DTN Reliability Considerations

Ed Birrane (chair hat off)

Edward.Birrane@jhuapl.edu

History

- RFC4838 commented on DTN Reliability
  - DTN basic service being unacknowledged, prioritized, best-effort
  - Enhanced reliability through end-to-end acknowledge and custody transfer
- Custody Transfer for Reliability
  - Mechanism to delegate retransmission to other nodes in the network
  - Conceptually, advancing retransmission along a path to a destination
- Changes from BPv6 to BPv7
  - Custody transfer mechanism removed in BPv7
  - BPv6 mechanism flawed
  - Sense that reliability was more than custody transfer
  - Custody transfer behavior could come back via extension block or CLA

Observation

- No single, end-to-end, formal definition of DTN reliability that
  - Is inclusive of components from sender to receiver
  - Differentiates the impact of default S&F and custodian retransmission
- Such a definition is achievable and necessary
  - Individual reliability statements exist (literature, CCSDS, elsewhere)
  - Work in reliability of underlay networks and convergence layer protocol
- Such a definition will help unify thoughts on:
  - Custody transfer mechanisms and signaling
  - Underlay and convergence layer protocol reliability
  - User service specifications
  - Application comfort with early data release

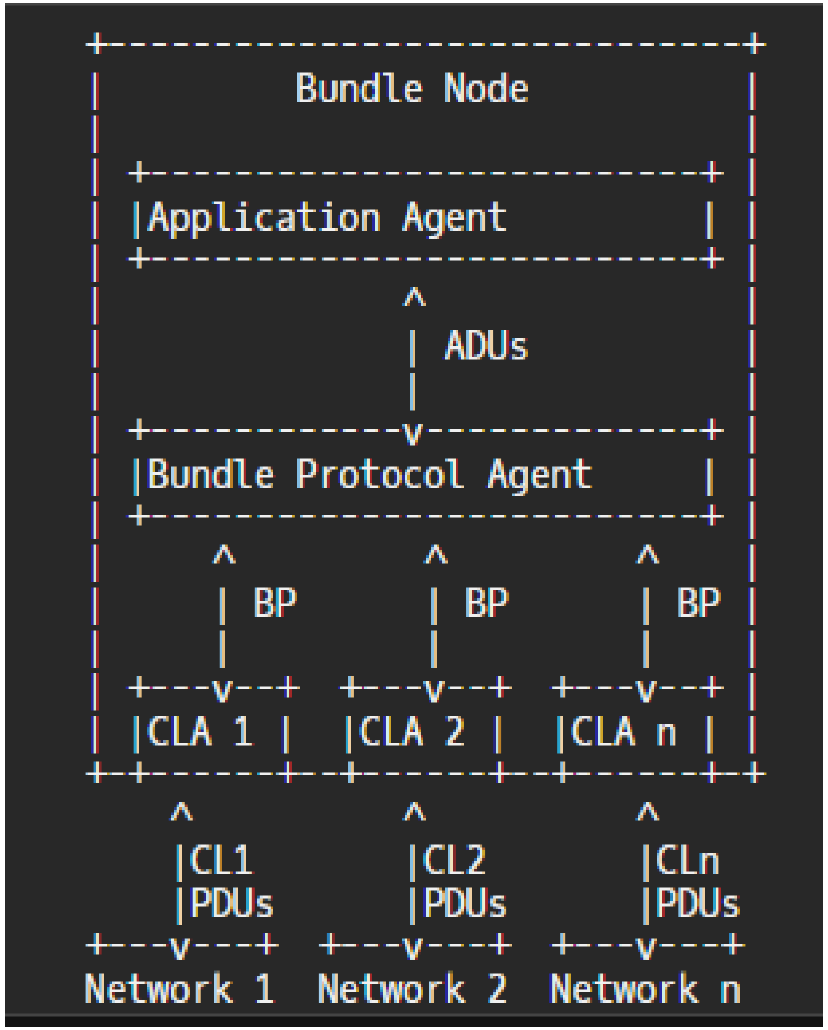
Recommendation

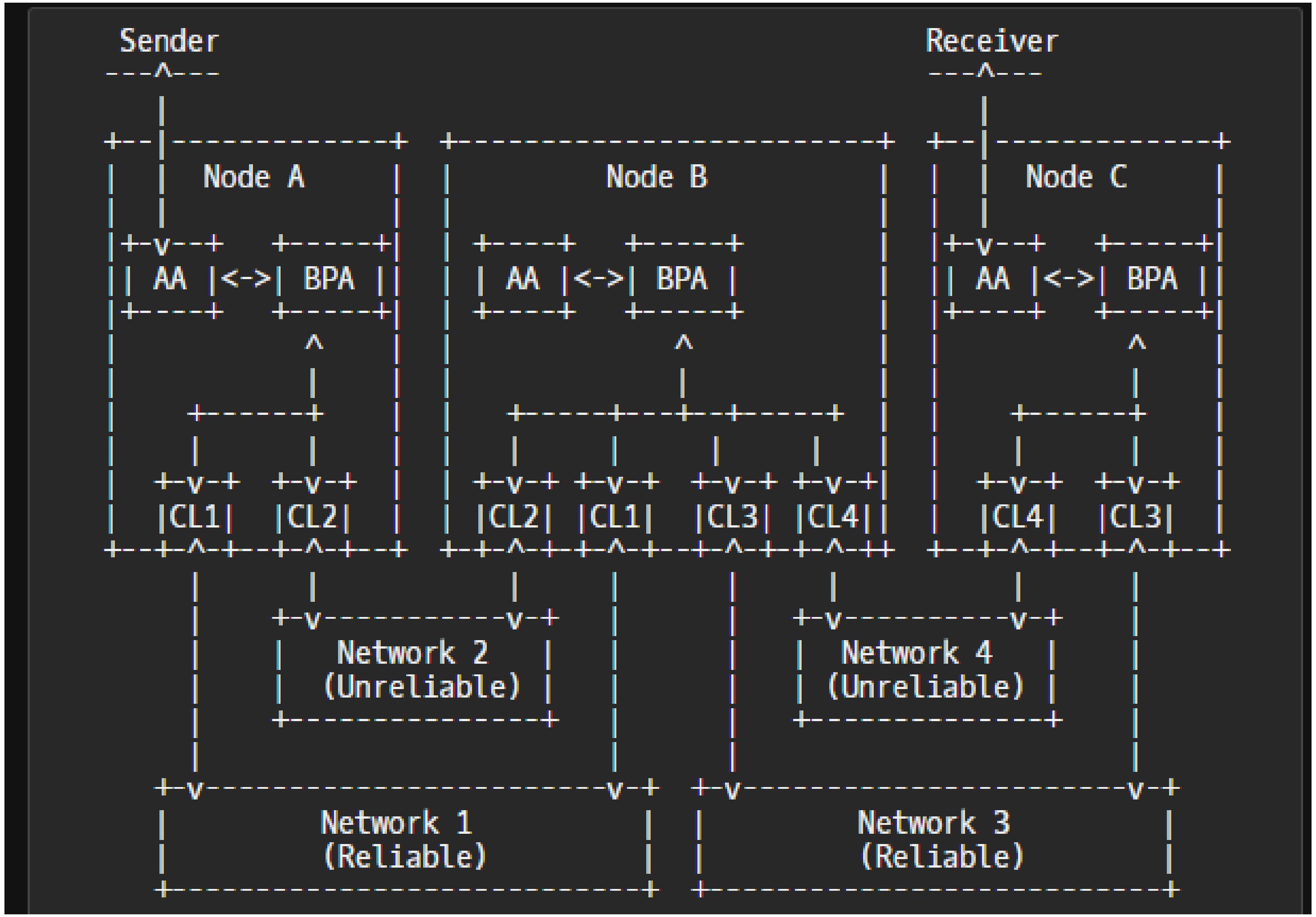
An informational RFC would go a long way to:

- Explain custody transfer as a network behavior
  - Networks define policies for retransmission and bundle storage
  - These policies do not need to be carried in-band in a bundle
    - Ex: whitelist accepted custodians
    - Ex: require minimum or maximum custodians in a given path
    - Ex: network segments connected with reliable underlays might not need custodians

- Define DTN reliability behaviors
  - Multiple “levels” of reliability that can be differentiated
  - Yield granularity for service specifications beyond “custody or not”
  - Signaling custodial transfer is a single piece of a reliability service

Start with a Sample Node and Network





Approach

- Fault analysis
  - What can go wrong and where
- Network User Indicators
  - What might users get to pre-negotiate or see in real time
- Reliability concepts and bundle layer definitions
  - How can we define reliability
- Reliability Mechanisms
  - What types of mechanisms exist to achieve this reliability
- Reliability Classes
  - How can we signal reliability as a class of service / network behavior?

Fault Analysis and User Indicators

- Fault analysis
  - What can go wrong where
    - Faults in the Application Agent, BPA, CLA, and underlays
    - Underlay faults include environmental faults
  - Focus on effects, not causes
    - “Bundle lost” can be due to underlay error, storage error, loss of node, etc…
    - Reduces complexity of fault analysis without impacting reliability statements
- Network User Indicators
  - Service specifications and agreements with network
  - Traffic acceptance/rejection notifications (per-bundle or per bundle flow)
  - Network delivery reporting (such as through report EIDs)

Reliability Concepts (at bundle layer)

- List network reliability concepts
  - Network reliability is extent to which you can… rely on the network
  - Combination of other attributes
    - Resiliency (range of tolerable operating conditions)
    - Availability (can network take user data)
    - Data Durability (can data be uncorrupted)
- Clarify unique definitions of concepts at the bundle layer
  - Ex: Resiliency does not mean recovery to a known nominal state
  - Ex: Availability means source node is online, not that end-to-end exists
  - Ex: Durability includes when the network is down (store/forward)

Reliability Mechanisms

- Acknowledgements
  - Application layer acknowledgements
  - Bundle layer acknowledgements
  - CLA/CLP acknowledgements

- Delegation
  - Underlayment trust
  - Application trust
  - Architecture

Reliability Classes (at the bundle layer)

- Class 0: No bundle layer reliability
  - Truly best effort - no requirement that data be stored at all
  - Beholden to mechanisms outside of bundle layer
- Class 1: Best Effort, Time-Variant, Store-and-Forward
  - Standard bundle-layer store and forward
  - Similar to best-effort, prioritized default service from RFC4838
- Class 2: Custodial Transfer (the network has custody)
  - Guaranteed storage for some type of data at some known custodian
  - Data can be removed when custody accepted by the network
- Class 3: Redundant Custodial Transfer
  - Network agrees to signal when multiple custodians have data.

Summary

Early work and comments appreciated!

- DTN Reliability
  - Is a function of services at the BP layer AND
    - Network architecture
    - Convergence layer protocols
    - Underlay capabilities
    - Application capabilities
- Custody transfer:
  - Is not a mechanism – it is a network behavior (and a reliability class)
  - Networks can provide that reliability class in a number of ways
- Define
  - Reliability classes
  - Standards to signal custodial acceptance by a BP Node
    - Might be used only at network edges – implementation dependent