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

- **EN**
  - IP:GA1
  - DNS Query
  - NTS server
    - alice??
    - GA2
    - Communication Notice
    - GA2
    - DNS Reply
    - NTS Negotiation
    - GA1, alice
    - Request Cache
    - Response

- **IN**
  - IP:PA1
  - IN(alice)
  - PHL
    - alice = PA1
  - NTS router
    - IP:GA2
    - Record
      - alice = GA2
    - GA1 → alice
    - Create Request Cache
Proposal System: Communication

Create NTS Table

<table>
<thead>
<tr>
<th>Outside</th>
<th>NAT</th>
<th>Inside</th>
</tr>
</thead>
<tbody>
<tr>
<td>GA1:s</td>
<td>GA2:d</td>
<td>PA1:d</td>
</tr>
</tbody>
</table>

GA1:s → GA2:d

GA1:s ← GA2:d

GA1:s → PA1:d

GA1:s ← PA1:d
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

Create NAT Table

Create APT Table

GA1:s → GA2:d

GA1:s ← PA1:d

GA1:s ← PA1:d

GA1:s → PA1:d

GA1:s ← GA2:d

GA1:s ← GA2:d

GA1:s → GA2:u

GA1:s ← GA2:u

IP:GA1

IP:GA2

NTS

NTS router

PHL + RC

GA1 → PA1

IN(alice)

IP:PA1

EN

EN
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.
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:

  - DNS-based NTS
  - SIP-based NTS

**Diagram:**

- DNS query from EN1 to NTS server
- Notification from NTS server to NAT router
- SIP message (INVITE) from EN2 to SIP-NTS server
- Notification from SIP-NTS server to NAT router
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

- DNS resolution
- forward
- notification
- response
- Generation of RC
- Generation of NAT table

Communication

Devices:
- IN2
- NAT router
- NTS server
- DDNS server
- IN1: alice
- PHL
- NTS router
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 router 1 and 2, the PHL of the address corresponding to each network is generated.
Double NAT (Name Resolution)

(1) Name Resolution
alice.example.net

(2) forwarder
alice.example.net
alice = GA2

(3) reply
(GA2)

(4) Notification
(GA1, alice)

(5) reply

(6) reply
(GA2)

NTS server
DDNS server
NTS router1
NTS router2
IN(alice)

IP: GA1
IP: GA2
IP: PA1
IP: PA2

Notification
alice = PA2
alice = PA1

reply

NAT Operations (from inside to outside)

WEB server

IP:GA1

NAT router

IP:GA2

terminal

IP:PA1

GA1:80  PA1:X

GA1:80  PA1:X

NAT table

GA2:Y  PA1:X

GA1:80  GA2:Y

GA1:80  GA2:Y

GA1:80  PA1:X

GA2:Y  PA1:X

reference

generation
STUN (Simple Traversal of UDP Through NATs) is defined in RFC 3489

STUN

EN

STUN server

IN

NAT router

UDP communication

Registration of PN (contents of NAT table)

Search of IN

Register the STUN information

Generation of A NAT table

Matching to the NAT table

EN : External Node
IN : Internal Node
AVES (Address Virtualization Enabling Service)

- EN (Address of waypoint)
- DNS server (Encapsulate and relay)
- Waypoint (Routing)
- NAT router (Decapsulate and relay)
- IN (Reply IP address)

Flow:
1. DNS name resolution
2. Route ascertainment
3. Want to access IN
4. TCP/UDP communication (GA1→GA2)
5. GA2→GA3 (GA1→PA1)
6. TCP/UDP communication
NAT-f (NAT-free protocol)

- **DNS name resolution**
  - Negotiation that reports Bob
  - Generate the NAT table about Bob

- **TCP/UDP communication**
  - Adapting to the NAT table
  - EN : External Node
  - IN : Internal Node
  - DDNS : Dynamic DNS

- **NAT-f Negotiation**
- **NAT-f router**

- **GN**, **DDNS**, **PN**
Use scene

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