Internet Engineering Task Force
Internet Draft
Intended status: Informational
Expires: January 17, 2017

Lijun Dong
Cedric Westphal
GQ Wang
Huawei Technologies
Jianping Wang
City University Hong Kong
July 18, 2016

Requirements of Name Resolution Service in ICN
draft-dong-icnrg-nrs-requirement-00

Abstract

This document summarizes the existing approaches for name resolution in various ICN architectures, and categorizes them into two groups: (1) standalone name resolution; (2) name based routing. It compares the two types of approaches from the aspects of update message overhead, resolution capability, node failure impact, and maintained database. And hybrid approaches also exist with a subnet of routers carrying out name based routing. Despite the coexistence of different name resolution approaches, the Name Resolution Service (NRS) is most essential service that shall be provided by the ICN infrastructure. The document gives the definition of NRS in ICN and proposes some requirements of NRS, i.e. resolution guarantee, delay sensitivity, minimum inter-domain traffic, failure resilience, accuracy, security and accessibility, scalability, and time transiency, support for manifest, interoperability, resolution result selection, heterogeneity, unspecified Content Name.

This document expires on January 17, 2017.

Copyright Notice

Table of Contents

1. Introduction

Information Centric Networking (ICN)[1] has been identified and acknowledged as the most promising architecture for the future Internet as well as the future Internet of Things(IoT)[2][3]. There are existing efforts in designing the ICN architecture, such as DONA[4], PURSUIT[5], NDN[7][10], CCN[8], SAIL[6], MobilityFirst[9]. Most ICN architectures are centered around routing for content retrieval.

ICN routing generally involves three steps:

- Name resolution[11][12][14][15][17][18]: matches/translates a content name to locators of providers/sources that can provide the content.

- Content request routing: routes the content request towards the producer either based on the name or the locator. The process of name resolution and content request routing can be integrated. If integrated, the content request is routed by name, such as in NDN/CCN. If not integrated, the content request is routed by the locator obtained from the previous name resolution step, such as in DONA, PURSUIT, SAIL, MobilityFirst.

- Content delivery: Constructs a path for transferring the content from the provider to the requester. In the integrated approach, content can be routed using breadcrumbs left by the request to define a reverse path, or by some other mechanism, such as including a locator for the requester in the content request. In the uncombined approach, the content can be routed from the provider back to the request through an independent path.

Thus the name resolution process in ICN architectures either can be separated from the message routing (e.g. routing of content request message) as a standalone process or can be integrated with the message routing as one combined process. The former is referred as standalone name resolution approach, the latter is referred as name based routing approach in this document.

In the case that the content request also specifies the reverse path, as in NDN/CCN, the name resolution mechanism also determines the routing path for the data. This adds a requirement on the name resolution service to propagate interest in a way that is consistent with the subsequent data forwarding. Namely, the interest must select a path for the data based upon the finding the copy of the content, but also properly delivering the data.

A hybrid approach would combine name resolution as a subset of routers on the path with some tunneling in between (say, across an administrative domain) so that only a few of the nodes in the architecture perform name resolution in the name-based approach.

Additionally, some other intermediary step may be included in the name resolution, namely the mapping of one name to other names, in order to facilitate the retrieval of named content, by way of a manifest[24][25]. The manifest is resolved using one of the two above approaches, and it may include further mapping of names to content and location. The steps for name resolution then become: first translate the manifest name into a location of a copy of the manifest; the manifest includes further names of the content components, and potentially locations for the content. The content is then retrieved by using these names and/or location, potentially resulting in additional name resolutions.

1.1. Comparison of Standalone Name Resolution and Name based Routing Approaches

The following compares the standalone name resolution and name based routing approaches from different aspects:

- Update message overhead: The update message overhead is due to the change of content reachability, which may include content caching or expiration, content producer mobility etc. The name based routing approach may require to flood part of the network for update propagation. In the worst case, the name based routing approach may flood the whole network (but mitigating techniques may be used to scope the flooding). The standalone name resolution approach only requires to update propagation in part of the name resolution overlay.

- Resolution capability: The standalone name resolution approach can guarantee the resolution of any content in the network if it is registered to the name resolution overlay (assuming the content is being broadcast in the overlay after it is registered). On the other hand, the name based routing approach can only promise a high probability of content resolution, depending on the flooding scope of the content availability information (i.e. content publishing message and name based routing table).

- Node failure impact: Nodes involved in the standalone name resolution approach are the name resolution overlay servers (e.g. Resolution Handlers in DONA), while the nodes involved in the name based routing approach are routers which route messages based on locally maintained name based routing tables (e.g. NDN routers). Node failures in the standalone name resolution approach may cause some content resolution to fail even though the content is available. This problem does not exist in the name based routing approach because other alternative paths can be discovered to

bypass the failed ICN routers, given the assumption that the network is still connected.

- Maintained databases: The storage usage for the standalone name resolution approach is different from that of the name based routing approach. The standalone name resolution approach typically needs to maintain two databases: name to locator mapping in the name resolution overlay and routing tables in the routers on the data forwarding plane. The name based routing approach needs to maintain different databases: name routing table and optionally breadcrumbs for reverse routing of content back to the requester.

2. Definition of Name Resolution Service in ICN

In ICN design, a name is used to identify an entity, such as named data content, a device, an application, a service. ICN requires uniqueness and persistency of the name of any entity to ensure the reachability of the entity within certain scope and with proper authentication and trust guarantees. The name does not change with the mobility and multi-home of the corresponding entity. A client can always use this name to retrieve the content from network and verify the binding of the content and the name. Ideally, a name can include any form of identifier, which can be flat, hierarchical, and human readable or non-readable.

The Name Resolution Service (NRS) is defined as the service that is provided by ICN infrastructure to help a client to reach a specific piece of content, service, or host using a persistent name. The NRS could take the standalone name resolution approach to return the client with the locators of the content, which will be used by the underlying network as the identifier to route the client's request to one of the producers. The examples are iDNS [18], Global Name Resolution Service (GNRS)[9], and Locator/ID Separation Protocol (LISP)[26][27]based approach. The NRS could take the name based routing approach, which integrates the name resolution with the content request message routing. No matter which approach is taken by the NRS in ICN, it is the most essential component or service of the ICN infrastructure. The NRS could also take hybrid approach which can perform name based routing approach from the beginning, when it fails at certain router, the router can go back to the standalone name resolution approach. The alternative hybrid NRS approach also works, which can perform standalone name resolution approach to find locators of routers which can carry out the name based routing of the client's request.

3. Requirements of Name Resolution Service in ICN

3.1. Resolution Guarantee

The NRS must ensure the name resolution success if the matching content exists in the network, regardless of its popularity, number of cached copies.

3.2. Delay Sensitivity

The name resolution process provided by the NRS must not introduce significant latencies. With more number of name record replications, the number of nodes involved in the name resolution may be reduced. For example, in the standalone name resolution approach, with the name record being replicated to higher hierarchy or the peer NRS server in the overlay, the name resolution can be responded more promptly. In the content based routing approach, with the content based routing table being broadcast within the larger scope in the network, the name resolution and request routing can have higher probability to successfully reach the nearer copy of the requested content.

The NRS deployment should balance the number of nodes involved in the name resolution and the overhead/cost for the name record replication. To ensure the low latency, the NRS should be able to route a content request to the closest copy. Message forwarding and processing should be efficient and computation complexity should be reasonable low and affordable by the current processor technologies.

3.3. Minimum Inter-Domain Traffic

The NRS must attempt to minimize total traffic, and inter-domain traffic in particular. In order to achieve that, message propagation for name resolution and retrieval should retain the locality and should be kept in the network domain if that domain contains both the client and the content copy.

For example, a client is requesting the temperature data of the building that he/she is residing in, the NRS should be able to return or route to the nearest gateway in the building that stores such data instead of a remote server in the cloud.

3.4. Failure Resilience

The NRS must ensure resilience to node failures. After a NRS node fails, the NRS system must be able to restore the name records

stored in the NRS node. The NRS must also ensure resolution failure at one NRS node would be resolved and corrected by other NRS nodes.

For example, in the standalone name resolution approach, when a NRS overlay server fails, the name records should be able to transferred and recovered in its peer server or its replacement. In the content based approach, the failure of one ICN router does not cause much trouble in the name resolution, because the other alternative paths can be established that bypass the failed ICN router. However, it requires that the ICN router has propagated its content based routing information in the network.

3.5. Accuracy

The NRS must provide accurate and up-to-date information on how to reach the producer(s) of requested content with minimum overhead in propagation the update information. Content mobility and expiration must be reflected in the corresponding records in the NRS system with minimum delay to guarantee the accurate resolution.

For example, a content can be moved from one domain to another domain due to the mobility of the producer, then the old name record should be deleted from the NRS system and a new name record should be added and updated with minimum delay.

3.6. Security and accessibility

The NRS system must be prevented from the malicious users attempting to hijack or corrupt name records.

The name records must have proper access rights such that the information contained in the name record would not be revealed to unauthorized users.

The name records may be associated within certain domain, and cannot be propagated outside the domain. For example, for content that is only shared within the community should be restricted within the community network, outside of which the content does not exist.

3.7. Scalability

The NRS system must to be extremely scalable to support a large number of content objects as well as billions of users, who may access the system through various connection methods and devices. Specially in IoT applications, the data size is small but frequently generated by sensors.

Message forwarding and processing, routing table building-up and name records propagation must be efficient and scalable. The memory requirement for NRS nodes should be achievable by the current memory technologies.

3.8. Time Transiency

The NRS should support time-transient content, which is frequently created in and disappearing from the network. This kind of content only stays in the network for a short time, which requires the NRS be able to promptly reflects the records of them in the system. For example, some video clip only exists in the network for a very short time, which requires the NRS to promptly update their name records.

3.9. Support for manifest

The NRS should support resolution using manifests. Namely, if a content object is described by a manifest, the NRS should support efficient recursive resolution of the names included in the manifest. Alternatively, if the manifest contains mapping of content names to location (for instance, DASH manifest contain additional Base URL for a specific content stream), then this should be consistent with the mapping obtained from the NRS.

3.10. Interoperability

Considering the emergence of IoT applications, many standard bodies for IoT have settled their ways for resource/data management. For example:

- oneM2M[19] uses tree structure to store resources. Each resource is addressable by its URI. oneM2M resources are linked together by parent-child relationship or link relationship with pointers. Resource resolution is indicated in the hierarchical name of the resources. With one entrance, a client can go anywhere within the tree structure. As an example, a content is stored under the container with URI prefix of /CSEBase-ID/AE-ID/container-ID/contentInstance-ID. From the URI of the content, a client would be able to easily do the name resolution and go to the oneM2M server identified by CSEBase-ID.

- IETF CoRE[21] specifies the Resource Directory (RD) [23] for resource registration and resolution. A RD is a database that stores links about resources hosted by endpoints (EP), which are called RD entries. An EP is a server that is associated with a scheme (e.g. CoAP[22] by default, or HTTP), IP address and port. It is likely that a physical IoT node may host one or more EPs.

The RD provides a set of RESTful interface for EPs to register and maintain sets of RD entries, and for clients to look up resources.

In order for the ICN infrastructure to support IoT applications, the NRS should provide the interoperability between those existing resource registries as well as integration of them into the ICN infrastructure. The NRS should allow different providers to coexist and for requesters to choose one or more preferred providers on their own.

3.11. Resolution Result Selection

The NRS may be able to return some of the active producers or all of them for the client's selection or select the best producer based on the client's criteria and context information, e.g. producer with least load, with least response time, etc.

3.12. Heterogeneity

There are heterogeneous content naming schemes[16][19] and name resolution approaches from different ICN architectures. For example:

- Names in DONA[1] consist of the cryptographic hash of the principal's public key P and a label L uniquely identifying the information with respect to the principal. Name resolution in DONA is provided by specialized servers called Resolution Handlers (RHs).

- Content in PURSUIT[5] is identified by a combination of a scope ID and a rendezvous ID. The scope ID represents the boundaries of a defined dissemination strategy for the content it contain. The rendezvous ID is the actual identity for a particular content. Name resolution in PURSUIT is handled by a collection of Rendezvous Nodes (RNs), which are implemented as a hierarchical Dynamic Hash Table (DHT)[13][14].

- Names in NDN/CCN[8][10] are hierarchical and may be similar to URLs. Each name component can be anything, including a dotted human-readable string or a hash value. NDN/CCN adopts the name based routing. The NDN router forwards the interest by doing the longest-match lookup in the Forwarding Information Base (FIB) based on the content name and the interest is stored in the Pending Interest Table (PIT).

- In MobilityFirst[9], every network entity, content has a Global Unique Identifier (GUID). GUIDs are flat 160-bit strings with no

semantic structure. Name Resolution in MobilityFirst all is carried out via a Global Name Resolution Service (GNRS).

Although the existing naming schemes are different, they all need to provide basic functions for identifying a content, supporting trust provenance, content lookup and routing. The NRS may combine the advantages of different mechanisms. The NRS may be able to provide a generic naming schema to resolve any type of content name, either it is flat or hierarchical.

3.13. Unspecified Content Name

Currently, both the standalone name resolution and name based routing approaches assume that the content name is known and specified by the client, which is sometimes not the case. A client may not know the exact name of the data that he/she is requesting, for example, a client wants to retrieve the temperature data on 07/21/2015 in San Diego. In this case, the client is only able to specify some semantics and contextual information of the data that he/she is looking for.

The NRS may be able to resolve those requests by having a northbound interface to the other services, which can return the content name(s) matching the client's request.

4. IANA Considerations

This document makes no specific request of IANA.

5. Conclusions

In this draft, we broaden the definition of NRS in the ICN infrastructure as the service which can help a client to reach a producer of the requested content. Thus the NRS could take the approaches of standalone name resolution, name based routing or hybrid of the two. With the essence of NRS, it is urgent to identify the requirements for the NRS design in ICN. In the draft, we propose the NRS requirements from the different aspects and elaborate each of them with examples for verification of its importance.

6. Informative References

[1] G. Xylomenos, C. N. Ververidis, V. A. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K. V. Katsaros, and G. C. Polyzos, A Survey of Information-Centric Networking Research, Communications Surveys and Tutorials, Vol. 16, No. 2, 2014, P. 1024-1049.

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

[3] Amadeo, M., Campolo, C., Iera, A., and A. Molinaro, Named data networking for IoT: An architectural perspective, in European Conference on Networks and Communications (EuCNC), 2014.

[4] T. Koponen, M. Chawla, B. Chun, A. Ermolinskiy, K. H. Kim,S. Shenker, and I. Stoica, "A Data-Oriented (and Beyond) Network Architecture." in ACM SIGCOMM, 2007, pp. 181-192.

[5] FP7 PURSUIT project. http://www.fp7-pursuit.eu/PursuitWeb/.

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

[7] NSF Named Data Networking project. http://www.named-data.net/.

[8] Content Centric Networking project. http://www.ccnx.org/.

[9] NSF Mobility First project. http://mobilityfirst.winlab.rutgers.edu/.

[10] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking Named Content." in ACM CoNEXT, 2009.

[11] A. Baid, T.Vu, and D. Raychaudhuri, "Comparing Alternative Approaches for Networking of Named Objects in the Future Internet." in IEEE Workshop on Emerging Design Choices in Name-Oriented Networking (NOMEN), 2012.

[12] M. F. Bari, S. R. Chowdhury, R. Ahmed, R. Boutaba and B. Mathieuy, "A Survey of Naming and Routing in Information-Centric Networks.", IEEE Communications Magazine, Vol. 50, No. 12, P. 44-53.

[13] J. Rajahalme, M. Sarela, K. Visala, and J. Riihijarvi, "On Name-based Inter-domain Routing," Computer Networks, vol. 55, no. 4, pp. 975-986,March 2011.

[14] K. V. Katsaros, N. Fotiou, X. Vasilakos, C. N. Ververidis, C. Tsilopoulos, G. Xylomenos, and G. C. Polyzos, "On Inter-Domain Name Resolution for Information-Centric Networks," in Proc. IFIP-TC6 Networking Conference,2012.

[15] Namespace Resolution in Future Internet Architectures,draft-wang-fia-namespace-01.

[16] PID: A Generic Naming Schema for Information-centric Network, draft-zhang-icnrg-pid-naming-scheme-03.

[17] D. Zhang, H. Liu, Routing and Name Resolution in Information-Centric Networks, 22nd International Conference on Computer Communications and Networks (ICCCN), 2013.

[18] S. Sevilla, P. Mahadevan, J. Garcia-Luna-Aceves, "iDNS: Enabling Information Centric Networking Through The DNS." Name Oriented Mobility (workshop co-located with Infocom 2014).

[19] On the Naming and Binding of Network Destinations, https://tools.ietf.org/html/rfc1498.

[20] oneM2M Functional Architecture TS 0001, http://www.onem2m.org/technical/published-documents.

[21] Constrained RESTful Environments, CoRE, https://datatracker.ietf.org/wg/core/charter/, 2013.

[22] RFC 7252, The Constrained Application Protocol (CoAP).

[23] CoRE Resource Directory, https://datatracker.ietf.org/doc/draft-ietf-core-resource-directory/.

[24] C. Westphal, E. Demirors, An IP-based Manifest Architecture for ICN, 2nd ACM Conference on Information-Centric Networking (ICN 2015).

[25] M. Mosko , G. Scott , I. Solis , C. Wood CCNx Manifest Specification, http://www.ccnx.org/pubs/draft-wood-icnrg-ccnxmanifests-00.html.

[26] The Locator/ID Separation Protocol (LISP), https://datatracker.ietf.org/doc/rfc6830/.

[27] Locator/ID Separation Protocol (LISP) Map-Server Interface, https://datatracker.ietf.org/doc/rfc6833/.

Authors' Addresses

Lijun Dong
Huawei Technologies
10180 Telesis Court
Suite 220
San Diego, CA, 92121

Phone:
Email: lijun.dong@huawei.com

Cedric Westphal, GQ Wang
Huawei Technologies
2330 Central Expressway
Santa Clara, CA 95050

Phone:
Email: {cedric.westphal,gq.wang}@huawei.com

Jianping Wang
City University Hong Kong

Email: jianwang@cityu.edu.hk