DTN Peering Protocol (DPP)

ietf://dtn/meetings/125

draft-taylor-dtn-dpp

rtaylor@aalyria.com

DTN Peering Protocol (DPP)

- Inter-domain routing protocol for DTN
- Analogous to BGP’s role in the Internet
- Exchanges reachability between Administrative Domains (ADs)
- Harmonizes `ipn` and `dtn` addressing into a unified routing framework
- Supports reactive routing and scheduled contact windows

The Problem

- Multiple agencies/organizations operate independent DTN networks
- No standardized way to exchange reachability across administrative boundaries
- Manual route configuration doesn’t scale
- A single global contact graph is neither practical nor desirable
- Each organization has its own mission planning and contact schedules

Use Cases

- **Inter-Agency:** NASA DSN ↔ ESA ESTRACK bundle routing
- **Commercial-Government:** Satellite operator provides transit to deep-space assets
- **Redundant Paths:** Multiple ground stations advertise paths with metrics
- **Scheduled Contacts:** Advertise future connectivity windows for proactive scheduling
- **Scalable CGR:** Each AD runs CGR internally; DPP connects the domains

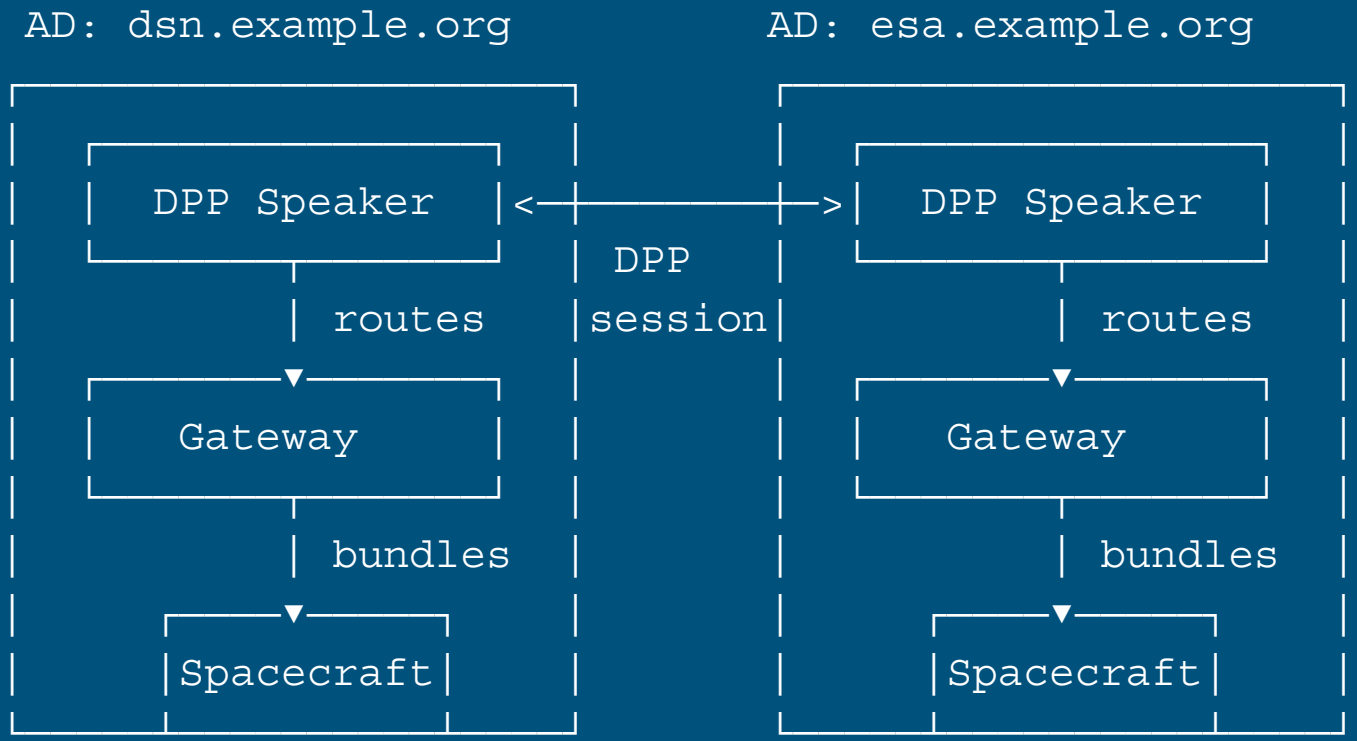
Key Design Principles

- **Transport Agnostic:** gRPC over any reliable transport (TCP/IP, QUIC)
- **Unified Routing:** `ipn` and `dtn` schemes in a single FIB
- **DNS-Rooted Identity:** AD identified by DNS domain name
- **Decoupled Trust:** “Who I am” (AD Identity) ≠ “What I route” (EID patterns)
- **Control/Data Plane Separation:** DPP speakers ≠ gateways

DPP Speakers vs Gateways

- **DPP Speaker:** Entity that runs the protocol (control plane)
  - Ground stations, route controllers, orchestration systems
  - Requires DNS access for identity verification
- **Gateway:** Border node that forwards bundles (data plane)
  - May be co-located with speaker, or separate
  - Can be anywhere — including on spacecraft or relay satellites
- `gateway_eid` attribute bridges the two when they are separate
- Multiple speakers per AD — loop-safe (AD_PATH uses domain identity)

Architecture



DNS-Based Identity

- AD identity = DNS domain name (e.g., `dsn.example.org`)
- Public key published in SVCB record at `_dtn_domain.<AD-Domain>`

```
_dtn_domain.dsn.example.org.  IN  SVCB  1 . (
    dtn-alg=ed25519
    dtn-pubkey=MCowBQYDK2VwAyEAGb9... )
```

- `_dtn_domain` prefix reserves `_dtn` for future transport-specific uses
- Multiple records for multiple speakers (per-speaker keys)
- DNSSEC SHOULD be used to protect against spoofing

Handshake Flow

1. **Hello** — Initiator sends `local_ad_id`
2. **DNS Lookup** — Responder fetches SVCB records at `_dtn_domain.<ad_id>`
3. **Challenge** — Responder sends random nonce (≥16 bytes)
4. **Response** — Initiator signs nonce with private key
5. **Verify** — Responder checks signature against DNS public key(s)
6. **ESTABLISHED** — Route exchange begins

- Multiple SVCB records → try each key until one succeeds
- No DNS needed after session establishment

Route Advertisements

- Modelled on BGP UPDATE messages
- **EID Patterns:** Destinations (`ipn:100.*`, `dtn://*.example.org`)
- **AD_PATH:** List of ADs traversed (loop detection + path length)
- **Metric:** Administrator preference (lower = preferred)
- **Extensible Attributes:**
  - `gateway_eid` — forwarding endpoint
  - `valid_from` / `valid_until` — scheduled contact windows
  - `bandwidth_bps`, `max_bundle_size` — link characteristics
  - Unknown attributes: propagate if transitive, discard if not

Addressing: Harmonized Specificity

`ipn` and `dtn` patterns scored uniformly for FIB lookup

`Score = (IsExact × 256) + LiteralLength`

Monotonic specificity constraint:

- wildcards only at the leaves

Pattern	Score
`ipn:100.1` (exact node)	320
`ipn:100.*` (allocator)	32
`dtn://rover1.example.org` (exact)	274
`dtn://rover*.example.org` (wildcard)	17

Route Selection

Best path tie-breaking order:

1. **Highest Specificity Score** — exact over wildcard
2. **Shortest AD_PATH** — fewer hops preferred
3. **Lowest Metric** — administrator preference
4. **Oldest Route** — stability

Local policy MAY override.

Time-Variant Routing

- `valid_from` / `valid_until` attributes on route advertisements
- Enables scheduled contacts for deep-space networks
- Multiple advertisements with non-overlapping windows
- Routes without time attributes are valid immediately until withdrawn
- Connects to CGR / CCSDS SABRE within each AD

Protocol: gRPC + Protobuf

- Single bi-directional gRPC stream per session
- Message types: Hello, HelloChallenge, HelloResponse, RouteUpdate, KeepAlive, Notification

```
service DtnPeering {
  rpc Peer(stream PeerMessage) returns (stream PeerMessage);
}
```

- Keepalives at `hold_time_seconds / 3`
- State machine: CONNECTING → HANDSHAKE → ESTABLISHED

Loop Detection

- AD_PATH attribute (like BGP AS_PATH)
- Operates on AD identity, not individual speaker identity
- Speaker prepends own `local_ad_id` when re-advertising
- Route discarded if AD_PATH contains own identity
- Multiple speakers per AD are inherently safe

Forward Compatibility

- Extensible route attributes (BGP-style)
- Unknown attributes with `transitive = true`: preserve and propagate
- Unknown attributes with `transitive = false`: silently discard
- Enables incremental deployment of new attribute types
- No protocol version negotiation needed

IANA Considerations

- Two new SVCB SvcParamKeys: `dtn-alg`, `dtn-pubkey`
- Registration of `_dtn_domain` in Underscored DNS Names registry
- Future: well-known port, route attribute type registry, ALPN `dpp`

Questions for the Working Group

- SVCB vs TXT records for identity verification?
- Scope of `gateway_eid` — sufficient for multi-gateway deployments?
- Time-variant routing interaction with CGR implementations
- Route filtering and policy — out of scope, but what do operators need?
- Relationship to draft-ek-dtn-ipn-arpa for CL discovery

Thank you