ICN Research Group
Internet-Draft
Intended status: Informational
Expires: April 2, 2017

J. Hong
T. You
Y-G. Hong
ETRI

September 29, 2016

# Requirements for Name Resolution Service in ICN
## draft-hong-icnrg-nrs-requirements-00

## Abstract

This document discusses the motivation and requirements for Name Resolution Service (NRS) in ICN. The NRS in ICN is to translate object names into routing hints such as locators, where names are location-independent and locators are network addresses.

## 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 http://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 April 2, 2017.

Table of Contents



## 1. Introduction

The current Internet is a host-centric networkAhlgrening, where hosts are uniquely identified with IP addresses and communication is possible between any pair of hosts. Thus, information in the current Internet is identified by the name of host where the information is stored. In contrast to the host-centric networking, the primary communication objects in Information-centric networking (ICN) are the

named data objects (NDOs) and they are uniquely identified by the location-independent names. Thus, ICN aiming to the efficient dissemination and retrieval of the NDOs in a global scale has been recognized as a promising technology for the future Internet





architecture to overcome the limitations of the current Internet such as scalability, mobility, etc [Ahlgren] [Xylomenos].

ICN alsoBaccelliBaccelliBaccelli has been emerged as a candidate architecture for IoT environment since IoT focuses on data and information rather than end-to-end communications [Baccelli] [Amadeo] [Quevedo]. In addition, the following ICN features are fulfilling well the architectural requirements of IoT such as naming, name resolution, scalability, resource constraints, mobility, caching, security, privacy, etc. [Amadeo2] [Zhang]:

- Naming of data, devices, and services independently from their locations
- Distributed caching and processing
- Decoupling between sender and receiver
- Mobility support
- Authentication and verification of content

Since naming data independently from the current location where it is stored is a primary concept of ICN, how to discover the NDO using the location-independent name is one of the most important design challenges in ICN. There are several projects for ICN which adopt the lookup-by-name routing scheme exploiting the name resolution service (NRS) to discover the NDO using the location-independent name, where the NRS for ICN is to translate object names into routing hints such as locators. Thus, in this document, we provide the motivation and the requirements in designing the NRS for ICN.

## 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. Motivation

In this section, we provide why NRS is needed in ICN and how it will fit into ICN architecture.

ICN routing is a process how to retrieve the NDO based on its name independently from its network address and may comprise three steps: name resolution, content discovery, and content delivery. Depending on how these steps are combined, ICN routing schemes can be categorized as Route-By-Name Routing (RBNR), Lookup-By-Name Routing





(LBNR), and Hybrid Routing (HR). RBNR omits the first name resolution step and directly uses the name to route the request to the NDO. LBNR uses the first name resolution step to translate the name into its locator and the second content discovery step is based on the locator. HR combines RBNR and LBNR to benefit from their advantages [RFC7927].

CCN [Jacobson] and NDN [Zhang2] are the instantiation of RBNR. On the other hand, LBNR is used in NetInf [Dannewitz], MobilityFirst [Seskar], and IDNet [Jung]. Consequently, NRS is necessary unless RBNR itself is chosen as an ICN routing scheme. NRS is also required in ICN for the efficient support of a flat name such as self-certifying identifier as well as the efficient mobility support including the provider mobility.

There are several ICN projects which have their own NRS mechanisms as an important component in their architecture. For instance, NetInf, MobilityFirst and IDNet have MDHT [Dannewitz2], DMap [Vu] and BNRS [Hong], respectively.

NRS for ICN will be a distributed system as an infrastructure in ICN and will be implemented as a control plane completely separated from data plan.

## 4. Requirements for NRS in ICN

In this section, we provide the requirements for designing NRS in ICN in terms of operability, security and manageability, respectively.

### 4.1. Requirements on Operability

The requirements on operability aspect are things that should be considered when the key operations of NRS are designed.

#### 4.1.1. Scalability

The number of NDOs as well as users/publishers is ever-increasing and it will be more than the order of 10^15 by the sensor data in IoT environment. Thus, NRS has to be scalable to support such a large number of NDOs.

#### 4.1.2. Low latency

The process of the name resolution has to be completed within a minimum delay. If the latency gets too long, then the initial packets of many new sessions may get dropped or it will yield the high response time for end users. For example, in order to browse one web-page which includes several data objects in it, multiple name





resolution queries can be processed at the same time and the latency has to be user-tolerant.

#### 4.1.3. Fast Update

The update process of NRS has to be fast enough to provide up-to-date information since the copies of the data objects are frequently created/disappearing as well as NDOs are moving in a highly dynamic environment. Otherwise, the NRS may return the stale information.

#### 4.1.4. Locality

In order to achieve the low latency, NRS has to minimize the total traffic and especially the inter-domain traffic. Thus, NRS has to keep the name resolution and data retrieval local, which yields the improvement of network efficiency.

#### 4.1.5. Resilience

If the resolution service fails, there is mostly no way for the user to reach other end systems as the user knows only their names. Thus NRS has to be resilience to the failures.

#### 4.1.6. Fault tolerance / Isolation

NRS has to be implemented as a distributed system in order to avoid a single point of failure. In addition, the architecture of NRS has to provide fault isolation, which means that the failure part of NRS has to have an impact only locally.

### 4.2. Requirements on Manageability

Requirements on manageability are things that should be considered in terms of the system management aspect.

#### 4.2.1. Manageabiliyt

NRS has to be manageable since some parts of the system may grow or shrink dynamically and a name resolution server may be added or deleted.

#### 4.2.2. Deployability

Deployability is important for a real world system. If the NRS can be deployed from the edges, then the deployment can be simplified.





#### 4.2.3. Interoperability

NRS has to support interoperability between the existing IoT applications since they have their own ways for data management.

### 4.3. Requirements on Security

Requirements on security are things that should be considered in terms of the security aspect for both the node and data.

#### 4.3.1. Access control

A user may want to make a data copy known and accessible only within the local network. In this case, the access control for the information of the data stored in NRS is required. In addition,

unauthorized devices may access the NRS network.

#### 4.3.2. Authentication

Users/nodes that register themselves with NRS server require the authentication to ensure who claims to be. For example, the attacker can act as a fake NRS server which causes disruption or intercepts the data.

#### 4.3.3. Data confidentiality

NRS has to keep the data confidentiality to prevent a lot of sensitive data from reaching unauthorized data requestor in IoT environment.

#### 4.3.4. Data integrity

NRS has to keep the data integrity to assure the trustworthiness and accuracy of the information.

#### 4.3.5. Privacy

When a private data is registered in the system, NRS has to support the privacy to avoid the information leaking. Otherwise, unauthorized entity may disclose the privacy.

## 5. Use case of NRS

### 5.1. Lookup by Name Routing (LBNR)

In this subsection, we discuss some use cases of NRS according to the mapping record type:





- Name to locator(s): Mapping name to locator(s) is a primary record type in NRS for ICN, where locator denotes routable information. Although name can be hierarchical or flat, this type of NRS is more essential for flat name support. In addition, provider mobility as well as host mobility can be supported efficiently and inherently through this type of mapping. A name registered in NRS can be mapped into multiple locators due to the in-network caches in ICN.

- Name to name (alias): Even in RBNR scheme, if provider changes the name to another name which is designed for aggregation by provider, the resolution of the initial name into the aggregated name is required [8].

- Name to IP address: From an incremental deployment perspective, even RBNR would need to map the name onto IP address to access the current Internet (IP network) if necessary.

## 5.2. Route by Name Routing (RBNR)

[TBD]

## 5.3. Hybrid Routing (HR)

[TBD]

# 6. IANA Considerations

There are no IANA considerations related to this document.

# 7. Security Considerations

[TBD]

# 8. Acknowledgements

[TBD]

# 9. References

## 9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.





[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", RFC 7927, DOI 10.17487/RFC7927, July 2016, <http://www.rfc-editor.org/info/rfc7927>.

## 9.2. Informative References

[Ahlgren] Ahlgren, B. et al, , "A Survey of Informaiton-Centric Networking", IEEE Communications Magazine vol. 50, no. 7, July 2012.

[Xylomenos] Xylomenos, G. et al., , "A Survey of Information-Centric Networking Research", IEEE Communications Surveys and Tutorials vol. 16, no. 2, 2014.

[Baccelli] Baccelli, E., Mehlis, C., Hahm, O., Schmidt, T., and M. Wahlisch, "Information Centric Networking in the IoT: Experiments with NDN in the Wild", ACM ICN , September 2014.

[Amadeo] Amadeo, M., Campolo, C., Iera, A., and A. Molinaro, "Named data networking for IoT: An architectural perspective", European Conference on Networks and Communications , July 2014.

[Quevedo] Quevedo, J., Corujo, D., and R. Aguiar, "A case for ICN usage in IoT environments", IEEE GLOBECOM , 2014.

[Amadeo2] Amadeo, M. et al., , "Information-centric networking for the internet of things: challenges and opportunitiesve", IEEE Network vol. 30, no. 2, July 2016.

[Zhang] Zhang, Y. et al., , "Requirements and Challenges for IoT over ICN", Internet Draft, draft-zhang-icnrg-icniot-requirements-01 , April 2016.

[Jacobson] Jacobson, V. et al., , "Networking named content", Proceedings of the 5th international conference on Emerging networking experiments and technologies , December 2009.

[Zhang2] Zhang, L. et al., , "Named data networking", ACM SIGCOMM Computer Communication Review vol. 44, no. 3, July 2014.

[Dannewitz]
Dannewitz, C. et al., , "Network of Information (NetInf)- An information centric networking architecture", Computer Communications vol. 36, no. 7, April 2013.

[Seskar] Seskar, I., Nagaraja, K., Nelson, S., and D. Raychaudhuri, "MobilityFirst Future Internet Architecture Project", 7th Asian Internet Engineering Conference , November 2011.

[Jung] Jung, H. et al., , "IDNet: Beyond All-IP Network", ETRI Jouranl vol. 37, no. 5, October 2015.

[Dannewitz2]
Dannewitz, C., DAmbrosio, M., and V. Vercellone, "Hierarchical DHT-based name resolution for Information-Centric Networks", Computer Communications vol. 36, no. 7, April 2013.

[Vu] Vu, T. et al., , "DMap: A Shared Hosting Scheme for Dynamic Identifier to Locator Mapping in the Global Internet", IEEE 32nd International Conference on Distributed Computing Systems , 2012.

[Hong] Hong, J., Chun, W., and H. Jung, "Demonstrating a Scalable Name Resolution System for Information-Centric Networking", ACM ICN , September 2015.

Authors' Addresses

Jungha Hong
ETRI
161 Gajeong-Dong Yuseung-Gu
Daejeon 305-700
Korea

Phone: +82 42 860 0926
Email: jhong@etri.re.kr

Tae-Wan You
ETRI
161 Gajeong-Dong Yuseung-Gu
Daejeon 305-700
Korea

Phone: +82 42 860 0642

Email: twyou@etri.re.kr





Yong-Geun Hong
ETRI
218 Gajeongno, Yuseong
Daejeon 305-700
Korea

Phone: +82 42 860 6557
Email: yghong@etri.re.kr