A Proposal for a NAT Traversal System that Does Not Require Additional Functions at Terminals

Yutaka Miyazaki, Hidekazu Suzuki, Akira Watanabe
Graduate School of Science and Technology, Meijo University
1-501 Shiogamaguchi, Tempaku-ku, Nagoya, 468-8502 JAPAN

Abstract— **Demand for users accessing networks anytime and from anywhere has been increasing in the forthcoming advent of ubiquitous society. Users would strongly desire to acquire the capability of accessing to their own terminals of the home or company networks from the outside. However, networks are usually constructed with private IP addresses, and a NAT stands on the way of a communication path. In such an environment, communication cannot be initiated from terminals in the Internet. This is called "NAT traversal problem". To solve this problem, we propose a new NAT traversal system based on the modified DNS server and NAT router and concerted work between them.**

I. Introduction

In order to avoid a situation where IP addresses, home as well as enterprise networks are usually constructed based on private IP addresses. A Network Address Translator (NAT) [1] is required between the private address network and the Internet. However, in such an environment, since the inside of private address networks cannot be seen from the side of the terminals on the Internet, communications cannot be initiated from the side of terminals on the Internet to terminals in the private address networks. This problem is called "NAT traversal problem".

Conventionally, a firewall is installed between an enterprise network and the Internet, and generally, the firewall prohibits any access from terminals on the Internet. Therefore the restriction by this NAT traversal problem has not been much recognized. However, in case of home networks, a severe security policy like that for enterprise networks is not required. In the meantime, requirements for accessing terminals in the home networks freely from a terminal on the Internet are increasing, and therefore, it is quite useful and important to remove the NAT traversal problem in our future ubiquitous society.

In order to solve the NAT traversal problem, various methods, such as Simple Traversal of User Datagram Protocol Through Network Address Translators (STUN) [2], Address Virtualization Enabling Service (AVES) [3] and NAT-free protocol (NAT-f) [4], etc. have been proposed.

STUN solves the problem by using a dedicated server on the Internet. However, a third device is required and its application is limited.

AVES uses a special device called "waypoint" and a modified router. It solves the problem by relaying packets via the waypoint. However, a third device is required like the case of STUN, and the communication path is redundant.

We have separately proposed a protocol called "NAT-f", which can realize the NAT traversal without requiring any special devices. In NAT-f, a NAT router and a terminal on the Internet negotiate with each other and make NAT tables dynamically. However, it is rather difficult for general users to use NAT-f because additional functions are required in the terminals on the Internet.

In this paper, we propose a NAT traversal method that does not require any additional functions at terminals. In our proposed method, the NAT traversal is realized with the concerted work of a NAT router and a DNS server.

The existing technologies of NAT traversal are explained in detail in Section II, and our proposed method is shown in Section III. Our evaluation is given in Section IV and finally conclusion in stated in Section V.

II. Existing Technologies

A. STUN

STUN is a technology that realizes a NAT traversal using by UDP hole punching [5]. A communication path is made in the NAT in advance of communication through the access to the STUN server on the Internet from the terminal inside the NAT. In STUN, an application program for STUN is required in every terminal in the system and a special server is required on the Internet.

Fig. 1 shows an example of the case where the terminal GN (Global Node) in a global address area starts communication to the terminal PN (Private Node) in a private address area.

PN accesses the SUTN server on the Internet before the communication, and registers the information on the PN (the

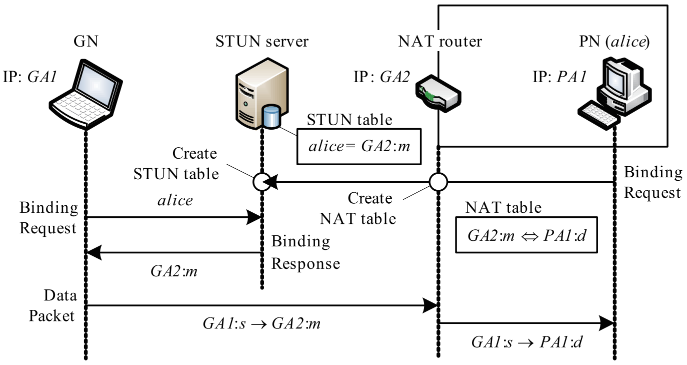


Fig. 1. Flow of STUN.

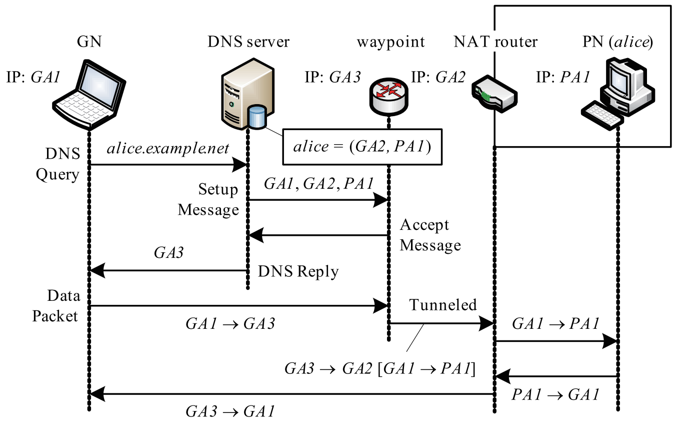


Fig. 2. Flow of AVES.

name and mapped IP address/port number generated by NAT) into the STUN table in the STUN server.

When the GN starts communication with the PN, the GN sends a query concerning the PN to the STUN server, and acquires information on the PN.

Then, the GN sends a packet to the NAT router based on the obtained information, and the NAT router sends the packet to the PN according to the NAT table.

STUN has an advantage that the existing NAT router can be used. However, a special server is required on the Internet, and its application is limited. Furthermore, it cannot be used depending on the types of NAT routers, Synmettric NAT.

B. AVES

In AVES, a server called "waypoint" is installed in the global address area, and communication is performed via the server.

Fig. 2 shows the flow of AVES. When the GN inquires the DNS server about the PN, the DNS server checks the waypoint to see whether the PN is registered or not. If the PN is registered, the DNS server sends a setup message to the waypoint. The setup message contains addresses of the GN, NAT router, and the PN, which are necessary to create a tunneling path between waypoint and NAT router. When the DNS server receives an accept message from the waypoint, it responds to PN's query for the GN with the IP address of the waypoint, "$GA3$". Next, the GN starts communication destined for the waypoint. The waypoint changes the destination address into PN's private address, $PA1$. The packet is encapsulated with the NAT router's global address, $GA2$, and sent to the NAT router. When the NAT router receives the above packet, the packet is decapsulated and sent to the PN. For the reverse direction, response packets from the PN are directly sent to the GN. This is the way communication is performed in AVES.

AVES has an advantage that the NAT traversal can be realized with normal terminals without any additional functions. However, a special server is required on the Internet. Also, the communication path becomes redundant and the packet length changes due to the encapsulation.

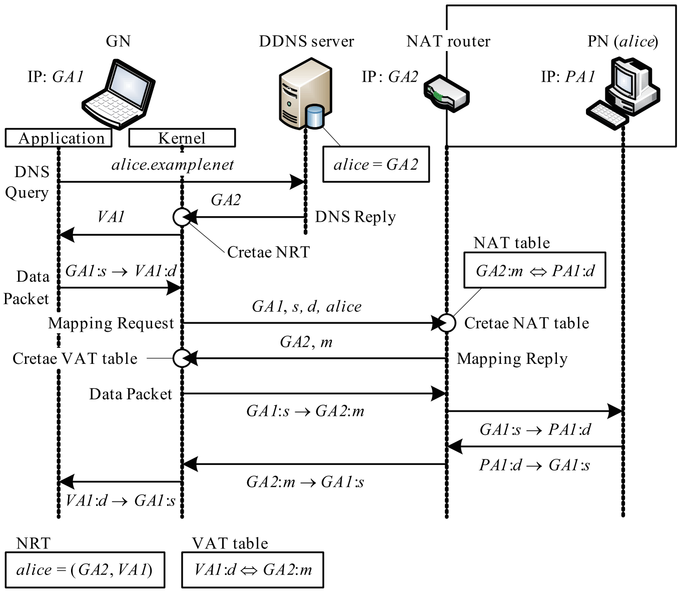


Fig. 3. Flow of NAT-f.

C. NAT-f

NAT-f can realize a NAT traversal without any additional devices. The GN that is equipped with NAT-f functions and the NAT router negotiate with each other in advance of the communication and generates NAT tables dynamically.

Fig. 3 shows the flow of NAT-f. When the GN starts communication with a PN, the GN inquires the Dynamic DNS (DDNS) [6] server about PN's IP address by the FQDN "$alice.example.net$". The DDNS server sends back to the GN the IP address of the NAT router, $GA2$. The kernel in the GN hooks the reply message, and gets the host name of the PN and the IP address of the NAT router. Furthermore, it changes the IP address of the NAT router, $GA2$ to a virtual IP address "$VA1$", and stores them in a Name Relation Table (NRT). The virtual IP address is defined to distinguish the communication partner behind the NAT-f router, and this is effective only in the GN. The virtual IP address, $VA1$ is reported to the application program in the GN as PN's IP address. When the GN transmits the packet destined for the NAT router, the kernel in the GN refers to a Virtual Address Translation (VAT) table that contains the virtual IP address and the port number corresponding to the PN, and the IP address and the port number in the NAT router. VAT table is generated at the time of the negotiation between GN and the NAT router. If the corresponding VAT table exists, the kernel in the GN changes the IP address and the port number in the packet according to the VAT table, and sends it to the NAT router. If the VAT table does not exist, the packet is temporarily stored in the kernel memory, and the NAT-f negotiation starts.

The GN reports such information as the source IP addresses "$GA1$", source/destination port numbers "s, d" obtained from the stored packet, the host name of PN, "$alice$" obtained from NRT.

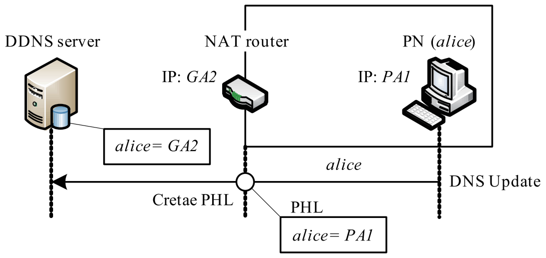


Fig. 4. DNS registration.

When the NAT router receives the above packet, it generates a NAT table from the private IP address of the PN, $PA1$ corresponding to $alice$. Then, the NAT router sends back the mapping reply that contains the mapped IP address and port number "$GA2 : m$" generated in the NAT table (See in Fig. 3).

When the GN receives the above packet, it generates the VAT table from the information in the packet. Then, the NAT-f negotiation is completed, and the packet which had been stored temporarily is restored.

After that, communications is executed by translating IP addresses and port numbers in the packets according to the VAT table in the GN and the NAT table in the NAT router. In NAT-f, peer-to-peer communication is executed and there is no need for encapsulation. Moreover, it has an advantage that a third device is not required. The problem is that the GN has to install NAT-f functions.

III. Proposed Method

A. Network configuration

In our proposed system, a NAT traversal is realized by adding functions to the DNS server and the NAT router. General terminals can be used both for the GN and the PN.

Devices required for our proposed system are, a NAT router that has a private network under itself, a NAT Traversal Support (NTS) server that works in concert with the NAT router, and a DDNS server. The NTS server is an extended version of the DDNS server. Various functions of our proposed method are implemented in the NTS server and the NAT router.

In the following, the case that the GN starts communication with PN ($alice$) is shown.

B. Prior setting

Before applying our proposed method, the GN has to be registered its NTS server as the primary DNS server.

Also, FQDN of the PN and the IP address of the NAT router are to be registered in the DDNS server shown in Fig. 4. These procedures are the same as those for a general DNS registration.

At the time of the DNS registration, a DNS update packet is sent to the DDNS server from the PN. The NAT router which receives the packet memorizes the private IP address and the host name of the PN in a Private Host List (PHL).

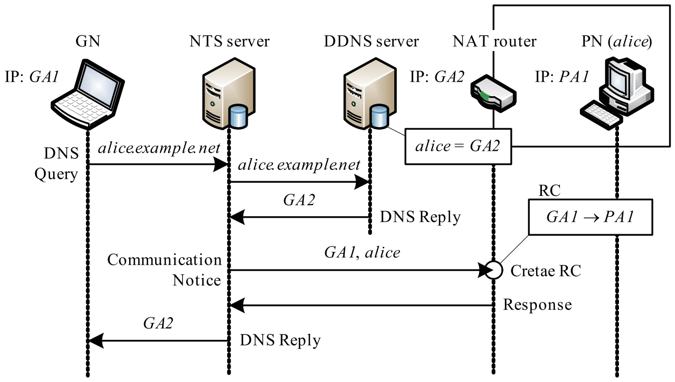


Fig. 5. Sequence of name resolution.

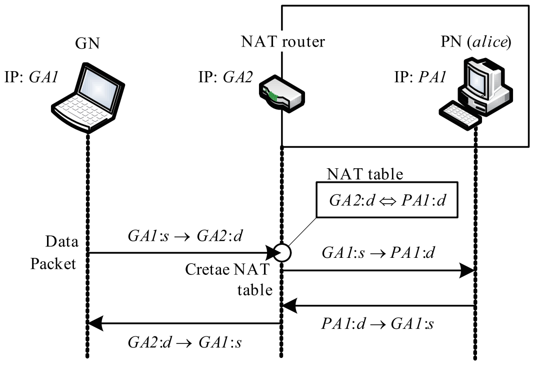


Fig. 6. Sequence of the start of communications.

C. Name resolution

An example of the name resolution sequence for the case where the GN starts communication with the PN ($alice$) is shown in Fig. 5. The GN sends a DNS query to the NTS server. The NTS server forwards the query to the upper DNS server, and obtains the IP address corresponding to alice, $GA2$. The NTS server then notifies the NAT router that there is a connection request to alice from the GN. The NAT router that receives the above packet refers to the PHL and memorizes the fact that $GA1$ is going to have a connection with $PA1$, in a Request Cache (RC), and responds to the NTS server. The NTS server then sends back the already obtained address, which is reported from the upper DNS server to $GA2$.

D. The start of communications

The sequence of the communication in our method is shown in Fig. 6. The GN sends packets to the NAT router. When the NAT router receives the above packet, it checks the RT. If the RC corresponding to the source IP address is existed, the NAT router creates a NAT table from the received packet and RC. The NAT router forwards the packet to $alice$ according to the created NAT table. The response packet from $alice$ for the GN is relayed with the usual NAT process. After that, communication continues according to the above-mentioned procedures.

As for the communications which begins from inside terminals, conventional NAT procedures are executed.

TABLE I

COMPARISON OF NAT TRAVERSAL TECHNOLOGIES

	Proposed method	STUN	AVES	NAT-f
GN	◯	×	◯	×
PN	◯	×	◯	◯
Third device	△	×	×	◯
DNS server	◯	◯	×	◯
NAT router	×	△	×	×
Application	◯	×	◯	◯

IV. EVALUATION

Comparison of our proposed method with the existing technologies is shown in Table I. In the items described as "GN", "PN", "DNS server", and "NAT router", ◯ indicates that new functions are not required in each device, and × indicates that they have to be modified. In the item "Third device", ◯ indicates that a third device is not required in the system, and × indicates that it is required. In the item "Application", ◯ indicates that there is no restriction on applications, and × indicates that there are some restrictions on them.

Although STUN can be realize a NAT traversal without adding any functions to the NAT router, it cannot be used depending on the types of NAT. Thus "NAT router" in STUN is mark as △. In addition, applications used in GN and PN are required to embed some functions of STUN client.

AVES does not need to have any additional functions at user terminals. However waypoints, special DNS server and NAT router for AVES are required. Moreover, it causes the performance degradation of communications due to relaying and encapsulation at waypoints.

NAT-f does not need a third device, but, it is necessary to add functions to the GN and the NAT router. On the other hand, our proposed system does not need to add any functions to user terminals. There is no restriction in its application and P2P communication is possible. Although a special NTS server is required, it can be realized by way of modifying a DNS server. Thus "Third device" of our proposed method is marked as △.

In proposed method, a NAT traversal is easily realized from any terminals wherever users go. Therefore, any Internet service provider can deploy wireless LAN services using private IP addresses with our proposed system.

V. CONCLUSION

In this paper, we have proposed a NAT traversal system that does not require additional functions at terminals. In our proposed system, a NTS server and a NAT router work in concert in advance of communications, and the NAT router generates a NAT table dynamically. Communications between terminals are possible by P2P.

In the future, we will complete the implementation of the NTS server and the NAT router functions, and make a thorough evaluation of our system. Moreover we will cover protocols ,which network layer information is embedded in an application layer, like SIP , with the proposed system.

REFERENCES

[1] P. Srisuresh and K. Egevang, "Traditional ip network address translator (traditional nat)," RFC 3022, Jan. 2001.

[2] 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.

[3] T. S. E. Ng, I. Stoica, and H. Zhang, "A waypoint service approach to connect heterogeneous internet address spaces," in *Proc. USENIX Annual Technical Conference*, June 2001, pp. 319–332.

[4] H. Suzuki and A. Watanabe, "Implementation and evaluation of nat-f actualizing address area transparency," in *Proc. Symposium on Multimedia, Distributed, Cooperative and Mobile Systems 2006 (DICOMO2006)*, vol. 2006, no. 6, July 2006, pp. 453–456.

[5] 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.

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

IEEE TENCON 2007
Oct.30 – Nov.2 ,2007
Taipei international Convention Center, Taipei, Taiwan

A Proposal for a NAT Traversal System that Does Not Require Additional Functions at Terminals

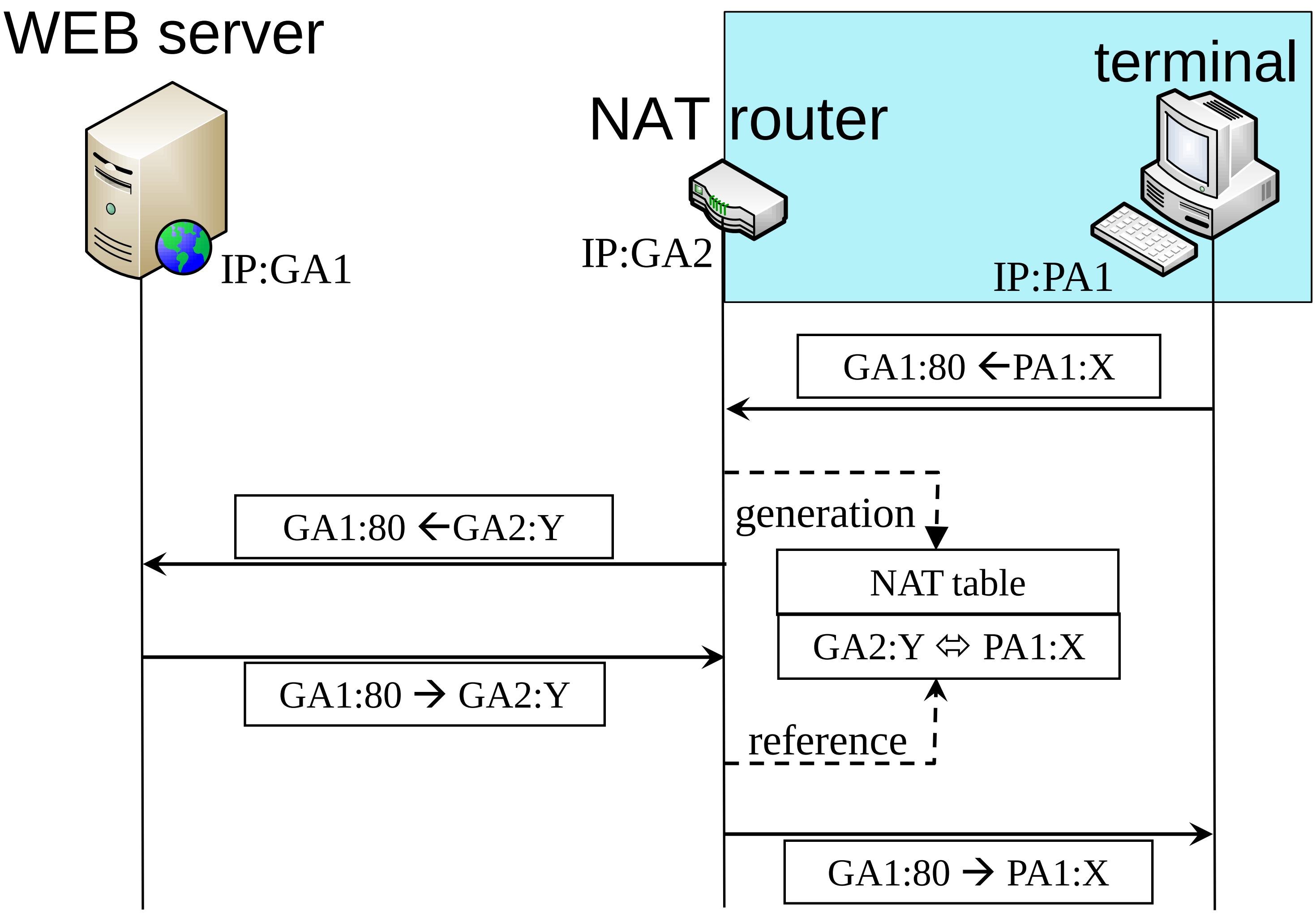
Graduate School of Science and Technology, Meijo University
Yutaka Miyazaki, Hidekazu Suzuki, Akira Watanabe

Introduction

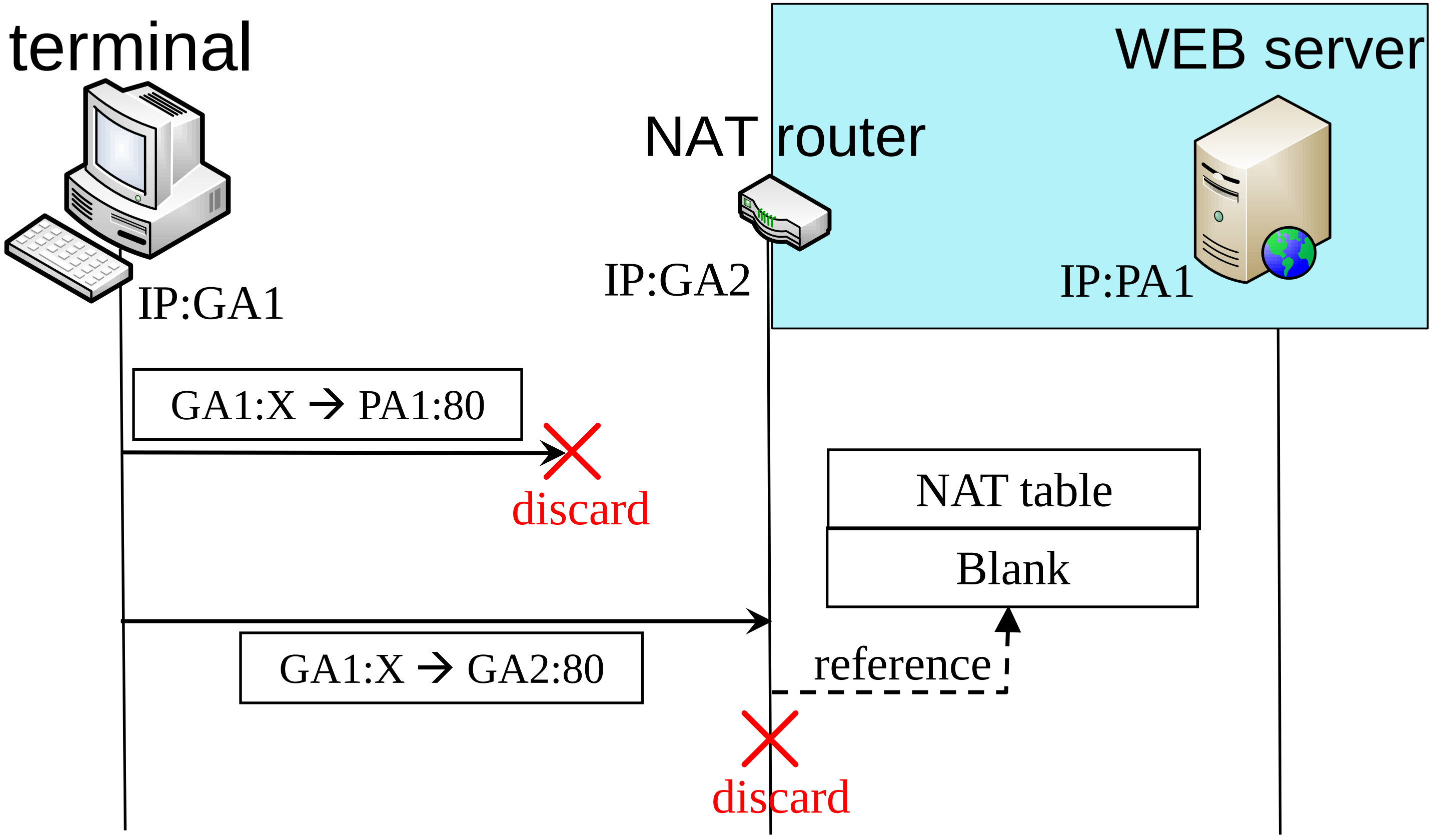
- Ubiquitous society is coming with the spread of the Internet.
  - ➢Users hope to access networks at anytime from anywhere .

- Home networks and enterprise networks are usually constructed with private IP addresses.
  - ➢NAT (Network Address Translator) is indispensable.

NAT Operations (from inside to outside)



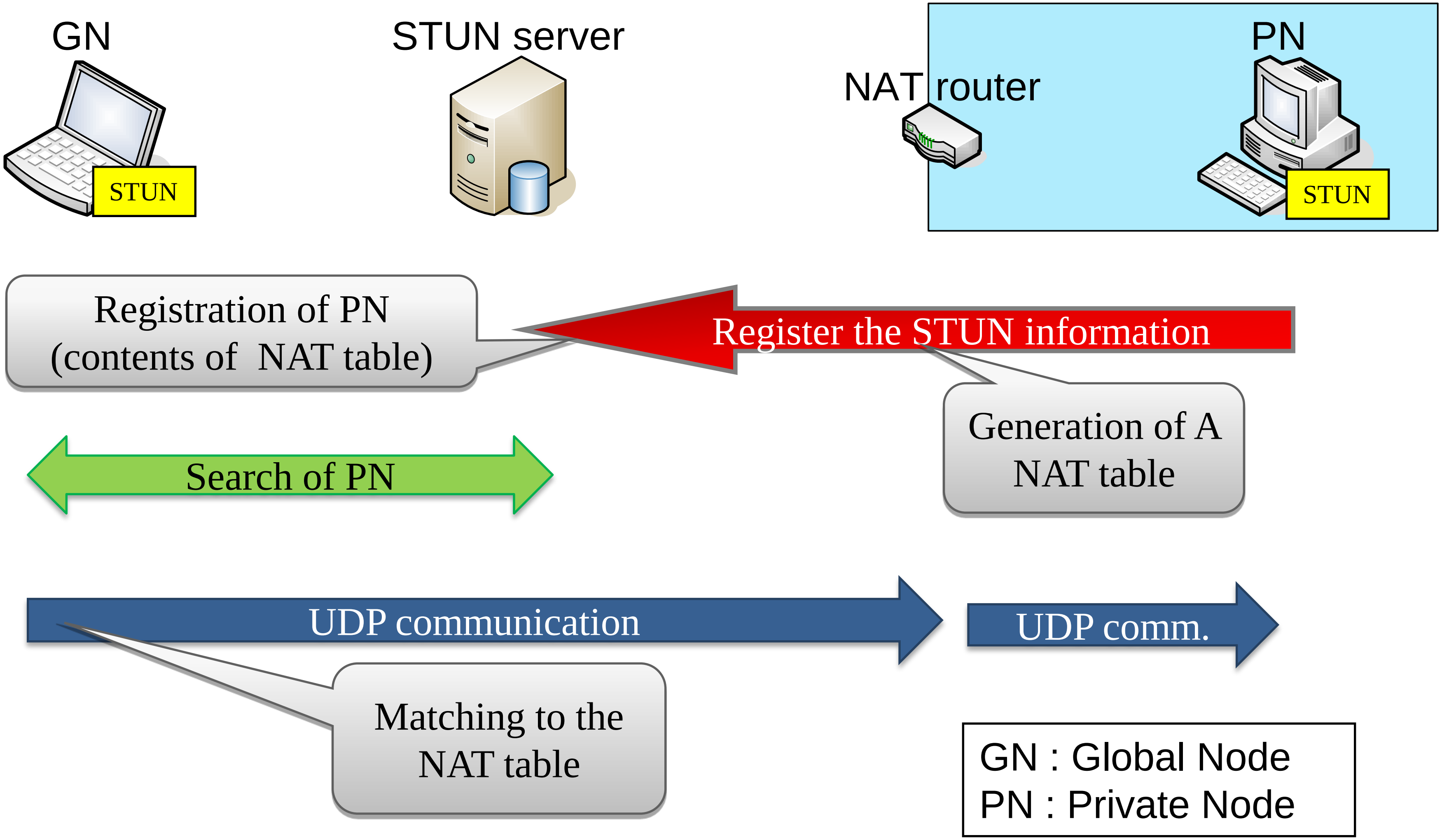
NAT Operations (from outside to inside)



A NAT Traversal Problem

STUN (Simple Traversal of UDP Through NATs)

is defined in RFC 3489



GN

STUN server

NAT router

PN

STUN

STUN

Registration of PN (contents of NAT table)

Register the STUN information

Generation of A NAT table

Search of PN

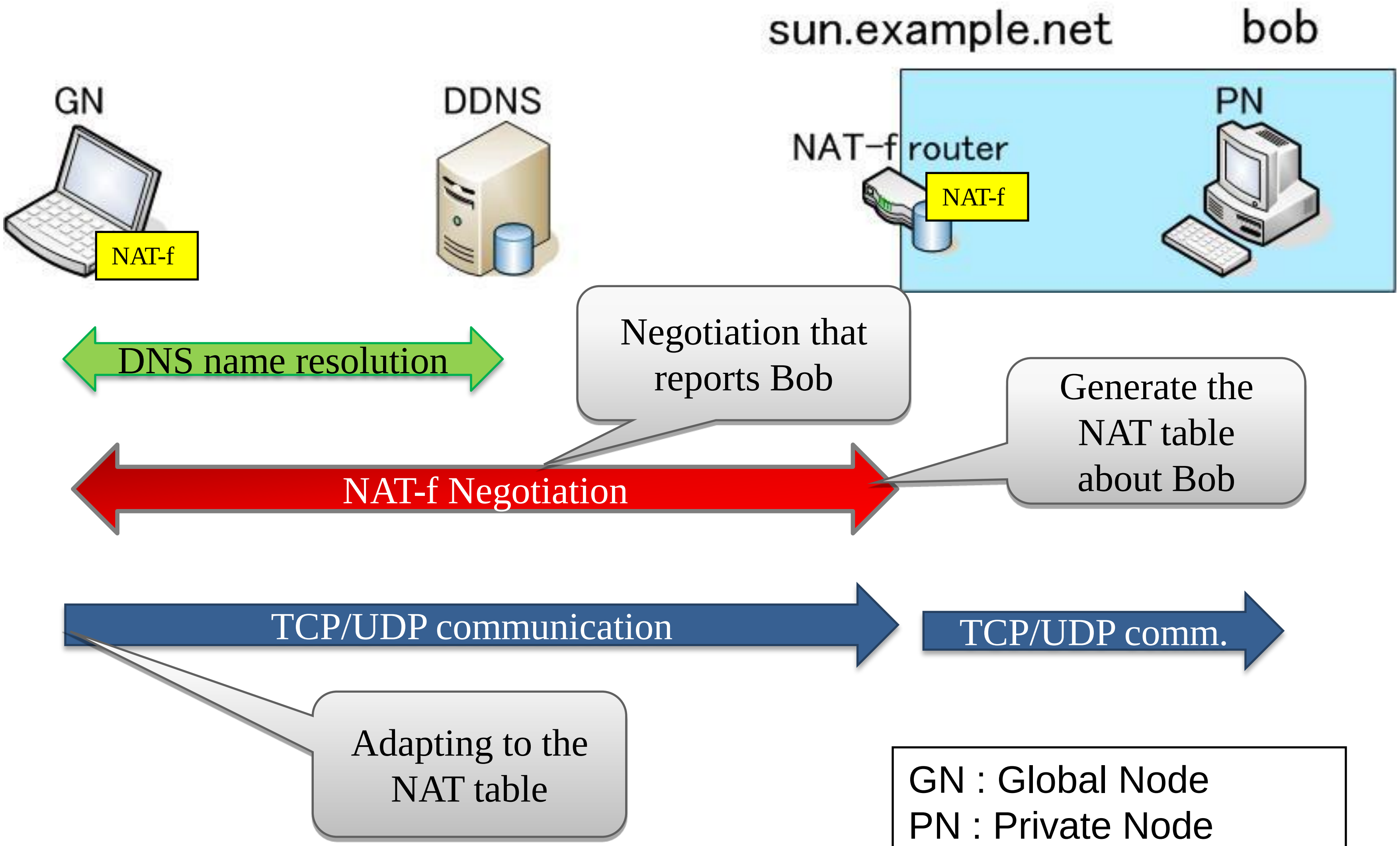
UDP communication

UDP comm.

Matching to the NAT table

GN : Global Node
PN : Private Node

NAT-f (NAT-free protocol)



DNS name resolution

Negotiation that reports Bob

Generate the NAT table about Bob

NAT-f Negotiation

TCP/UDP communication

TCP/UDP comm.

Adapting to the NAT table

GN : Global Node
PN : Private Node
DDNS : Dynamic DNS

A Proposal for a NAT Traversal System

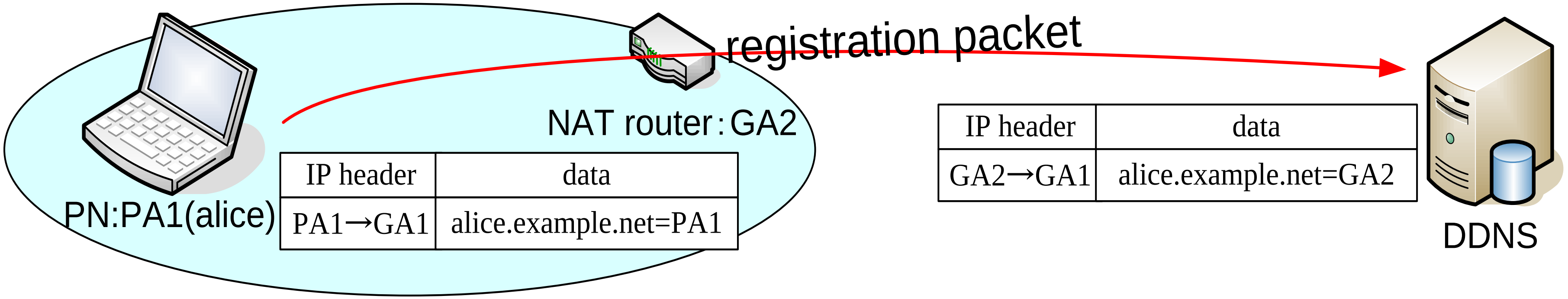
The problem is solved without modification to the end terminals.

In this system, a NAT router and a DNS server are modified to solve the NAT Traversal problem.

The modified DNS server → NAT-Traversal Support Server (NTS server)

Proposal system : Advanced setting

- “the PN’s name” and “The NAT router’s Global IP address” are registered to a DDNS server in advance.



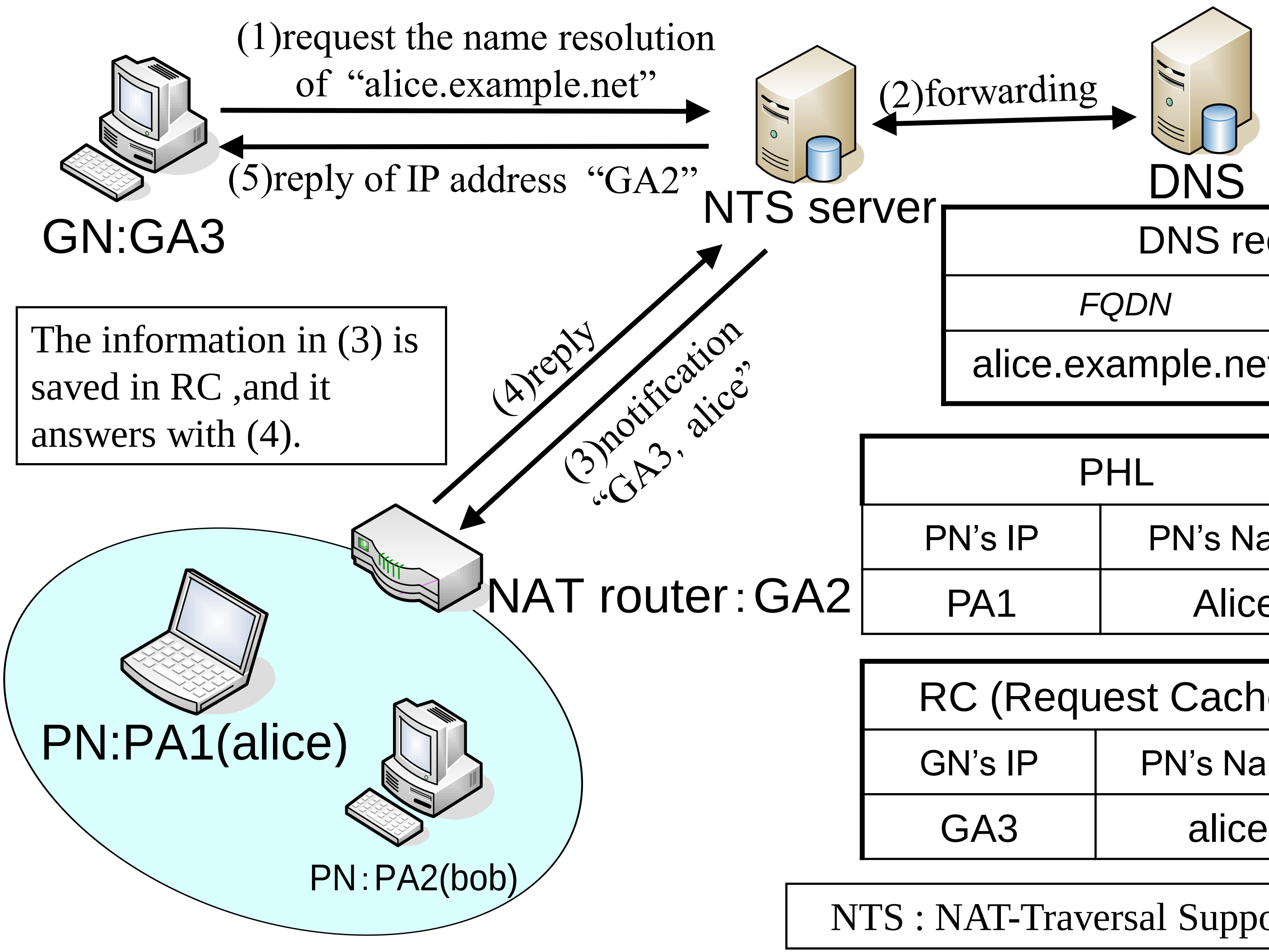
IP header	data
PA1→GA1	alice.example.net=PA1

IP header	data
GA2→GA1	alice.example.net=GA2

- In the NAT router, a Private Host List (PHL) is generated in the NAT router at the time of the DDNS registration.

PHL (Private Host List)	
PN’s IP	PN’s Name
PA1	alice

Proposal system : Name resolution


(1)request the name resolution of "alice.example.net"
(5)reply of IP address "GA2"
(2)forwarding
DNS
NTS server
GN:GA3
(4)reply
(3)notification "GA3, alice"
NAT router：GA2
PN:PA1(alice)
PN：PA2(bob)

The information in (3) is saved in RC ,and it answers with (4).

DNS record	
FQDN	*NAT router*
alice.example.net	GA2

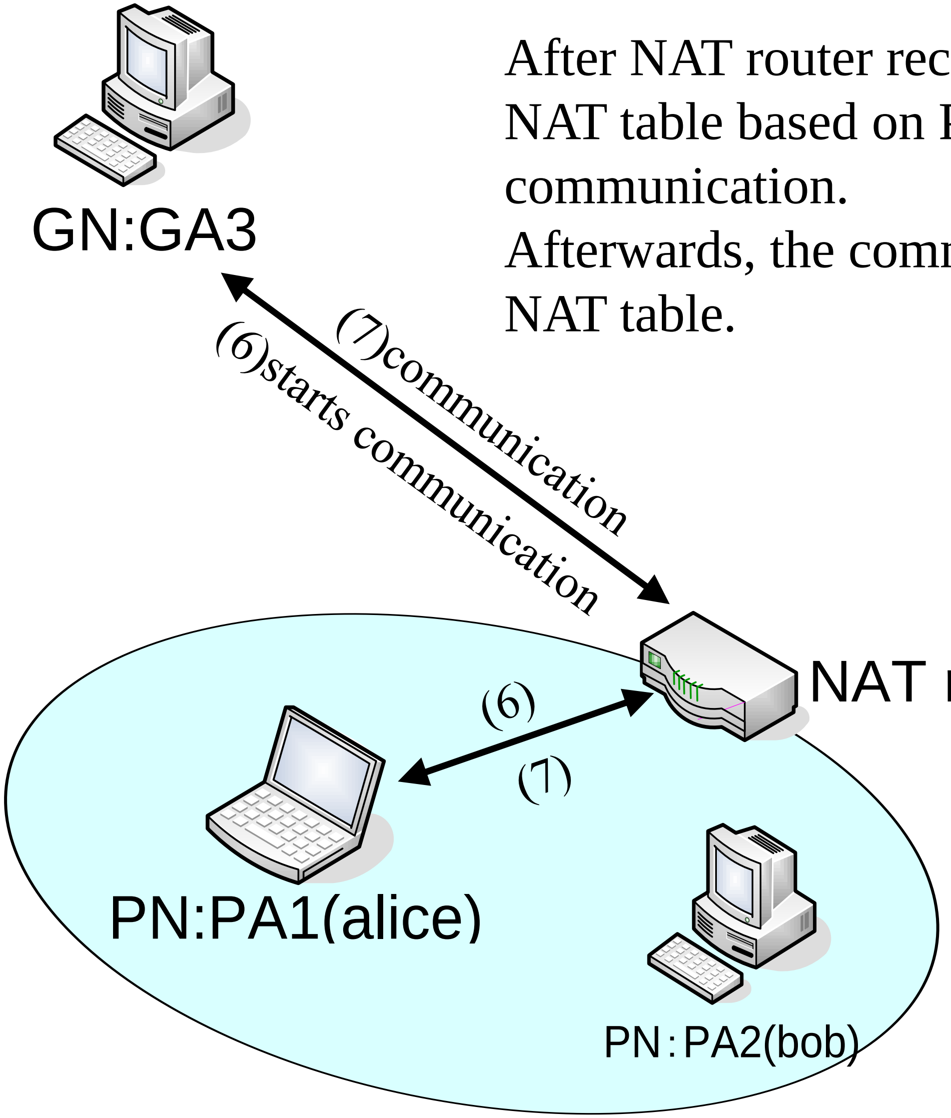
PHL	
PN's IP	PN's Name
PA1	Alice

RC (Request Cache)	
GN's IP	PN's Name
GA3	alice

NTS : NAT-Traversal Support

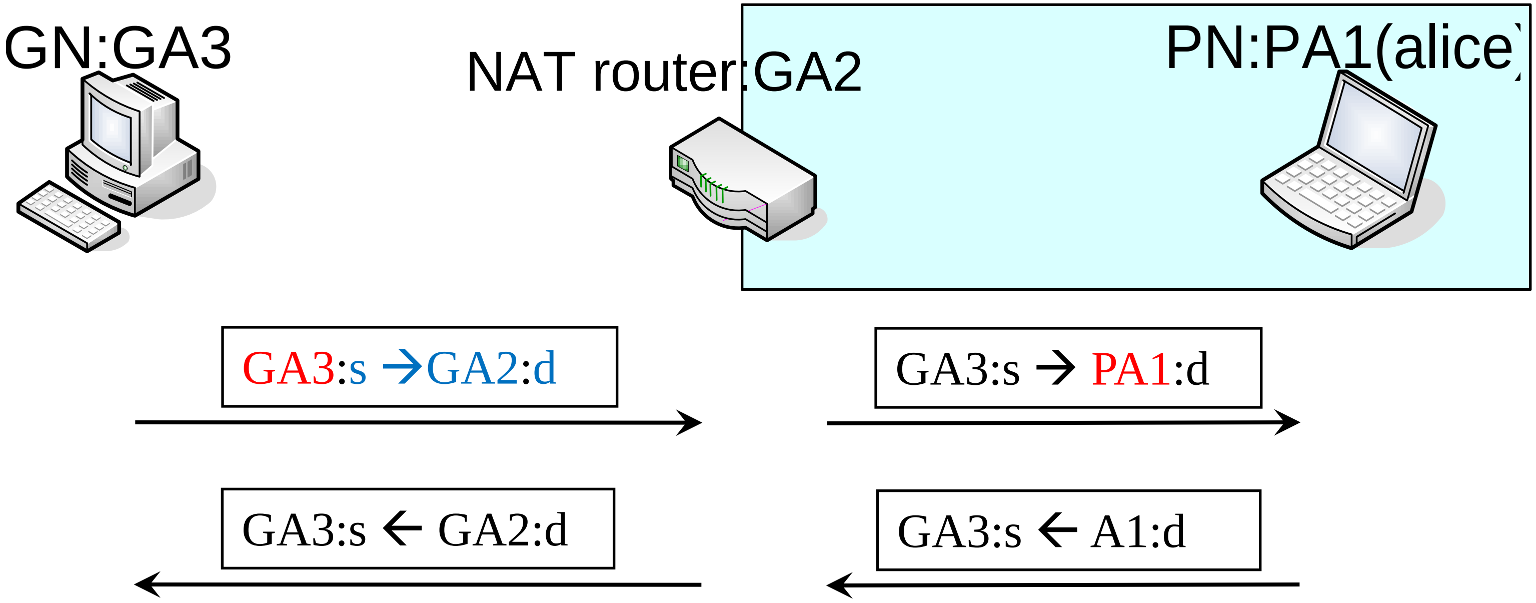
Proposal system : Communication

After NAT router receives (6), it generates an original NAT table based on PHL and RC, and can relay communication.
Afterwards, the communication is performed with the NAT table.



PHL + RC		
PN‘s IP	PN‘s Name	GN’s IP
PA1	alice	GA3

Generation of an Original NAT table



PHL	
PN's IP	PN's Name
PA1	Alice

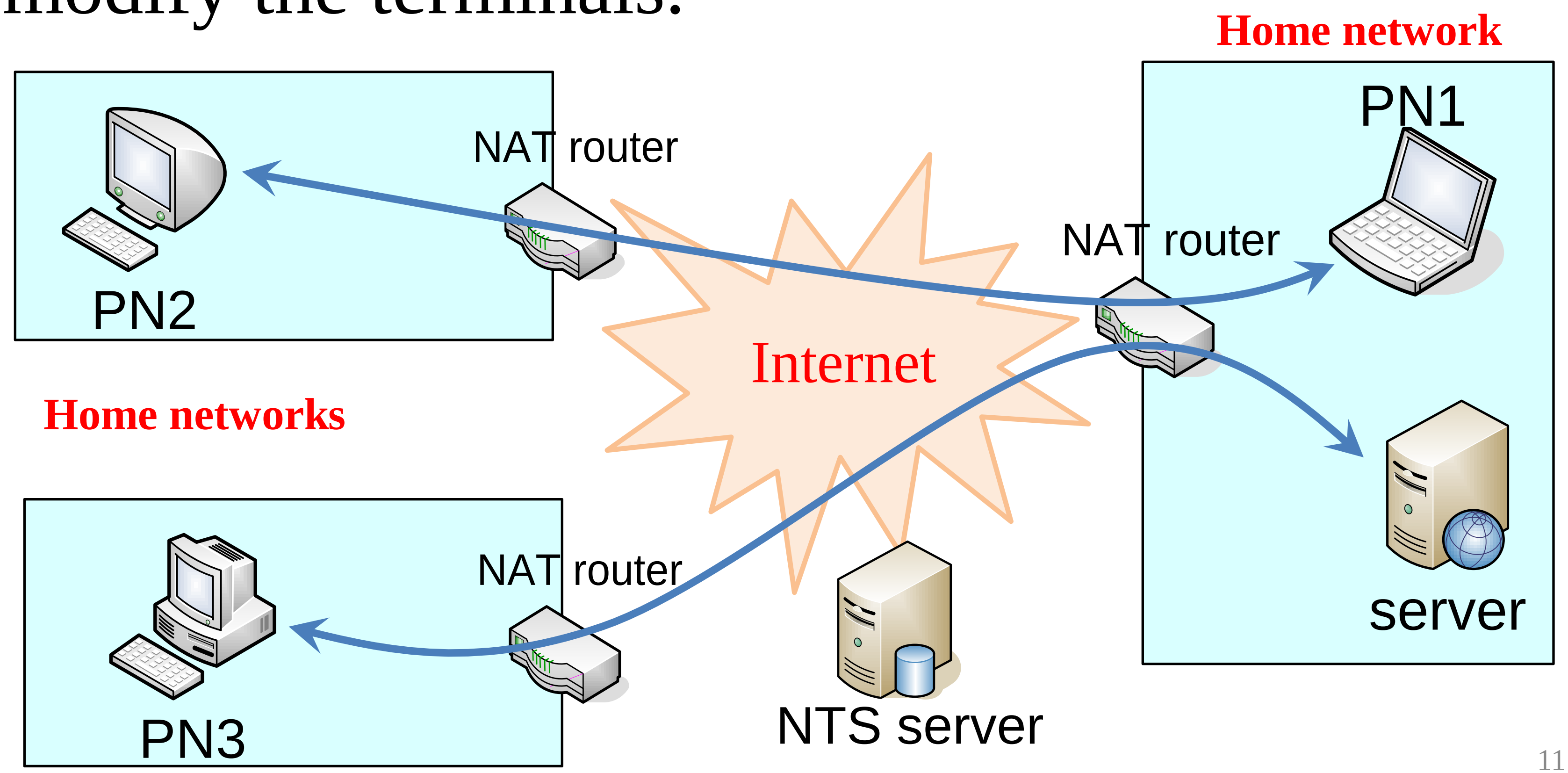
RC	
GN's IP	PN's Name
GA3	alice

NAT table

GN		NAT router		PN		Protocol
address	port	address	port	address	Port	
GA3	s	GA2	d	PA1	d	TCP

Use scene

- users can start communication without being conscious of the NAT router and it is not needed to modify the terminals.



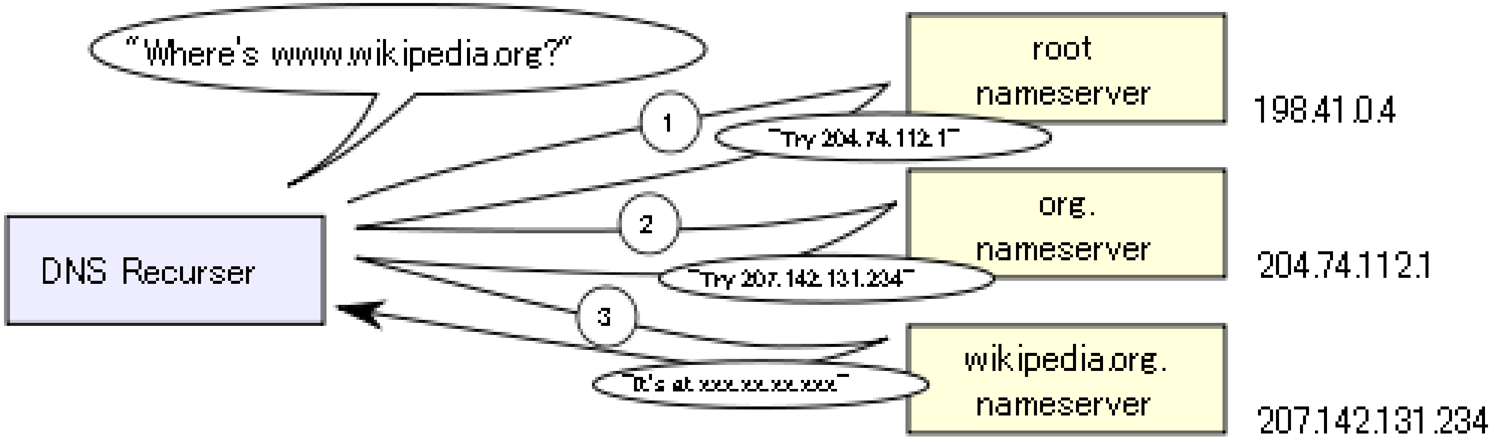
Conclusion

- The proposal system
  - It can solve the NAT Traversal Problem with the modified NAT router and the modified DNS server, NTS server, without modifying terminals.
  - The NAT router generates an original NAT table from PHL and RC made in the NAT router previously.
- Future
  - Realization of the proposal system

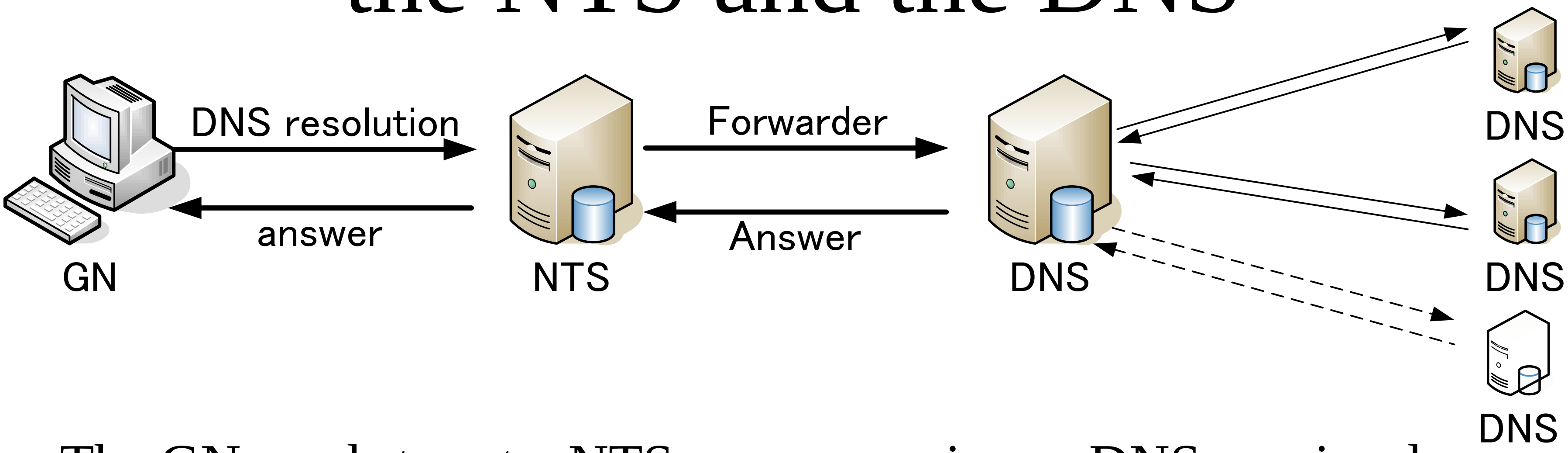
Appendixes

RFC1034,1035 DNS（Domain Name system）

- Port No.：53/UDP and 53/TCP
- It serves as the "phone book" for the Internet.
- It translates human-readable computer hostnames into the IP addresses that networking equipment needs for delivering information.



Relation between the NTS and the DNS



- The GN needs to set a NTS server as primary DNS previously.

  → The NTS server gets the IP address of the GN by performing communication with the GN directly.
- If the PN of a different address space increases, correspondence of the NTS server may worsen.
- If this system spreads, and the function to exchange with a router like NTS to a general DNS is mounted, a GN can be realized, without changing a primary DNS.

The case which cannot support

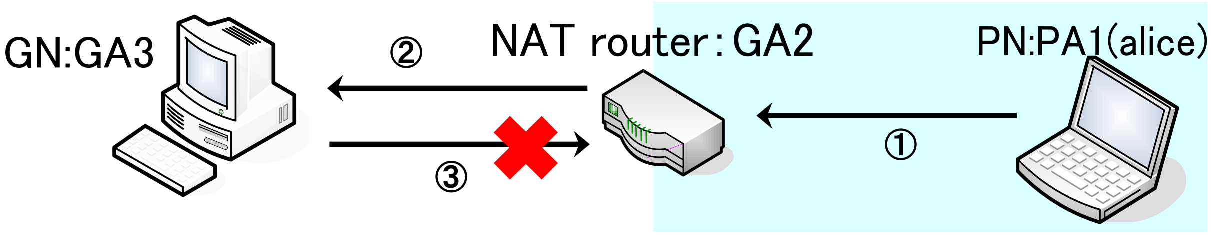
- When application controls IP addresses and ports.
  - FTP
  - SIP

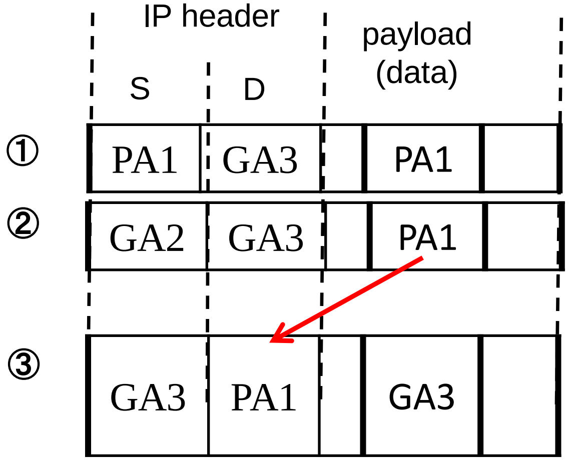
➢ The information on a IP address or a port is included in the payload of the packet, and it is not changed at the time of NAT passage.

ALG (Application Layer Gateway)
is mounted in a NAT router and solved.

ALG (Application Layer Gateway)

- Session establishment between the different-species networks with NAT.



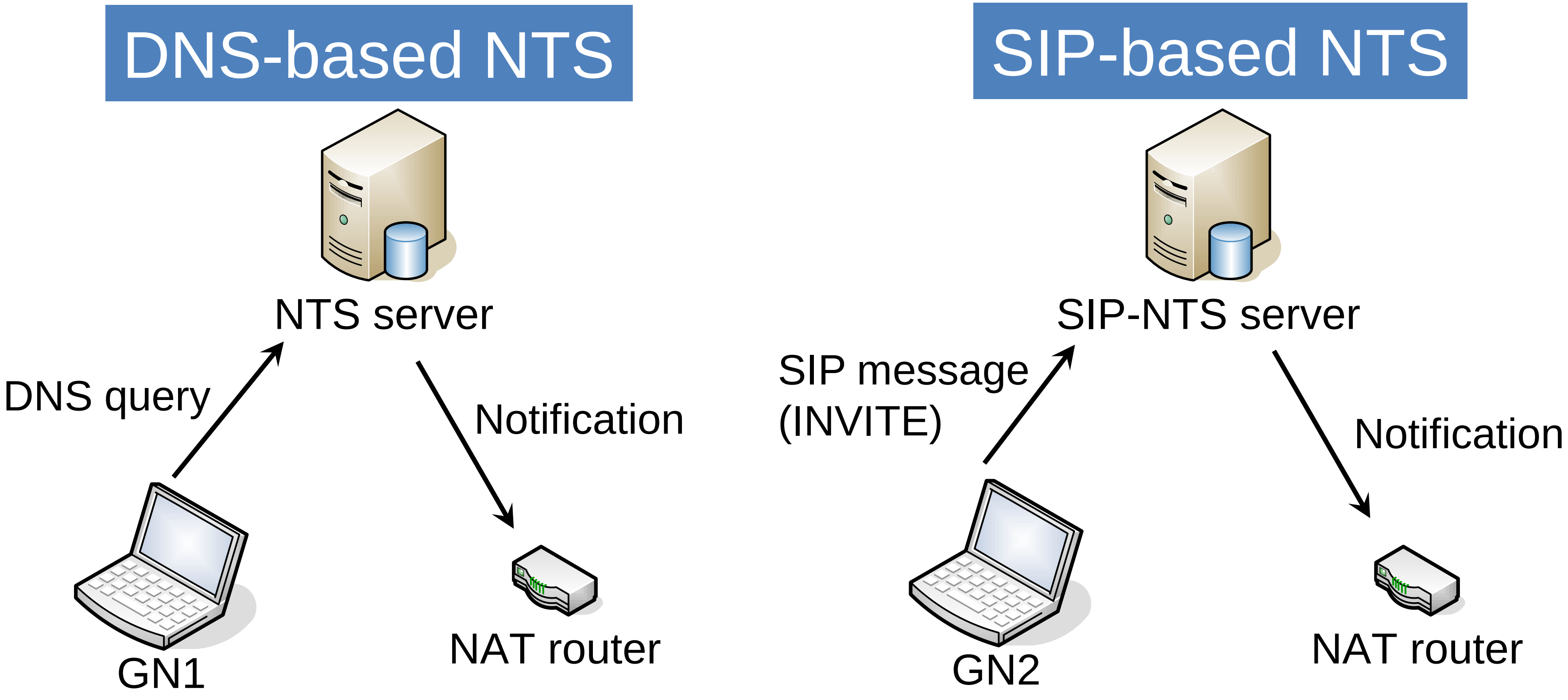


	IP header			payload (data)	
	S	D			
①	PA1	GA3		PA1	
②	GA2	GA3		PA1	
③	GA3	PA1		GA3	

- Although the address indicated to IP/TCP / UDP header is rewritten in NAT, it does not involve in payload part.
- The IP address in application is also rewritten by ALG.

Can you use SIP Applications ?

- Proposed method does not support SIP
- Difference of the name resolution processes

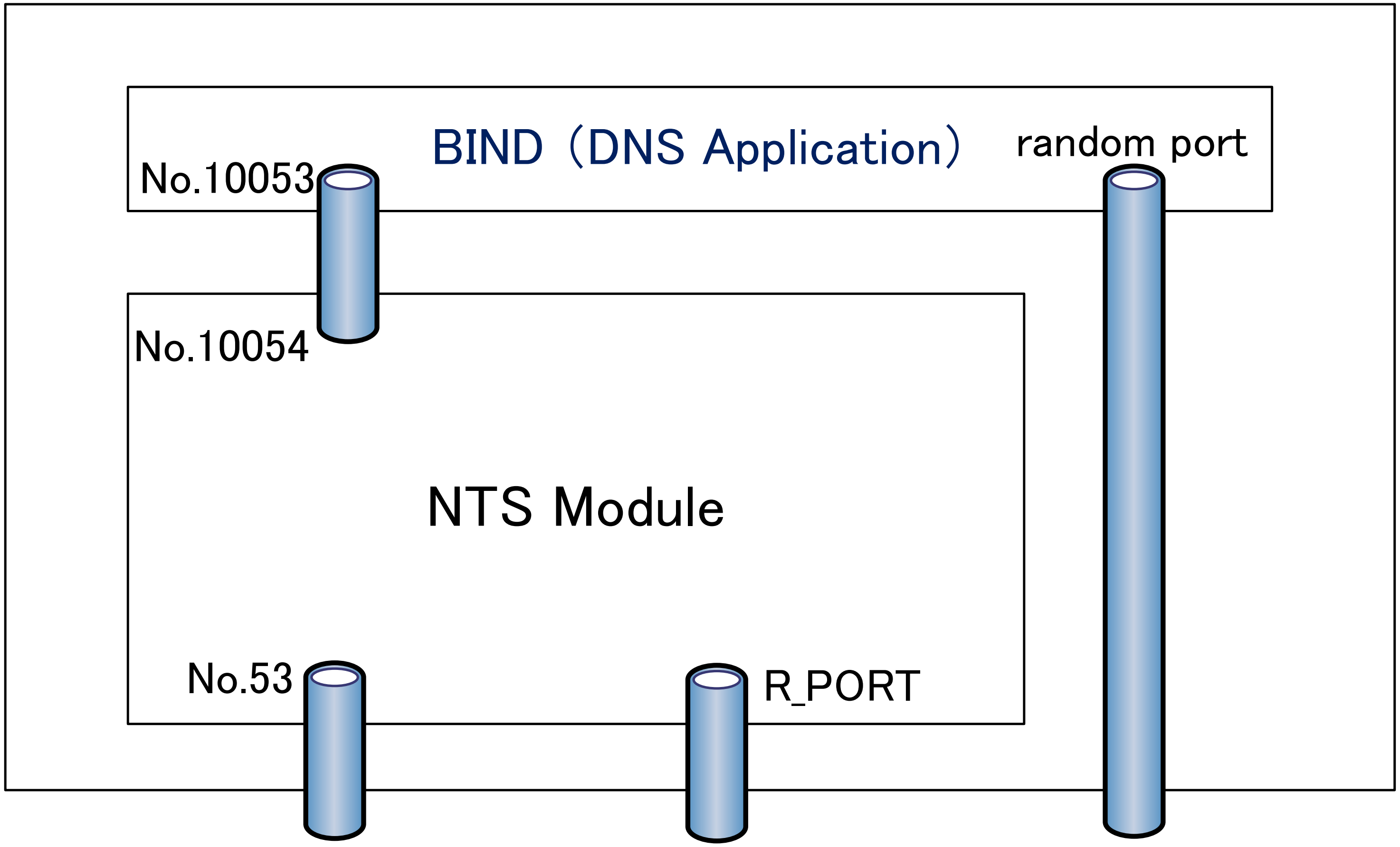


DNS-based NTS

SIP-based NTS

Implementation (NTS)

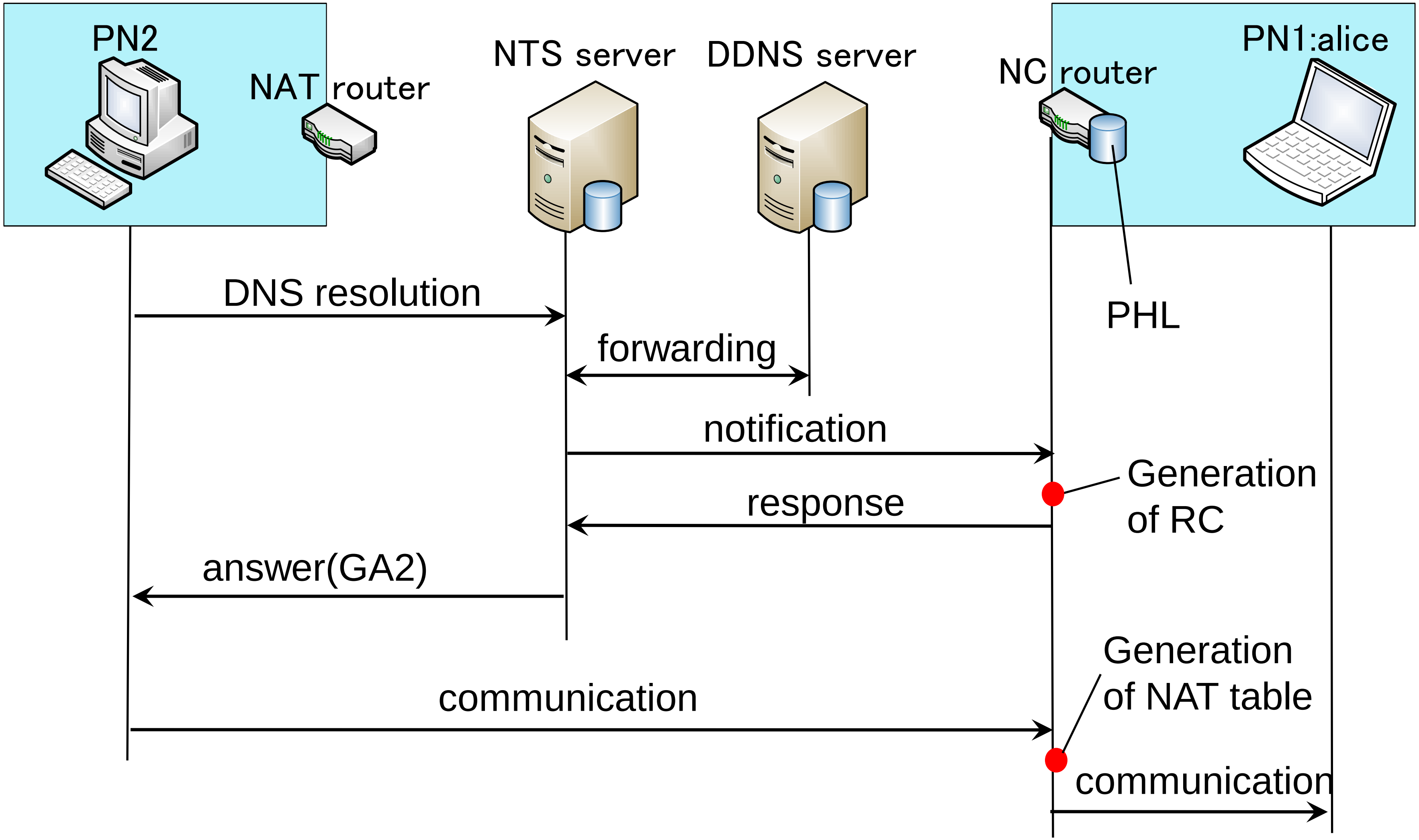
- The NTS module is implemented in the application layer



Future Works

- Collaboration with DLNA (Digital Living Network Alliance)
  - A user can discover and download the contents in home devices from the internet or other home networks
- Security Considerations
  - Advanced authentication
  - Distributed Denial-of-Service attack

Private-to-Private Communication



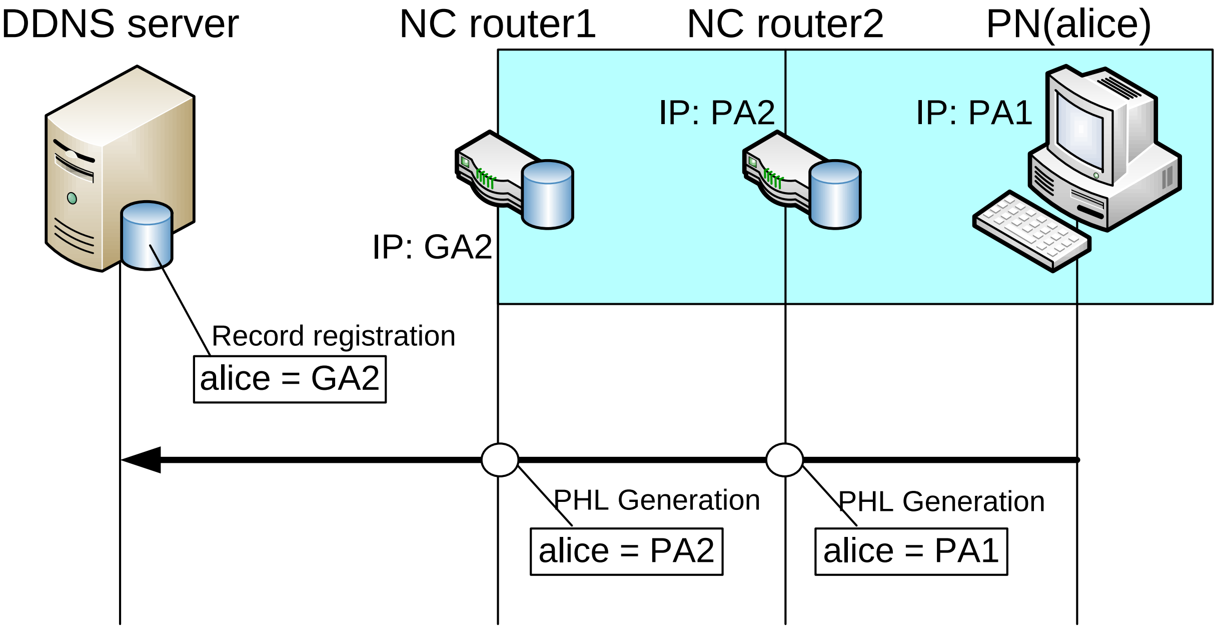
Simultaneous communication from multiple PNs in the same router

- When simultaneously accessed from the terminal which has the same global IP address to the different terminal in the same NAT, the NAT delays the response to one of the two's notice of communication.
- By the consideration, the NAT is not mistaken in the relation of PN and GN for every communication.

The Operations
# of the modified NAT router

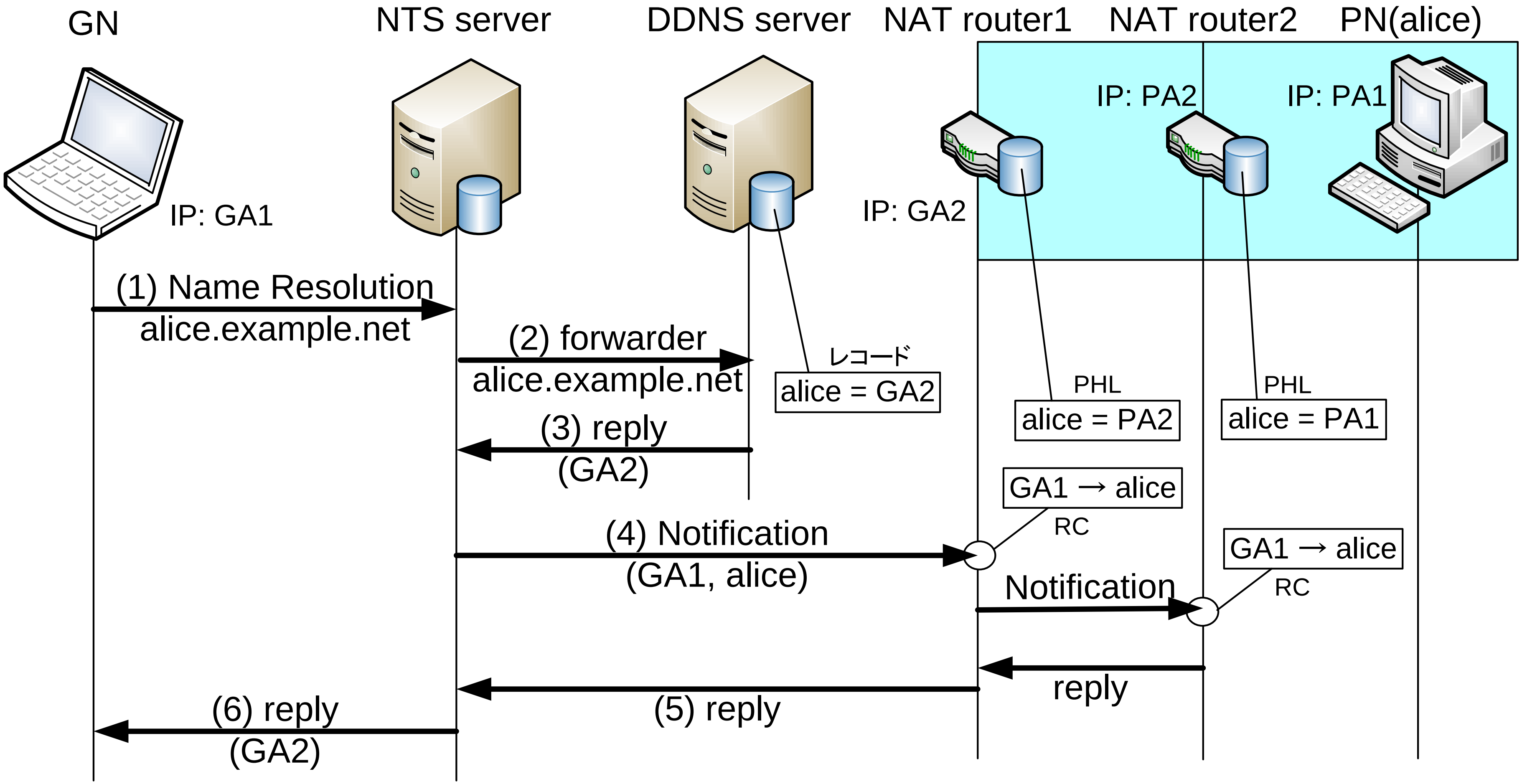
- When communication passes from the inside
  1. If it is a DNS registration packet, it evacuates and analyzes.
  2. the PHL is generated according to the contents of a packet.
  3. A registration packet is relayed.
- When communication is received from an outside
  1. If an NAT table corresponds, it will be natural NAT operation.
  2. If it is communication from a NTS server, cash of the contents is temporarily carried out to RC.
  3. If it is communication from others and corresponds with reference to RC and PHL, an NAT table will be generated and RC will be canceled.
  4. If it does not correspond, it is processing of a natural NAT router.

Double NAT (Name Registration)

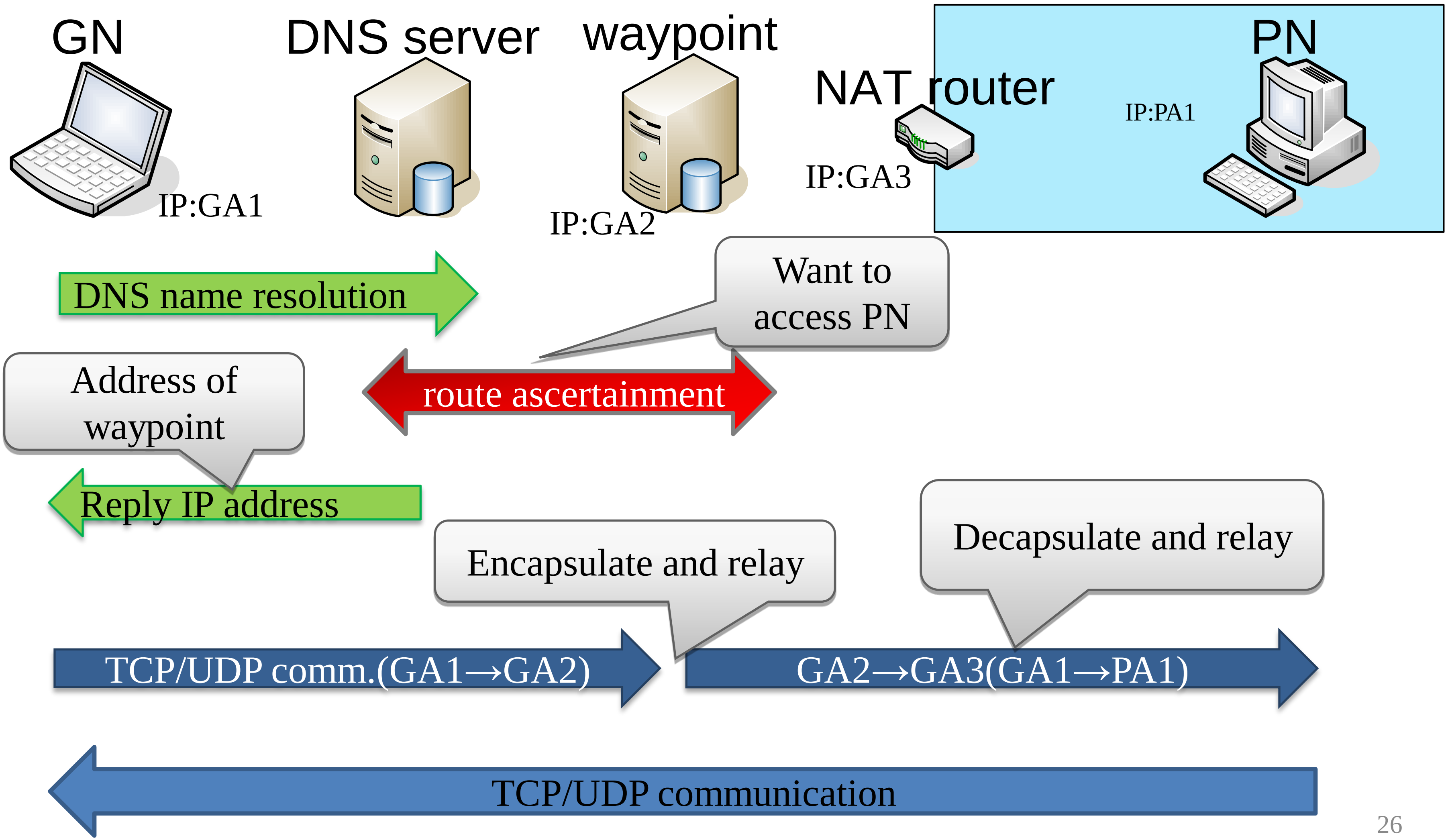


- The NAT router generates a PHL, when each name registration packet passes from the inside.
- After The NAT changes the source of the packet from the inside into an effective IP address on its outside, it is relayed.
- So, in NAT router1 and 2, the PHL of the address corresponding to each network is generated.

Double NAT (Name Resolution)



AVES (Address Virtualization Enabling Service)



GN

DNS server

waypoint

NAT router

PN

IP:GA1

IP:GA2

IP:GA3

IP:PA1

DNS name resolution

Want to access PN

Address of waypoint

route ascertainment

Reply IP address

Encapsulate and relay

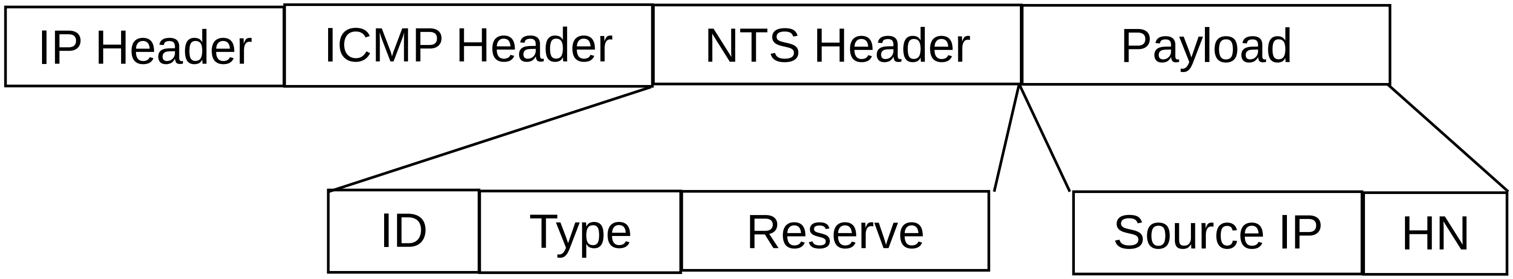
Decapsulate and relay

TCP/UDP comm.(GA1→GA2)

GA2→GA3(GA1→PA1)

TCP/UDP communication

The packet between a NTS server and a NAT router



IP Header | ICMP Header | NTS Header | Payload

ID | Type | Reserve

Source IP | HN

- IP header (20Bytes)
- ICMP header (24Bytes)
- NTS header (4Bytes)
  - Type : The portion the type of a packet judges a notice or a response (8bits)
  - ID : The portion which matches a name resolution and a response when the NTS receives a packet. It is corresponding with transaction ID which DNS uses at the time of a name resolution.
  - Reserve : (8bits)
- Payload (68Bytes)
  - Source IP : (32bits)
  - HN : Host Name (64Bytes)