ICN Research Group
Internet-Draft
Intended status: Informational
Expires: May 6, 2016

R. Ravindran
A. Chakraborti
Huawei Technologies

November 3, 2015

Forwarding-Label support in CCN Protocol
draft-ravi-ccn-forwarding-label-01

Abstract

The objective of this proposal is to enable ID/Locator split in CCN protocol. We enable this through the notion of forwarding-label (FL) object, which is an optional hop-by-hop payload in the Interest message with locator name which identifies a network domain, router, or a host. Depending on the application and trust context FL object is subjected to policy based actions by the forwarders such as invoking security verification or enabling other service-centric actions such as FL object replacement. FL can be inserted by the applications or by the network. To enable dynamic name resolution FL can be modified in the network by designated points such as the edge routers. Enabling ID/Locator split in CCN has several applications such as towards routing optimization, mobility, handling indirections in manifests, and routing scalability.

Table of Contents

1. ID/Locator Split in CCN

We discuss here the motivations behind the need for separation between persistent name (ID) and a locator (LID) in the Interest message in the context of CCN and a proposal to achieve this. The advantages of ID/Locator has been extensively studied and has been part of many host-centric protocols such as HIP[2], ILNP [3], and LISP [4] and also is part of FIA architectures such as MobilityFirst[13]. Specifically in CCN, ID based routing is not efficient considering dynamic replication of content, mobile entities, or address the problem of routing scalability [9] issue, hence providing this distinct separation in the protocol offers the following advantages:

- ID and Locator namespaces are managed by different entities. IDs are managed by applications, hence relevant only to consumers ,

producers and intermediate service points, while locator names are managed by network administrator. Locators map to network domains or specific network element through which the named entity is reacheable. The relationship between the two is established during the publishing phase, and managed by a separate name resolution function. ID/Locator distinction in CCN allows applications to manage its own name space and not be restricted by network naming rules.

- Today, CCN Applications bind to persistent IDs, while its resolution is handled by per-hop name-based routing in CCN forwarder using unicast/anycast/broadcast means, with routing scalability linked to name aggregation. This model has issue when the named entity is mobile, migrated, or replicated, as the names have to be announced in the routing control plane introducing instability and churn. Enabling ID/Locator split and managing this mapping in a separate name resolution system shall address the routing churn introduced by dynamic entities. CCN is unique in the sense that both name-based routing and resolution system can operate simultaneously driven by its use based on a given context, for e.g. while inter-domain routing can be handled using name resolution system, intra-domain routing can be based on name-based routing.

- Affording ID/Locator split in an Interest message offers many advantages in many network and application functions such as towards name resolution optimization, mobility, handling indirections in manifests [6], and routing scalability.

Considering the above requirements, we propose Forwarding-label (FL) object which provides flexibility to forward Interests on a name other than the one in the Interest message with the ability to modify it in the network. Handling ID/Locator mapping requires a control plane infrastructure and appropriate network layer state with security functions to avoid malicious usage. Specific control plane or security mechanism of ID/Locator mapping is out of the scope of this document as many techniques can be used towards achieving this. This draft presents various considerations towards FL management (insertion/modification/deletion), processing by a CCN forwarder, PIT/CS implications, FL packet format, and security/trust and discusses its application in various scenarios.

2. Forwarding-Label Management

FL is used in scenarios where routing by Interest name for name resolution when dynamic scenarios are considered which include replicated content, device mobility, or where scalability challenges exist when ID based routing is employed. FL objects are subjected to

processing and modification in the network depending specific use case scenario. Following we discuss various aspects of FL related to its semantics and management.

2.1. FL Naming

FL are container objects which include LID, service specific metadata, and security attributes for authentication. LIDs are hierarchically structured topologically names where the names follow the definition in [1]. The security attributes are optional and may include validation payload and algorithm as discussed in [1].

2.2. FL Insertion

A FL object can be inserted in an Interest message by the consuming application or by the network.

In general in CCN, applications requests a service or content by ID, which is feasible today due to the aggregatable nature of ID. But in certain situations, the application logic may use a FL object in addition to the ID in the Interest message or this action may also be triggered because of feedback from the network on failing to route the Interest message based on ID . Networks which processes traffic from applications outside its trust domain require a way to validate the FL object, one of which is discussed in [9]. Another possibility is that networks may ignore FL object from untrusted applications and only choose to route by the Interest ID.

This FL object insertion can also be triggered at the ingress points of a network domain. Network inserts a FL to an incoming Interest message if the Interest message satisfies flow service profiles imposed by the network administrator in the ingress routers, these services functions include mobility or special handling for content distribution. These service profile matching actions include matching Interest name to service prefixes or triggered by certain marking in the Interest message. FL object inserted within trust domain require may not require security validation.

In situations where a forwarder handles both these scenarios, policies can be applied in the ingress router to handle the two cases appropriately. These policies include the face on which the Interests arrives on, Interest ID etc.

2.3. FL Swapping

One FL object can be swapped by another in the network in the context of a given service by designated points in the network. As FL objects carry a LID, and with appropriate representation and security

considerations in the Interest message, FL objects also can be potentially stacked if the Interest message has to be tunneled through a domain where routing based on the current FL object is not applicable.

2.4. FL Termination

FL objects are terminated by a forwarder when the LID in it matches its own set of names, here we assume a forwarder could have many LIDs such as domain-ID or router-ID. For e.g. a forwarder in a domain identified as /att/santaclara can process FL object with LID set to this domain name or forwarder ID such as /att/santaclara/pop-x. Whenever a FL object is terminated by the forwarder, depending on the service context, it can attach a new FL object, or conduct processing based on the Interest ID.

3. FL Message Format

As FL object is swappable in the network, hence it is proposed as a hop-by-hop field in the optional body of the fixed header as shown in Figure 1. The optional FL container includes attribute of type T_LID_NAME, where the LID (Figure 2) are hierarchically structured variable length ID [1]. A LID implies an locator such as an AS-, Gateway-, Router- or Host- ID. In addition to the LID, optional FL metadata includes information on the application or service context to aid network to invoke appropriate FL processing, such as trust validation of the FL object. Optional security attributes such as authentication information can be included depending on specific use case scenarios, such as secure name delegation information discussed in [9], or signature of the consumer.

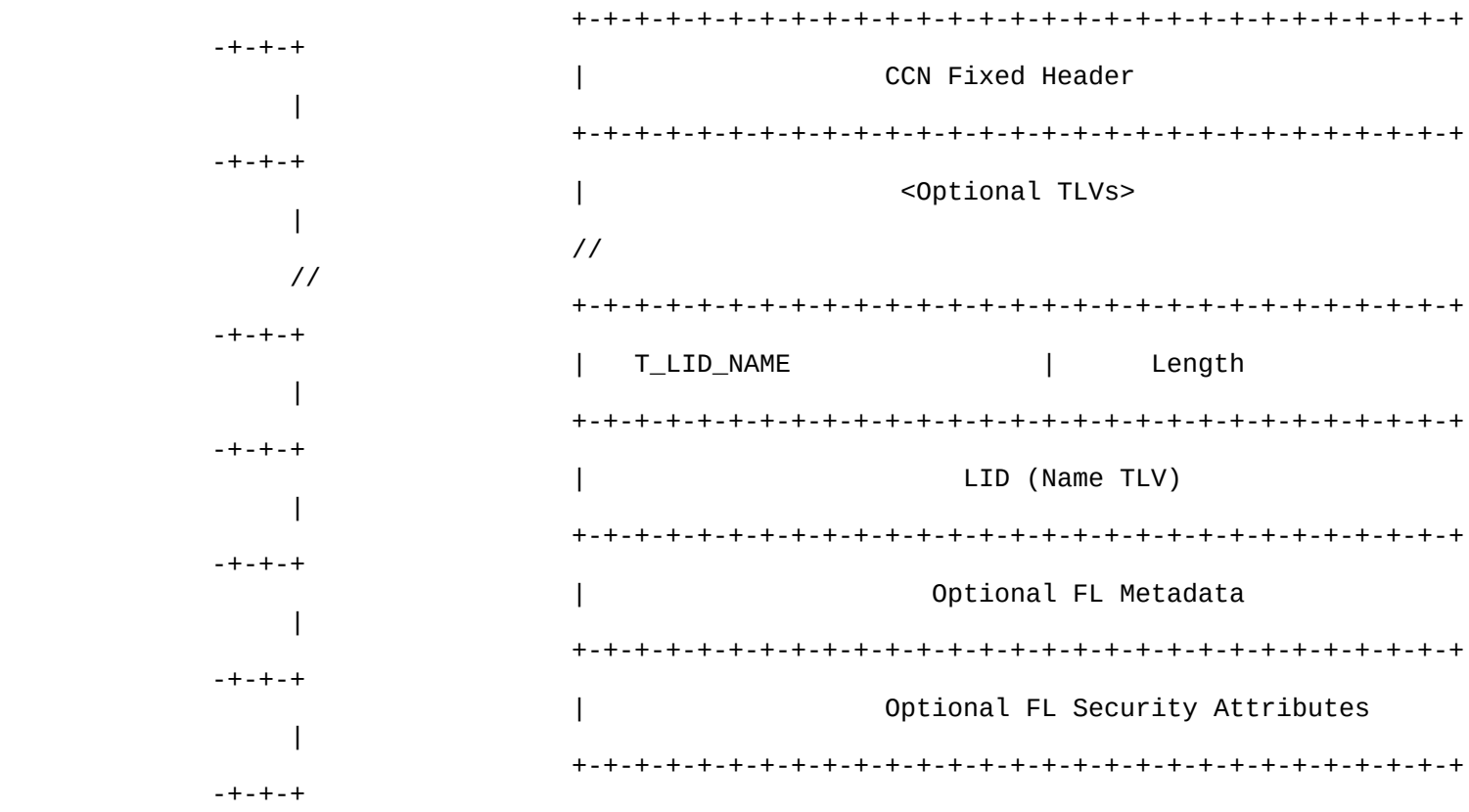

Figure 1: Optional TLV to include a Forwarding-Label Object

Forwarding-Label	Meaning	Value
T_LID_NAME	Identifies an AS-ID/Gateway-ID/Host-ID	Name TLV

Figure 2: Locater-Name Definition

4. Forwarding Label Processing Rules

The following discussion is based on the assumption that all forwarders must process optional header fields. In the context of CCN packet processing, FL object is relevant when the decision to forward the Interest message is to be made. At this stage, multiple options exist, assuming consistency of policy across the domain: 1) in a simpler scenario the rule may be that if a FL is included in an Interest message, then it should be given preference to the Interest

name. This is under the assumption that FL objects are trusted indirections included in the Interest message, which can be validated by the router if required; 2) in another scenario the forwarder could prioritize forwarding on the ID, and then forward on the LID at every hop; 3) in scenario where policy based routing is involved, more complex routing approaches can be considered at the network edge, such as the forwarder could apply service policy on the Interest ID

and choose to remove or swap with a new FL object irrespective of the FL object inserted in the Interest message, while the core nodes could use more simpler approach 1 or 2. Following are the steps when approach 1 is applied.

- During Interest packet processing when the forwarding decision is being made, if a LID is available then it should be preferred to the name in the Interest message for forwarding irrespective of feasibility of ID based routing.

- The validation of the FL depends on trust context. In trusted scenarios where the applications and network are managed by the same authority the forwarder can bypass validation. In untrusted scenarios the edge router may validate the FL send from the sender, and to avoid re-checks by successive forwarders these Interests can be marked to have been validated at the ingress point.

- If the lookup based on LID in the FL object succeeds then two possibilities exist: for non-terminating flows i.e. the LID FIB lookup results in a next hop and the Interest is forwarded ; for terminating flows, LID lookup invokes a service logic wherein the service either re-resolves the Interest ID to another LID hence a new FL object or removes the current FL object and subjects the Interest to regular processing based on the ID in the Interest message.

- If the FIB lookup based on the LID fails, then the router can try to forward it based on the Interest ID. If the latter fails, then the router could raise a error condition and feedback the message to the previous hop with appropriate error code.

-

5. PIT Processing Implications

To maintain simplicity of forwarding logic the purpose of FL object should be to guide the Interest to the producer or the closest source of the content/service, hence only be used for forwarding decision and not required for content object processing, however there may be usage scenarios where the FL state is required to be saved in the PIT and even piggybacked in the content object (CO).

In scenario when there is no binding between the ID and LID, and multiple Interests may arrive with different LID, then the expected outcome is to forward all such Interests with unique LID; in this case the PIT is required to save the LID along with the Interest ID and forward the duplicate Interest.

In another application it may be required to decouple the choice of one consumer's LID from another, i.e a secure binding exists between the ID and the LID. In this case, the PIT saves the FL object, and the returning CO should piggyback the Interest FL object and match it against the pending PIT entry before reverse forwarding. In case the FL object is swapped by intermediate routers, then the CO should be updated with the appropriate FL to ensure the PIT match the previous hops, these considerations are similar to those elaborated in [12].

6. Caching Implications

The considerations here follows from our previous discussion where the FL object is piggybacked in the CO as well. If there is a implicit security binding between the Interest ID and the LID then the FL object state is piggybacked along with the CO, and should be matched against the incoming Interest FL object before the cached content object is returned.

7. Multiple Domain Scenario

In wide area network scenarios, Interests cross multiple domains. If FL object is only trusted within domain boundaries, then the FL is removed before forwarding the Interest to the next domain, which then inserts a new forwarding label with associated security attributes at the ingress of the next domain. But if sufficient trust exists between domains to use the FL inserted by the previous domain, then the intermediate domains could avoid FL processing and use the FL passed on by the previous domains.

8. FL Security

FL object security is related to the purpose it is used for and the control plane mechanism used to manage them. Depending on the use case scenario of the FL appropriate security mechanisms should be applied to secure the control and data planes to avoid exploitation of this feature.

Generally, the major threats against the FL approach is to manipulate the relationship between the name and the FL. Such manipulations can happen in various scenarios, some of which are listed as follows: (i) a malicious interceptor (acting as a publisher) intentionally injects incorrect mapping into the name resolution system; (ii) the malicious interceptor (between the edge router and the resolution server) manipulates the mapping sent back from the name resolution system when the edge router queries the mapping system ; (iii) compromised intermediate routers maliciously change the FL, e.g., with the wrong FL object or out-dated FL object; (iv) untrusted application may inject invalid FL object in the Interest message.

Towards network level FL security, appropriate mechanisms should be applied to provide mapping provenance, mapping integrity and anti-replay attack to address these issues. The security mechanisms applicable to (i) and (ii) are similar to ones applied to secure other mapping systems such as LISP [5],DNS[7], (iii) requires new security mechanisms, one such way is to enable a domain level trust infrastructure so that the mapping between the name and the forwarding-label can be authenticated by successive routers.

In untrusted environments, when FL object is inserted in the Interest message from end hosts, appropriate authentication information should be included in the FL object to allow ingress routers to optionally validate the Interest ID to LID delegation [9]. Further, network could enable several policies, such as even to ignore the FL object, to handle FL objects from untrusted applications.

9. Use Case Scenarios

Here we provide the discussions related to using forwarding-label in different scenarios.

9.1. Handling Producer Mobility

In this application we discuss the use FL object to handle producer mobility using late-binding technique which is discussed in [8]. Here the mobile entity (ME) registers the persistent names which require mobility with its current point-of-attachment (PoA). The PoA then registers the mapping between the name and the PoA’s locator in its local name resolution system. Further the domain updates the ME’s home domain name resolution system with its current domain LID. When a correspondent nodes expresses Interest for the name, it is first resolved to the current ME domain by the home domain. When the Interest ingresses the domain, it is resolved again to the ME’s current location. Further PoA to PoA signaling can be enabled to enable seamless forwarding of Interests whenever ME changes its PoA.

9.2. Manifests

Manifests [6] may contain indirections to named content objects. In this case, FL object can be used to indicate its location while hierarchical or flat name ID map to the named object.

9.3. Interest Routing Optimization

Networks which hosts its own or third party content/service can benefit from the ability to handle Interest routing logic in its domain opportunistically. When Interests seeking a specific content

or service ingresses a network domain, the ingress router can redirect the Interest to the closest cache point or service location.

9.4. Routing Scalability

As discussed in [9], locator based routing can address routing scalability as the number of ASs are many orders less than the number of information objects. This reduces the forwarding table in the DFZ zone to order of number of AS in the Internet.

10. Informative References

[1] CCN Wire format, CCNX1., "http://www.ietf.org/id/draft-mosko-icnrg-ccnxmessages-00.txt.", 2013.

[2] Nikander, P., Gurtov, A., and T. Henderson, "Host identity protocol (HIP): Connectivity, mobility, multi-homing, security, and privacy over IPv4 and IPv6 networks", IEEE Communications Surveys and Tutorials, pp: 186-204, 2010.

[3] Atkinson, R., "An Overview of the Identifier-Locator Network Protocol (ILNP)", Technical Report, University College London, 2005.

[4] LISP, RFC6380., "https://tools.ietf.org/html/draft-ietf-lisp-sec-07.", 2014.

[5] LISP-Security, LISP-SEC., "https://tools.ietf.org/html/draft-ietf-lisp-sec-07.", 2014.

[6] CCNx, Manifest., "http://www.ccnx.org/pubs/draft-wood-icnrg-ccnxmanifests-00.html.", 2015.

[7] DNS-SEC, RFC4033., "DNS Security Introduction and Requirements.", 2005.

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

[9] Azgin, A., Ravindran, R., and G. Wang, "A Scalable Mobility-Centric Architecture for Named Data Networking.", ICCCN (Scene Workshop) , 2014.

[10] Cisco System Inc., CISCO., "Cisco visual networking index: Global mobile data traffic forecast update.", 2009-2014.

[11] Zhang, Y., Zhang, H., and L. Zhang, "Kite: A Mobility Support Scheme for NDN.", NDN, Technical Report NDN-0020 , 2014.

[12] CCNx Label Forwarding, CCNLF., "http://www.ccnx.org/pubs/ccnx-mosko-labelforwarding-01.txt.", 2013.

[13] NSF FIA project, MobilityFirst., "http://www.nets-fia.net/", 2010.

Authors' Addresses

Ravishankar Ravindran
Huawei Technologies
2330 Central Expressway
Santa Clara, CA 95050
USA

Email: ravi.ravindran@huawei.com

Asit Chakraborti
Huawei Technologies
2330 Central Expressway
Santa Clara, CA 95050
USA

Email: asit.chakraborti@huawei.com