IEEE TENCON 2008
Nov.17-21 ,2008
University of Hyderabad, India

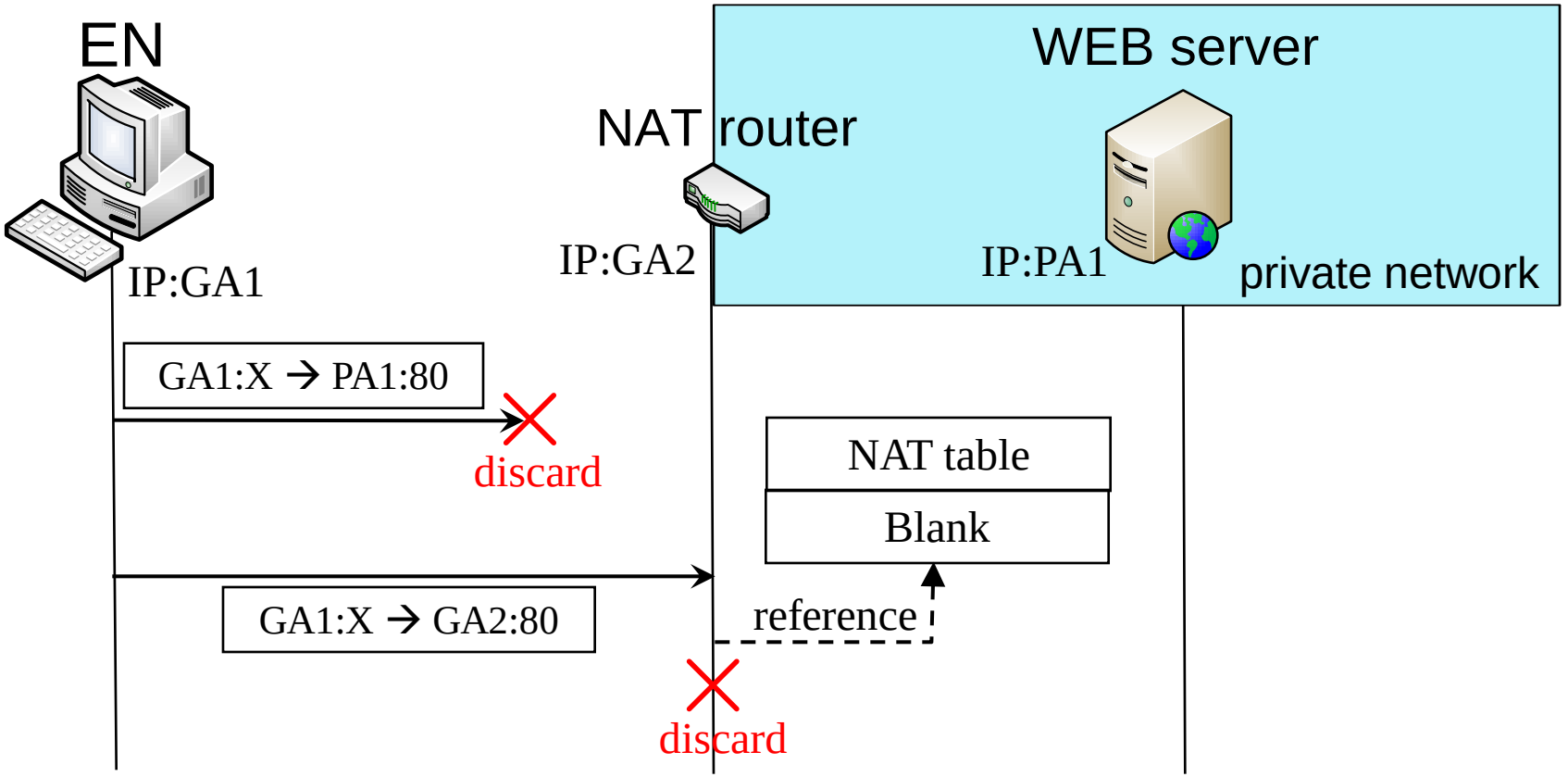
# Proposal of a NAT traversal system independent of user terminals and its implementation

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

# Backgrounds

- with the spread of the Internet.
  - there are increasing demands of accessing networks at anytime from anywhere .
- Global IP addresses are exhausted in the Internet.
- general home networks are usually constructed with private IP addresses.
  - NAT (Network Address Translator) is needed.

# NAT Operations (from outside to inside)




# A NAT Traversal Problem

# A Proposal for a NAT Traversal System

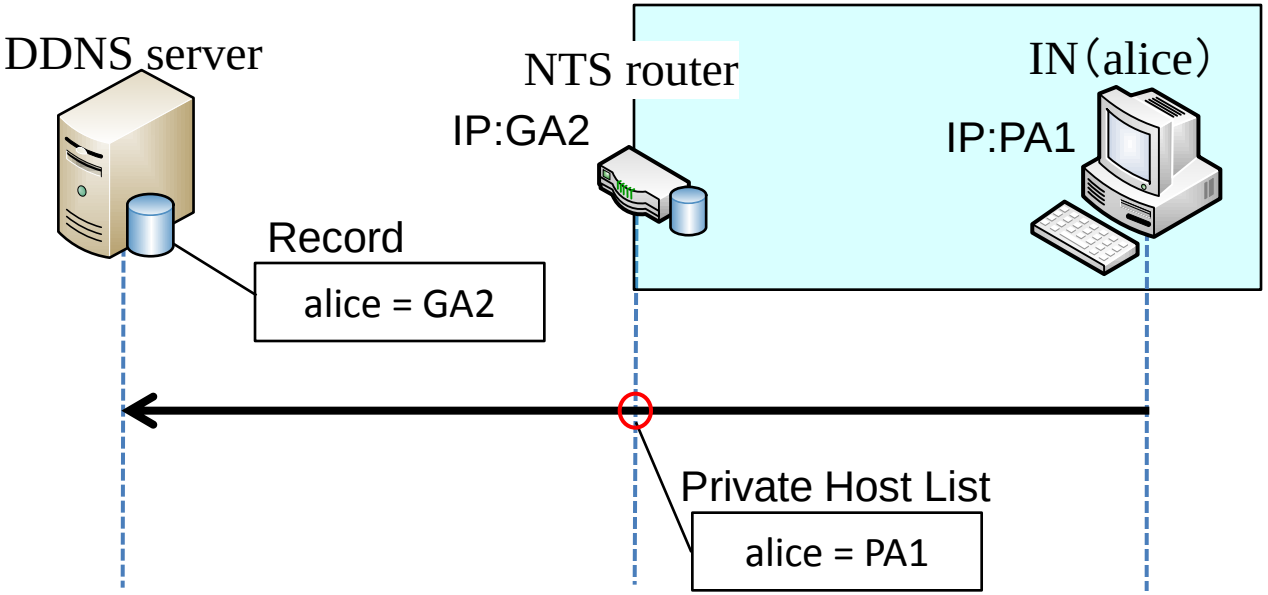
We have solved the problem without remodeling the end terminals.

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

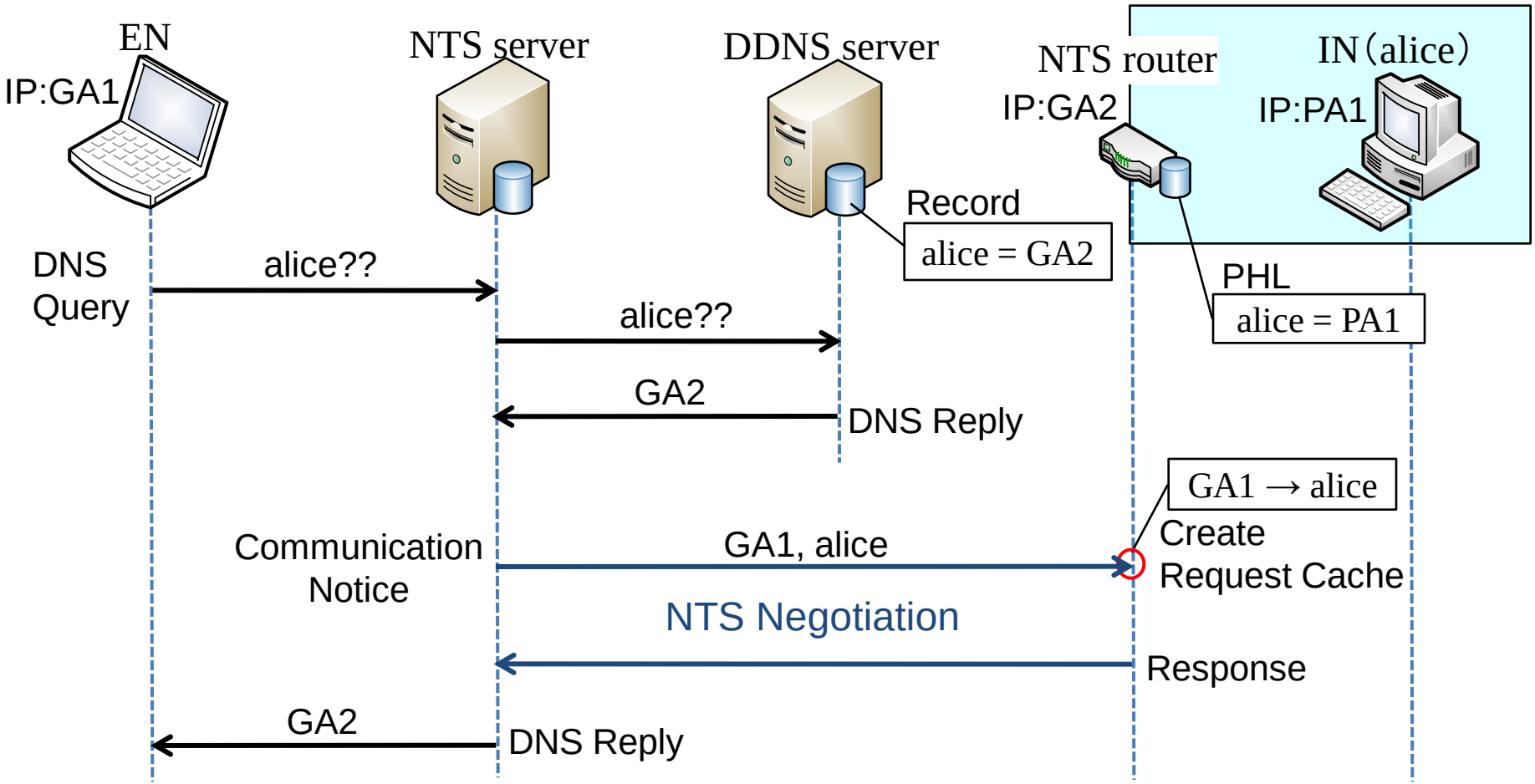
The modified DNS server → NAT-Traversal Support Server (NTS server)
The modified NAT router → NAT-Traversal Support Router (NTS router)

# Proposal System : Advanced Setting

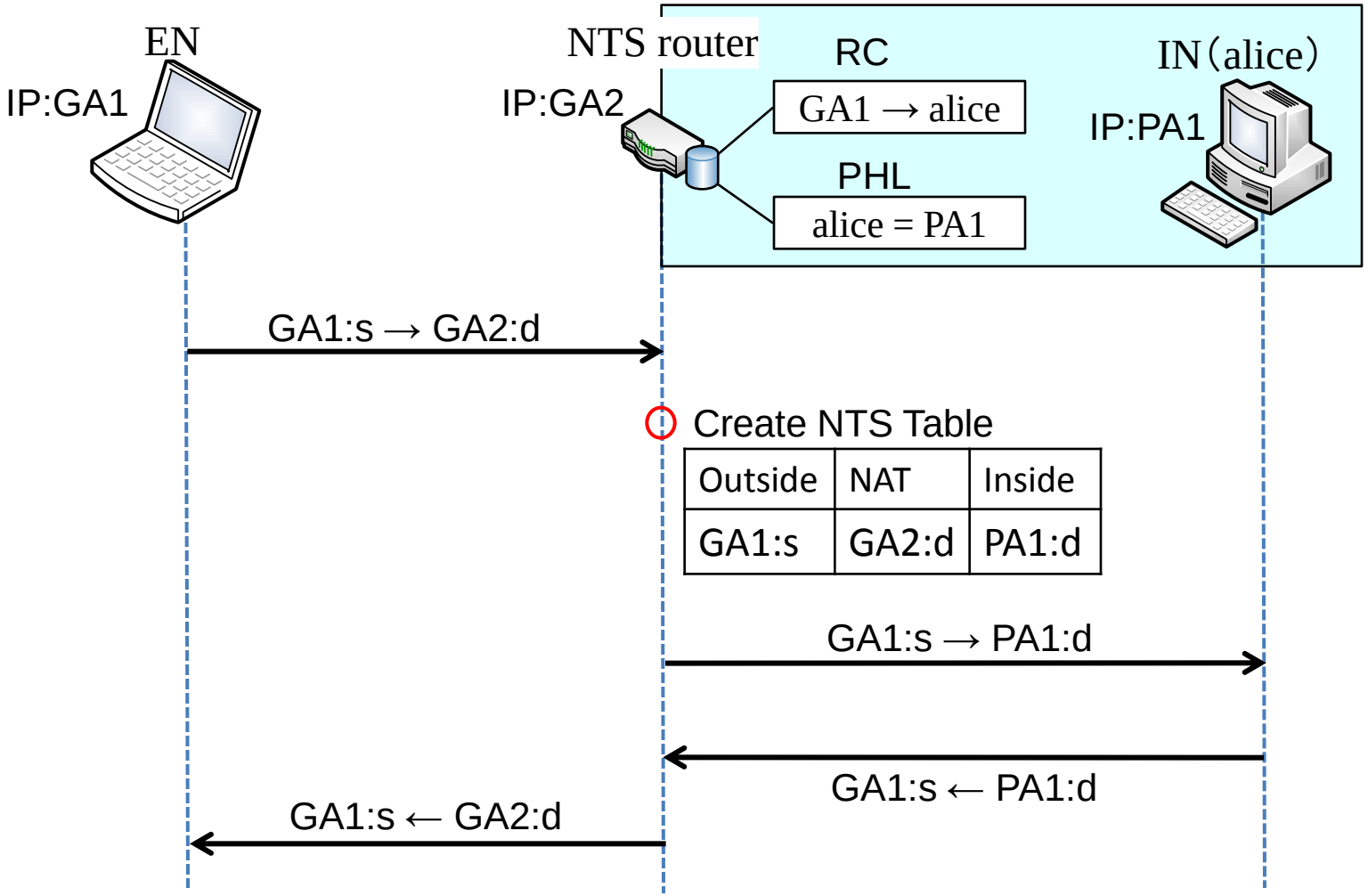
- User has to register “the IN’s name (FQDN)” and “The NAT router’s Global IP address” to a DDNS server in advance.
- The NTS router generates a Private Host List (PHL) at the time of the DDNS registration.



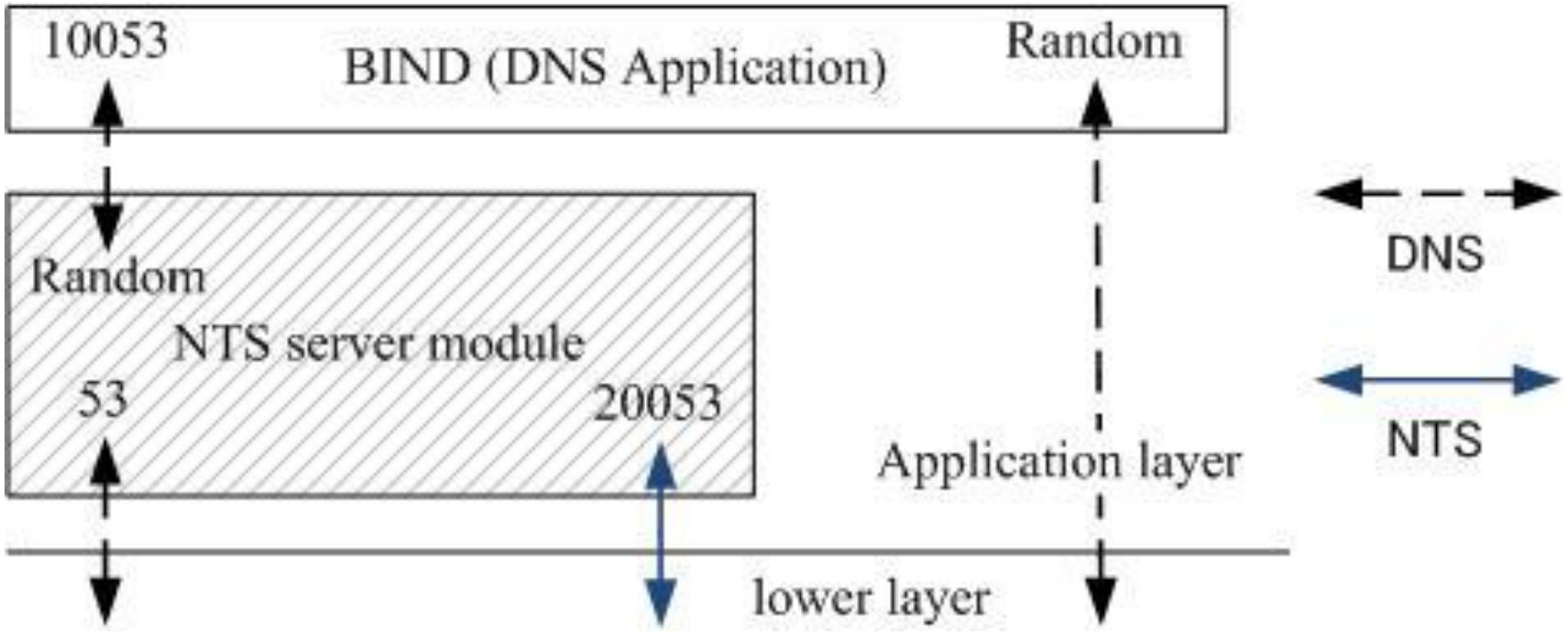
# Proposal System : Name Resolution



# Proposal System : Communication

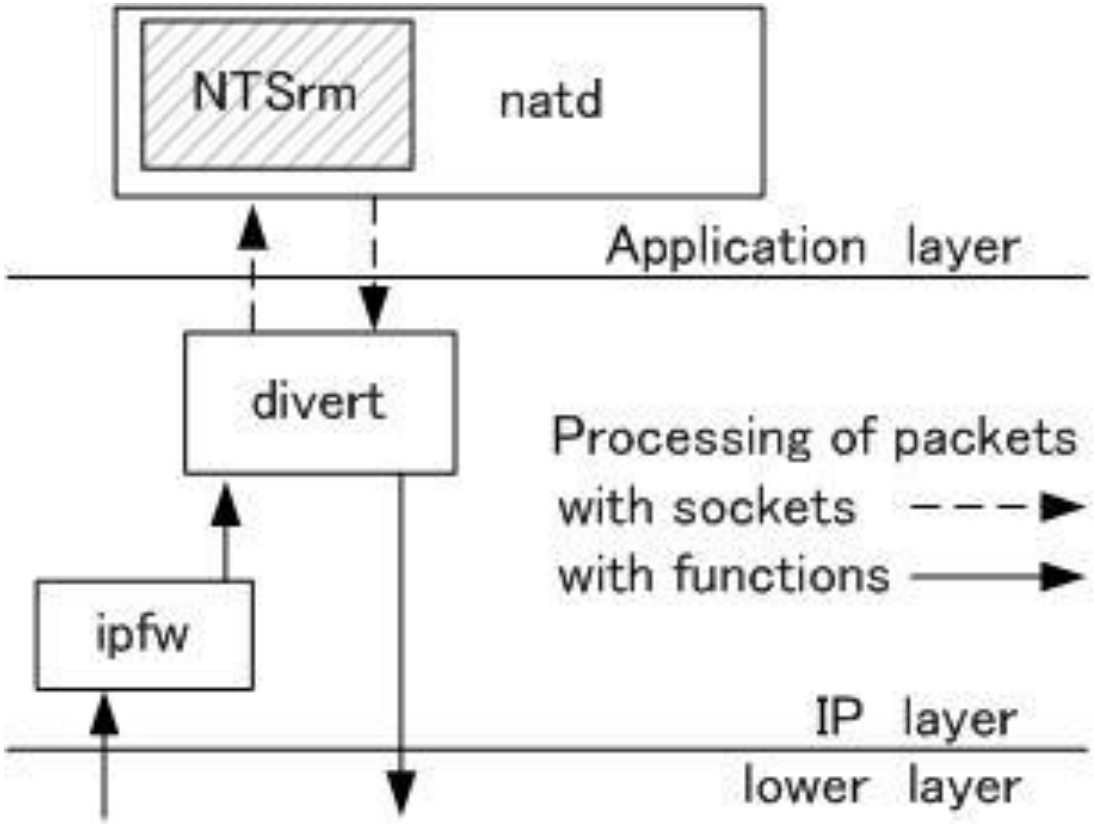


# Implementation : NTS Server



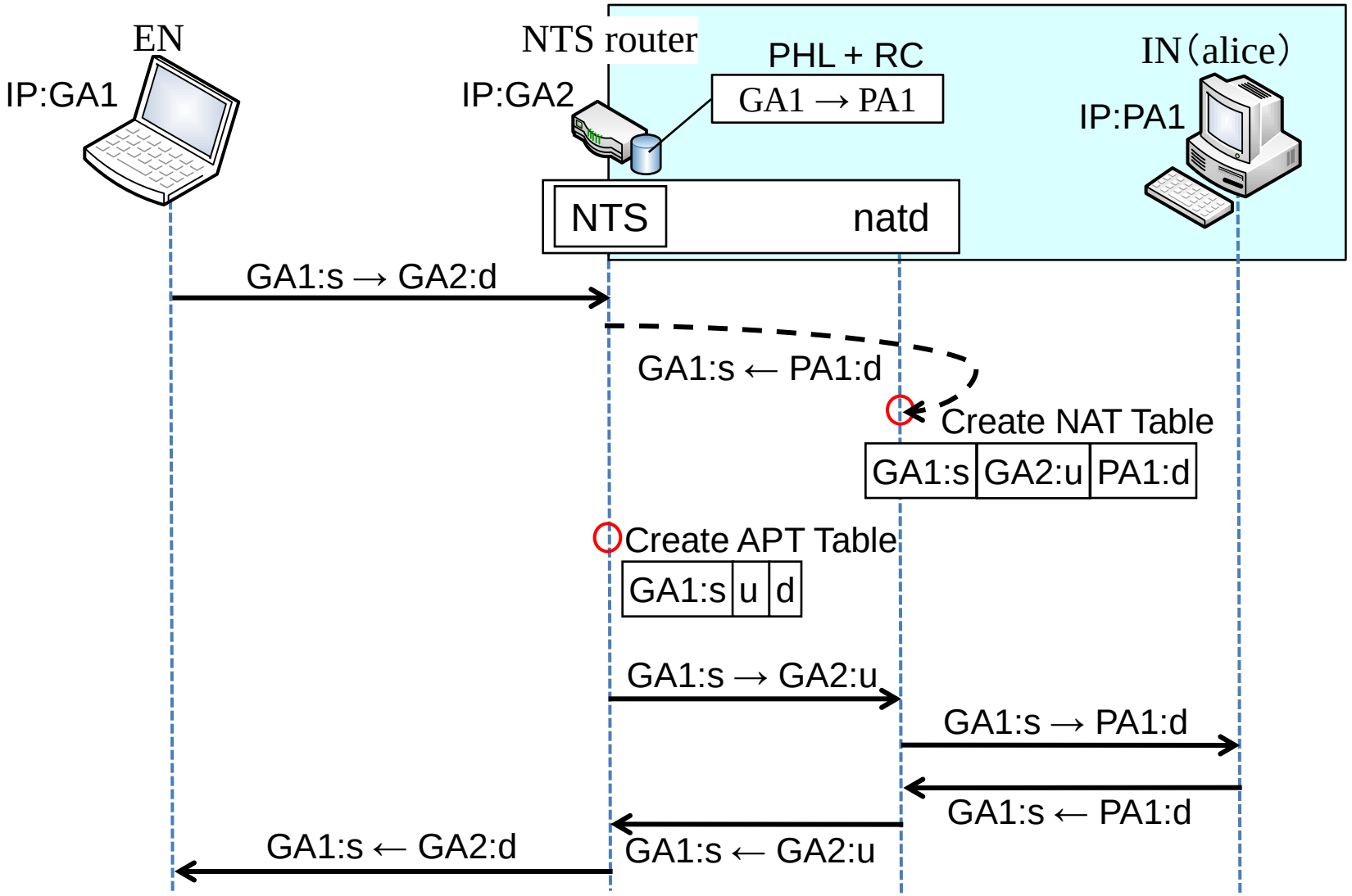

- DNS application listens to port 10053 and NTS server listens to port 53.

# Implementation : NTS Router




- add NTS router module in natd(NAT daemon)
  - natd has NAT functions in FreeBSD

# Proposal System: Generation Method of Original NAT Table



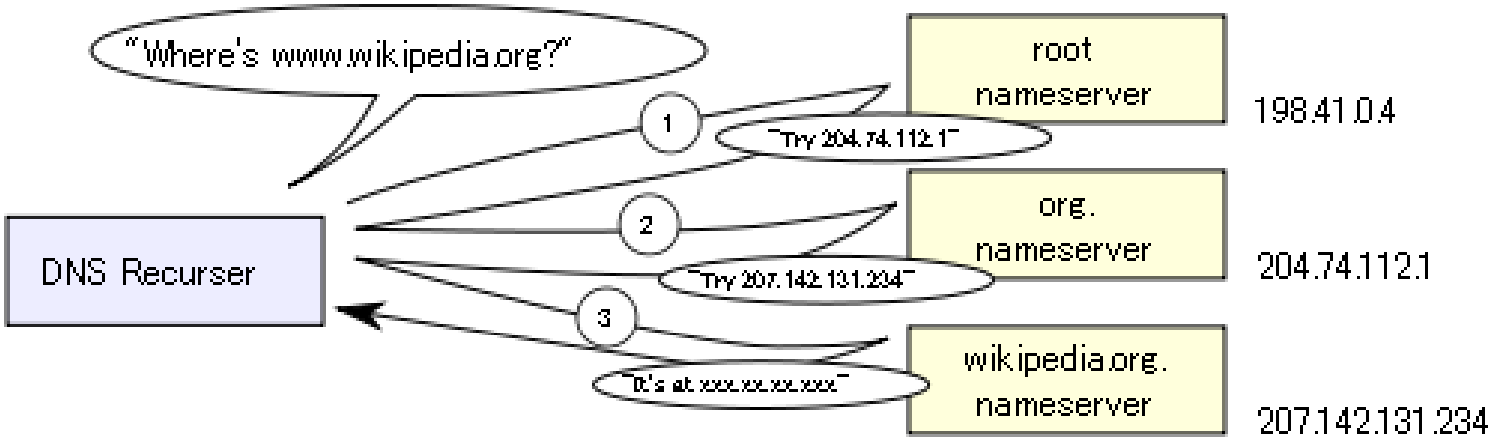
# Appendixes

# Conclusion

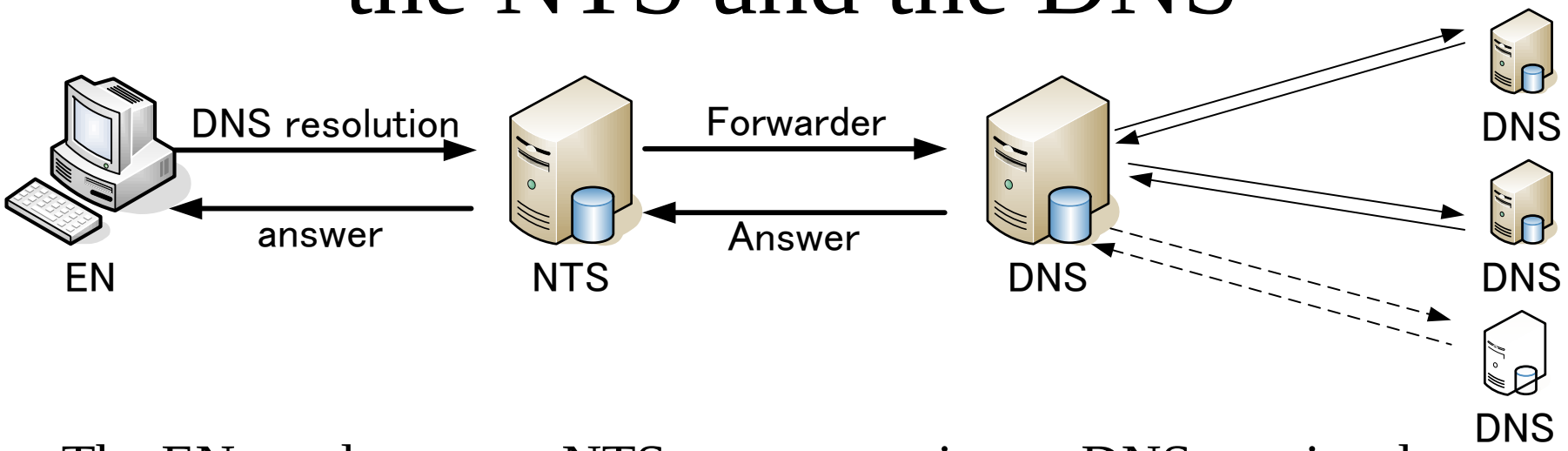
- The proposal system
  - It can solve the NAT Traversal Problem with the modified NAT router and the modified DNS server, NTS server, without modifying terminals.
  - The NAT router generates an original NAT table from PHL and RC made in the NAT router previously.
- Future
  - Evaluation of the proposal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

# 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

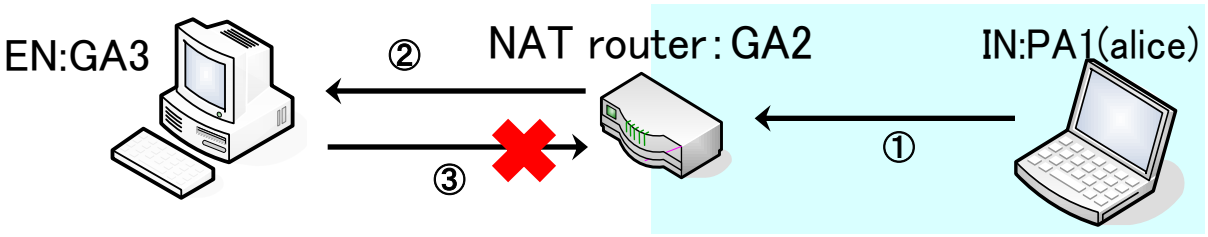


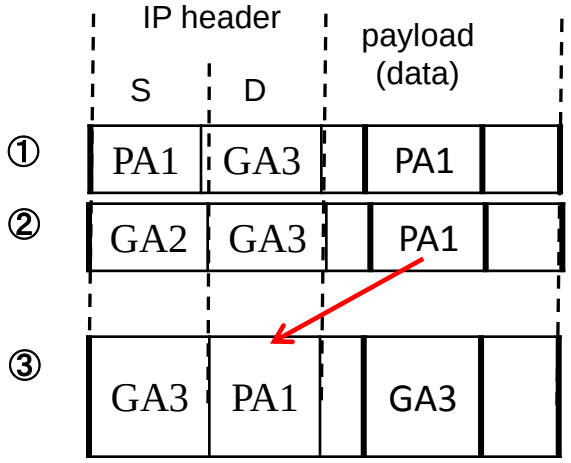

- The EN needs to set a NTS server as primary DNS previously.

  → The NTS server gets the IP address of the EN 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 EN can be realized, without changing a primary DNS.

# ALG (Application Layer Gateway)

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

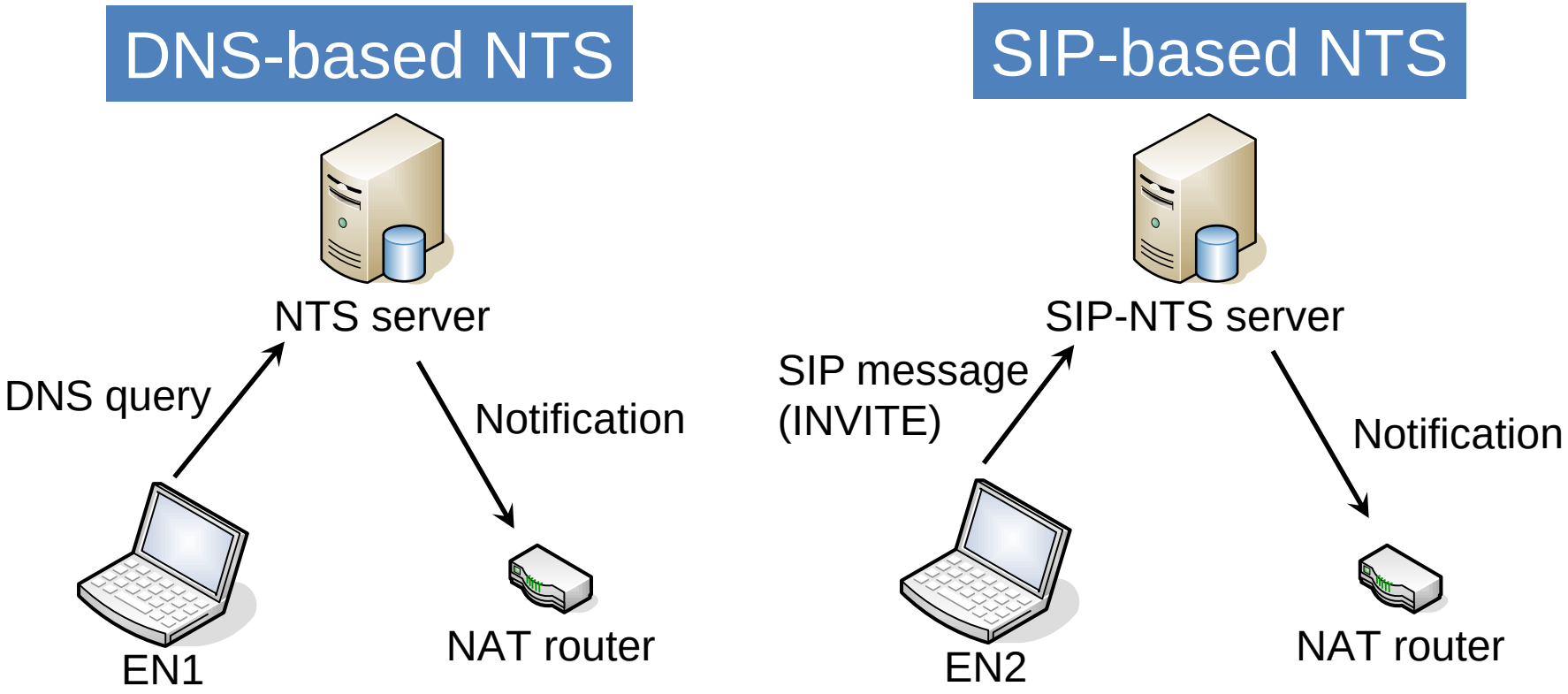



- Although the address indicated to IP/TCP / UDP header is rewritten in NAT, it does not involve in payload part.
- The IP address in application is also rewritten by ALG.

# Can you use SIP Applications ?

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



# Future Works

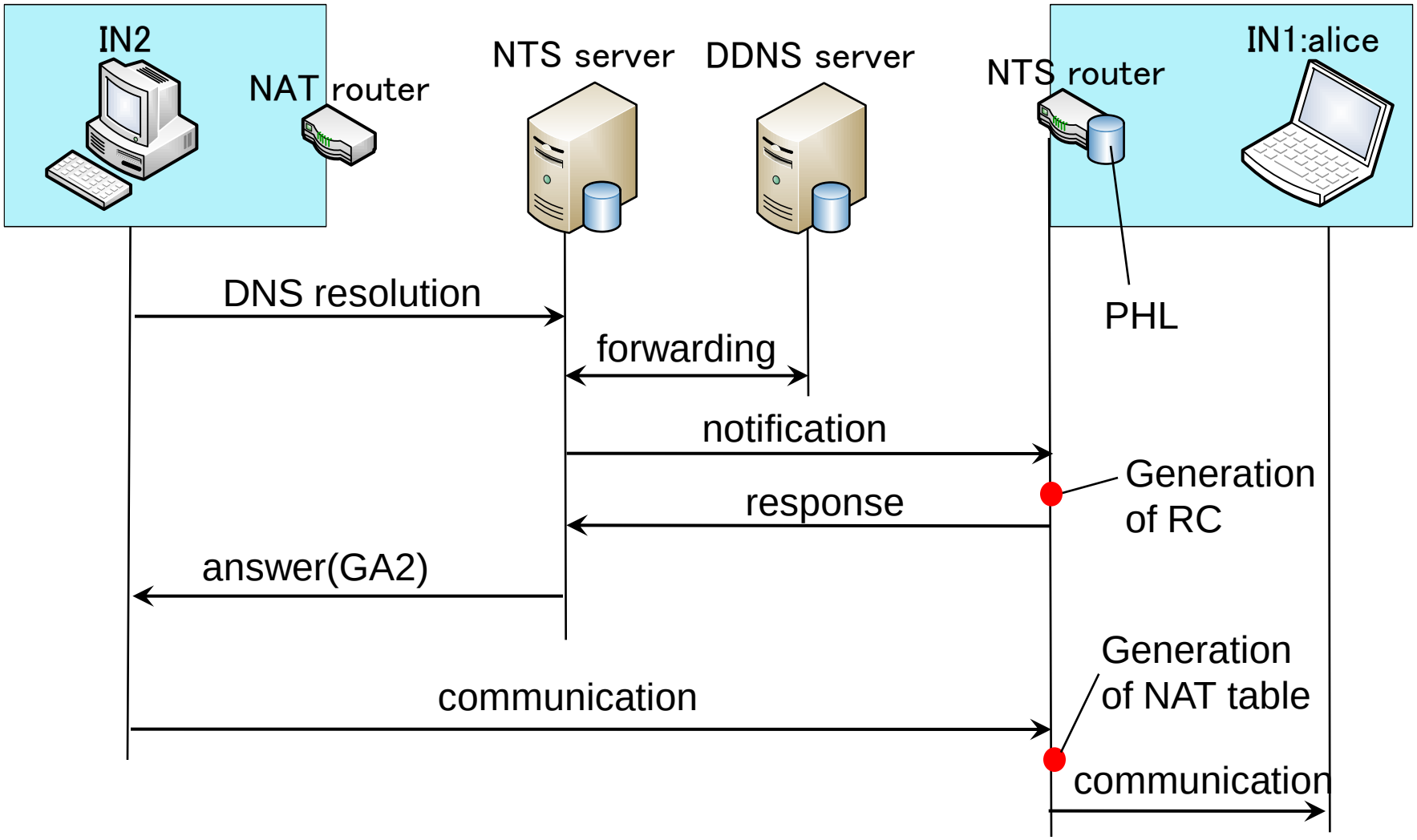
- Collaboration with DLNA

  (Digital Living Network Alliance)

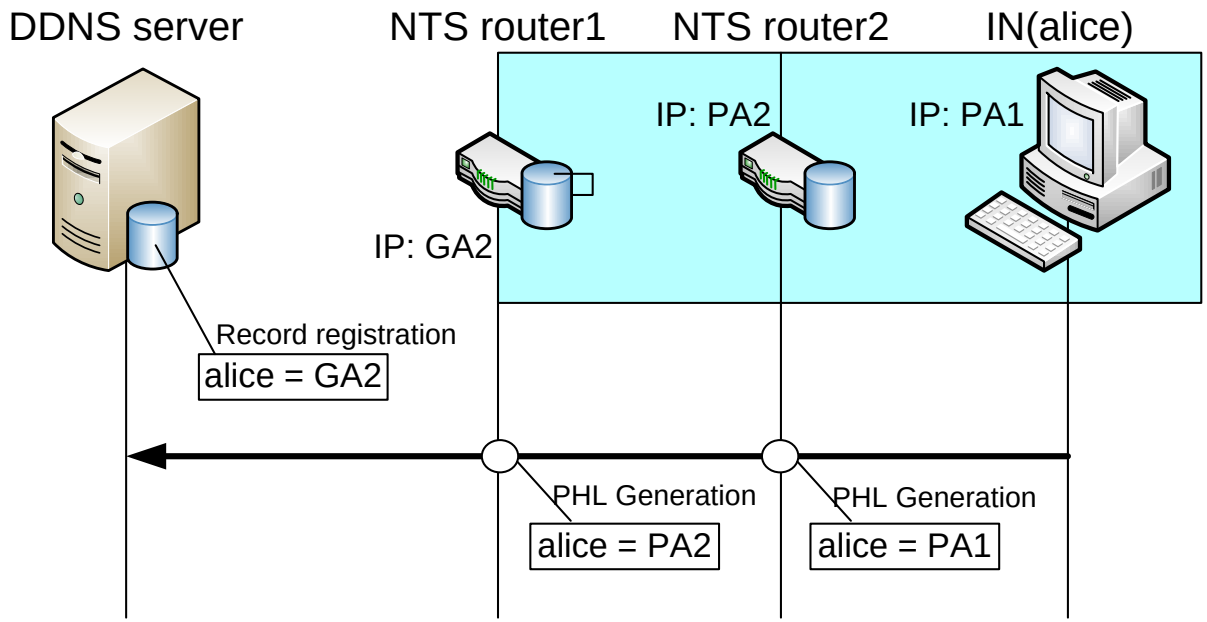
  - A user can discover and download the contents in home devices from the internet or other home networks

- Security Considerations
  - Advanced authentication
  - Distributed Denial-of-Service attack

# Private-to-Private Communication

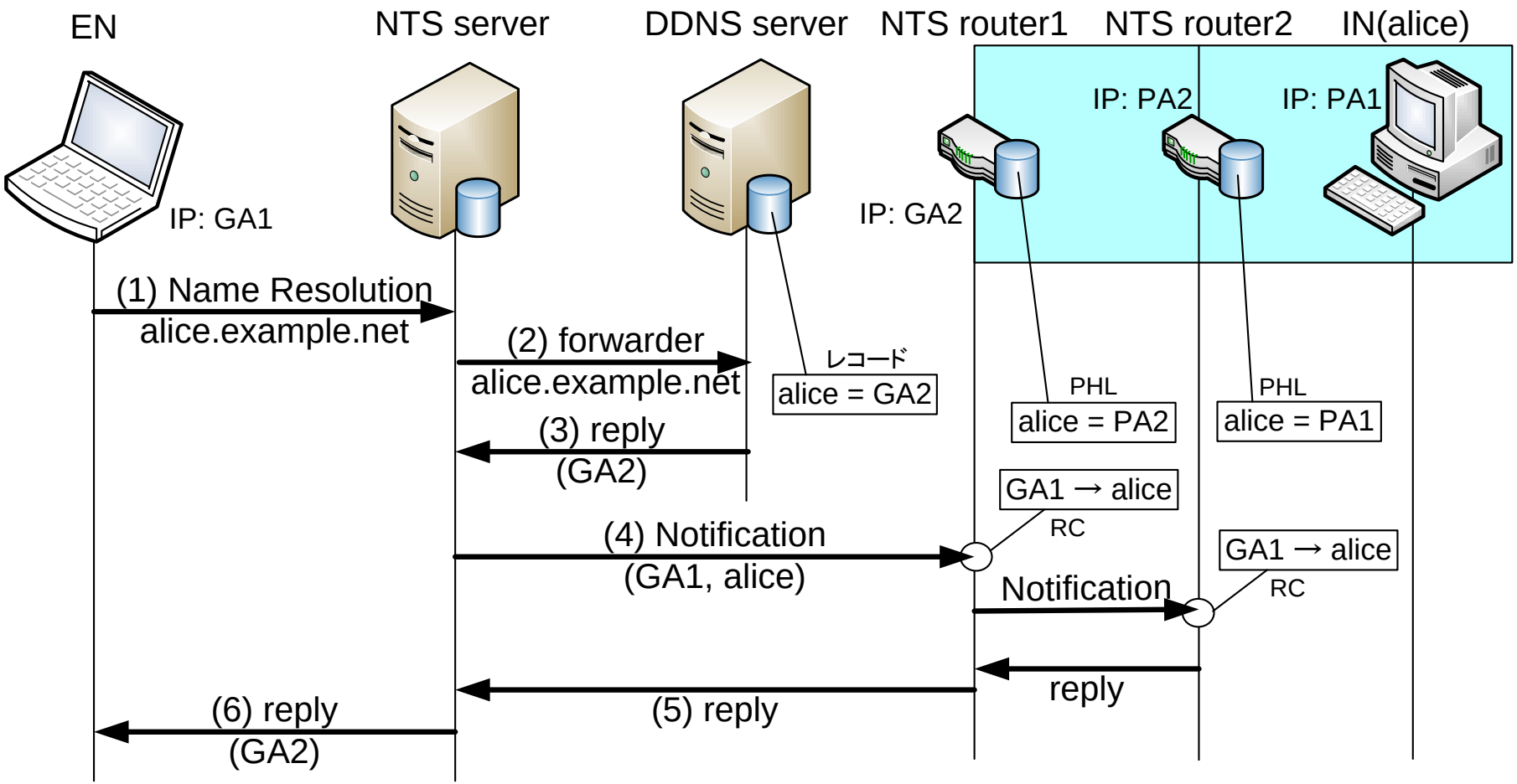


# Double NAT (Name Registration)

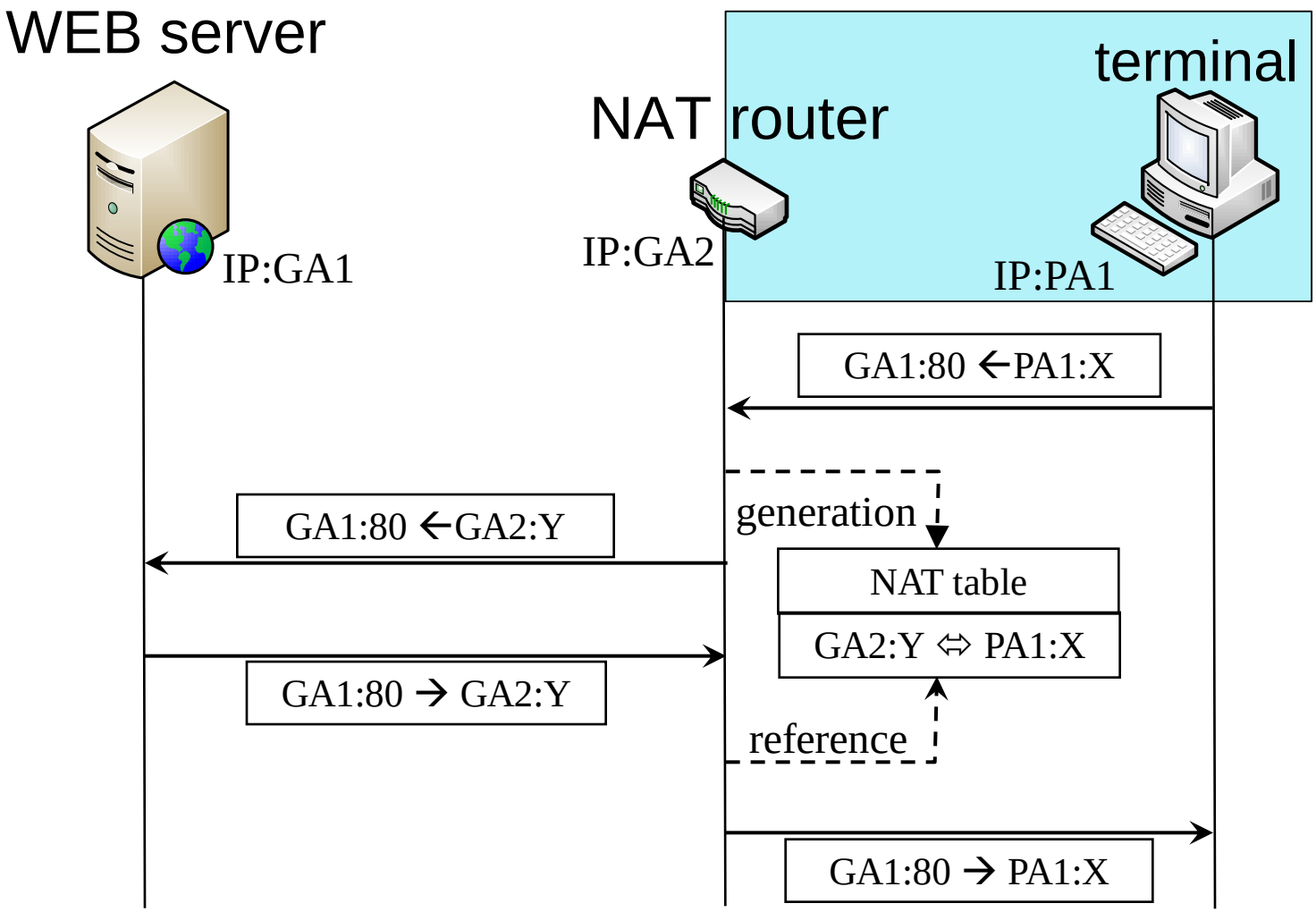



- The NTS router generates a PHL, when each name registration packet passes from the inside.
- After The NAT changes the source of the packet from the inside into an effective IP address on its outside, it is relayed.
- So, in NTS router1 and 2, the PHL of the address corresponding to each network is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

# Double NAT (Name Resolution)

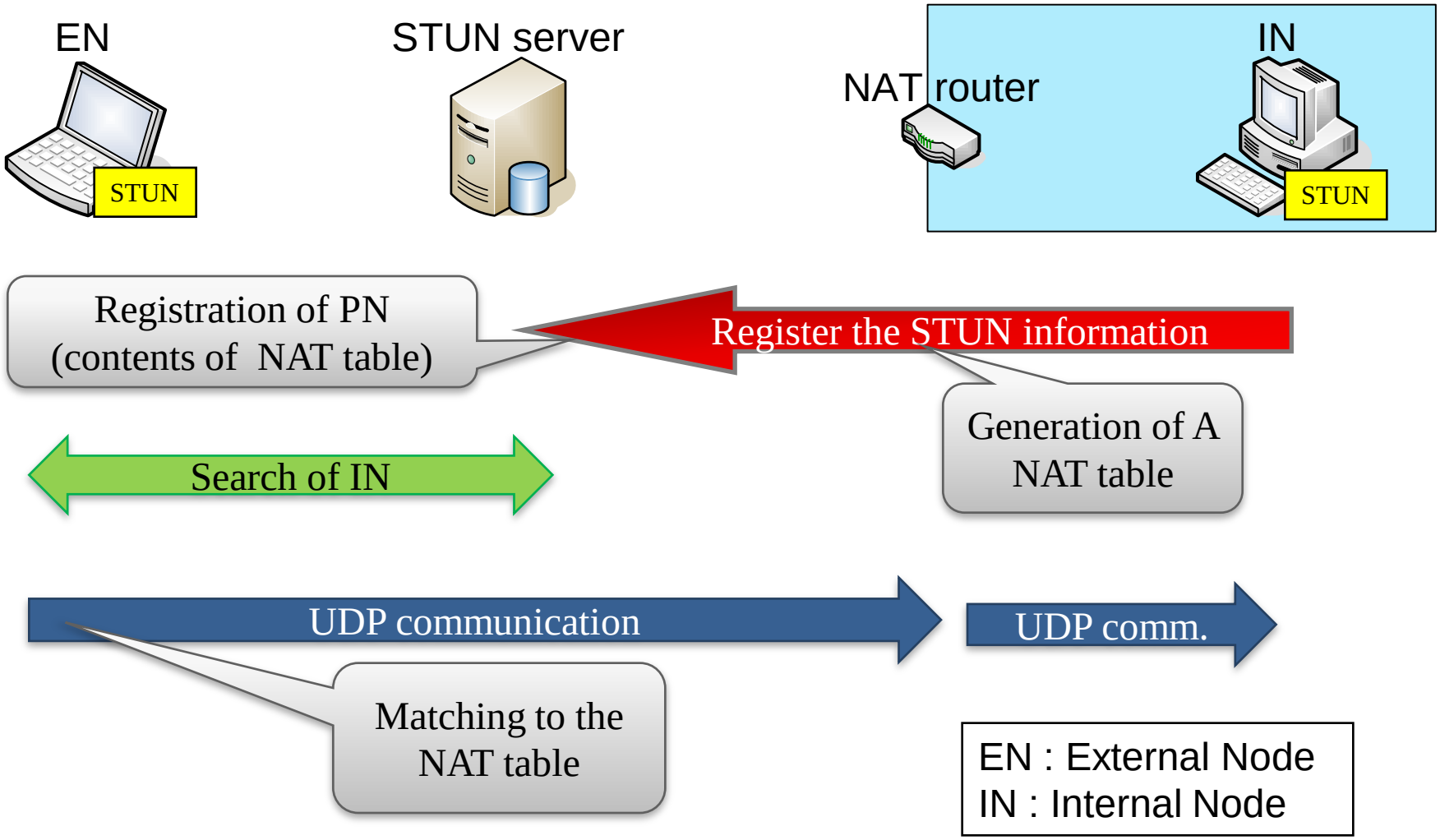


# NAT Operations (from inside to outside)

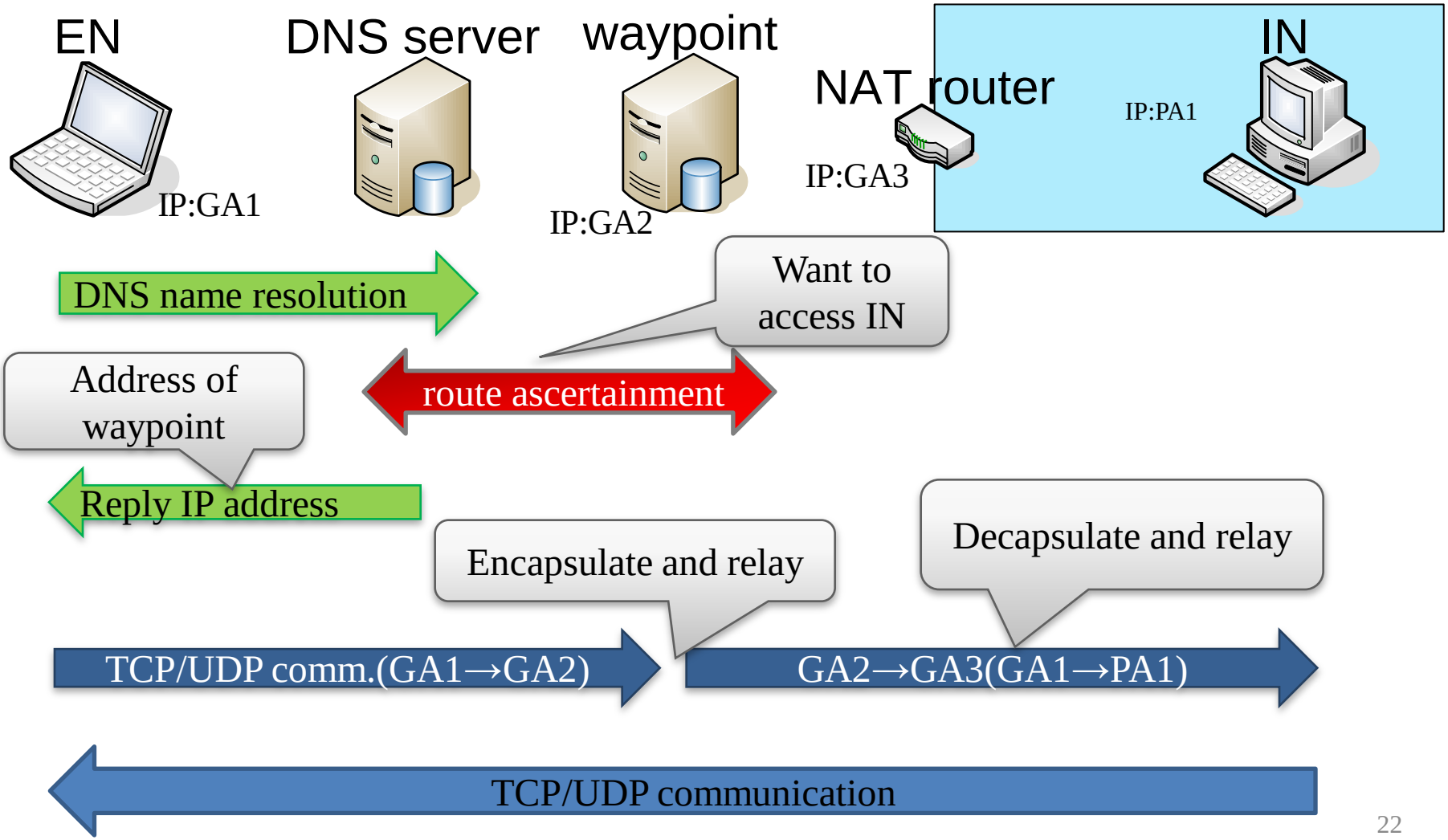


# STUN (Simple Traversal of UDP Through NATs)

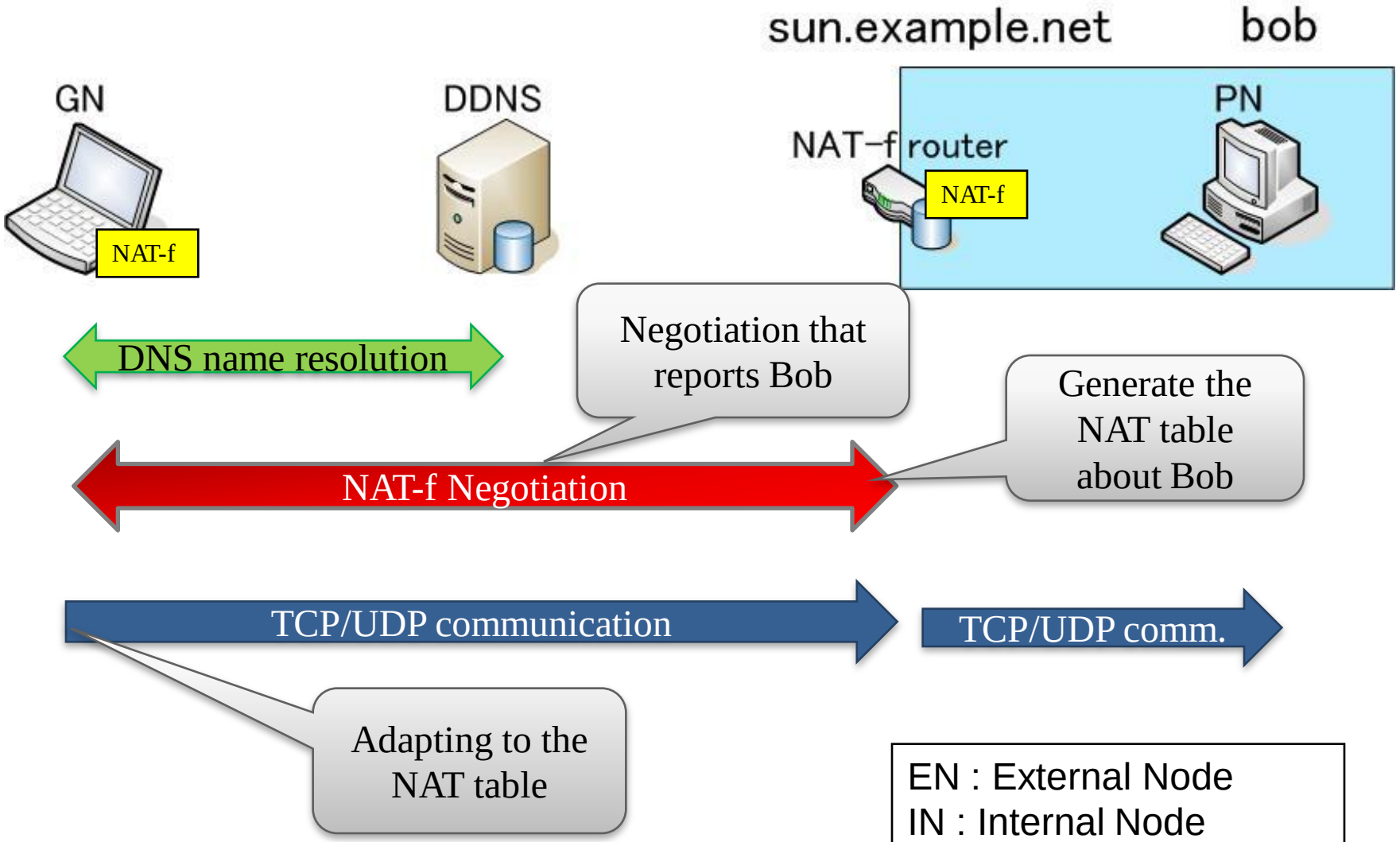
is defined in RFC 3489



# AVES (Address Virtualization Enabling Service)



# NAT-f (NAT-free protocol)



# Use scene

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