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 BCP 78 and BCP 79.

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 May 7, 2020.

Copyright Notice

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

This document is subject to BCP 78 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

1. Introduction .................................................. 2
2. Terminology .................................................. 2
3. Background ..................................................... 3
4. Implications of NRS in ICN ................................. 4
5. ICN Architectural Considerations for NRS ............... 5
   5.1. Name mapping records registration, resolution, and update 5
   5.2. Protocols and Semantics ................................. 6
   5.3. Routing System .......................................... 7
6. IANA Considerations ......................................... 7
7. Security Considerations ...................................... 7
8. References ..................................................... 8
   8.1. Normative References .................................... 8
   8.2. Informative References .................................. 8
Authors’ Addresses ............................................... 9

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 has inherent challenges in supporting globally scalable routing system, producer mobility, off-path caching, etc. In order to address these challenges, 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 introduced 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 view of the ICN architecture and routing system when NRS is integrated into ICN. The NRS itself discussion is provided in the NRS design guidelines [NRSguidelines] document.

2. Terminology

   o Name Resolution Service (NRS): NRS in ICN is defined as the service that provides the name resolution function for translating an object name into some other information such as a locator,
another name, etc. for forwarding the object request [NRSguidelines].

- NRS server: The NRS is a service maintained by a distributed mapping database system. The NRS consists of the distributed NRS servers storing the mapping records in database. NRS servers store and maintain the mapping records that keep the mappings of name to some other information that is used for forwarding content request.

- NRS resolver: The client side of the NRS is called an NRS resolver. The resolver is responsible for initiating the name resolution request queries that ultimately lead to a name resolution of the data objects. NRS resolvers can be located in the consumer (or client) nodes and ICN routers. NRS resolver may also cache the mapping records obtained through the name for later usage.

- Name registration: In order to create the NRS, the content names and their mapping records must be registered in NRS system by a publisher who has at least one authoritative NRS server or by a producer who generates named data objects. The mapping information is the mapping of a name to some information such as another names and locators, which are used for forwarding the content request. Thus, a publisher or producer creates an NRS registration request and send to an NRS server. On registration, the NRS server stores the mapping record in the database and sends an ACK as a response back to the producer or publisher.

- Name resolution: Name resolution is the main process of the NRS. It is performed by an NRS resolver which can be deployed on a consumer node or an ICN router. When the required name mapping record has not been stored in the cache of a NRS resolver, it sends a name resolution request toward the NRS server. The NRS server searches the content name in its mapping record database, retrieves and sends the mapping record in the name resolution response message to the NRS resolver.

3. Background

The name-based routing in ICN has inherent challenges in supporting globally scalable routing system, producer mobility, off-path caching, etc. In order to address these challenges, an NRS has been integrated into several ICN projects and literature as follows:

- 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, integrating an NRS with ICN 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 name domain, which is assigned by another authoritative of publish, or a different 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.

- Off-path caching: In-network caching is a feature of an ICN architecture. Caching approaches can be categorized into on-path caching and off-path caching according to 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

The majority of ICN projects use the name-based routing which omits the name resolution. So, NRS would not be mandatory in an ICN architecture. The integration of NRS would change the ICN
architecture at least with respect to procedures, latency, and
security, as follows:

- **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.

- **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.

- **Security**: When NRS is adopted into an ICN architecture, security
  threats 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 ICN 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 mapping records registration, resolution, and update

When an NRS is integrated in an ICN architecture, the functions
related with the registration, resolution and update of name mapping
records have to be considered. The NRS nodes maintain the name
mapping records and may exist in an overlay network over the ICN
routers, that is, they communicate to each other through ICN routers.
The NRS nodes exist in a distributed manner so that an NRS node is
always available closer to an ICN node and communication latency for
the name registration and resolution performed by the ICN node
remains very low.

- **Name registration**: Name registration is performed by the producer
  when it creates a new content. When a producer creates a content
  and assigns a name to it from the name prefix space assigned to
  it, the producer performs the name registration in an NRS node.
  Name registration is possibly performed by an ICN router when it
does off-path caching or cooperative caching since involving an 
NRS may be a good idea for off-path caching. As a content gets 
cached in many ICN routers, all of them may register the same 
content names in the same NRS node multiple times. In this case, 
the NRS node adds the new location of the content to the name 
record together with the previous locations. In this way, each of 
the name records stored in the NRS node may contain multiple 
locations of the content.

- Name resolution: Name resolution is performed to obtain the name 
  record from an NRS node by sending a name resolution request 
  message and getting the response containing the record. Regarding 
  the name-based ICN routing context, the name resolution will be 
  mostly performed by an ICN router that does not contain the name 
  in its FIB table. The name resolution may also be performed by 
  the consumer (in case the consumer is multihomed) to make decision 
  to forward the content request in a better direction so that it 
  obtains the content from the nearest cache. If the consumer is 
  single homed, it may not perform the name resolution. It creates 
  the content request packet containing the content name and 
  forwards to the nearest ICN router. The ICN router checks its FIB 
  table to see where to forward the content request. If the ICN 
  router fails to know the requested content reachable, it performs 
  name resolution to obtain the name mapping record and adds to FIB 
  table. The ICN router may also perform name resolution even 
  before the arrival of the content request time to use the name 
  mapping record to configure the FIB table.

- Name record update: Name record update is carried out when a 
  content name mapping record changes, e.g. the content is not 
  available in one or more of previous locations.

5.2. Protocols and Semantics

In order to develop an 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 among different name spaces.

One way of implementing an NRS is by extending the basic ICN TLV 
format and semantics [RFC8609] [RFC8569]. For instance, name 
resolution and response messages can be implemented by defining new 
type fields in the Interest and Content Object messages [CCNxNRS]. 
Then it allows the ICN architecture to minimize implication of ICN 
arachitectural changes. But NRS system cannot support more flexible 
and scalable designs cause to restrict basic ICN protocol and 
semantics.
On the other hand, an 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 an 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.

6. IANA Considerations

There are no IANA considerations related to this document.

7. Security Considerations

When NRS is integrated into an ICN architecture, security threats will be increased in various aspects as follows:

- Name Space Management: In order to deploy an NRS in ICN architecture, ICN name spaces, which are assigned by various authoritative publishers, 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, so that the verification for mapping among different name spaces should be securely required.

- 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.

- NRS Protocols and Messages: In NRS system, additional messages relatively lookup, update, etc., are flooding to unauthorized networks, so that more security threats can be increased, such that an adversary can manipulate these messages by hijacking to response fake messages. After then a lot of problems as similar with IP network's security issues, affect whole ICN architectures. Therefore, security mechanisms such as accessibility, authentication, etc., [NRSguidelines] for NRS system should be considered to protect the ICN architecture as well as the NRS.

8. References

8.1. Normative References


8.2. Informative References


[SAIL] "FP7 SAIL project.", http://www.sail-project.eu/.

[MF] "NSF Mobility First project.", http://mobilityfirst.winlab.rutgers.edu/.


Authors’ Addresses

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

Email: jhong@etri.re.kr
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

Ved Kafle
NICT
4-2-1 Nukui-Kitamachi
Koganei, Tokyo 184-8795
Japan
Email: kafle@nict.go.jp