Delay-Tolerant Networking Previous Hop Insertion Block
draft-irtf-dtnrg-bundle-previous-hop-block-11

Abstract

   This document defines an extension block for use with the DTN Bundle
   Protocol. This Previous Hop Insertion Block (PHIB) extension block
   is designed to be inserted by a forwarding node to provide the
   endpoint identifier (EID) of an endpoint of which the forwarding node
   is a member so that this EID may be conveyed to the next-hop
   receiving node. Knowledge of an EID of an endpoint of which a
   previous-hop node is a member may be required in some circumstances
   to support certain routing protocols (e.g., flood routing). If this
   EID cannot be provided by the convergence layer or other means, the
   PHIB defines the mechanism whereby the EID can be provided with the
   bundle. Each PHIB is always removed from the bundle by the receiving
   node so that its presence within the bundle is limited to exactly one
   hop. This document defines the format and processing of this PHIB.
   This document is a product of the Delay Tolerant Networking Research
   Group and has been reviewed by that group. No objections to its
   publication as an RFC were raised."

Status of this Memo

This Internet-Draft will expire on August 21, 2010.

Copyright Notice

Table of Contents

1. Introduction

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in RFC 2119 [RFC 2119].

   This document defines an extension block for use with the Bundle
   Protocol [RFC 5050] within the context of a Delay-Tolerant Network
   architecture [RFC 4838]. The DTN Bundle Protocol defines the bundle
   as its protocol data unit and defines "bundle blocks" to carry data
   of different types. This document defines an optional bundle block
   called a Previous Hop Insertion Block (PHIB).

   The PHIB is inserted into a bundle by a forwarding node to provide
   the endpoint ID (EID) of an endpoint of which the forwarding node is
   a member so that this EID may be conveyed to the next-hop receiving
   node. (Hereafter, an EID of an endpoint of which a node is a member
   will be referred to as an "M-EID" of that node. A node may have one
   or more M-EIDs, depending on the number of endpoints to which it
   belongs. An EID of a singleton endpoint of which a node is a member
   will be referred to as a "singleton M-EID" of that node.) In
   situations where there is a requirement that the receiving node be
   able to determine an M-EID of a forwarding node, but the M-EID of the
   forwarding node cannot be inferred by the receiving node through
   existing mechanisms, the forwarding node must explicitly provide this
   M-EID in the bundle. This specification defines the mechanism
   whereby a node can insert such an M-EID into a bundle before
   forwarding it to the bundle's next hop.

   This previous-hop M-EID information may be used in some circumstances
   to support various routing protocols. For example, the PHIB could be
   helpful when implementing flood routing because each receiving node
   could use the PHIB to determine which EID to exclude from the list of
   adjacent nodes to which it forwards received bundles as it does its
   part in flooding the bundle. A node will flood the bundle to all
   neighboring nodes except for the node from which it received the
   bundle, as identified in the PHIB.

   The PHIB could also be used in conjunction with the Bundle
   Authentication Block (BAB) of the DTN Bundle Security Protocol
   [DTNBSP] to provide the security source EID for the BAB. The PHIB
   can be used to carry the BAB's security source EID instead of
   conveying this EID using a reference in the BAB's EID reference field
   or including the EID as part of the BAB's key information parameters.

   In many situations, a node that receives a bundle may be able to
   infer an M-EID of the node that forwarded the bundle. In some
   situations, however, no M-EID will be able to be inferred by the

receiving node. For example, if tunneling DTN bundles across some
portion of the DTN network, it is not possible for the node at the
receiving end of the tunnel to determine from the convergence layer
the M-EID of the node at the sending end of the tunnel. The node at
the receiving end of the tunnel will receive an encapsulating bundle
from one of its adjacent nodes and it may be able to tell the M-EID
of this adjacent node using the convergence layer protocol. However,
the node at the sending end of the tunnel is most likely not adjacent
to the node at the receiving end of the tunnel, so in order for the
node at the receiving end of the tunnel to be able to learn the M-EID
of the node at the sending end of the tunnel, which is the previous
hop node of the tunneled bundle, the M-EID must be provided within
the tunneled bundle. In this case, the PHIB is the vehicle for
enabling the node at the sending end of the tunnel to provide its
M-EID to the node at the receiving end of the tunnel.

EIDs may be presented in two ways within the PHIB. If the M-EID of
the forwarding node is already in the dictionary field of the
bundle's Primary Bundle Block, the PHIB MAY identify this EID using
its Block EID reference count and EID references field. Otherwise,
the PHIB MUST identify this EID by providing the EID in its block-
type-specific data field. These two alternative ways of presenting
EIDs in the PHIB are further discussed in Section 3.

The lifetime of the PHIB is always exactly one hop in the DTN. If a
bundle containing a PHIB is received, the receiving node is assured
that this PHIB was inserted by the previous node, assuming all nodes
are operating correctly; likewise, this PHIB is not retained with the
bundle when the bundle is forwarded. If the bundle is forwarded with
a PHIB, this PHIB MUST identify an M-EID of the forwarding node.

This document defines the format and processing of the PHIB. The
capabilities described in this document are OPTIONAL for deployment
with the Bundle Protocol. Bundle Protocol implementations claiming
to support the PHIB MUST be capable of:

   -Generating a PHIB and inserting it into a bundle,

   -Receiving bundles containing a PHIB and making the information
   contained in this PHIB available for use, e.g., in forwarding
   decisions.

   -Deleting a PHIB from a bundle

as defined in this document.

2. **Previous Hop Insertion Block Format**

   The PHIB uses the Canonical Bundle Block Format as defined in the
   Bundle Protocol [RFC 5050]. That is, the PHIB is comprised of the
   following elements, which are defined as in all bundle protocol
   blocks except the primary bundle block. Note that SDNV encoding is
   also described in the Bundle Protocol:

      -Block-type code (one byte) - The block type code for the PHIB is
      0x05.

      -Block processing control flags (SDNV) - The following block
      processing control flag MUST be set:

         -Discard block if it can't be processed.

      -Block EID reference count and EID references (optional) -
      composite field defined in [RFC 5050] containing a count of EID
      references (expressed as an SDNV) followed by an EID reference
      (expressed as a pair of SDNVs).

      Whether or not this field is allowed in the PHIB is determined by
      whether or not an M-EID of the node inserting the PHIB is already
      in the Dictionary Field of the Primary Bundle Block (e.g., whether
      an M-EID of the inserting node is also an M-EID of the bundle's
      source, current custodian, or report-to endpoint, or is the same
      as some other endpoint in the dictionary that is referenced by
      another block in the bundle).

      If an M-EID of the inserting node is already in the dictionary,
      this field MAY be present in the PHIB. If this field is present
      in the PHIB, the value of the EID reference count MUST be one,
      meaning that the field contains exactly one EID reference, which
      MUST be a reference to an M-EID of the inserting node. Presence
      of this field MUST be indicated by a set "block contains an EID
      reference field" flag in the block processing control flags.

      If no M-EID of the inserting node is in the dictionary, this field
      MUST NOT be present in the PHIB, which MUST be indicated by an
      unset "block contains an EID reference field" flag in the block
      processing control flags

      -Block data length (SDNV) - If this value is zero, there are no
      block-type-specific data fields. In this case, the M-EID of the
      inserting node must be in the dictionary and it MUST be referenced
      in the Block EID reference count and EID references field as
      described above.

-Block-type-specific data fields (optional) as follows:

   -Inserting Node's EID Scheme Name - A null-terminated array of
   bytes that comprises the scheme name of an M-EID of the node
   inserting this PHIB.

   -Inserting Node's EID SSP - A null-terminated array of bytes
   that comprises the scheme-specific part (SSP) of an M-EID of
   the node inserting this PHIB.

If the Block EID reference count and EID references field is not
present in the PHIB, the above two EID scheme name and SSP block-
type-specific data fields MUST be present. If the Block EID
reference count and EID references field is present in the PHIB,
the above two EID scheme name and SSP block-type-specific data
fields MUST NOT be present.

The Structure of a PHIB is as follows:

PHIB Format:
```
+----+-----------+------------------------------- -+------------+
|type|flags (SDNV)|EID ref count and list (comp) (opt)|length (SDNV)|
+----+-----------+-------------------------------+------------+
| Inserting Node EID Scheme Name (opt)| Inserting Node EID SSP (opt)|
+-------------------------------------------------------------+
```

                          Figure 1

3. Previous Hop Insertion Block Processing

   The following are the processing steps that a bundle node must take
   relative to generation, reception, and processing of a PHIB.

3.1. Bundle Transmission

   When an outbound bundle is created per the parameters of the bundle
   transmission request, this bundle MAY include one or more PHIBs.
   Whether or not PHIBs are included is a local bundle agent
   configuration option and may be influenced by other factors, such as
   the routing protocol in use.

3.2. Bundle Forwarding

   Before forwarding a bundle, the node SHALL delete all PHIBs that were
   in the bundle when it was received (if any). As described in the
   Bundle Protocol, the node MAY delete all strings (scheme names and
   SSPs) in the bundle's dictionary to which no endpoint ID references
   in the bundle currently refer (if any).

   The node MAY insert one or more PHIBs into the bundle before
   forwarding it, as dictated by local policy. If there are already
   strings (scheme names and SSPs) in the bundle's dictionary that
   denote the M-EID of the inserting node, the PHIB MAY reference these
   strings and, if it does, it MUST NOT include any block-type-specific
   data fields. The inserting node MUST NOT insert strings into the
   bundle's dictionary in order that they may be referenced by only the
   PHIB. If the PHIB is constructed such that it does not reference any
   strings from the dictionary, the inserting node MUST include the
   scheme name and SSP of one of its M-EIDs as the PHIB's block-type-
   specific data fields.

   The node that is inserting a PHIB into the bundle may have more than
   one endpoint in which it is a member. The choice of which M-EID to
   insert into the PIB SHALL be made as follows:

      - If the inserting node is a member of exactly one singleton
      endpoint, the node may insert at most one PHIB into the bundle and
      the EID of this singleton endpoint is what MUST be inserted into
      the PHIB.

      - If the inserting node is a member of more than one singleton
      endpoint, then:

         If the inserting node has a priori knowledge of the URI schemes
         supported by the next hop node and if the inserting node has
         one or more singleton M-EIDs that are expressible in one or

more of those URI schemes, then the inserting node MAY insert
one or more PHIBs into the bundle being forwarded. The EIDs in
the inserted PHIBs MUST be unique, they MUST be singleton
M-EIDs of the inserting node, and they MUST be expressed in URI
schemes supported by the next hop node. Mechanisms for
determining what URI schemes are supported by particular next
hop neighbors are not defined here.

If the inserting node has one or more singleton M-EIDs that are
expressible in the same URI scheme as the destination of the
bundle that is being forwarded, then the inserting node MAY
insert one or more PHIBs into the bundle being forwarded. The
EIDs in the inserted PHIBs MUST be unique, they MUST be
singleton M-EIDs of the inserting node, and they MUST be
expressed in the destination URI scheme of the bundle.

Else if the inserting node has neither a singleton M-EID that
is expressible in a URI scheme known to be supported by the
next hop node nor a singleton M-EID that is expressible in the
same URI scheme as the destination of the bundle that is being
forwarded, then the inserting node MAY insert one or more PHIBs
into the bundle being forwarded. The EIDs in the inserted
PHIBs MUST be unique, and they MUST be singleton M-EIDs of the
inserting node.

3.3. Bundle Reception

If the bundle includes a PHIB, the EID identified in the PHIB SHALL
be made available for use at the receiving node (e.g., in forwarding
decisions or, if the receiving node is the bundle destination, the
EID may be made available to the receiving application; whether or
not it is made available to the receiving application is an
implementation matter). If the EID is identified both by a reference
in the PHIB's Block EID reference count and EID references field and
by a scheme name and SSP in the block-type-specific fields, the PHIB
is not considered to be well-formed. In the case of reception of
such an ill-formed PHIB, if the identified EIDs are the same, the
receiving node MAY process the PHIB as if it were well-formed.
However, if the identified EIDs differ, the receiving node MUST NOT
process the PHIB and must take action on the PHIB as specified by the
PHIB's Block Processing Control Flags.

[4](#). **Security Considerations**

   The DTN Bundle Security Protocol [DTNBSP] defines security-related
   blocks to provide hop-by-hop bundle authentication and integrity,
   end-to-end integrity, and end-to-end confidentiality of bundles or
   parts of bundles, as well as a set of ciphersuites that may be used
   to calculate security results carried in these security blocks. The
   PHIB will not be encrypted when using the PCB-RSA-AES128-PAYLOAD-PIB-
   PCB ciphersuite with the Payload Confidentiality Block (PCB) to
   provide end-to-end confidentiality. This ciphersuite only allows for
   payload and Payload Integrity Block (PIB) encryption. If encryption
   of the PHIB block is desired, the Extension Security Block (ESB)
   could be used for this purpose.

   All ciphersuites that use the strict canonicalisation algorithm
   [DTNBSP] to calculate and verify security results (e.g., many hop-by-
   hop authentication ciphersuites) apply to all blocks in the bundle,
   and so would apply to bundles that include an optional PHIB and would
   include that block in the calculation of their security result. In
   particular, bundles including the optional PHIB would have their
   integrity protected in their entirety for the extent of a single hop,
   from a forwarding node to an adjacent receiving node, using the
   Bundle Authentication Block (BAB) with the BAB-HMAC ciphersuite
   defined in the Bundle Security Protocol.

   Ciphersuites that use the mutable canonicalisation algorithm to
   calculate and verify security results (e.g., the PIB-RSA-SHA256
   ciphersuite and most end-to-end authentication ciphersuites used with
   the PIB) will (correctly) omit the PHIB from their calculation. The
   fact that several different instantiations of this PHIB block may be
   added to and deleted from the bundle as the bundle transits the
   network will not interfere with end-to-end security protection when
   using ciphersuites that use mutable canonicalisation.

   As stated above, the BAB can be used to ensure the integrity of the
   PHIB. Nodes receiving bundles with PHIBs should be aware, however,
   that forwarding nodes that insert PHIBs might lie about the EIDs of
   endpoints of which they are members. Lying in this way could provide
   a mechanism for subverting routing strategies that base routing
   decisions on EID information in the PHIB.

   Note that if some Bundle Protocol implementation does not support the
   PHIB but does not properly implement the "Discard block if it can't
   be processed" flag, then a PHIB may unexpectedly persist for longer
   than a single hop.

5. IANA Considerations

   If the bundle protocol becomes a standards track protocol, then we
   may want to consider having IANA establish a register of block types,
   of which the PHIB would be one. The block type code being suggested
   for the PHIB is 0x05.

6. References

6.1. Normative References

[RFC 2119]
          Bradner, S. and J. Reynolds, "Key words for use in RFCs to
          Indicate Requirement Levels", RFC 2119, October 1997.

[RFC 5050]
          Scott, K. and S. Burleigh, "Bundle Protocol
          Specification", RFC 5050, November 2007.

6.2. Informative References

[RFC 4838]
          Cerf, V., Burleigh, S., Hooke, A., Torgerson, L., Durst,
          R., Scott, K., Fall, K., and H. Weiss, "Delay-Tolerant
          Network Architecture", RFC 4838, April 2007.

[DTNBSP]   Symington, S., Farrell, S., Weiss, H., and P. Lovell,
          "Bundle Security Protocol Specification",
          draft-irtf-dtnrg-bundle-security-14.txt, work-in-progress,
          January 2010.

Author's Address

    Susan Flynn Symington
    The MITRE Corporation
    7515 Colshire Drive
    McLean, VA 22102
    US

    Phone: +1 (703) 983-7209
    Email: susan@mitre.org
    URI: http://mitre.org/