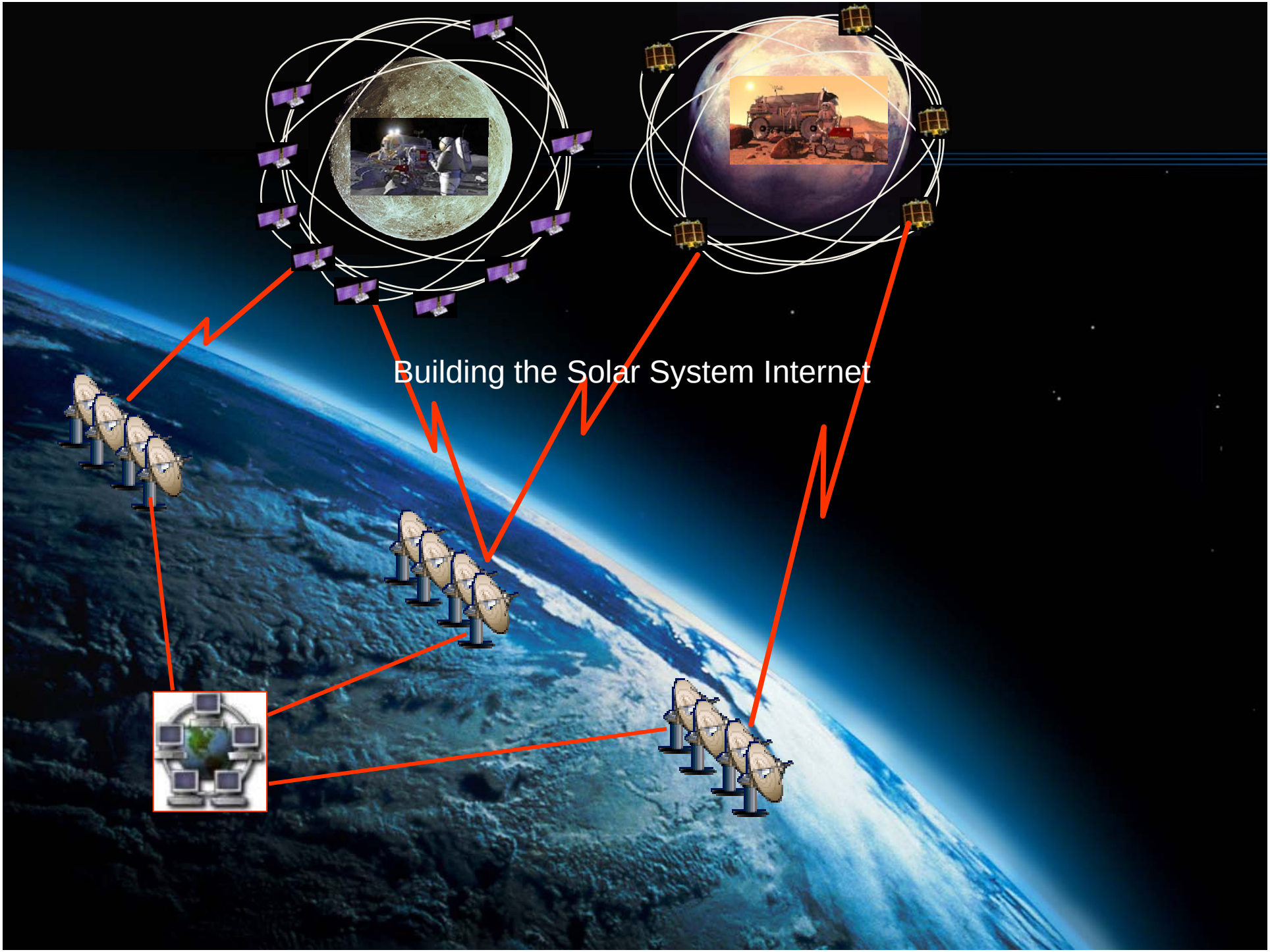
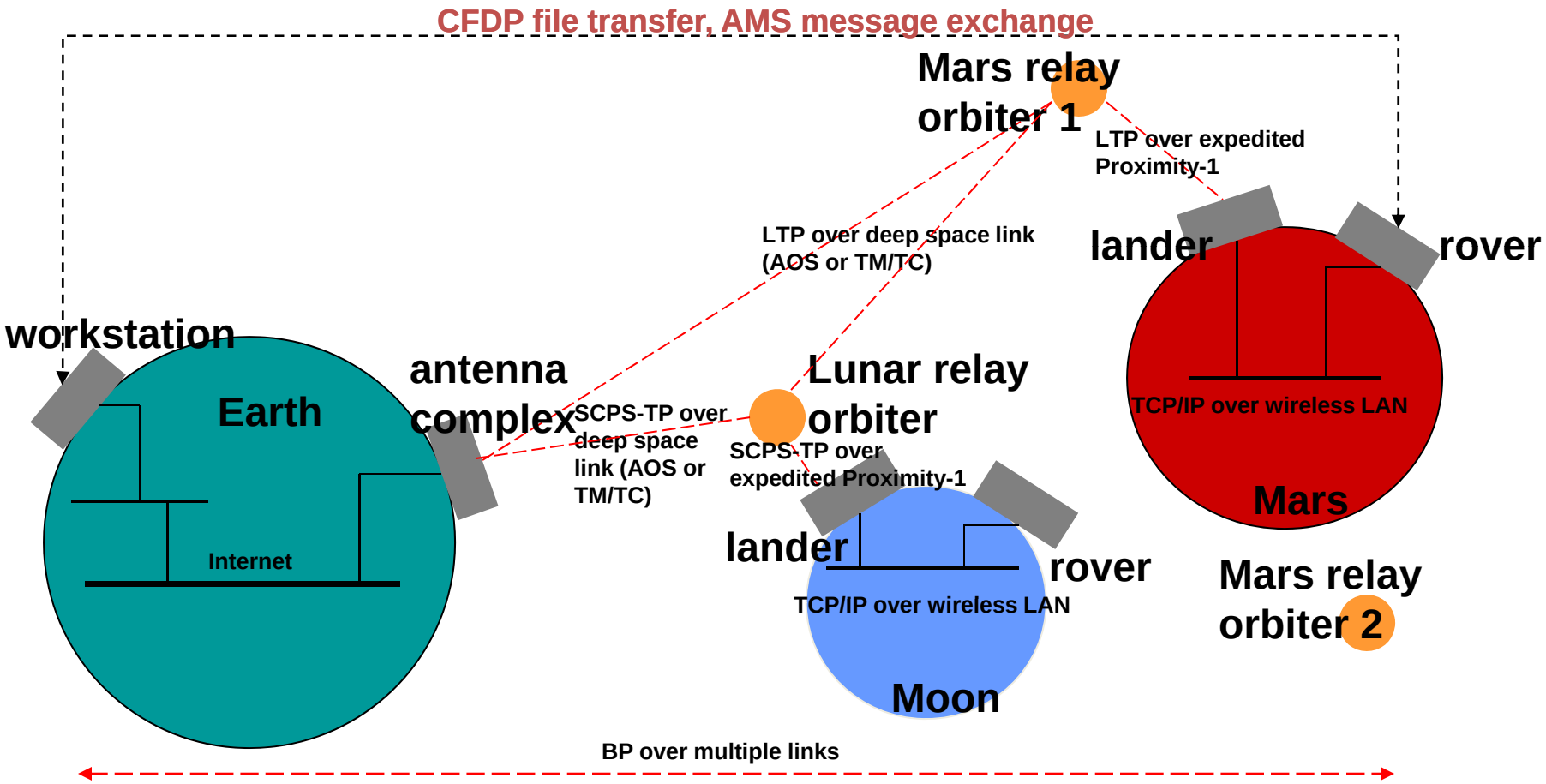
Disruption-Tolerant Networking Across Mission-Critical Ground Networks

Rashied Amini, Scott Burleigh, Joshua Schoolcraft, Jordan L. Torgerson
Jet Propulsion Laboratory, California Institute of Technology
Andrew Jenkins, Sebastian Kuzminsky
University of Colorado, Boulder
Christopher Krupiarz
Johns Hopkins University Applied Physics Laboratory
2 March 2010


Building the Solar System Internet

DTN Operations in Space



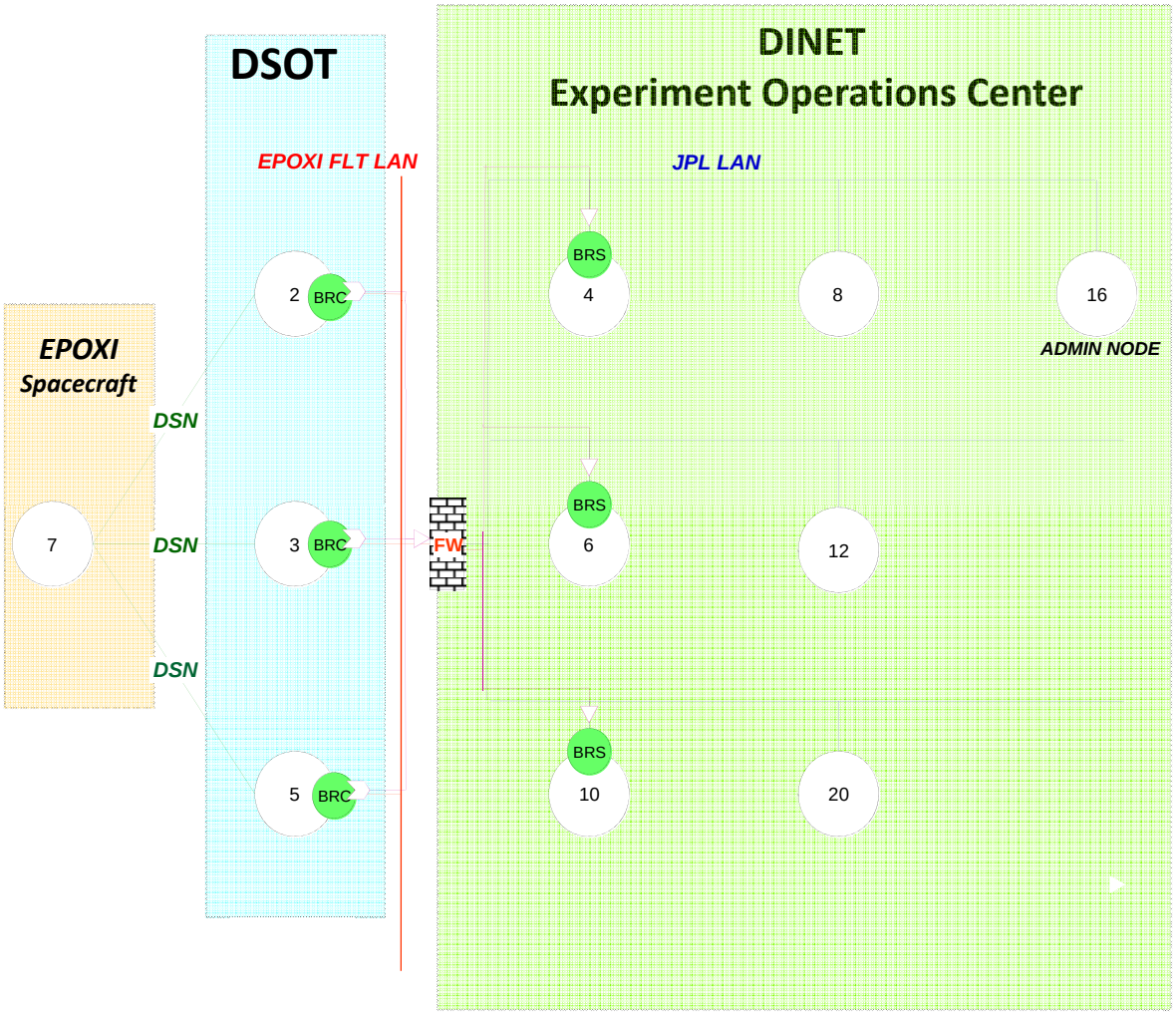
DTN Operations on the Ground

- The terrestrial segments of the end-to-end path suffer little disruption or delay, but they are still part of the DTN architecture.
  - At minimum, the terminus of the end-to-end path for mission data will be a DTN node in a mission operations center on Earth.
  - Deploying DTN nodes at ground stations as well opens opportunities for parallel transmission, custodial retransmission, and rate-matched queuing, increasing reliability and throughput while reducing latency.
  - Extending DTN out to instrument teams and project scientists at their home institutions can make science operations simpler and less expensive.
- And at least one constraint is even more severe on the ground than in space: security.
  - DTN nodes in Earth networks are easier for denial-of-service attacks to reach.
  - Mission operations centers operate behind robust firewalls to mitigate this vulnerability.

The Deep Impact Network (DINET) Experiment

- First deep space node on the Interplanetary Internet:
  - Loaded DTN software onto the EPOXI spacecraft, 49-81 light seconds away, and operated it as a router in space for 4 weeks in Oct.-Nov. of 2008.
  - Eight low-data-rate contacts with DSN stations.
  - Moved 292 images (about 14.5 MB) through the network.
  - DTN prioritization assured that all high-priority images were successfully delivered by DINET.
  - No data loss or corruption anywhere in the network.
- Used all new software on the spacecraft, but minimized risk in the ground data system.
  - Ground segment of the network extended only within JPL; no connectivity to external sites, no seamless interoperation with remote users.
  - For sustained operations to provide maximum value, the network must be extended securely to flight teams, instrument teams, and mission scientists.

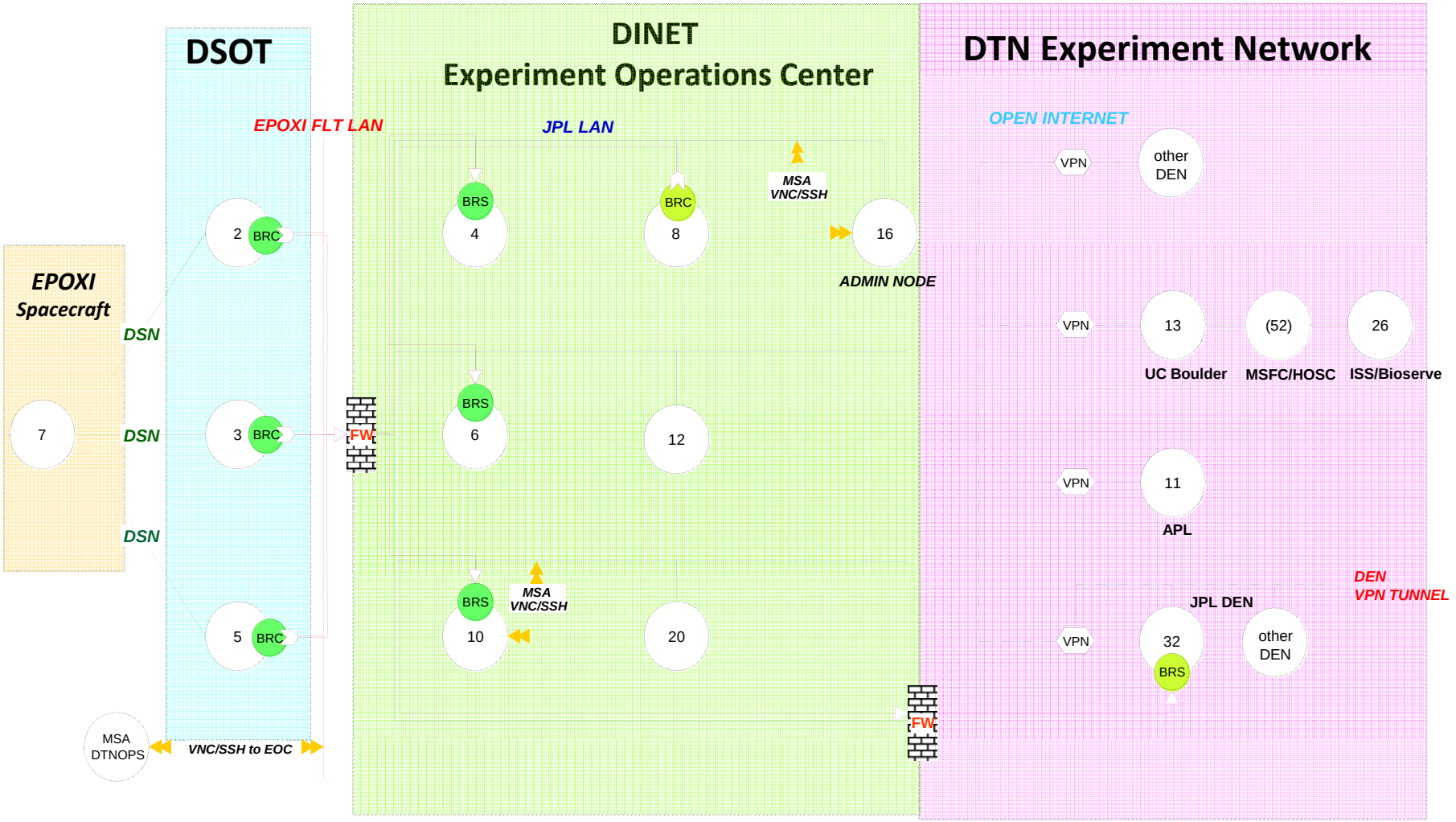
DINET Network Topology



DINET 2

- Objectives
  - Develop and validate additional DTN functionality:
    - Unacknowledged CFDP service
    - *Bundle Security Protocol (BSP)*
    - Dynamic contact graph management
    - An extended DTN priority system.
    - *Demonstrate DTN installed and operating on nodes beyond JPL , **including a node on ISS***
  - Develop and validate key elements supporting the operational use of DTN on EPOXI for future space flight operations.
- Flight operations originally planned for November 2009 but postponed until after EPOXI's encounter with comet Hartley 2 in November 2010.
- Meanwhile, performing "dry run" exercise in Feb./Mar. 2010 involving all elements except EPOXI spacecraft itself – use testbed simulator instead.
- Integrating DTN nodes beyond the JPL firewall into the DINET 2 topology was a key challenge.

DINET 2 Network Topology



DINET 2 Topology Controls

- No process outside the flight LAN firewall is permitted to connect to a socket on the flight LAN.
  - Developed Bundle Relay Service (BRS) convergence-layer protocol adapter for original DINET experiment, to enable conformant TCP connectivity.
    - DINET processes inside the firewall connect to a BRS server that's outside.
    - From that point on, secure traffic can be exchanged in both directions over that connection.
    - All connections are cryptographically authenticated by both server and client.
- Access to the Flight LAN is only by connection to BRS servers in the EOC.
- Access to the EOC is only by connection to a BRS server on the DEN – which physically resides inside the cipher-locked EOC lab, to prevent physical compromise.
- By mission rule, the BRS connection from EOC to the DEN BRS server is disabled whenever the link from simulated "Earth" in DSOT (deep space operations) to the spacecraft is enabled.

DINET 2 Security Measures

- JPL flight LAN protection rule: data from outside JPL may be allowed into the flight LAN for uplink to the spacecraft – but only after manual inspection and verification.
  - Developed bundle inspection and deletion utilities for this purpose.
- Bundle Security Protocol (BSP) is globally utilized to authenticate traffic between neighboring nodes within the DTN network.
  - This is DTN's defense against DOS attacks: only the node that is directly attacked is affected – it never forwards the attack traffic within the network.
- The DEN is a DTN overlay on top of an Internet virtual private network. Only authenticated nodes that can access the VPN can communicate over the DEN.

DINET 2 Dry Run, Feb./Mar. 2010

- Objectives:
  - Validate use of BSP for data transfer
  - Validate use of BSP in discriminating against unsecured traffic
  - Validate the ability to change BSP keys and policies during operations
  - Utilize bundle examiner to inspect bundles arriving at the EOC
  - Collect CPU utilization data on the SCU with BSP Tx policy on and off
  - Demonstrate the robustness of DTN software for use across nodes at multiple institutions in an operational scenario
  - Validate the DTN effectiveness in an operational scenario
- **5 of 7 key objectives related directly to cross-network security.**

DINET 2 Dry Run Tests

- Send “command” bundles from APL to a node in JPL flight LAN.
  - Verify bundle inspection, manual deletion, and rejection.
- Send “telemetry” bundles from simulated Mars nodes in EOC to APL.
  - Measure testbed CPU utilization when conveying bundles that are BSP authenticated bundles versus those that are not.
  - Verify rejection of unauthenticated bundles by Testbed.
- Send authenticated “load & go” command bundle from APL to simulated Mars node in EOC via Testbed router.
- Send solar flare warning from simulated Mars node in EOC to node on International Space Station via University of Colorado at Boulder.

DINET 2 Dry Run Status

- Pending…

Conclusion

- Implications for DTN support in future ground data systems:
  - Network security measures can reduce the risk of successful attack on a spacecraft to acceptable levels, even when the spacecraft is a node on an automatic digital communication network supported in part by the public Internet.
  - Future missions should be able to conduct secure remote operations over a wide area terrestrial network based on DTN protocols.
- Future work:
  - DINET 2 flight exercise planned for winter of 2010-2011.