Workgroup:
Delay/Disruption Tolerant Networking
Internet-Draft: draft-ietf-dtn-ipn-update-01
Updates: [9171, 7176] (if approved)
Published: 13 March 2023
Intended Status: Standards Track
Expires: 14 September 2023
Authors: R. Taylor E. Birrane
Ori Industries JHU/APL

Update to the ipn URI scheme

Abstract

This document updates both the specification of the ipn URI scheme previously defined in [RFC7116] and the rules for encoding of these URIs when used as an Endpoint Identifier (EID) in Bundle Protocol Version 7 (BPv7) as defined in [RFC9171]. These updates update and clarify the structure and behavior of the ipn URI scheme, define encodings of ipn scheme URIs, and establish the registries necessary to manage this scheme.

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/ipn2/draft-taylor-dtn-ipn-update.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-dtn-ipn-update/.

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/ipn2.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction
2. Conventions and Definitions
3. The ipn URI scheme
  3.1. Numbering Authorities
    3.1.1. The Default Numbering Authority
    3.1.2. Numbering Authority Identification
    3.1.3. Authority Number Ranges
  3.2. Node Numbers
  3.3. Service Numbers
4. Usage of ipn URIs with BPv7
  4.1. Uniqueness Constraints
  4.2. The Node ID
  4.3. Special Node Numbers
    4.3.1. The Null Endpoint
    4.3.2. Localnode Endpoints
    4.3.3. "Private Use" Endpoints
  4.4. Service Number Constraints
    4.4.1. Administrative Endpoints
5. Encoding ipn URIs with BPv7
  5.1. ipn EID CBOR Encoding
    5.1.1. Two-Element Scheme-Specific Encoding
    5.1.2. Three-Element Scheme-Specific Encoding
  5.2. ipn EID CBOR Decoding
  5.3. ipn EID Matching

6. Special Considerations
  6.1. Scheme Compatibility
  6.2. Late Binding
7. Security Considerations
  7.1. Reliability and consistency
  7.2. Malicious construction
  7.3. Back-end transcoding
  7.4. Rare IP address formats
  7.5. Sensitive information
  7.6. Semantic attacks
8. IANA Considerations
  8.1. 'ipn' Scheme URI Numbering Authority Identifiers registry
    8.1.1. Guidance for Designated Experts
  8.2. 'ipn' Scheme URI Default Numbering Authority Node Numbers registry
  8.3. 'ipn' Scheme URI Service Numbers registry
9. References
  9.1. Normative References
  9.2. Informative References
Appendix A. ipn URI Scheme Text Syntax
Appendix B. CBOR Encoding
Appendix C. Encoding Examples
  C.1. Using the Default Numbering Authority
  C.2. Using a non-default Numbering Authority
  C.3. The 'null' Endpoint
Acknowledgments
Authors' Addresses

1. Introduction

The ipn URI scheme was originally defined in [RFC7116] as a way to identify network nodes and node services using concisely-encoded integers that can be processed faster and with fewer resources than other verbose identifier schemes. The scheme was designed for use with the experimental Bundle Protocol version 6 (BPv6, [RFC5050]) and IPN was defined as an acronym for the term "InterPlanetary Network" in reference to its intended use for deep-space networking. Since then, the efficiency benefit of integer identifiers makes ipn scheme URIs useful for any networks operating with limited power, bandwidth, and/or compute budget. Therefore the term IPN is now used as a non-acronymous name.

Similar to the experimental BPv6, the standardized Bundle Protocol version 7 (BPv7, [RFC9171]) codifies support for the use of the ipn URI scheme for the specification of bundle Endpoint Identifiers (EIDs). The publication of BPv7 has resulted in operational deployments of BPv7 nodes for both terrestrial and non-terrestrial use cases. This includes BPv7 networks operating over the terrestrial Internet and BPv7 networks operating in self-contained environments behind a shared administrative domain. The growth in the number and scale of deployments of BPv7 DTNs has been accompanied by a growth in the usage of the ipn URI scheme which has highlighted areas to improve the structure, moderation, and management of this scheme.

This document updates the specification of the ipn URI scheme, in a backwards-compatible way, to provide needed improvements both in the scheme itself and its usage to specify EIDs with BPv7. Specifically, this document introduces a hierarchical structure for the assignment of ipn scheme URIs, clarifies the behavior and interpretation of ipn scheme URIs, defines efficient encodings of ipn scheme URIs, and updates/defines the registries associated for this scheme.

2. Conventions and Definitions

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.

3. The ipn URI scheme

All ipn scheme URIs comply with [RFC3986], and are therefore represented by scheme identifier, and a scheme-specific part. The scheme identifier is: ipn, and the scheme-specific parts are represented as a sequence of numeric components separated with the '.' character. It is formally defined in Appendix A (Appendix A), and can be informally considered as:

```
ipn:authority-number.node-number.service-number
```

Working from left-to-right, each component has the following definition:

- *authority-number: The "Authority Number" of the authority that allocated the subsequent Node Number. See Numbering Authorities (Section 3.1).

- *node-number: The "Node Number" assigned to all ipn scheme URIs for resources co-located on a single node. See Node Numbers (Section 3.2).

- *service-number: The "Service Number" of a particular type of service for a resource. See Service Numbers (Section 3.3).

When considered from the perspective of BPv7, a Node Number is shared by all endpoints co-located on a single bundle processing node, and a Service Number identifies a certain type of bundle processing service.

For the remainder of this document the term "ipn URI" is used to refer to a URI that uses the ipn scheme.

3.1. Numbering Authorities

A "Numbering Authority" (NA) is any organization (e.g., vendor, manufacturer, or other entity) that wishes to assign Node Numbers for use with the ipn URI scheme. The authorization to assign these numbers is provided through the inclusion of the NA in a controlled registry of ipn URI scheme NAs (Section 8.1).

The use of NAs with the ipn URI scheme reduces the administrative burden of ensuring the uniqueness of Node Numbers. Each NA is responsible for ensuring that any Node Numbers it allocates are unique. However, Node Numbers assigned by other NAs do not otherwise need to be coordinated or synchronized.

3.1.1. The Default Numbering Authority

As of the publication of [RFC7116], the only organization permitted to assign Node Numbers was the Internet Assigned Numbers Authority (IANA) which assigned Node Numbers through the IANA "CBHE Node Numbers" registry. This means that all ipn URIs created prior to the addition of Numbering Authorities are assumed to have Node Number allocations that comply with the IANA "CBHE Node Numbers" registry.

The presumption that, unless otherwise specified, Node Numbers are allocated by IANA from a specific registry is formalized in this updated ipn URI scheme by designating IANA as the "Default Numbering Authority". In any case where an ipn URI does not explicitly identify a Numbering Authority, an implementation **MUST** assume that the Node Number has been allocated by the Default Numbering Authority.

To formalize IANA as the Default NA, a new IANA "'ipn' Scheme URI Default Authority Node Numbers" registry is defined to control the allocation of Node Numbers values by the Default NA. This new registry inherits behaviours and existing assignments from the IANA "CBHE Node Numbers" registry, reserves the value zero (0), and assigns values in the range [1 .. 2^14-1] as "Private Use", as defined in [RFC8126].

3.1.2. Numbering Authority Identification

Regardless of other attributes of a NA, such as a name, point of contact, or other identifying information, NAs are identified by

Authority Numbers. An Authority Number is a unique, unsigned integer with a minimum value of zero (0).

The use of this identifier allows a Numbering Authority to allocate Node Numbers according to it's own policies, without risk of creating an identical ipn URI, as permitted by the rules in the Node Numbers (Section 3.2) section of this document. The Authority Number **MUST** be the sole mechanism used to differentiate between NAs.

A single NA may have multiple Authority Numbers assigned to it, but a given Authority Number **MUST** only be associated with a single NA.

A new IANA "'ipn' Scheme URI Authority Numbers" registry is defined for the registration of NAs, see IANA Considerations (Section 8). Although the uniqueness of Authority Numbers is required to enforce uniqueness of ipn URIs, identifier ranges are explicitly reserved for experimentation. Authority numbers greater than 2^32-1 are Reserved and **MUST NOT** be used.

3.1.3. Authority Number Ranges

Some organizations with internal hierarchies may wish to delegate the allocation of Node Numbers to one or more of their sub-organizations. Rather than allocating unique Authority Numbers to each sub-organization on a first-come first-served basis, there are operational benefits in allocating Authority Numbers to a single organization in a structured way so that an external observer can detect that a series of Authority Numbers are organizationally associated.

An Authority Number Range (ANR) is a set of consecutive Authority Numbers that are all associated with the same NA. Each individual Authority Number in a given range **SHOULD** be allocated to a distinct sub-organization of the NA. Allocating numbers in this way allows external observers to both associate individual Authority Numbers with a single organization and to usefully differentiate amongst sub-organizations.

The practice of associating a consecutive range of numbers with a single organization is inspired by the Classless Inter-domain Routing assignment of Internet Addresses described in [RFC4632]. In that assignment scheme, an organization (such as an Internet Service Provider) is assigned a network prefix such that all addresses sharing that same prefix are considered to be associated with that organization.

Each ANR is identified by the first Authority Number in the range and the number of consecutive numbers in the range. Every number in an ANR **MUST** be a valid Authority Number, meaning that the number must be no larger than a 32-bit unsigned integer.

ANRs differ from CIDR addresses in several important ways.

1. Authority Numbers are used to identify organizations and are not, themselves, addresses.

2. Authority Numbers may be less than 32 bits in length.

An example of the use of ANRs would be three organizations: A, B, and C.

Organization	Range Length (Bits)	Range (dec)	Range (hex)
Org A	7 bits	36864-36991	0x9000-0x907F
Org B	4 bits	36992-37007	0x9080-0x908F
Org C	1 bits	37008-37010	0x9090-0x9092

Table 1: ANR Example Allocation

With these allocations, any Authority Number whose most-significant 25 bits match 0x9000 belong to organization A. Similarly, any Authority Number whose most-significant 28 bits match 0x9080 belong to organization B and any Authority Number whose most-significant 31 bits are 0x9090 belong to organization C.

3.2. Node Numbers

A "Node Number" identifies a resource in the context of a Numbering Authority. A Node Number is an unsigned integer with a minimum value of zero (0) and a maximum value of 2^32-1.

A Node Number is associated with a Numbering Authority when both the Authority Number and Node Number appear together in an ipn URI. If an Authority Number is omitted from an ipn URI then it **MUST** be assumed that the Node Number has been allocated by the Default Numbering Authority.

A single Node Number allocated by a single Numbering Authority **MUST** refer to a single network node.

3.3. Service Numbers

A "Service Number" identifies a network service operating on a network node. The purpose of the Service Number is to provide unique, numeric identifiers for types of service in a network. A Service Number is an unsigned integer with a minimum value of zero (0) and a maximum value of 2^64-1.

A new IANA "'ipn' Scheme URI Service Numbers" registry is defined for the registration of Service Numbers, see IANA Considerations (Section 8). This registry defines standardized Service Numbers for services such as an administrative or well-known protocol service endpoints. This registry also defines ranges explicitly reserved for both experimentation and ad-hoc service identification.

4. Usage of ipn URIs with BPv7

From the earliest days of experimentation with the Bundle Protocol there has been a need to identify the source and destination of a bundle. The IRTF standardisation of the experimental BPv6 termed the logical source or destination of a bundle as an "Endpoint" identified by an "Endpoint Identifier" (EID). BPv6 EIDs are formatted as URIs. This definition and representation of EIDs was carried from the IRTF BPv6 specification to the IETF BPv7 specification. BPv7 additionally defined an IANA registry called the "Bundle Protocol URI Scheme Types" registry which identifies those URI schemes than might be used to represent EIDs. The ipn URI scheme is one such URI scheme.

This section identifies the behavior and interpretation of ipn URI schemes that **MUST** be followed when using this URI scheme to represent EIDs in BPv7. An ipn URI used as a BPv7 or BPv6 EID is termed an "ipn EID".

4.1. Uniqueness Constraints

An ipn EID **MUST** identify a singleton endpoint. The bundle processing node that is the sole member of that endpoint **MUST** be the node identified by the combination of the Authority Number and Node Number.

A single bundle processing node **MAY** have multiple ipn EIDs associated with it. However, every ipn EID that shares the combination of Authority Number and Node Number **MUST** refer to the same bundle processing node.

For example, "ipn:1.100.1", "ipn:1.100.2", and "ipn:1.100.3" **MUST** all be registered on the bundle processing node identified by "1.100". None of these EIDs could be registered on any other bundle processing node.

4.2. The Node ID

Section 4.2.5.3 of [RFC9171] introduces the concept of a "Node ID" that uniquely identifies a bundle processing node. Any EID that can be used to unambiguously identify a bundle processing node can be used as a "Node ID".

As all ipn EIDs must be singleton endpoints, any ipn EID **MAY** serve as a "Node ID".

4.3. Special Node Numbers

Some special-case Node Numbers and EIDs are required for the correct behaviour of BPv7, and these numbers are taken from the ANR of the Default Numbering Authority, as defined in the 'ipn' Scheme URI Default Authority Node Numbers registry (Section 8.2).

4.3.1. The Null Endpoint

Section 3.2 of [RFC9171] defines the concept of the 'null' endpoint, which is an endpoint that has no members and which is identified by a special 'null' EID.

Within the ipn URI scheme, the 'null' EID is defined by the Default Numbering Authority and has the value zero (0) for the 'node-number' component and the value zero (0) for the 'service-number' component. The textual expression of this EID is "ipn:0.0".

The Default Numbering Authority reserves the use of Node Number zero (0) solely for identifying the 'null' EID. This means that any other ipn EID which uses the Default Numbering Authority, and has the value zero (0) for the node-number component but a non-zero service-number component **MUST** be considered malformed and **MUST NOT** be used to represent any BPv7 EID.

4.3.2. Localnode Endpoints

The Default Numbering Authority reserves Node Number one (1) to specify endpoints on the local node, rather than on any specific individual node. This means that any ipn EID of the form "ipn:1.X" refers to service X on the local bundle node. EIDs of this form are termed "localnode EIDs".

Because a localnode EID only has meaning on the local bundle node, any such EID **MUST** be considered 'non-routeable'. This means that any bundle using a localnode EID as a bundle source or bundle destination **MUST NOT** be allowed to leave the local node. Similarly, localnode EIDs **SHOULD NOT** be present in any other part of a bundle that is transmitted off of the local node. For example, a localnode EID **SHOULD NOT** be used as a Bundle Protocol Security [RFC9172] security source EID for a bundle transmitted off of the local bundle node, because such a source EID would have no meaning at a downstream bundle node.

4.3.3. "Private Use" Endpoints

The Default Numbering Authority provides a range of Node Numbers that are reserved for "Private Use".

Any ipn EID whose Node Number is one reserved for "Private Use" is not guaranteed to be unique. Bundles destined for such EIDs must be considered 'non-routeable' to the extent that they **MUST NOT** be permitted to exit a single administrative domain. They can be considered to be equivalent to "Private Address Space" IPv4 addresses, as defined in [RFC1918]. An administrative domain, as used here, is defined as the set of nodes that share a unique allocation of Node Numbers from the "Private Use" range.

4.4. Service Number Constraints

The following constraints are placed on the Service Numbers used with ipn EIDs. These constraints are imposed independent of the Numbering Authority or Node Number of an ipn EID.

4.4.1. Administrative Endpoints

The service type identified by a Service Number of zero (0) **MUST** be interpreted as the administrative endpoint of the node, as defined in Section 3.2 of [RFC9171].

Non-zero Service Numbers **MUST NOT** be used to identify the administrative endpoint of a bundle node in an ipn EID.

5. Encoding ipn URIs with BPv7

Section 4.2.5.1 of [RFC9171] requires that any URI scheme used to represent BPv7 EIDs **MUST** define how the scheme-specific part of the URI scheme is CBOR encoded. To meet this requirement, this section describes the CBOR encoding and decoding approach for ipn EIDs. The formal definition of these encodings is presented in Appendix B (Appendix B).

While there is a single, canonical, textual representation of an ipn URI, there may exist multiple encodings for that URI. For example, Section 2.1 of [RFC3986] defines a percent-encoding mechanism for a URI text string. Alternatively, Section 3.4.5.3 of [RFC8949] allows for the encoding of URIs as CBOR text strings identified with a CBOR tag value of 32.

5.1. ipn EID CBOR Encoding

Generic URI approaches to encoding ipn EIDs are unlikely to be efficient because they do not consider the underlying structure of the ipn URI scheme. Since the creation of the ipn URI scheme was motivated by the need for concise identification and rapid processing, the encoding of ipn EIDs should maintain these properties.

Fundamentally, [RFC9171] ipn EIDs are represented as a sequence of identifiers. In the text syntax, the numbers are separated with the '.' delimiter; in CBOR, this ordered series of numbers can be represented by an array. Therefore, when encoding ipn EIDs for use with BPv7, the scheme-specific part of an ipn URI **MUST** be represented as a CBOR array of either two (2) or three (3) elements. Each element of the array **MUST** be encoded as a single CBOR unsigned integer.

The structure and mechanisms of the two-element and three-element encodings are described below, and examples of the different encodings are provided in Appendix C (Appendix C).

5.1.1. Two-Element Scheme-Specific Encoding

In the two-element scheme-specific encoding of an ipn EID, the first element of the array is a numeric representation of the concatenation of the Authority Number and the Node Number of the ipn EID and the second element of the array is the ipn EID Service Number.

The first array element for this encoding **MUST** be a 64 bit unsigned integer constructed in the following way: 1. The least significant 32 bits **MUST** represent the Node Number associated with the ipn EID. 1. The most significant 32 bits **MUST** represent the Authority Number associated with the ipn EID.

For example the ipn EID of "ipn:1.100.1" would compute the first array element value as 0x0100000064. The resulting two-element array [0x0100000064, 0x01] would be encoded in CBOR as the 11 octet value 0x821B000000010000006401.

The two-element scheme-specific encoding provides for backwards compatibility with the encoding provided in Section 4.2.5.1.2 of [RFC9171]. When used in this way, the numeric representation of the concatenation of the Authority Number and the Node Number defined in this document replaces the use of the "Node Number" that was specified in RFC9171. When the Node Number is allocated by the Default Numbering Authority, then the numeric representation and the use of the "Node Number" in RFC9171 are identical.

This encoding scheme **MUST** be implemented by any BPv7 bundle processing node that supports ipn URIs for the specification of BPv7 EIDs.

5.1.2. Three-Element Scheme-Specific Encoding

In the three-element scheme-specific encoding of an ipn EID, the first element of the array is the Authority Number, the second element of the array is Node Number, and the third element of the array is the Service Number.

For example, the ipn EID of "ipn:1.100.1" would result in the three-element array of [1,100,1] which would be encoded in CBOR as the 5 octet value 0x8301186401.

The three-element scheme-specific encoding allows for a more efficient representation of ipn EIDs using smaller Authority Numbers. In the examples in Appendix C (Appendix C), the two-element encoding of "ipn:1.100.1" was more then double the size of the three-element encoding.

When encoding an ipn EID using the Default Numbering Authority with this encoding scheme, the first element of the array **MUST** be the value zero (0). In this case using the two-element encoding will result in a more concise CBOR representation, and it is **RECOMMENDED** that implementations do so.

5.2. ipn EID CBOR Decoding

The presence of different scheme-specific encodings does not introduce any decoding ambiguity.

An ipn EID CBOR decoder can reconstruct an ipn EID using the following logic. In this description, the term "enc_eid" refers to the CBOR encoded ipn EID, and the term "ipn_eid" refers to the decoded ipn EID.

```
if enc_eid.len() == 3
{
  ipn_eid.authority-number := enc_eid[0];
  ipn_eid.node-number := enc_eid[1];
  ipn_eid.service-number := enc_eid[2];
}
else if enc_eid.len() == 2
{
  N = enc_eid[0];
  ipn_eid.service-number := enc_eid[1];

  if N >= 2^32
  {
    ipn_eid.authority-number := N >> 32;
    ipn_eid.node-number := N & (2^32-1);
  }
  else
  {
    ipn_eid.authority-number := 0;
    ipn_eid.node-number := N;
  }
}
```

5.3. ipn EID Matching

Regardless of whether the two-element or three-element scheme-specific encoding is used, ipn EID matching **MUST** be performed on the decoded EID information itself. Different encodings of the same ipn EID **MUST** be treated as equivalent when performing EID-specific functions.

For example, the ipn EID of "ipn:1.100.1" can be represented as either the two-element encoding of 0x821B000000010000006401 or the three-element encoding of 0x8301186401. While message integrity and other syntax-based checks may treat these values differently, any EID-based comparisons **MUST** treat these values the same - as representing the ipn EID "ipn:1.100.1".

6. Special Considerations

The ipn URI scheme provides a compact and hierarchical mechanism for identifying services on network nodes. There is a significant amount of utility in the ipn URI scheme approach to identification. However, implementers should take into consideration the following observations on the use of the ipn URI scheme.

6.1. Scheme Compatibility

The ipn scheme update that has been presented in this document preserves backwards compatibility with any ipn URI scheme going back to the provisional definition of the ipn scheme in the experimental Compressed Bundle Header Encoding [RFC6260] in 2011. This means that ipn URI that was valid prior to the publication of this update remains a valid ipn URI.

Similarly, the two-element scheme-specific encoding (Section 5.1.1) is also backwards compatible with the encoding of ipn URIs provided in [RFC9171]. Any existing BPv7-compliant implementation will produce an ipn URI encoding in compliant with this specification.

The introduction of optional non-default numbering authorities and a three-element scheme-specific encoding make this ipn URI scheme update not forwards compatible. Existing software **MUST** be updated to be able to process non-default numbering authorities and three-element scheme-specific encodings. It is **RECOMMENDED** that BP implementations upgrade to process these new features to benefit from the scalability provided by numbering authorities and the encoding efficiencies provided by the three-element encoding.

6.2. Late Binding

[RFC9171] mandates the concept of "late binding" of an EID, where-by the address of the destination of a bundle is resolved from its identifier hop by hop as it transits a DTN. This per-hop binding of identifiers to addresses underlines the fact that EIDs are purely names, and should not carry any implicit or explicit information concerning the current location or reachability of an identified node and service. This removes the need to rename a node as its location changes.

The concept of "late binding" is preserved in this ipn URI scheme. Elements of an ipn URI **SHOULD NOT** be regarded as carrying information relating to location, reachability, or other addressing/routing concern.

An example of incorrect behaviour would be to assume that a given Numbering Authority always allocated Node Numbers as link-layer addresses and to then use the node-number component of an ipn URI directly as a link-layer address. No matter the mechanism a Numbering Authority uses for the allocation of Node Numbers, they remain just numbers, without additional meaning.

7. Security Considerations

This update to the IPN URI scheme does not change the security considerations for this scheme presented in [RFC9171]. This section repeats the security considerations from Section 4.2.5.1.2 of [RFC9171] here for completeness.

7.1. Reliability and consistency

None of the BP endpoints identified by ipn EIDs are guaranteed to be reachable at any time, and the identity of the processing entities operating on those endpoints is never guaranteed by the Bundle Protocol itself. Verification of the signature provided by the Block Integrity Block targeting the bundle's primary block, as defined by Bundle Protocol Security [RFC9172], is required for this purpose.

7.2. Malicious construction

Malicious construction of a conformant ipn URI is limited to the malicious selection of Node Numbers and the malicious selection of Service Numbers. That is, a maliciously constructed ipn URI could be used to direct a bundle to an endpoint that might be damaged by the arrival of that bundle or, alternatively, to declare a false source for a bundle and thereby cause incorrect processing at a node that receives the bundle. In both cases (and indeed in all bundle processing), the node that receives a bundle should verify its authenticity and validity before operating on it in any way.

7.3. Back-end transcoding

The limited expressiveness of URIs of the ipn scheme effectively eliminates the possibility of threat due to errors in back-end transcoding.

7.4. Rare IP address formats

Not relevant, as IP addresses do not appear anywhere in conformant ipn URIs.

7.5. Sensitive information

Because ipn URIs are used only to represent the identities of Bundle Protocol endpoints, the risk of disclosure of sensitive information due to interception of these URIs is minimal. Examination of ipn URIs could be used to support traffic analysis; where traffic analysis is a plausible danger, bundles should be conveyed by secure convergence-layer protocols that do not expose endpoint IDs.

7.6. Semantic attacks

The simplicity of ipn URI scheme syntax minimizes the possibility of misinterpretation of a URI by a human user.

8. IANA Considerations

The following sections detail requests to IANA for the creation of a new registry, and the renaming of two existing registries.

8.1. 'ipn' Scheme URI Numbering Authority Identifiers registry

IANA is requested to create a new registry entitled "'ipn' Scheme URI Numbering Authority Identifiers"

The registration policy for this registry is:

Range	Registration Policy
0 .. 4095	Expert Review
4096 .. 2^16-1	First-come first-served for allocations of length < 256, otherwise Expert Review
2^16 .. 2^32-1	First-come first-served for allocations of length < 65536, otherwise Expert Review
>= 2^32	Reserved

Table 2: 'ipn' Scheme URI Numbering Authority Identifiers registration policies

Values may be allocated in blocks. Any values allocated in blocks **MUST** have the first number of the block be a power of 2 and the number of allocations in the block **MUST** also be a power of 2.

The initial values for the registry are:

Value	Description	Reference
0	Default Numbering Authority	This document
1	Allocated to [CCSDS]	To be defined - pre-allocated as a courtesy, as they have a long-standing existing allocation in Section 3.2.1 of [RFC7116]

Table 3: 'ipn' Scheme URI Authority Numbers initial values

8.1.1. Guidance for Designated Experts

New assignments within this registry require review by a Designated Expert (DE). This section provides guidance to the DE when performing their reviews. Specifically, a DE is expected to perform the following activities.

1. Determine that the requesting Numbering Authority will reasonably provide operational Node Numbers for itself or others beyond that which is already provided by the Default Numbering Authority.

2. Ensure that the requesting Numbering Authority represents an organization and not an individual.

3. Ensure that the requesting Numbering Authority does not already provide the same Node Numbers under the auspices of some other registered Numbering Authority (except in the cases of allocating a block of identifiers).

4. Ensure that any block of contiguous identifiers allocated to a single Numbering Authority has its first identifier given as a power of 2 and that the length of the identifiers allocated is also a power of 2. This allows the block allocation to be bit-masked.

8.2. 'ipn' Scheme URI Default Numbering Authority Node Numbers registry

IANA is request to rename the "CBHE Node Numbers" registry defined in Section 3.2.1 of [RFC7116] to the "'ipn' Scheme URI Default Numbering Authority Node Numbers" registry.

The registration policy for this registry is updated to be:

Range	Registration Policy
0	Reserved for Null Endpoint
1	Reserved for Localnode
2 .. 2^14-1	Private Use
2^14 .. 2^32-1	Expert Review
>= 2^32	Reserved

Table 4: 'ipn' Scheme URI Default Authority Node Numbers registration policies

The initial values for the registry remain as is, namely:

Value	Hex	Description	Reference
16384-2097151	0x4000-0x1FFFFF	Allocated to the Space Assigned Numbers Authority (SANA) for use by Consultative Committee for Space Data Systems (CCSDS) missions.	Inherited from [RFC7116]
268435456-268451839	0x10000000-0x10003FFF	Allocated to Spacely	Scott Johnson - see

Value	Hex	Description	Reference
		Packets, LLC to provide IPN/IP Gateway services to private sector stakeholders.	existing allocation in CBHE Node Numbers registry.
268451840-268468223	0x10004000-0x10007FFF	Allocated to SPATIAM CORPORATION to provide DTN services to organizations.	Alberto Montilla - see existing allocation in CBHE Node Numbers registry.

Table 5: 'ipn' Scheme URI Default Authority Node Numbers initial values

8.3. 'ipn' Scheme URI Service Numbers registry

IANA is requested to rename the "CBHE Service Numbers" registry defined in Section 3.2.2 of [RFC7116] to the "'ipn' Scheme URI Service Numbers" registry.

The registration policy for this registry is updated to be:

Range	Registration Policy
0 .. 23	RFC Required
24 .. 4095	Specification Required
4096 .. 2^64-1	Private Use
>= 2^64	Reserved

Table 6: 'ipn' Scheme URI Service Numbers registration policies

The current values for the registry remain, and are rewritten as:

Value	Version	Description	Reference
0	BPv6, BPv7	The Administrative Endpoint	[RFC7116], This document
1	BPv6	CCSDS File Delivery Service	CCSDS 727.0-B-4
2	BPv6	Reserved	[RFC7116]
2	BPv7	Unassigned	
3 .. 63	BPv6, BPv7	Unassigned	
64 .. 1023	BPv6	Allocated to the Space Assigned Numbers Authority (SANA) for use by Consultative Committee for	[RFC7116]

Value	Version	Description	Reference
		Space Data Systems (CCSDS) missions	
64 .. 1023	BPv7	Unassigned	

Table 7: 'ipn' Scheme URI Service Numbers initial values

9. References

9.1. 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>.

[RFC5050] Scott, K. and S. Burleigh, "Bundle Protocol Specification", RFC 5050, DOI 10.17487/RFC5050, November 2007, <https://www.rfc-editor.org/rfc/rfc5050>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/rfc/rfc5234>.

[RFC7116] Scott, K. and M. Blanchet, "Licklider Transmission Protocol (LTP), Compressed Bundle Header Encoding (CBHE), and Bundle Protocol IANA Registries", RFC 7116, DOI 10.17487/RFC7116, February 2014, <https://www.rfc-editor.org/rfc/rfc7116>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/rfc/rfc8126>.

[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>.

[RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <https://www.rfc-editor.org/rfc/rfc8610>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/

RFC8949, December 2020, <https://www.rfc-editor.org/rfc/rfc8949>.

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

9.2. Informative References

[CCSDS] "The Consultative Committee for Space Data Systems", <http://www.ccsds.org>.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <https://www.rfc-editor.org/rfc/rfc1918>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/rfc/rfc3986>.

[RFC4632] Fuller, V. and T. Li, "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan", BCP 122, RFC 4632, DOI 10.17487/RFC4632, August 2006, <https://www.rfc-editor.org/rfc/rfc4632>.

[RFC6260] Burleigh, S., "Compressed Bundle Header Encoding (CBHE)", RFC 6260, DOI 10.17487/RFC6260, May 2011, <https://www.rfc-editor.org/rfc/rfc6260>.

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

Appendix A. ipn URI Scheme Text Syntax

The text syntax of an ipn URI **MUST** comply with the following ABNF [RFC5234] syntax, including the core ABNF syntax rule for DIGIT defined by that specification:

```
ipn-uri = "ipn:" ipn-hier-part

ipn-hier-part = auth-part? node-number "." service-number

auth-part = authority-number "."

authority-number = non-zero-number

node-number = number

service-number = number

number = "0" \ non-zero-number

non-zero-number = (%x31-39 *DIGIT)
```

The ABNF above explicitly states:

- The authority-number component **MUST NOT** be zero ('0').
- Additional leading zeros ('0') **MUST NOT** appear as part of any component.

Appendix B. CBOR Encoding

A BPv7 endpoint identified by an ipn URI, when encoded in Concise Binary Object Representation (CBOR) [RFC8949], **MUST** comply with the following Concise Data Definition Language (CDDL) [RFC8610] specification:

```
eid = $eid .within eid-structure

eid-structure = [
  uri-code: uint,
  SSP: any
]

; ... Syntax for other uri-code values defined in RFC9171 ...

$eid /= [
  uri-code: 2,
  SSP: [
    ? authority-number: uint,
    node-numeral: uint,
    service-number: uint
  ]
]
```

Note: The node-numeral component will be the numeric representation of the concatenation of the Authority Number and Node Number when the 2-element encoding scheme has been used.

Appendix C. Encoding Examples

This section provides some example encodings of ipn EIDs.

C.1. Using the Default Numbering Authority

Consider the ipn EID "ipn:1.1". This textual representation of an ipn EID identifies Service Number 1 on Node Number 1 allocated by the Default Numbering Authority.

The complete five octet encoding of this EID using the two-element scheme-specific encoding would be as follows.

```
82       # 2-Element Endpoint Encoding
   02    # uri-code: 2 (IPN URI scheme)
   82    # 2 Element ipn EID scheme-specific encoding
      01 # Node Number
      01 # Service Number
```

The complete six octet encoding of this EID using the three-element scheme-specific encoding would be as follows.

```
82       # 2-Element Endpoint Encoding
   02    # uri-code: 2 (IPN URI scheme)
   83    # 3 Element ipn EID scheme-specific encoding
      00 # Default Numbering Authority
      01 # Node Number
      01 # Service Number
```

C.2. Using a non-default Numbering Authority

Consider the ipn EID "ipn:100.1.1". This textual representation of an ipn EID identifies Service Number 1 on Node Number 1 allocated by Numbering Authority 100.

The complete thirteen octet encoding of this EID using the two-element scheme-specific encoding would be as follows.

```
82                       # 2-Element Endpoint Encoding
   02                    # uri-code: 2 (IPN URI scheme)
   82                    # 2 Element ipn EID scheme-specific encoding
      1B 0000006400000001 # Authority Number/Node Number numeral
      01                 # Service Number
```

The complete seven octet encoding of this EID using the three-element scheme-specific encoding would be as follows.

```
82          # 2-Element Endpoint Encoding
   02       # uri-code: 2 (IPN URI scheme)
   83       # 3 Element ipn EID scheme-specific encoding
      18 64 # Numbering Authority
      01    # Node Number
      01    # Service Number
```

C.3. The 'null' Endpoint

The 'null' EID of "ipn:0.0" can be encoded in the following ways:

The complete five octet encoding of the 'null' ipn EID using the two-element scheme-specific encoding would be as follows.

```
82       # 2-Element Endpoint Encoding
   02    # uri-code: 2 (IPN URI scheme)
   82    # 2 Element ipn EID scheme-specific encoding
      00 # Node Number
      00 # Service Number
```

The complete six octet encoding of the 'null'' ipn EID using the three-element scheme-specific encoding would be as follows.

```
82       # 2-Element Endpoint Encoding
   02    # uri-code: 2 (IPN URI scheme)
   83    # 3 Element ipn EID scheme-specific encoding
      00 # Default Numbering Authority
      00 # Node Number
      00 # Service Number
```

Acknowledgments

Add here!!

Keith Scott Scott Burleigh

Authors' Addresses

Rick Taylor
Ori Industries

Email: rick.taylor@ori.co

Ed Birrane
JHU/APL

Email: Edward.Birrane@jhuapl.edu