The Delay-Disruption Tolerant Working Group (DTNWG)

A brief history and overview of DTN and the Bundle Protocol (BPv7)

Edward J. Birrane, Ph.D.
Johns Hopkins University,
Applied Physics Laboratory (JHU/APL)
Edward.Birrane@jhuapl.edu

Rick Taylor
Airbus Defence & Space
Rick.taylor@airbus.com

Overview

- A Brief History of Delay-Tolerant Networking
- DTN Ecosystem and the IETF
- The Bundle Protocol (Version 7)
- A Little More About Security
- A NASA Case Study

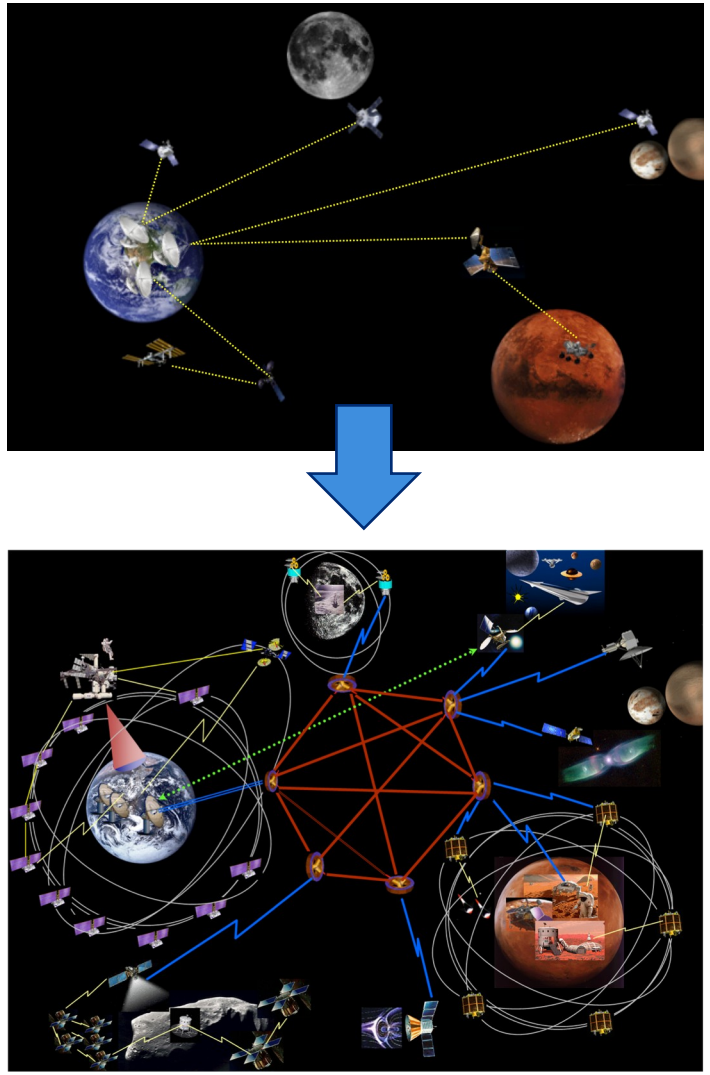
A Brief History of Delay-Tolerant Networking

https://www.nasa.gov/directorates/heo/scan/engineering/technology/disruption_tolerant_networking_history
https://www.nasa.gov/directorates/heo/scan/engineering/technology/disruption_tolerant_networking

It Came From Outer Space…

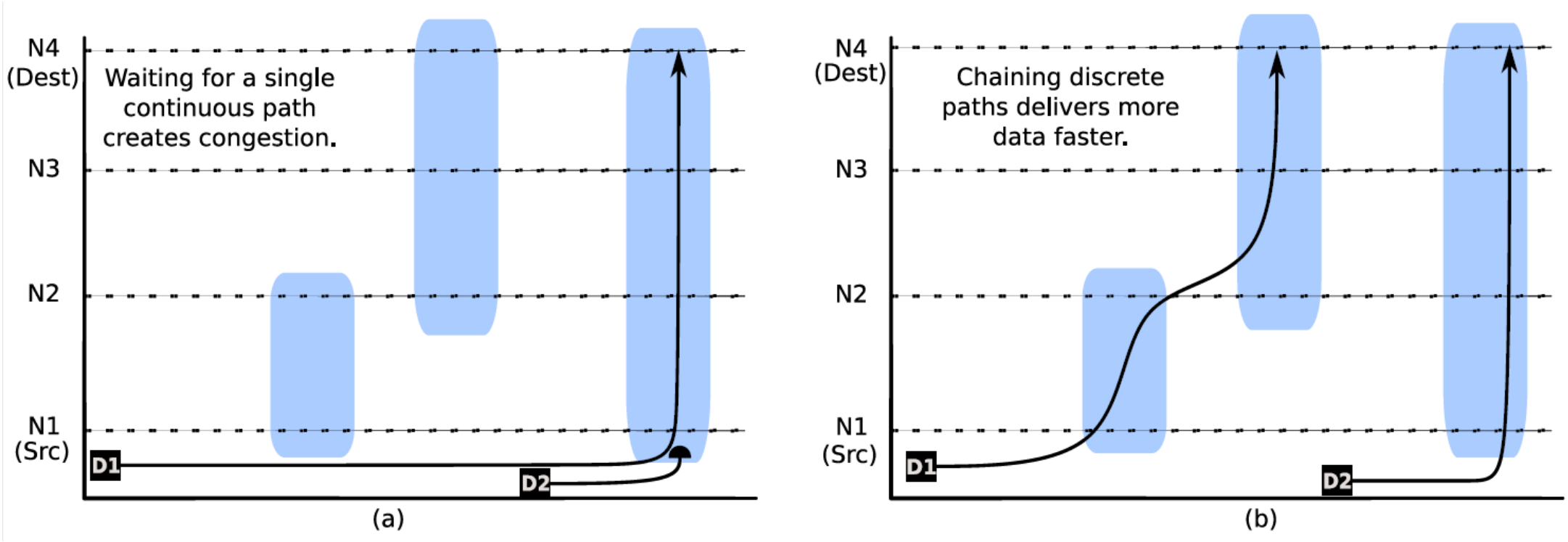
What does an interplanetary network look like?

- Store and Forward Data Exchange
  - **Do not** assume a path exists all at once.
  - **Do not** assume endpoints remember things for you.
  - **Do not** retransmit from the source. Inchworm through the network.
  - **Do** store data for milliseconds… or days.
  - **Do** carry all data and metadata in the same message.
- End-to-end Security
  - **Do not** rely solely on physical layer security.
  - **Do** secure different parts of a packet separately.
  - **Do** optimize for security at rest.
- Autonomy as Network Management
  - **Do not** assume an operator in the loop.
  - **Do** incorporate autonomy and automation. Operator “on” the loop.
  - **Do** push information proactively into the network.
  - **Do** be compatible with terrestrial management approaches.
- Routing
  - **Do** adjust to time-variant topologies.



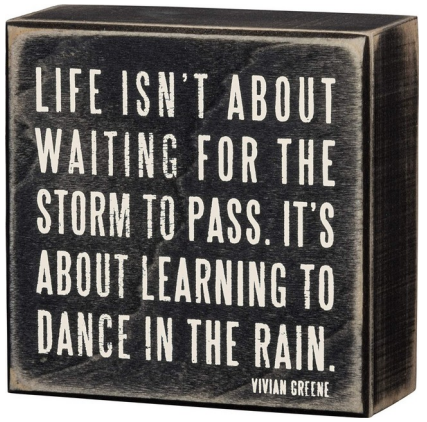
What Makes These Problems Different? Delays.

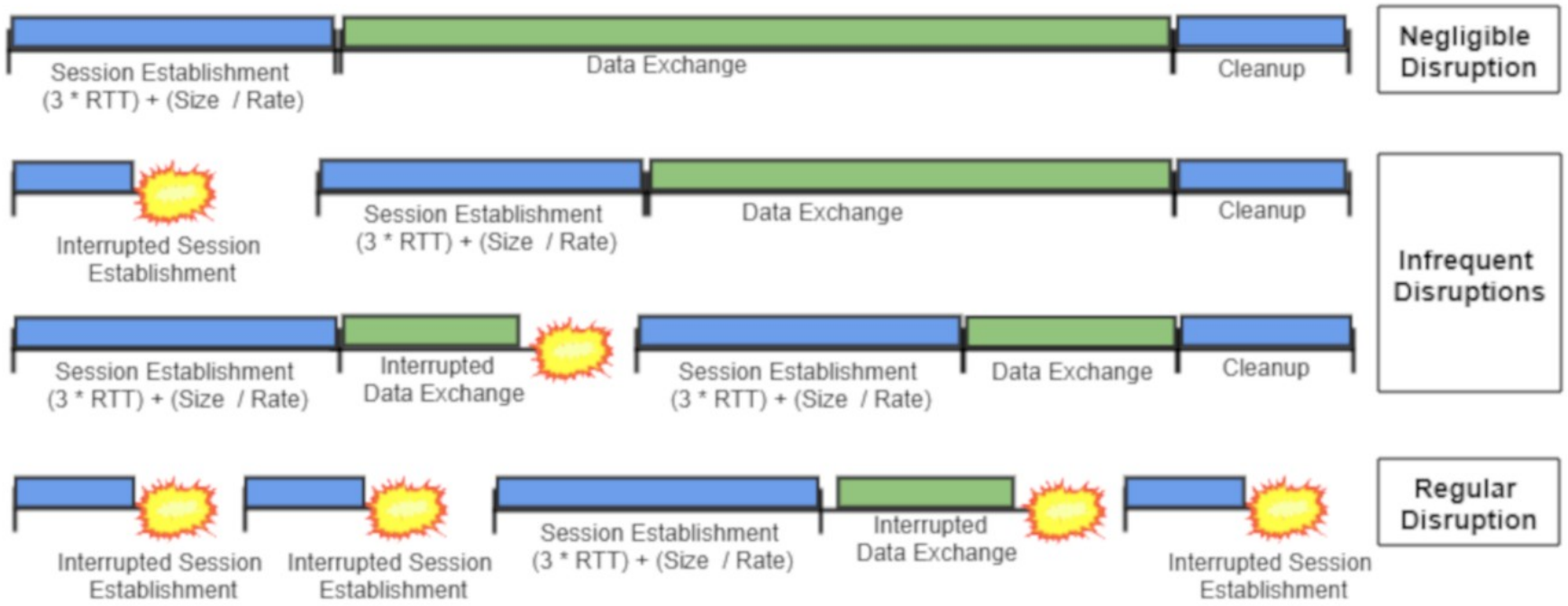
Don’t wait for an end-to-end path.



What Makes These Problems Different? Disruptions.

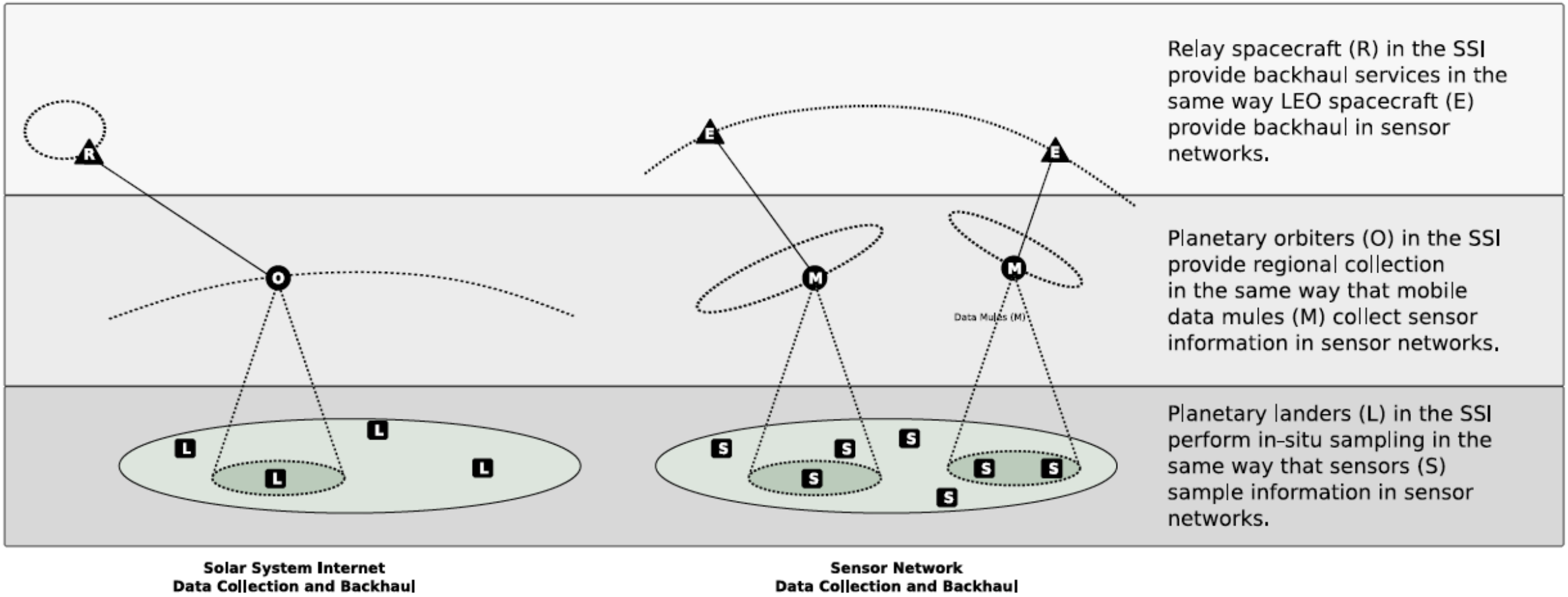
Don’t wait for things to get better.





But the feature sets are similar to nearer-Earth scenarios…

Like near-Earth sensor networks.

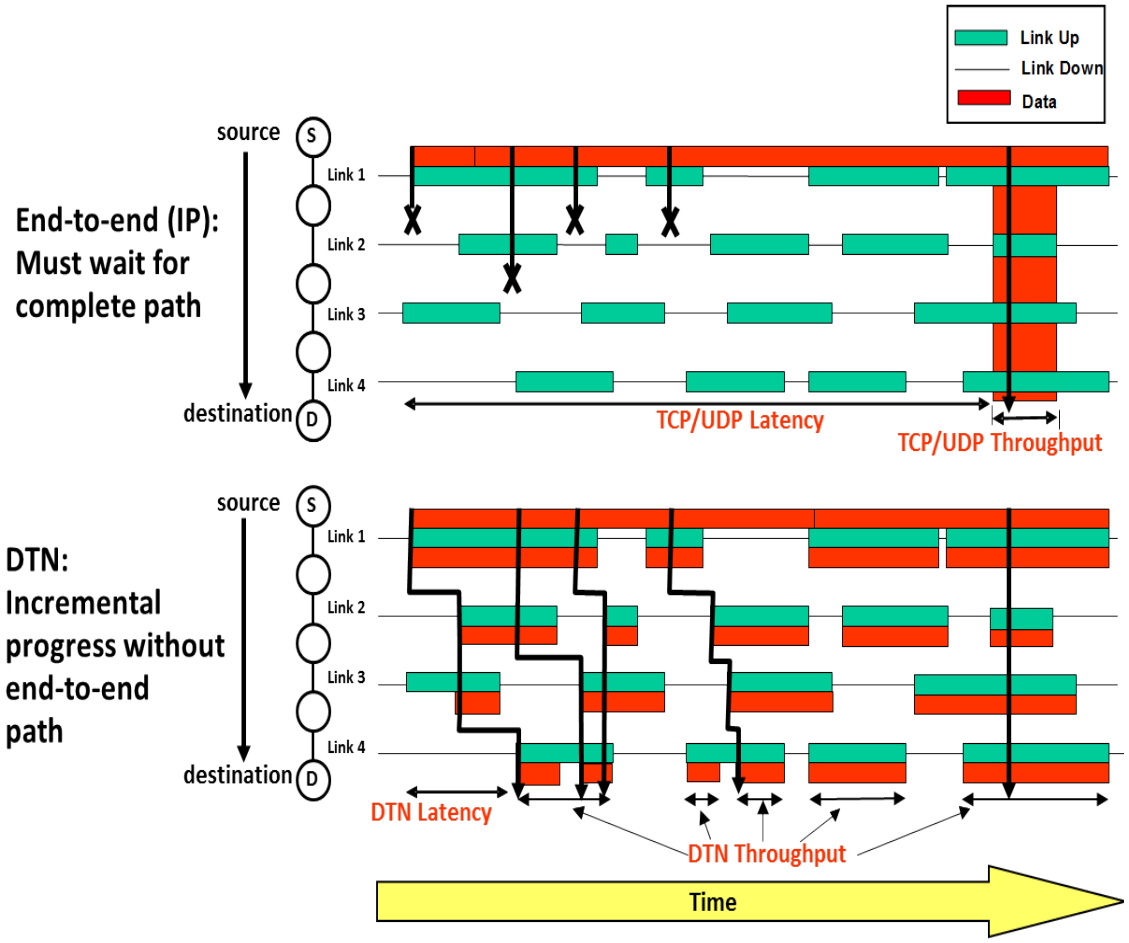


The DTN Ecosystem and the IETF

DTN features useful even in resourced networks

Modern networks encounter problems similar to high delays and frequent disruptions.

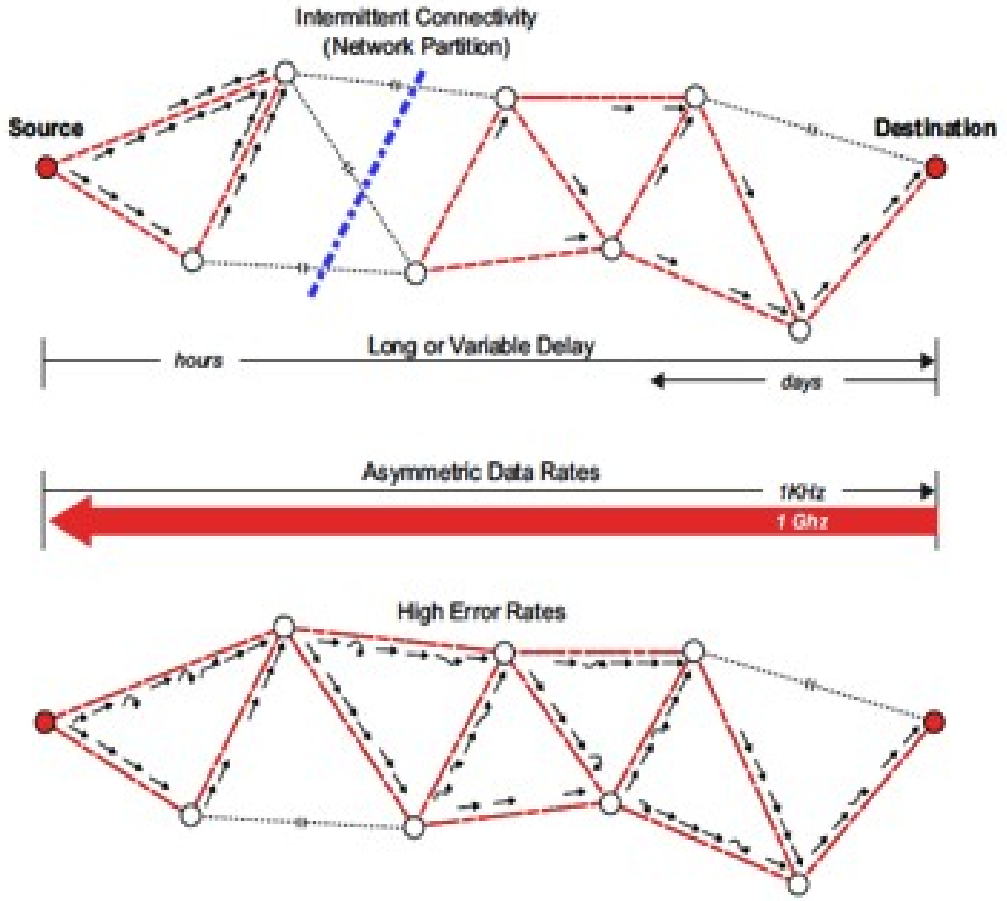
- What's useful on the Internet today?
  - Content delivery networks (caching)
  - Data subscriptions (push mechanisms)
  - Autonomic computing (rules/automation)
  - Stateless data (RESTful interfaces)
- We do not have infinite access to bandwidth.
  - High priority data delays low-priority data.
  - Chatty protocols are clogging links.
  - Untrusted infrastructure may as well not exist.
- Assuming infinite bandwidth leads to problems.
  - Lots of state information at endpoints.
  - Lots of bandwidth used for "real time updates"
  - Dropping low-priority data clogs the network…
    - Re-transmitted again to be dropped again.



What kind of features do we want?

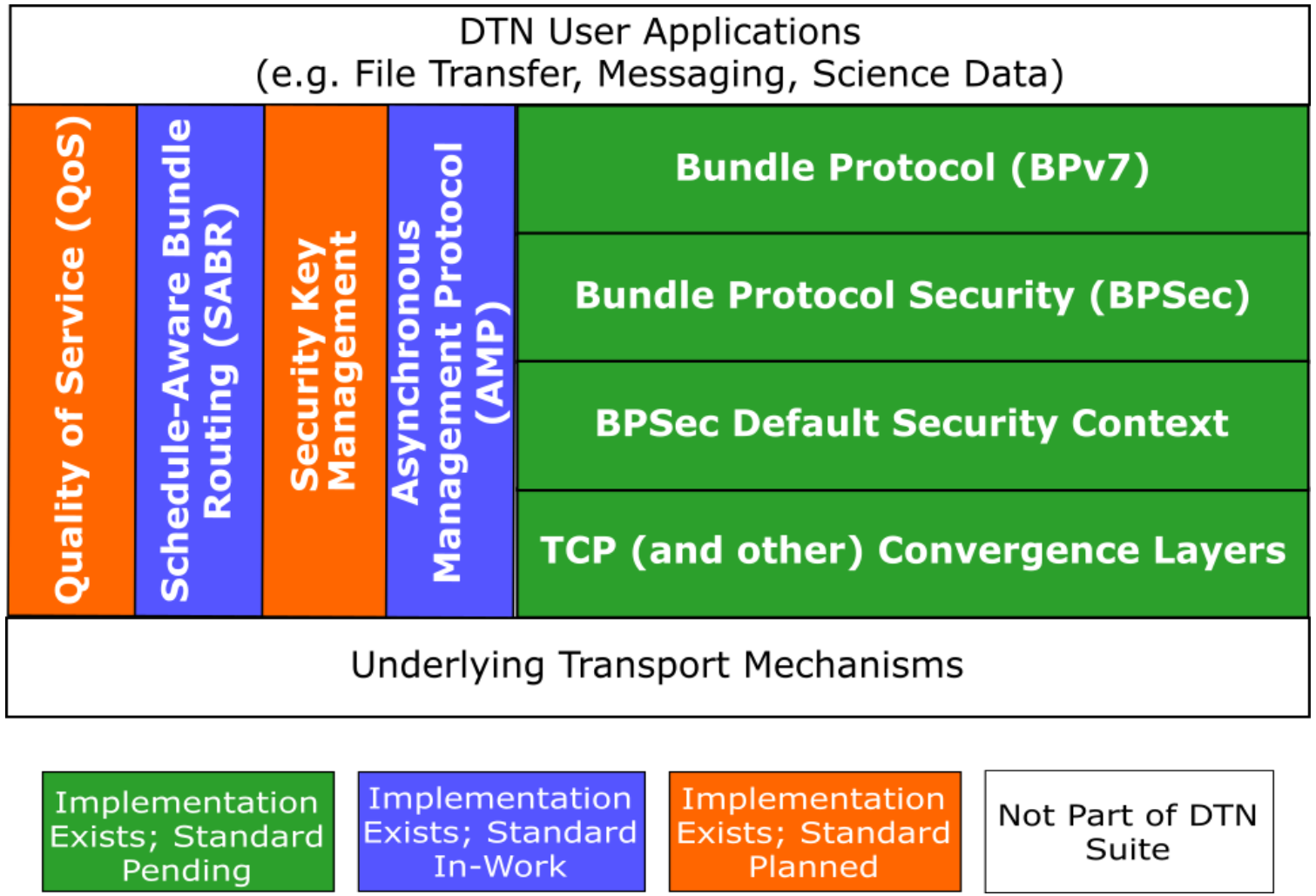
"Challenged" includes predictably disrupted, randomly degraded, and intentionally contested.

- You can send data without knowing if the destination is connected or on-line.
- Re-transmissions don't have to start over from the beginning.
- You can "bundle" payloads and annotative data together to avoid synchronization problems later.
- Endpoints do not need to remember sessions or special states. DTN bundles carry everything they need with them.
- Familiar features! Similar to text messaging and e-mail.
- But as a standard networking protocol – every application gets these benefits. No more point solutions.



Delay/Disruption Tolerant Networking (DTN) gives us new tools

DTN is a family of protocols that can be applied in whole or in part.



The problem went from NASA to DARPA to CCSDS to IETF

First the IRTF and then the IETF.

The **DTNRG** was formed in 2002.

"Observation that a noninteractive, asynchronous form of messaging service, able to operate over diverse types of networks, would be useful for several networks currently in use or being contemplated."

-https://irtf.org/concluded/dtnrg

Produced 14 RFCs, notably:

- *RFC4838* DTN Architecture
- *RFC5050* BPv6
- *RFC6257* Bundle Security Protocol
- *RFC7242* TCP Convergence Layer

The **DTNWG** was formed in 2014, IETF 91

Current Major Work Items

- Update RFC5050
- Update RFC6257
- Provide Convergence Layer RFCs

Documents in RFC Editors Queue

- *draft-ietf-dtn-bpbis-31* BPv7
- *draft-ietf-dtn-bpsec-27* BPv7 Security
- *draft-ietf-dtn-tcpclv4-26* TCP CL

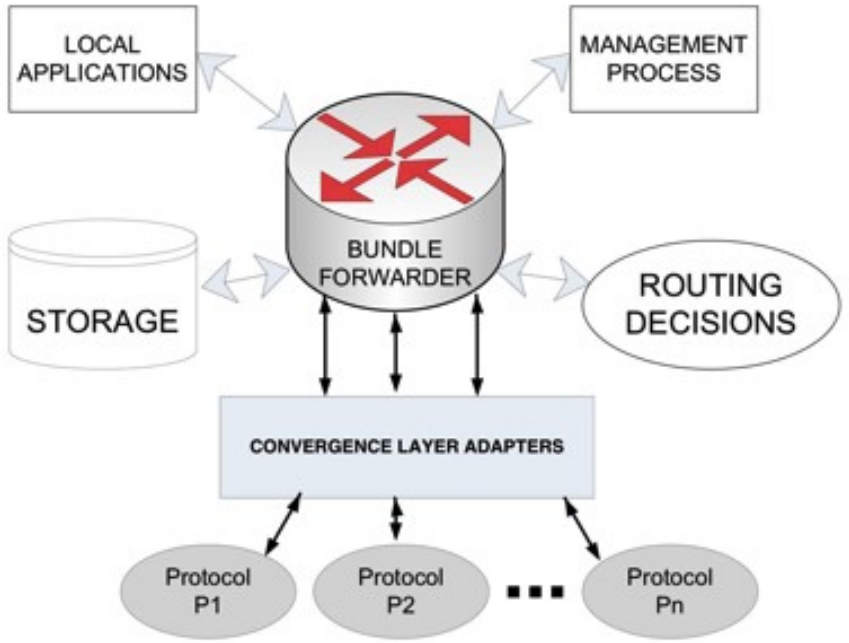
Documents in AD Evaluation

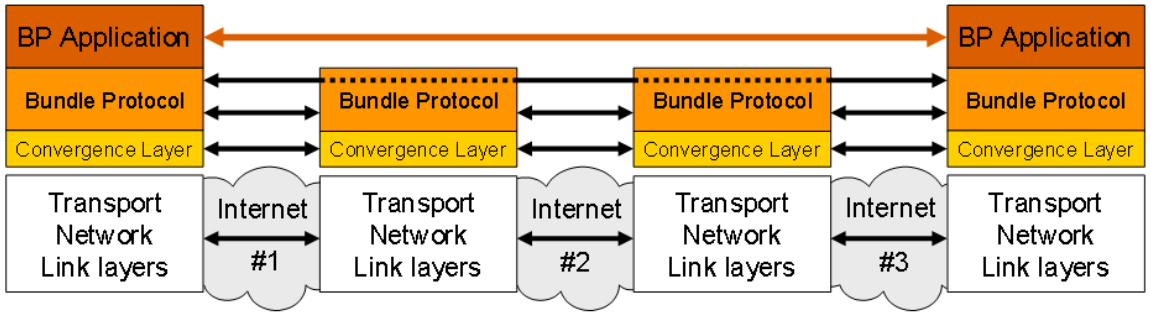
- draft-ietf-dtn-bpsec-default-sc-02

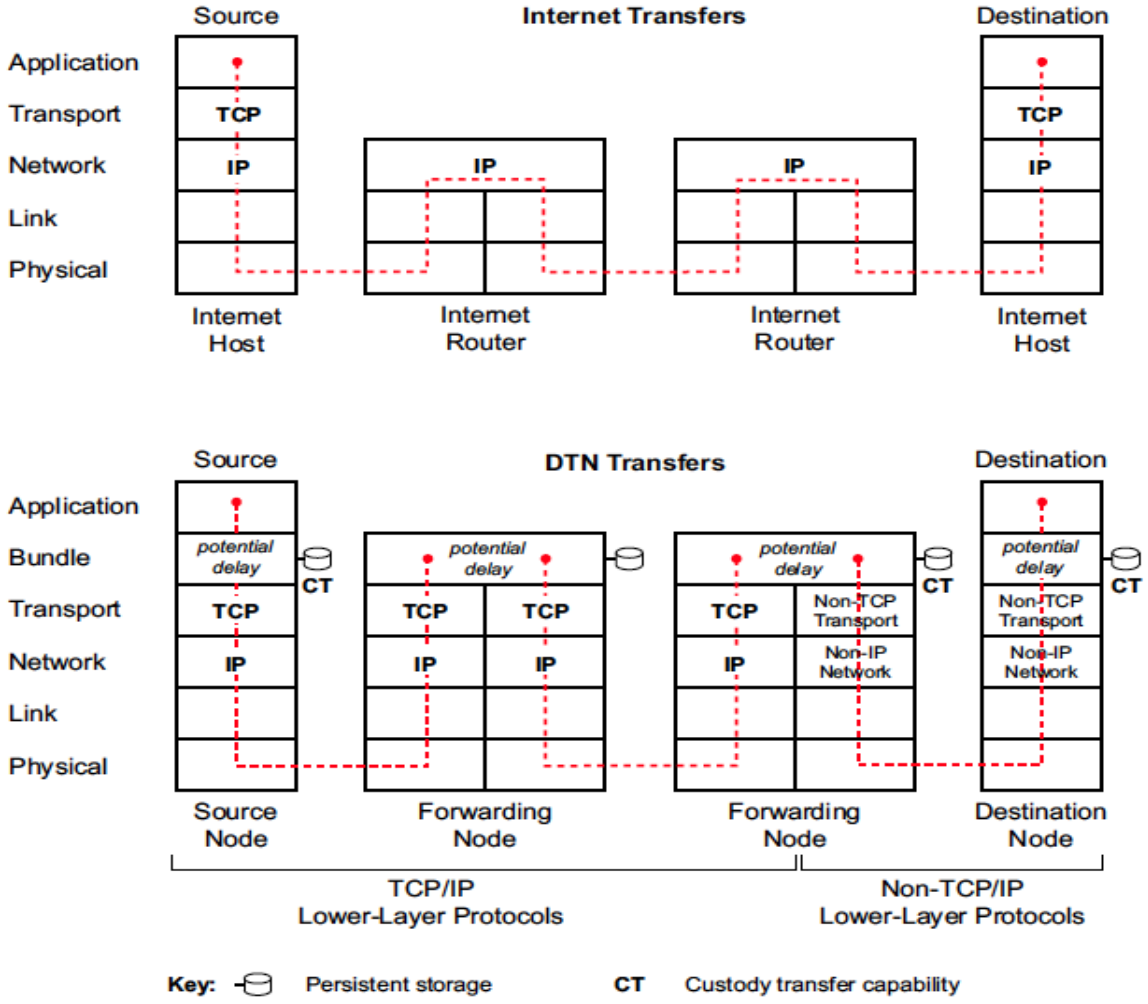
DTNWG working on a milestone update, IETF 110

The Bundle Protocol (Version 7)

Where does the Bundle Protocol "Live"?

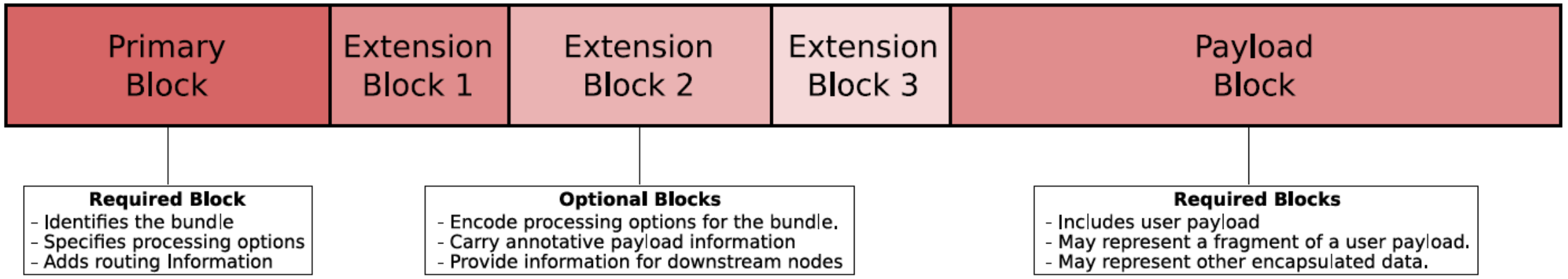






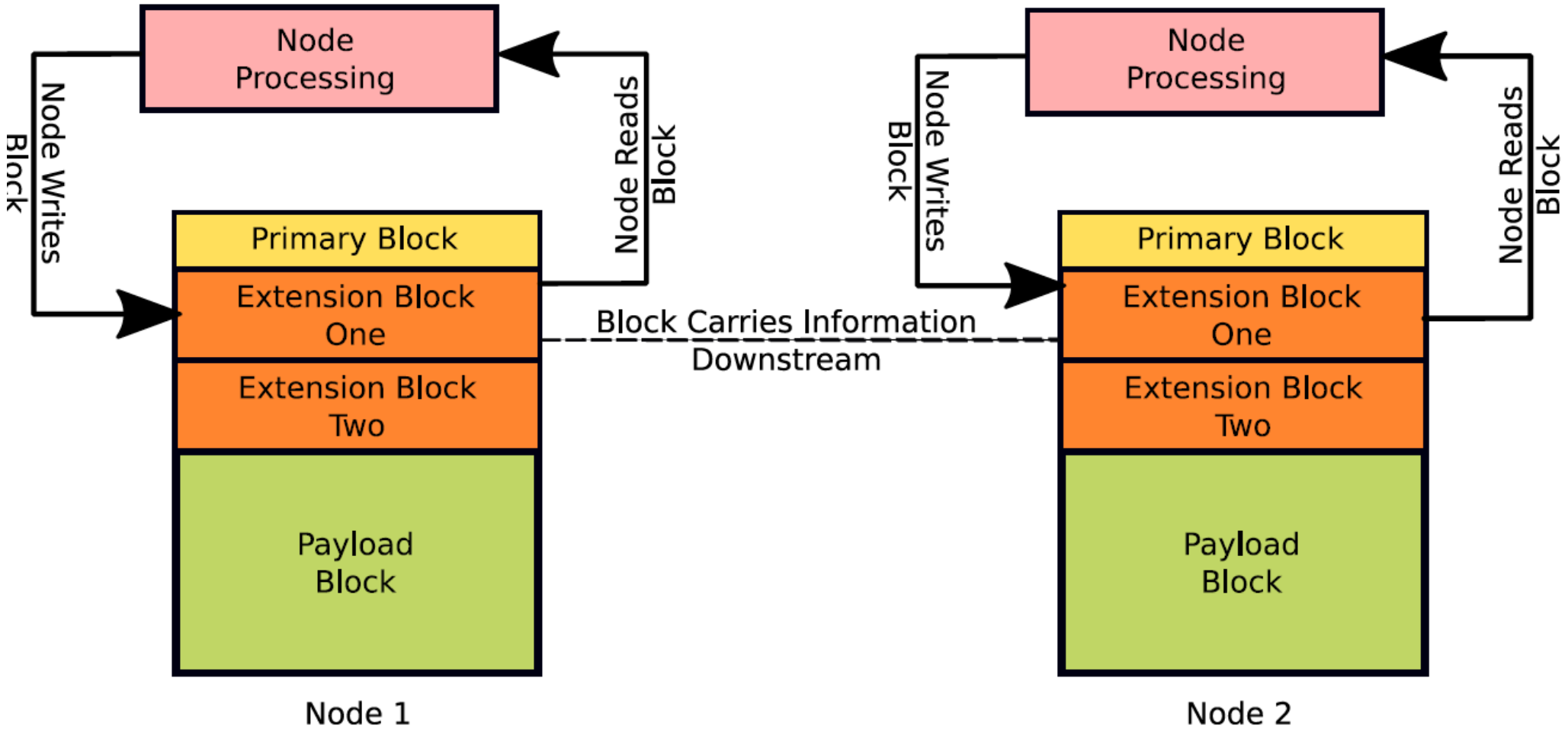
The Bundle Protocol Self-Extension Mechanism

Nodes in a network add extensions over the life of the “bundle”.



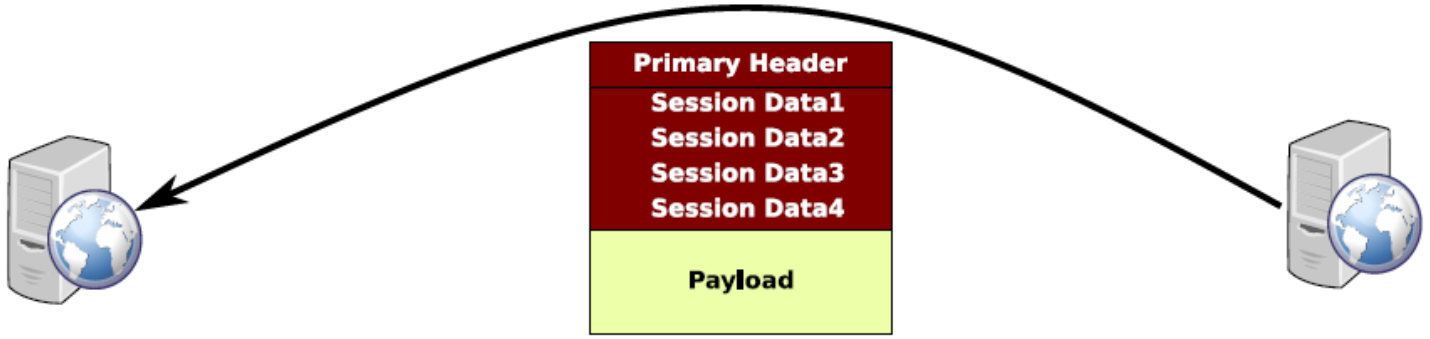
Bundle Extensions Add Processing In the Network

You can implement per-message processing as needed.

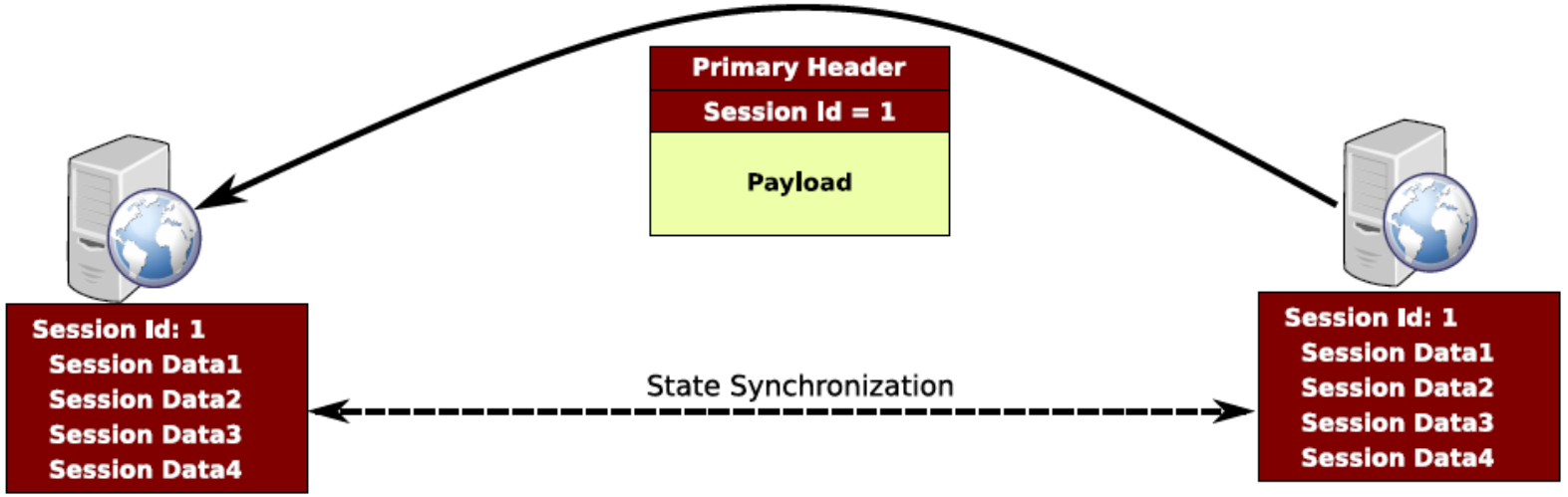


BP Extensions can carry end-to-end information

Less traffic spent maintaining sessions in contested environments.



Without shared state at message endpoints, individual messages must carry important annotative information.



With shared state at message endpoints, individual messages can reference this information to reduce message overhead.

Bundle Protocol Blocks

A few extension block types have been standardized

- **Required Blocks**
  - Primary Block
    - Immutable Header
    - Source/Destination
  - Payload Block
    - User payload
    - Last Block in a bundle
- **Extension Block Format**
  - Block Type
  - Unique Identifier
  - Block processing flags
  - Optional CRC
  - Block-type-specific fields
- **Transport-Focused Blocks**
  - Previous Node Block
    - The ID of the last transmitter of the bundle.
  - Bundle Age Block
    - Milliseconds between bundle creation and last forwarding of the bundle.
  - Hop Count Block
    - Carries an updated hop count and a hop limit.
- **Security Blocks**
  - Block Integrity Block
    - Carry integrity results for other blocks
  - Block Confidentiality Block
    - Encrypt other blocks
    - Provide authentication
  - *More on these blocks later*

A Little More About Security

BPSec: Design Decisions

- Block-Level Granularity
  - Security services applied to blocks, not bundles.
    - *Sign extension block 1.*
    - *Encrypt payload block*
- Multiple Security Sources
  - BPAs can apply security to both transmitted and forwarded bundles.
    - *Source adds an integrity signature to the payload. Gateway node adds encryption.*
- Mixed Security Policy
  - Waypoints must pass integrity-protected block without the keys to verify the integrity.
  - Waypoints may add security services en-route.
- User-Selected cipher suites
  - Encoding of cipher suite identifiers and parameters
  - Different networks will have different security requirements.
  - A bit like “Extensible Authentication Protocol” (EAP) in this regard.
- Deterministic Processing
  - Specific behavior when fragmenting PDUs.
    - *Encapsulate a fragment in a new bundle if it needs security services.*
  - Precise order of operations for confidentiality and integrity services.
  - Ambiguous processing points captured in required policy considerations.

BPSec: Services designed as blocks

- The Block Integrity Block (BIB)
  - Plain-Text Integrity only.
  - Can sign multiple blocks at once.
  - Some Constraints
    - Cannot target another BIB or a BCB
- The Block Confidentiality Block (BCB)
  - Plain-text Confidentiality
  - Cipher-Text Integrity
  - Constraints
    - Cannot target the primary block or other BCB.
    - Must use AEAD Cipher Suite
  - Operation
    - Contents of each target block replaced by cipher text.
    - Any overflow cipher text or other results stored in security results in the BCB.

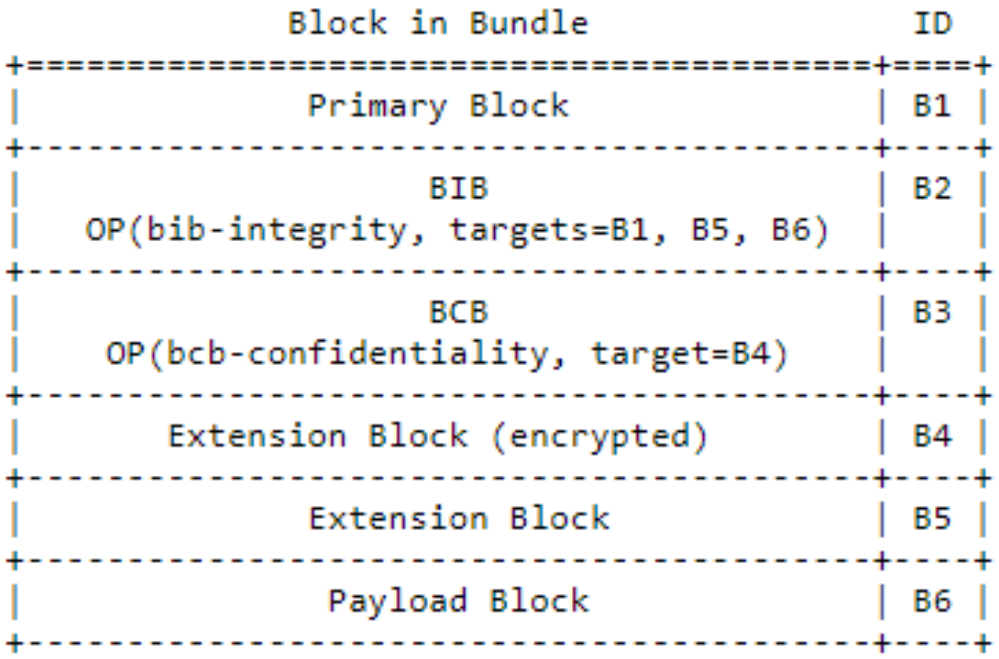


Figure 3: Security at Bundle Creation

https://tools.ietf.org/html/draft-ietf-dtn-bpsec-27#section-3.11

BPSec: Security Considerations

- Focus on MitM Attacks
  - Natural issue with store-and-forward protocols and imprecise timing.
- Eavesdropping
  - Time-to-Live and cipher suite selection must be appropriate for long-lived data.
- Modification
  - Block removal cannot be detected in-band.
  - Policy must set expectations out-of-band and before secure exchange.
  - BIB alone can be subject to signature substitution.
- Topology
  - Special case of modification applied to routing.
  - Some security patterns may be adopted to obscure primary header information.
- Message Injection
  - Cipher suites such as those using counter-based modes may resist replay attacks.

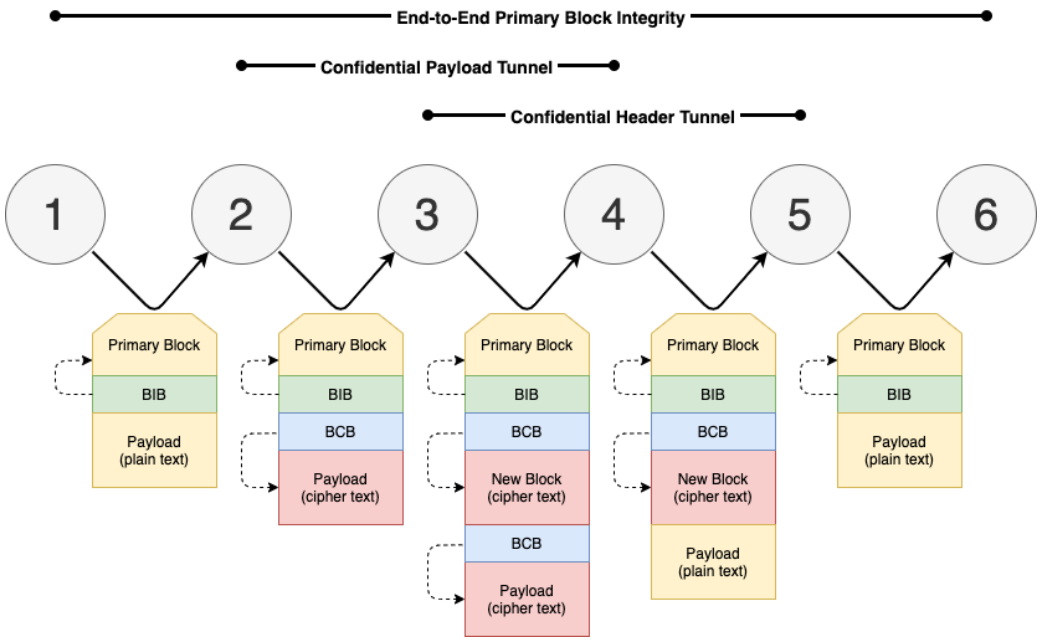
BPSec: When to Use It

- Alternatives to BPSec
  - No Network Security Protocol
    - Payloads given to the network layer already secured.
    - No need to secure anything other than the payload.
  - Internet Security Mechanisms (IPSec, TLS)
    - Using IP in a non-challenged network.

- Why use BPSec?
  - Secure data at rest.
    - Bundles remain encrypted while at rest at BPAs.
  - Security properties change en-route
    - Such as our gateway example above.
  - Different security levels within a single PDU
    - In challenged networks, PDUs need to carry annotative information with them.

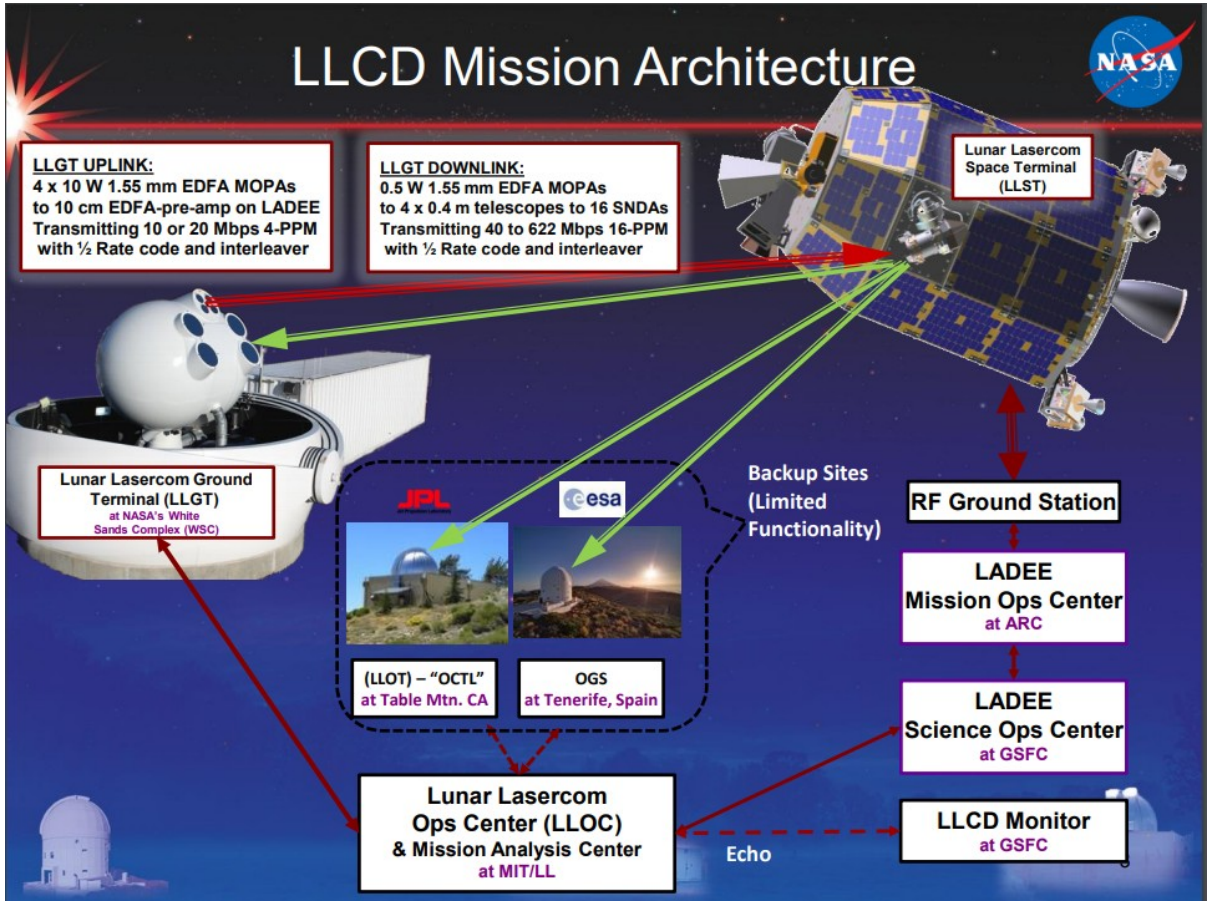
- Efficiency requires compact encodings
  - *Alternate encodings (e.g., CMS) might add too much processing and bandwidth overhead.*

- Multiple Security Tunnels
  - *Routing through various security endpoints.*



NASA Case Study: Lunar optical comm

http://ipnsig.org/wp-content/uploads/2014/02/LLCD-DTN-Demonstration-IPNSIG-Final.pdf



The experiment:

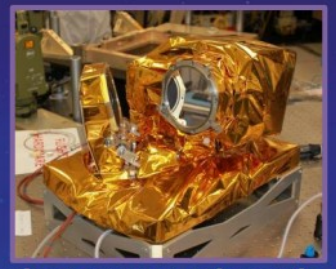
Comparing RF and Optical: *Equivalent Isotropic Radiated Power*

NASA Deep Space Network
- 34-m antenna
- S-band (~2-2.3 GHz)
- 20-kW transmit power

→ EIRP = 8.3 GW!

Lunar Lasercom Space Terminal
- 10-cm space terminal
- Optical (1550 nm, or 200,000 GHz)
- 0.5-W transmit power

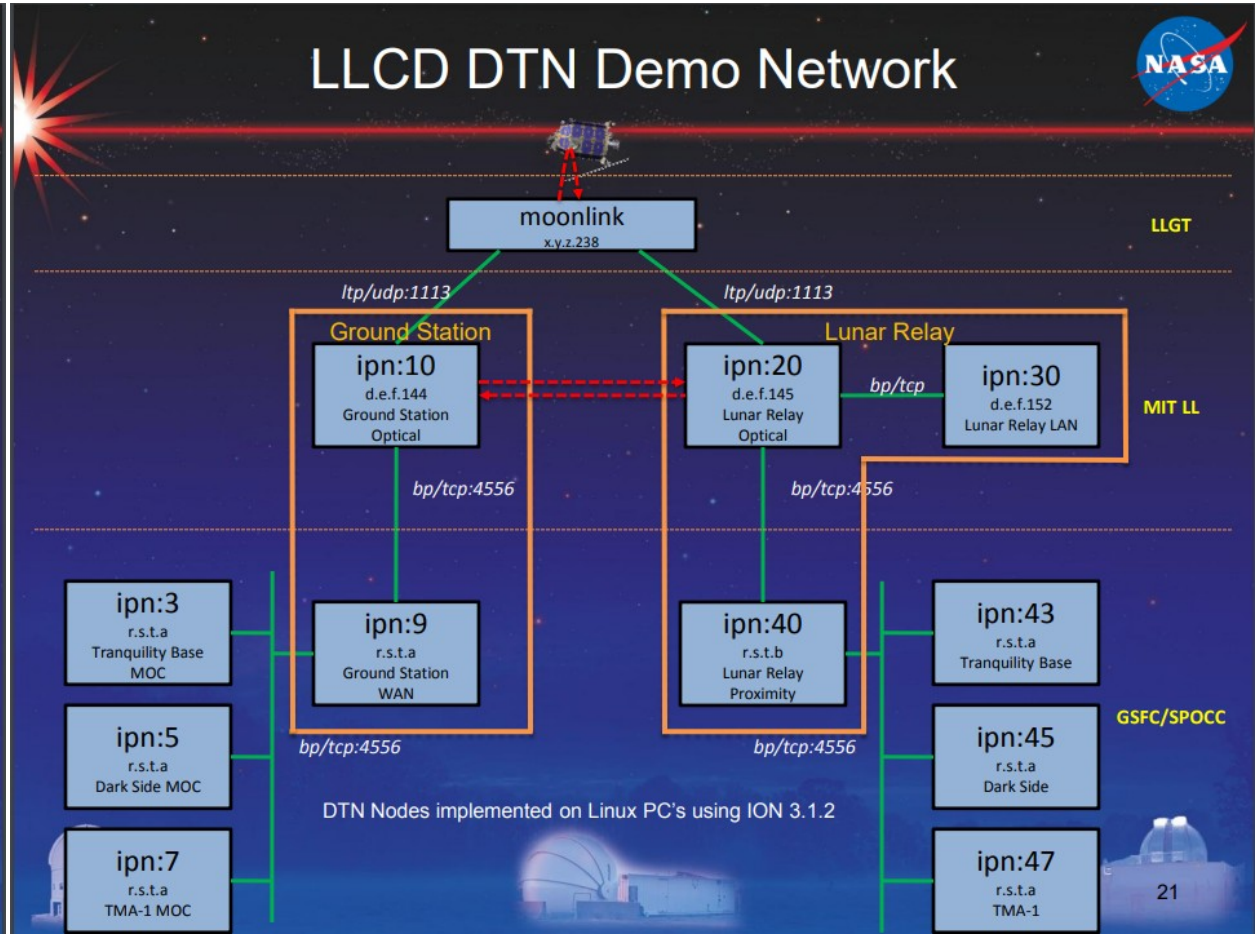
→ EIRP = 8.1 GW!



Optical's shorter wavelengths allow for smaller terminals using less power for equivalent or higher data rates…

Chart courtesy of Don Boroson, MIT Lincoln Laboratory

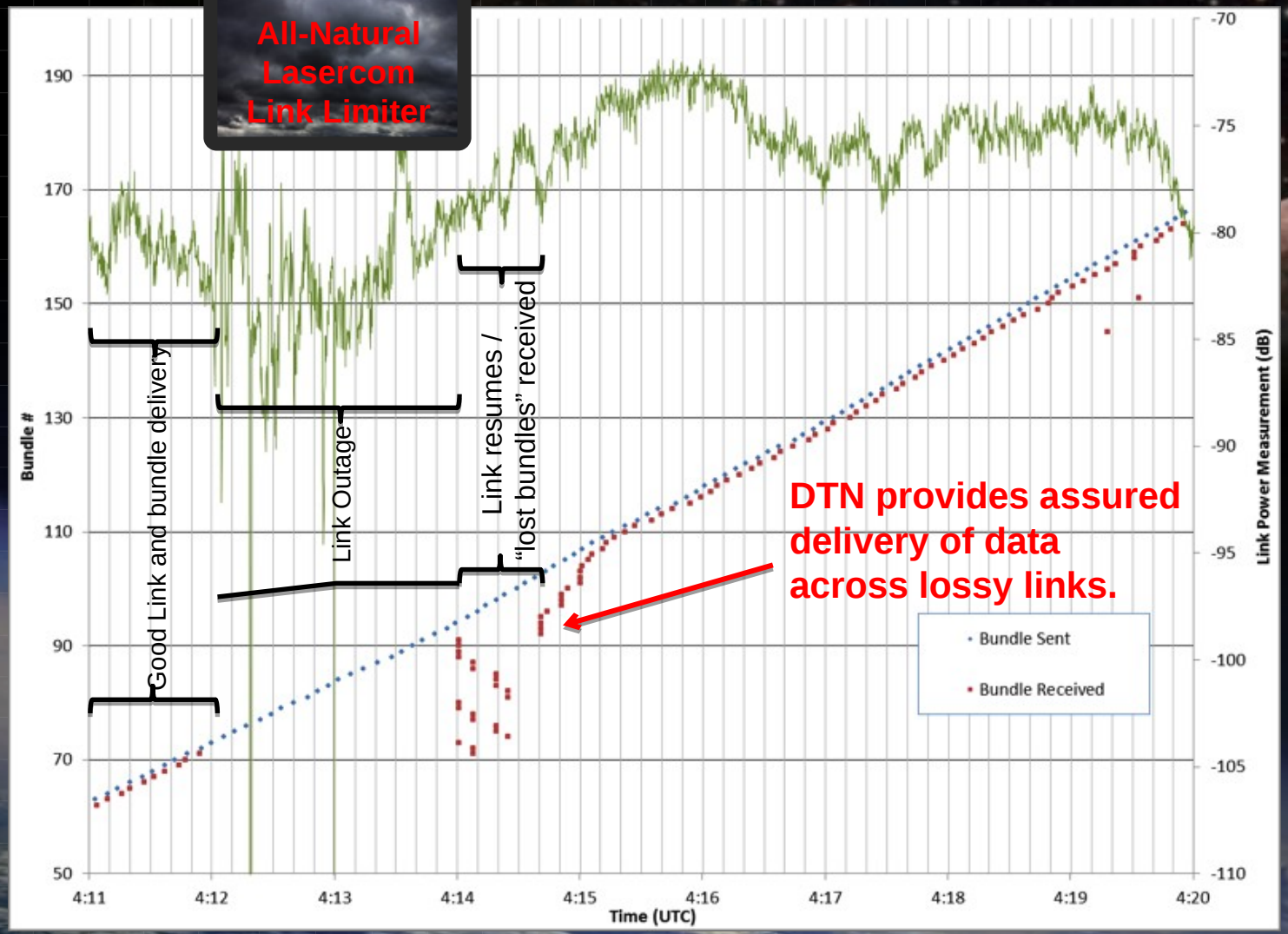
LLCD DTN Demo Network



http://ipnsig.org/wp-content/uploads/2014/02/LLCD-DTN-Demonstration-IPNSIG-Final.pdf

What did they see? DTN solves the "Cloud Problem"

Bundle Delivery Across LLCD Optical Links (18 Nov 2013)



http://ipnsig.org/wp-content/uploads/2014/02/LLCD-DTN-Demonstration-IPNSIG-Final.pdf

Credit: DTN Overview – NASA/J.Soloff – 19 June, 2015