Securing Delay and Disruption Tolerant (DTN) Service Provider Networks

Considerations for LunaNet

Authors: Dr. Alberto Montilla and Alberto Montilla Ochoa, Spatiam Corporation

Presenter: Dr. Alberto Montilla, Spatiam Corporation
a.montilla@spatiam.com

SCSN: Secure and Automated Communication for Space Networks – 2024
SPACOMM 2024. The Sixteenth International Conference on Advances in Satellite and Space Communications. May 26-30, 2024

About the Authors

Dr. Alberto Montilla
Co-Founder and CEO
Spatiam Corporation

Dr. Montilla accumulates 25+ years of R&D experience in communication networks. He is a Board member of the Interplanetary Networking Special Interest Group. Holder of four patents. Currently researching on delay and disruption tolerant networking (DTN) as enabler of the Interplanetary Internet. Doctor of Engineering from the Universidad Carlos III de Madrid, and MBA from the Instituto de Estudios Bursátiles (IEB).

Alberto Montilla Ochoa
Co-Founder. Engineering Director
Spatiam Corporation

Alberto Jr. is the technical leader of the Spatiam DTN Platform, the first commercial DTN platform for space. Currently research on asynchronous management for DTN networks and extending zero trust security to DTN. Alberto Jr. is a member of Team USA Field Hockey Men's National Team and a Pan-American medalist. He holds a Bachelor degree in Computer Engineering from the University of California San Diego.

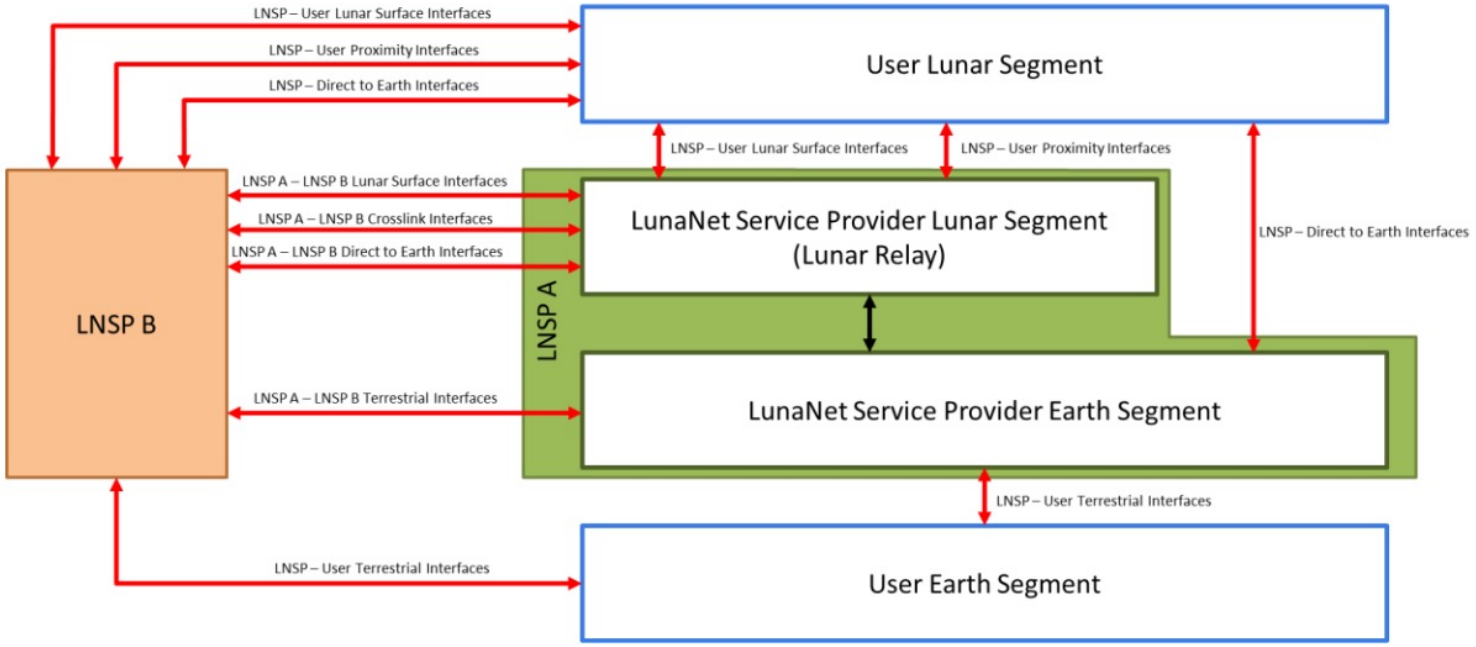
Agenda

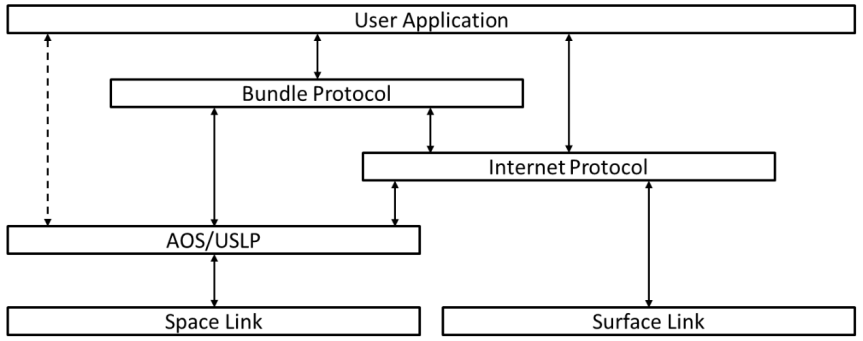
- Intro - LunaNet Service Providers (LNSP)
- Existing security considerations for LunaNet (and DTN).
- DTN Security for LNSPs
  - Operational security challenges
  - Securing User – LNSP interface
  - Inter-LNSP interface(s)
  - End-user and Application-Level Security
- Open Items
- Conclusions

Generated by AI

LunaNet Service Providers (LNSP)

LunaNet is the communications and positioning, navigation and timing (PNT) network architecture for cislunar operations.
It establishes LunaNet Service Providers (LNSP), analog to the terrestrial Internet Service Providers (ISP). The communications architecture uses Delay and Disruption Tolerant Networking (DTN).





LunaNet Service Provider Interfaces & Protocol stack – from the LunaNet interoperability specification

Existing LunaNet (and DTN) Security

The Bundle Protocol [1] is the core internetworking protocol for DTN.

LunaNet security considerations [2]

- Users and LNSPs shall protect confidentiality, integrity and availability of systems, data and communications paths.
- Prevent unauthorized access, corruption, interception & data loss.
- Users are expected to protect their data using encryption.
- Networking - IPSEC and BPSEC.

Bundle Protocol security (BPSEC) [3, 4]

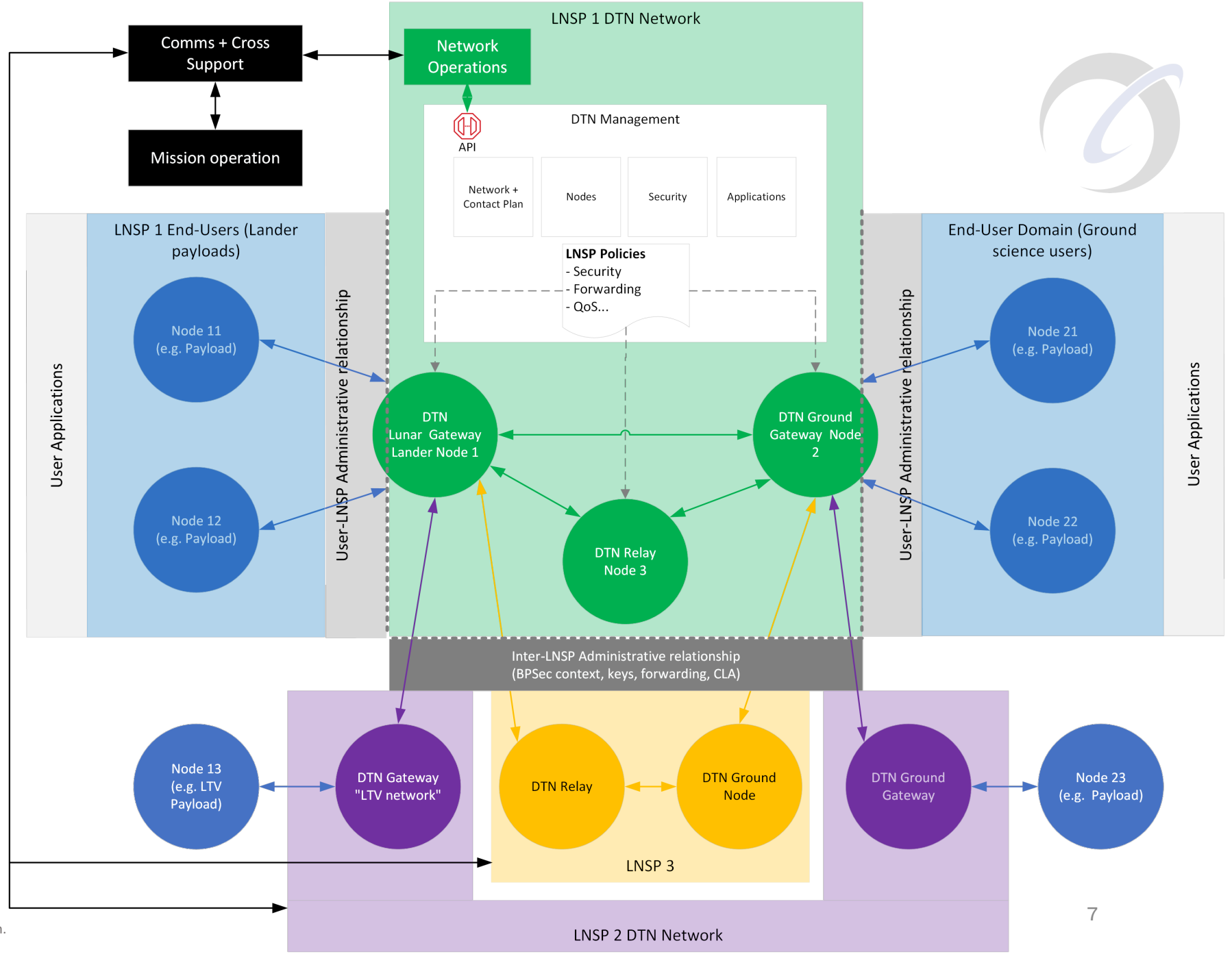
- Protects integrity (BIB) and confidentiality (BCB) of bundle targets.
- BPSEC uses security contexts [5] – configurations, algorithms and policies to provide consistency in the application of BPSec across the network.

LNSP - Operational Security Challenges [6, 7]

Challenge	Consideration details
Attack surface susceptible to lateral movement and topology attacks	BP Node IDs are public identifiers. Service ID are like ports in TCP/UDP. Network topology is open due to contact plan structure.
Current BPSec setup is complex in a User – LNSP scenario.	Requires tight coordination (and administrative trust) among two or more parties.
Security Management and automation for LNSPs is yet to be accomplished	Implementation of policies, Analysis of security posture, key management.
Content inspection is challenged by infrastructure limitations	Round trip time prevents centralized content inspection*

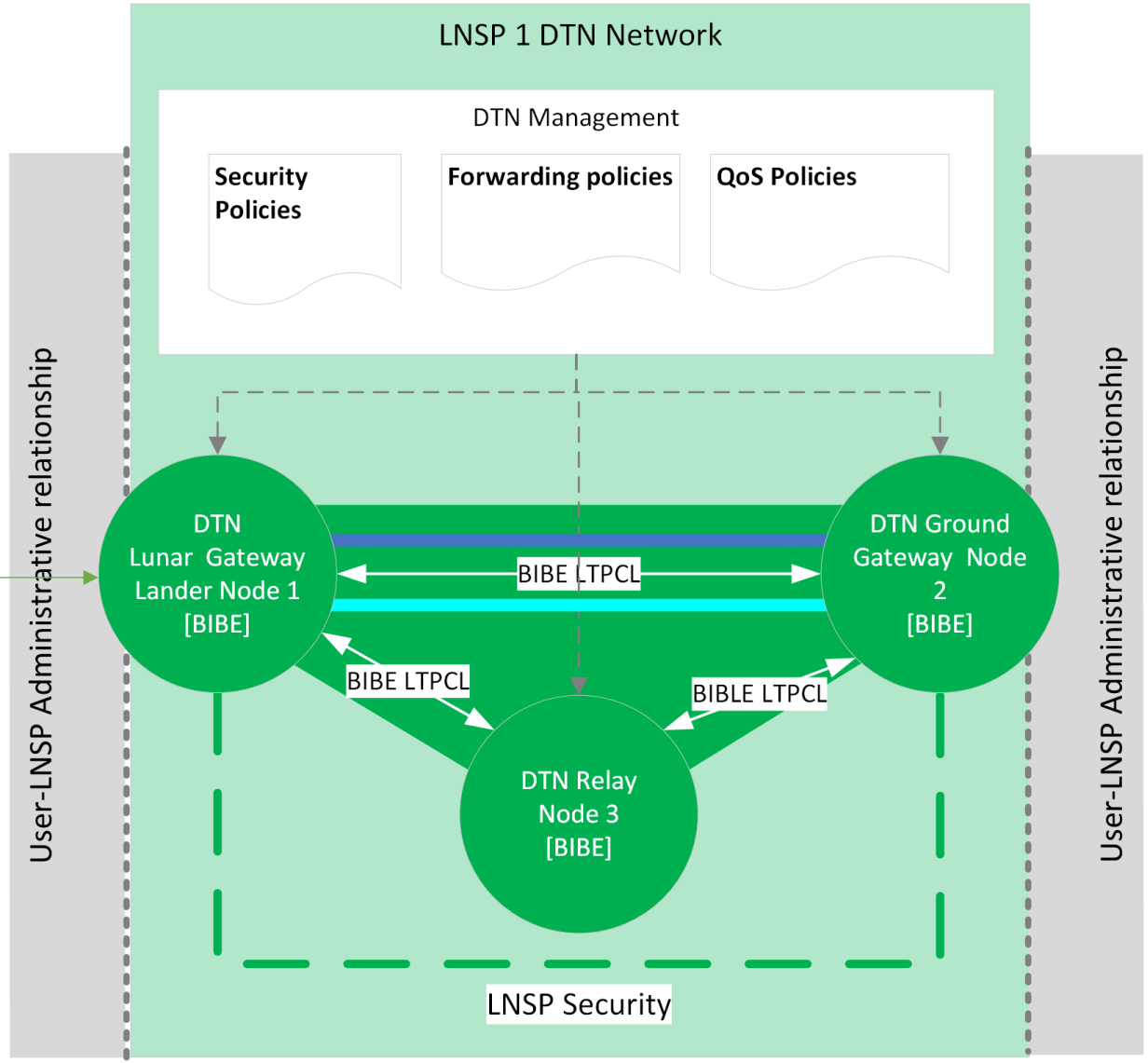
LNSP 1 example deployment

- User-LNSP interface
- Inter-LNSP interface
- User Applications
- Network Management
- Operations



Securing User-LNSP Interface

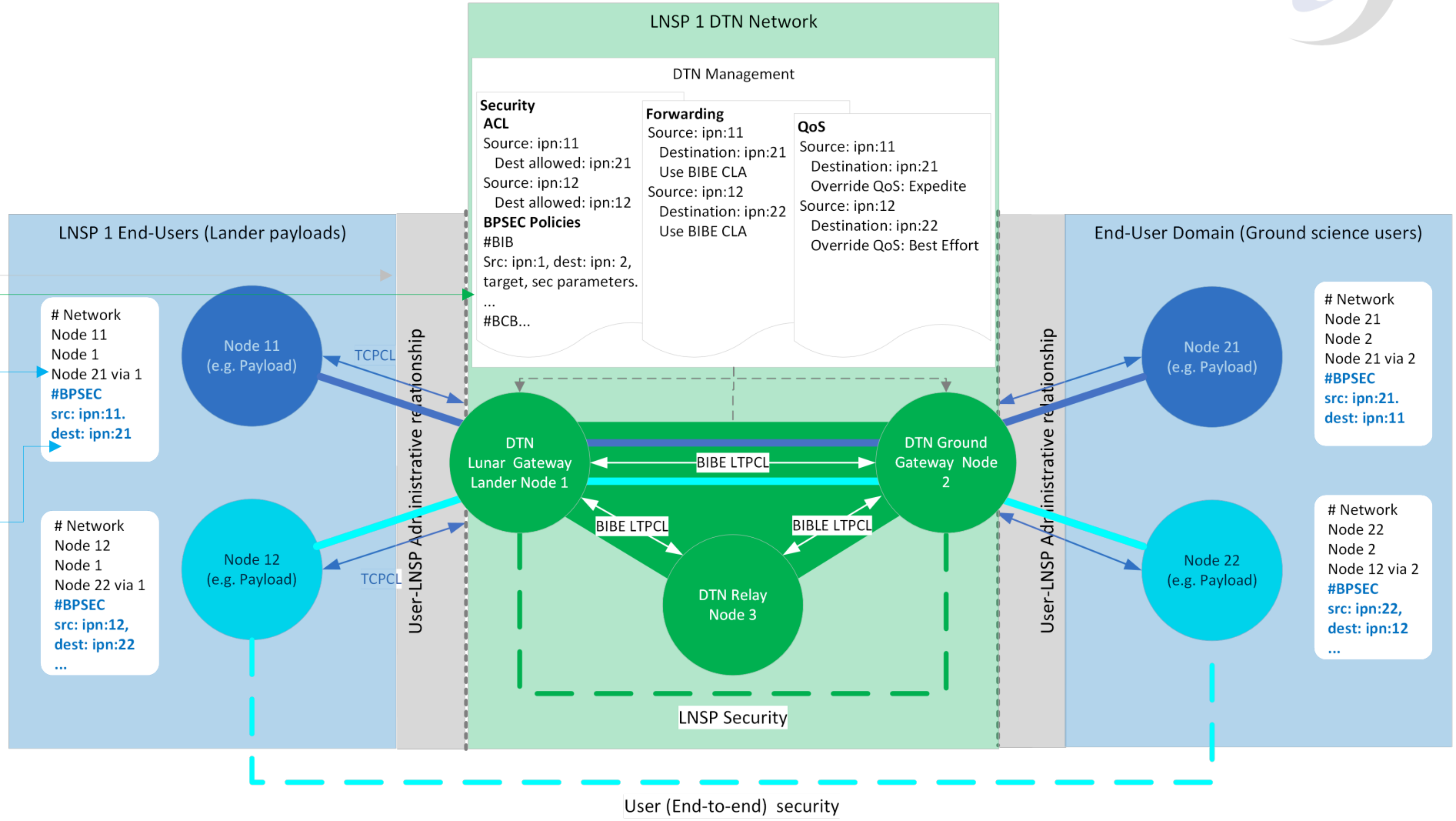
- Gateway Nodes with simplified interface configuration.
- Use Bundle in Bundle Encapsulation (BIBE) to allow for simpler setup
  - Enforcing network user security policies at the edge
  - Topology hiding – default routes
  - LNSP specific contexts
  - Require end-to-end security for securing last mile.



Securing User-LNSP Interface with BIBE

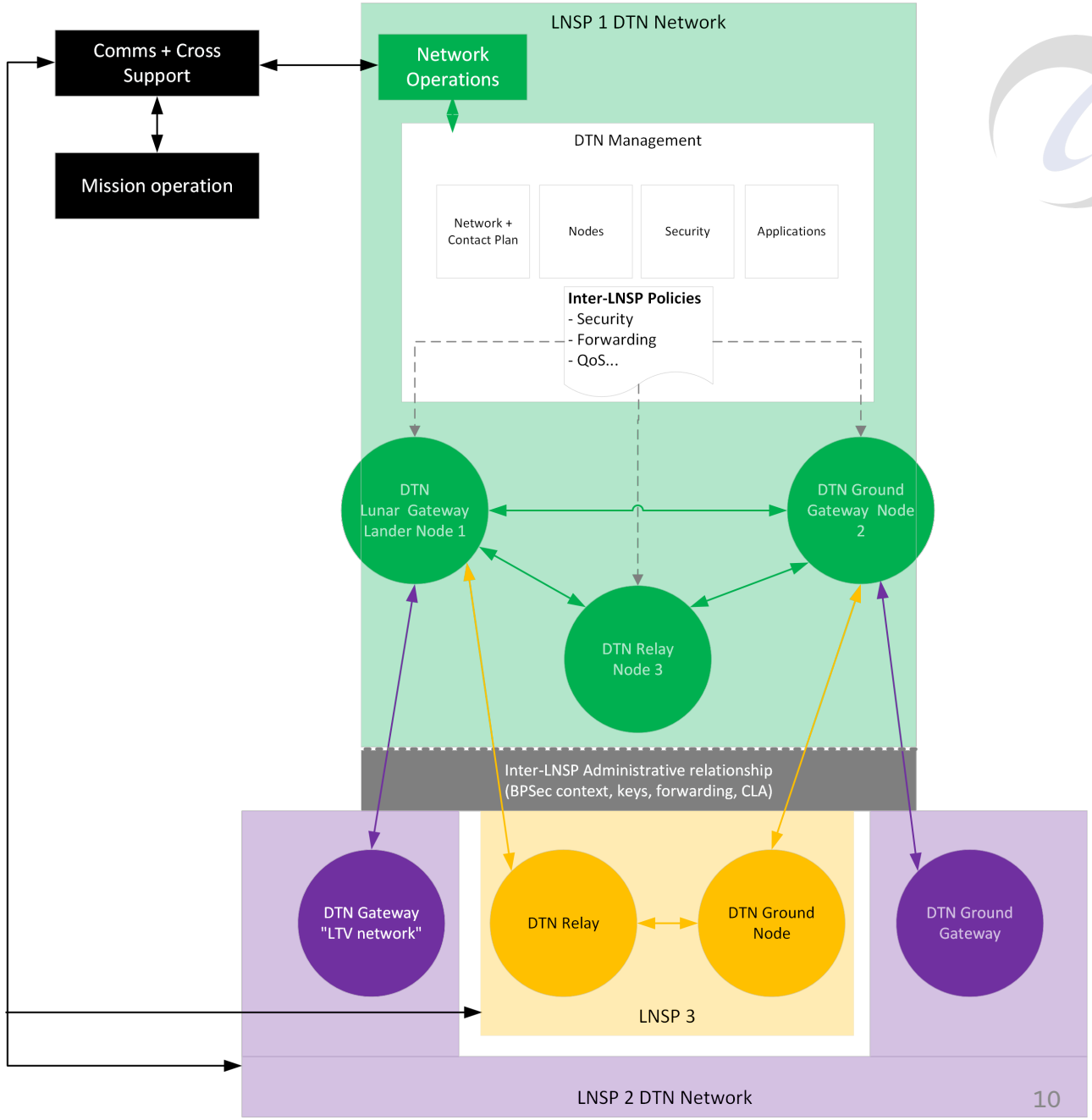
Benefits

- Simplified configuration
- Enforcing network user security policies at the edge
- LNSP specific contexts
- Topology hiding – default routes
- Require end-to-end security for securing user data.



Inter-LNSP security considerations

- Security policies
  - BPSec (shared) context
  - Key distribution
  - ACL
  - Ground IP routing security.
- Forwarding policies
  - Use BIBE for ”trunking” service.
- QoS policies
  - SLAs (administrative)
- **Operations**
  - Registry of interface configurations
  - Management automation (contact plan distribution, security policies, ACLs)

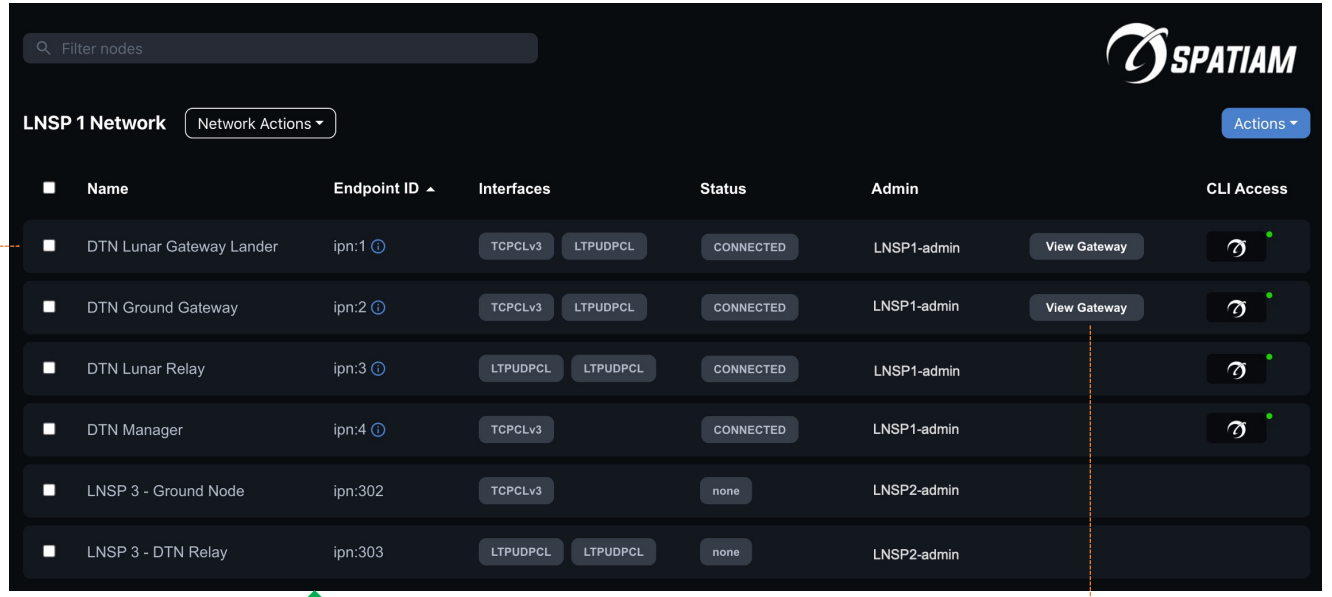


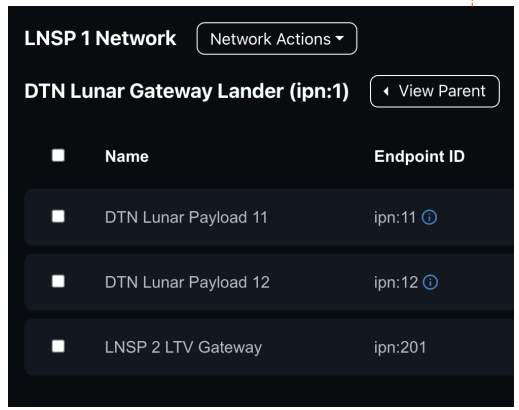
End User and Application security

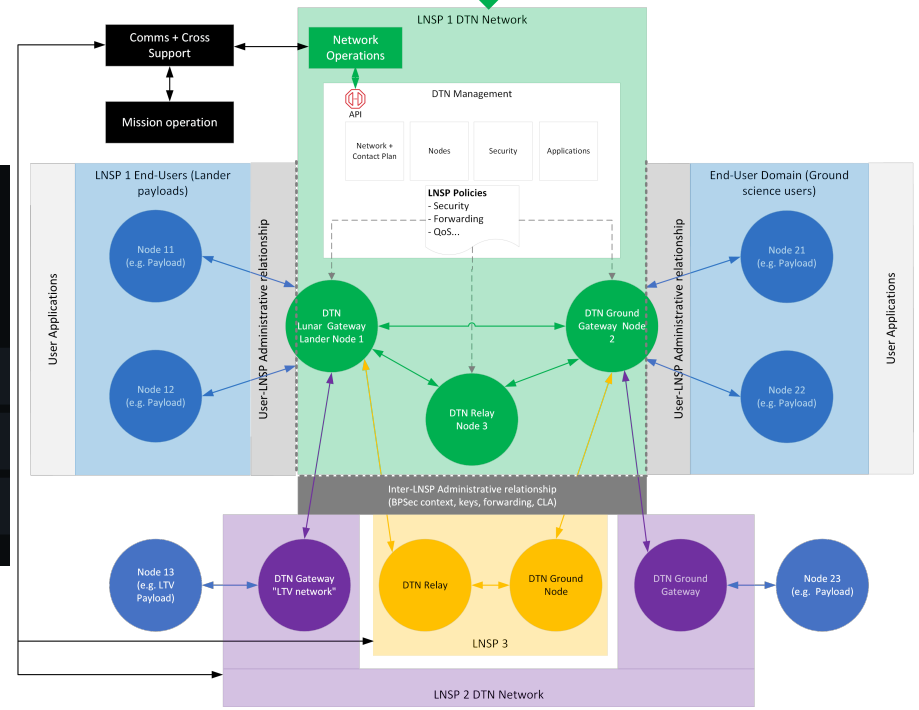
- There is currently no control between Service-IDs and applications
  - Service-IDs open BP application interfaces.
  - *What application can you run on each Service ID in a LNSP*?
- Payload nodes' administrators shall implement BP application security.
  - User authentication
  - Application – Service ID(s) mapping and control

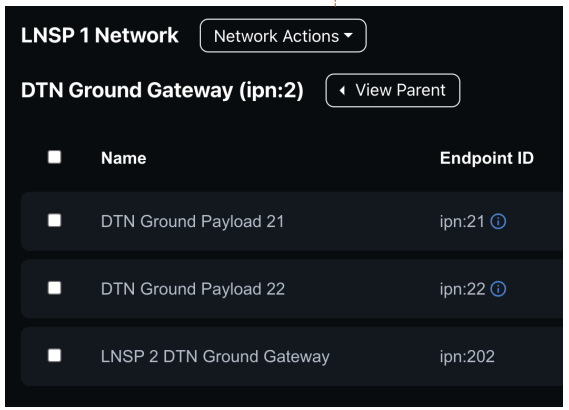
LNSP DTN Network Management

- Essential for network and application security
  - Node Configuration
  - Contact Plan Management
  - Security policies
- APIs are essential for efficient operations
  - Integration with network operations.
  - Integration for cross-support needs









Open items

Open Item	Commentary
Network & application	
Node ID allocation	Validating Node ID allocations require a common registry and an allocation hierarchy. Node ID allocation ID in draft by IETF.
Content inspection	Round Trip time imposes a challenge to create centralized (typically cloud) content inspection. Area for further research.
Key Distribution	Delay Tolerant Key Distribution is an ongoing research item.
Operational	
Inter-LNSP administration	Network registry, network management automation via API.

Conclusions

- LunaNet Service Providers shall secure their networks against known attacks.
- User-LNSP interface security can benefit from deploying DTN Gateways with Bundle in Bundle Encapsulation.
- Network management is critical to ensure LNSP and cross-support security automation.
- End-user application security requires service-ID registration and mapping.
- DTN Security is an evolving topic, with open items including node ID allocation, delay tolerant key distribution, among others.
- The goal is to enable Zero Trust for DTN.

References

1. IETF RFC 9171. Bundle Protocol Version 7. January 2022.
2. LunaNet Interoperability specification (v4). A security specification is pending for release. https://esc.gsfc.nasa.gov/static-files/LunaNet%20Interoperability%20Specification.pdf
3. IETF RFC 9172. Bundle Protocol Security (BPSec). January 2022.
4. Montilla Bravo, Alberto. Security Interplanetary Networks, applications and users. Blog article. October 2023. https://www.spatiam.com/blogs/blog_015.html
5. IETF RFC 9173. Default Security Contexts for Bundle Protocol Security (BPSec). June 2022.
6. Ivancic, William. Security Analysis of DTN Architecture and Bundle Protocol Specification for Space-Based Networks. IEEEAC 2010.
7. Montilla Bravo, A and Montilla Ochoa, A. Extending Zero Trust to Delay and Disruption Tolerant Networks (DTN) in Space. IEEE/NASA Cognitive Communications for Aerospace Applications Workshop 2023. https://ccaaw.ieeecleveland.org/wp-content/uploads/sites/574/2023/06/28.pdf

Thank You!

Securing DTN Service Provider Networks

Considerations for LunaNet

Dr. Alberto Montilla, Spatiam Corporation

Alberto Montilla Ochoa, Spatiam Corporation

SCSN: Secure and Automated Communication for Space Networks – 2024
SPACOMM 2024. The Sixteenth International Conference on Advances in Satellite and Space Communications
May 26-30, 2024