draft-forwarding-label-ccn-01.txt

Ravi Ravindran and Asit Chakraborti

Huawei

(IETF/ICNRG, Yokohama, 94)

[ravi.ravindran@huawei.com]

[asit.chakraborti@huawei.com]

Agenda

- Draft Objectives
- Terminology
- Why ID/Locator Split in CCN
- FL Object Management
- FIB Processing
- PIT/CS Processing
- Multi-Domain Considerations
- Security Consideration
- Use case scenarios
- Next Steps

Draft Objectives

- Second iteration of this draft.

- Proposes to have ID/Locator Split in CCN.
  - The locator is called **Forwarding-Label** which can be modified in the infrastructure.

- Could be used by for different purposes:
  - Mobility
  - Opportunistic Indirections (off-path caching)
  - Service Affinity (Edge Computing)
  - In-Network Computing (e.g. NFN)
  - Inter-domain Routing
  - ..

- The draft talks about FL management, PIT/CS Processing, Multi-Domain Scenario Handling, Usage Scenarios.

- Also also opens many questions around managing two names in the Interest message.

Terminology

- Interesting discussion during the Interim meeting
  - Don't want to use these terminologies because they meant something in the past.
  - For our discussion **ID=Locator=Name**
  - **Name := Hierarchically Structured Identifier**
    - **Should this be Routable ?**
    - **CCN1.0 or NDN Name definition doesn't require Routeability**
  - We should eventually address, non Routable names too, e.g. self-certified ID, e.g. M2M communications.

- **For this discussion we assume, ID are names managed by Applications and Locators are Names managed by the infrastructure provider, hence topologically relevant.**
  - **They are Routable Names in a given context.**
  - **ID :/disney/video/….**
  - **Locator : /att/santaclara/..**

ID/Locator Split in CCN

- Why do we need ID/locator Split?
  - **Management**: ID and Locator belong to different administrative authorities, and do not want to be influenced by each other.
  - **Security/Turst** : Security/Trust over IDs independent of the network requirements.
  - **Flexibility** : In the context of CCN, this it to aid dynamic scenarios like content replication, mobility, migration, multihoming etc.
  - **Scalability** : Routing on IDs (even though aggregateable) is challenging.
    - Better for core networks to only deal with locator name which is O(#of AS)

CCN Routing on IDs

- **Advantages**
  - A single name space for both network and applications.
  - IDs are contextual, hence several services can be invoked: Security, Policy Based Routing, Strategy layer forwarding
- **Disadvantages**
  - Infrastructure provider may not want to work with Application IDs.
    - Large name space - always growing
    - ID Dynamism affect its stability: Replication, Migration, Mobility etc.

CCN Routing on ID+Locators

- **Advantages**
  - Achieves Management, Flexibility, Scalability, Security requirements.
  - The network can apply name based routing only at the edges routers, but the core can be based on locators only.
  - Core Network independent of application name dynamism
 - Edge networks can be Name based

- **Disadvantages**
  - Explicit guidelines on handling two names in the Interest/Content Packet.
  - Mapping required from names to locators, either managed by the application or by the network or both.
  - Forwarding looses contextual operation that it can derive from names, e.g. strategy forwarding features.
  - Open to malicious acts, e.g. cache poisoning, but primarily a trust concern.

→ **We see there are considerable benefits with Challenges too, so these have to be studied further.**

FL Object Encoding

- As a Optional hop-by-hop Header TLV.
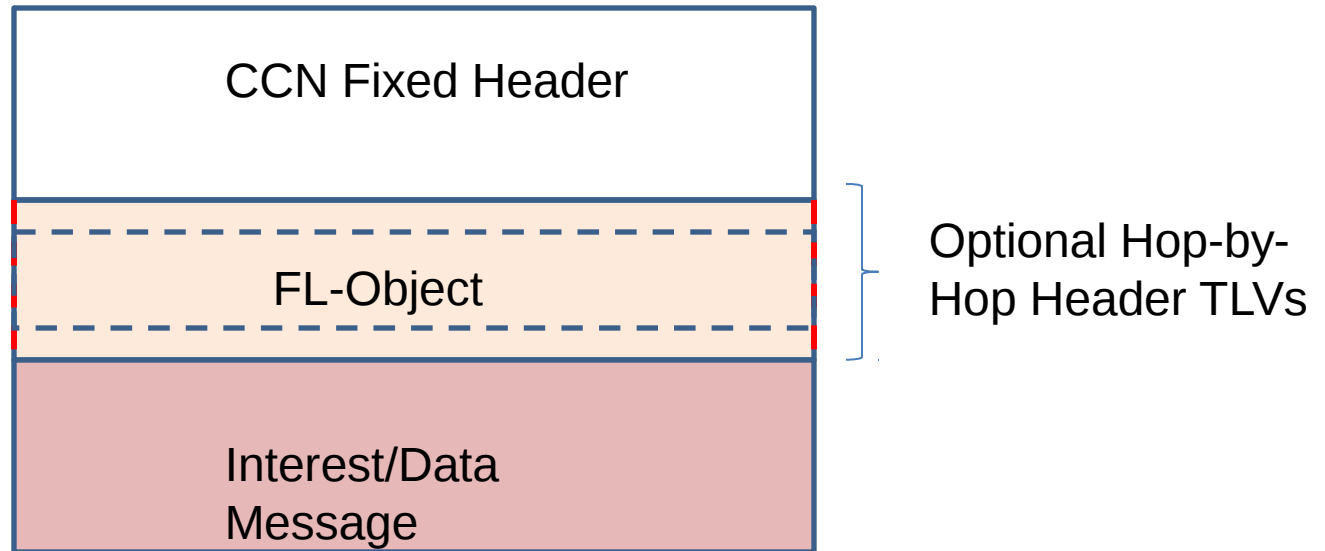
FL-Object

Object embeds three kinds of information:

- **LID** : Locator ID (T_LID_NAME): AS-ID/Router-ID etc

- **FL-Metadata** (**optional**) : Service specific metadata, to aid FL processing in a given context, e.g. as in Mobility, In-Network Computing etc.

- **FL-Security** (**optional**) : ID to LID binding Security information, similar to LINK-Object [1]

[1] Afanasyev, A., "Map-and-Encap for Scaling NDN Routing.", NDN Technical Report ndn-004-02, 2015.

FL Object Insertion

- FL can be inserted by applications or the network.
- FL insertion by the network can be policy based
  - Policy based actions on the names, Interest Marking etc.
  - For Applications this may be a default choice, or based on feedback from the network.
  - Depending on the trust context, networks may or may not choose to trust these suggestions.
  - FL insertions by applications may be subjected to security validation.
  - Validation is between ID and the LID

→ **The infrastructure may choose to only accept FL Object from trusted applications, while ignoring or explicitly removing the rest.**

FL Object Swapping/Termination

- FL objects may be swapped at designated points in the network.
- FL can be terminated by designated points in the network
  - Edge Service Routers, Middlebox, Border Routers
- Here the FL matches one of the LocatorID of the forwarder
  - A node may have multiple locator names.
  - e.g. /att/santaclara or /att/santaclara/poa
- Further service logic is applied, and the FL can be replaced by another FL Object
  - Else Name based routing may ensue

FIB Processing

- Depends on the use of FL Object, hence multiple possibilities.
  - Case 1: the FL can always given priority over ID in the Interest, assuming they are always trusted in-directions.
  - Case 2: forwarder could always prioritize ID based routing, and if that fails, use the FL for forwarding
  - Case 3: If policy based routing is involved, the ID could be used to decide the FL insertion, while the core nodes always uses 1 or 2.

- Then we discuss the FIB processing for case 1.
  - Validate FL Object if it is not trusted
    - If lookup(LID) is a Node ID
      - Then invoke appropriate service logic
    - else if it results in a next-hop
      - Forward it.

PIT Processing

The question here is if we need to have FL Object state in the PIT or the CS ?

Depends on the purpose of the FL Object
- **Case 1**: If it is simply a in-direction directive
- **Case 2**: Consumer imply more meaning on the ID and FL Object.

Case 1:
- FL-Objects purpose is to guide Interest messages to improve routing efficiency and offer flexibility.
- Simple policy is not to have any FL state in the PIT
    - In certain situations, for the same Interest Name and different FL aggregation will not allow those Interests to be forwarded
    - In this case, the PIT will require saving the FL Object state
        - Is it only LID or the whole FL Object ?

Case 2:
- Consumers implies a tight binding between ID and the FL Object.
- In this case, PIT saves the whole FL Object, which is also returned with the CO.
- In this case, if the FL Object is swapped, then the it should be replaced by appropriate FL Object in the return path.

CS Processing

- Follows the PIT processing discussion.
  - CO may carry the FL Object only if there is a such an expectation from the Consumers.

FL Security

Depends on the purpose it will be used for.

- Security Considerations:
  - 1) Malicious publisher injecting incorrect mapping between ID and the LID
  - 2) Malicious interceptor between the node seeking mapping and the mapping system
  - 3) Compromised intermediate router maliciously changing the FL
  - 4) Untrusted application may inject invalid FL Object

- 1&2 are issues addressed in other protocols like DNS-SEC, LISP-SEC
- 3 requires new security mechanisms to enable a domain level trust infrastructure
- 4 is policy driven, require authentication of the consumer and the ID/LID binding, more lightweight mechanisms can be studied.

FL Object Application Scenarios

- **Producer Mobility:**
  - Late Binding
    - Edge Routers/PoA late binds Interest to its current location
  - Using semantic names, can be used to realize a Decentralized Name Resolution
- **Manifests**
  - Contains indirections to CO. Here FL Object can contain the LID, while CO has the immutable name.
    - Related to discussion around Nameless CO.
- **Routing Optimization**
  - Application controllers in the domain can apply policy based routing based on service names.
  - So request for a CO can be handled in a specialized manner.
- **Inter-domain Routing**
  - Routing scalability problem is handled, as LID is a bounded name space, in DFZ it will bound it O(#of AS).

Evolving the draft

- Clarification of Terminologies

- More details on FL Management/Processing

  - Security Considerations

  - Detailing use case scenarios

→Feedback is welcome..anytime.

Thank You and Questions