Addressing in Future Internet: Problems, Issues, and Approaches

Jaeyoung Choi, Chulhyun Park, Hakyung Jung, Taekyoung Kwon, Yanghee Choi
School of Computer Science and Engineering
Seoul National University, Seoul, Korea
{jychoi, chpark, hkjung}@mmlab.snu.ac.kr and {tkkwon, yhchoi}@snu.ac.kr

Abstract

The current Internet addressing has faced several challenges such as routing scalability, mobility and multi-homing support. To solve the current problems, it is required to redesign the basic principles of Internet addressing architecture. This paper investigates the major requirements of addressing, and pinpoints two viable principles for Future Internet: identifier / locator split and route-by-name. We also explore other research issues in designing an addressing architecture.

Introduction

As the Internet is widely deployed and commercially used, many unexpected problems arise. First, it can happen the exhaustion of address in the Internet. Some people insist that we can overcome with help of Network Address Translation (NAT) or IPv6 protocol. But, NAT violates the end-to-end principle of Internet and IPv6 is not practically used yet. Also, IAB workshop has addressed the problem of routing scalability [1], and it has not clearly resolved yet. Moreover, the current architecture of Internet hardly supports mobility, multi-homing, and QoS provision. Although several novel schemes are proposed to solve these issues, most of the schemes cannot overcome the bounds of the underlying architecture.

To break through this situation, some researchers start to rethink about the fundamental design principles of Internet. The Future Internet Design (FIND) project of United States [2], Network of the Future project of European Union [3], New Generation Network (NGN) project of Japan [4], and Future Internet Forum (FIF) of Korea [5] are the most representatives. There is a consensus that clean-slate approach may have to be taken for the fundamental design of Internet. For convenience, we call an ideal network which is free from current architectural limitations and can meet the emerging requirements as the *Future Internet*.

In this paper, we focus on only addressing among numerous areas of Future Internet. The identification scheme including naming and addressing is the most essential and important part of a network because the basic functionalities of a network tightly depend on it. Also, addressing may be the most critical part which influences on performances and functionalities of a network.

This paper is organized as follows. First, we investigate the major requirements which should be considered in designing addressing in Future Internet. Then, we present the outline of the addressing architecture in Future Internet based on identifier / locator split and route-by-name paradigm, and contemplate which is appropriate for each namespace of identifier and locator. Lastly, we explore the other research issues related with the addressing of Future Internet.

Requirements for the Future Internet addressing

Routing Scalability

In current Internet, it is known that the increasing rate of unaggregatable routing entries is so fast that the development speed of high-end hardware for core routers will not meet the performance requirement of processing routing entries [1]. The first reason is that the customers generally prefer to get Provider Independent address (PI address) space, which remains unchanged even though the customer changes its provider. So the PI address space can give many benefits in management of IP addresses, while usually the PI address space of a customer cannot be aggregated with provider's address space. Multihoming is another reason. When a site has two or more outgoing internet connectivity through more than one ISP, an address block given by each ISP should be stored in other ISPs' routing tables. The last reason is traffic engineering. Because of traffic engineering, a path to destination may not be equal to shortest path in the topology. In this case, each path information is also stored in the routing table individually. For these reasons, the size of routing table at core routers is increasing rapidly, and the performance of core routers may reach its

performance limit in near future. So it is required that the addressing and routing architecture of the Future Internet should scale well.

Identifier/Locator split

The fact that an IP address serves as both an endpoint identifier for the transport layer and a locator for the routing protocol is referred to as *Identifier/Locator overload*. Overloading an address with two semantics has hindered the Internet from supporting routing scalability, mobility, and multi-homing. Stated reversely, we may resolve the above issues just by decoupling the semantics of locators and identifiers. By separating them, we can make the routing infrastructure scalable by promoting topological aggregation of locators. Moreover, a mapping function between identifiers and locators naturally can support mobility and multi-homing features by establishing one-to-one or one-to-many relationships, respectively. Thus, we insist that the Future Internet have separate addressing schemes for each identifier and locator.

Security

Most of the security problems of the current Internet stem from the open communication principle and global addressing: in Internet, every host has been assigned a global address and any host can send a packet to any place only if the host knows only the address. The first problem is that a server cannot identify whether the client is malicious or not before communicating for some time. Even though the server can identify the malicious client, it cannot prevent the attack like Denial-Of-Service (DOS) [6]. The second problem is the open networking: a host can overhear the packet which is destined to any host who shares the medium. Even though some schemes are proposed to solve the issue like IPsec [7], the overhead is not negligible. Therefore, the Future Internet should provide security mechanisms as one of the basic funationalities because the Internet is a commercial network and several applications which require the high level of security like e-commerce should be used on the Internet.

Big picture of addressing architecture in the Future Internet

Identifiers and locators are the most essential elements in a network. As described before, an IP address takes in charge of these two roles. Many well-known problems stem from overloading semantics of IP addresses such as mobility, multi-homing, routing scalability, and so on. To prevent this kinds of architectural limitations for the Future Internet, we suggest an identifier and locator should be split in Future Internet.

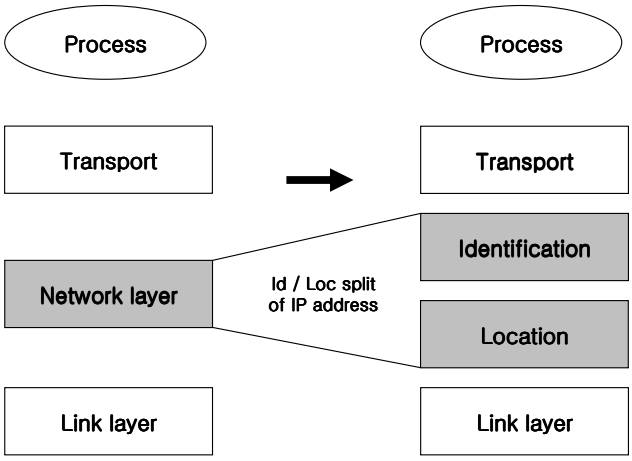

Figure 1. Layering architecture under Id / loc split.

Fig. 1 shows how the Internet layering changes under identifier and locator split; the existing network layer will be split into identification and location layer. In the identification layer, every object has an identifier which is not dependent on the topology or physical location. The identification layer should provide the high-level functionalities which make the Future Internet extensible and useful like access control, QoS provision, mobility and multi-homing supports, dissemination, content/service discovery, and so on. Besides, the location layer should focus on the fast and reliable transmission. Namespace for identifiers and locators will be described below. Fig. 2 summarizes the candidates.

Candidates for identifiers

This subsection compares three types of identifiers for candidates in Future Internet. First, the public key (or its hashed value) of an asymmetric cryptographic scheme may be used as proposed in [8]. As an identifier, a public key of a node has a global uniqueness. Furthermore, it can be exploited to authenticate the node and to encrypt packets to prevent from being attacked. Its human-unfriendly form, however, requires additional indirection overhead from human-readable identifiers such as domain name. Second, we may use a domain name in current Internet as a host identifier in Future Internet. A domain name is also global unique, and does not require additional indirection overhead originated by introducing new identifer name-space. The DNS used to bind domain names to locators in current Internet is inadequate to be adopted intact in Future Internet due to its slow update propagation; thus necessitating a new binding system. Lastly, content iden-

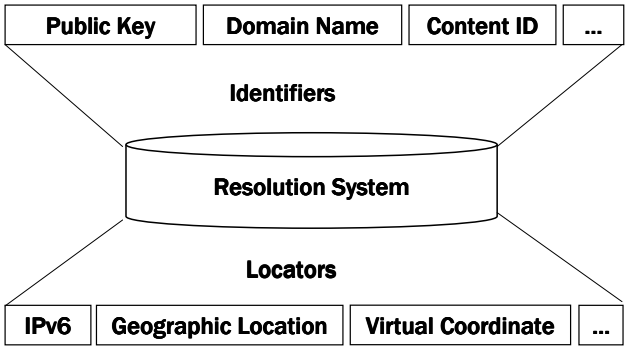

Figure 2. Candidates for identifiers and locators.

tifiers (*e.g.*, URN) can substitute for host identifiers. This type of identifiers naturally support data-oriented paradigm which will be discussed. The suitable structure of a content identifier is an open issue to study.

Candidates for locators

We investigate possible candidates for locator of the Future Internet in this section. First, IPv6 can be regarded as the strongest candidate for locator in the Future Internet. As a substitution of IPv4, IPv6 a provides much larger address space. Moreover, since IPv6 is already being deployed, no radical change for the current routing protocol or device is needed. But the large size of the address field of IPv6 may be unappropriate to the networks composed of nodes with limited capacity, i.e. a sensor network. Because a sensor node is usually battery-powered, the processing and communication capability of a sensor node is adapted to low-power operation. Under this situation, a large size of locator field may act as a burden to a sensor node due to cost in processing and transmitting the packet. The second candidate is the geographical location of a node. A locator based on the geographical location makes routing simpler as greedy routing based on geographical distance can be used, and does not need a central addressing agent like a DHCP server. But all nodes adopted locator based on the geographical location should equip a device for localization like GPS. Last candidate is a virtual coordinate as a locator of a node. Virtual coordinate system usually does not represent an exact location of a node in the topology. Instead, local connectivity information [9] or link-weighted topology information [10] is translated into a virtual coordinate and used for routing. Routing based on virtual coordinates is also performed in a greedy manner in which a packet is sent to a nearer neighbor according to the virtual distance to the destination. The complexity of assigning locators is a defect of the virtual coordinate.

	Lookup-by-name	Route-by-name
Extensibility	bad	good
Routing Efficiency	good	poor
Robustness	poor	good

Table 1. Comparison between lookup-by-name and route-by-name approach.

Route-by-name paradigm

There are two kinds of resolution model: *lookup-by-name* and *route-by-name*. In lookup-by-name, a host first inquires the corresponding locator based on the identifier of a peer before transmission; resolution is decoupled with routing itself. On the other hand, a host transmits its message with the peer's identifier not locator under route-by-name; resolution happens with routing simultaneously. Table 1 shows the qualitative comparison between two approaches. The route-by-name approach is good for extensibility, because it has large room to provide an additional functionality like mobility or multicast streaming. However, the route-by-name approach may decrease the routing performance as it does not forward a packet along with optimal routing path. The route-by-name approach will be more appropriate for the resolution between identifier and locator in Future Internet because extensibility will become more important than routing efficiency due to improvement of hardware technology.

Future Internet research issues related with addressing

Many research issues still remain unresolved in the field of addressing for the Future Internet after the deployment of our proposed addressing architecture. At the same time, we also have many choices to design the addressing architecture of the Future Internet. The design of addressing should be accompanied together with many other research activities such as routing/resolution, QoS provision, or security. Because addressing is the most essential part of a network, once an addressing scheme of a network is accomplished, all other parts of the network will be indispensably confined and restricted. This section lists the remaining research issues and alternatives in addressing.

Content-oriented Network

According to the recent results of traffic measurement of the Internet, most of people use the Internet to acquire the data or get the service [11]. While real Internet usage

Access network integration	Integrated addressing	Separated addressing
Pros	No need for an additional addressing entity	Makes the best use of each access network
Cons	May be unappropriate for each access network	Needs an additional entity to connect to the Internet

Table 2. Access network integration model.

shows patterns like the data-oriented paradigm, the current Internet is designed based on the host-oriented paradigm. This kind of discordance between historical design and current usage lets the design of efficient and flexible data retrieval expensive [12]. We define a network which is designed based on data-oriented paradigm as the *Content-oriented Network*. In content-oriented networks, basic elements of identification scheme will be totally changed from the existing network. The fresh naming and addressing scheme should be investigated with network architecture of content-oriented network.

Location-based addressing

In the case that the geographic location of a host can be easily obtained from its address, we can utilize or optimize the functionalities of a network easily. One area in which we can utilize its functionalities might be the routing; we can reduce the size of routing table drastically by using greedy routing. Geographic routing is already investigated in wireless sensor networks and various geographical routing schemes are proposed including GPSR [13]. But several problems, like traffic engineering or provider-customer relationship support arise when the geographical routing scheme is adapted to the Internet. Besides geographic routing, geographical location of a node can be utilized in many areas of the Future Internet. So it is worth considering location-based addressing and investigating its impact in the Future Internet.

Access network integration

Most of emerging networks such as wireless sensor networks or mesh networks assume that they can be connected with Internet. These access networks may adopt different addressing schemes according to the purpose or characteristics of each network. Therefore, two kinds of major scenarios for integration is possible. Under an integrated addressing scenario, each access network uses the same addressing scheme as the global Internet addressing. On the other hand, in separated addressing scenario an access network uses its own addressing scheme and uses a gateway to communicate with a plain Internet node. Table 2 represents the comparison between these two integration models.

Anonymity, Dynamicity, Temporality

While a traditional network only assumes that objects in the network are stable, permanent and globally unique, an object may need to be anonymous, dynamic, or temporal in the Future Internet. It is because we can not easily emulate the various kinds of semantics, which is required in representing the whole real life, only with stable, premanent, and globally unique objects. Obviously, it is very hard to support this kinds of properties in the network efficiently. With the above properties realized, it can make the Future Internet more richer and extensible to support an object which has no identifier (anonymity), which can mutate (dynamicity), or which exists and then disappears (temporality).

Conclusions

In this paper, we have pointed out the most important requirements of addressing in Future Internet. To reflect these, we propose an outline of the addressing architecture combined with identifier / locator split and route-by-name approach for their resolution. But, there still remain many requirements which are not solved with our proposed architecture. We have realized that the addressing researches should be collaborated with activities of other research areas. It is because that the scope of addressing architecture is too broad to be resolved with a single scheme. Moreover, addressing is too much correlated with other areas like routing, resolution, mobility and multi-homing support, or QoS provision to be investigated alone.

Acknowledgement

This work was supported by the IT R&D program of MKE/IITA [2007-F-038-02, Fundamental Technologies for the Future Internet]. Also, the ICT at Seoul National University provides research facilities for this work.

References

[1] K. F. D. Meyer, L. Zhang. RFC 4984: IETF report from the iab workshop on routing and addressing, September 2007.
[2] http://find.isi.edu/.
[3] http://cordis.europa.eu/fp7/ict/future-networks/.

[4] http://forum.nwgn.jp/.
[5] http://www.fif.kr/.
[6] M. Handley and E. Rescorla. RFC 2401: IETF internet denial-of-service considerations, November 2006.
[7] S. Kent and R. Atkinson. RFC 2401: IETF security architecture for the internet protocol, November 1998.
[8] P. N. R. Moskowitz. RFC 4434: IETF host identity protocol, May 2006.
[9] A. Rao, S. Ratnasamy, C. Papadimitriou, S. Shenker, and I. Stoica. Geographic routing without location information. In *MobiCom '03: Proceedings of the 9th annual international conference on Mobile computing and networking*, pages 96–108, New York, NY, USA, 2003. ACM.
[10] R. Gummadi, R. Govindan, N. Nothari, B. Karp, Y. J. Kim, and S. Shenker. Reduced state routing in the internet. In *HotNets '04: Proceedings of ACM HotNets III Workshop*, November 2004.
[11] http://netflow.internet2.edu/weekly/.
[12] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica. A data-oriented (and beyond) network architecture. In *SIGCOMM '07: Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 181–192, New York, NY, USA, 2007. ACM.
[13] B. Karp and H. T. Kung. Gpsr: greedy perimeter stateless routing for wireless networks. In *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 243–254, New York, NY, USA, 2000. ACM.