Design of NAT Traversal for Mobile PPC Applying Hole Punching Technology

Hidekazu Suzuki* and Akira Watanabe†
Graduate School of Science and Technology, Meijo University
1-501 Shiogamaguchi, Tempaku-ku, Nagoya 468-8502 JAPAN
Telephone: +81-52-838-2406, Fax: +81-52-838-2406
Email: *h.suzuki@wata-lab.meijo-u.ac.jp, †wtnbakr@ccmfs.meijo-u.ac.jp

***Abstract*—Mobile Peer-to-Peer Communication (Mobile PPC) is a mobility protocol that enables mobility with only end nodes in an IPv4 network. It is assumed that a mobile node moves between a global network and a private network in the IPv4 network during communication. In the existing Mobile PPC, communication cannot be maintained when a mobile node moves if a Network Address Translator (NAT) exists on the communication path because the IP address of the packet is translated by the NAT. This paper presents a NAT traversal scheme to solve the above-mentioned problem by applying the principle of hole punching technology to Mobile PPC.**

I. Introduction

With the spread of portable devices and wireless networks, users can connect networks at anytime and from anywhere. Devices having a wireless LAN interface are rapidly increasing these days, and it is expected that the number of users who use public wireless LAN services will increase more and more in future. In IP networks, however, communication breaks when a node moves during communication because the IP address of the node changes according to its location. In order to solve this problem, various kinds of technologies, "called mobility technologies", have been studied [1].

Most mobility protocol technologies are based on IPv6 [2]–[4], but IPv6 networks are not yet widely used. It is thought that IPv4 networks will still play an important role in future. Therefore, the realization of mobility in IPv4 networks has great significance. In IPv4 networks, however, it is difficult to assign global IP addresses to all mobile nodes because of the address depletion problem. Thus, it is necessary to actively use private IP addresses. In such networks, a mobile node (MN) may move between a global network and a private network during communication, and a Network Address Translator (NAT) [5] needs to exist on the communication path either before the movement or after the movement. Consequently, the new IP address reported by the movement notification will not match with the IP address used in the actual communication. Therefore, the relation of IP address before the movement and that after the movement will not be correctly maintained. In order to solve this problem, several schemes have been studied for Mobile IP [6], such as an encapsulation of the movement notification with UDP, and addition of original functions in the NAT [7]–[9]. However, these schemes tend to degrade the data transmission efficiency due to the header overhead caused by the encapsulation, and have the problem that a special NAT is required.

We have proposed Mobile Peer-to-Peer Communication (Mobile PPC) [10], [11] that can realize mobility in IPv4 networks with only end nodes. In the Mobile PPC system, an MN starts communication with a correspondent node (CN) by using a dynamic DNS (DDNS) [12] to resolve the IP address. When an MN moves to another network during the communication with the CN and the MN's IP address is changed, the MN directly notifies the CN of the relationship between the IP addresses before and after the movement, and then both end nodes save it in their respective IP layers. After that, they translate the IP addresses of all communication packets in the IP layers, and thus, the change in the IP address is concealed in the upper layer software. The Mobile PPC can realize a high throughput communication because there is no redundant route and no encapsulation process is required. Consequently, this system is suitable for future ubiquitous networks. We have also proposed a NAT traversal scheme for Mobile PPC by modifying Mobile PPC and NAT functions [13]. This scheme realizes the mobility in the case where an MN moves between a global network and a private network during communication. The problem is, however, that an extended NAT is required.

In this paper, we propose a new NAT traversal scheme for Mobile PPC that can work with the existing NAT, whereby an MN can move freely between different address areas. Our proposed method uses the principle of hole punching technology [14], which is widely known as a NAT traversal technology. This paper assumes the case where a CN is located in a global network and that the MN moves between a global network and a private network. The MN executes a binding process equivalent to hole punching towards the CN, so that the NAT creates mapping information. Then, the MN obtains from the CN the IP address and the port number allocated to the exterior of the NAT, and sends a movement notification with the information to the CN. In this way, the CN can appropriately translate IP addresses and port numbers of communication packets by the Mobile PPC function without being affected by the address translation by the NAT. With our proposed method, Mobile PPC works well in normal networks constructed with existing NATs.

The rest of this paper is compiled in the following manner.

Section II describes the existing Mobile PPC and the principle of hole punching technology. Section III presents the scheme of our proposed method and gives detailed procedures about two mobility patterns. Then, Section IV describes some considerations about security etc, and finally Section V summarizes this paper.

II. Existing Technologies

A. Mobile PPC

Symbols described in this paper are defined as follows:

- Pi; Private IP address.
- Gi; Global IP address.
- $A : p$; IP address A and port number p.
- $S \rightarrow D$, $D \leftarrow S$; Communication from S to D.
- $S \leftrightarrow D$; Communication between S and D.
- $S \Leftrightarrow D$; Address translation from S to D, or from D to S.

Fig. 1 shows the procedure of Mobile PPC from the beginning of communication through the continuation process of communication when an MN moves to another network. At the beginning of the communication, the MN shares an authentication key with the CN by means of Diffie-Hellman (DH) key exchange [15] procedure. The authentication key is used for the movement notification process in the later phase. The MN creates a Connection Identification Table (CIT) related to the TCP/UDP packet that the MN is going to send, as shown in (1) [1], and then starts communication. The CN also creates the same CIT just like the MN when it received the first TCP/UDP packet.

$$G1 : s \leftrightarrow G2 : d \tag{1}$$

When an MN moves to another network during communication, it acquires a new IP address "$G3$" from a DHCP server at the visiting network. The MN then executes movement notification process with the CN. The MN generates a CIT Update (CU) Request message that contains the connection identification (CID) [2] before the movement and the new IP address after the movement, and signs the message with the authentication key and then sends it to the CN. After receiving the CU Request, the CN verifies the signature with the authentication key. If the authentication is successful, the CN updates its own CIT with the notified information as follows:

$$\{G1 : s \Leftrightarrow G3 : s\} \leftrightarrow G2 : d \tag{2}$$

Here, (2) means that the MN's IP address before the movement "$G1$", is translated to the IP address after the movement "$G3$". After that, the CN creates a CU Response message with its own signature and sends it to the MN. The MN also updates its own CIT with the same process when it receives the response message. In this way, the movement notification process is completed. Afterwards, IP addresses of all communication packets are translated in the IP layers of both end nodes according to the new CIT.

[1]CIT entry is created on each protocol (TCP or UDP), the description of the protocol is omitted in this paper.

[2]CID is information to identify a TCP connection or an UDP stream and is composed of five elements; namely, source and destination IP addresses/port numbers and protocol type.

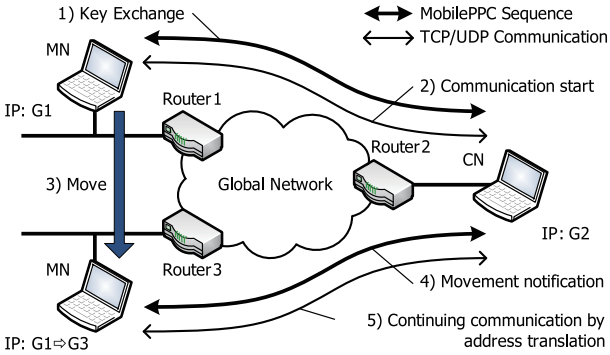


Fig. 1. Communication procedure of Mobile PPC

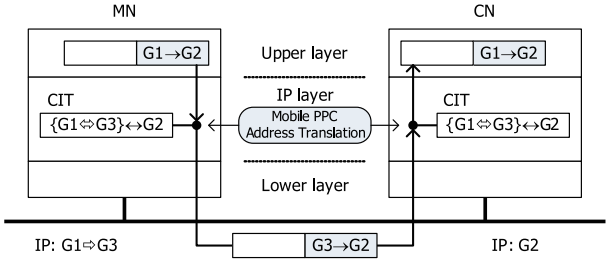


Fig. 2. Address translation based on CIT

Fig. 2 shows the procedure of the address translation based on the CIT after the movement. The MN translates the source IP address of a packet passed from the upper layer from "$G1$" to "$G3$", and sends it to its CN. The CN reversely translates the source IP address of the received packet from "$G3$" to "$G1$", and passes it to the upper layer software. Consequently, the change in the IP address is concealed in the upper layer and packets are correctly routed, and the communication is maintained.

Now, following problems arise when a NAT exists on the communication path between an MN and its CN as assumed in this paper.

1) In the case where an MN moves from a global network to a private network, the reported new IP address after movement from the MN to its CN is a private IP address, and thus, packets cannot be correctly routed on the global network.
2) If the CN can translate the IP address of the packet for the MN into the external IP address of the NAT, packets can be routed to the NAT. However, they never reach the MN because the NAT does not have mapping information.
3) In the case where the MN moves from a private network to a global network, the reported IP address before movement in the notification message is a private IP address. In this case, the CN cannot update its own CIT correctly because it recognizes the IP address before the movement of the MN as the external IP address of the

NAT.

B. Hole Punching

"Hole punching" is widely known as a NAT traversal technology and has been applied to some conventional technologies such as Simple Traversal of UDP Through NATs (STUN) [16] and Teredo [17]. A node behind a NAT establishes a session with a rendezvous server on the Internet in advance, and make the NAT create mapping information. A communication peer of the node acquires the external IP address and the port number allocated to the exterior of the NAT from the rendezvous server or the node, and initiates end-to-end communication.

The hole punching technology has the advantage of solving the NAT traversal problem without any modification to existing NATs. By applying the above technology to the Mobile PPC, an MN can notify its CN of the external IP address and the port number of the NAT, and a NAT mapping is created by the hole punching. Thus, this technology can solve the problems described in II-A.

However, the hole punching technology has disadvantages of not working with Symmetric NAT [3] and not supporting TCP-based communication. Also, it needs a rendezvous server on the Internet and special applications of the function at both end nodes. These disadvantages may degrade the advantages of Mobile PPC, namely, such advantages that it does not depend on any upper layer protocol, and that it requires no special servers. Therefore, a new NAT traversal scheme cannot use the conventional hole punching technology as it is. Some new ideas must be considered to keep the advantages of Mobile PPC.

III. Proposed Method

In consideration of the above-mentioned problems, a new NAT Traversal scheme for Mobile PPC needs to consider the following points.

1) An MN can traverse NAT without any extra server on the Internet.
2) End nodes can execute both TCP and UDP communication.
3) All types of NATs including the Symmetric NAT are usable.
4) Special applications are not needed in end nodes.

To satisfy the above requirements, a binding process tantamount to hole punching is to be executed directly between the MN and the CN in the Mobile PPC negotiation when CN acknowledges the presence of a NAT on the communication path with the MN. In order to execute the process, a Binding Request and a Binding Response are defined as new messages in Mobile PPC.

Hereinafter, we give a detailed description of the procedures in the case where an MN moves from a global network to a private network, and in the case of the reverse movement.

[3]A kind of NAT that creates different mapping information when the destination is different.

A. Definitions of Address-Related Terms

Addresses-related terms in the proposed method are defined as follows:

- **PREV-ADDRESS**
  A set of an MN's IP address and a port number before the movement, viewed from the CN.
- **MOVED-ADDRESS**
  A set of an MN's IP address and a port number after the movement, viewed from the CN.
- **MAPPED-ADDRESS**
  A set of an external IP address and a port number of the NAT, allocated by the binding process.
- **REAL-PREV-ADDRESS**
  A real MN's IP address before the movement.
- **REAL-MOVED-ADDRESS**
  A real MN's IP address after the movement.

B. Movement from a Global Network to a Private Network

Fig. 3 shows the sequence in the case where an MN (IP address "$G1$") moves from a global network to a private network during communication with its CN (IP address "$G2$"). Before the communication, the MN and the CN mutually share an authentication key with the same procedure as that for normal Mobile PPC. After the key sharing procedure, they create CITs as shown in (3) and start communication.

$$G1 : s \leftrightarrow G2 : d \tag{3}$$

When an MN moves to a private network during communication, it obtains a new private IP address "$P1$" from the DHCP server embedded in the NAT, which has a global IP address "$G3$". The MN immediately executes movement notification process with the CN. A CU Request for the CN contains the new IP address "$P1$" as the MOVED-ADDRESS and signs the message with the authentication key. The CN receives the above CU Request and performs authentication. After successful authentication, the CN compares the MOVED-ADDRESS in the message and the source IP address in the IP header. The CN acknowledges the presence of a NAT because they are different, and obtains the global IP address of the NAT, "$G3$" from the source IP address of the CU Request. In this case, the CN does not update the CIT and returns a CU Response to the MN with a newly defined flag "NAT-ON-PATH". Additionally, CN starts the monitoring of the destination port number "d" notified by the CU Request for a given length of time, expecting a Binding Request message to come from the MN. When the MN receives the CU Response with a "NAT-ON-PATH" flag, it sends a Binding Request message to the CN. Fig. 4 shows the packet format of the Binding Request/Response messages. In general, the destination port number in the message of the hole punching system is fixed with a specific value, but in our proposed method, its value is chosen as follows — The IP header and the transport protocol header of the Binding Request/Response messages are the same as the communication packet before the

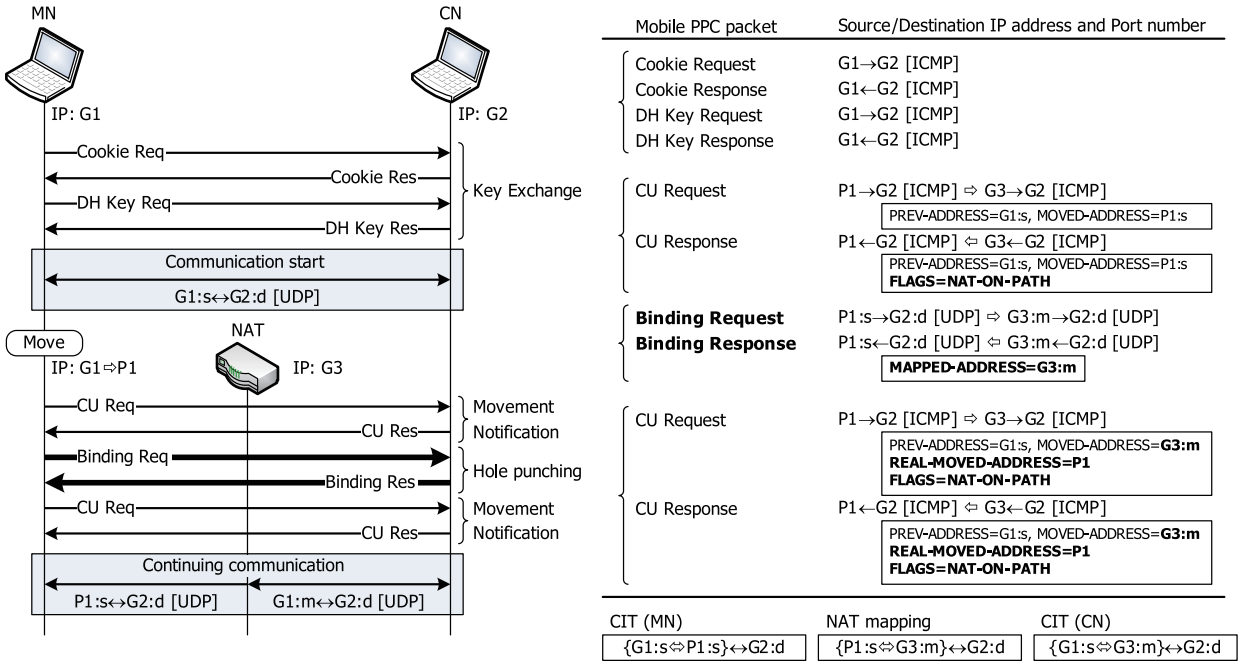


Fig. 3. Sequence in the case MN moves from a global network to a private network

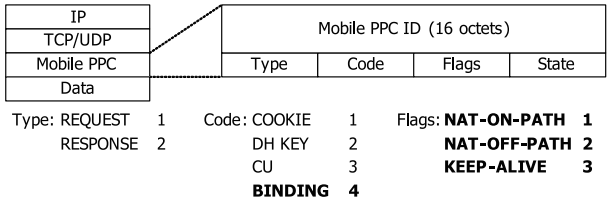


Fig. 4. Packet format of Binding Request/Response

movement of the MN, as shown in (4). — in order to manage the Symmetric NAT.

$$P1 : s \rightarrow G2 : d \quad [protocol] \tag{4}$$

NAT receives a Binding Request from an MN and then creates the following mapping information based on the principle of the NAT, and forwards it to the CN:

$$NAT: \quad \{P1 : s \Leftrightarrow G3 : m\} \leftrightarrow G2 : d \quad [protocol] \tag{5}$$

Since the CN receives a packet with the monitoring port number "d", the CN distinguishes whether it is a Binding Request message or not by checking the Mobile PPC header defined in the TCP/UDP payload and further checking the newly defined values of *Code* and *Flags* fields (see the parts indicated by boldface in Fig. 4). If it is a Binding Request message, the CN sends back to the MN a Binding Response message that contains the source IP address and the port number of the received packet (i.e., "$G3 : m$") as a MAPPED-ADDRESS.

The MN, upon receiving the above Binding Response, takes out the MAPPED-ADDRESS from the message, changes it to the MOVED-ADDRESS, and adds the MN's private IP address "$P1$" as the REAL-MOVED-ADDRESS to the CU Request message. The MN also establishes a "NAT-ON-PATH" flag and send another CU Request with this flag to the CN. The CN receives the above CU Request and updates its own CIT with the same procedure as that for existing Mobile PPC as shown in (6) after successful authentication process.

$$CN: \quad \{G1 : s \Leftrightarrow G3 : m\} \leftrightarrow G2 : d \tag{6}$$

After that, CN makes a CU Response message with the same information in the CU Request (i.e., PREV-ADDRESS, MOVED-ADDRESS, REAL-MOVED-ADDRESS, and the flag "NAT-ON-PATH") and replies it to the MN.

When the MN receives the above message, it updates its own CIT with the REAL-MOVED-ADDRESS "$P1$" as shown in (7), whereby the MOVED-ADDRESS "$G3 : m$" is ignored.

$$MN: \quad \{G1 : s \Leftrightarrow P1 : s\} \leftrightarrow G2 : d \tag{7}$$

Thereafter, address translation of every communication packet is executed according to the new CIT in the IP layer. The MN translates the source IP address of the packet passed from the upper layer from "$G1$" (address before the movement) to "$P1$" (address after the movement), and sends it to the CN. When the NAT receives the packet from the MN, it translates the source IP address and the port number from "$P1 : s$" to "$G3 : m$", according to the mapping information created by the binding process and forwards it to the CN. The CN reversely translates the IP address and the port number in the received packet from "$G3 : m$" (mapped address) to "$G1 : s$" (address before the movement), and passes it to the upper layer software. In this way, communication between an MN and a CN is maintained even if the MN moves from a global network to a private network.

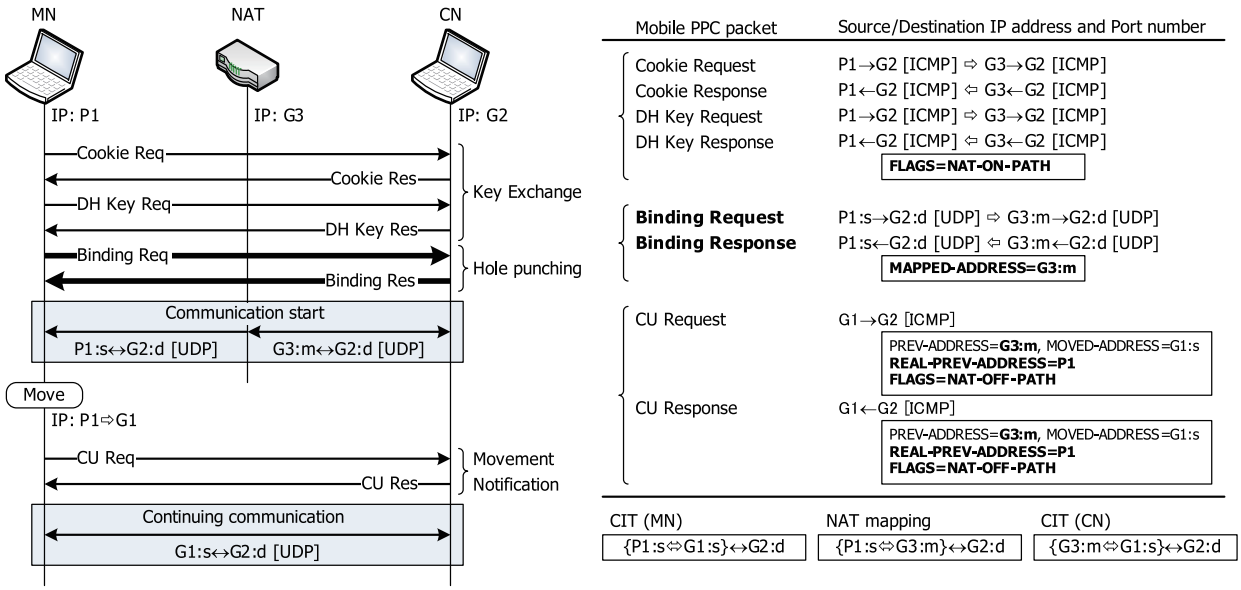


Fig. 5. Sequence in the case MN moves from a private network to a global network

C. Movement from a Private Network to a Global Network

Next, Fig. 5 shows the sequence in the case where an MN (IP address "$P1$") moves from a private network to a global network. A procedure in this case is the same as that described in III-B. The MN shares an authentication key with the CN through the DH key exchange procedure at the start of communication. Although this procedure succeeds without fail, the CN recognizes the presence of a NAT by comparing the reported IP address of the MN (i.e., the private IP address) with the source IP address of the message (i.e., the global IP address). The CN then establishes a "NAT-ON-PATH" flag in the last message of the key exchange sequence. After the MN created an authentication key, it executes the binding process with the CN and obtains the MAPPED-ADDRESS "$G3 : m$".

When an MN moves to a global network during communication with its CN and is assigned a new global IP address "$G1$", it executes movement notification process with the CN. Since the MN knows the presence of a NAT on the previous communication path from the notified "NAT-ON-PATH" flag sent by the CN, it describes in the CU Request message the MAPPED-ADDRESS "$G3 : m$" as the PREV-ADDRESS and the private IP address of the MN before the movement "$P1$" as the REAL-PREV-ADDRESS. The MN further establishes a "NAT-OFF-PATH" flag in the message and sends it to the CN which, upon receipt of the above CU Request, updates its own CIT with the same procedure as that for the existing Mobile PPC as shown in (8).

$$CN: \quad \{G3 : m \Leftrightarrow G1 : s\} \leftrightarrow G2 : d \tag{8}$$

And then, the CN sends a CU Response with a "NAT-OFF-PATH" flag to the MN. Upon receiving the above message, the MN updates its own CIT entry so that the source IP address is equal to the REAL-PREV-ADDRESS "$P1$" to correspond to the MOVED-ADDRESS "$G1$" as follows:

$$MN: \quad \{P1 : s \Leftrightarrow G1 : s\} \leftrightarrow G2 : d \tag{9}$$

Finally, the MN translates the source IP address of a packet passed from the upper layer software from "$P1$" to "$G1$" and sends it to the CN. The CN reversely translates the source IP address and the port number on the received packet from "$G1 : s$" to "$G3 : m$" and passes it to the upper layer software. In this way, the communication between an MN and a CN is maintained even if the MN moves from a private network to a global network.

IV. Considerations

As described above, the proposed method can realize mobility even if the MN moves between a global network and a private network even in the case where the CN is located in a global network. In addition to this, there is a case where an MN moves between different private networks, that is to say, from one private network to another private network. For this case, it is possible to combine the procedure at the beginning of communication described in III-B with the procedure after the movement described in III-C. Furthermore, the proposed method is operable in hierarchically-organized private networks by the use of the hole punching technology.

A. Keep-alive

In NAT traversal systems using the existing NAT, we have to consider a keep-alive signal to maintain mapping information in the NAT. In UDP communication in particular, the continuation of communication easily fails because NAT mapping information is deleted if both end nodes of the NAT are out of communication for a period of time after the information is created by a binding process. The MN needs to periodically send keep sending a keep-alive packet to the CN. In general,

it is necessary to send it at shorter intervals than the effective duration of the NAT mapping. However, CN's workload might increase because the MN has to send a keep-alive packet in each established session. Besides, the effective duration of NAT mapping depends on the type of its implementation as well as its configuration, and thus, we need to consider the optimum value. Meanwhile, the keep-alive interval for Mobile IP system is set at 110 seconds as the default value in [7].

B. Security

In this subsection, we describe some security considerations about the binding process adopted in the proposed method. An attacker might attempt to hijack a session by altering the MAPPED-ADDRESS included in a Binding Response. In Mobile PPC, the message integrity of the Binding Request/Response is secured through addition of a signature of the MN or the CN because they share an authentication key at the beginning of communication. Therefore, an alteration attack for the binding process can be detected.

An attacker might attempt to disrupt a session by sending a false binding message. The attacker sends a false Binding Response to an MN immediately after the MN sends a Binding Request to its CN. Just like the above-said alteration attack, this attack can also be prevented completely through the Binding message integrity mechanism.

For the address translation by a NAT, the range of the integrity is limited below the TCP/UDP payload. Therefore, the attacker can eavesdrop on a legitimate Binding Request and might attempt to send a Binding Request with a spoofed source IP address to a CN. In this case, the CN authenticates the Binding Request as a legitimate message, and creates a Binding Response, considering the spoofed IP address as a MAPPED-ADDRESS and sends it to spoofed IP address (usually the attacker's IP address). When the attacker receives the Binding Response, it spoofs the source IP address of the message as the CN and sends it to the MN via a NAT. Since the MN also authenticates the Binding Response, the session will be hijacked by the attacker after the movement notification process is completed. It is possible to prevent this kind of attack from occurring, by assigning sequence numbers to the message portion of the Binding Request so that retransmission of the Binding messages is avoided, or by establishing Ingress Filtering [18].

V. Conclusion

In this paper, we have proposed a new NAT traversal scheme for the Mobile PPC which enables an MN to move between a global network and a private network when the CN is located in a global network. The proposed method works with any kind of existing NATs through the application of the principle of hole punching technology for Mobile PPC.

In the future, we will implement our proposed method and confirm its effectiveness by conducting a performance evaluation. Furthermore, we will combine the proposed method with another NAT traversal technology, namely NAT-free protocol (NAT-f) that we have separately proposed in [19], [20], and also study the mechanism which enables the mobility even when the CN is located in a private network.

Acknowledgment

This research was partially supported by Japan Society for the Promotion of Science (JSPS), Grant-in-Aid for JSPS Fellows, 20-1069, 2008.

References

[1] F. Teraoka, "Node mobility protocols in the internet," *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, vol. 88, no. 6, pp. 39–59, Feb. 2005.

[2] D. Johnson, C. Perkins, and J. Arkko, "Mobility support in ipv6," RFC 3775, June 2004.

[3] M. Ishiyama, M. Kunishi, K. Uehara, H. Esaki, and F. Teraoka, "Lina: A new approach to mobility support in wide area networks," *IEICE transactions on communications*, vol. E84-B, no. 8, pp. 2076–2086, Aug. 2001.

[4] R. Inayat, R. Aibara, K. Nishimura, T. Fujita, and K. Maeda, "An end-to-end network architecture for supporting mobility in wide area wireless networks," *IEICE transactions on communications*, vol. E87-B, no. 6, pp. 1584–1593, June 2004.

[5] P. Srisuresh and M. Holdrege, "Ip network address translator (nat) terminology and considerations," RFC 2663, Aug. 1999.

[6] C. Perkins, "Ip mobility support for ipv4," RFC 3220, Jan. 2002.

[7] H. Levkowetz and S. Vaarala, "Mobile ip traversal of network address translation (nat) devices," RFC 3519, Apr. 2003.

[8] G. Montenegro, "Reverse tunneling for mobile ip, revised," RFC 3024, Jan. 2001.

[9] A. Idoue, H. Yokota, and T. Kato, "Proposal of hierarchical mobile ip supporting private addresses utilizing nat function and its implementation on unix operating system," *IEICE transactions on communications*, vol. E84-B, no. 12, pp. 3155–3165, Dec. 2001.

[10] M. Takeuchi, H. Suzuki, and A. Watanabe, "A proposal of mobile ppc that realizes end-to-end mobility and its implementations," *Transactions of Information Processing Society of Japan*, vol. 47, no. Dec., pp. 3244–3257, 2006, (in Japanese).

[11] M. Sejimo and A. Watanabe, "Implementation of mobile ppc realizing mobility of mobile nodes," in *Proc. The International Symposium on Information Theory and its Applications (ISITA2006)*, Seoul, Korea, Oct. 2006.

[12] P. Vixie, S. Thomson, Y. Rekhter, and J. Bound, "Dynamic updates in the domain name system (dns update)," RFC 2136, Apr. 1997.

[13] K. Enomoto, H. Suzuki, J. Sakamoto, and A. Watanabe, "Researches on mobile communications over a private address area and a global address area," in *Proc. The International Symposium on Information Theory and its Applications (ISITA2006)*, Seoul, Korea, Oct. 2006.

[14] B. Ford, P. Srisuresh, and D. Kegel, "Peer-to-peer communication across network address translators," in *Proc. USENIX Annual Technical Conference*, Anaheim, CA, Apr. 2005, pp. 179–192.

[15] M. Sejimo and A. Watanabe, "Implementation of authentication mechanisms in mobile ppc," in *Proc. Multimedia, Distributed, Cooperative, and Mobile Symposium (DICOMO2006)*, vol. 2006, no. 6, Kagawa, Japan, July 2006, pp. 809–812, (in Japanese).

[16] J. Rosenberg, J. Weinberger, C. Huitema, and R. Mahy, "Stun - simple traversal of user datagram protocol (udp) through network address translators (nats)," RFC 3489, Mar. 2003.

[17] C. Huitema, "Teredo: Tunneling ipv6 over udp through network address translations (nats)," RFC 4380, Feb. 2006.

[18] P. Ferguson and D. Senie, "Network ingress filtering: Defeating denial of service attacks which employ ip source address spoofing," RFC 2827, May 2000.

[19] H. Suzuki, S. Usami, and A. Watanabe, "Proposal and implementation of nat-f for realizing nat traversal communication with external dynamic mapping method," *Transactions of Information Processing Society of Japan*, vol. 48, no. Dec., pp. 3949–3961, 2007, (in Japanese).

[20] H. Suzuki, Y. Goto, and A. Watanabe, "External dynamic mapping method for nat traversal," in *Proc. IEEE 7th International Symposium on Communications and Information Technologies (ISCIT2007)*, Sydney, Austraria, Oct. 2007, pp. 723–728.

IEEE Region 10 Conference (TENCON2008)
Nov. 18th – 21th, 2008
University of Hyderabad, Hyderabad, India

Session: O28-2 Networks

Design of NAT Traversal for Mobile PPC Applying Hole Punching Technology

Hidekazu Suzuki **Akira Watanabe**

Meijo University, JAPAN

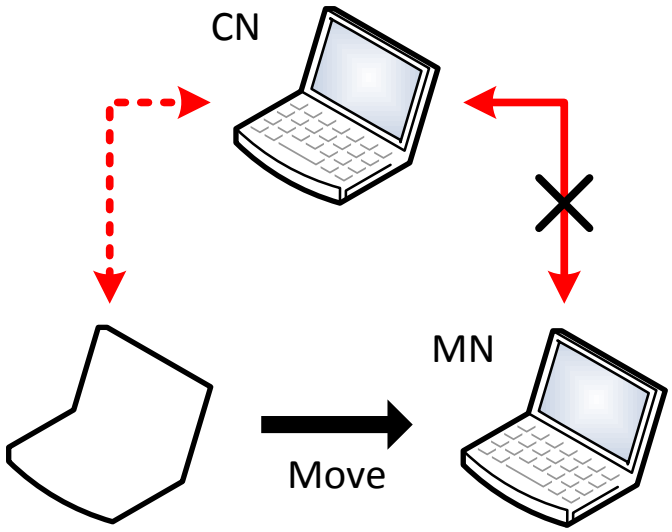
Background

- Communication breaks when an MN moves to another network during communication with a CN

MN: Mobile Node
CN: Correspondent Node

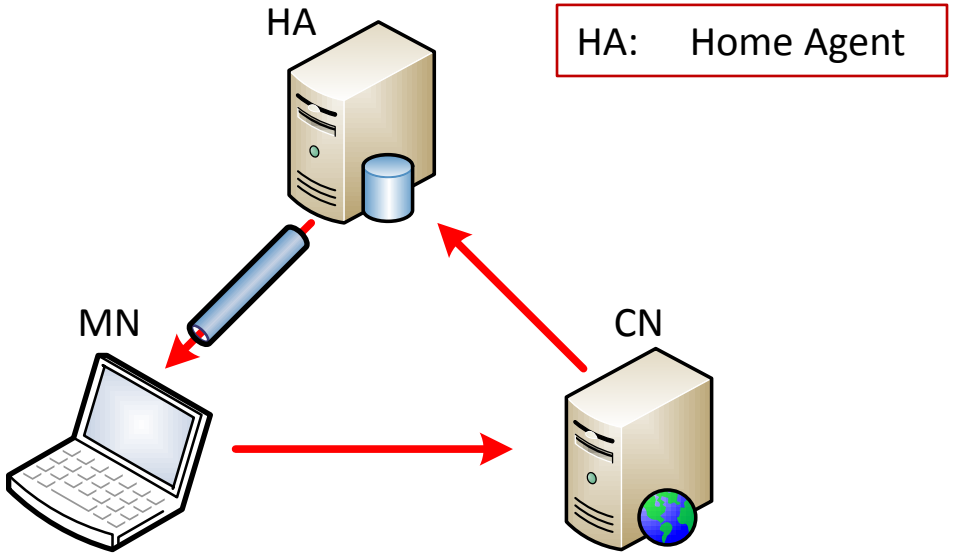
➔Reason:

- IP address is changed due to movements
  - Transport sessions are broken
  - CN cannot identify the location of MN

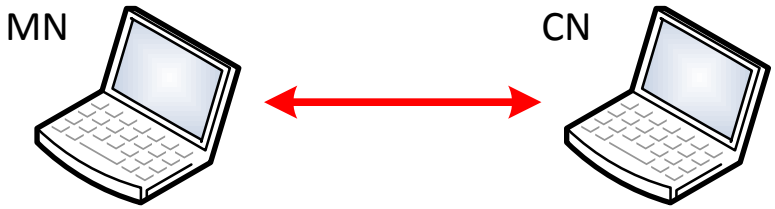


IP Mobility Technologies

- Mobile IPv4 (RFC3344)
  - Proxy approach
  - Encapsulation



- Mobile PPC ← Our original technology
  - End-to-End approach
  - Address translation

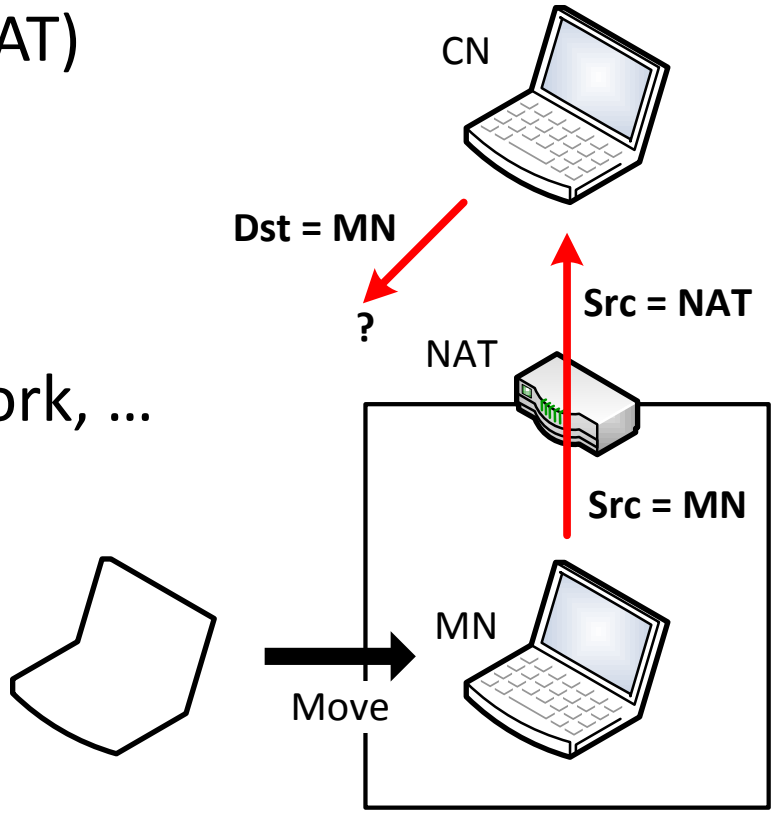


IP Mobility Issues in IPv4

- Network Address Translator (NAT)
  - Global network
  - Private network
- If MN moves to a private network, …
  - Communication is broken

➔Reasons:

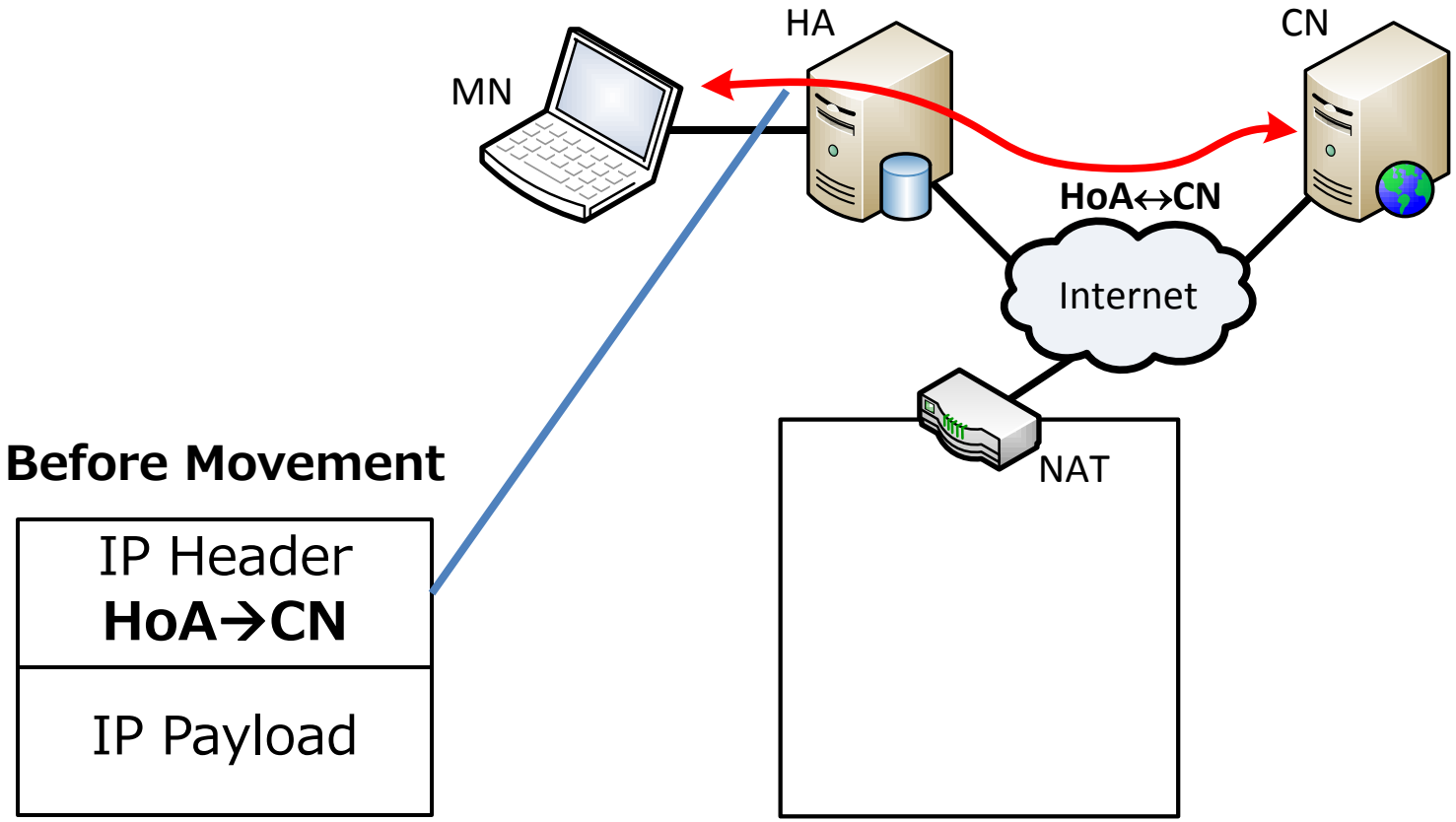
- Translation of IP address by NAT
  - Transport session identifier is changed
- Private IP address (Non-reachable)



Existing Method (By Mobile IPv4)

- Mobile IP Traversal of NAT Devices (RFC3519)
  - UDP Tunneling

HA: Home Agent
HoA: Home Address

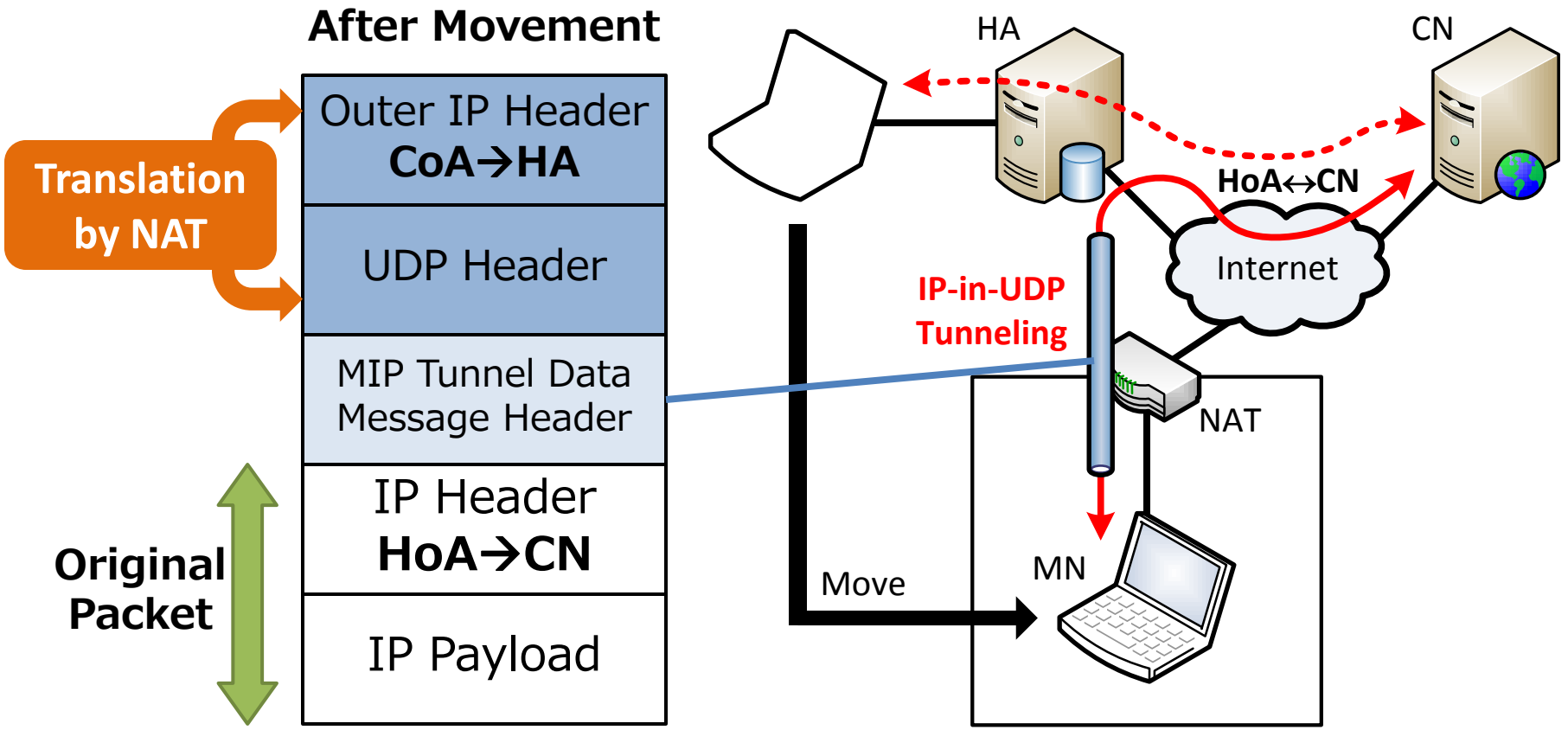


Existing Method (By Mobile IPv4)

Watanabe Lab.
Department of Information Engineering, Meijo University
Information Networks Laboratory

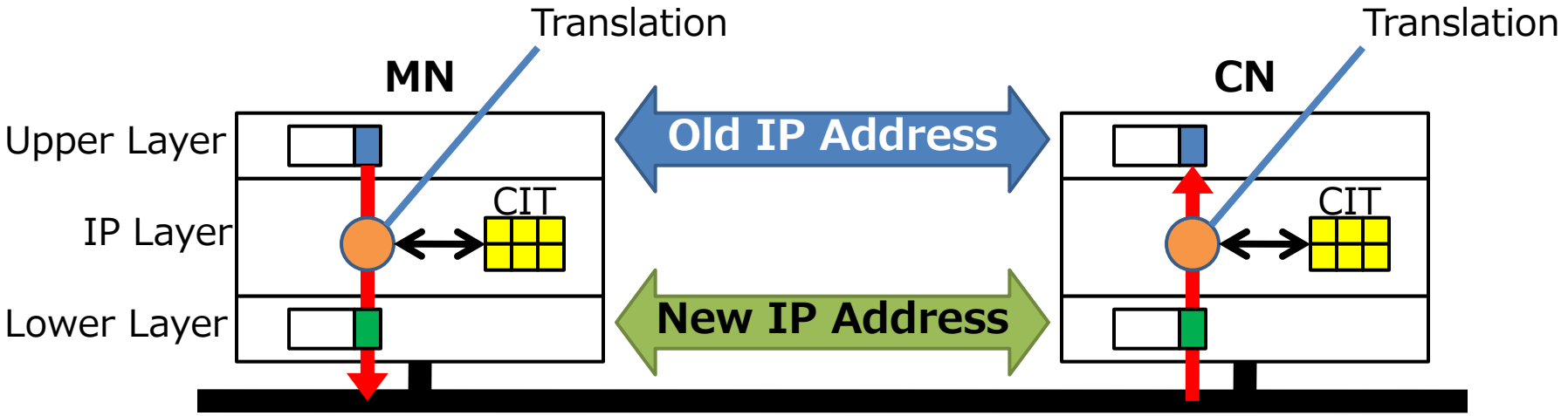
- Mobile IP Traversal of NAT Devices (RFC3519)
  - UDP Tunneling

HA: Home Agent
HoA: Home Address
CoA: Care-of Address



Outline of Mobile PPC

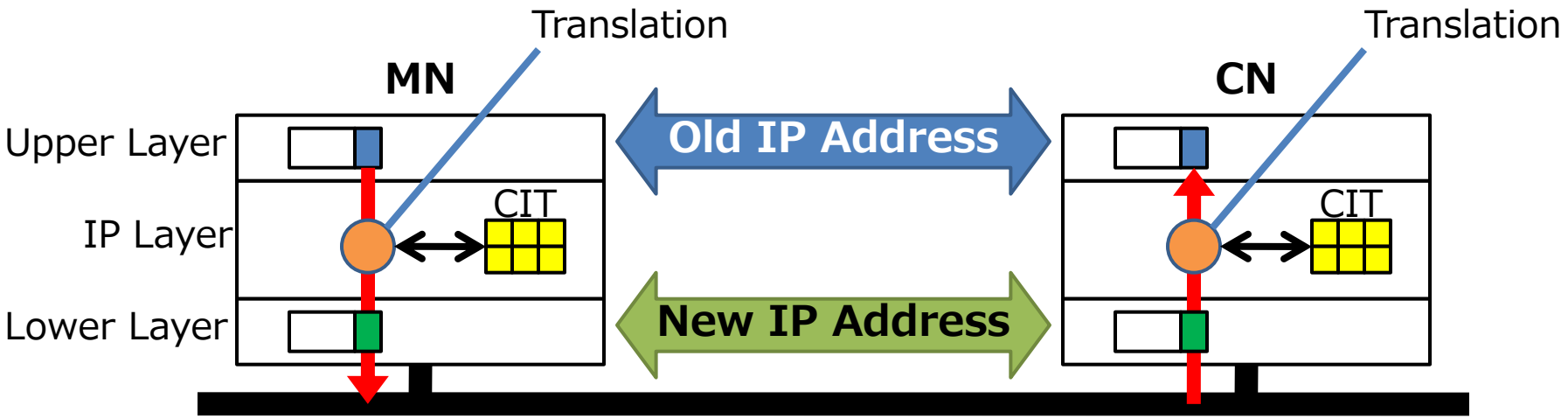
- MN notifies CN of its migration directly
- Creating "**Connection ID Table**" (**CIT**)
- Translation in IP layers
  - When sending: Old address → New address
  - When receiving: New address → Old address



Outline of Mobile PPC

- MN notifies CN of its migration directly
- Creating "**Connection ID Table**" (**CIT**)
- Translation in IP layers

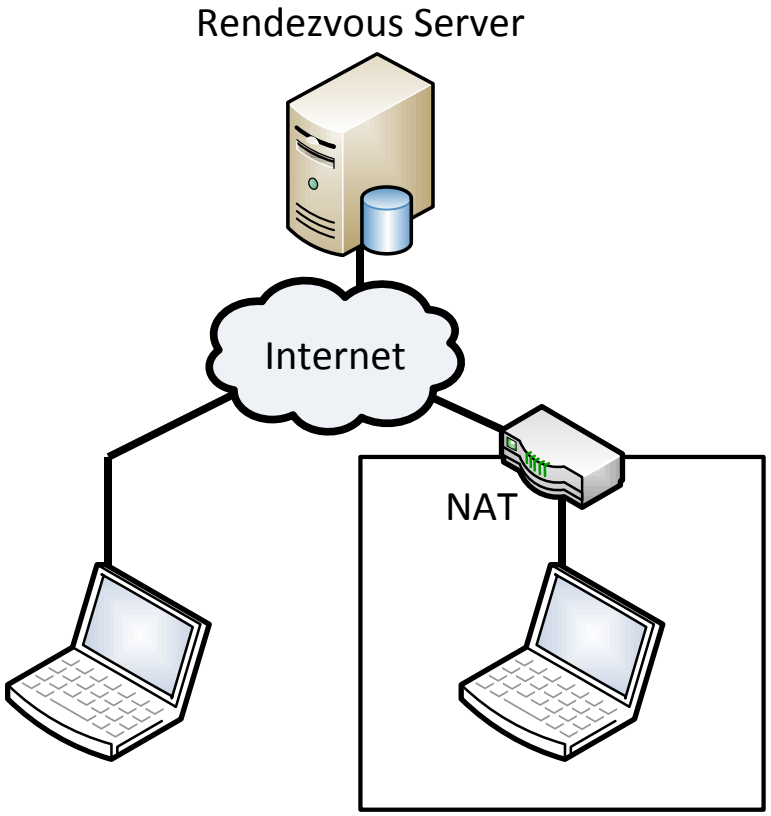
The change of the IP address is concealed to the upper layer and the transport session is maintained.



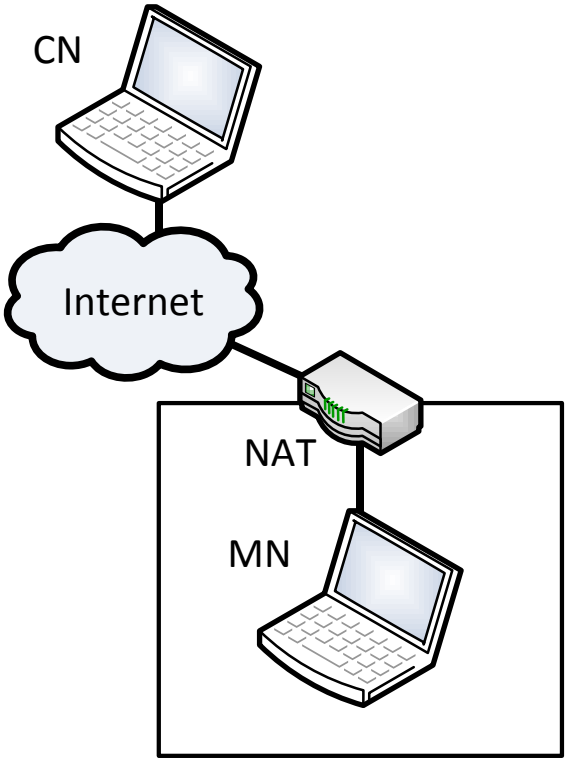
Proposed Method (Key Idea)

- Applying the principle of "**Hole Punching**" technology

Hole Punching



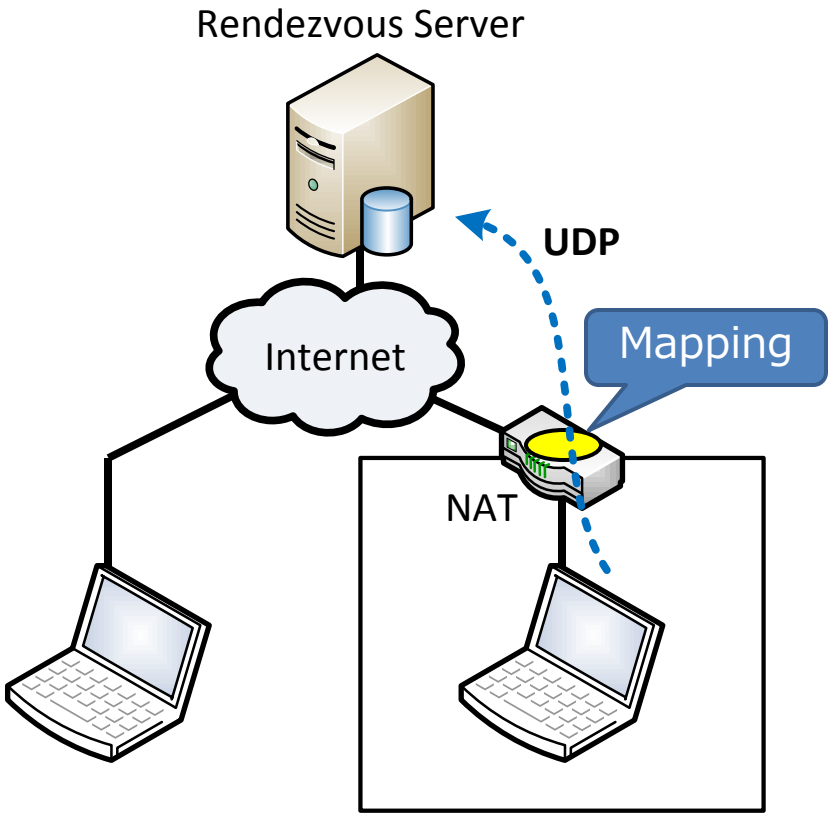
Proposed Method



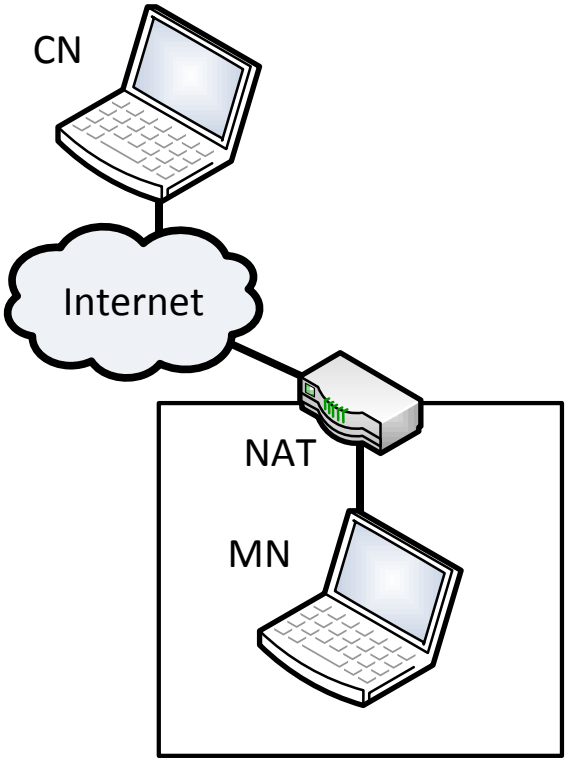
Proposed Method (Key Idea)

- Applying the principle of "**Hole Punching**" technology

Hole Punching



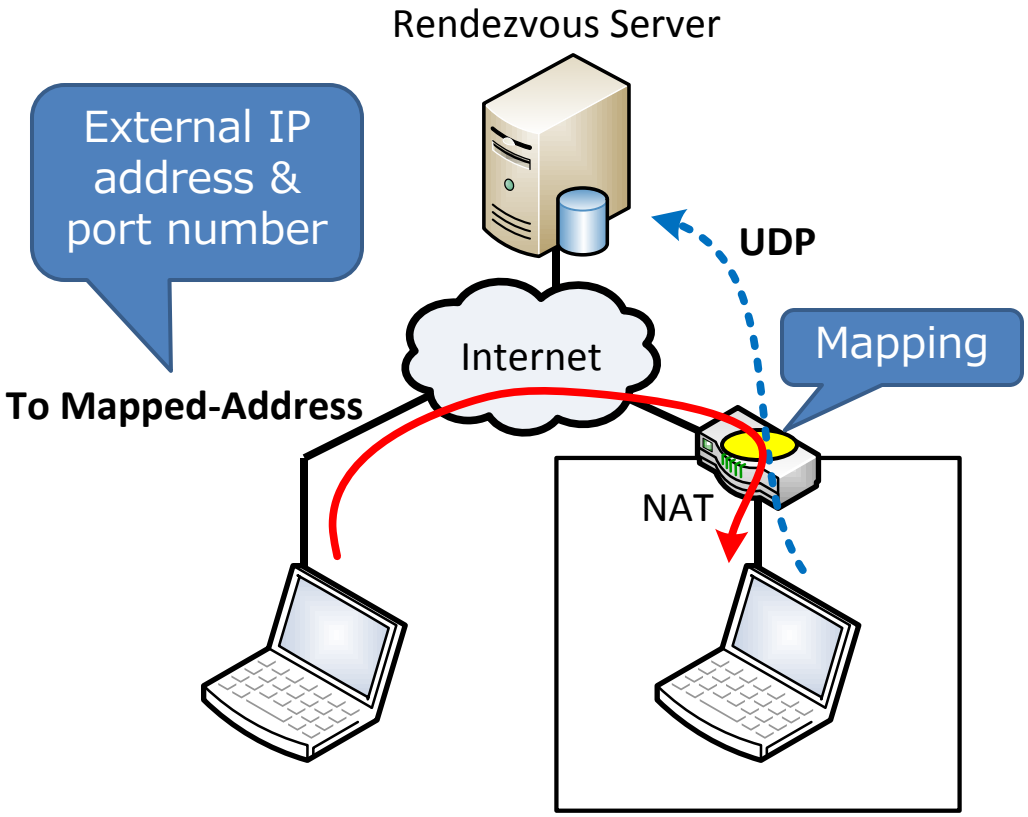
Proposed Method



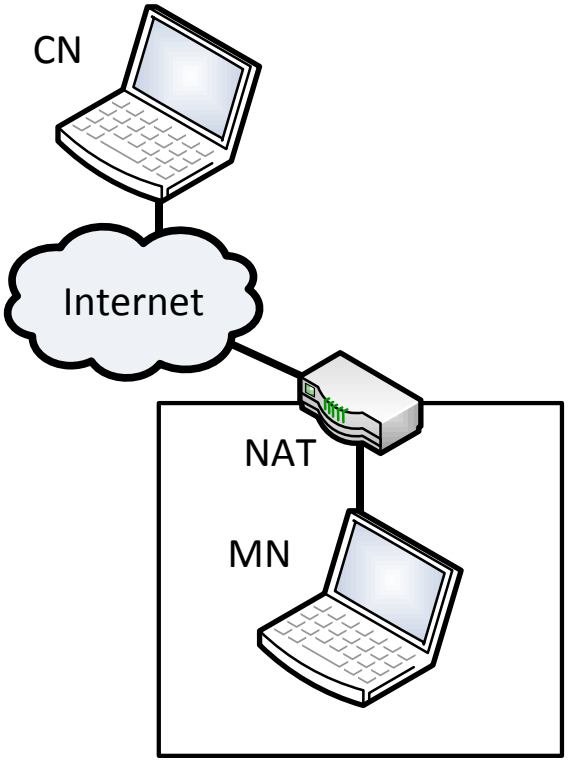
Proposed Method (Key Idea)

- Applying the principle of "**Hole Punching**" technology

Hole Punching

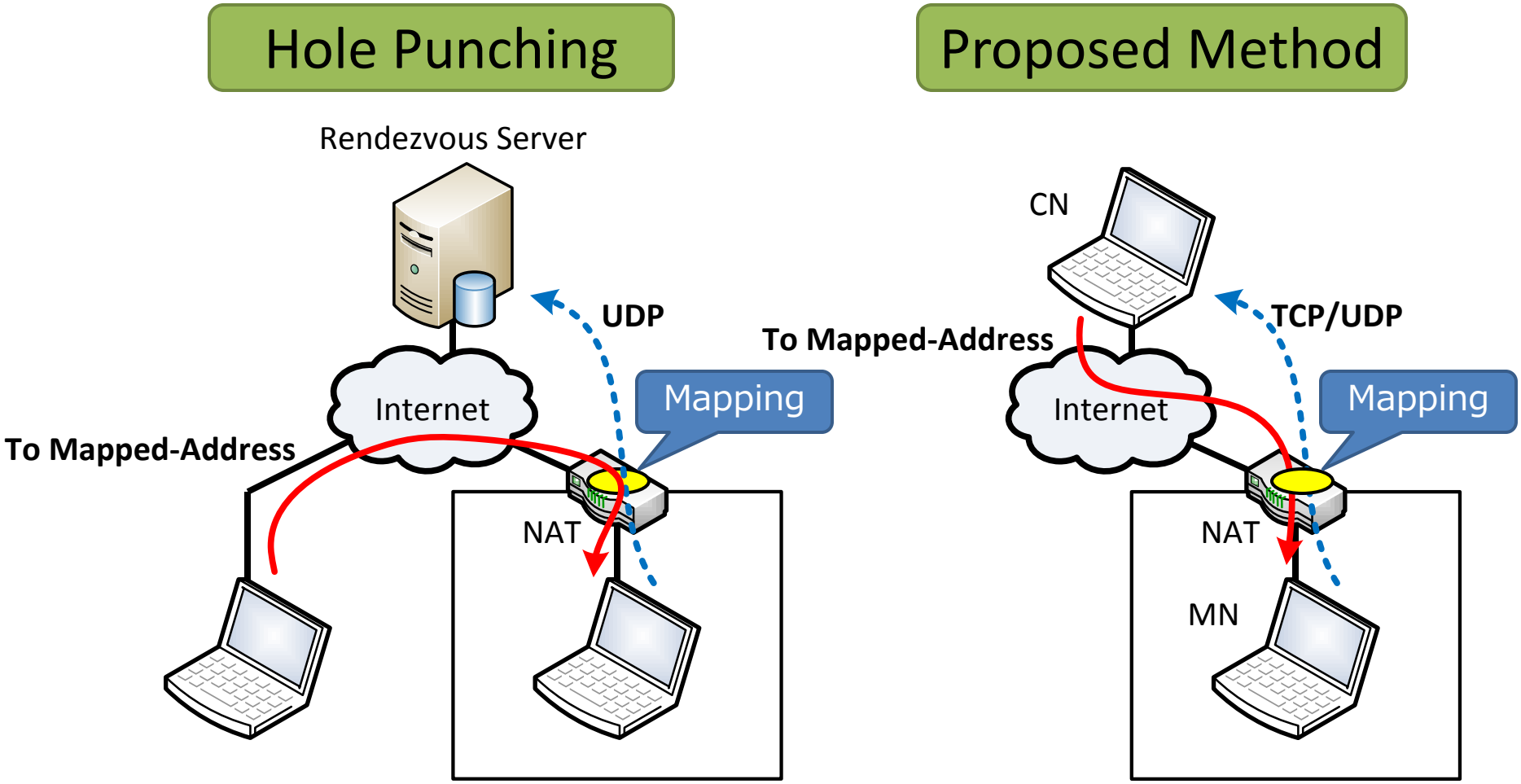


Proposed Method



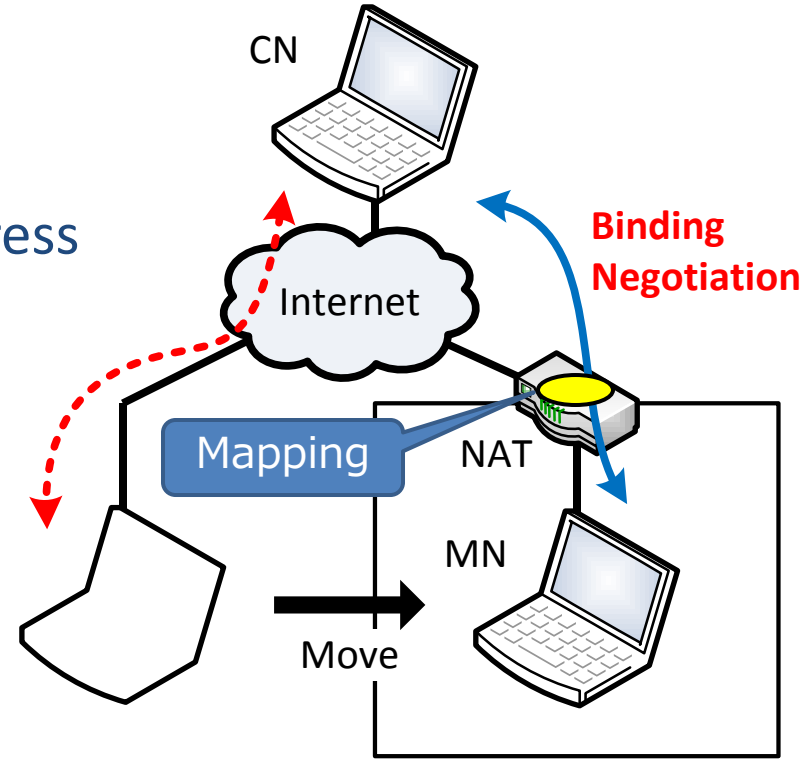
Proposed Method (Key Idea)

- Applying the principle of "**Hole Punching**" technology



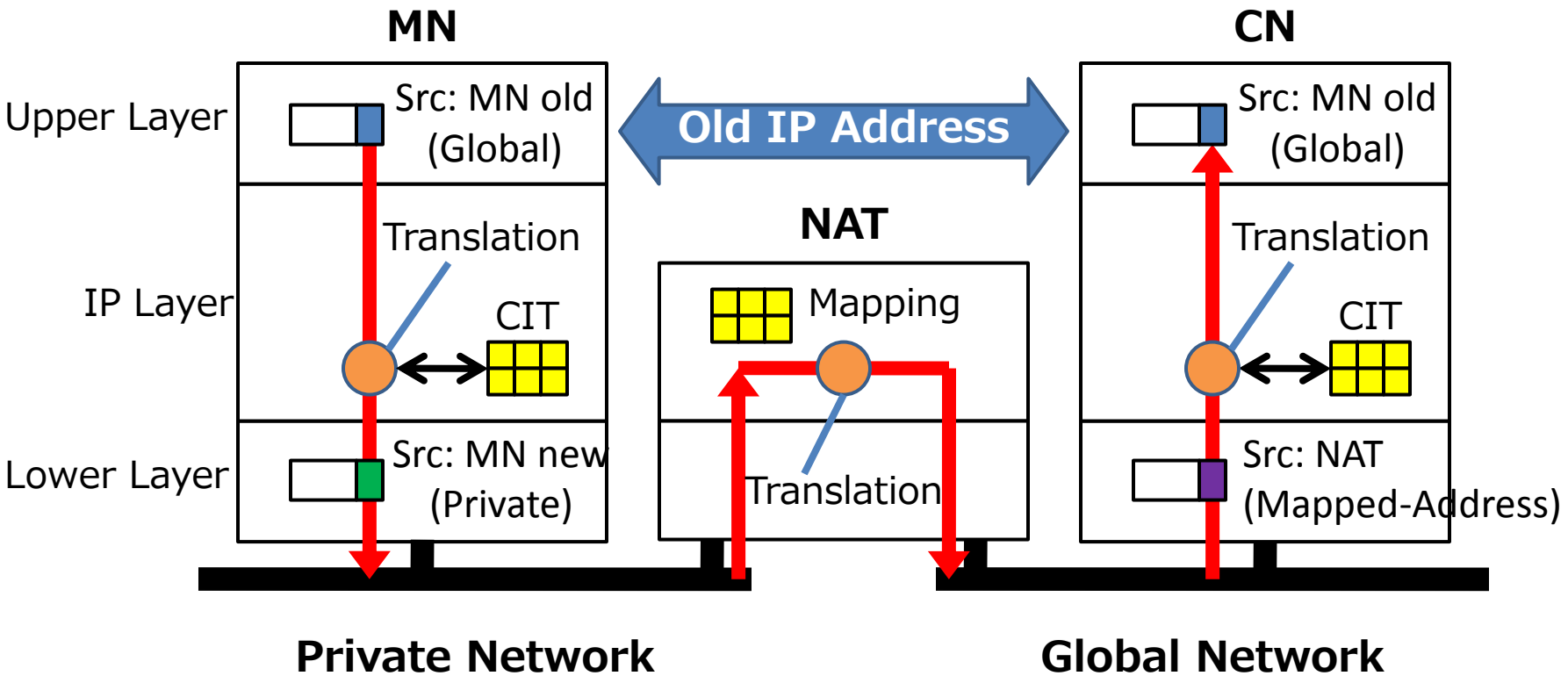
Moving to Private Network

- Binding Negotiation
  - NAT creates mapping information
  - CN replies the Mapped-Address to MN
- Movement Notification
  - Mapped-Address as Moved-Address
- Creating CITs
  - MN: Actual change
  - CN: Notified information



Address Translation

- Sending packet from MN to CN (After the movement)



Summary

- **New NAT traversal scheme for Mobile PPC**
  - End-to-End “Hole Punching”
  - MN can move between global and private networks during the communication with only end nodes

Appendixes

Benefits

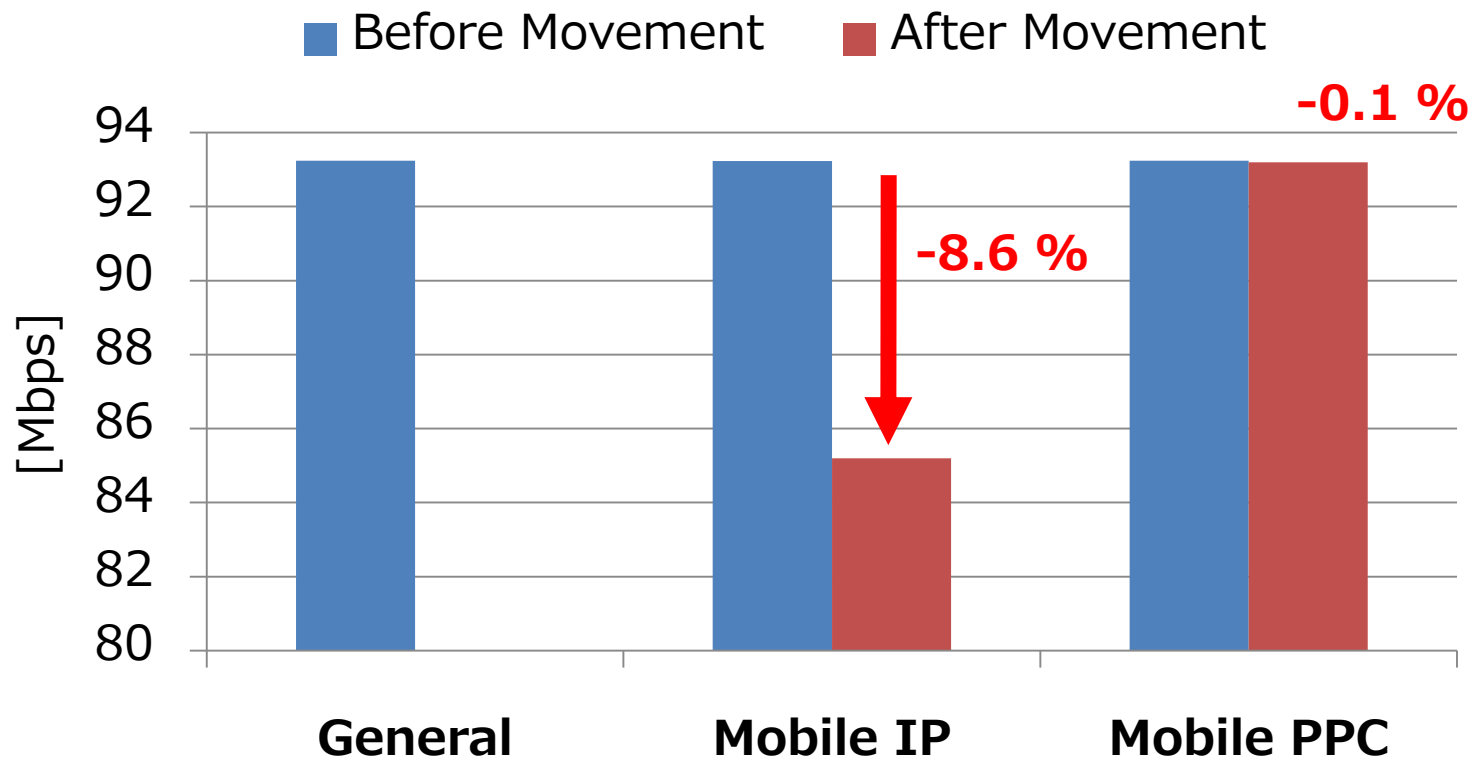
- End-to-End “Hole Punching”
  - No rendezvous server
    - No communication delay
    - No single point of failure
  - Supporting UDP and TCP communications
  - Supporting all types of NATs

- Only address translation
  - No encapsulation

    ➔ High throughput

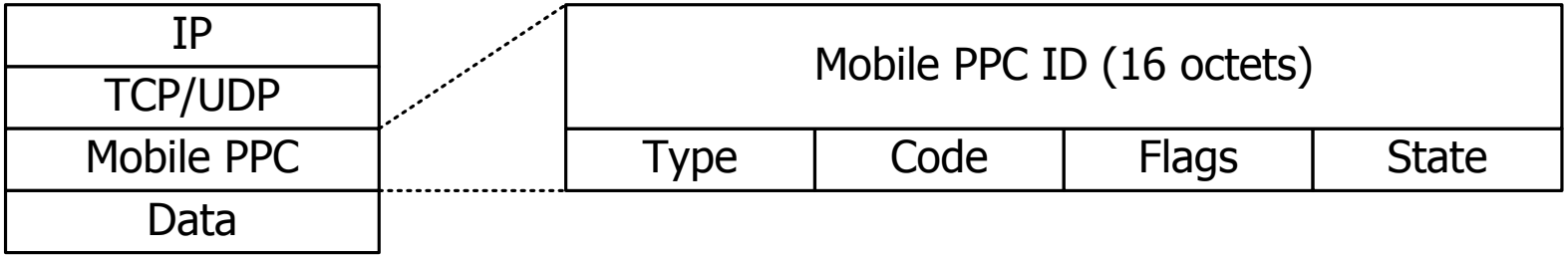
Comparison of Throughput

- "Original" Mobile IP & "Original" Mobile PPC
  - No NAT traversal



Binding Message Format

- IP header and the transport header are the same as the communication packet after the movement

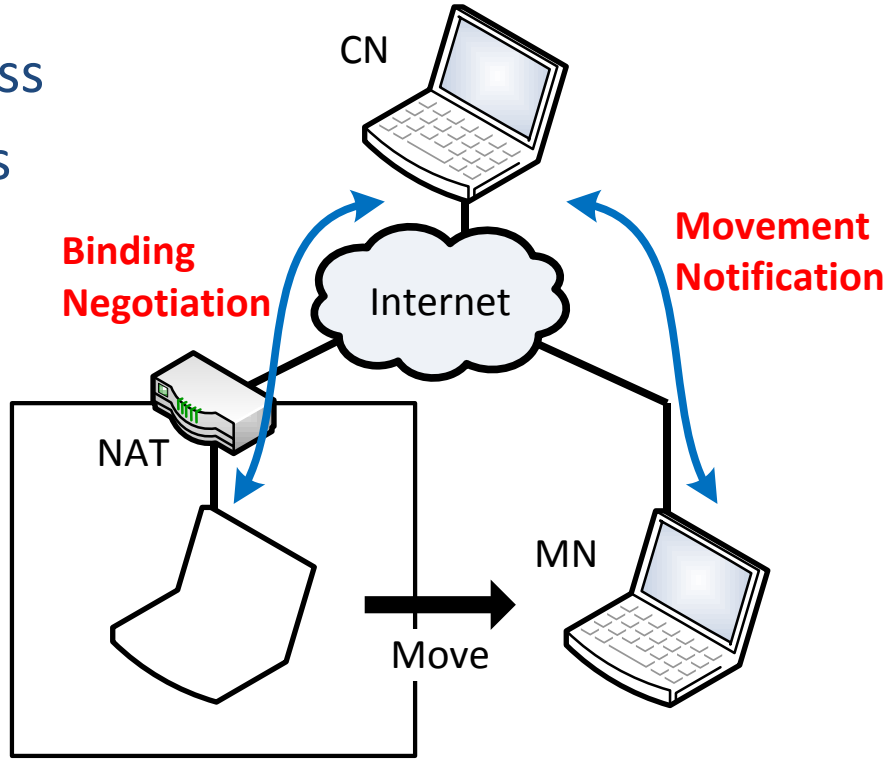


Type:	REQUEST	1	Code:	COOKIE	1	Flags:	**NAT-ON-PATH** **1**
	RESPONSE	2		DH KEY	2		**NAT-OFF-PATH** **2**
				CU	3		**KEEP-ALIVE** **3**
				BINDING	**4**		

Moving from Private to Global

- Executing the binding negotiation before the movement

- Movement notification
  - Old address: Mapped-Address
  - New address: Global address



Moving from Private to Private

- 1st Binding negotiation (Before the movement)
  - Mapped-Address 1
- 2nd Binding negotiation (After the movement)
  - Mapped-Address 2
- Movement notification
  - Old: Mapped-Address 1
  - New: Mapped-Address 2