Beneficial Functions of Middleboxes

draft-dolson-plus-middlebox-benefits-03

Authors: D. Dolson, J. Snellman, M. Boucadair, C. Jacquenet

IETF 98

Presenter: David Dolson

Purpose

- Discuss benefits of network devices to provide context for discussion of trade-offs
- Inspired by PLUS, focus on transport layer (esp. TCP) functions
- Application-layer middlebox functions are out of scope (but useful functions exist)
  - See draft-mm-wg-effect-encrypt
- Look at (1) passive measurements and (2) active traffic modification
- Manual trouble-shooting (Wireshark) & proactive monitoring

Stating the Obvious

- The Internet is complicated; the end-to-end principle is an idealization
- The network operator:
  - often called upon first when applications are broken
  - expected to do capacity planning and upgrades

Measurements (Management and Diagnosis)

From the ToC:

Example: Diagnose Video Quality

(First assume the video traffic can be identified.)

- Missing frames? Packet loss upstream.
- Duplicate frames? Packet loss/corruption downstream.
- Reordered frames? ECMP issue upstream.
- Corrupted frames? Bad hardware upstream.
- High RTTs? Downstream buffer bloat.
- Full window? Bottleneck at receiver node.
- Otherwise healthy? Sender too slow (server, proxy, or cache).

Active Functions

From the ToC:

Example: Firewall

Policy: Permit only internally-initiated connections

- Maintain state per TCP connection
- Only permit state to be created by outbound SYN
- Deny inbound packets not matching any state
- Deny inbound packets with inappropriate sequence numbers
- Deny non-sane packets

Recurring Transport-Layer Tools

- Connection state (TCP start/established/end)
- Association and Confirmation signalling
- Tracking sequence numbers (loss, reordering and retransmissions)
- Correlating acknowledgements to data
- Measuring receive window
- Sanity checking

Virtually all of the TCP header and option fields are used.

Of Concern to IETF

- Buffer bloat - detected with round-trip times
- DDoS detection and mitigation - assisted by association/confirmation signaling
- Network-assisted bandwidth aggregataion

What's Next?

- It is clear that functions and observations within the network improve the network for the users.
- It has been our goal to socialize these.
- To share this with the larger IETF community, can we progress towards publication?
- Request feedback about:
  - Is this the correct list of functions, and are they described properly?
  - Security: can exposing some information improve security functions?
  - Would it be good to provide measurement hooks in protocols?