



Summary of Technical Topics

Scott Burleigh
Jet Propulsion Laboratory
California Institute of Technology

23 July 2014

This research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. © 2014 California Institute of Technology. Government sponsorship acknowledged.



What We've Got Now

- Experimental RFCs developed by DTN Research Group
 - Bundle Protocol
 - 5050 BP specification
 - 6257 security protocol specification
 - Extension blocks: 6258 metadata, 6259 previous-hop
 - 6260 compressed bundle header encoding
 - 6693 probabilistic routing protocol
 - Convergence-layer protocols
 - Licklider Transmission Protocol: 5326 (specification), 5327 (security extensions)
 - 7122 UDP adapter
 - 7242 TCP adapter
- Informational RFCs
 - 4838 architecture
 - 5325 LTP motivation
 - 6256 self-delimiting numeric values
 - IANA registries: 6255, 7242

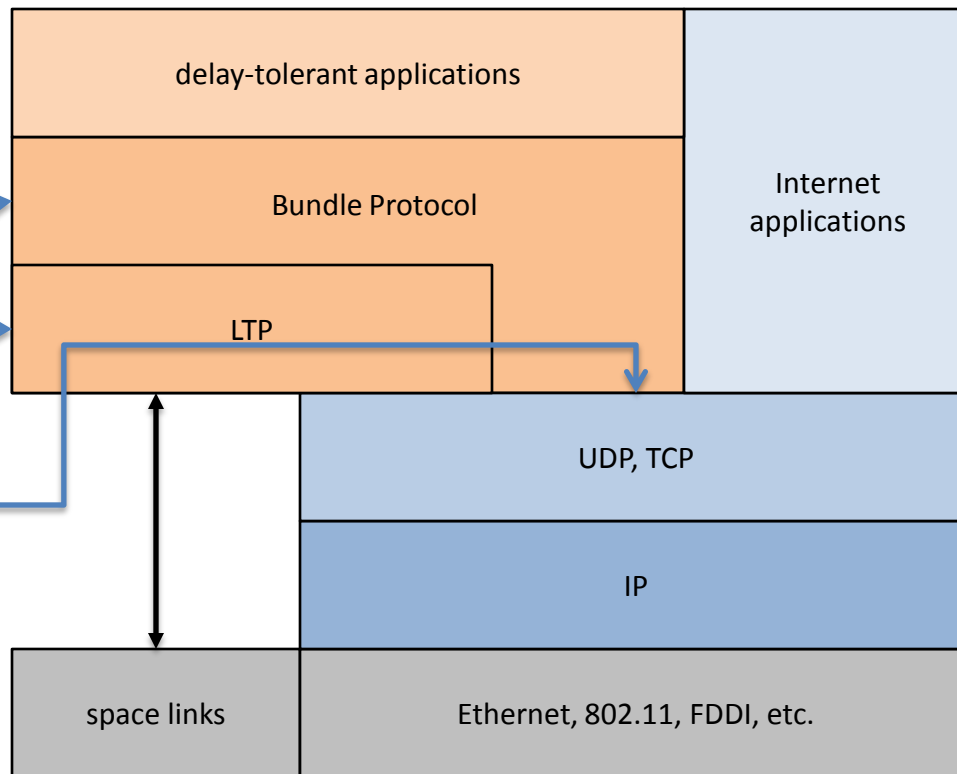


A Sample Stack

5050, 6257, 6258, 6259, 6260, 6693

5326, 5327

7122, 7242





Implementations

- **DTN2** reference implementation, open source on SourceForge, originally developed at UC Berkeley.
- **ION** (Interplanetary Overlay Network), developed at JPL for use in resource-constrained embedded systems, particularly spacecraft.
- **Postellation**, developed by Viagenie, packaged for easy installation and immediate trial by end-users, supports http/https browsing over dtn.
- **IBR-DTN**, developed at Technische Universität Braunschweig, designed to run on embedded systems using OpenWrt.
- **JDTN**, developed by Cisco, runs on any platform that supports Java; includes UIs for Android.
- **SCAMPI**, developed at Aalto University (Comnet), is also in Java; designed as a platform for opportunistic services.
- **Bytewalla**, developed at KTH in Stockholm and also in Java, aims at connecting African rural villages using Android phones with delay-tolerant networking.
- Others less widely used.



What We've Done With DTN So Far

- Deep Impact Network experiment in deep space in 2008: operating a DTN router 81 light seconds from Earth.
- European N4C (Networking for Communications Challenged Communities) program 2008-2011:
 - Testbed in Lapland, Sweden
 - Testbed in Kočevje, Slovenia
 - Experiments in Galway, Ireland, and in the south of Spain
- Too many University experiments to list.
- Continuous pilot science data delivery from the International Space Station since 2009.
 - Permanent operations on Joint Station LAN will begin in 2015.



What's Wrong With What We've Got?

- The specifications are all experimental.
 - Excellent as a level playing field for a wide range of research studies.
 - But can be perceived as too risky a foundation for investment in commercial products.
- Not all facilities required for large-scale operation are complete yet, e.g., security key distribution, network management.
- The original protocol designs were experimental, and they were not perfect. We've learned a few things.



“A Bundle of Problems” (Wood et al)

- No checksums on bundle metadata or payload.
- Requirement for accurate clocks at all nodes, to support bundle expiration at end of time-to-live.
- Many possible convergence-layer adapters – too much work to define them all.
- Reactive fragmentation needs to be reconciled with security.
- No definition of naming schemes [*prior to RFC 6260*].
- No standard routing methods [*prior to RFC 6693*].
- No network management protocol.
- QoS: priorities undefined, no flow labels.
- Headers are too bulky for small bundles, e.g., sensor nets, streaming voice.
- Complexity: self-delimited numeric values, dictionary. Hard to implement.
- No security key management, no firewalls.
- No content identification [*prior to RFC 6260*].



Further Issues

- Most BP operations are performed with reference to nodes rather than endpoints, but there is no notion of node identifier in the specifications.
- Block mutability and the dictionary mechanism make security canonicalization difficult.
- Security protocol is very complex, reportedly includes some variations that can't be implemented.
- No guidance on how to deal with routes that are temporarily unavailable.
- Still no consensus on how to do multicast.



All the same...

- Despite these deficiencies, the DTN architecture has already had significant impact.
- For example, the Inter Operation Plenary of national space agencies has selected DTN as the basis for the Solar System Internetwork architecture that will support flight missions over the coming decades.
- This is not an Internet application of DTN, but it does demonstrate consensus that DTN is an engineering success.
- Deep space is in some ways a more challenging communication environment than Earth's surface. If DTN works there, it will work here.



Near-Term Work Items (1 of 5)

- Update the Bundle Protocol; proposed revisions posted 6 June 2014 as [draft-burleigh-bpv7-00](#).
 - Incorporate the Compressed Bundle Header Encoding [[RFC 6260](#)] concepts into the base specification: nodes are explicitly identified by node numbers, and operations that pertain to nodes are described in terms of node numbers rather than endpoint IDs.
 - Restructure the primary block, making it immutable. Add CRC, as long advocated by Lloyd Wood. Remove the dictionary.
 - In the course of making the primary block immutable, move current custodian to an extension block. (Possibly multiple occurrences of this block, potentially supporting the MITRE idea of multiple concurrent custodians, from several years ago.) Define that block within the BP spec, as well as other extension blocks identified in the spec.



Near-Term Work Items (2 of 5)

- (Continuing)
 - Incorporate "Extended Class of Service" features (incl. flow labels) into the primary block. Ref. [draft-irtf-dtnrg-ecos-05](#) posted 1 July 2013.
 - Add optional Payload CRC extension block. Ref. [draft-eddy-dtnrg-checksum-00](#) posted 14 August 2007.
 - Incorporate basic ("imc") multicast into the BP spec. Add another administrative record, Multicast Petition. Ref. [draft-burleigh-dtnrg-imc-00](#) posted 7 November 2012.
 - Add Destination EID extension block for destinations that can't be expressed in "ipn"-scheme and "imc"-scheme URIs.
 - Add the notion of "embargoes", i.e., what do you do when a route unexpectedly goes bad for a while? Add another extension block (Forwarding Anomaly) and an administrative record (Reopen Signal).



Near-Term Work Items (3 of 5)

- (Continuing)
 - Add block ID number to canonical block format, to support streamlined Bundle Security Protocol discussed below.
 - Add bundle age extension block. Ref. [draft-irtf-dtnrg-bundle-age-block-01](#) posted 25 October 2010.
 - Two additional extension blocks: previous node number (superseding RFC 6259), hop count (ref. [draft-ellard-dtnrg-reltime-htl-00](#) posted 24 February 2010).
 - Clean up a conflict between fragmentation and custody transfer identified by Ed Birrane.
 - Remove unused "DTN time" values from administrative records.
 - Explicitly note that CL protocols are supposed to discard data that they find to have been corrupted.



Near-Term Work Items (4 of 5)

- Streamlined Bundle Security Protocol; BSP revisions posted 27 May 2014 as [draft-irtf-dtnrg-sbsp-01](#).
 - Simplifies structure, eliminating Extension Security Block and generalizing PIB and PCB to Block Integrity Block and Block Confidentiality Block.
 - Decouples security measures from routing mechanisms.
 - Increases flexibility in security policy and ciphersuite selection.
 - Excludes explicit security measures for fragmentary payloads, simplifying bundle fragmentation and reassembly.
 - Block ID number, together with elimination of nested security operations, removes constraint on maintaining block sequence throughout path.
 - Block immutability simplifies canonicalization.



Near-Term Work Items (5 of 5)

- Bundle-in-Bundle Encapsulation Protocol, posted 26 March 2013 as [draft-irtf-burleigh-bibe-00](#).
 - Enables control over routing where required by security policy.
 - Enables security operation nesting and explicit security for fragmentary bundles, where needed.
- Registry for service identifiers (as adapted from [RFC 6260](#)).
- Network Management Protocol:
 - Current draft specification posted 1 October 2013 as [draft-irtf-dtnrg-dtnmp-00](#), initial implementation available in ION.
 - Earlier work: [draft-irtf-dtnrg-ding-network-management-02](#), [draft-ivancic-dtnrg-network-management-reqs-00](#).



Longer-Term Work Items

- Security Key Management Protocol.
 - Requirements identified in draft-farrell-dtnrg-km-00 (18 June 2007) and draft-templin-dtnskmps-00 (12 March 2014).
 - Prototype implementation developed at JPL is under evaluation at Boeing Co. and Harvard University.
- Generalized solution to routing in DTNs.
 - P_{Ro}PHET (RFC 6693).
 - Contact Graph Routing (draft-burleigh-dtnrg-cgr, 8 July 2010).
- Standards for opportunistic forwarding based on node and contact discovery – ref. draft-irtf-dtnrg-ipnd-02, 8 November 2012.



Summary

- There's plenty for a DTN Working Group to do in the near term, but most of it is well understood and – in many cases – already prototyped.
- There are still a few long-term open work items that must be addressed to support broad deployment.