

Researches on Extended Dynamic Process Resolution Protocol that Can Traverse NAT

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

Abstract—As the security measures against threats such as illegal access, etc. it is useful to define and from communication groups in order to make communications secure. IPsec is not appropriate in the case where system configurations frequently change like intranets, because the management loads on the network manager is quite large. To solve this problem, we have been proposing Dynamic Process Resolution Protocol (DPRP), by which devices in the network learn changes in system configurations automatically, and maintain communication groups. However, the conventional DPRP is not applicable when a Network Address Translator (NAT) exists on the way of the communication path. In this paper, we have studied the Extended DPRP that can traverse NAT.

I. INTRODUCTION

In recent years, security measures against threats, such as unauthorized access, eavesdropping, and falsification, have been an important subject in the enterprise network. For the threats from the outside of companies, high level security systems are utilized, such as cipher communications and digital signature, in conjunction with a firewall (FW) and an Intrusion Detection System (IDS). However, security threats against the enterprise network also exist in intranets, and inside crimes by employees have been constantly reported in [1]. At present, a very simple authentication method using user name and passwords is being used as the security measures in intranets and it is seriously considered that more effective measures should be adopted.

In order to cope with such a situation, an effective way is to form communication groups. IPsec [2] is a typical network security technique that can form communication groups. IPsec dynamically generates parameters required for cipher communications and authentication in advance of every communication, and accordingly, secure communication is executed. However, in IPsec, the transport mode used for host-to-host communications, and the tunnel mode used for network-to-network communication is not compatible. Therefore, it is difficult to use IPsec in intranets where the communication groups of secure domains and those of individual terminals coexist. To solve this problem, we have been proposing a network architecture called GSCIP (Grouping for secure Communication for IP) [3] that can realize a secure network and at the same time reduce management load. Dynamic Process Resolution Protocol (DPRP) [4] is one of the most important protocols with which the devices which form communication groups learn changes in system configurations, and generate process information automatically. DPRP is executed in advance of communications, and the definitions of communication groups are maintained

even if the system configurations change. However, the present DPRP does not support the environment where NAT [5] exists on the communication paths. In this paper, we have studied Extended-DPRP that can traverse the NAT. With this system, definitions of communication groups extending from the global address area to the private address area become possible. The term “NAT” in this paper includes the Network Address Port Translator (NAPT) [6] that translate TCP/UDP port numbers in addition to the IP addresses.

The outline of GSCIP is shown in Section II, and DPRP is described in Section III. We present the Extended DPRP in Section IV, and describe its implementation in Section V. Finally, our conclusion is stated in Section VI.

II. THE OUTLINE OF GSCIP

GSCIP is a network architecture that can realize secure and yet flexible networks, where communication groups of secure domains and those of individual terminals coexist. Communications within the same group are encrypted. It is possible to refuse access from terminals belonging to other groups. Even when a host moves around, for example, between inside and outside the sub-network, the relationships of the communication group are maintained. In GSCIP, because the devices which form communication groups generate process information tables automatically, management load on network managers is quite small.

Fig. 1 shows the method to define communication groups. Devices which form communication groups are called GEs (GSCIP Elements). GES (GE realized by Software) is a software type GE installed in a terminal, GEN (GE for Network) is a router type GE which protects general terminals (Terms) in a sub-network under the GEN. In GSCIP, communication groups are defined by the GEs which have the same common key, “GK” (Group Key). Communications among the GEs are encrypted with the GK. In GSCIP, communication groups are independent of IP addresses because communication groups are defined with the GKs. Individual-based and domain-based communication groups can coexist, and communication groups belonging to plural groups can be defined easily. When a GE is powered on, the number of communication group together with its GK is delivered by the GSCIP Management Server (GMS). A sure authentication and encryption using public keys are executed between the GMS and the GEs. Group keys are periodically updated by the GMS.

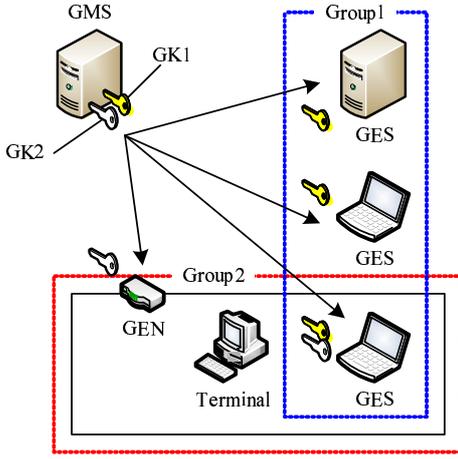


Fig. 1. Method to define communication groups.

A GE handles packets according to the Process Information Table (PIT) in the GE. In the PIT, IP address and port number of source/destination terminal, protocol number, process information (encrypt/decrypt, relay, discard), and group number are described. A Connection Identification (CID), a set of IP addresses and port numbers of source/destination terminals, and a protocol number are used for searching PITs. If no corresponding PIT is found, DPRP is executed to generate a new PIT.

III. DYNAMIC PROCESS RESOLUTION PROTOCOL

DPRP is one of the most important protocols in GSCIP. In advance of the communication between terminals, all GEs on the communication path mutually exchange their information set by the GMS, and generate a PIT in each GE. DPRP negotiation is shown in Fig. 2. When GES1 is to send a TCP/UDP packet, it searches its own PIT. If a corresponding PIT exists, a packet is processed according to the PIT. If PIT does not exist, GES1 stores the triggered packet, and starts DPRP negotiation in order to make a PIT. DPRP negotiation consists of two-way control packets based on ICMP. Detect Destination End GE (DDE) detects the GE nearest to the communication partner, and it is GES2 in case of Fig. 2. Report GE Information (RGI) collects the information of GEs on the communication path set by the GMS, including group numbers of GEs. DDE and RGI carry the CID of the triggered packet that starts the DPRP negotiation. GES1 which receives RGI checks whether it can communicate with the partner or not. If they can communicate, GES1 determines the process information of each GE. Make Process Information Table (MPIT) notifies each GE of the determined process information. Complete DPRP Negotiation (CDN) notifies each GE of the completion of the DPRP negotiation. Then, the source GE restores the triggered packet, and sends it to GES2 according to the process information in the PIT. The contents of the generated process information are, encrypt/decrypt in GES1 and GES2, and relay transparently in GEN in Fig. 2.

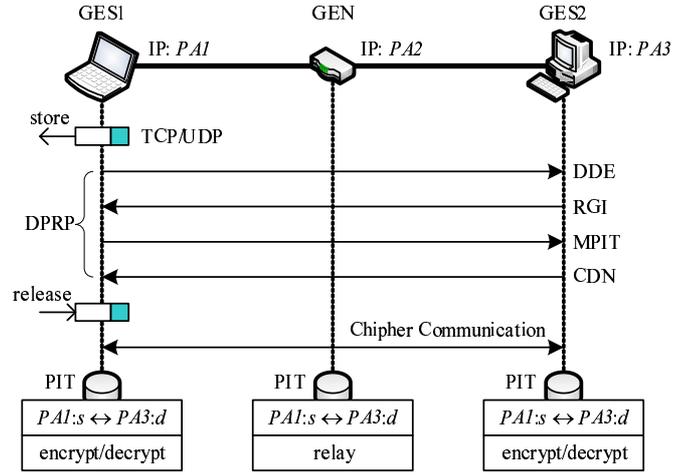


Fig. 2. DPRP negotiation.

The above mentioned DPRP is effective in the case where all terminals exist in a global address area or in a private address area. In the environment where a NAT exists on the communication path, it becomes useless because the IP addresses of packets are changed in the NAT. To solve the problem, it is necessary to study two cases; i.e., one case is that the communication starts from the private address (PA) area, and the other case is that the communication starts from the global address (GA) area. The former case is already studied in [7]. In this paper, we have studied the latter case in detail. For this study, it is necessary to solve the NAT traversal problem. The problem is that, terminals in the GA area cannot start communications with terminals in the PA area because the terminals in the GA area cannot see the network behind the NAT. In order to solve the problem, we have extended the function of DPRP by using a technique of NAT-free (NAT-f) [8] that is our proposed protocol for realizing NAT traversal communications, like ICE [9], UPnP [10], and AVES [11], etc.

IV. PROPOSED METHOD

A. Extended DPRP

A system configuration together with initial information of Extended DPRP is shown in Fig. 3. GES1 is in the GA area and GES2 is in the PA area. The GEN to which the NAT function is added is called GNAT. The host name of the GES2 *bob*, in the PA area, and the IP address of the GNAT are registered in a Dynamic DNS (DDNS) server [12]. Also, the name of GES2 *bob*, the private IP address of GES2 *PA1*, and the property of access control whether it can be accessed from the outside or not, have to be registered in an Access Control Table (ACT) in GNAT.

When GES1 starts a communication with GES2, it sends a name query to the DDNS server with FQDN of GES2. The DDNS server replies the IP address of GNAT, *GA2*. When GES1 receives the reply packet, it gets the IP address of GNAT, and the host name *bob*, in the kernel. Also, it changes the IP address of GNAT *GA2* to a certain virtual IP address *VA1*,

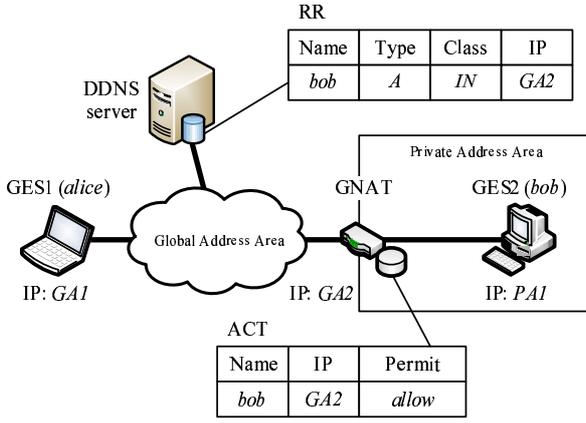


Fig. 3. System configuration and initial information.

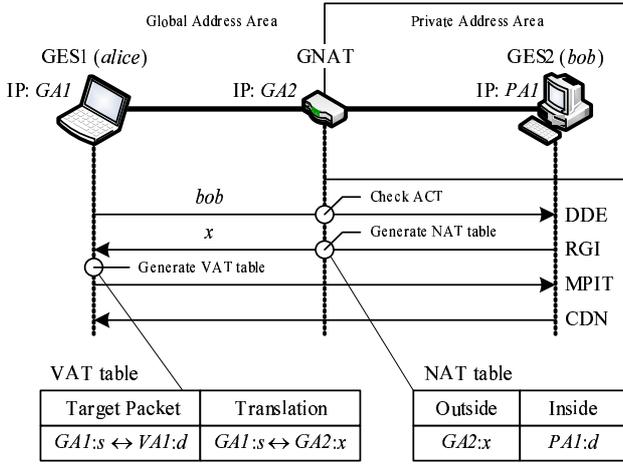


Fig. 4. Extended DPRP negotiation.

and saves their relations in the Name Relation Table (NRT). The virtual IP address is used to distinguish the terminal in the PA area. The virtual address $VA1$ is reported to a higher layer software. Then, when a TCP/UDP packet is sent to GNAT from higher layer applications, the packet is temporarily saved in the kernel memory and the Extended DPRP negotiation starts. Extended DPRP negotiation is shown in Fig. 4. The host name *bob* that is obtained from the NRT is added to the DDE, and GES1 sends it to GNAT. When GNAT receives the above packet, it searches the ACT using the received host name *bob*, and checks whether communication is permitted or not. If communication is permitted, DDE is forwarded to GES2 in the PA area.

When GES2 receives the above DDE, it defines the new CID from CID written in DDE and $PA1$. This information is added to RGI, and GES2 sends it to GES1. When GNAT receives the above RGI, GNAT generates a NAT table dynamically. GNAT adds the port number “ x ” mapped in the NAT table to RGI, and sends RGI to GES1. When GES1 receives the above RGI, GES1 generates the VAT (Virtual Address Translation) table which defines the relationship between the virtual IP

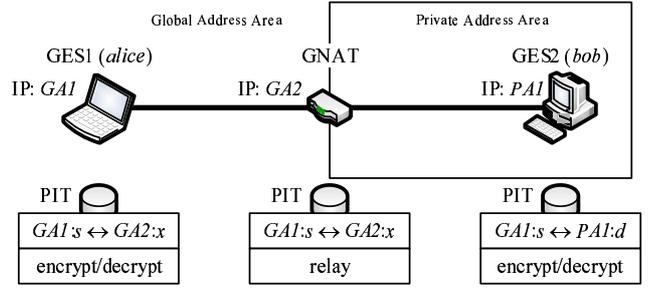


Fig. 5. PITs generated by Extended DPRP.

address/port number, and the IP address/mapped port number “ x ” in GNAT. Subsequent process is the same as that of the conventional DPRP negotiation. The proposed method can be used in the case that a terminal of a PA area does not support GSCIP. In this case, the NAT table and the VAT for the terminal in the PA area are generated with the Extended DPRP between GES1 and GNAT.

B. PIT corresponding to NAT

When a NAT exists on the communication path, the IP address and the port number of communication packets are changed by the NAT. Therefore, PITs have to be generated in each GE, according to that who seems to be the communication partner. The PITs generated with Extended-DPRP are shown in Fig. 5. Since GES2 regards that the communication partner is GES1, it generates the PIT with the connection ID corresponding to GES2 and GES1. Since GES1 regards that the communication partner is GNAT, it generates the PIT with the connection ID corresponding to GES1 and GNAT. In GNAT, it generates the PIT with the same connection ID as GES1.

C. Address Translation Process

Address translation process of communication packets is shown in Fig. 6. After the completion of the Extended DPRP negotiation, GES1 restores the triggered TCP/UDP packet which had been temporarily saved. Then GES1 changes the destination IP address and the port number of the packet from “ $VA1 : d$ ” to “ $GA2 : x$ ” according to the VAT, and sends it to GNAT. In GNAT, it changes the destination IP address and the port number from “ $GA2 : x$ ” to “ $PA1 : d$ ” according to the NAT table, and sends it to GES2. A packet of the opposite direction performs the reverse changes to the above.

V. IMPLEMENTATION

We have added the NAT traversal function to the existing DPRP module in IP layer of FreeBSD. The implementation of GES is shown in Fig. 7. Extended DPRP module is called from input/output function, $ip_input()/ip_output()$. When performing a DPRP negotiation, the initial TCP/UDP packet that triggers the DPRP, is saved in the kernel. This packet is passed to $ip_output()$, after Extended DPRP completes, and is sent to the destination immediately. PIT, NRT, and VAT tables are generated in the kernel space, and are deleted when they

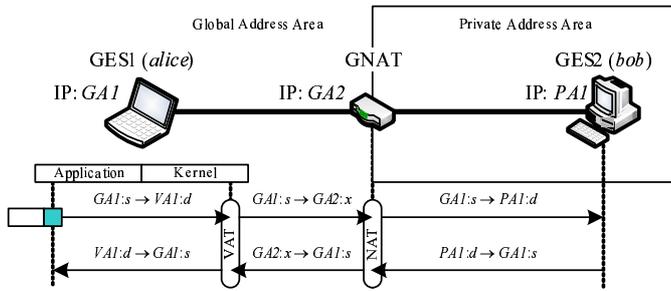


Fig. 6. Address translation process.

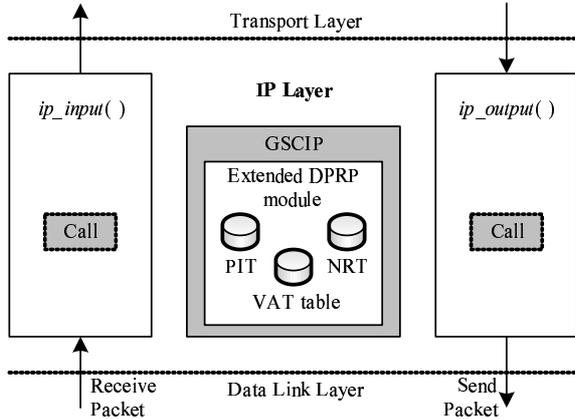


Fig. 7. Implementation of GES.

become useless. The implementation of GNAT is shown in Fig. 8. In addition to the Extended DPRP module, `natd` which is a standard daemon in FreeBSD is made to execute. PIT and ACT tables are generated in the kernel space like GES. IP addresses and port numbers of packets received in GNAT are changed in `natd` via a divert socket. `natd` can be used as it is. In GNAT, the Extended DPRP module is called from the side of the global address interface.

VI. CONCLUSION

We have proposed Extended DPRP which can traverse NAT. With this system, communication groups can be defined and formed even in the environment where the global address area and the private address area coexist. We will complete the implementation of this proposed system and make its evaluation in future.

REFERENCES

- [1] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Richardson, "2006 csi/fbi computer crime and security survey," Computer Security Institute, Tech. Rep., 2006.
- [2] S. Kent and R. Atkinson, "Security architecture for the internet protocol," RFC 2401, Nov. 1998.
- [3] H. Suzuki, M. Takeuchi, N. Kato, S. Masuda, and A. Watanabe, "A proposal of secure communication architecture gscip realizing flexible private network," in *Proc. Symposium on Multimedia, Distributed, Cooperative and Mobile Systems 2005 (DICOMO2005)*, vol. 2005, no. 6, July 2005, pp. 441–444.
- [4] H. Suzuki and A. Watanabe, "Implementation and its evaluation of dynamic process resolution protocol in flexible private network," *IPSI Journal*, vol. 47, pp. 2976–2991, Nov. 2006.

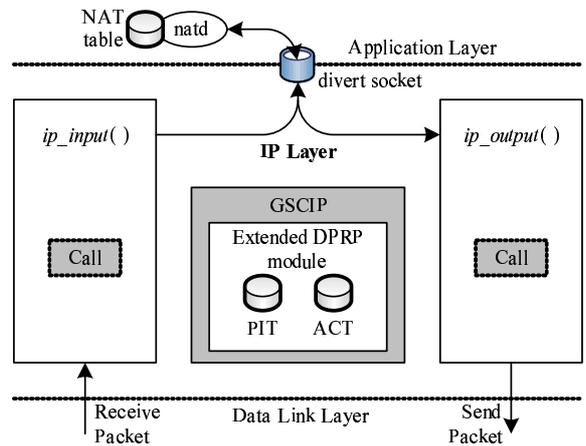


Fig. 8. Implementation of GNAT.

- [5] K. Egevang and P. Francis, "The ip network address translator (nat)," RFC 1631, May 1994.
- [6] P. Srisuresh and M. Holdrege, "Ip network address translator (nat) terminology and considerations," RFC 2663, Aug. 1999.
- [7] Y. Goto, H. Suzuki, and A. Watanabe, "Researches on extended dynamic process resolution protocol between global and private address area," in *Proc. the 68th National Convention of IPSJ*, Mar. 2006.
- [8] 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.
- [9] J. Rosenberg. (2006) Interactive connectivity establishment (ice): A methodology for network address translator (nat) traversal for offer/answer protocols. Internet draft. [Online]. Available: <http://tools.ietf.org/id/draft-ietf-mmusic-ice-12.txt>
- [10] (2001, Nov.) Internet gateway device (igd) standardized device control protocol v 1.0. UPnP Forum. [Online]. Available: http://www.upnp.org/standardizeddcp/docs/UPnP-IGD_1.0.zip
- [11] 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.
- [12] 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 Taipei International Convention Center
October 30 – November 3 ,2007 Taiwan, Taipei

Researches on Extended Dynamic Process Resolution Protocol that Can Traverse NAT

Yuji Goto

Hidekazu Suzuki

Akira Watanabe

Meijo University, JAPAN

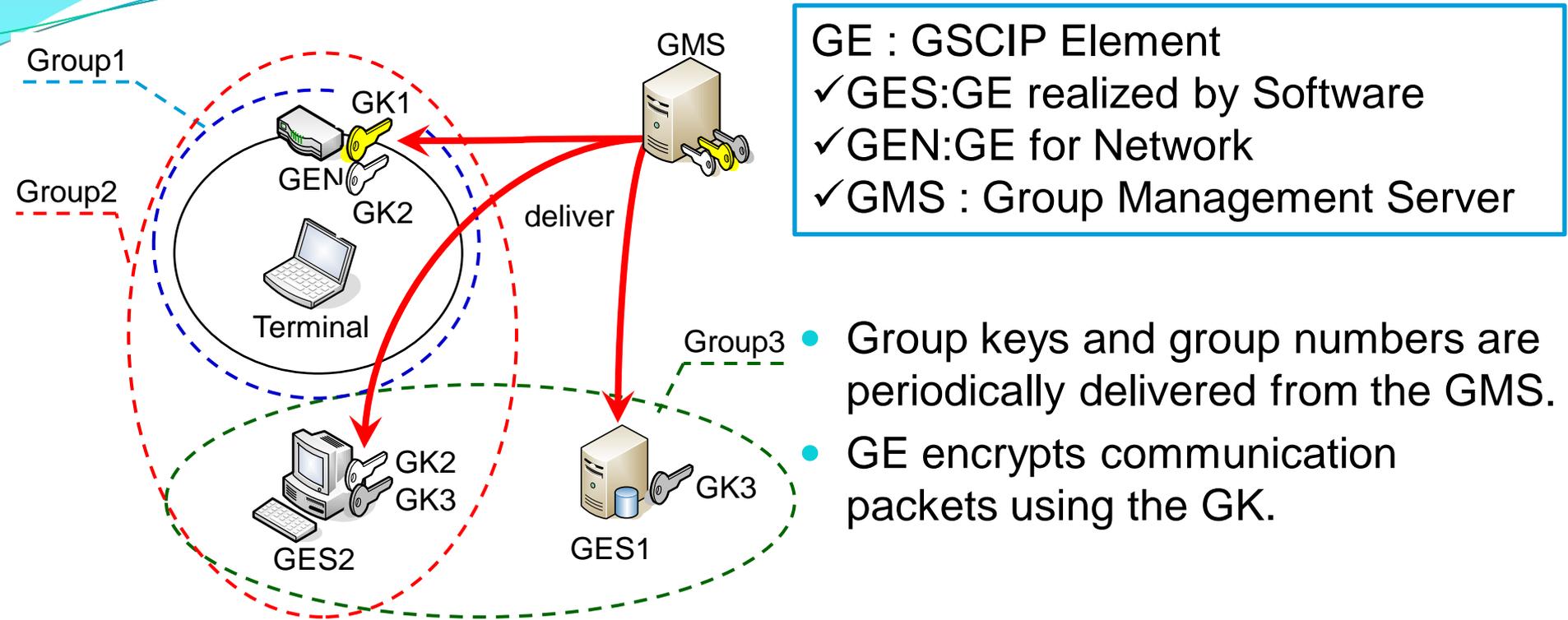
Introduction

- The needs of ubiquitous networks
 - Accessible at anytime
 - Accessible from anywhere
 - Secure communication



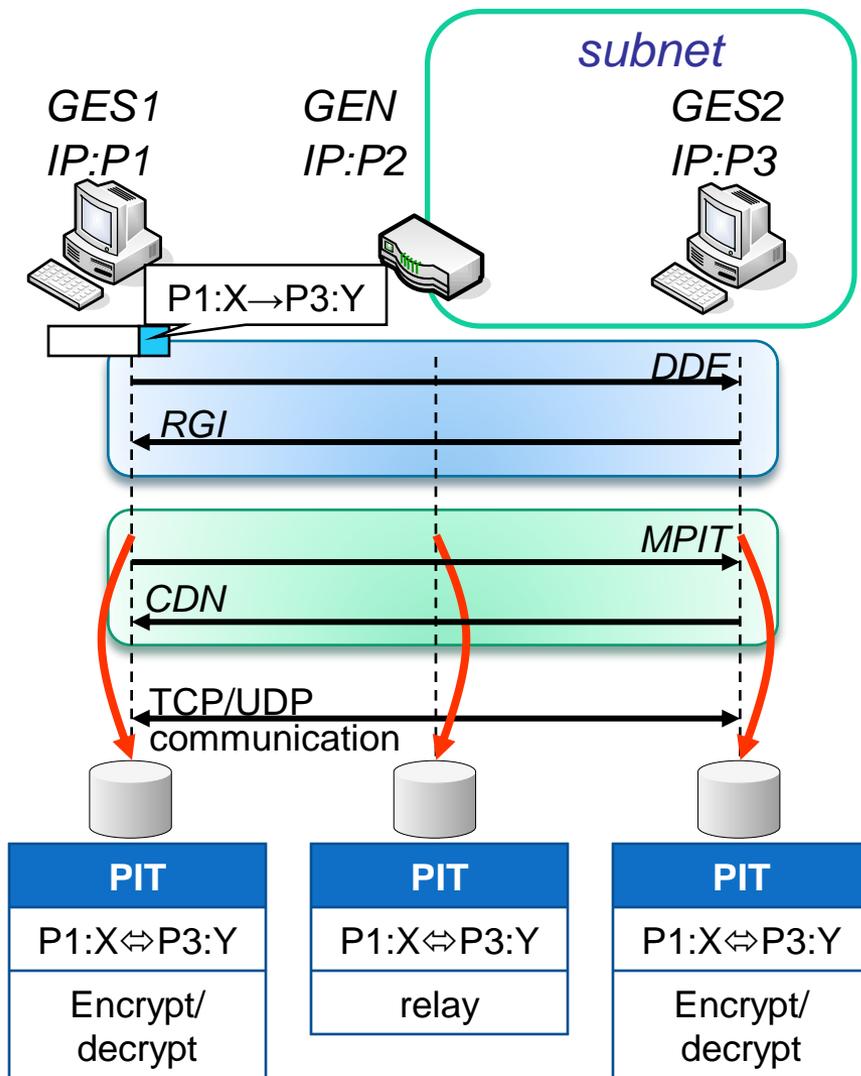
Grouping for Secure Communication for IP (GSCIP) that can realize a group communication securely and Flexibly .

The outline of GSCIP



- A communication group and a group key (GK) have a 1 to 1 correspondence.
- Communication groups are defined with the GKs.
- The definitions of communication groups are maintained even if a system configuration changes.

Dynamic Process Resolution Protocol (DPRP)



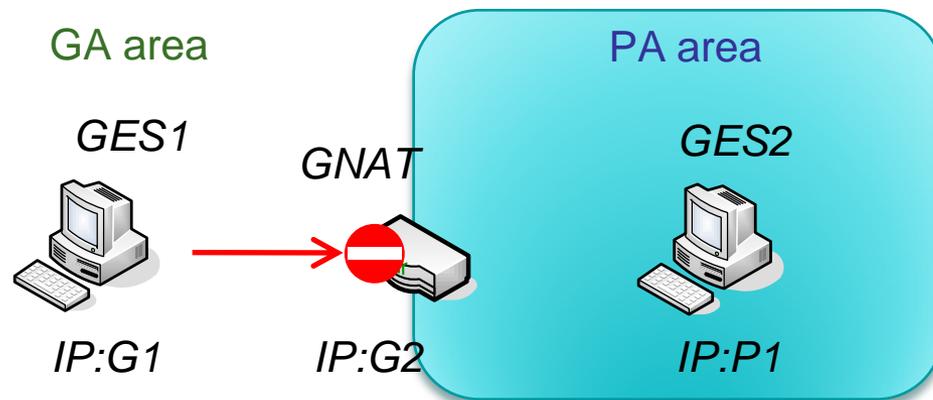
Four control packets (defined on ICMP)

- (DDE) Detect Destination End GE
- (RGI) Report GE Information
- (MPIT) Make Process Information table
- (CDN) Complete DPRP Negotiation

Operation of DPRR (2 round - trip negotiation)

1. Detect destination end GE.
 2. Collection of information of GEs on the communication path
 3. Check whether it is the same group or not using the GK.
 4. Determine the process information.
5. Notification of process information.
 6. GEs handle packets according to PIT.
 7. Closing of the negotiation.

DPRP Negotiation from global address (GA) area to private address (PA) area



The NAT traversal problem

- A terminal in GA area can not start communications with a terminal in the PA area.
- GES1 in GA area can not see the network behind GNAT.

We have proposed extended DPRP and solved the NAT traversal problem

Extended DPRP : Initial information

- Registration to Dynamic DNS (RR)
 - The host name “bob” of GES2 in PA area
 - The IP address “G2” of GNAT
- Registration to GNAT(ACT)
 - The host name “bob”
 - The private IP address “P1”
 - Authorization

DNS



RR (Resource Records)

Name	IP
bob	G2

ACT (Access Control Table)

Name	IP	Authorization
bob	P1	allow

GA area

GES1



IP:G1
HN:alice

GNAT



IP:G2
HN:sun

PA area

GES2

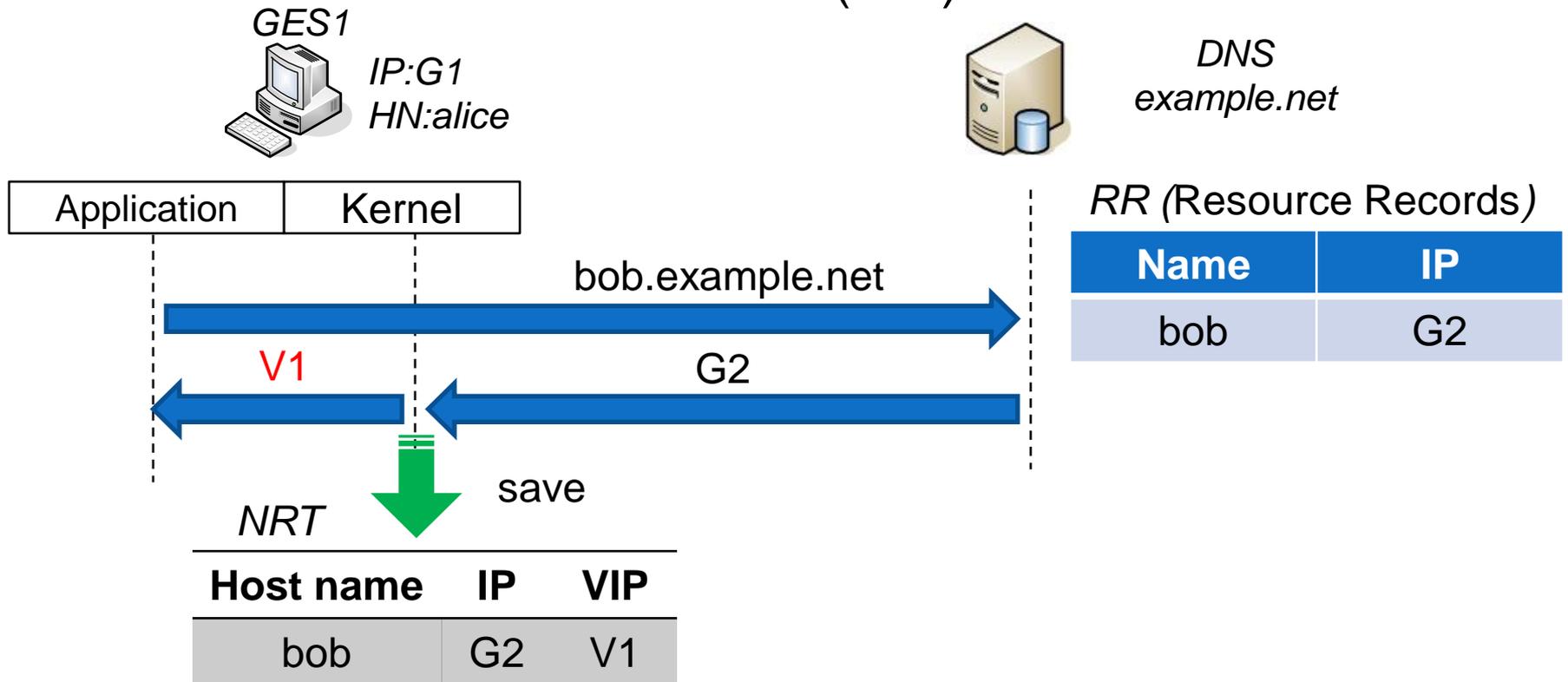


IP:P1
HN:bob

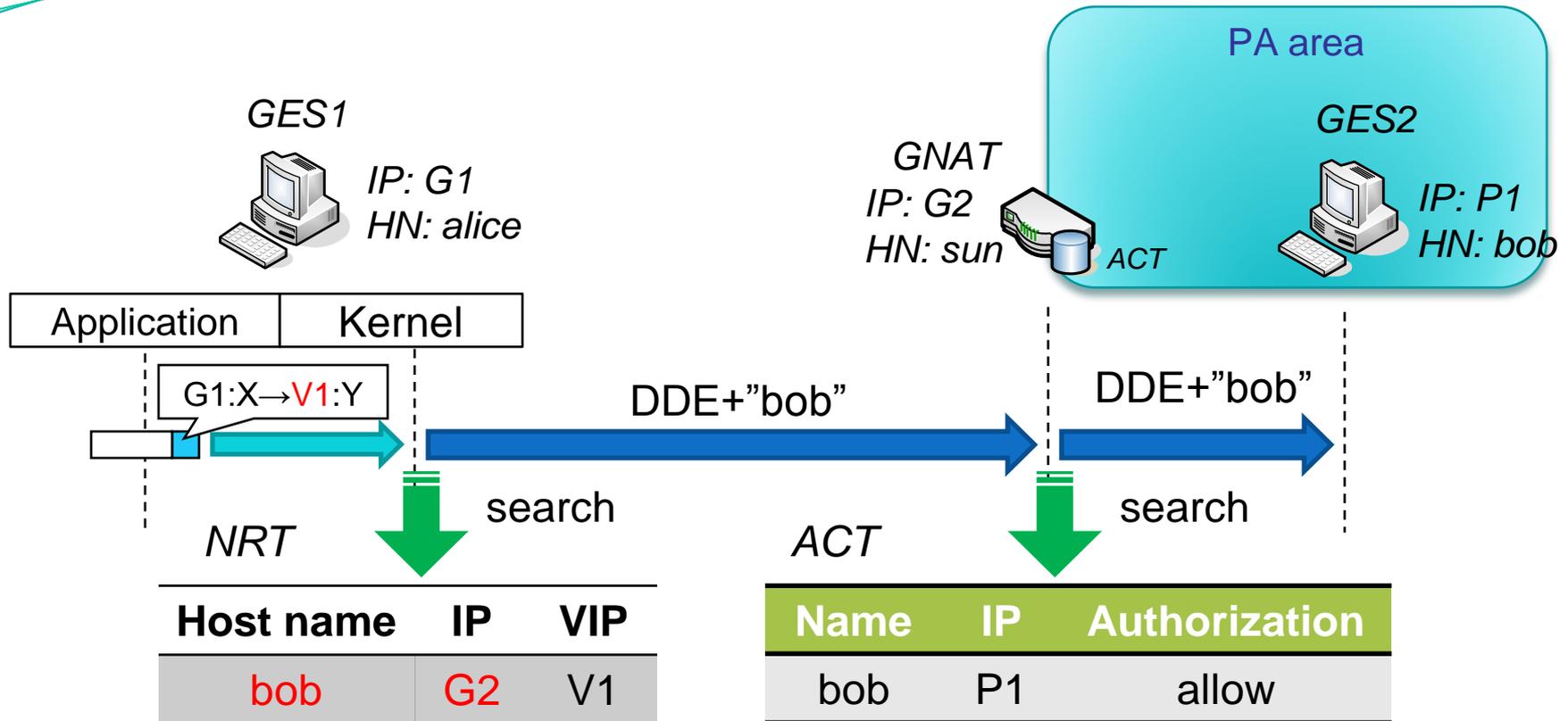
ACT

DNS name resolution process

- GES1 changes the IP address “G2” to a certain virtual IP address “V1”
- NRT (Name Resolution Table)
 - Consists of a host name, an IP address of GNAT, and a Virtual IP Address (VIP).

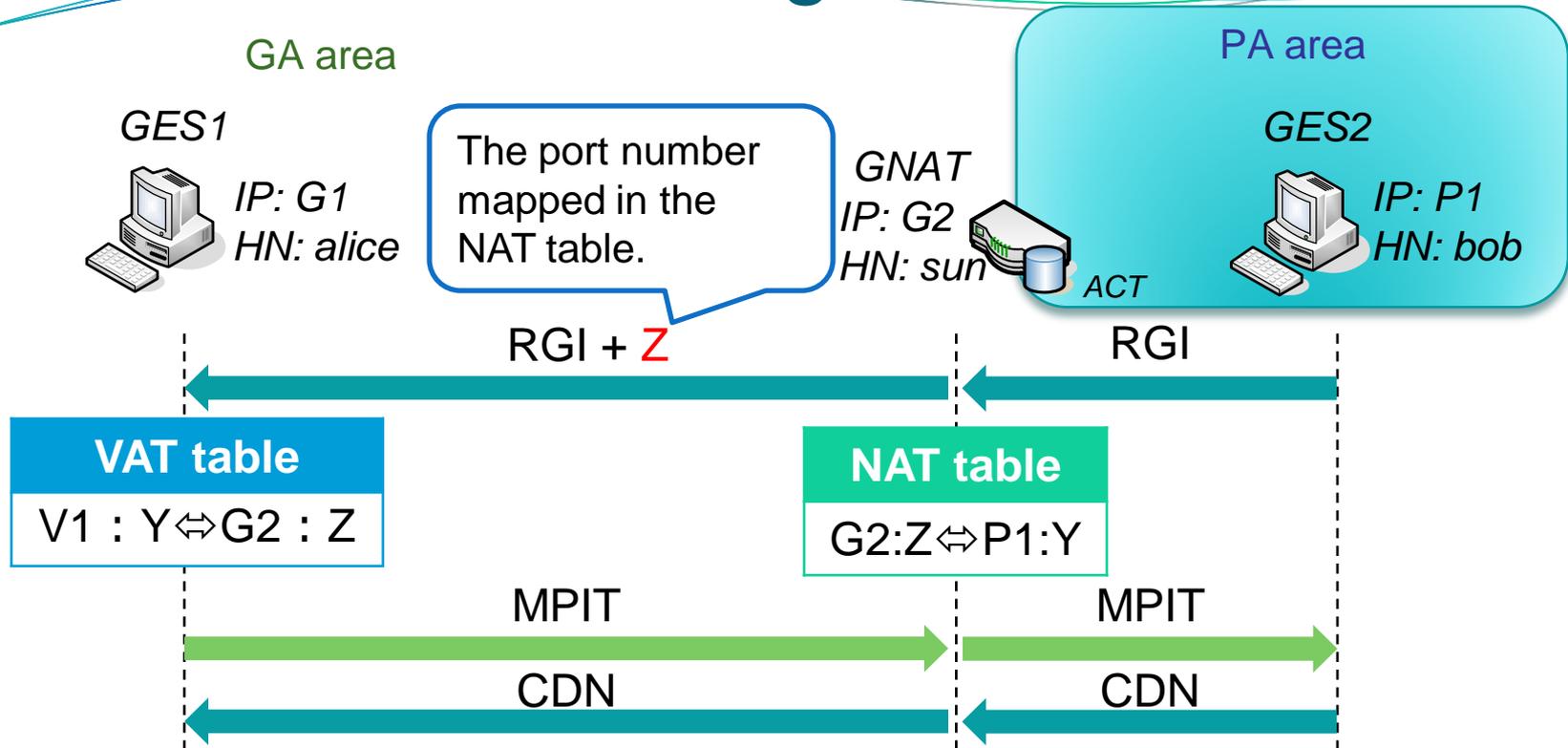


Extended DPRP Negotiation 1



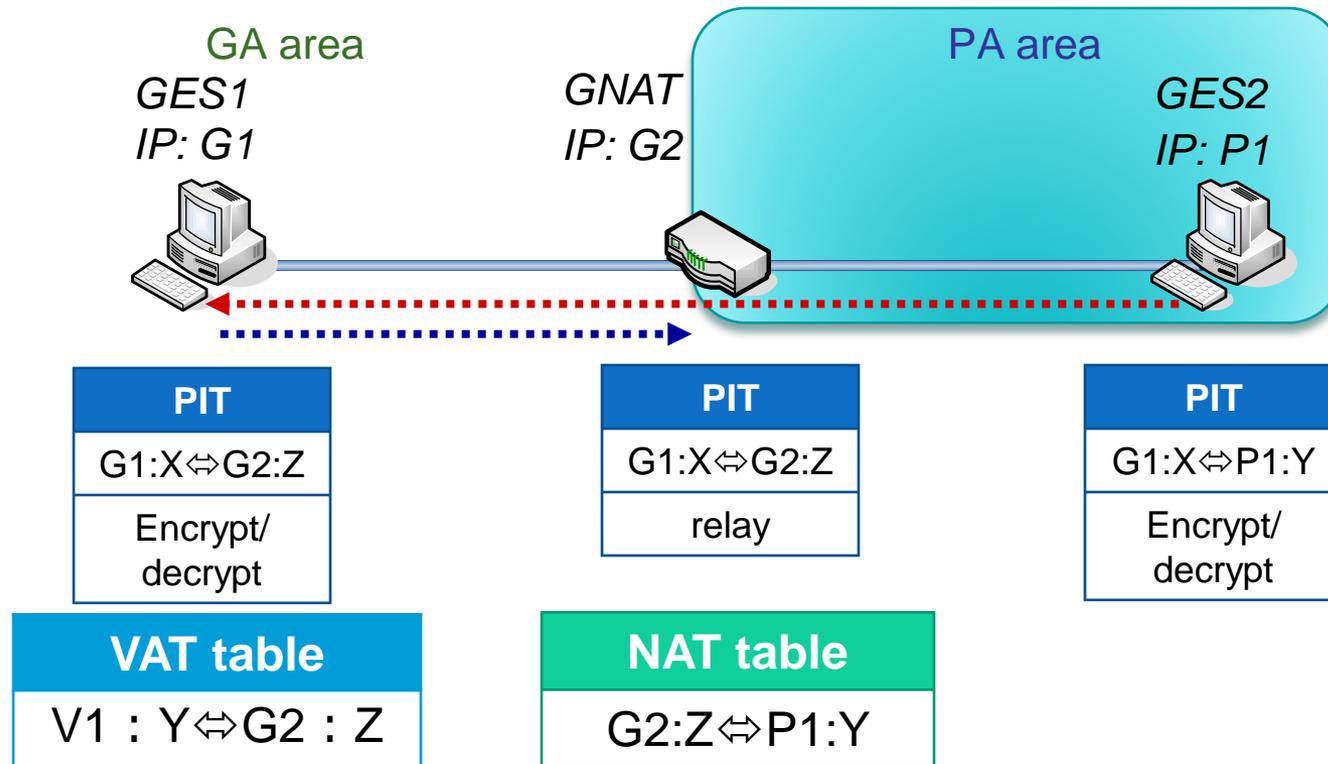
- GES1 sends DDE with the host name “bob”.
- GNAT searches the ACT to find the private IP address “P1” using “bob”
- If communication is allowed, GNAT relays DDE + “bob” to GES2

Extended DPRP Negotiation 2



- GNAT generates a NAT table corresponding to GES1 and GES2.
- GES1 generates a Virtual Address Translation (VAT) table.
- MPIT and CDN are the same with the normal DPRP negotiation.

PIT for the proposed method

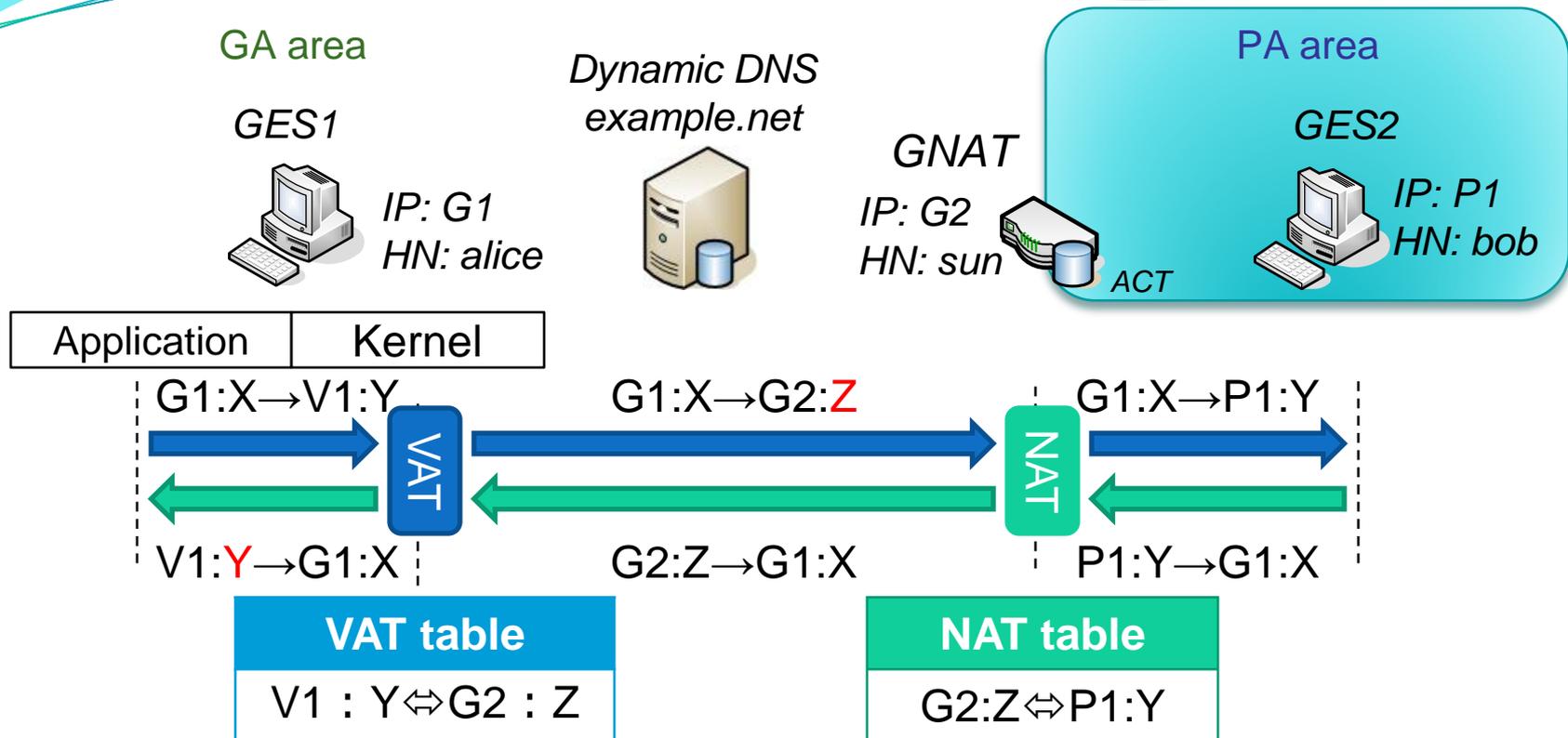


GES2 regards the communication partner as GES1.

GES1 regards the communication partner as GNAT.

Each GE generates different PITs

Address Translation Process



- GES1 changes the destination IP address and the port number of the packet from “V1:Y” to “G2:Z” according to the VAT table.
- The NAT traversal problem is solved and the secure communication group is established

Summary

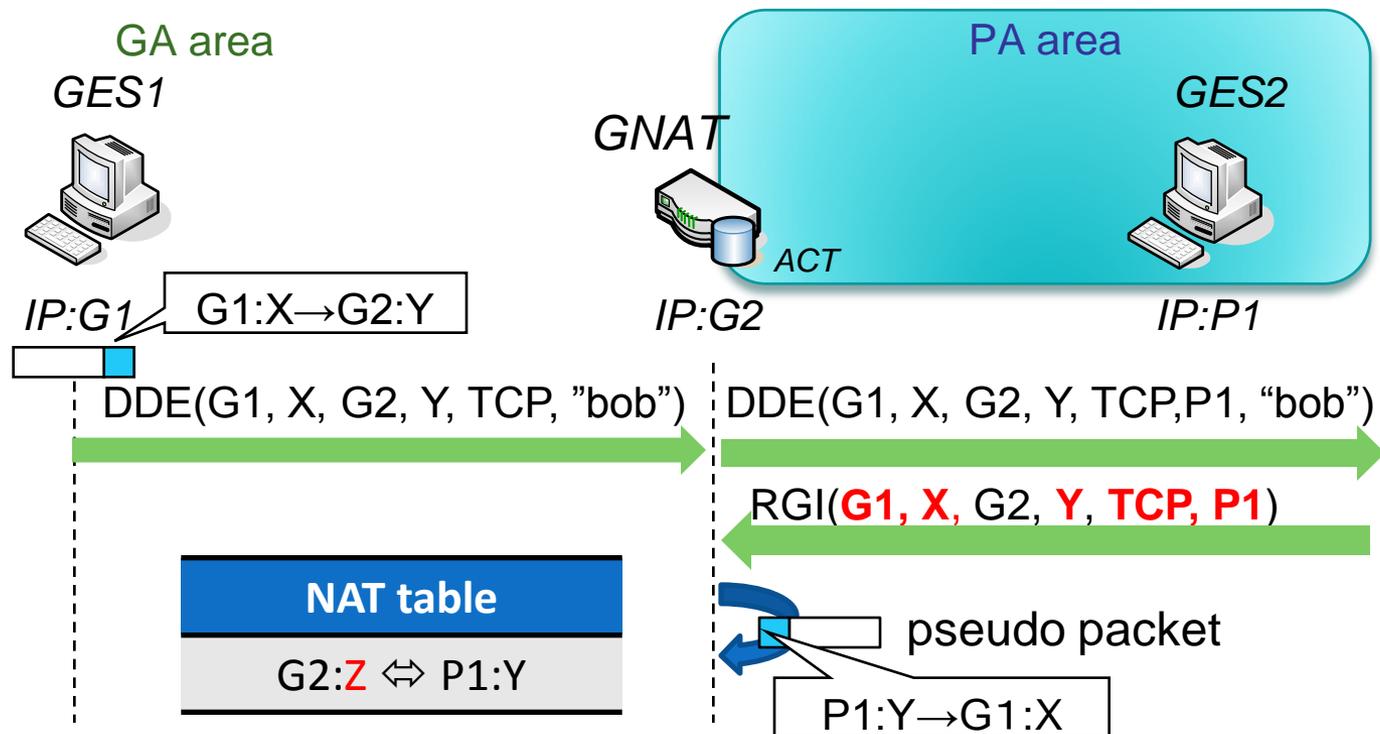
- The problem in case that NAT exists on communication path is:
 - The NAT traversal problem
- We have proposed Extended DPRP which can traverse NAT
 - The making of communication groups ranging from a GA area to a PA area has become possible
- Future plans
 - We will complete the implementation of the proposed system and evaluate the system



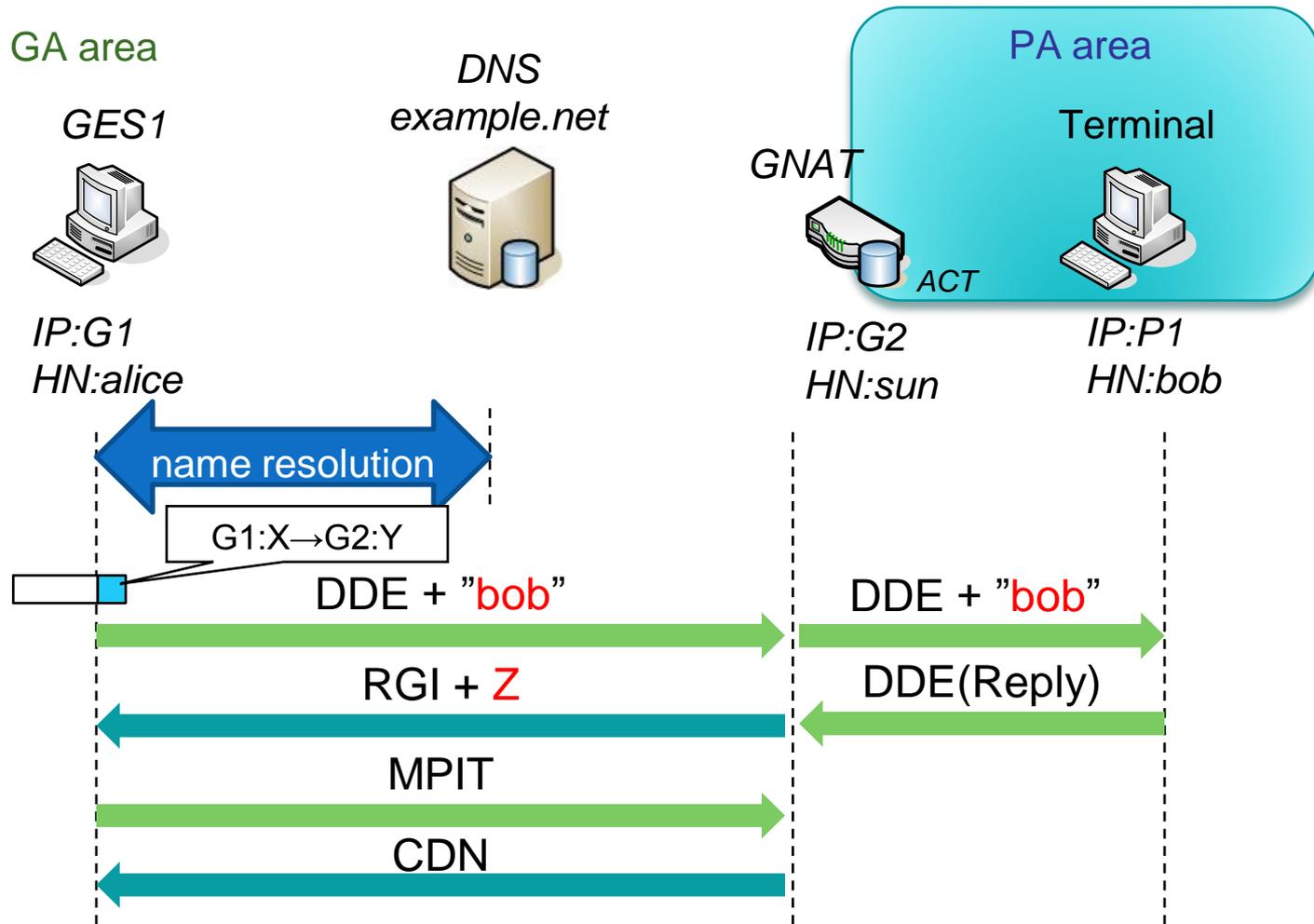
Appendixes

The NAT table generation method

- A pseudo packet is generated from information of RGI and the private IP address in ACT
- It pretends to be a packet which transmits to GES1 from GES2

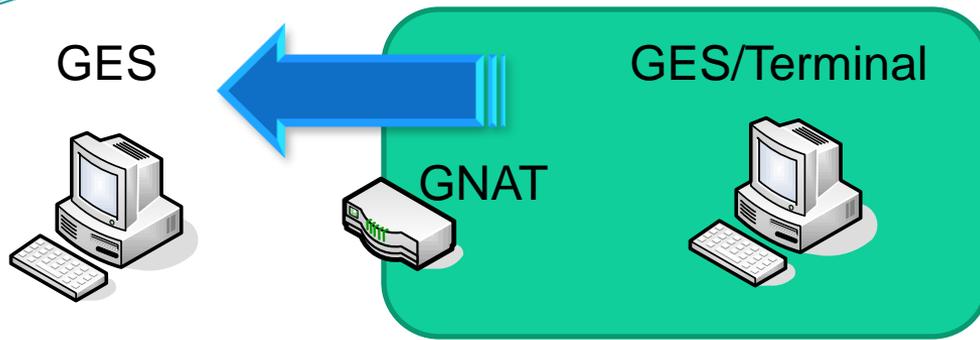


When the terminal of PA area is a general terminal

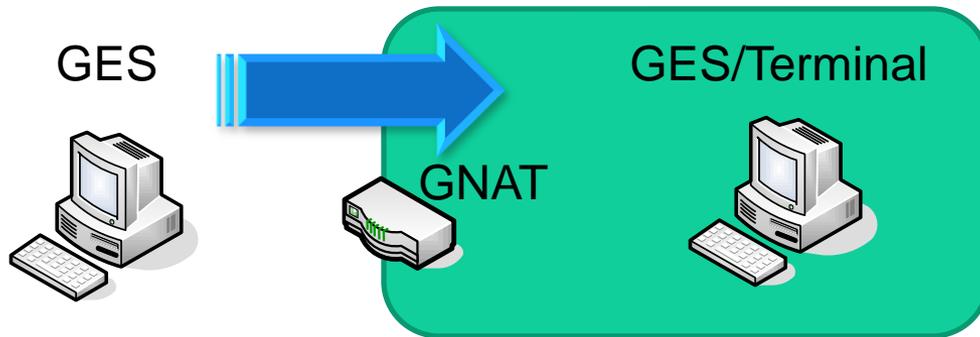


- DDE Reply is answered from a terminal
- The negotiation after RGI is performed between GES1 and GNAT.

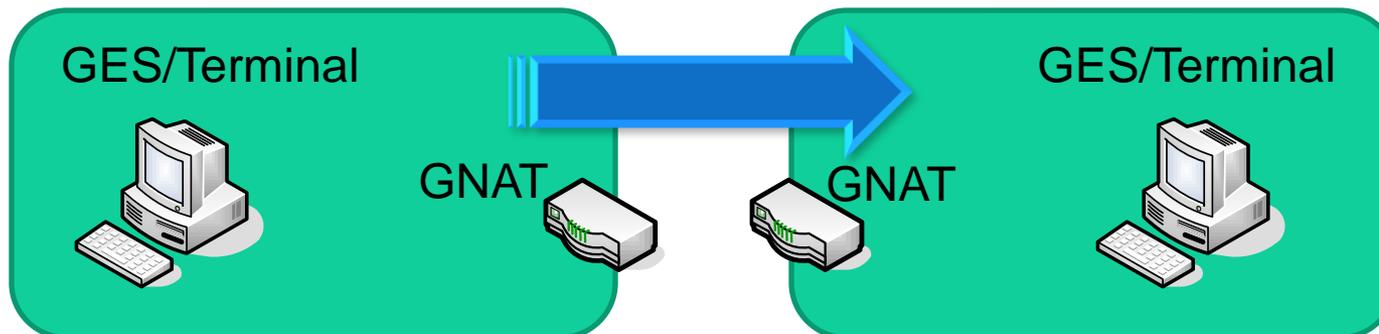
The scene which DPRP can use



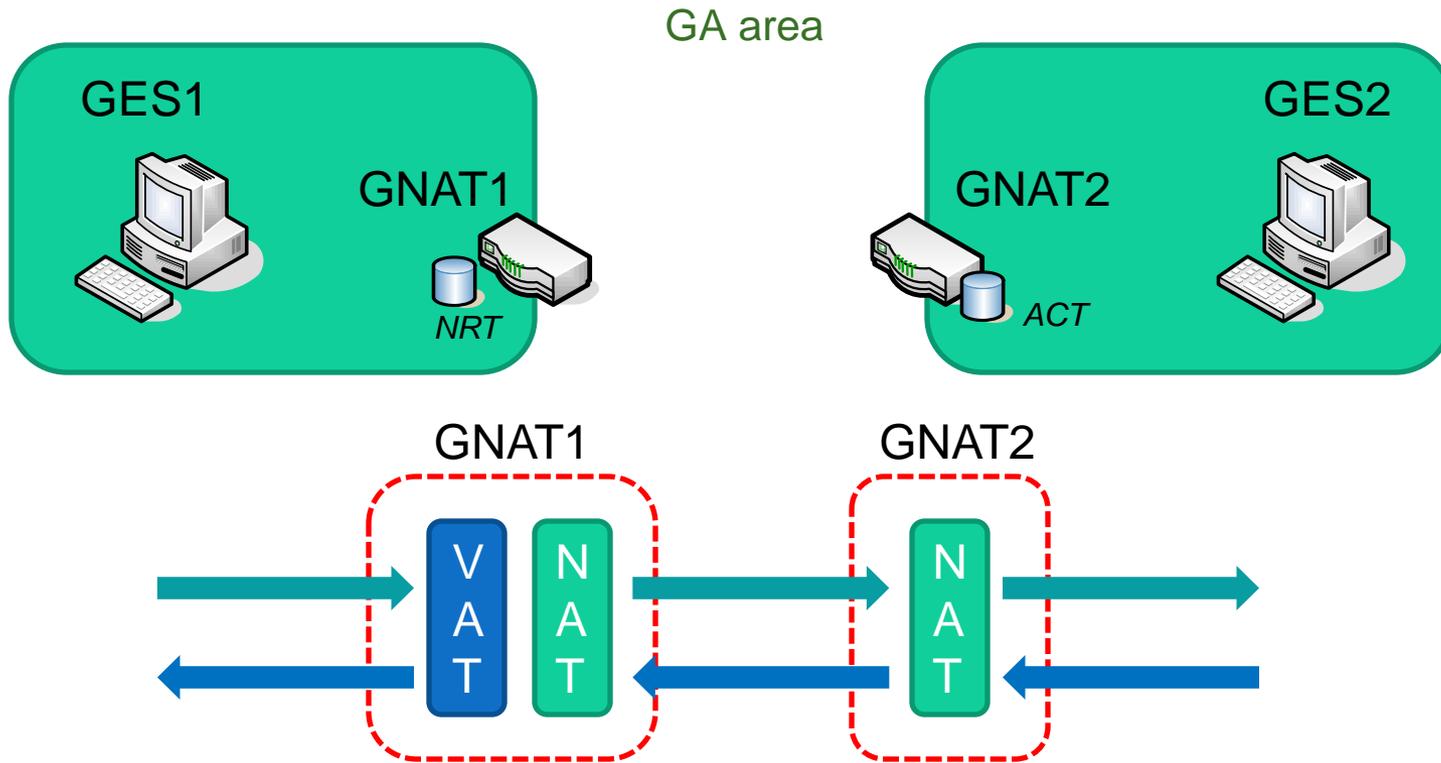
 Private Address area
 communication start direction



- DPRP can be used in the case that a terminal of a PA area does not support GSCIP.
- Different PA area by extending DPRP can be used.

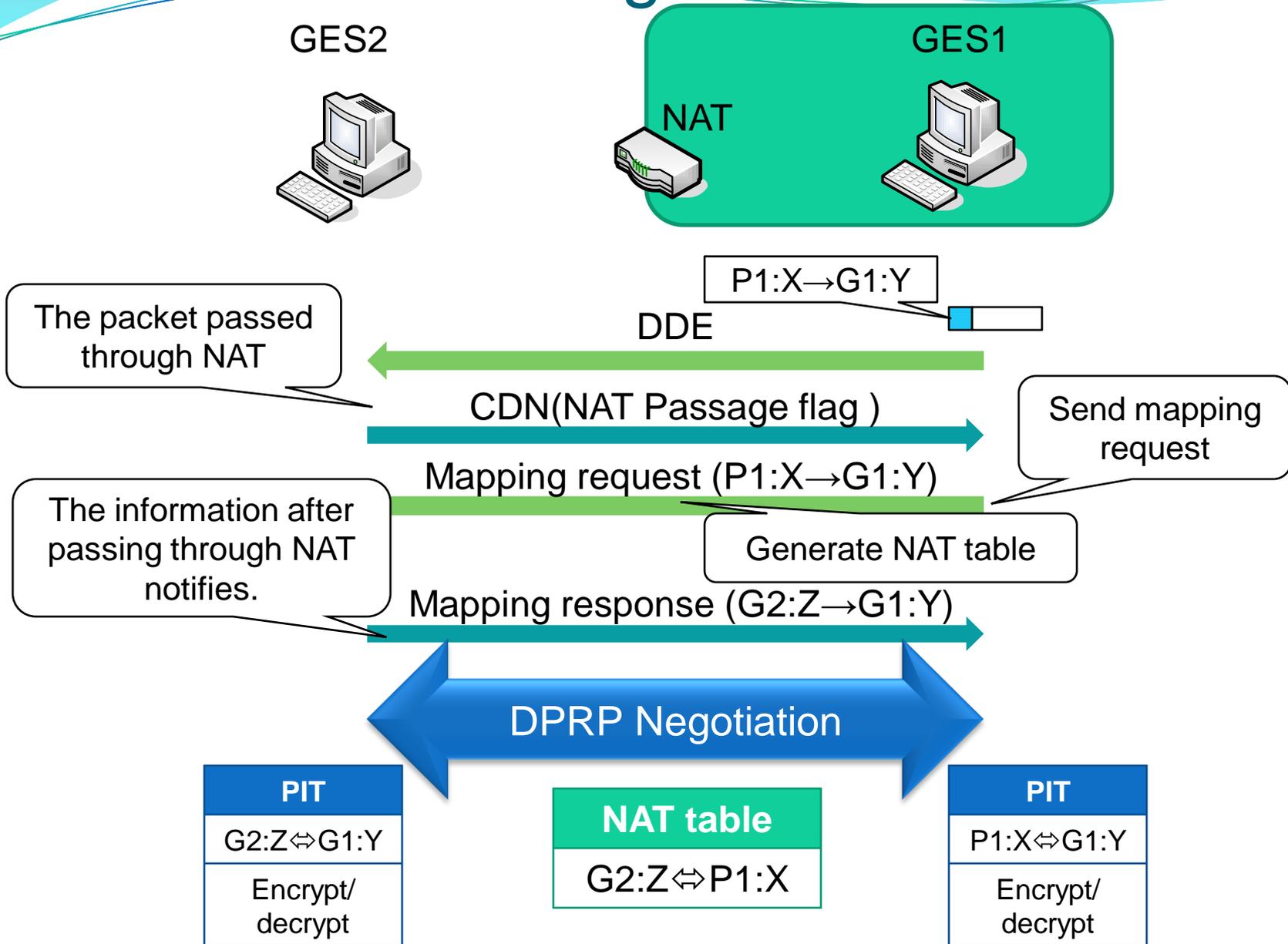


Communication of different PA area

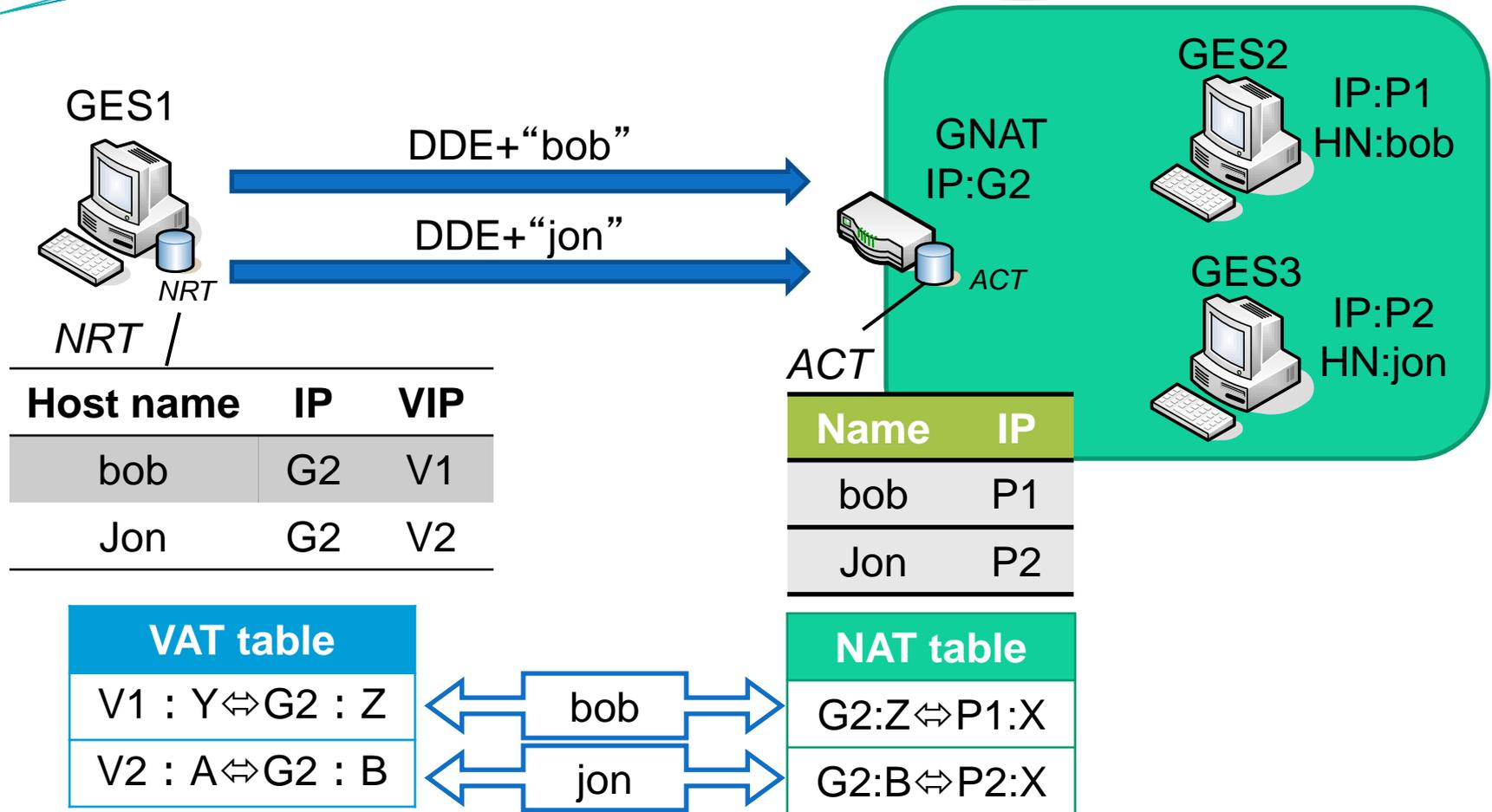


- It is possible in private address area which is different by performing VAT and DNS processing instead of GNAT being GES1.

In the case of the general NAT device



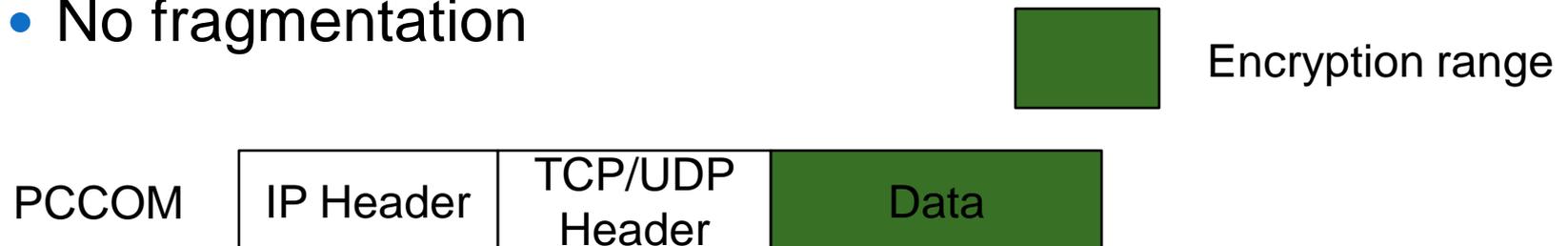
Simultaneous communication



- The application of GES1 recognizes bob as V1 and jon as V2
- Generate the NAT table corresponding to a host name
- Generate the VAT table corresponding to NAT table

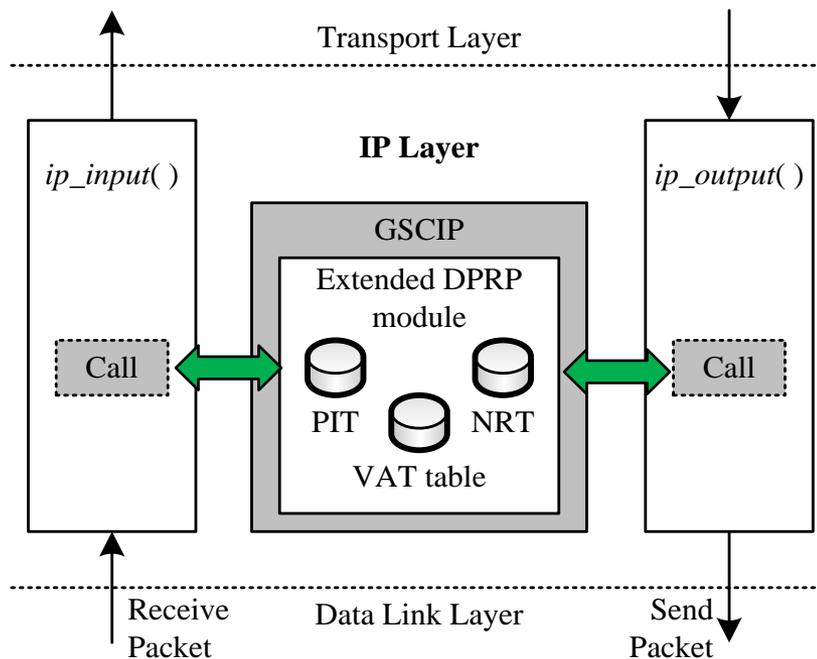
PCCOM (Practical Cipher COMMunication)

- NA (P) T and a firewall can be passed
 - The encryption range is user data
 - When the packets pass through NAT, IP addresses and port numbers are not included in integrity range.
 - An IP address port number, a TCP/UDP checksum, etc
 - It assures in the search process of PIT.
- Packet length does not change.
 - No fragmentation

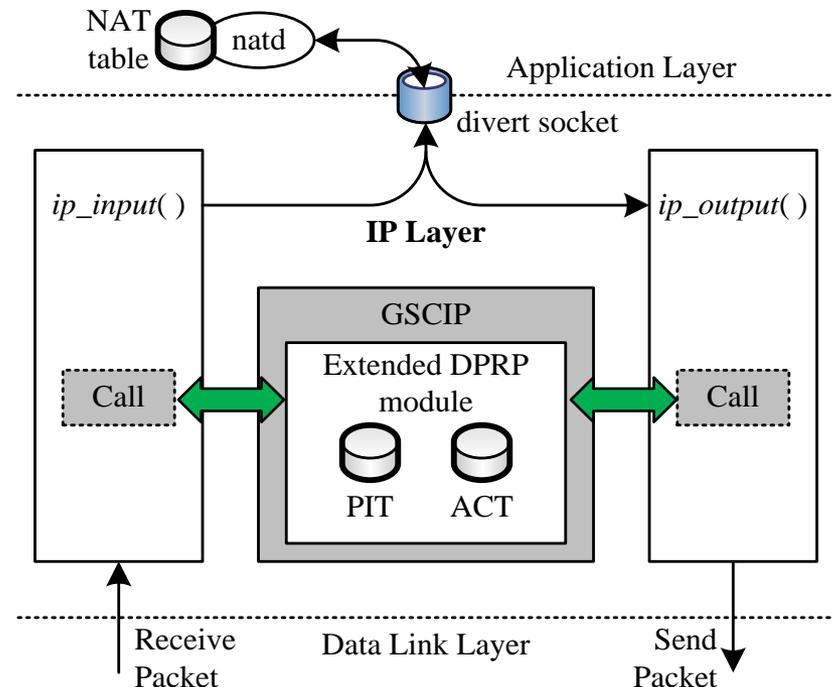


Implementation

- Added the NAT traversal function to the existing DPRP module in IP layer of FreeBSD.
- Extended DPRP module is called from input/output function, `ip_input()/ip_output()`.
- It does not affect the existing process in the IP layer.

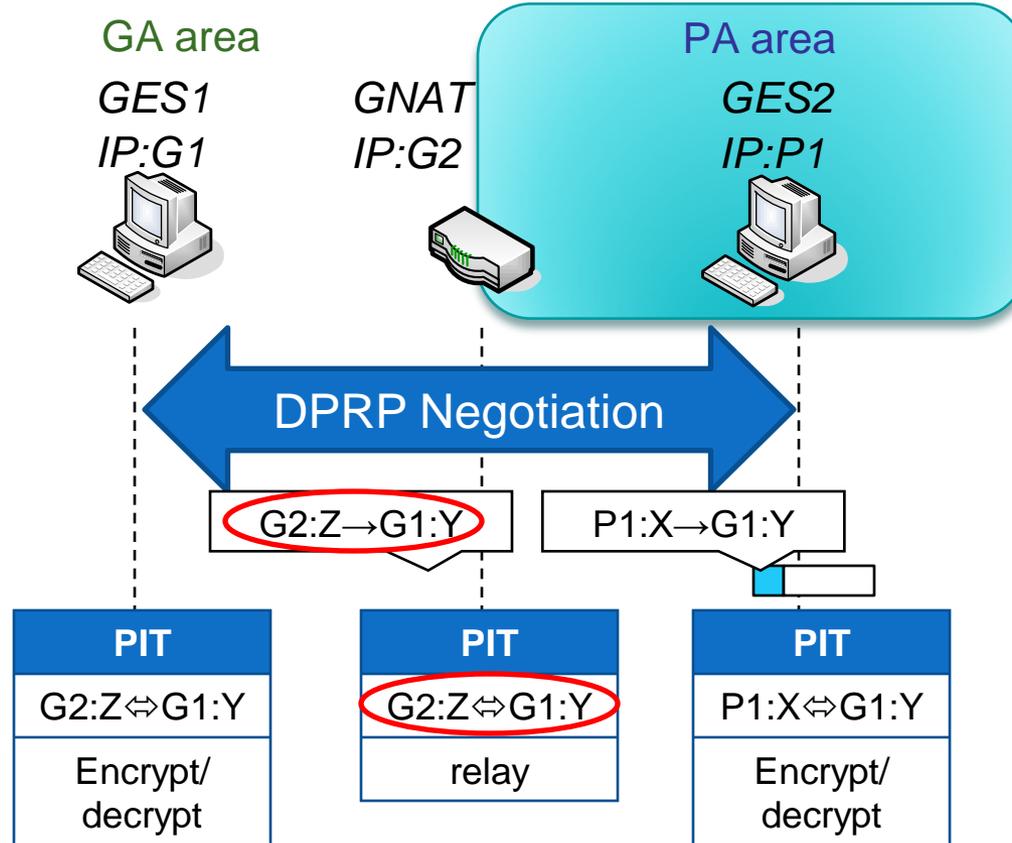


Implementation outline of GES



Implementation of GNAT

DPRP Negotiation from PA area to GA area



- PIT in GES1 and GNAT generates using the information translated by the NAT.
- GNAT and GES1 generates PIT which the connection information of communication packet.

Multistep NAT

