ICN Research Group Internet-Draft Intended status: Informational Expires: September 12, 2019

J. Hong T. You Y-G. Hong ETRI March 11, 2019

Architectural Considerations of ICN using Name Resolution Service draft-irtf-icnrg-nrsarch-considerations-01

Abstract

This document discusses architectural considerations and implications of Information-Centric Networking (ICN) related to the usage of the Name Resolution Service (NRS). It describes how ICN architectures may change and what implications are introduced within the ICN routing system when NRS is integrated into ICN.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of <u>BCP 78</u> and <u>BCP 79</u>.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 12, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to <u>BCP 78</u> and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

$\underline{1}$. Introduction	2	
$\underline{2}$. Conventions and Terminology	<u>3</u>	
<u>3</u> . Background		
$\underline{4}$. Implications of NRS in ICN	<u>4</u>	
5. ICN Architectural Considerations for NRS	<u>4</u>	
<u>5.1</u> . Name resolution	<u>5</u>	
5.2. Protocols and Semantics	<u>5</u>	
<u>5.3</u> . Routing System	<u>6</u>	
$\underline{6}$. Security Considerations	<u>6</u>	
<u>6.1</u> . Name Space Separation	<u>6</u>	
<u>6.2</u> . NRS System	<u>6</u>	
<u>6.3</u> . NRS Protocols and Messages	<u>6</u>	
<u>7</u> . Acknowledgements	7	
<u>8</u> . References	7	
<u>8.1</u> . Normative References	7	
<u>8.2</u> . Informative References	7	
Authors' Addresses	<u>8</u>	

1. Introduction

Information-Centric Networking (ICN) is an approach to evolve the Internet infrastructure to directly access Named Data Objects (NDOs) by its name, i.e., the name of NDO is directly used to route the request to the data object. Such name based routing in ICN poses a number of issues, which are not solved yet in ICN. These issues includes global scalability of routing, producer mobility, off-path cache, etc. In order to address these issues, the Name Resolution Service (NRS) has been integrated into several ICN projects and literature [Afanasyev][Zhang2][Ravindran][SAIL][MF][Bayhan].

This document describes how ICN architectures may change and what implications are introduces within the ICN routing system when NRS is integrated into ICN. It also discusses ICN architectural considerations for an NRS. In other words, the scope of this document includes considerations in the veiw of the ICN architecture and routing system when integrating NRS into ICN. However, it does not include the NRS discussion, itself, which is presented in [NRSrequirements].

2. Conventions and Terminology

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 [RFC2119].

3. Background

The name based routing in ICN can be helpful to address a number of challenges, such as global scalability of routing, producer mobility, and off-path caching in ICN. In order to address these challenges, an NRS has been integrated into several ICN projects and literature:

- o Routing scalability : In ICN, application names identifying contents are used directly for packet delivery, so ICN routers run a name-based routing protocol to build namebased routing and forwarding tables. Similar to the scalability challenge of IP routing, if non-aggregatable name prefixes are injected to the Default Route Free Zone (DFZ) of ICN, they would be driving the growth of the DFZ routing table size. Thus, applying an NRS can be a feasible solution to keep the routing table size under control, where the NRS resolves name prefixes which do not exist in the DFZ forwarding table into globally routable prefixes such as one proposed in NDN [Afanasyev]. Another approach deal with routing scalability is the Multi-level Distributed Hash Table (MDHT) used in NetInf [Dannewitz]. It provides name-based anycast routing that can support a non-hierarchical namespace can be adopted on a global scale [Dannewitz2].
- Producer mobility : In ICN, if a producer moves into a different authority domain or network location, the request for a content produced by the moving producer with the origin name would be hardly forwarded to the moving producer's new location.
 Especially, in a hierarchical name scheme, producer mobility support is much harder than in a flat name scheme since the routing tables in broader area need to be updated according to the producer movement. Therefore, various ICN architectures such as NetInf [Dannewitz] and MobilityFirst [MF] have adopted NRS to tackle the producer's location.
- o Off-path caching : Caching in-network is considered a basic architectural component of an ICN architecture and caching approaches can be categorized into off-path caching and on-path caching based on the location of caches in relation to the forwarding path from the original server to a consumer. Off-path caching, also referred as content replication or content storing, aims at replicating content in various locations within a network in order to increase availability, where the caching locations may

not be lying along the content forwarding path. Thus, finding off-path cached objects is not trivial in name-based routing of ICN. In order to support off-path caches, the locations of replicas are usually advertised into a name-based routing system or into NRS such as in [Bayhan].

This document discusses architectural considerations and implications of ICN when NRS is integrated into ICN to solve such challenges due to the name-based routing in ICN.

4. Implications of NRS in ICN

In general, NRS would not be mandatory in an ICN architecture if the name-based routing system can be scalable enough to timely reflect the optimal location of requested content in the routing table. However, due to the unlimited size of content namespace, it is not easy to achieve such a scalable routing system in near future. Therefore, the adoption of an NRS is a design choice for making ICN routing and forwarding scalable. Integration of NRS would change the ICN architecture at least with respect to procedures, latency, and security, which are described below.

- o Procedure : When NRS is adopted into an ICN architecture, the procedure of the name resolution has to be integrated into ICN overall procedures. For NRS integration, there are certain things that have to be decided such as where and how the name resolution task is performed.
- o Latency : When NRS is adopted into an ICN architecture, the additional latency of the resolution obviously occurs in the routing and forwarding system. Although the latency of the resolution is added, the total latency could be minimized if the nearest copies or off-path caches can be located by the NRS lookup procedure. Additionally, there might be a trade-off between the resolution latency and inter-domain traffic reduction.
- o Security : When NRS is adopted into an ICN architecture, security treats may increase. Protection of the NRS system against attacks such as Distributed Denial of Service (DDoS) and authentication of name mapping records and related signaling messages would be challenging.

5. ICN Architectural Considerations for NRS

This section discusses the various items that have to be considered from the point of view of ICN architecture when it utilizes an NRS. These items are related with the name mapping records registration,

resolution, and update, protocols and messages, and integration with the routing system.

5.1. Name resolution

When an NRS is integrated into an ICN architecture, the followings related with the registration and resolution of name mapping records have to be considered.

- o Who performs the name resolution?
- o How is the name resolution performed?

The name resolution in ICN can be performed by consumer, routers, or both. Once it is decided where the name resolution will take place, it has to be considered how the name resolution will be performed. The name provided by a consumer might be always resolved to identifiers in a differnet namespace just like a DNS lookup. Conversely, an NRS is always needed to map names to a different namespace.

5.2. Protocols and Semantics

In order to develop a NRS system within a local ICN network domain or global ICN network domain, new protocols and semantics should be designed to manage and resolve names between different name spaces.

One way of implementing an NRS is by extending the basic ICN TLV format and semantics [<u>CCNxMessages</u>] [<u>CCNxSemantics</u>]. For instance, name resolution and response messages can be implemented by defining new type fields in the Interest and Content Object messages [<u>CCNxNRS</u>]. Then it allows the ICN architecture to minimize implication of ICN architectural changes. But NRS system cannot support more flexible and scalable designs cause to restrict basic ICN protocol and semantics.

On the other hand, a NRS system can be implemented by using its own protocol and semantics like existing NRS systems, such as [Hong]. For instance, the NRS protocol and messages can be implemented by using a RESTful API. Then a NRS as application protocol can be operated independently from a basic ICN architecture, but an ICN architecture cannot be assisted with the routing protocol itself effectively.

5.3. Routing System

It has to be considered how to process the information resolved by an NRS lookup. The results of an NRS operation can be intended to be used just to construct tunnels resulting in NRS identifying tunnel endpoints.

Another way to process the information resolved by an NRS lookup is to use it as routing hints in request messages. In this case, request message needs to be re-written with the resolved information including the original name that was requested by a consumer to check the data integrity.

<u>6</u>. Security Considerations

When NRS is integrated into an ICN architecture, security threats shall be increased in various aspects such as followings.

6.1. Name Space Separation

In order to deploy an NRS on ICN architecture, ICN name spaces are separated into more than two name spaces. Thus these name spaces should be mapped and managed securely. According to the ICN research challenge [RFC7927], new name space can also provide an integrity verification function to authenticate its publishers. In addition to the verification, binding two different name spaces should be securely required.

6.2. NRS System

NRS enables deployment of new entities to build distributed and scalable NRS systems. Thus, the entities, e.g., mapping server that can be a mapping database, could be a single point of failure receiving malicious requests from innumerable adversaries like Denial of Service or Distributed Denial of service attacks. Additionally, in order to communicate with the entities to build a NRS system, an initiator should rely on other NRS entities that are designed to be distributed deployed mapping servers in each network domain. Because malicious entities should be involved in this communication to impersonate control functions. Thus, NRS entities should trust each other and communications with them should be protected securely.

<u>6.3</u>. NRS Protocols and Messages

Regarding NRS messages, such as lookup, update, etc., if these messages are transported unauthenticated, an adversary can manipulate them and hijack the important communication to response or to store fake data. Thus, the adversary can generate malicious traffic to be

redirected to victim hosts. Therefore, security requirements for NRS should be considered to protect the ICN architecture as well as the NRS.

7. Acknowledgements

[TBD]

<u>8</u>. References

8.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", <u>BCP 14</u>, <u>RFC 2119</u>, DOI 10.17487/RFC2119, March 1997, <<u>https://www.rfc-editor.org/info/rfc2119</u>>.
- [RFC7927] Kutscher, D., Ed., Eum, S., Pentikousis, K., Psaras, I., Corujo, D., Saucez, D., Schmidt, T., and M. Waehlisch, "Information-Centric Networking (ICN) Research Challenges", <u>RFC 7927</u>, DOI 10.17487/RFC7927, July 2016, <<u>https://www.rfc-editor.org/info/rfc7927</u>>.

8.2. Informative References

[Afanasyev]

Afanasyev, A. et al., "SNAMP: Secure Namespace Mapping to Scale NDN Forwarding", IEEE Global Internet Symposium , April 2015.

[Zhang2] Zhang, Y., "A Survey of Mobility Support in Named Data Networking", NAMED-ORIENTED MOBILITY: ARCHITECTURES, ALGORITHMS, AND APPLICATIONS(NOM), 2016.

[Ravindran]

Ravindran, R. et al., "Forwarding-Label support in CCN Protocol", <u>draft-ravi-icnrg-ccn-forwarding-label-01</u>, July 2017.

- [SAIL] "FP7 SAIL project.", <u>http://www.sail-project.eu/</u>.
- [MF] "NSF Mobility First project.", http://mobilityfirst.winlab.rutgers.edu/ .
- [Bayhan] Bayhan, S. et al., "On Content Indexing for Off-Path Caching in Information-Centric Networks", ACM ICN , September 2016.

[CCNxSeman	tics] Mosko, M., Solis, I., and C. Wood, "CCNx Semantics", <u>draft-irtf-icnrg-ccnxsemantics-06</u> , October 2017.	
[CCN×Messa	ges] Mosko, M., Solis, I., and C. Wood, "CCNx Messages in TLV Format", <u>draft-irtf-icnrg-ccnxmessages-06</u> , October 2017.	
[CCN×NRS]	Hong, J. et al., "CCNx Extension for Name Resolution Service", <u>draft-hong-icnrg-ccnx-nrs-02</u> , July 2018.	
[Hong]	Hong, J., Chun, W., and H. Jung, "Demonstrating a Scalable Name Resolution System for Information-Centric Networking", ACM ICN , September 2015.	
[NRSrequir	rements] Hong, J. et al., "Requirements for Name Resolution Service in ICN", <u>draft-irtf-icnrg-nrs-requirements-01</u> , March 2019.	
[Dannewitz] Dannewitz, C. et al., "Network of Information (NetInf)-An information centric networking architecture", Computer Communications vol. 36, no. 7, April 2013.	
[Dannewitz	2] Dannewitz, C., DAmbrosio, M., and V. Vercellone, "Hierarchical DHT-based name resolution for Information- Centric Networks", Computer Communications vol. 36, no. 7, April 2013.	
Authors' Addresses		
Jungha Hong ETRI 218 Gajeong-ro, Yuseung-Gu Daejeon 34129 Korea		
Email: jhong@etri.re.kr		

March 2019

Tae-Wan You ETRI 218 Gajeong-ro, Yuseung-Gu Daejeon 34129 Korea

Email: twyou@etri.re.kr

Yong-Geun Hong ETRI 218 Gajeong-ro, Yuseung-Gu Daejeon 34129 Korea

Email: yghong@etri.re.kr