Proposal on the Concealment of the Network Topology in IPv6

Toru Kuboshiki and Hidekazu Suzuki and Akira Watanabe
Graduate School of Science and Technology
Meijo University, Nagoya 468-8502, JAPAN
Telephone and Fax: +81-52-838-2279
+81-52-838-2406
Email: toru.kuboshiki@wata-lab.meijo-u.ac.jp
hsuzuki@meijo-u.ac.jp
wtnbakr@meijo-u.ac.jp

***Abstract*—With a possible exhaustion of global IPv4 addresses, shifting to IPv6 is thought to be inevitable. However, when the shifting to IPv6 actually occurs, network topology could be inferred from addresses in the organization. Thus, as a means to conceal network topology, various methods, including the use of Mobile IPv6 and the setting-up of routers for host routes, are being proposed. However, redundant routings become a problem in the case of Mobile IPv6, and increases in the routing tables become a problem in the case of host routing. In this paper, we define new addresses to conceal network topology and propose a communication method using these addresses. We also describe our idea of implementing our method.**

***Index Terms*—IPv6, Topology, Concealment.**

I. Introduction

With a rapid increase in the use of the Internet, possible exhaustion of global IPv4 addresses has become a serious concern. As a short-term solution for the address exhaustion, private addresses have been defined, and in that way, the life of IPv4 has been prolonged. In order to connect private address space with the Internet, NAT (Network Address Translation) is required. Thus, when connection is initiated from the side of the Internet towards a node in the private address space, communication cannot be initiated, because the topology within the private network is unknown. This problem is called "NAT traversal problem", which is an element impeding the universal use of IPv4. In addition, since packet addresses are translated in NAT, applications dealing with address information cannot be used.

On the other hand, the use of NAT has resulted in getting an advantage, as a secondary benefit,that the network topology and addresses in an organization can be concealed. Network administrator within a company usually have a desire of preventing leakage of information to outsiders as much as possible, and therefore, they believe it effective from a viewpoint of security if information of the network can be concealed. Meanwhile, in the Data Security Standard of Payment Card Industry (PCI) [1], organizations handling payment card information are not allowed to reveal addresses within their individual organizations on the Internet.

While NAT has the above-said advantage, we are now facing a serious problem of exhaustion of global IPv4 addresses. In fact, the distribution of addresses from ICANN (Internet Corporation for Assigned Names and Numbers) to Registries in each region was already terminated. It is also reported that the inventory of IPv4 addresses kept at JPNIC (Japan Network Information Center) has also been exhausted [2]. Such being the situation, shifting to IPv6 has become inevitable as a fundamental means of resolving the IPv4 addresses exhaustion problem.

In the case of IPv6, because it does not require NAT, such problems as NAT traversal or restricted applications are automatically resolved, and end-to-end communication (which is the fundamental function of the Internet) is possible. However, at the same time, the secondary benefit of concealing network topology by NAT is also lost. Then, nodes and network topology could be identified from the addresses.

Accordingly, various methods capable of concealing nodes and network topology, even after the shifting to IPv6, have been studied. As a means of resolving the privacy problem with nodes, a method using Temporary Address that creates low-level 64 bit Interface ID on an at-random basis has been defined. However, while Temporary Address can prevent identification of nodes, there is a concern that network topology is still inferred, because the actual Subnet ID is revealed. There are presently the following methods as the technologies capable of concealing network topology.

NPTv6 (IPv6-to-IPv6 Network Prefix Translation) [3], which is a method to translate addresses, has a function similar to NAT in IPv4. Although NPTv6 can conceal the inside of the network, it has a similar problem as NAT in IPv4 has; i.e. applications containing address information in messages like SIP cannot be used. Mobile IPv6 uses a method that applies mobility transparency technology to conceal the network [4]. However, this method has shortcomings of causing extra routing that goes through Home Agent. There exists also a method to use addresses on an at-random basis to conceal network topology. In this method, host routes [4], which are used as the routing means, are set up for all nodes in the router. The problem of this method is that the number of entries at the routing table becomes quite large and as a result, the load on the router may get quite high.

978-1-4577-1295-1/11/$26.00©2011IEEE

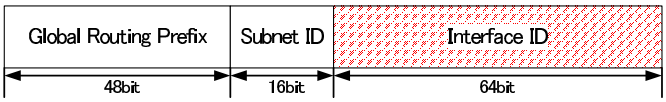


Fig. 1. Temporary Address

Under such circumstances, we propose in this paper a new method to conceal network topology. In our method, we use two different addresses in each node inside the network; namely, one for internal communications and the other for external communications. The selection where address to use out of the two, depends on the location of the node of the communication partner. For communications with a node located outside the network, we use the address of which the portion of Subnet ID and Interface ID are at-randomly generated. We employed the tunnel technology for the routing of packets having this address.

Hereinbelow, we explain several existing technologies in Chapter 2, our proposed method in Chapter 3, our idea of implementing our proposed system in Chapter 4, and the summary in Chapter 5.

II. Existing Technologies

A. Temporary Address

Fig. 1 shows the configuration of Temporary Address (TA) [5]. One of the characteristics of IPv6 is its stateless address automatic configuration. Higher order of 64 bit Global Routing Prefix and Subnet ID are obtained from the advertisement from the router, and Interface ID is generated from MAC address. However, IPv6 has a problem that the node is identified because it contains MAC address. TA can solve this problem and prevent identification of the node by generating lower order of 64 bit on an at-random basis. However, since Subnet ID is shown on the Internet "as is", the internal network topology could be inferred.

B. NPTv6

NPTv6 is a method where addresses are translated even in IPv6. In the case of IPv6, it is normally not necessary to translate addresses because there are plenty of addresses. However, network administrators think that the address management of the network will become easier by using NAT. Although concealment of addresses is not the primary purpose of NPTv6, the interior of the network can be concealed from the side of the Internet as a secondary benefit. In the case of NPTv6, unlike NAT in IPv4, the same number of global addresses as the number of internal nodes is assigned. When translating addresses by NPTv6, the NAT traversal problem does not occur because addresses on the side of the Internet and those of the internal network are translated by matching them one by one. In the outside of NPTv6, addresses having global prefix are assigned, while ULAs (Unique Local Unicast IPv6 Address) [6], which are effective only in the local network, are assigned in the inside of the network. When translating addresses, higher order of 64 bit only is translated while lower order of 64 bit Interface ID is untouched. At that occasion, address translation must be done in such a way that the value of Subnet ID is so adjusted that the check sum does not change. In this method, it is not possible to make communications in the case of applications containing address information in the message, and thus, the advantage of IPv6 is not taken here.

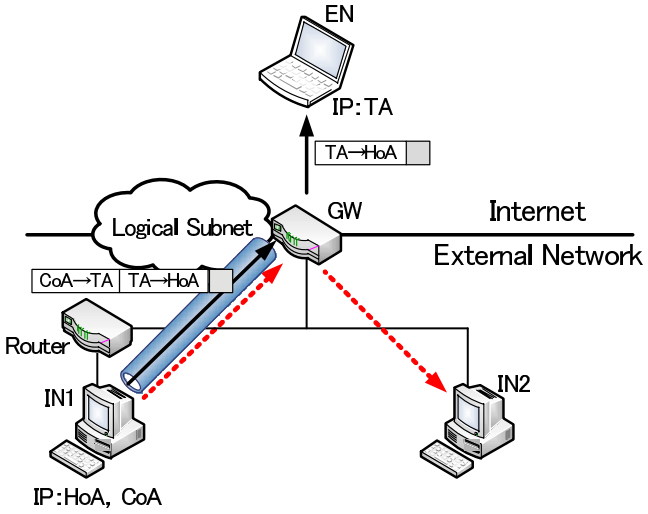


Fig. 2. Network topology concealment by Mobile IPv6

C. Method using Mobile IPv6

Fig. 2 shows an example of network topology concealment by Mobile IPv6. Mobile IPv6 is a technology to realize mobility transparency. Gateway functions as Home Agent (HA) in Mobile IPv6, Internal Node (IN) 1 and 2 function as Mobile Node (MN), and External Node (EN) functions as Correspondent Node (CN). An address, which arbitrarily assigned Subnet ID capable of hiding the inside of the network, is assigned as Home Address (HoA) at IN1. The address area of the Subnet ID is called Logical Subnet. This Logical Subnet exists regardless of the actual network topology. And an address corresponding to the actual network topology is allocated as Care-of Address (CoA). When EN communicates with IN1, IN1 sets a source address at HoA and sends the packet by CoA after encapsulating it. The packet which reached Gateway is decapsulated and delivered to EN. EN is unable to know the actual network topology because the address of IN1 is seen as HoA from the side of EN.

However, this method has the following problems. Mobile IPv6 has a function of route optimization, and when activating this function, IN1 sends the address after move to its communications partner, and intends to make a direct communication without going through HA. In this case, the address containing the network topology is transmitted to CN (namely, CoA is notified to CN), and the network is not concealed. Therefore, it is necessary to inactivate the function of route optimization. As a result, the communication between inside nodes should necessarily go through Gateway. If you want to apply the route optimization to inside nodes only, it is necessary to incorporate a function to filter the route optimization packet in Gateway.

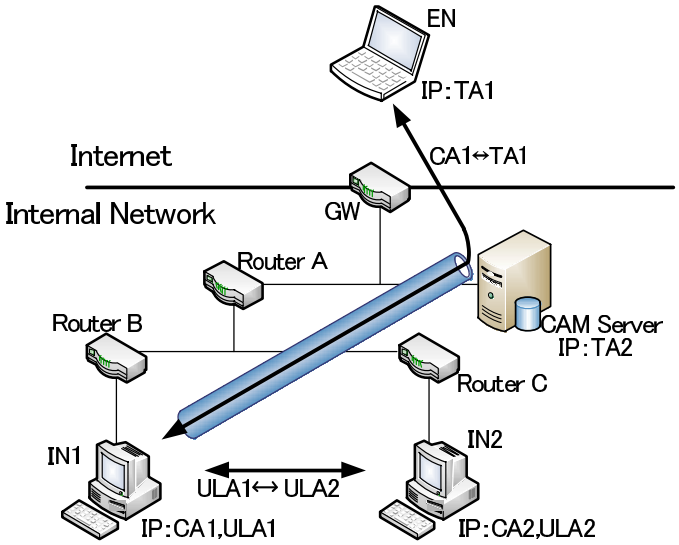


Fig. 3. System configuration of our proposed method

Then, communications go through Gateway, only at the time of communication's start-up.

D. Method using Host Routing

In the case of the method using host routes, an address which sets an arbitrary value in Subnet ID is assigned to each host, and a host route is set for the routing of this address. In this method, routes for all hosts are individually set up in the routing table of the router. In the case of this Host Routing method, routing is possible whatever value is given to the Subnet ID. However, because as many host routes as the number of the hosts are required to be set up in the router, the number of entries of the routing table will be quite large, and a quite heavy load may be imposed on the router.

III. Our Proposed Method

A. System Configuration

In our proposed method, the network is concealed by having each node possess two addresses and use them properly according to the location of the corresponding node. When communicating with an external node, an at-randomly generated address is used and when communicating with an internal node, an address effective within the internal network is used. Fig. 3 shows the system configuration of our proposed system. It is assumed that IN1 and IN2 exist within the internal network, and that EN exists on the Internet. Two addresses, namely one for external communications and the other for internal communications, are assigned to the internal node IN1 and IN2. Concealed Address (CA) is a concealment address defined anew in our proposal and Unique Local IPv6 Unicast Address (ULA) is used for communication within the internal network. Concealed Address Management Server (CAMS) to be used for the management of addresses is set up just below Gateway. When IN1 communicates with EN, it starts communication using CA1 as the Source Address, and when

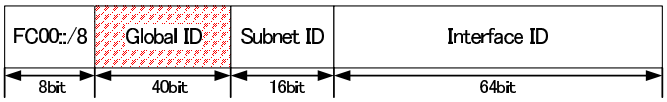


Fig. 4. Unique Local IPv6 Unicast Address

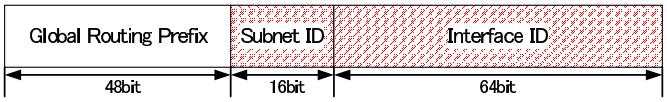


Fig. 5. Concealed Address

IN1 communicates with IN2, it starts communication using ULA.

B. Definitions of Addresses

When the corresponding node exists inside the network, ULA is used. Fig. 4 shows its address configuration. There was once a time when Site Local Address (SLA) was defined as the address effective in the internal network. However, it was abandoned due to the reason that the definition of its scope is unclear [7], and ULA was later defined in the place of SLA. ULA is an address in which 40 bit global identifiers are at-randomly generated. Because of that, there is little possibility that addresses duplication with each other occurs even if addresses are leaked. ULA was defined with a view to making communications within the same network, and its use on the Internet is not recommended.

For communications with an external node, our newly defined Concealed Address (CA) is used. The address configuration of CA is shown in Fig. 5. CA uses the value which generates lower order of 80 bit including Subnet ID on an at-random basis. With this configuration, we can avoid the situation where nodes or network topology are identified. Because Subnet ID is generated at-randomly, a tunnel is created between the CAMS and the internal node for the purpose of routing in the internal network, and ULA is use for the newly added IPv6 header. In general, duplicate addresses detection range is effective only in the same link. CA can avoid address duplication in the entire internal network by generating it by CAMS.

C. Communication Method

Fig. 6 shows the operation sequence when an internal node IN1 communicates with an external node EN. The network topology is the same as that shown in Fig. 3. First, the internal node IN1, after the start-up, generates ULA1 by way of stateless address automatic configuration. Thereafter, when a communication with EN is required, IN1 sends CA Request packet to CAMS in order to obtain CA. The source address of this packet is ULA1. Upon receipt of the packet, CAMS generates CA1 and verifies if there is no duplication with any other CAs. If there is no duplication, CAMS registers the relations between ULA1 and CA1, and sends CA Response of CA1 to IN1. Through the above procedure,

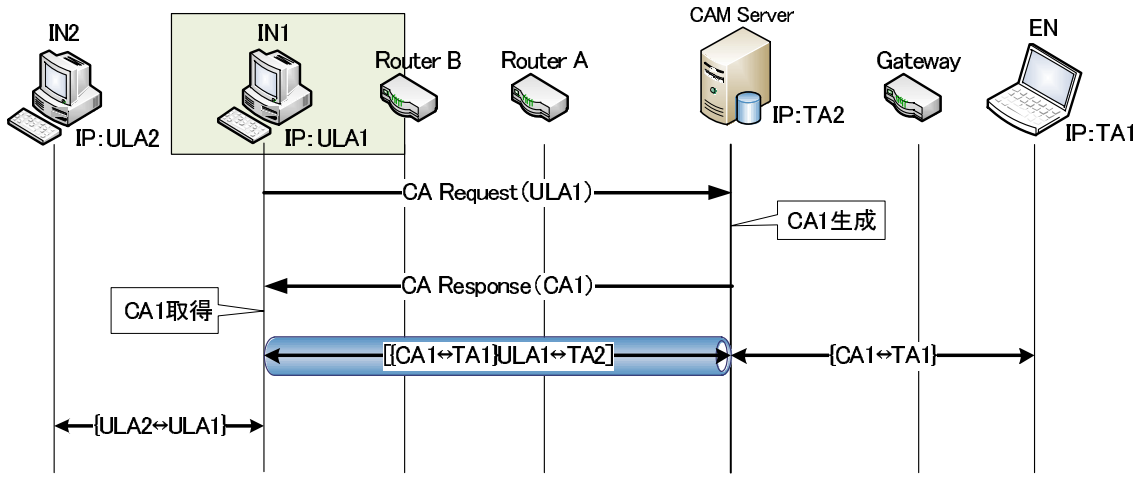


Fig. 6. Communication behavior with external node

```
prefix ::1/128 label 0
prefix ::/96 label 3
prefix ::ffff:0.0.0.0/96 label 4
prefix 2001::/32 label 6
prefix 2001:10::/28 label 7
prefix 2002::/16 label 2
prefix fc00::/7 label 5
prefix ::/0 label 1
```

Fig. 7. Policy Table

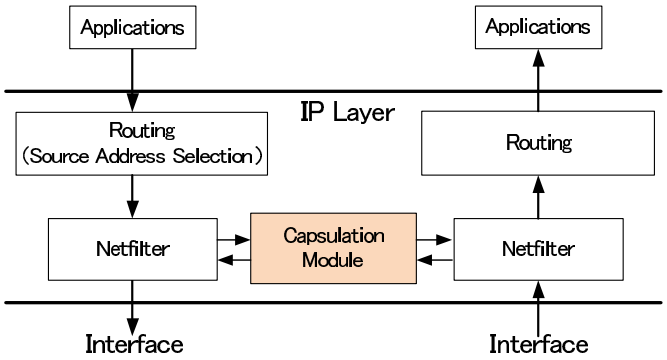


Fig. 8. Implementation to Linux

the communication between IN1 and EN becomes possible. At the time of initiating a communication with EN, IN1 determines CA1 as the source address, in the case that the corresponding node is found to be an external node. Then, in order to make the routing within the network possible, the packet is encapsulated. The source address for encapsulation header is designated as ULA1 and the destination address is designated as CAMS address TA2. Upon arrival of the packet, CAMS performs its decapsulation and takes out the packets of the source address CA1 and the destination address TA1, and sends them to EN. When a packet is sent from EN to IN1, the packet arrives at Gateway, and in the case that the destination address is CA, it is forwarded to CAMS. Because the relationship between CA1 and ULA1 is registered at CAMS, the packet is encapsulated by IP header of the source address TA2 and the destination address ULA1, and sent to IN1.

In the case that the corresponding node is IN2 within the network, the source address is set as ULA1, and communication is conducted directly without encapsulation.

Through the above-mentioned process, our proposed method using CA can successfully conceal network topology from the node on the Internet. It also realizes end-to-end communications and there is no restriction on the use of applications.

IV. Implementation

We have examined the case of implementing our proposed system to Linux. In our proposed method, two different addresses are used separately in accordance with the location of the corresponding node. In determining the source address (namely, which one of the addresses to use), a function called Source Address Selection [8] is used. In the case of IPv6, multiple addresses can be assigned. Therefore, it is necessary to choose one appropriate address according to the destination address [9], and various patterns need to be considered. A selection rule can be determined based on the policy table. Fig. 7 shows the default policy table of Linux. Various prefixes are registered and the source address of the prefix close to the destination address is selected. The prefix of ULA used for communications between internal nodes of our proposed method is already added to the policy table as `fc00::/7`. In the case of ULA being the destination, the address, whose value of the prefix is close, namely ULA itself, is chosen as the source address.

Fig. 8 shows a design of implementing our proposed method. When the source address is CA, encapsulation is required in order to make the routing in the internal network.

The encapsulation of the packet is realized by Capsulation Module in the kernel, and Netfilter is used to hook the packet in the processing. First, the packet received is forwarded from Application to IP layer for routing processing. At that time, the source address is determined by Source Address Selection function as mentioned above, and the source address corresponding to the destination address is established. Thereafter, the packet to be dispatched is hooked by Netfilter and forwarded to Capsulation Module to perform encapsulation processing. At Capsulation Module, the source address determined by the Source Address Selection is checked and when the source address is CA, the packet to be dispatched is returned to the normal routing processing after encapsulation. When the source address is not CA, the packet to be dispatched is returned to Netfilter as it is without encapsulation processing. In the case of the packet received, it is hooked at Netfilter and it is determined whether the packet has been encapsulated or not. If it is encapsulated, it is returned to Netfilter after decapsulation processing. In this way, source addresses are checked at Capsulation Module for each packet, and decapsulation processing is performed at the kernel.

V. Summary

In this paper, we described operational problems of various existing methods to conceal network topology when using IPv6. In the case of the method using Mobile IPv6, it has a problem of extra routing and also, the introduction cost of Mobile IPv6 seems to be fairly high. In the case of NPTv6, it is thought that we may not be able to satisfy the need of end-to-end communications, which is the fundamental function of the Internet. Thus, we proposed a new method using two addresses, where one address is "ULA" for internal communications and the other is concealment address "CA" for external communications, depending on the location of the corresponding node.

We intend to implement our proposed system to Linux and conduct verification of and evaluation of its operation.

References

[1] PCI Security Standards Council, LLC, "Pci security standards council." [Online]. Available: https://www.pcisecuritystandards.org/

[2] Task Force on IPv4 Address Exhustion, "Task force on ipv4 address exhustion." [Online]. Available: http://www.kokatsu.jp/blog/ipv4/

[3] M. Wasserman and F. Baker, "Ipv6-to-ipv6 network prefix translation," IETF, RFC 6296, Jun. 2011.

[4] G. V. de Velde, T. Hain, R. Droms, B. Carpenter, and E. Klein, "Local network protection for ipv6," IETF, RFC 4864, May 2007.

[5] T. Narten, R. Draves, and S. Krishnan, "Privacy extensions for stateless address autoconfiguration in ipv6," IETF, RFC 4941, Sep. 2007.

[6] R. Hinden and B. Haberman, "Unique local ipv6 unicast addresses," IETF, RFC 4913, Oct. 2005.

[7] C. Huitema and B. Carpenter, "Deprecating site local addresses," IETF, RFC 3879, Sep. 2004.

[8] R. Draves, "Default address selection for internet protocol version 6 (ipv6)," IETF, RFC 3484, 2003.

[9] A. Matsumoto, T. Fujisaki, R. Hiromi, and K. Kanayama, "Problem statement for default address selection in multi-prefix environments: Operational issues of rfc 3484 default rules," IETF, RFC 5220, Jul. 2008.

Proposal on the Concealment of the Network Topology in IPv6

Graduate School of Science and Technology
Meijo University
Toru Kuboshiki, Hidekazu Suzuki, Akira Watanabe

Watanabe Lab.

Background of the research

- Exhaustion of Global IPv4 Addresses
  - A short term solution
    - Definition of the private address
    - Introduction of NAT
  - A long term solution
    - Transition to IPv6 addresses

- Effects of NAT
  - NAT traversal problem
  - End-to-end communication is not possible
  - Network topology of an enterprise network is concealed

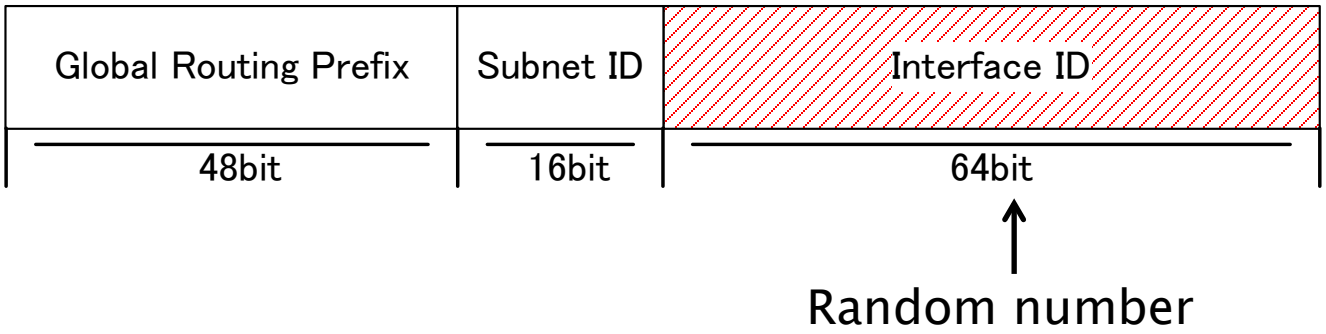
Purpose

- In an IPv6 environment
  - Global addresses are assigned to every terminals
  - There is no NAT traversal problem and end-to-end communication is possible
  - Node and network topology could be identified from the address
    - Network administrators do not want to disclose information as much as possible
    - This is an element of uncertainty for the transition to IPv6

Concealment of the network topologies in IPv6

Temporary Address

- Temporary Address (TA)
  - To protect the privacy of terminals
  - TA is defined in RFC 4941
  - Lower order 64 bit is generated as a random number



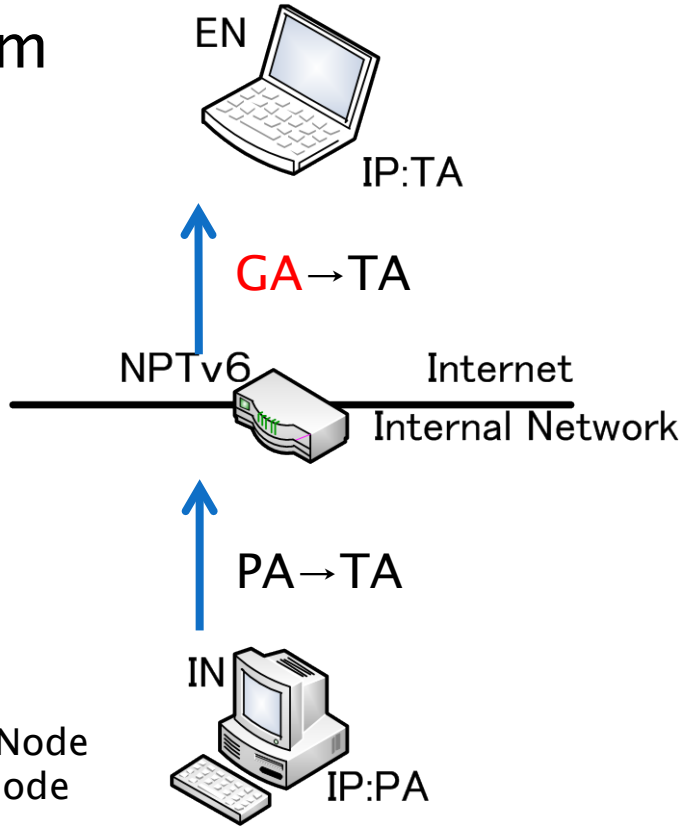
- A Network topology can not be concealed because Subnet ID is open to the public

Narten, T., Draves, R. and Krishnan, S.: Privacy Extensions for Stateless Address Autoconguration in IPv6, RFC 4941, IETF (2007).

NPTv6

- NPTv6(IPv6-to-IPv6 Network Prefix Translation)
  - NTPv6 device performs address translation
  - There is no NAT traversal problem

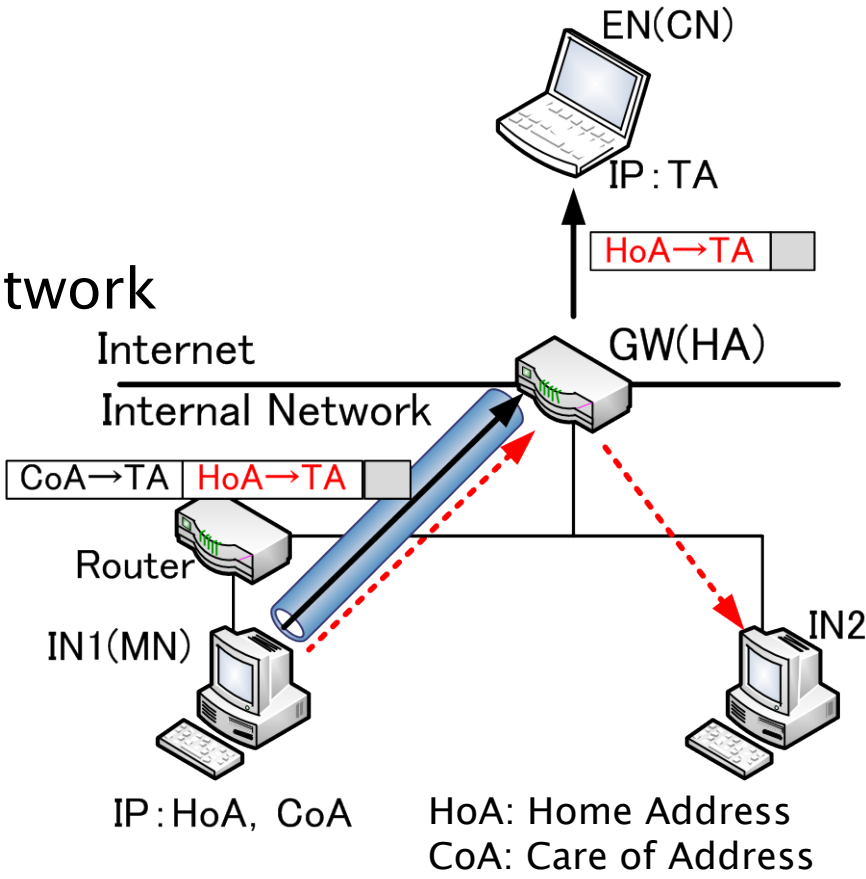
- Problem
  - End-to-end communication is not possible



M. Wasserman and F. Baker, "Ipv6-to-ipv6 network prefix translation," IETF, RFC 6296, Jun. 2011.

Method using Mobile IPv6

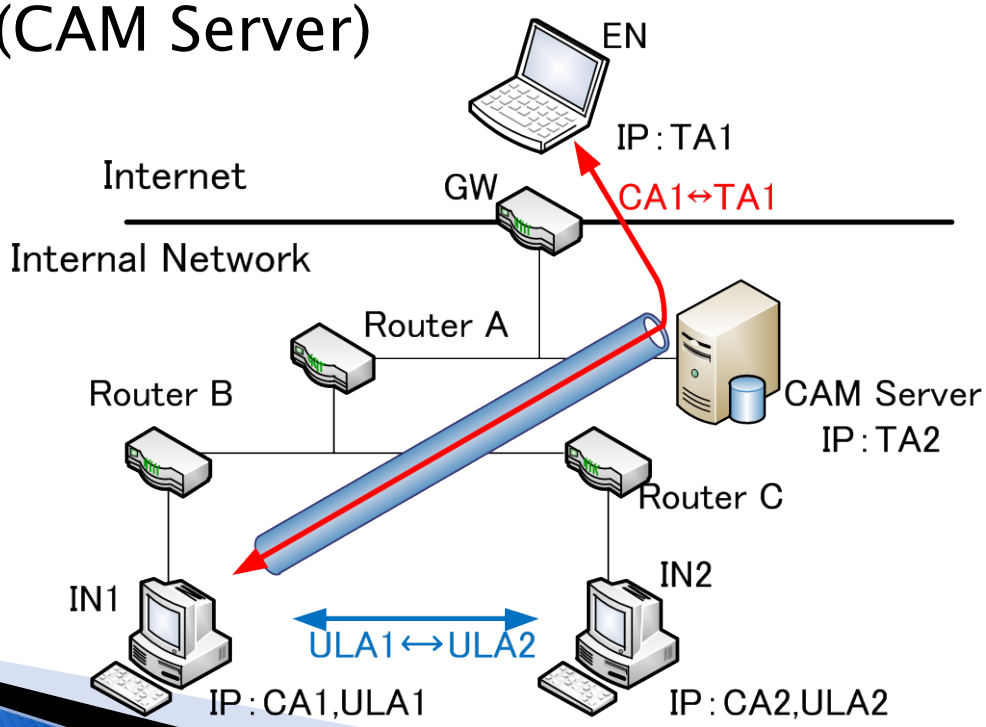
- Applying Mobile IPv6 (RFC4864)
  - Home Address (HoA)
    - Any value
  - Care of Address (CoA)
    - Routable address in actual network
- Problems
  - Redundant route at the start of communication
  - Unnecessary features and so many settings



de Velde, G.V., Hain, T., Droms, R., Carpenter, B. and Klein, E.: Local Network Protection for IPv6, RFC 4864, IETF (2007).

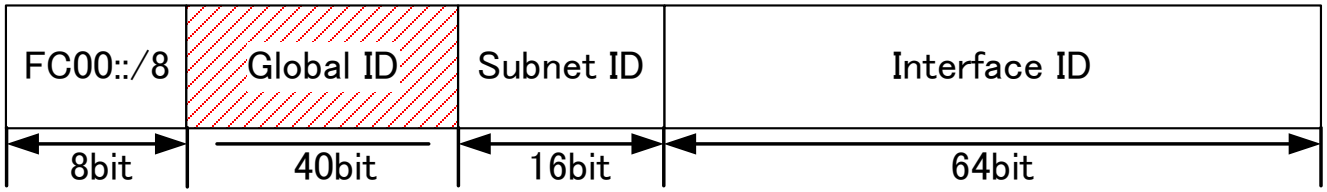
Proposed Method

- For the concealment of network topology
  - Two addresses assigned to terminals
  - Concealed Address (CA) is newly defined
  - Introduction of Concealed Address Management Server (CAM Server)

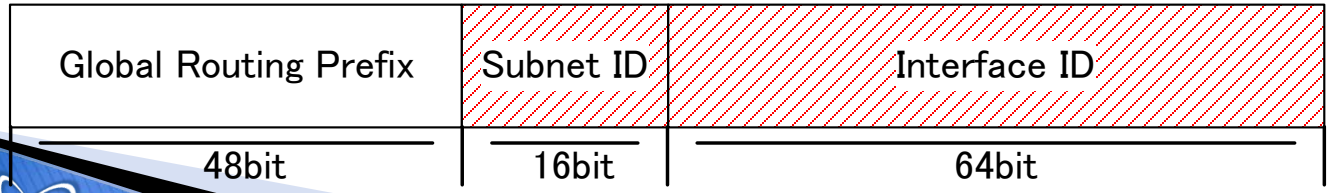


Address definition

- Unique Local Unicast IPv6 Address（RFC4913）
  - Used to communicate between the internal
  - ULA was defined for communications within the same network



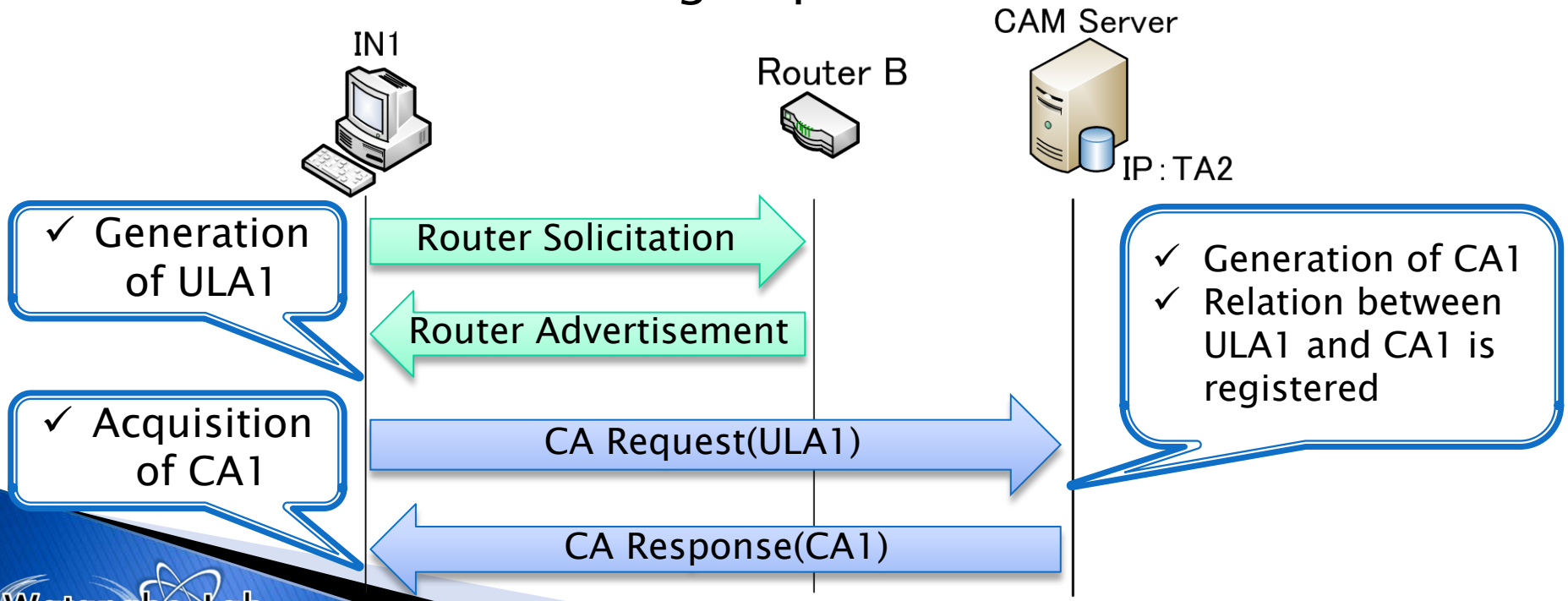
- Concealed Address (CA)
  - Used to communicate to external node
  - Lower order of 80 bit including Subnet ID are randomly generated



Hinden, R. and Haberman, B.: Unique Local IPv6 Unicast Addresses, RFC 4913, IETF (2005).

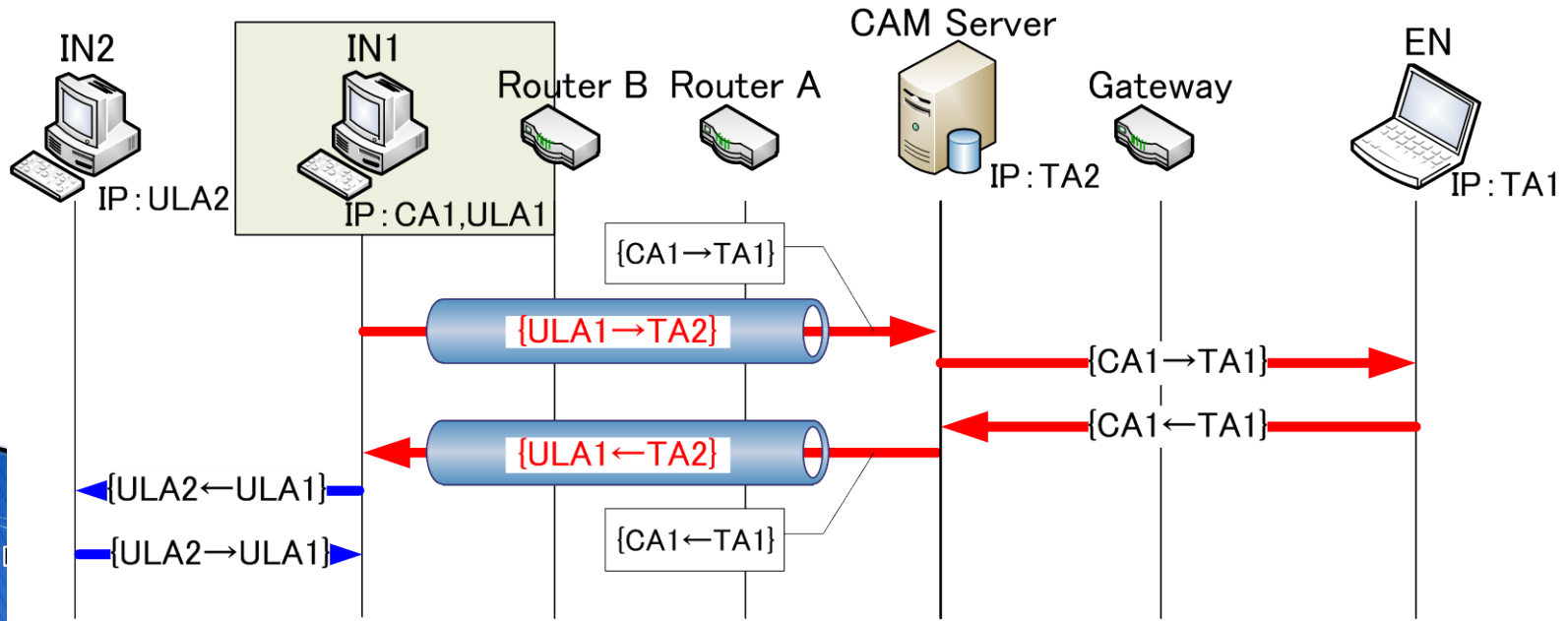
Concealed Address Management Server

- Management of CA
  - Generation and distribution of CA
- Creation of a tunnel table
  - To enable the routing of packet



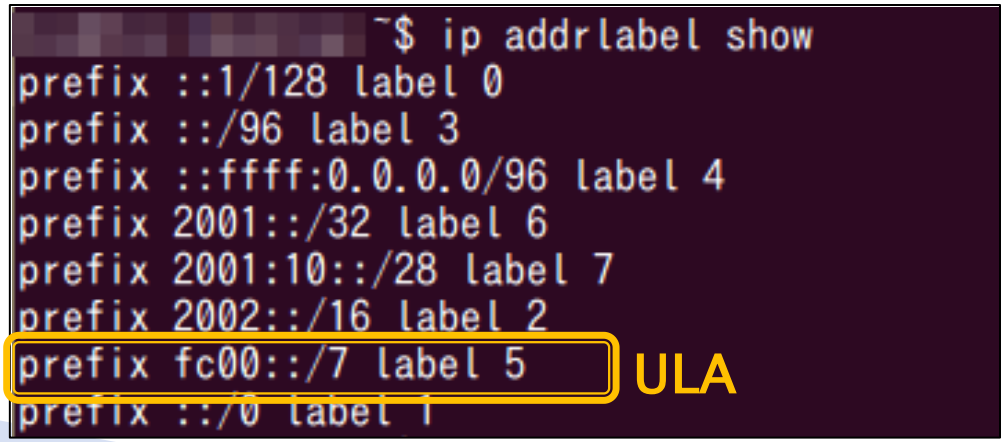
Communication Overview

- With an external node
  - A packet is encapsulated by ULA1 in order to route it in the network
- With an internal node
  - Normal communication is performed using ULA1 and ULA2



Idea of Implemention (1)

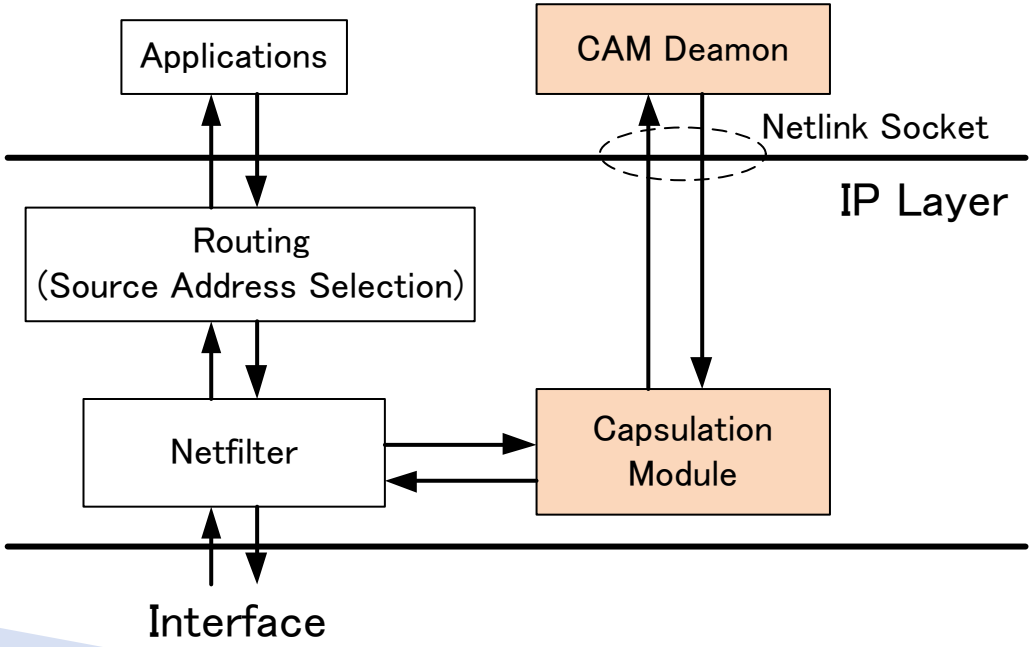
- Default Address Selection (RFC3484)
  - The source address can be selected according to the communication partner
  - Selection rules can be added in policy table
- “ip addrlabel show”
  - The policy table of ULA is previously set in Linux system



Draves, R.: Default Address Selection for Internet Protocol version 6 (IPv6), RFC3484, IETF (2003).

Idea of Implemention (2)

- Implementation in Linux
  - Encapsulation is realized by Capsulation Module in the kernel
  - Netfilter is used to hook packets



Summary

- Proposal on the Concealment of the Network Topology in IPv6
  - Concealed Address (CA) is newly defined
  - Introduction of Concealed Address Management Server (CAM Server)

- Future study
  - Implementation
  - Evaluation