Bundle Protocol
Endpoint ID Patterns

IETF 116 DTN WG

Emery Annis, Brian Sipos
JHU/APL
Background

• Use cases on the following slide motivate the need for a mechanism to define a set of EIDs in a structured way
  - Goal is to ensure the writer and the user have the same interpretation

• Simple globs or regular expressions could be used, but these are not ideal
  - Purely text-based
  - Do not take advantage of the structure for DTN or IPN schemes
  - Do not handle numeric intervals for IPN scheme
  - Do not have an efficient binary encoding

• Pattern matching syntax has a “network effect”
  - The more tools that use a common syntax the more value it has
  - If established, new tools do not need to reinvent a robust mechanism
  - Lessens the possibility of security vulnerabilities from misconfiguration
    “is this parameter an EID or some glob expression?”

• This proposal is compatible with IPN Scheme update draft
Use Cases

• Security identities
  - Allow a certificate holder to be authorized to sign for dtn://node/** or for ipn:3.*.* or even ipn:3.*.0
  - The same way as wildcard certificates, it is a CA obligation to ensure endpoint ownership of all matching EIDs

• Routed blocks
  - EID Patterns are meant for a more structured situation than “huge list of EIDs”
  - The same purpose as IP CIDR notation e.g. 192.168.30.0/24

• BP Agent configuration / policy
  - Allow BPA configuration to use consistent pattern syntax
  - Allow node ipn:3.5.0 to sign bundles from ipn:3.*.*
  - Provide the same kind of ubiquity as CIDR does for IP configuration
  - Avoids policy engines with over-restrictive or limited expressive syntax

• Colloquial use
  - Have an understandable way to convey technical comments like:
    * I’m having trouble sending to ipn:3.**
    * Please allocate your services within ipn:**.[5-10]
Proposed Capabilities

• Draft in
  https://www.ietf.org/archive/id/draft-sipos-dtn-eid-pattern-00.html

• DTN Scheme Patterns
  - Separate the EID into node-name and service-path segment
  - Each part can be one of:
    ▪ Exact-match literal
    ▪ Match-all one-part wildcard
    ▪ Match-any-parts wildcard
    ▪ Regular expression, percent-encoded

• IPN Scheme Patterns
  - Separate the EID into single-integer parts
  - Each part can be one of:
    ▪ Exact-match value (compared as integer)
    ▪ Match-all one-part wildcard
    ▪ Match-any-parts wildcard
    ▪ Range expression (set of discrete intervals)
  - Compressed CBOR encoding using integers
  - Simple set logic (“Pattern A contains B” or “Pattern A overlaps with B”)

Examples of EID Patterns

• Singleton pattern:
  dtn://node-name/serv ipn:3.10.5

• All services on a node
  dtn://node-name/** ipn:3.10.*

• One service on any node
  dtn:///**/serv/name ipn:**.5

• Complex wildcard patterns
  dtn:///**/prefix/* ipn:3.*.5 ipn:3.*.*

• Expressions and ranges
  dtn://[prefix.*]/serv ipn:3.[5-10,100-110].5

• Mixed patterns
  dtn://[node%5BA-Z%5D]** ipn:3.[10,12,14].*
Considerations

• An EID Pattern is *not* an EID, they cannot be used interchangeably
  - This is a security risk *à la* the wildcard DNS names in early PKIX certificates
  - The syntax has been designed that a range (IPN) or expression (DTN) is specifically *not* a valid EID value per the ABNF syntax

• An EID Pattern is a superset of EIDs
  - It is a design goal that an EID is a singleton-matching pattern for itself

• Patterns are conceptually simple but can be complex in practice
  - A common specification can allow shared-use implementations

• Syntax special considerations
  - `ipn:3.*.*` is only authority number 3
  - `ipn:3.**` also includes node number 3
  - `ipn:*.*.5` will not match any EID with an authority
  - `ipn:*.*.5` will *only* match an EID with authority
  - `ipn:**.5` will match any node with this service
Next Steps

• Feedback on current proposals
  - What is valuable immediately?
  - What should be deferred?
  - Any issues with the current syntax or special cases to be avoided?

• Trial or example implementations
  - Existing BPAs that want to try out this syntax?
  - Potential hackathon topic?