NAT 越えが可能な DPRP の検討

Researches on an Extended Dynamic Process Resolution Protocol for NAT-Traversal

後藤　裕司[*1]　鈴木　秀和[*2]　渡邊　晃[*1]
Yuji Goto　　Hidekazu Suzuki　　Akira Watanabe

*1　名城大学理工学部　*2 名城大学大学院理工学研究科
Graduated School of Science and Technology, Meijo University

1. はじめに

近年，ネットワーク経由の情報漏洩などの驚異に対するセキュリティ対策が重要視されている．そこで我々は柔軟かつ安全なグループ通信を可能とするためにシステム構成が変化してもその変化を動的に学習することができる DPRP（Dynamic Process Resolution Protocol）[1]と呼ぶ通信プロトコルを提案してきた．しかし，既存の DPRP は同一アドレス空間でしか動作せず，通信経路上に NAT（Network Address Translation）が介在するような通信環境では利用することができなかった．この課題を解決するために，これまでプライベートアドレス（以下 PA）空間からグローバルアドレス（以下 GA）空間への通信を開始する場合についての検討を行ってきた[2]． 本稿ではさらに GA 空間から PA への通信を開始する場合についての検討を行った．具体的には我々が別途提案してきた NAT 越え技術 NAT-f（NAT free protocol）[3]と組み合わせることにより NAT 越えが可能な DPRP を実現した．

2. 既存技術

2.1 DPRP

DPRP は通信端末間が通信に先立って 2 往復のネゴシエーションを行う．1 往復目で通信経路上の DPRP 対応装置がどの通信グループに帰属するかという情報を収集する．収集した情報より動作処理情報を決定し，各装置に対し動作処理情報テーブル PIT（Process Information Table）を通知する．PIT には，透過中継，暗号化，破棄など通信パケットに対する処理内容が記述されている．ネゴシエーション終了後は生成した通信 PIT に従ってパケットを処理する．グループ番号や暗号鍵はあらかじめ DPRP 対応装置に設定されている必要がある．

2.2 NAT-f

NAT-f は GA 空間上の端末（以下 GN）と NAT-f に対応したルータ（以下 NAT-f ルータ）が連携することにより GN から PA 空間内にいる端末（以下 PN）に通信の開始が可能になるプロトコルである．GN は通信に先立ち NAT-f ルータに対し 1 往復の NAT-f ネゴシエーションを行い，NAT テーブルを生成するために必要な情報を NAT-f ルータに通知する． NAT-f ルータは，NAT テーブルを強制的に生成し，NAT テーブル生成時にマッピングされたポート番号を GN へ応答する．GN はポート変換テーブルを生成し，送受信パケットに対しポート番号の変換を行う．以後の GN からの通信は通知されたポート番号に向けて送信されるため，NAT-f ルータは通常の NAT 処理により通信を行うことができる．

3. NAT 越え DPRP

DPRP と NAT-f は IP 層に実装され，かつ通信に先だってネゴシエーションであるため統合することが可能である．図 1 に NAT 越え DPRP の動作について示す．DPRP ネゴシエーションの 1 往復目に NAT-f のネゴシエーションに必要な情報を追加し，NAT テーブルを強制的に生成する． 2 往復目で GN は NAT-f ルータから通知されたポート番号を用いて PIT 生成し，NAT-f ルータおよび PN に通知する．GN はポート変換を行ってから PIT に従った処理を行うため PN と通信が可能となる．

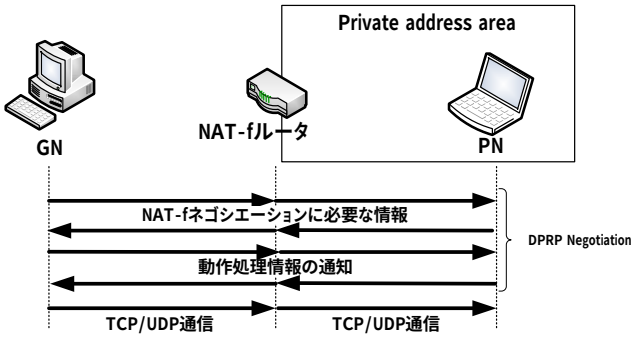


図 1　NAT 越え DPRP の動作

4. まとめ

本稿では DPRP と NAT-f を組み合わせることにより NAT 越えが可能な DPRP について提案した．これまで検討してきた PA 空間から GA 空間への DPRP と組み合わせることによりアドレス空間の違いを意識しない DPRP が可能となる．今後は，本提案を実装し評価を行う．

参考文献

[1] 鈴木秀和，渡邊晃：フレキシブルプライベートネットワークにおける動的処理可決プロトコル DPRP の実装と評価，情報処理学会論文誌，Vol.47，No.11，pp.2976-2991，Nov.2006

[2] 後藤裕司，鈴木秀和，渡邊晃：グローバルアドレスとプライベートアドレス空間を跨る DPRP の検討，第 68 回情報処理学会全国大会講演論文集，Mar.2006

[3] 鈴木秀和，渡邊晃： アドレス空間透過性を実現する NAT-f の実装と評価，DICOMO2006 シンポジウム論文集(I)，Vol.2006，No.6，pp.453-456，Jul.2006.

NAT越えが可能なDPRPの検討

名城大学理工学部
後藤　裕司
鈴木　秀和
渡邊　晃

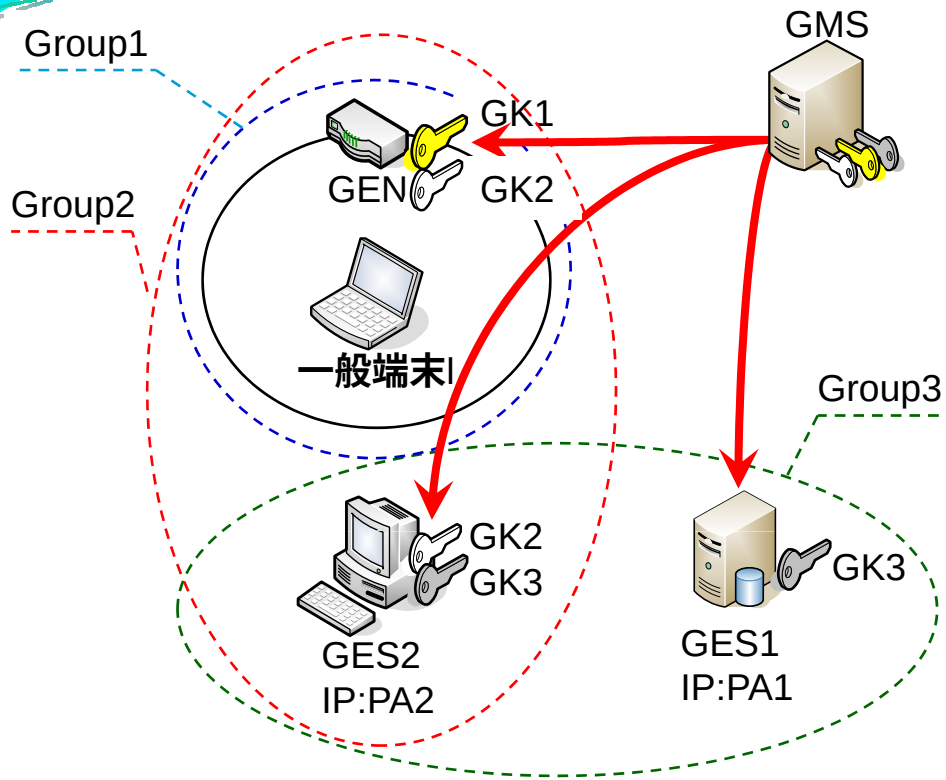
はじめに

- ユビキタスネットワークでは
  - いつでもネットワークに繋げたい（外出中・移動中）
  - どこからでもアクセス（屋外・友人宅・移動体など）
  - 安全な通信（盗聴・改竄などがない）

柔軟性とセキュリティを兼ね備えたグループ通信を可能にする

GSCIP（Grouping for Secure Communication for IP）

GSCIP (Grouping for Secure Communication for IP)



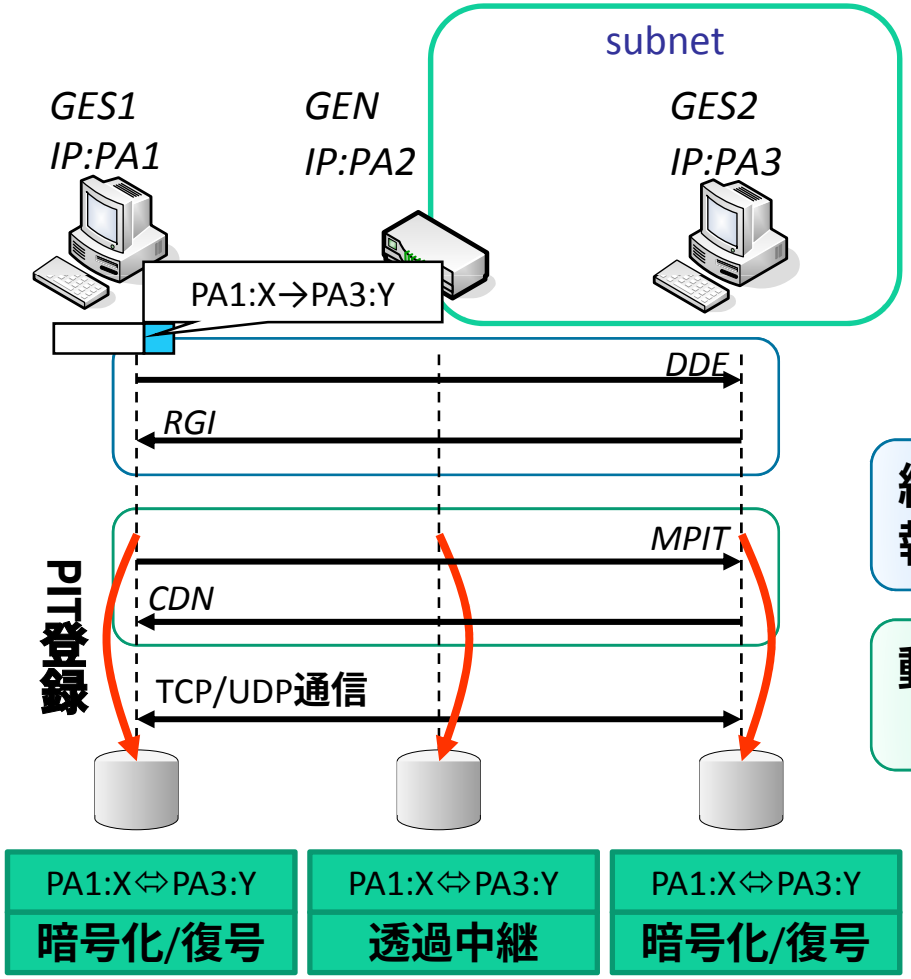
GE：GSCIP**対応した装置**
◆GES (Software**型**) :**ホストタイプ**
◆GEN (Network**型**) ：**ルータタイプ**
GMS：**管理装置**

GMS**は各**GE**にグループ番号とグループ鍵**GK**を配送**

- **通信グループとグループ鍵**GK**を１：１に対応づける**
  - IP**アドレスに依存しないグループを定義**

システム構成が変化してもグループ関係は維持される

DPRP (Dynamic Process Resolution Protocol)



4つの制御パケット (ICMP**ベース**)

DDE (Detect Destination End GE)

RGI (Report GE Information)

MPIT (Make Process Information table)

CDN (Complete DPRP Negotiation)

DPRP**の動作** (2**往復のネゴシエーション**)

終端GEの決定、通信経路上の各GEの設定情報を取得し動作処理情報を決定

動作処理情報の通知と動作処理情報テーブル PIT (Process Information Table) **の生成**

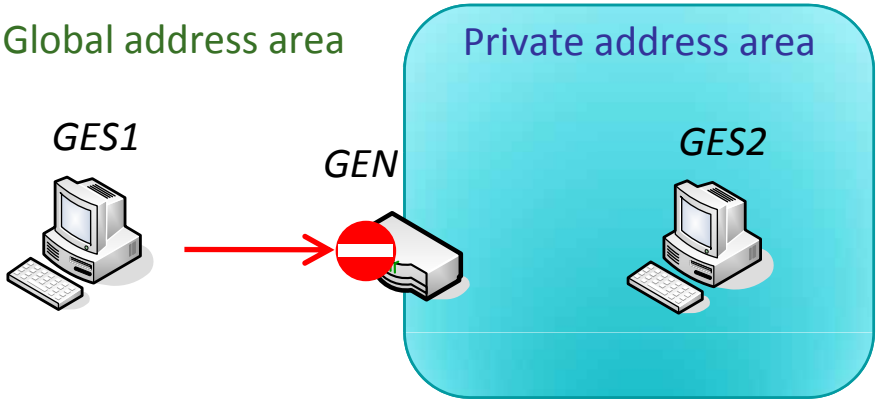
- **GKにより通信相手が同一グループであるかどうかを確認**
- **パケットは動作処理情報に従って処理される**

通信経路上にNATが存在する場合

GA空間側の端末：*GES1*

PA空間側の端末：*GES2*

NAT機能を追加したGEN



NAT越え問題

- GA空間側から通信開始ができない
  - GA空間からPA空間の中が見えないため

DPRPを拡張することによりNAT越えを実現

NAT越えDPRP：事前設定

- Dynamic DNSへの登録
  - PA空間の端末のホスト名
  - GENのIPアドレス

Dynamic DNS

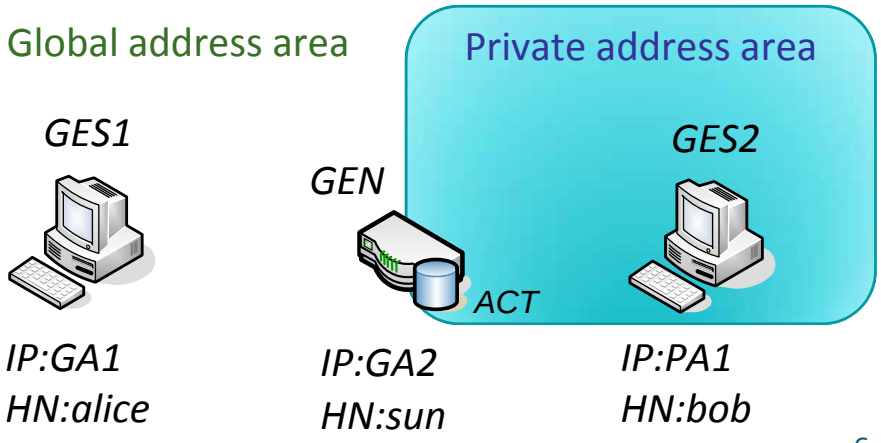
RR (Resource Records)

Name	IP
Bob	GA2

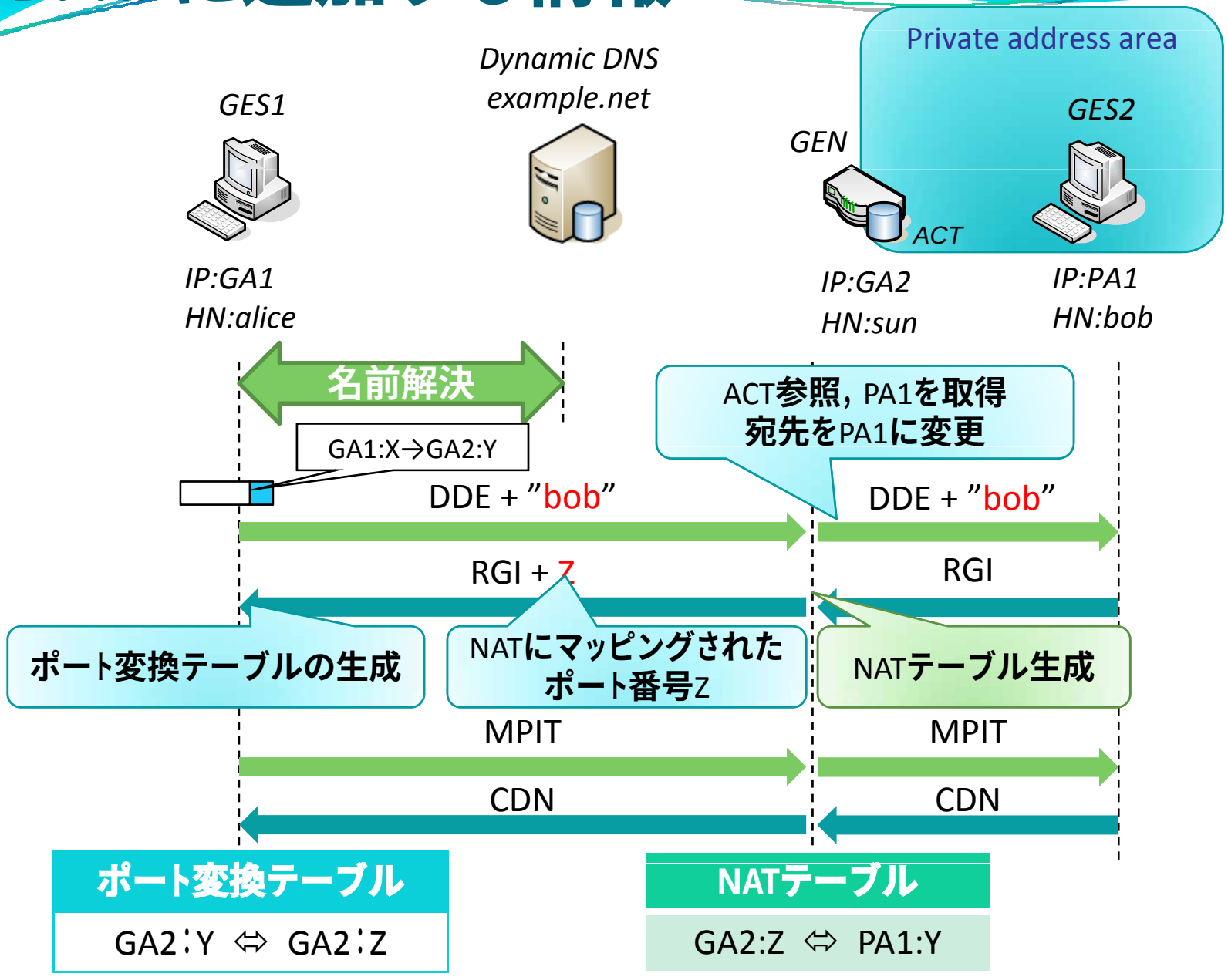
- GENへの登録
  - PA空間の端末のホスト名とIPアドレス
  - アクセス許可情報

ACT (Access control table)

Name	IP	Authorization
bob	PA1	allow

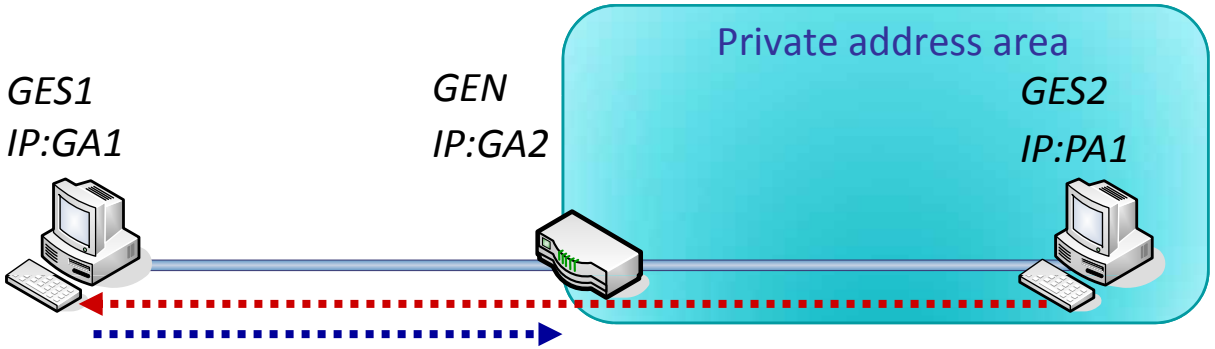


DPRPに追加する情報



生成されるPIT

通信経路上にNAT



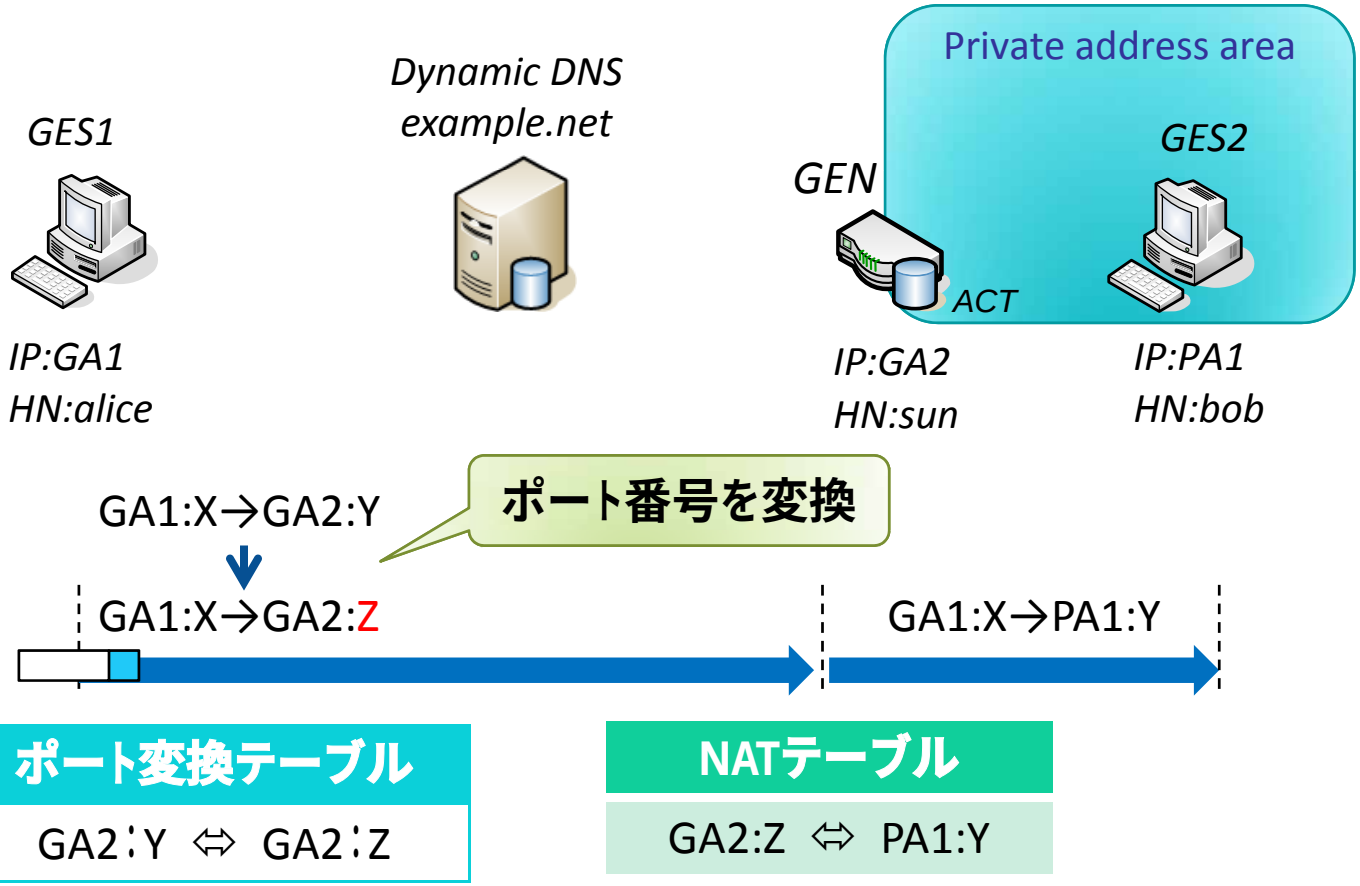
GA1:X ⇔GA2:Z	GA1:X ⇔GA2:Z	GA1:X⇔PA1:Y
暗号化/復号	透過中継	暗号化/復号

ポート変換テーブル	NATテーブル
GA2¦Y ⇔ GA2¦Z	GA2:Z ⇔ PA1:Y

- GES2はGES1が通信相手に見える
- GES1はGENが通信相手に見える

通信相手の見え方によって異なるPITが生成される

通信開始



- GES1はNATにマッピングされたポート番号に変換して送信
- GA空間側から通信開始が可能になる

まとめ

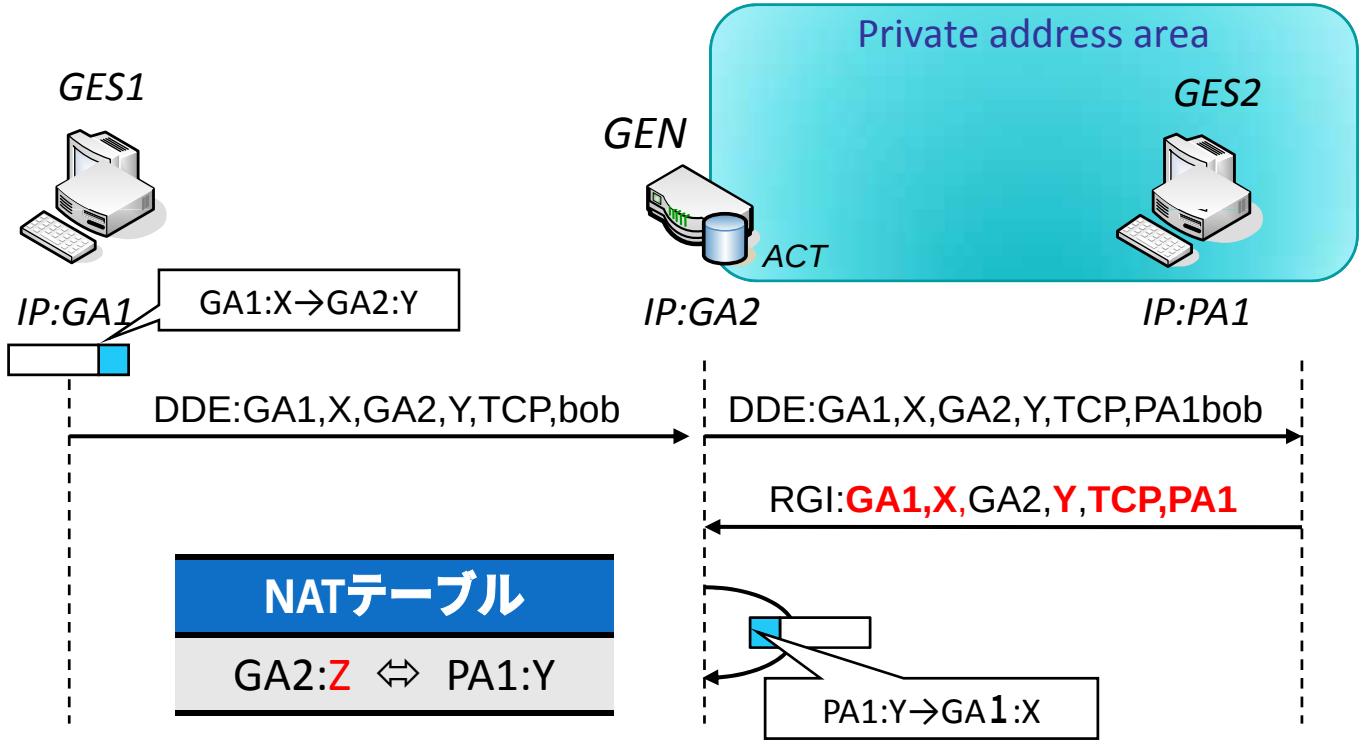
- DPRPの概要
- NAT越え問題
- NAT越えDPRPの提案
  - GA空間からの通信が可能に
  - アドレス空間を意識しないグループ通信を実現

- 今後の予定
  - 提案の実装・性能評価

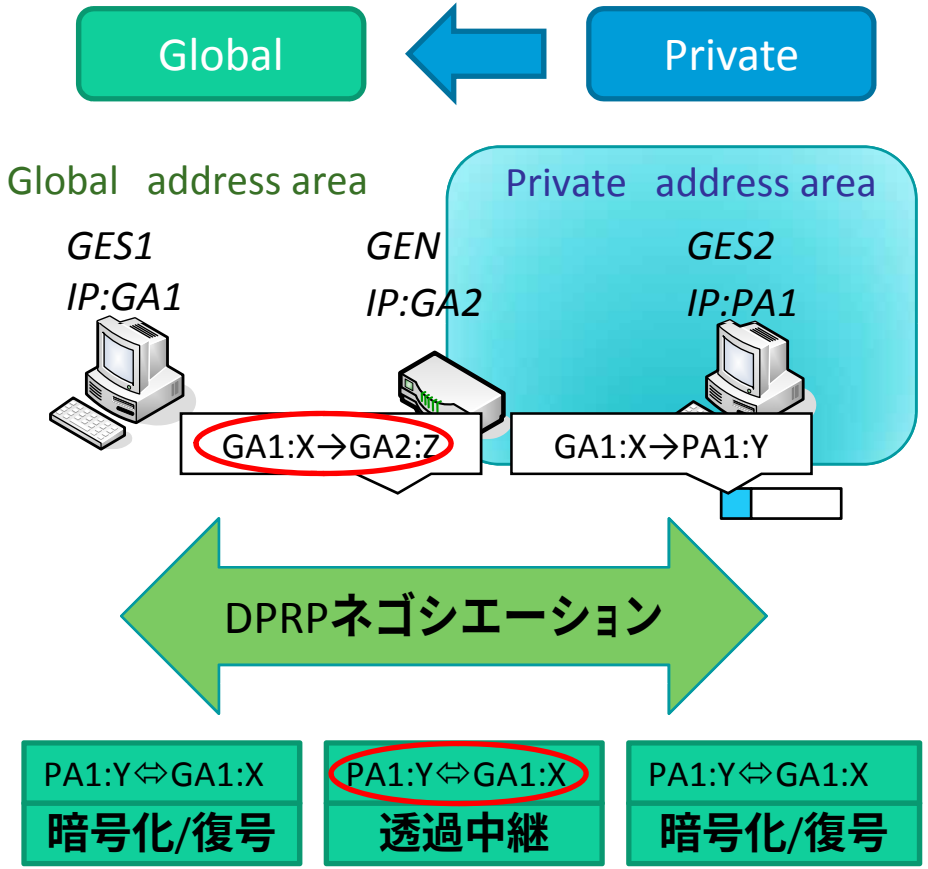
付録

NATテーブル生成方法

- RGIの情報から疑似パケットを生成
  - 通信パケットのコネクション情報とACTで得たIPアドレス
  - GES2からGES1に送信するパケットと見せかけたもの



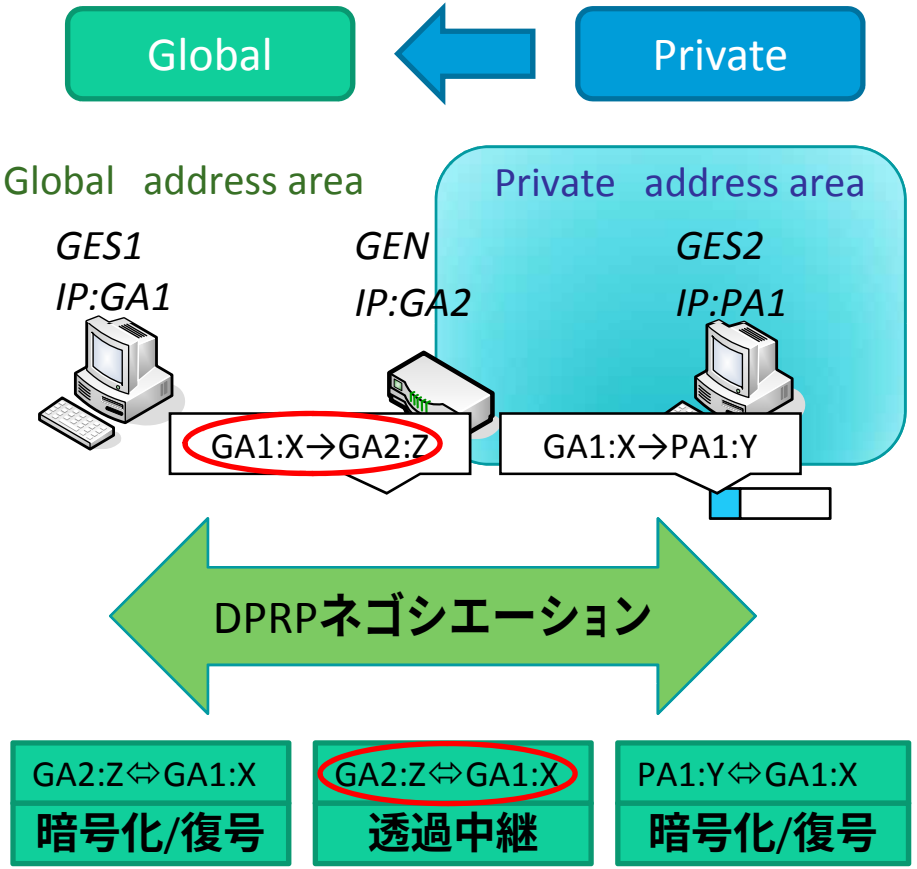
通信経路上にNATがある場合の問題点



- パケットとPITの情報が一致しない
  - 通信パケットのコネクション情報でPITが生成される
  - NATでアドレスとポート番号が変換される

PA空間からGA空間へのDPRP

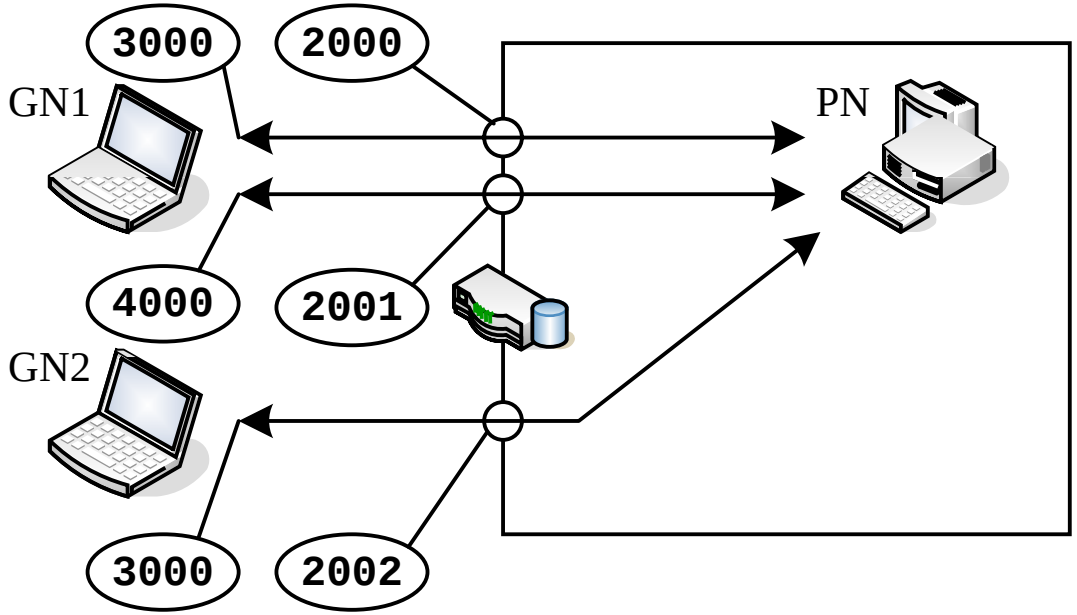
実装済み



- GES1とGENではNATで変換後の情報でPITを生成
- NATでアドレス変換されてもPITが一致
- PA空間からGA空間へのDPRPはすでに実装済み

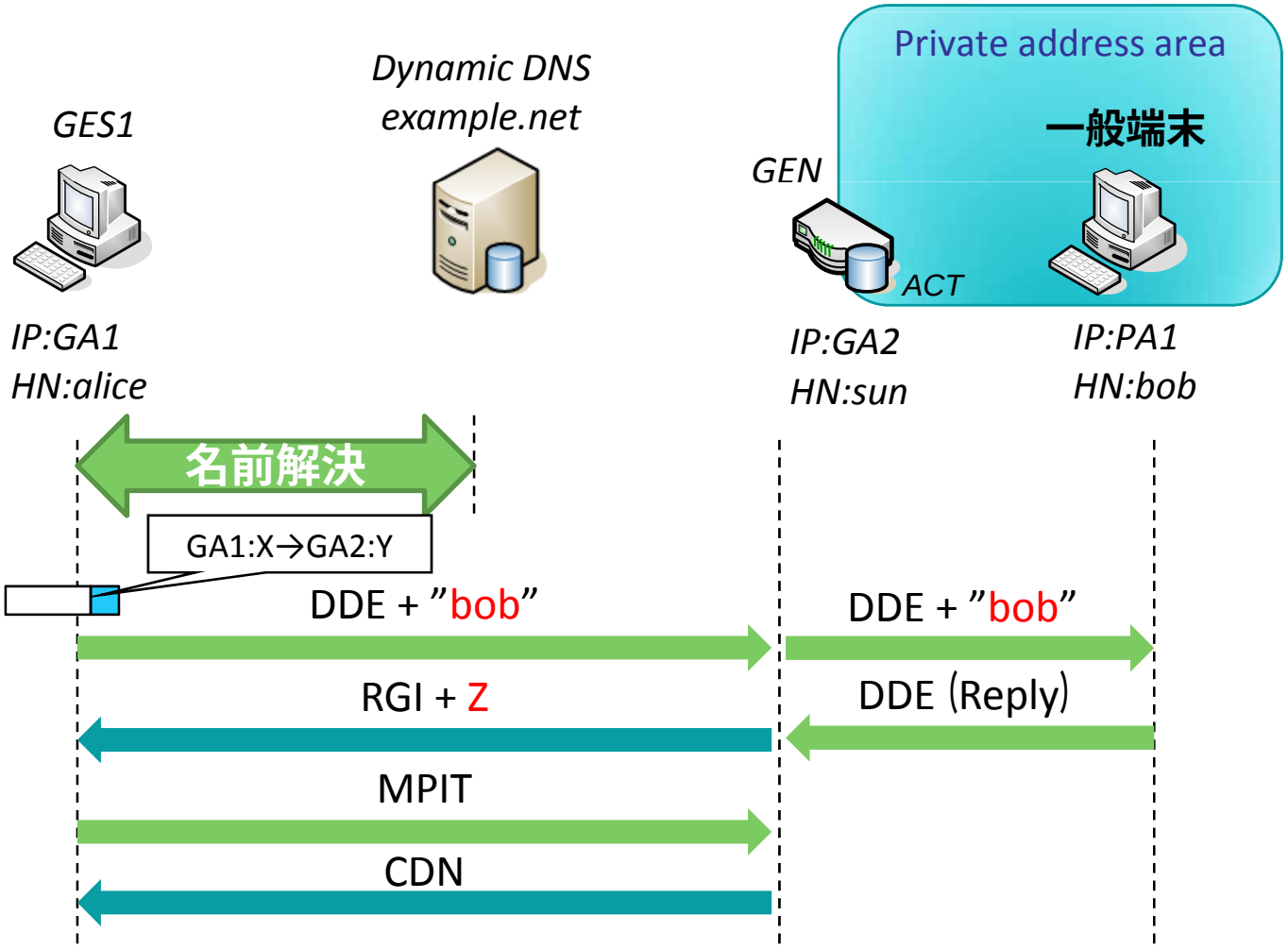
Symmetric NAT

- 宛先ごとに異なるポート番号がマップされる



外部	NATルータ	内部
GN1:3000	NAT:2000	PN:1000
GN1:4000	NAT:2001	PN:1000
GN2:3000	NAT:2002	PN:1000

PA空間の端末が一般端末の場合



◆DDEはICMPのEchoパケット
◆一般端末からReplyが応答される
◆GENが終端GEとなる

ALG (Application Layer Gateway)

- IPアドレスやポートを制御するアプリケーション
  - FTP
  - SIP

➔IPペイロード内にIPアドレス・ポートの情報が記載されており，NAT通過時に変換されない

ALG (Application Layer Gateway) を
NAT-fルータに実装して解決