GREEN Working Group
Internet-Draft
Intended status: Informational
Expires: 12 October 2026

J. Moore
J. Kinsler
Vettic LLC

10 April 2026

Resource-Aware Routing and Mechanical Displacement for Energy-Efficient Networking (GREEN)
draft-moore-green-mechanical-displacement-00

Abstract

The evolving draft-ietf-green-framework provides necessary YANG data models for monitoring Device Level Energy Efficiency (DLEE) and Component Level Energy Efficiency (CLEE). However, mitigating high-volume East-West traffic (e.g., massive inference synchronization) during peak grid carbon-intensity remains a structural challenge.

This document proposes an architectural extension utilizing Delay-Tolerant Networking (DTN). It introduces "Mechanical Displacement"—the physical routing of encrypted cold data via autonomous or commercial logistics—as a zero-marginal-emission routing path, managed by hardware-rooted out-of-band blind packet switching.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 12 October 2026.

Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

As hyperscale compute environments push unprecedented power densities, systems operating with unmitigated execution authority generate massive data payloads (e.g., AI model weight updates, cold-storage mirroring). While the GREEN framework effectively monitors network energy consumption, rerouting petabyte-scale traffic across alternate digital fiber paths still incurs a massive continuous energy cost.

This draft extends the GREEN framework by defining how physical transport logistics can be structurally integrated as high-latency, zero-marginal-emission network nodes, physically offloading digital traffic from carbon-heavy grids.

2. Terminology

* *Mechanical Displacement:* The physical transportation of encrypted digital payloads via non-traditional network couriers (e.g., autonomous delivery vehicles, commercial aviation) to bypass digital transmission energy costs.

* *Sentry Node:* An out-of-band hardware apparatus that acts as an Executive Anchor, evaluating payload characteristics and enforcing routing thresholds physically isolated from the host operating system.

* *Blind Packet Switching:* The routing methodology used by the Sentry Node to make physical displacement decisions based strictly on hardware-level trace signatures, payload weight, and urgency, without decrypting the payload.

3. The Architectural Bottleneck

Currently, when GREEN YANG models detect high carbon intensity on a route, the network attempts to throttle or redirect traffic. For delay-tolerant, high-volume data, this still results in significant energy expenditure over extended transmission windows. The framework lacks a mechanism to drop digital transmission energy to absolute zero while maintaining cryptographically secure data transport.

4. The Vettic Currier Network (VCN) Integration

The proposed solution integrates the Vettic Currier Network (VCN) as a delay-tolerant routing layer directly responsive to GREEN metrics.

4.1. Blind Packet Switching

Sentry Nodes operate at the silicon level, utilizing blind packet switching to identify the volume and urgency of a payload. Critical telemetry (e.g., execution tokens, failsafe commands) is prioritized for immediate digital backhaul, while massive "cold" data is flagged for potential physical displacement.

4.2. Telemetry Ingestion and Threshold Triggers

The routing logic ingests real-time YANG energy metrics (e.g., ietf-power-management) from the GREEN framework. The Sentry Node evaluates the data weight against the local grid’s current carbon intensity and power stress.

4.3. Physical Offload and Mechanical Displacement

If a high-volume payload encounters a high-stress grid threshold, the VCN triggers the physical routing path. The payload is spool-written to encrypted, localized storage mediums and handed to the courier layer (Mechanical Displacement). By treating autonomous vehicles or commercial logistics as network nodes, the digital grid’s power constraints are structurally mitigated.

5. Hardware-Rooted Executive Interlock

Because this routing architecture shifts data outside traditional digital perimeters, it requires a hardware-rooted Failsafe. The Sentry Node serves as this Executive Anchor. If an unauthorized state divergence or tamper attempt is detected during the offload process, the Sentry Node deterministically drops voltage to zero (V=0) exclusively to the compromised interface, physically severing the connection before data exfiltration can occur.

6. Security Considerations

Mechanical Displacement introduces physical custody vectors. To mitigate this, the VCN architecture ensures the physical courier acts purely as a "blind relay." The courier transports the encrypted spool but lacks the cryptographic keys required for decryption or inspection. Data sovereignty is maintained via hardware-enforced encryption, and physical tampering triggers a verifiable failure state sealed in an air-gapped ledger.

6.1. Temporal Data Sovereignty (The Digital Fuse)

To secure data in transit via Mechanical Displacement, the VCN enforces Temporal Data Sovereignty. Encrypted data bundles contain an unencrypted header defining strict expiration criteria (e.g., time-to-live thresholds, transit duration limits). If the physical courier fails to reach the destination network within the defined window, a digital fuse logic permanently purges the payload, structurally mitigating data capture if an asset is intercepted.

6.2. Post-Severance Data Custody and Entropy Flush

When the Executive Anchor initiates a V=0 severance, it manages residual data at rest. Prior to total power loss, the Sentry Node utilizes blind packet switching to extract critical operational payloads laterally via the VCN, preserving mission continuity. Concurrently, the architecture executes an Active Physical Entropy Flush. It injects a localized voltage spike into the compromised asset’s volatile memory (VRAM), obliterating localized data to defend against post-mortem physical extraction attacks.

7. Informative References

[GREEN-FRAMEWORK]
Internet Engineering Task Force, "draft-ietf-green-framework-00".

Authors' Addresses

Jonathon Moore
Vettic LLC
Email: jon.moore@vettic.ai

Jacob Kinsler
Vettic LLC
Email: jacob.kinsler@vettic.ai