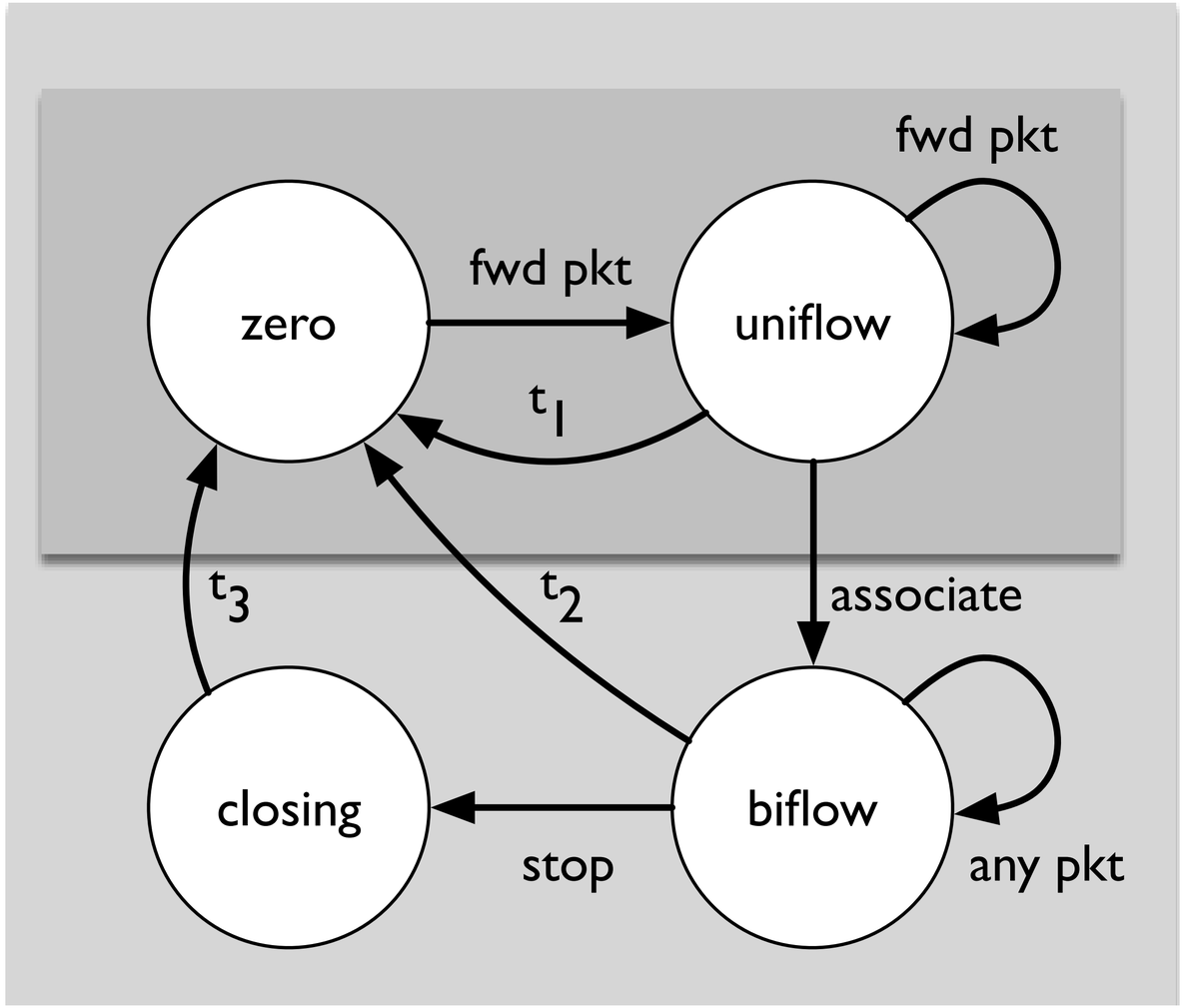
- **Session establishment:** Session identity, Routability and Consent, Resource Requirements
- **Network Measurement:** Path Latency, Path reliability and consistency

- **Options for future protocols**
  - Do not restore these signals —> leading to earlier state expiry for non-identifiable traffic?
  - Replace these with network layer signals —> deployment problems of IPv6 HBH headers…
  - Replace these with per-transport signals —> for each new transport separately…
  - Create a set of signals common to multiple transports —> PLUS **<— we are here**

draft-trammell-plus-statefulness

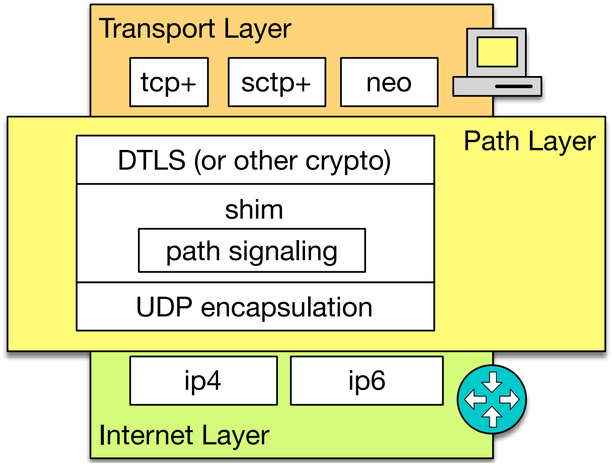
- State machine intended to replace the de-facto use of the TCP state machine or incomplete forms thereof by stateful network devices
- Transport-independent signaling based on network point of view
  - Which information is really needed for state management in the network?
- Common *wire image* to manage state for UDP-based, encrypted transport protocols like QUIC
- While still allowing for fast state timeout of non-established or undesirable flows

Transport-Independent State Machine for Stateful On-Path Devices



draft-trammell-plus-abstract-mech

- Mechanism Definitions
  - Sender-to-Path Declarations
  - Path-to-Receiver Declarations with Feedback
  - Direct Path-to-Sender Declarations



- Technical Considerations
  - Cryptographic Context Bootstrapping
  - Adding Integrity and Confidentiality Protection Along thePath

Next steps

- Define narrowed scope
  - Step 1: state exposure
  - Step 2: transport-layer measurability
    (explicit seqnr/acknr/ts equivalent)
- Write protocol spec (wire formats are easier to argue about)
- Another BoF: Chicago? Prague?
- Sign up editors, authors, and reviewers

Proposed charter

- https://github.com/ietf-plus/charter/blob/master/charter-plus.txt

- This proposed working group will define a new Path Layer UDP Substrate (PLUS) protocol, that supports in-band management of in-network state (e.g. on firewalls and NAT boxes) in a transport-independent way. PLUS will, in effect, provide a common "wire image" for new, encrypted transport protocols. PLUS is intended to be deployed underneath encrypted transport protocols, which protect the confidentiality of their payloads and most of their headers, and can protect the integrity of those headers exposed to the network. Given current deployment practices and the constraints they impose on deploying new protocols, PLUS will be defined as a shim layer, on top of UDP and underneath the actual transport protocol.