Issues(1): L4S-Internet Coexistence

• Receiver cannot distinguish whether CE marks are L4S vs. RFC-3168 (Classic)
  • Fundamental confusion that underpins most of the L4S issues
  • Not compatible with RFC 4774 Option 3 (Friendly Coexistence)

• L4S transports assume CE marks are L4S signals - often untrue today
  • Significant middlebox deployments of RFC 3168
  • Alternative Backoff with ECN (RFC 8511) requires multiplicative decrease, L4S transports don’t do that.

• If L4S & conventional flows share a FIFO & AQM:
  • Conventional flows may suffer (badly),
  • Even though the FIFO & AQM comply with all applicable RFCs

• Safety, Compatibility, Coexistence - still problematic in L4S “running code”
Issues(2): Dual Queues and AQM

• Creates DoS (Denial-of-Service) vulnerability in some tunnels
  • Attacker advances replay protection window by sending low-latency traffic
  • Conventional traffic arrives after window has advanced, gets discarded

• Uncontrolled throughput bonus to traffic in low latency queue
  • Easily exploited – no enforced congestion control or required admission control
  • Diffserv PHB would likely require admission control (e.g., VOICE-ADMIT)

• AQM disadvantages fragmented and small-MTU traffic
  • Congestion marking algorithm biased against small packets

• DualQ AQM algorithm intolerant of bursty traffic
  • Bursty applications (e.g., real-time video) and links (e.g., WiFi) cause large reduction in goodput