Delay/Disruption Tolerant Networking
Internet-Draft
Updates: 9758 (if approved)
Intended status: Standards Track
Expires: 16 September 2026

R. Taylor
Aalyria Technologies

15 March 2026

BP Address Resolution Protocol
draft-taylor-dtn-bp-arp-00

Abstract

This document specifies the Bundle Protocol Address Resolution Protocol (BP-ARP), a mechanism for discovering the Node ID of a Bundle Protocol Agent (BPA) that is reachable at a known Convergence Layer (CL) address. BP-ARP enables a BPA to resolve CL-layer adjacency into BP-layer peer relationships, bootstrapping higher-level protocols such as SAND. This document updates RFC 9758 to allow externally received bundles destined to the LocalNode administrative endpoint for registered administrative record types.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://ricktaylor.github.io/bp-arp/draft-taylor-dtn-bp-arp.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-taylor-dtn-bp-arp/.

Discussion of this document takes place on the Delay/Disruption Tolerant Networking Working Group mailing list (mailto:dtn@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/dtn/. Subscribe at https://www.ietf.org/mailman/listinfo/dtn/.

Source for this draft and an issue tracker can be found at https://github.com/ricktaylor/bp-arp.

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/.

Copyright Notice

Table of Contents

1. Introduction

1.1. Problem Statement

In Bundle Protocol networks, a Convergence Layer Adapter (CLA) may discover link-layer adjacency with another node without learning that node's Node ID. For example:

* A UDP-based CLA receives packets from a previously unknown IP address.

* A Bluetooth CLA discovers a nearby device.

* A satellite link becomes available to a ground station.

In these cases, the CLA knows _how_ to reach the neighbour (CL address) but not _who_ they are (Node ID). Without the Node ID, the BPA cannot:

* Install routes to the discovered node.

* Make forwarding decisions for bundles destined to that node.

* Participate in neighbour discovery protocols like SAND.

Additionally, some CL protocols convey only a single Node ID during session establishment. For example, TCPCLv4 [RFC9174] exchanges one Node ID per peer during contact header negotiation. A node that supports multiple Node IDs — such as both an ipn-scheme and a dtn-scheme Node ID — cannot advertise all of its identities through the CL protocol alone. BP-ARP allows discovery of the complete set of Node IDs associated with a peer, regardless of CL protocol limitations.

1.2. Relationship to SAND

The IETF SAND protocol [I-D.ietf-dtn-bp-sand] provides secure advertisement and neighbourhood discovery at the Bundle Protocol layer. However, SAND requires the ability to send bundles to discovered neighbours. BP-ARP provides the bootstrap mechanism to resolve CL addresses to Node IDs, enabling SAND to operate.

```
CLA discovers CL adjacency (Neighbour)
    -> BP-ARP resolves Neighbour -> Peer (learns Node ID)
        -> SAND can exchange topology information with known Peer
```

1.3. Design Rationale

BP-ARP is designed as a BPA-level operation, not a service-level one. The question "what is your Node ID?" is directed at the BPA itself, similar to how ICMP messages in IP are handled by the IP stack rather than applications. BP-ARP resolves the singleton identity of a specific node; it is analogous to ICMP, not IGMP. Group membership discovery for multicast or anycast endpoints is out of scope.

For this reason, BP-ARP uses the administrative endpoint rather than a dedicated service endpoint.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Bundle Protocol Agent (BPA): The node-level entity that implements the Bundle Protocol.

Convergence Layer Adapter (CLA): A component that adapts the Bundle Protocol to a specific underlying transport.

Convergence Layer Address (CL Address): A transport-specific address used by a CLA (e.g., IP address + port for TCP/UDP).

Endpoint Identifier (EID): A name for a Bundle Protocol endpoint, using either the ipn or dtn URI scheme, as defined in [RFC9171], Section 4.2.5.1.

Node ID: The EID that identifies a BPA as a whole, as distinct from

any application service endpoints. [RFC9171], Section 3.1 defines the Node ID as the endpoint that identifies the BPA itself. Each URI scheme defines the Node ID as follows:

* ipn scheme: The Node ID is the administrative endpoint, formed by setting the service number to 0. For example, ipn:42.0 or ipn:1.42.0 (with allocator). This is defined in [RFC9758], Section 3.3.

* dtn scheme: The Node ID is the node name with no demux part. For example, dtn://node42/. This is defined in [RFC9171], Section 4.2.5.1.1.

A node MAY have multiple Node IDs across different URI schemes. For example, a node might be identified as both ipn:42.0 and dtn://node42/. Node IDs are by definition singleton endpoints that uniquely identify a single BPA; multicast and anycast EIDs are not Node IDs.

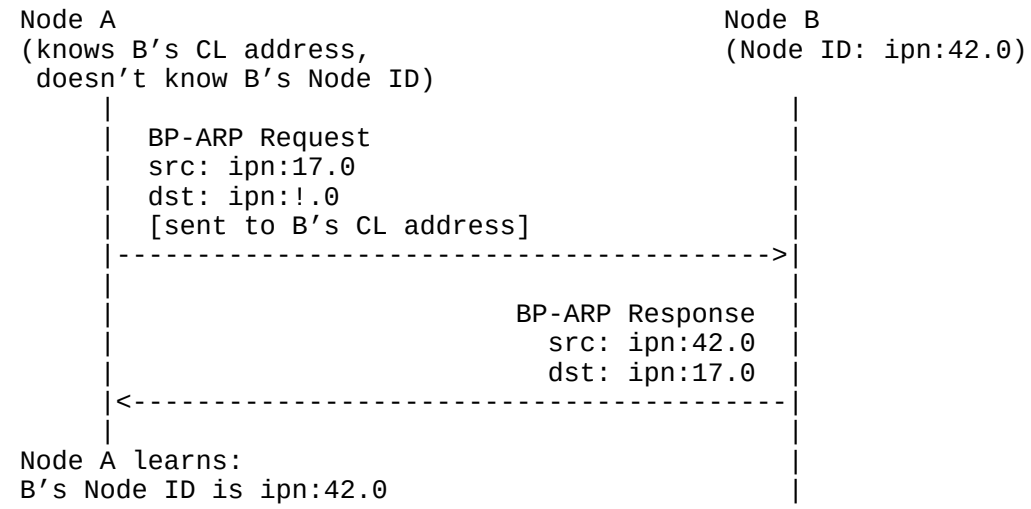
Peer: A remote BPA with a known Node ID and reachable via a known CL address.

Neighbour: A CL adjacency where the CL address is known but the Node ID is unknown.

Address Resolution: The process of discovering the Node ID(s) associated with a Neighbour’s CL address.

3. Protocol Overview

3.1. Message Flow



3.2. Addressing

BP-ARP uses IPN addressing exclusively for the probe mechanism. The ARP Request is sent to the LocalNode administrative endpoint ipn:!.0, and the BP-ARP Response source is the responding node's ipn-scheme Node ID (e.g., ipn:<node>.0). Nodes that do not support IPN addressing cannot participate in BP-ARP.

While the probe mechanism requires IPN addressing, the BP-ARP Response payload carries the complete set of Node IDs for the responding node, including dtn-scheme Node IDs (e.g., dtn://node42/) alongside ipn-scheme Node IDs (e.g., ipn:42.0). This enables discovery of all of a node's identities regardless of URI scheme, supporting dual-stack deployments.

3.2.1. RFC 9758 Constraint

[RFC9758], Section 3.4.2 defines LocalNode as Node Number 2^32-1 (0xFFFFFFFF), represented as ipn:!.<service> or ipn:4294967295.<service>.

However, [RFC9758], Section 5.4 states that "all externally received bundles featuring LocalNode EIDs as a bundle source or bundle destination MUST be discarded as invalid."

This means LocalNode (ipn:!.0) cannot be used as the destination for BP-ARP probes under current [RFC9758] rules. This specification updates [RFC9758] to relax this restriction for BP-ARP bundles; see Section 4.4 for the full specification.

4. Normative Specification

4.1. Administrative Record Type

BP-ARP uses a single Administrative Record type (TBD1) for both requests and responses. The bundle's destination EID distinguishes the two:

* A bundle destined to ipn:!.0 is a BP-ARP Request.

* A bundle destined to a node's own administrative endpoint is a BP-ARP Response.

This distinction is unambiguous: a receiving BPA always knows whether the bundle was addressed to LocalNode or to its own Node ID.

4.2. BP-ARP Request

A BP-ARP Request is a bundle with the following properties:

4.2.1. Primary Block

* Source EID: The requesting node's administrative endpoint (e.g., ipn:<node>.0).

* Destination EID: ipn:!.0 (LocalNode administrative endpoint).

* Bundle Processing Control Flags: Administrative record flag MUST be set.

4.2.2. Hop Count Extension Block

BP-ARP Request bundles SHOULD include a Hop Count extension block (block type 10, per [RFC9171], Section 4.3.3). The hop limit SHOULD be set to 1. This prevents the BP-ARP Request from being routed beyond the immediate neighbour.

4.2.3. Payload Block

The payload block contains an Administrative Record with type TBD1.

The payload content is either:

* Empty: requesting the complete set of Node IDs from the responding node.

* A CBOR array of already-known Node IDs: requesting only Node IDs not included in the list (a delta query).

The payload format is defined in Figure 1 using CDDL.

4.2.4. Transmission

The bundle MUST be sent via the CLA to the specific CL address of the Neighbour. The bundle MUST NOT be routed through normal RIB lookup. The Hop Count limit of 1 provides defence-in-depth against mis-routing.

4.3. BP-ARP Response

Upon receiving a BP-ARP Request, a BPA MUST respond with a BP-ARP Response.

4.3.1. Primary Block

* Source EID: The ipn-scheme Node ID of the responding node (e.g., ipn:<node>.0). This MUST NOT be ipn:!.0.

* Destination EID: The source EID from the BP-ARP Request.

* Bundle Processing Control Flags: Administrative record flag MUST be set.

4.3.2. Payload Block

The payload block contains an Administrative Record with type TBD1 (the same type as the request).

If the BP-ARP Request payload was empty, the response payload MUST contain a CBOR array of all Node IDs for the responding node, including Node IDs of all supported URI schemes (e.g., both ipn and dtn). If the BP-ARP Request payload contained a list of known Node IDs, the response payload MUST contain only those Node IDs not present in the request (the delta). If the requesting node already knows all Node IDs, the response payload is an empty CBOR array.

The response MUST contain only singleton Node IDs that uniquely identify the responding BPA. Multicast, anycast, or other group EIDs MUST NOT be included in the response payload.

The payload format is defined in Figure 1 using CDDL:

```
arp-payload = [* eid]
eid = $eid  ; As defined in RFC 9171 Section 4.2.5.1
```

Figure 1: BP-ARP Payload Format

An example response payload in CBOR diagnostic notation:

```
[
  [2, [1, 42, 0]],    / ipn:1.42.0 (3-element encoding) /
  [1, "//node42/"]    / dtn://node42/                   /
]
```

Figure 2: Example BP-ARP Response Payload

This example shows a node reporting both an ipn-scheme and a dtn-scheme Node ID, demonstrating dual-stack identity discovery.

4.3.3. Processing

The requesting node associates all Node IDs in the response with the Neighbour's CL address. The Neighbour is promoted to Peer with the discovered Node IDs. Routes MAY be installed for each discovered Node ID.

A response to a delta query is additive: the requesting node combines the previously known Node IDs with the newly received Node IDs.

4.4. LocalNode Address Handling

This section specifies the update to [RFC9758], Section 5.4.

A BPA implementing BP-ARP:

* MUST accept bundles destined to ipn:!.0 from external sources if:
  - The bundle is marked as an administrative record, AND
  - The administrative record type is BP-ARP (type TBD1).
* MUST validate that such bundles are properly formatted.
* MUST process valid BP-ARP Requests and generate BP-ARP Responses.
* SHOULD apply rate limiting to prevent denial-of-service attacks.
* MUST continue to discard other externally received LocalNode destination EIDs unless specifically permitted by a registered administrative record type.

4.5. BP-ARP Policy

A BPA SHOULD provide a configurable policy that controls whether and when BP-ARP resolution is performed. This allows administrators to select an appropriate trust model for their deployment (see Appendix A for example configurations).

5. Security Considerations

5.1. BPSec Authentication

BP-ARP bundles SHOULD be authenticated using BPSec Block Integrity Block (BIB) as defined in [RFC9172].

BP-ARP Request bundles SHOULD include a BIB targeting the payload block, with the requesting node's administrative endpoint as the security source. BP-ARP Response bundles SHOULD include a BIB targeting the payload block, with the responding node's administrative endpoint as the security source.

BP-ARP assumes that key material is pre-placed and identity is already established through out-of-band mechanisms. BP-ARP performs address resolution only — mapping a CL address to Node IDs. It does not establish trust relationships, exchange credentials, or perform identity bootstrapping. Deployments requiring credential exchange or identity verification SHOULD use SAND [I-D.ietf-dtn-bp-sand] after BP-ARP resolution.

5.2. Relaxation of LocalNode Rule

Accepting external bundles destined to ipn:!.0 introduces potential security risks:

Spoofing: A malicious node could send false BP-ARP Responses.

Denial of Service: Flooding with BP-ARP Requests could overwhelm a BPA.

Information Disclosure: BP-ARP Responses reveal a node's Node IDs.

Mitigations include BPSec BIB authentication (Section 5.1), rate limiting on BP-ARP Request processing, validation that BP-ARP Requests are properly formatted administrative records, and policy configuration to disable BP-ARP in sensitive environments.

5.3. Trust Model

The BP-ARP policy configuration allows administrators to choose appropriate trust levels for their deployment. For example, closed networks may disable BP-ARP entirely and trust only CLA-provided Node IDs, while open networks may use BP-ARP to resolve unknown neighbours. High-security deployments may choose to always verify, even when the CLA provides Node IDs.

6. IANA Considerations

6.1. Administrative Record Type

This document requests allocation of a new Bundle Protocol Administrative Record type from the "Bundle Administrative Record Types" registry:

Value	Description
TBD1	BP-ARP

Table 1

A single type is used for both requests and responses. The bundle's destination EID distinguishes the two: bundles destined to ipn:!.0 are requests; bundles destined to a node's own administrative endpoint are responses.

6.2. No Service Number Required

BP-ARP uses the existing administrative endpoint (ipn:X.0) and does not require allocation of a new service number.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC9171] Burleigh, S., Fall, K., and E. Birrane, III, "Bundle Protocol Version 7", RFC 9171, DOI 10.17487/RFC9171, January 2022, <https://www.rfc-editor.org/rfc/rfc9171>.

[RFC9172] Birrane, III, E. and K. McKeever, "Bundle Protocol Security (BPSec)", RFC 9172, DOI 10.17487/RFC9172, January 2022, <https://www.rfc-editor.org/rfc/rfc9172>.

[RFC9758] Taylor, R. and E. Birrane III, "Updates to the 'ipn' URI Scheme", RFC 9758, DOI 10.17487/RFC9758, May 2025, <https://www.rfc-editor.org/rfc/rfc9758>.

7.2. Informative References

[I-D.ietf-dtn-bp-sand] Sipos, B. and J. Deaton, "Bundle Protocol (BP) Secure Advertisement and Neighborhood Discovery (SAND)", Work in Progress, Internet-Draft, draft-ietf-dtn-bp-sand-02, 18 December 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-dtn-bp-sand-02>.

[RFC9174] Sipos, B., Demmer, M., Ott, J., and S. Perreault, "Delay-Tolerant Networking TCP Convergence-Layer Protocol Version 4", RFC 9174, DOI 10.17487/RFC9174, January 2022, <https://www.rfc-editor.org/rfc/rfc9174>.

Appendix A. Policy Configuration

The decision to perform BP-ARP resolution is a BPA configuration option, not a CLA implementation choice. The following table illustrates example policy settings:

Policy	Behavior
as-needed	Only probe if CLA provides no Node IDs (default)
always	Always probe, verify/augment CLA-provided Node IDs
never	Trust CLA, fail if no Node IDs provided

Table 2

This separation ensures:

* CLAs report facts (what they learned from the CL layer).

* Administrators configure policy (trust model for deployment).

* The BP-ARP subsystem executes the configured policy.

Appendix B. CLA Interface

CLAs report discovered adjacencies to the BPA. A CLA provides:

* The CL address of the discovered adjacency.

* Zero or more Node IDs, if the CLA learned them from the CL layer.

When the Node ID list is empty, the CLA has discovered CL adjacency but does not know the Node ID (Neighbour). When the list is non-empty, the CLA has learned one or more Node IDs, which may be incomplete due to CL protocol limitations. For example, TCPCLv4 [RFC9174] exchanges a single Node ID during contact header negotiation; a node with additional Node IDs in other URI schemes cannot advertise them through TCPCLv4 alone.

Multi-homing is supported: a single CL address may be associated with multiple Node IDs.

Appendix C. Implementation Notes

C.1. Integration with BPA

The BP-ARP subsystem integrates with the BPA as follows:

1. CLA reports a new adjacency, optionally with a Node ID learned from the CL layer.

2. BPA checks BP-ARP policy configuration.

3. If policy requires probing, the BP-ARP subsystem sends a Request to ipn:!.0 via the CLA. If a Node ID is already known, it may be included in the request payload as a delta query.

4. The BP-ARP subsystem receives a Response and extracts the Node ID from the source field and any additional Node IDs from the payload.

5. The Neighbour is promoted to Peer with all discovered Node IDs.

6. The Routing Information Base (RIB) is updated with routes to the new Peer.

C.2. Generic Implementation

BP-ARP is implemented generically in the BPA core, not per-CLA:

* The discovery probe is a BP-layer bundle (CL-agnostic).
* The CLA provides "send to CL address" capability.
* The BP-ARP subsystem orchestrates the resolution process.
* No duplicate resolution logic is needed in each CLA.

Acknowledgments

Thanks are due to Erik Kline and Brian Sipos of early review and discussion.

Author’s Address

Rick Taylor
Aalyria Technologies
Email: rtaylor@aalyria.com