NAT越えが可能な拡張DPRPの検討

073432016　後藤　裕司
渡邊研究室

1　はじめに

企業ネットワークでは不正侵入，データの盗聴，改竄などの脅威に対するセキュリティ対策が課題となっている．組織外部からの脅威に対しては通信の暗号化やディジタル署名など，セキュリティ強度の高い技術が利用されている．しかし，企業ネットワークのセキュリティ脅威はイントラネット内にも存在しており，多くの不正による犯罪が報告されている．イントラネット内のセキュリティ対策は，ユーザ名とパスワードによる簡単な認証，アクセス制御しかされていない場合が多く，今後有効な対策が必要となると考えられる．そこで，この様な状況に対応するために通信グループの構築が有効であると考えられる．通信グループを構築することができるセキュリティ技術として IPsec がある．しかし，端末が移動するなどしてシステム構成が頻繁に変わるような環境では，それに応じて IKE の設定情報を変更する必要がある．そのため管理者の負担が大きく，IPsec はイントラネット内ではほとんど利用されていない．そこで，我々はシステム構成が変化しても端末や中継装置が自身がその変化に動的に対応することができる DPRP（Dynamic Process Resolution Protocol）と呼ぶプロトコルを提案している [1]．DPRP は通信に先立ってネゴシエーションを行い，通信経路上に存在する装置が情報を交換することにより，パケットの暗号化処理や破棄などの通信の処理を決める動作処理情報を動的に生成する．しかし，既存の DPRP は通信経路上に NAT が介在すると動作することができない．

そこで，本稿ではこの課題を解決するための方法を提案する．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）[2] と組み合わせることにより NAT 越えが可能な拡張 DPRP を実現した．

2　DPRP とその課題

DPRP を実装した装置を GE と呼び，各端末にインストールされるソフトウェアタイプの GES（GE realized by Software），一般端末を保護することができるルータタイプの GEN（GE for Network）がある．

GE は，通信パケットの送信時に自身が保持する動作処理情報のテーブル PIT（Process Information Table）を検索する．PIT には送信元/宛先の IP アドレス，ポート番号，プロトコル番号とパケットの処理内容を示した動作処理情報（暗号化/復号，透過中継，破棄）などの情報が記載されている．検索には通信パケットのコネクション識別子 CID（Connection IDentification : 送信元/宛先の IP アドレス，ポート番号，プロトコル番号の組）を用いて PIT の検索を行う．該当する PIT がない場合はパケットを一時的に待避して DPRP を実行することにより PIT の生成を行う．DPRP は 4 つの制御パケット DDE(Detect Destination End GE)，RGI(Report GE Information)，MPIT(Make Process Information Table)，CDN(Complete DPRP Negotiation) を用いて図 1 に示す 2 往復のネゴシエーションを行う．DDE は通信相手に最も近い GE を特定する．RGI は，通信経路上の各 GE の情報を収集する．収集した情報から動作処理情報を決定し，MPIT により各 GE に対して動作処理情報の通知と PIT の登録を行う．そして，CDN により DPRP ネゴシエーション終了を各 GE に知らせる．

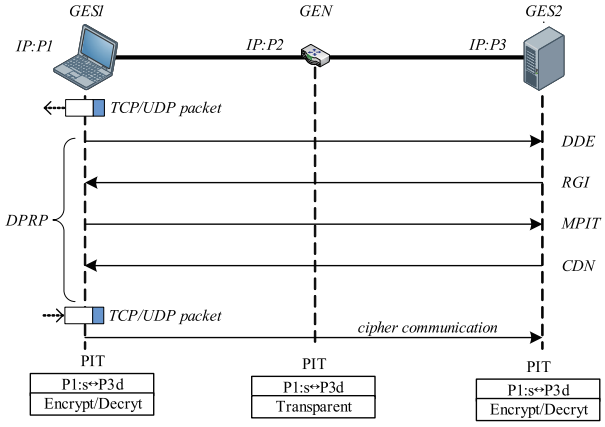


図 1: DPRP の動作概要

各 GE に生成される PIT には，DPRP のトリガとなった通信パケットのコネクション識別子から生成される．しかし，通信経路上に NAT が介在すると，通信パケットの IP アドレスとポート番号が NAT により変換されてしまうため変換後のコネクション識別子と PIT の内容が一致しないという問題が発生する．また，NAT 越え問題というグローバル空間側の端末からプライベートアドレス空間側の端末に通信を開始できない NAT 越え問題もある．

3　提案方式

3.1　拡張 DPRP の動作概要

拡張 DPRP では新たに GNAT と呼ぶ装置を導入する．GNAT は GEN に NAT 機能を追加した装置である．

拡張 DPRP のシステム構成と初期情報を示す．グローバルアドレス空間に GES1，GNAT の配下にプライベートネットワークの GES2 が存在する．GNAT には配下の端末のホスト名と IP アドレスの関係およびアクセスの可否をアクセス制御テーブル ACT に登録しておく．DDNS サーバには PA 空間の端末 GES2 のホスト名 “alice” と GNAT の IP アドレス “G2” を関連づけて登録しておく．

図 2 に拡張 DPRP の動作を示す．GES1 は GES2 と通信を行うために DDNS サーバに名前解決を依頼する．DDNS サーバは GNAT の IP アドレス “G2” を応答する．GES1 はこれを受信すると IP 層において “G2” を仮想アドレス “V1” に書き換えて上位層に通知する．そのため，上位ソフトウェアは通信相手が仮想アドレス “V1” だと認識する．その後，GES1 は上位層から仮想アドレス宛のパケットを IP 層で受け取るとパケットをカーネル内に待避し DPRP ネゴシエーションを開始する．まず最初の DDE パケットにコネクション識別子（G1:s → V1:d）と GES2 のホスト名 “alice” を記述して GNAT に送信する．GNAT はこれを受信するとホスト名 “alice” をキーにして ACT の検索を行う．ACT に “alice” のホスト名がある場合は，関連づけられた GES2 のプライベート IP アドレス “P1” を取得し，DDE パケットを GES2 に転送する．GES2 は DDE を受

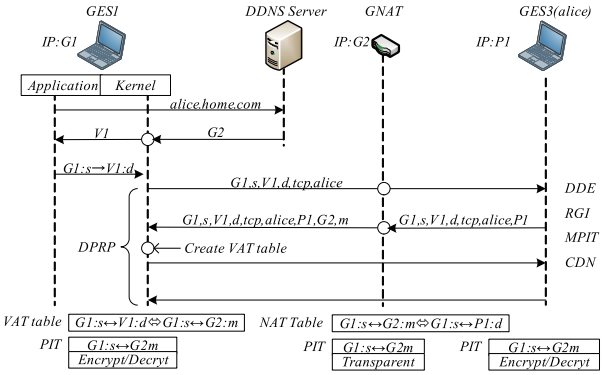


図 2: NAT 越え DPRP の動作

信後，RGI パケットを生成する．RGI パケットに GES2 の IP アドレス “P1” を追加して GES1 宛に送信する．GNAT はこれを受信すると RGI の内容から強制的に NAT テーブルを生成する．

｛G1:s↔G2:m ⇔ G1:s↔P1:d ｝

GNAT はこの時 NAT にマッピングされたポート番号を “m” を RGI に追加して GES1 に送信する．GES1 はこれを受信すると，GES2 に対応づけられた仮想アドレス “V1”，ポート番号 “d” と GNAT の IP アドレス “G2”，ポート番号 “m” の変換関係が記された VAT（Virtual Address Translation ）テーブルを生成する．

｛G1:s↔V1:d ⇔ G1:s↔G2:m ｝

以下の MPIT，CDN の処理は既存の DPRP と同様である．各 GE に生成される PIT は次に示す NAT に対応した PIT となる．

3.2 NAT に対応した PIT

通信経路上に NAT が介在する場合は，NAT により通信パケットの IP アドレスとポート番号が変換される．この様な場合の PIT は，通信相手の見え方によって各 GE ごとに異なる内容となる．これを NAT に対応した PIT と呼ぶことにする．GES3 は，GES1 が通信相手に見えるため GES1 と GES3 に対応した PIT となる．GES1 は，通信相手が GNAT に見えるため GES1 と GNAT に対応した PIT となる．GNAT においては PIT を作る方法としてはグローバルアドレス側で作る方法とプライベートアドレス側で作る方法がある．NAT 処理はアプリケーションに近い部分で実行されるため，拡張 DPRP ではグローバルアドレス側，すなわち GES1 と GNAT に対応した PIT を生成することにした．

4 実装と評価

4.1 実装

拡張 DPRP を FreeBSD7.0-Release の IP 層に実装した．図 3 に GES の実装概要を示す．DPRP は IP 層の入出力関数 ip_input(), ip_output() から呼び出され，処理を終えたら差し戻す仕組みになっているため，既存のカーネル処理には影響を与えない．GES のモジュールには新たに VAT 処理モジュールの追加を行った．図 4 に GNAT の実装概要を示す．GNAT には新たに ACT 処理モジュールを追加し，さらに FreeBSD 標準の NAT デーモン natd を動作させる．GNAT が受信したパケットは divert ソケットを通じて natd で NAT のアドレス変換処理が行われる．natd は改造を必要とせず，そのまま利用することができる．GNAT では DPRP モジュールはグローバル側のインタフェースのみから呼び出される．

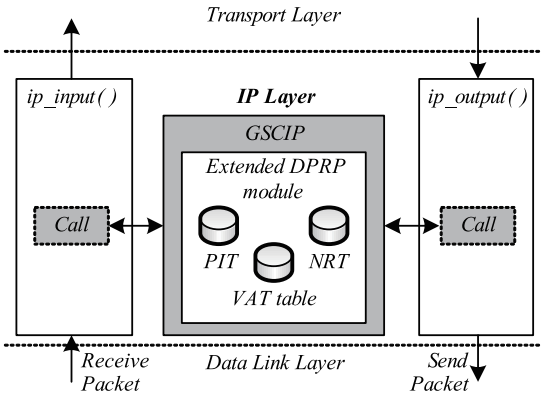


図 3: GES の実装概要

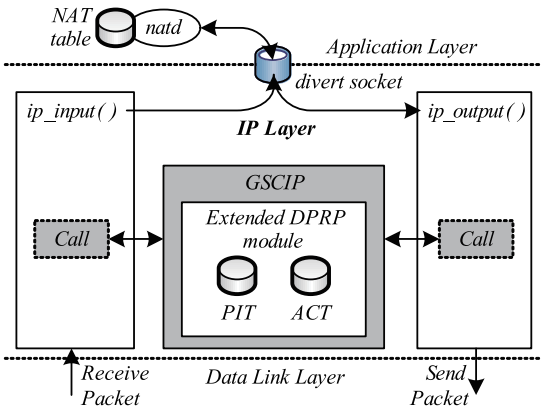


図 4: GNAT の実装概要

4.2 スループット

拡張 DPRP を実装しない場合と実装した場合の 100BASE 環境におけるスループットを測定した．測定には Netperf を用いてメッセージサイズを変えて 10 回の平均値を取った．表 1 に結果を示す．100BASE 環境の結果ではいずれも 94.1Mbps となり拡張 DPRP の実装を行ってもスループットに変化がないことが分かる．

表 1: スループットの結果

拡張 DPRP 実装	スループット
なし	94.1（Mbps）
あり	94.1（Mbps）

5 まとめ

本稿では DPRP を拡張し NAT 越えを可能とする拡張 DPRP の提案を行った．提案方式を実装し評価を行った結果，実装によるオーバヘッドはほとんどないことを確認することができた．

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解決プロトコル DPRP の実装と評価，情報処理学会論文誌， Vol. 47, No. 11, pp. 2976–2991 (2006).

[2] 鈴木秀和，渡邊　晃：外部動的マッピングにより NAT 越え通信を実現する NAT-f の提案と実装，情報処理学会論文誌，pp. 3949–3961 (2007).

NAT越えが可能な拡張DPRPの検討

名城大学
渡邊研究室
後藤　裕司

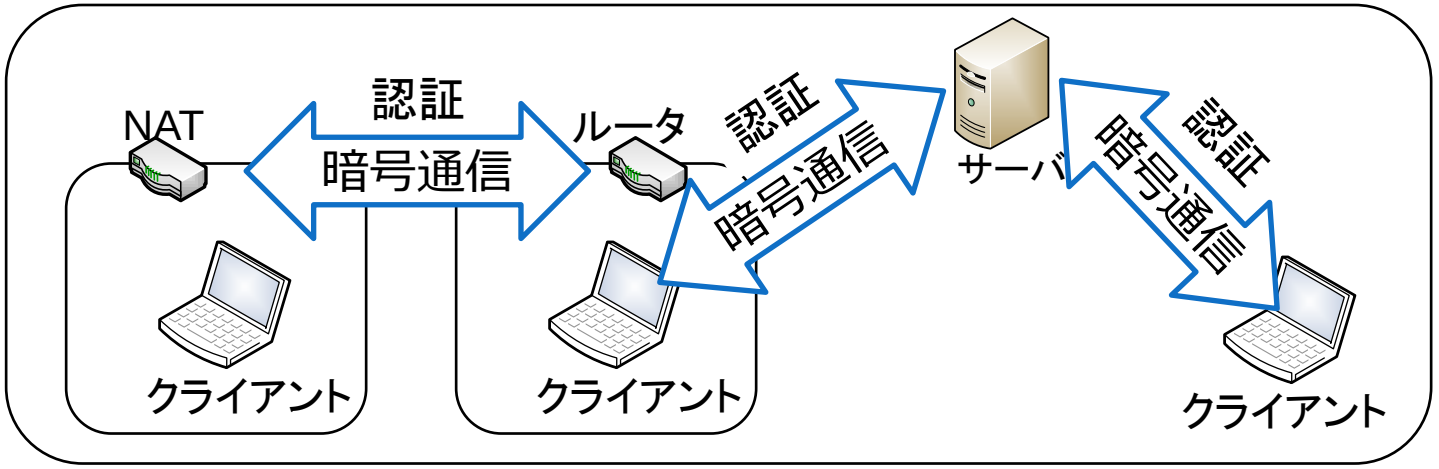
研究背景

- 不正侵入，データの盗聴・改ざん
- 外部から脅威に対しては強固
  - ファイアウォール
  - 通信の暗号化
  - ディジタル署名など
- 内部のセキュリティ対策は・・・
  - ユーザ名やパスワードによる簡単な認証
  - アクセス制御

これらの脅威に対して通信グループの構築が有効

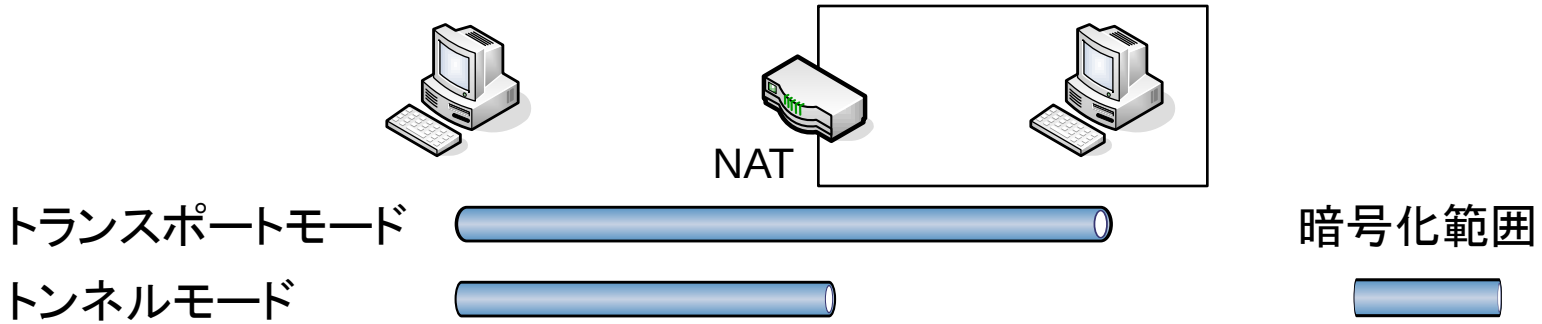
グループ通信に求めること

- 通信相手と確実な認証
- 通信内容の暗号化
- あらゆる環境で利用可能
  - 個人単位とドメイン単位が混在
  - 通信経路上にNATがある場合
    - 企業内でもセキュリティのために利用される
  - 一般家庭でもグループ通信を利用



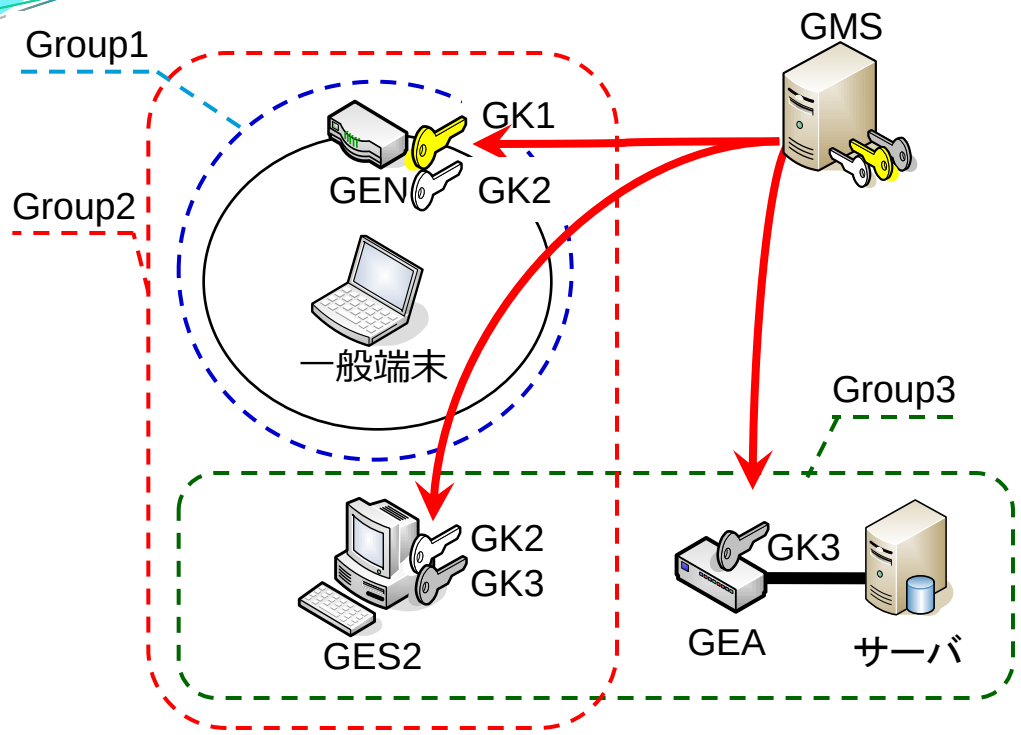
IPsecを利用する場合の問題点

- トランスポートモードとトンネルモードで互換性がない
- 個人単位とドメイン単位の通信グループが混在するような環境では利用は設定が煩雑
- NATと相性が悪い
  - NATによりアドレスとポート番号が変換されるため偽造パケットと判断される



柔軟かつセキュアなグループ通信を実現する
GSCIP(*Grouping for Secure Communication for IP*)

GSCIPの概要



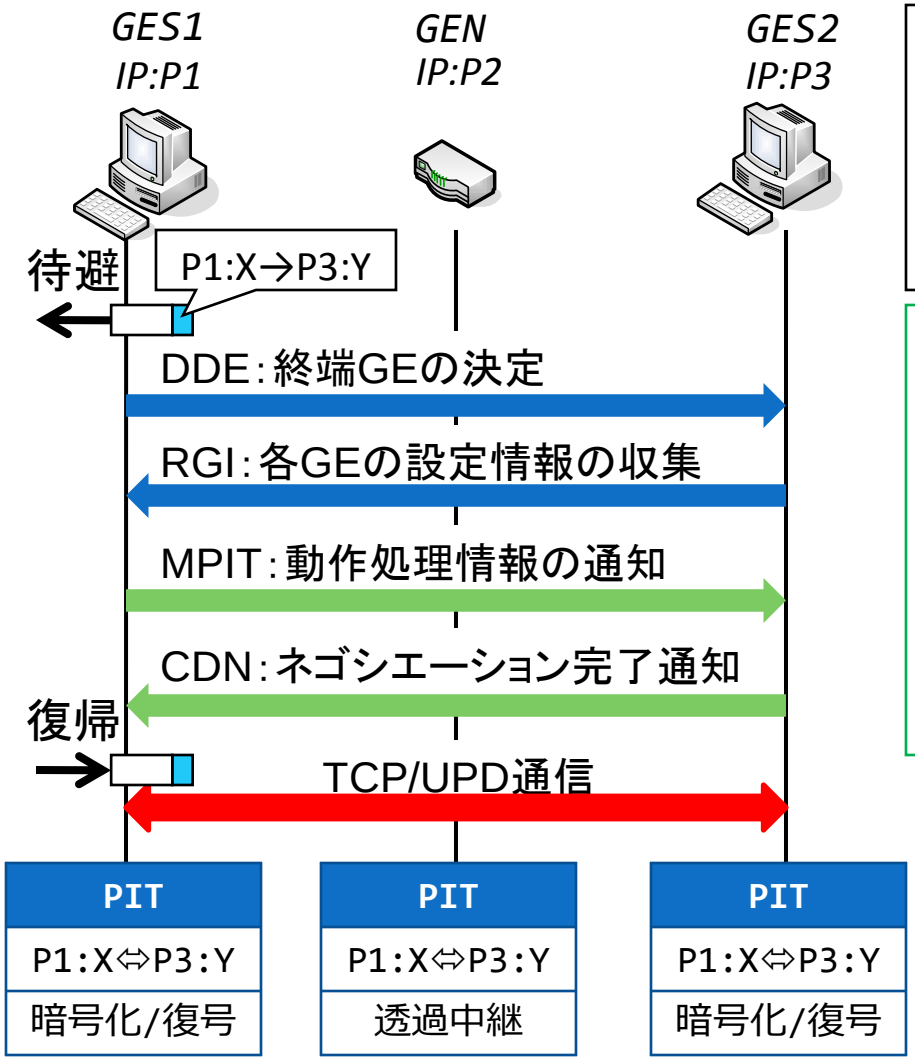
GE：GSCIP対応した装置
GES(Software型):ホストタイプ
GEN(Network型):ルータタイプ
GEA(ブリッジ型)：ブリッジタイプ
GMS：グループ管理装置

- 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*)

- 通信開始時にDPRPネゴシエーションを実行



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

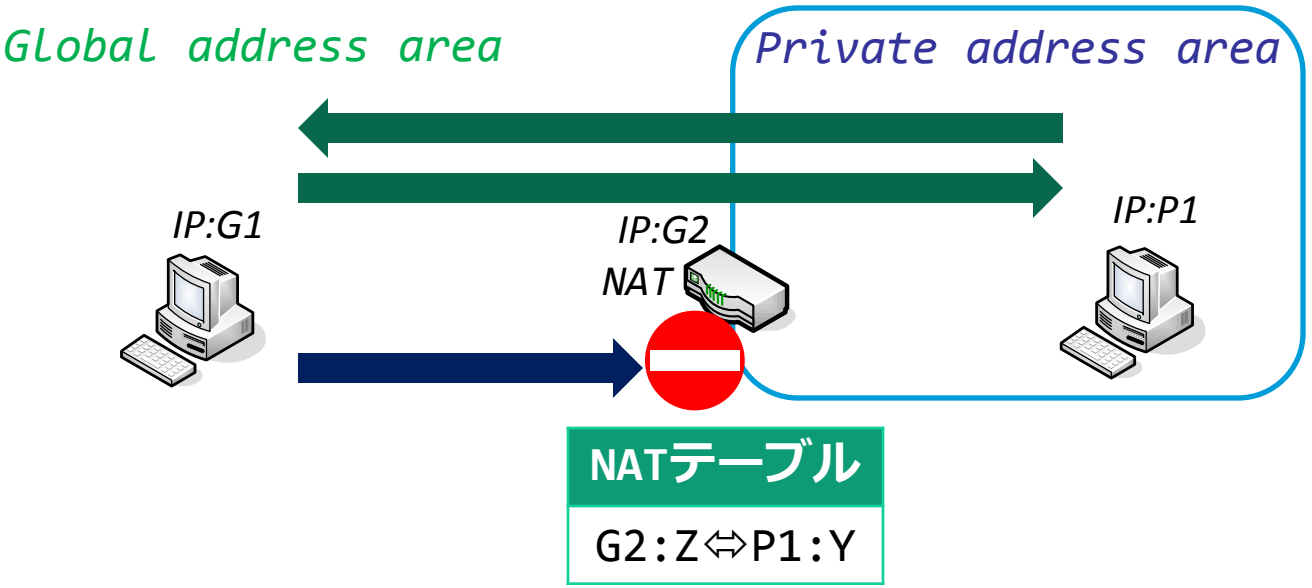
- グループ情報の収集
- 相手認証
- 動作処理情報テーブルPIT（Process Information Table）の生成
  - 暗号化/復号，透過中継，破棄
- PITに従ってパケットを処理

各GEに生成されるPITは同一のコネクション情報となる.

コネクション情報（送信元/宛先IPアドレス，ポート番号，プロトコル番号）

通信経路上にNATがある場合の問題点

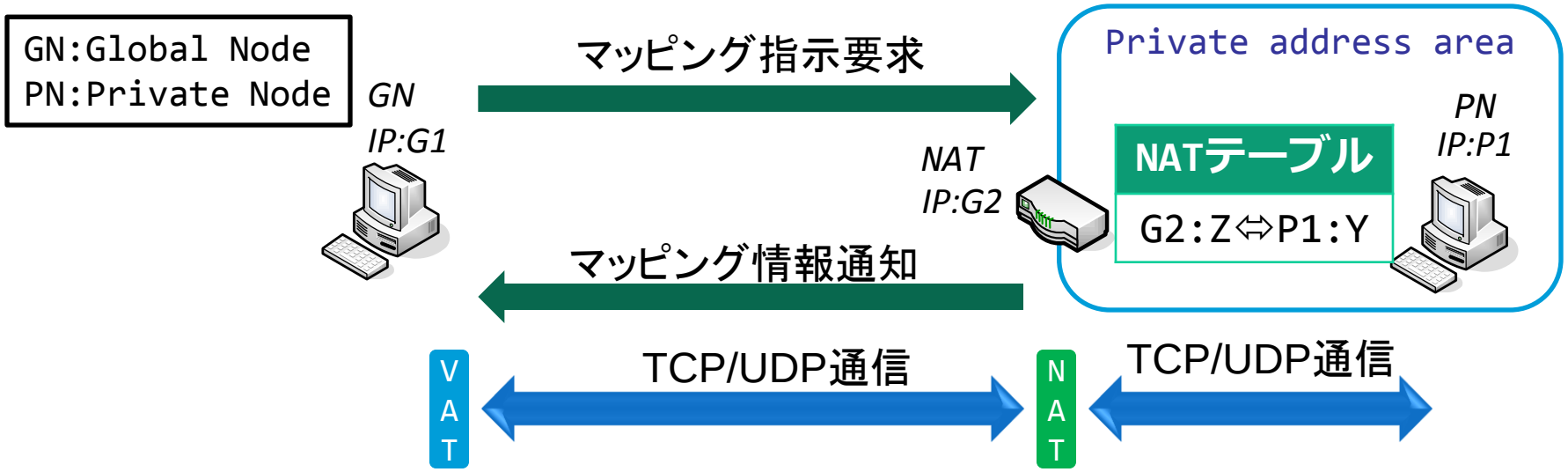
- PITとパケットのコネクション情報が一致しない
  - NATによるアドレス・ポートの変換に対応していない
- NAT越え問題
  - グローバルアドレス(GA)空間側からプライベートアドレス（PA）空間側に通信開始できない



NAT-fの仕組みを追加することでNAT越えを実現

NAT-f（NAT-free protocol）

- NAT越えを実現するためのプロトコル
  - 通信相手を仮想IPアドレスで認識
  - 外部ノードからNATに対してマッピング処理を指示
  - 仮想IPアドレスをマッピング情報に変換するVAT（Virtual Address Translation）テーブルを作成



DDEとRGIにNAT-fの仕組みを追加

拡張DPRP：事前設定

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

Dynamic DNS

*RR (*Resource Records)

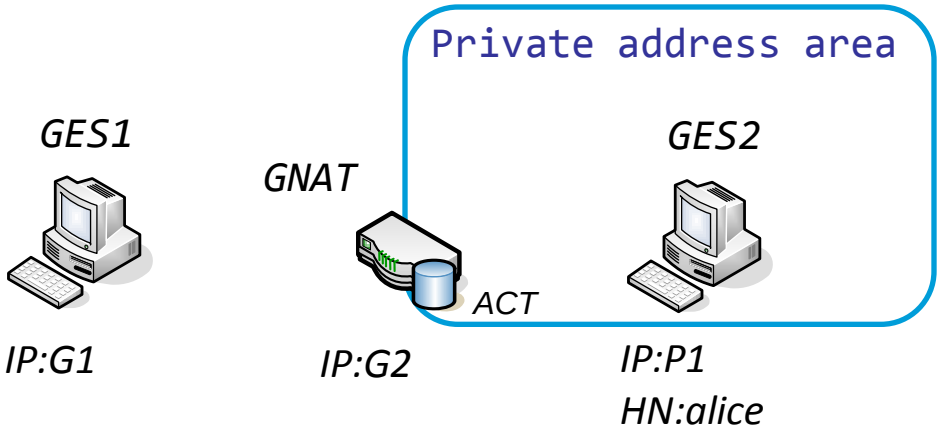
Name	IP
alice	G2

- GNAT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

GNAT:GENにNAT機能を追加

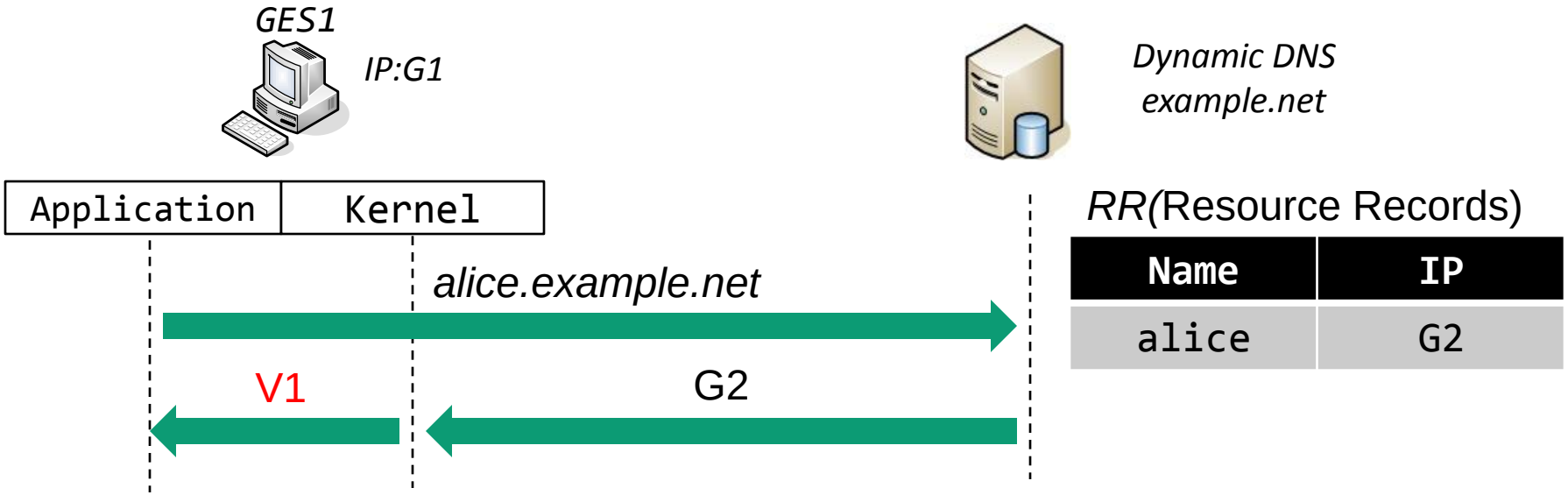
ACT（Access control table）

Name	IP	Authorization
alice	P1	allow



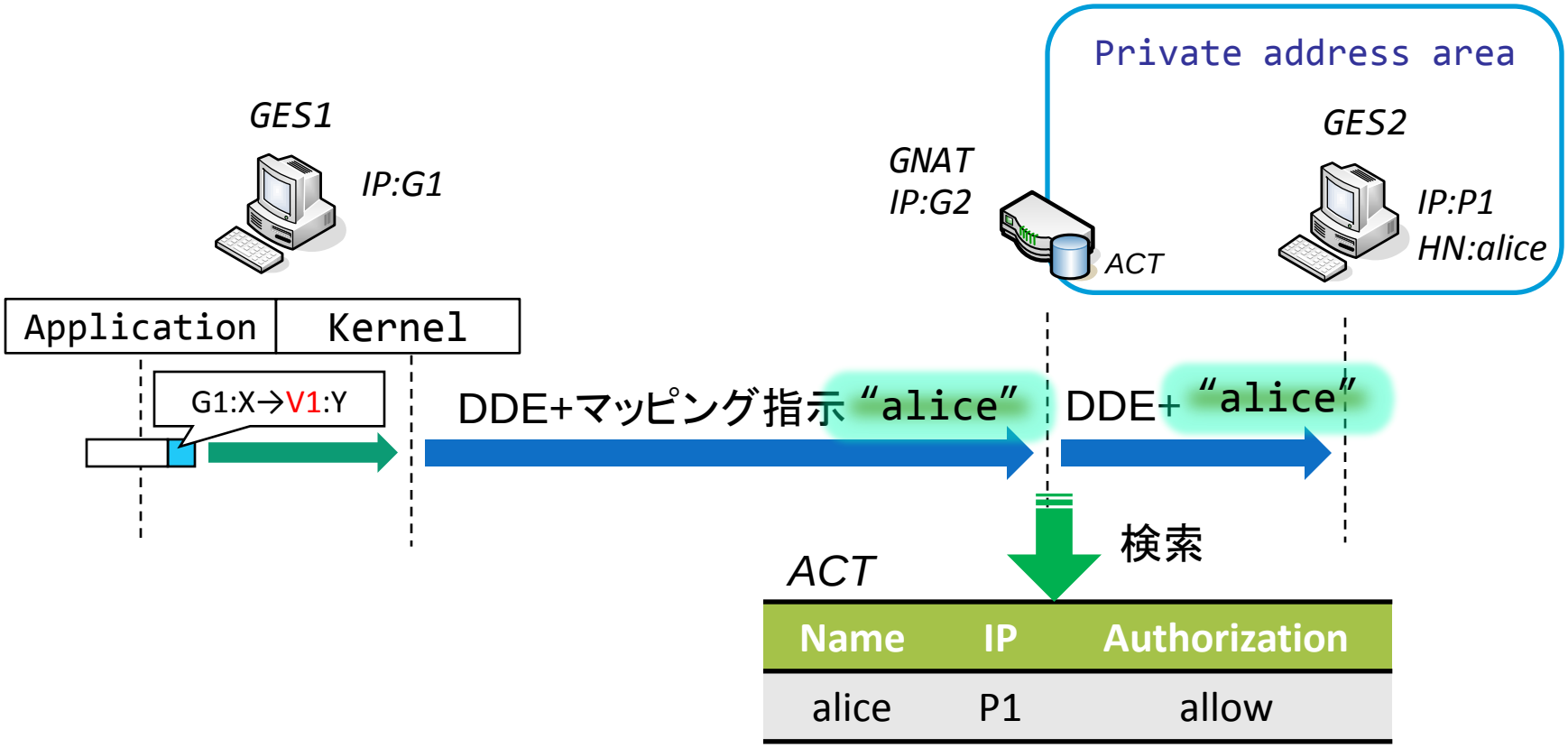
名前解決処理

- 取得IPアドレスを仮想IPアドレスに書き換え



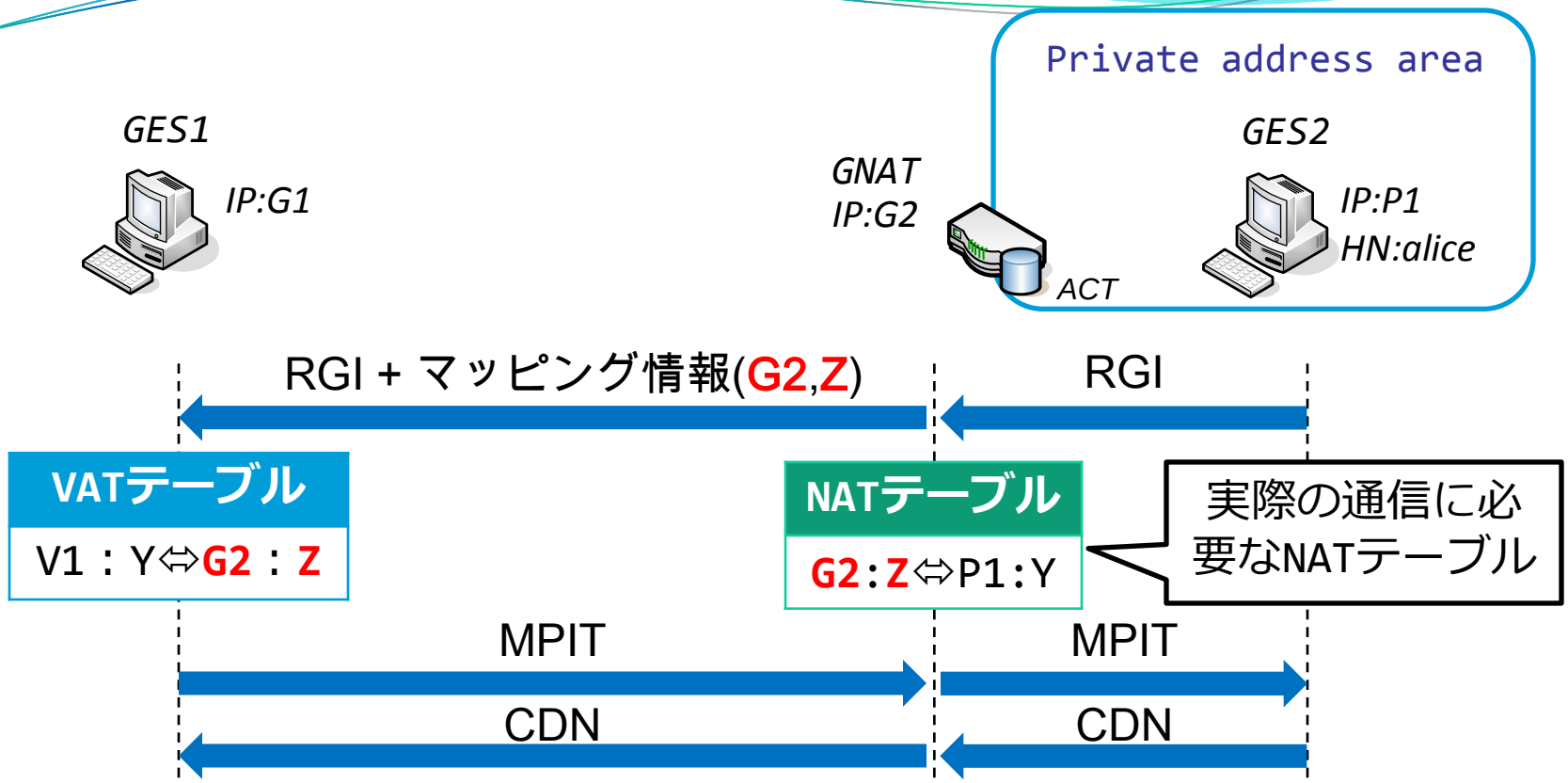
- 仮想IPアドレスはNAT配下の端末を特定するために利用

拡張DPRPネゴシエーション



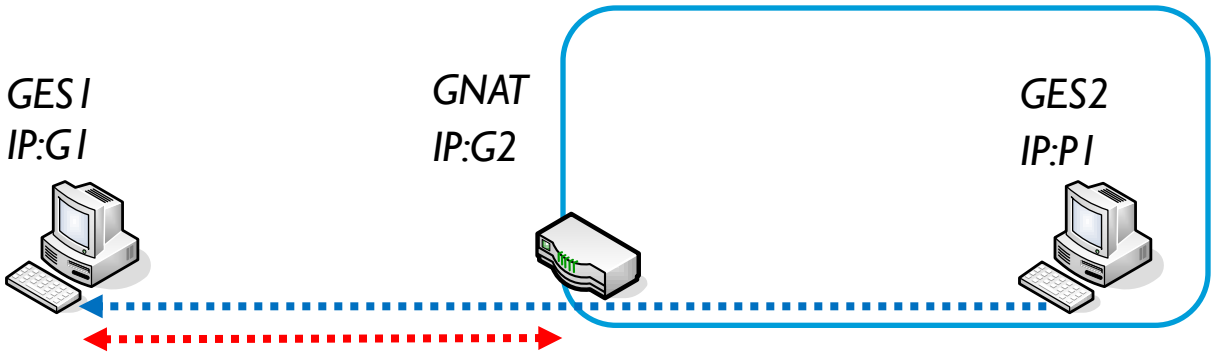
- マッピング指示に必要なホスト名を追加
- ホスト名を用いてACT検索
  - 対応するホスト名のIPアドレスを取得

拡張DPRPネゴシエーション



- GES1とGES2に対応するNATテーブルを生成
- VATテーブルを生成
  - 仮想アドレスをNATにマッピングされた情報に変換

NATに対応したPIT



PIT
G1:X⇔G2:Z
暗号化/復号

PIT
G1:X⇔G2:Z
透過中継

PIT
G1:X⇔P1:Y
暗号化/復号

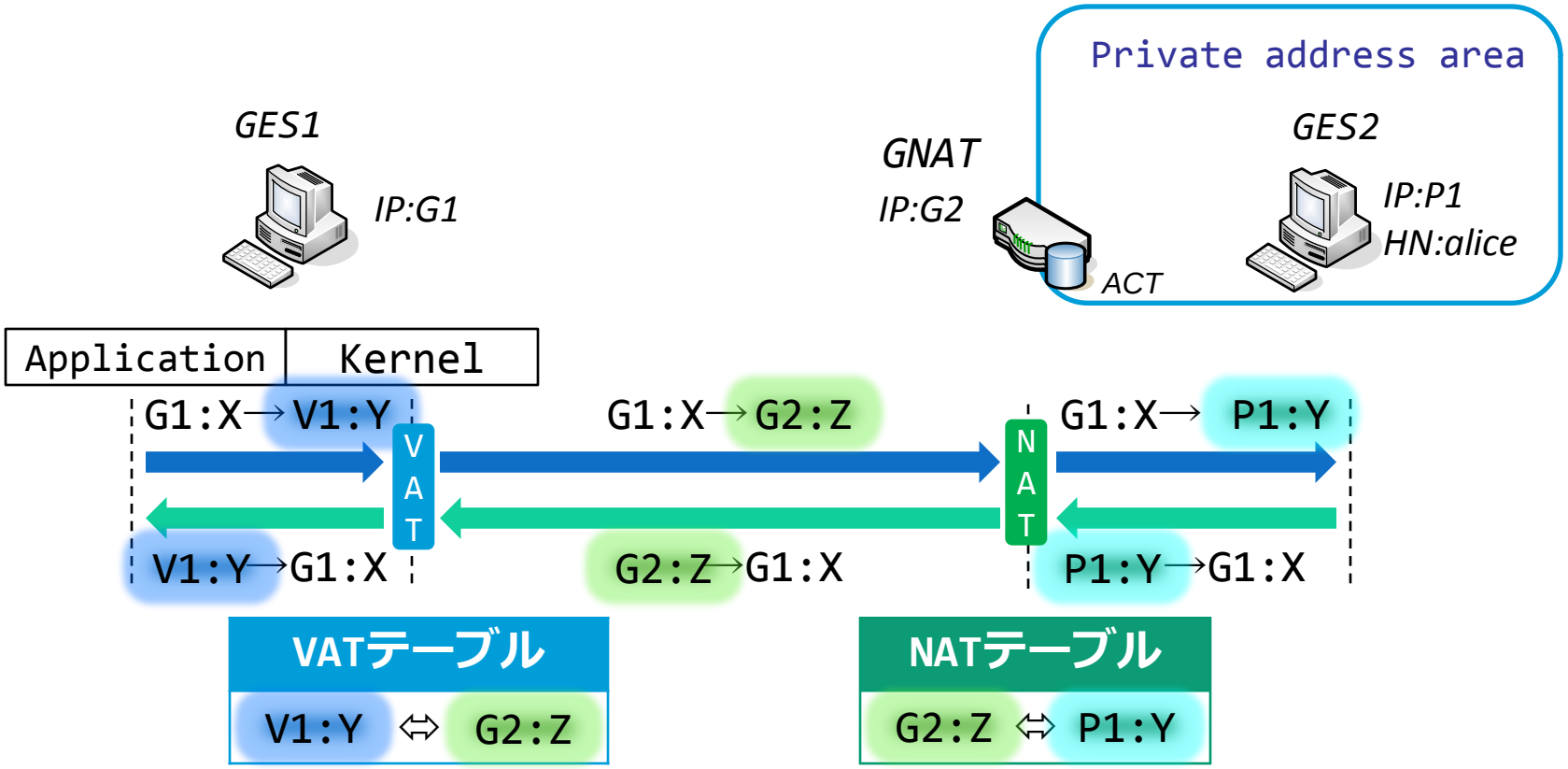
VATテーブル
V1 : Y⇔G2 : Z

NATテーブル
G2:Z⇔P1:Y

- GES2はGES1が通信相手に見える
- GES1はGNAT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を生成

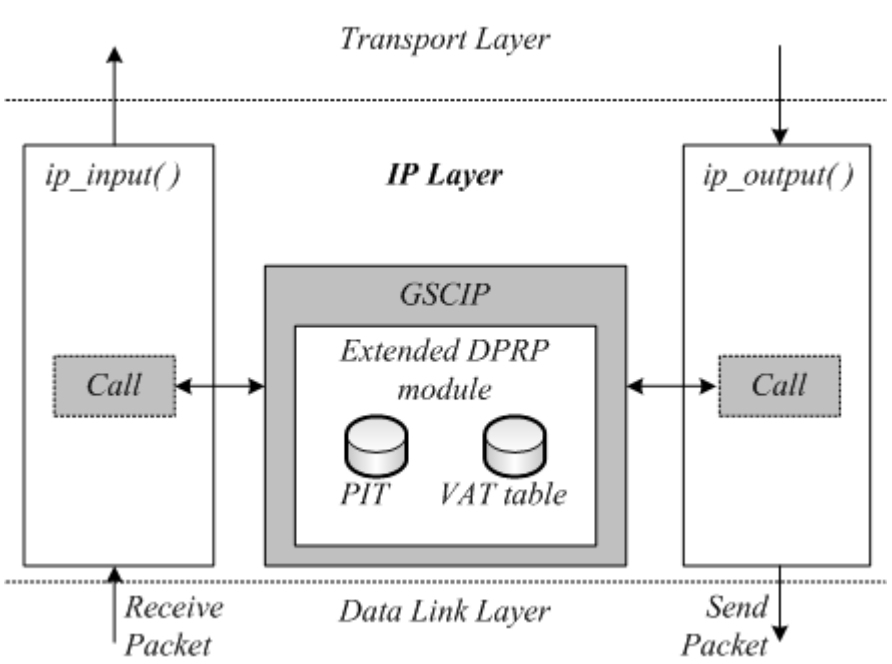
アドレス変換処理



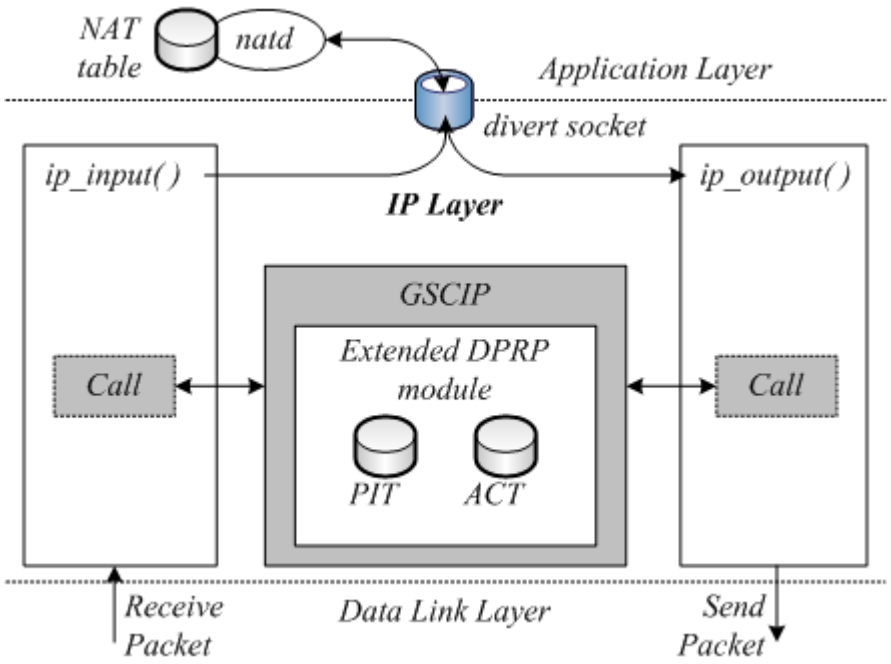
- GES1はNATにマッピング情報に変換して送信
- GA空間側から通信開始が可能になる

実装

- FreeBSDのカーネルにモジュールを組み込む
- IP層の入出力時に呼び出し，処理を終えたら差し戻す方式
- IP層で行われる処理に変更を加えない
- GNATはグローバル側のインターフェイスのみで処理



GESの実装概要

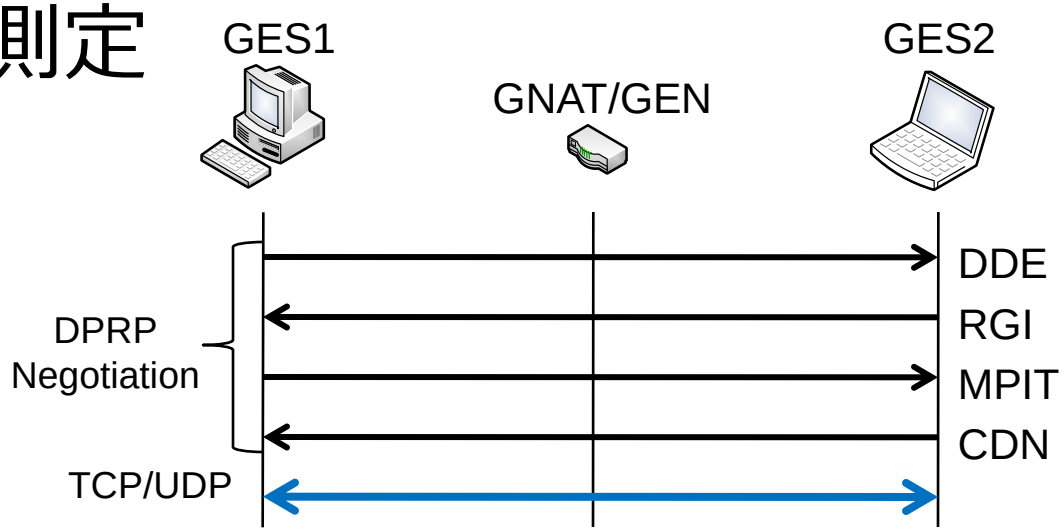


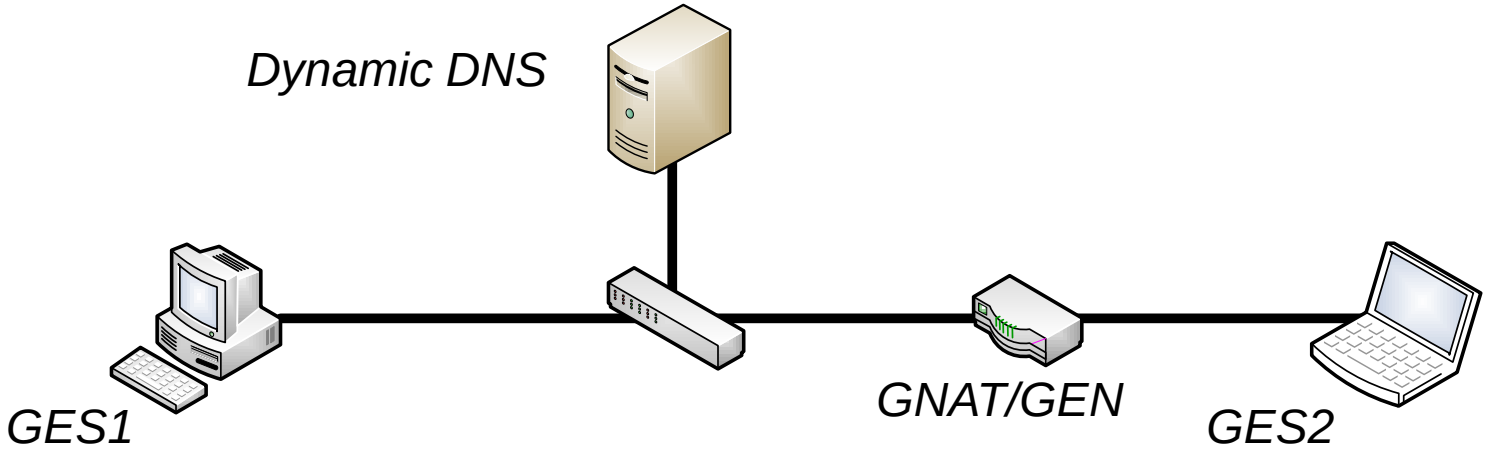
GNATの実装概要

性能測定

- DPRPネゴシエーション時間
- スループットの測定
  - Netperfを利用

```
OS:FreeBSD7.0
CPU：Pentium4 3.0GHz
Memory：512MB
Ethernet:100BASE-TX
```





性能測定

- DPRPの処理時間(10回試行の平均値)

	ネゴシエーション時間	通信開始までの時間
GEN	1010μsec	1025μsec
GNAT	1144μsec	1162μsec

- スループット(10回試行の平均値)

実装なし	94.1Mbps
実装あり	94.1Mbps

DPRPが通信に与える影響はほとんどない

まとめ

- DPRPの概要
- 経路上にNATがある場合の問題点
  - パケットとPITのコネクション情報内容が一致しない
  - NAT越え問題
- NAT越えDPRP
  - NAT-fの仕組みを追加
  - アドレス空間を意識しないグループ通信を実現
  - 通信に与える影響はほとんどない
- 今後の予定
  - DPRPをIPv6に対応

付録

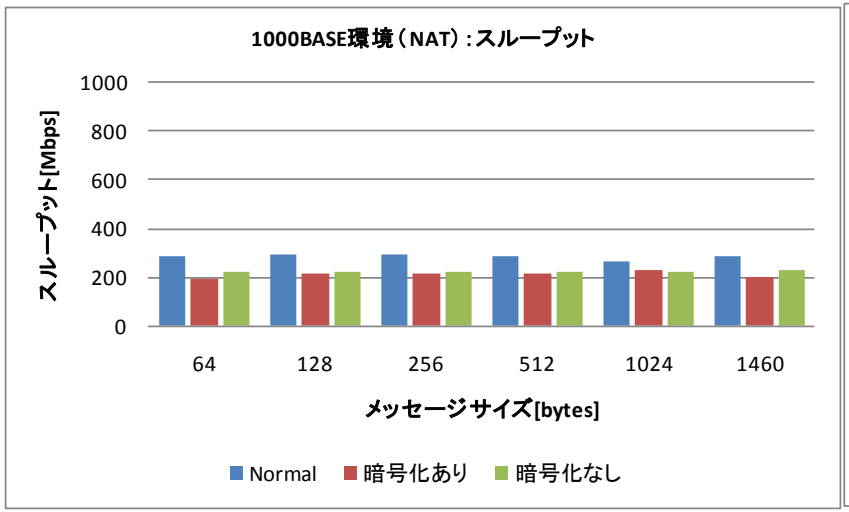
PCCOM (Practical Cipher COMmunication)

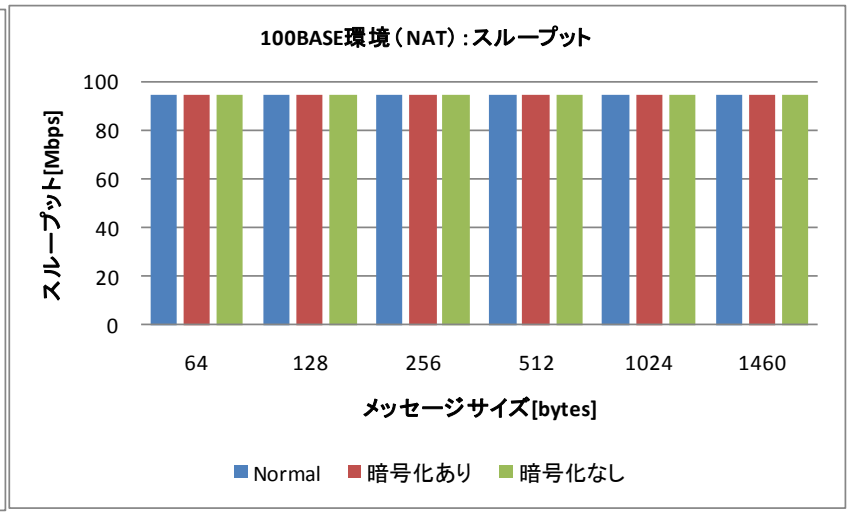
- NA(P)T，ファイアウォールを通過できる
  - 暗号化範囲はユーザデータ部分のみ
  - 完全保証の範囲はIPヘッダから
    - PITの検索過程で保証

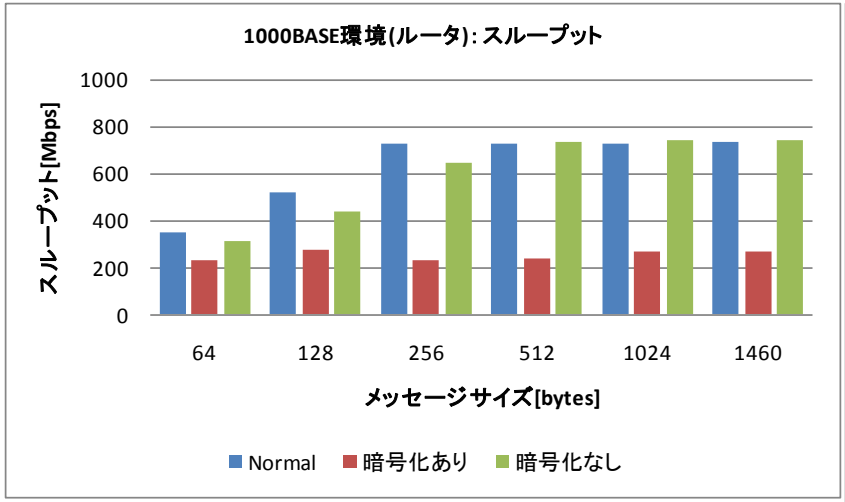
- パケット長変化しない
  - PCCOMによるフラグメントは発生しない
  - 任意長のデータを暗号化できるブロック暗号を採用

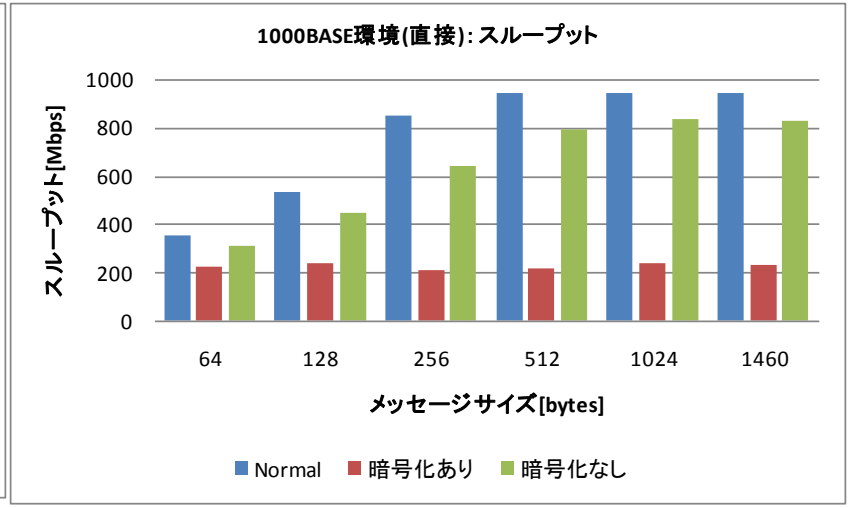
NATやファイアウォールと共存できる暗号化通信方式PCCOMの提案と実装
情報処理学会論文誌,Vol.47,No7,pp.2258-2266,jul.2006.

スループット結果

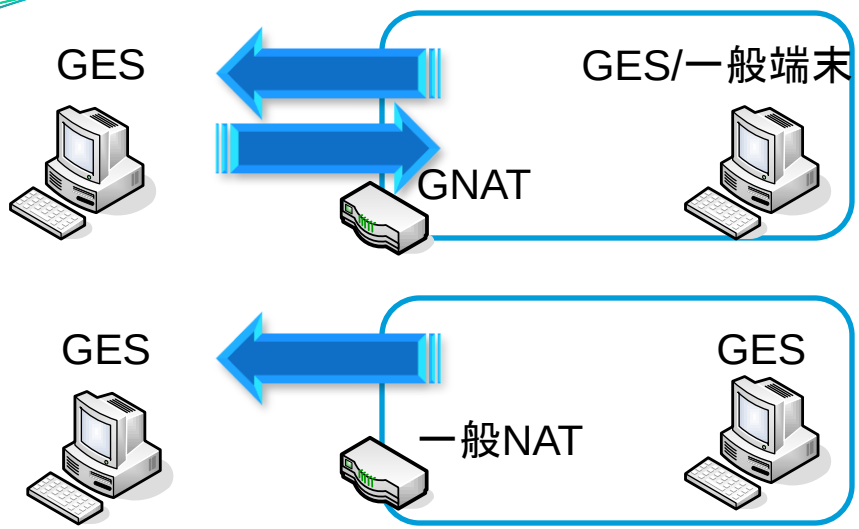

1000BASE環境（NAT）：スループット
スループット[Mbps]
1000
800
600
400
200
0
64
128
256
512
1024
1460
メッセージサイズ[bytes]
Normal
暗号化あり
暗号化なし

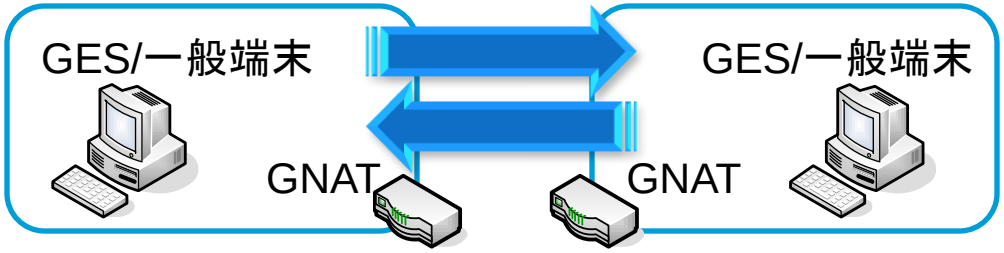

100BASE環境（NAT）：スループット
スループット[Mbps]
100
80
60
40
20
0
64
128
256
512
1024
1460
メッセージサイズ[bytes]
Normal
暗号化あり
暗号化なし

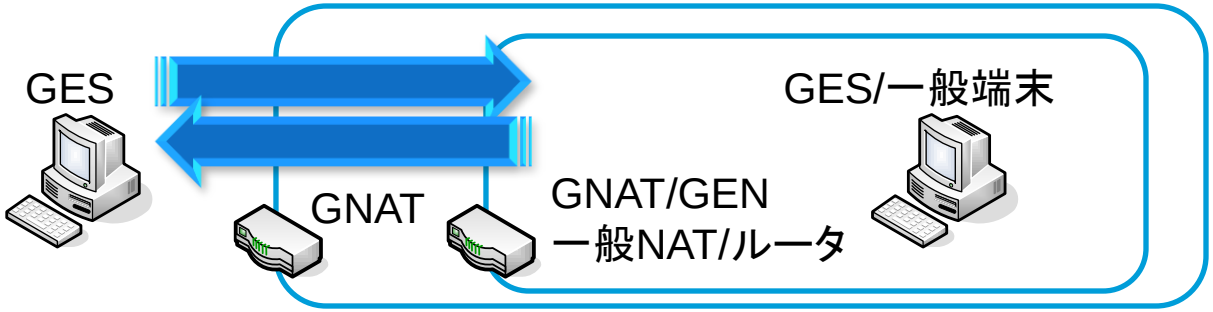

1000BASE環境(ルータ)：スループット
スループット[Mbps]
1000
800
600
400
200
0
64
128
256
512
1024
1460
メッセージサイズ[bytes]
Normal
暗号化あり
暗号化なし

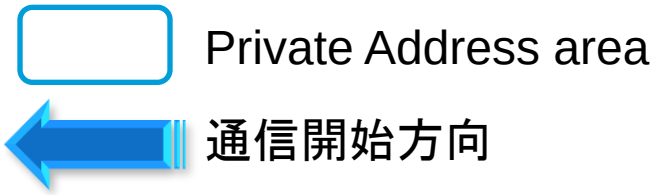

1000BASE環境(直接)：スループット
スループット[Mbps]
1000
800
600
400
200
0
64
128
256
512
1024
1460
メッセージサイズ[bytes]
Normal
暗号化あり
暗号化なし

DPRPが利用可能な環境



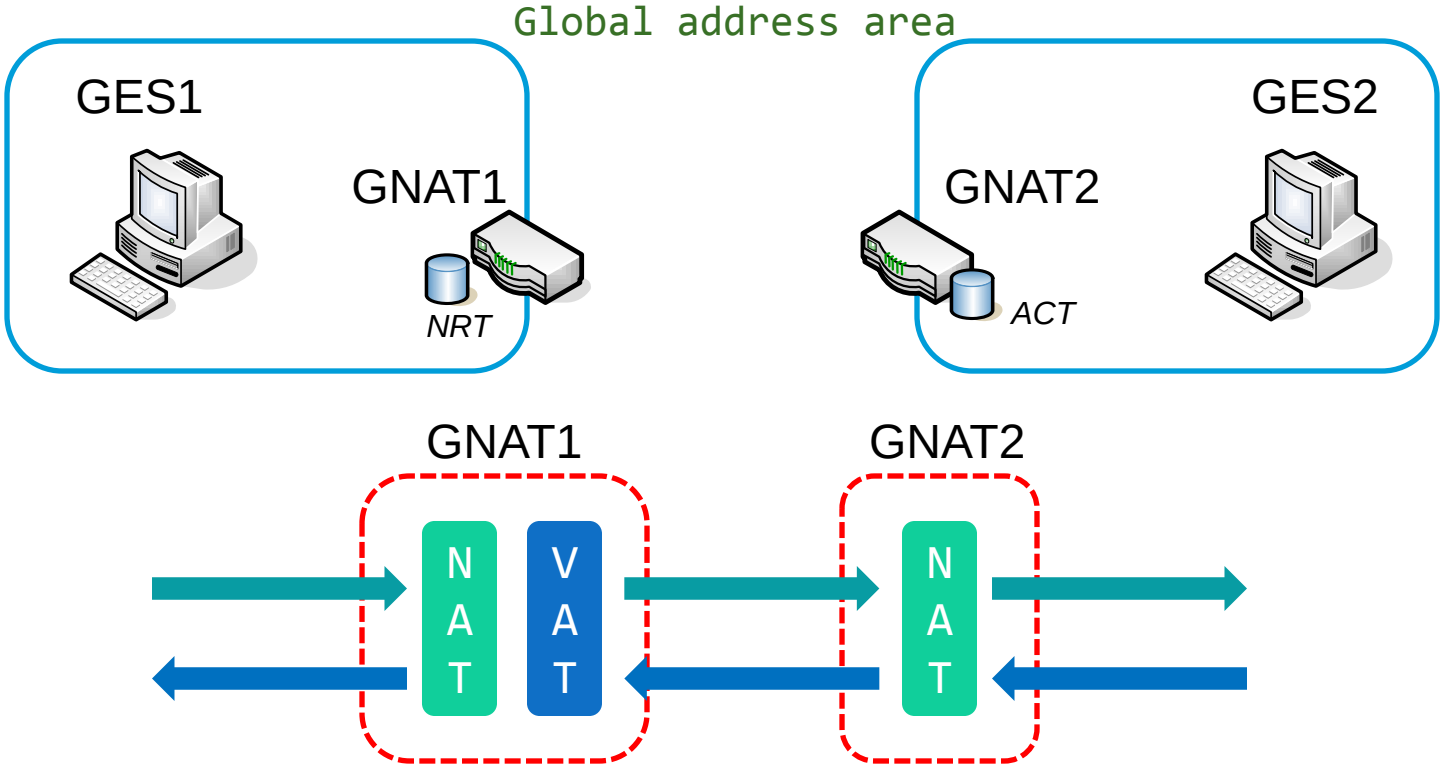






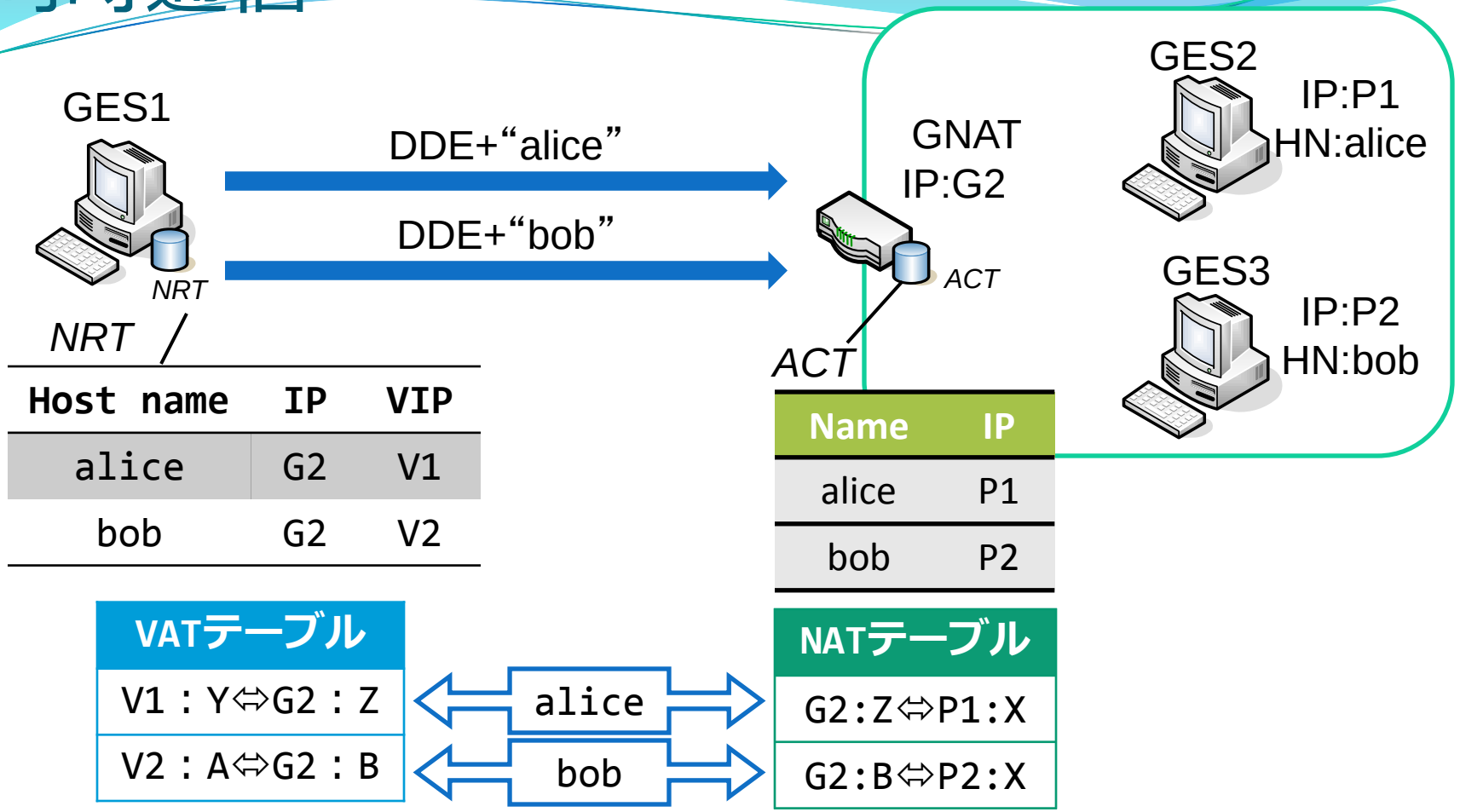
- PA空間から通信開始する場合は一般NATでも利用可能
- 異なるPA空間同士や多段NAT環境でも利用可能

異なるPA空間同士の通信



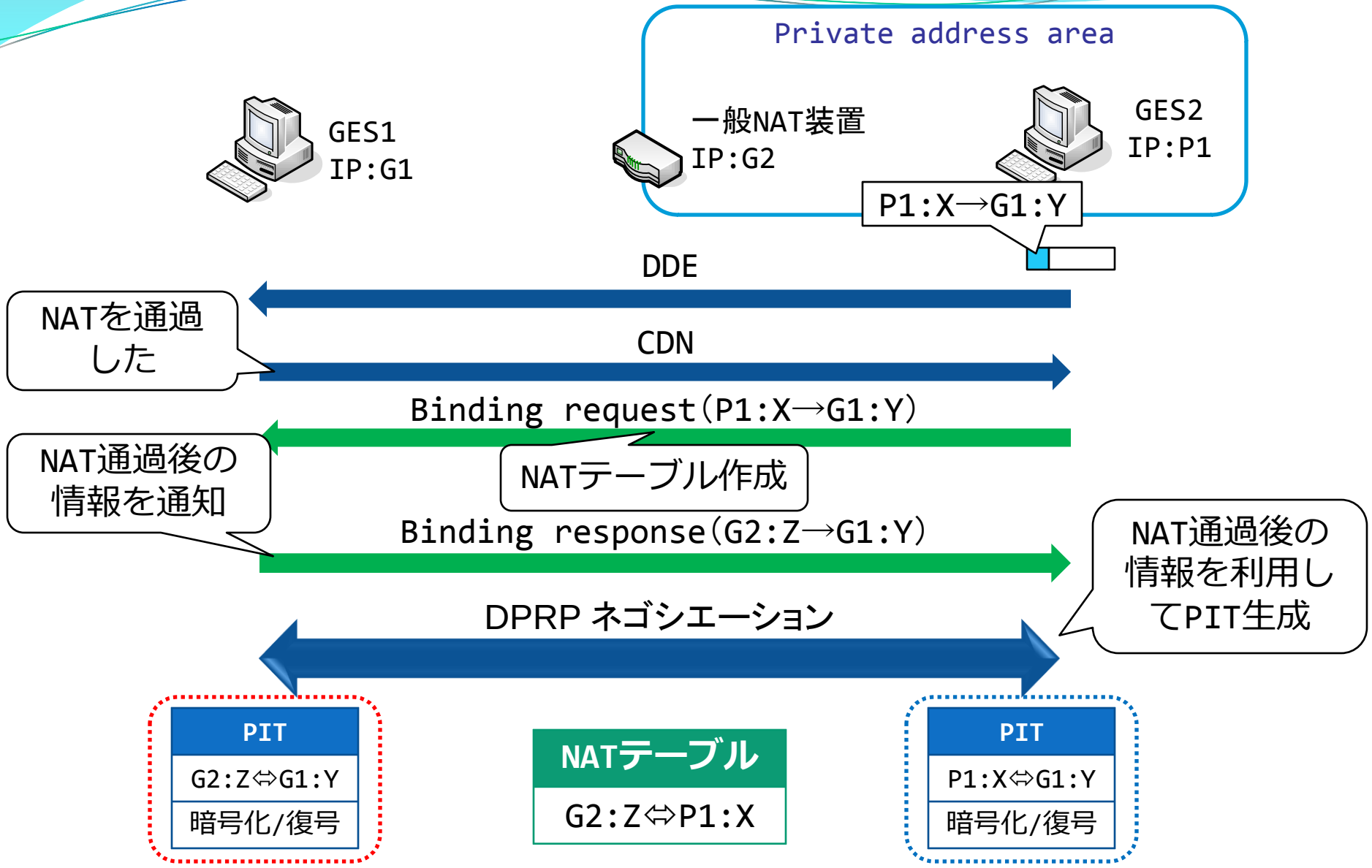
- NRT，VAT処理の位置をGESからGNATに変更
- GNAT 1 とGNAT2でNAT越えに必要な情報を交換

同時通信



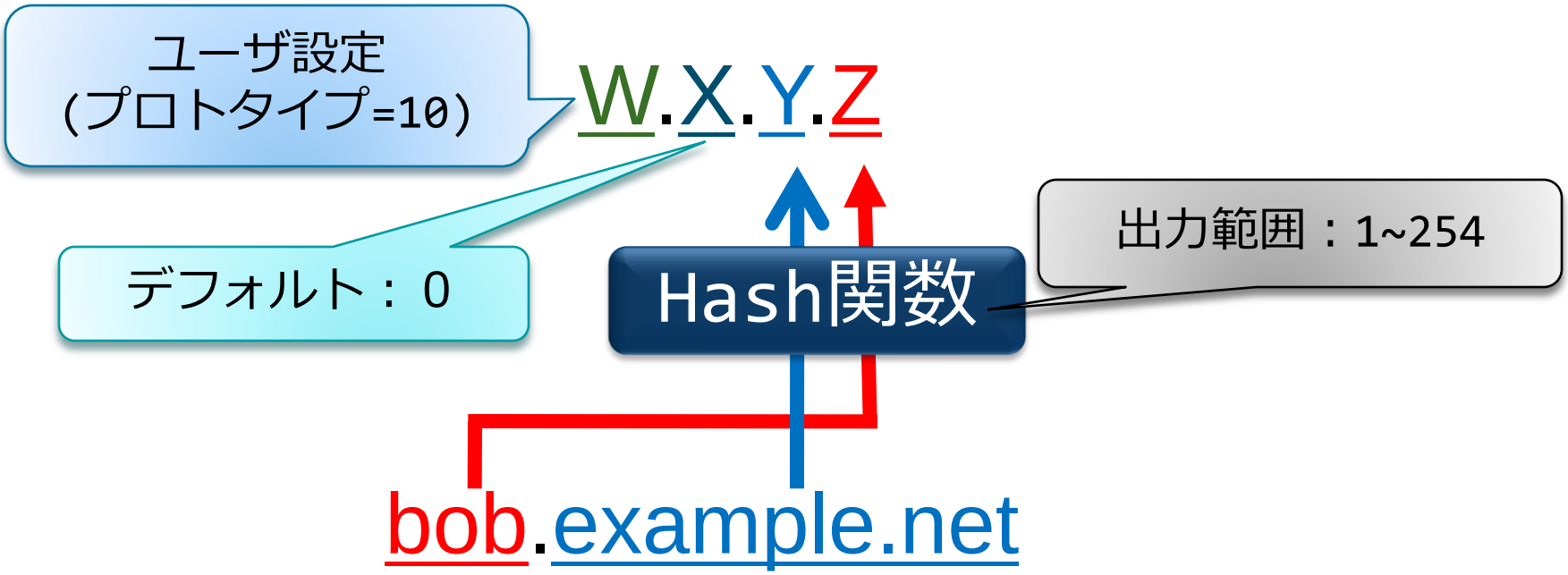
- GES1のアプリケーションは仮想IPアドレスにより NAT配下の端末を区別することが可能
- ホスト名に対応するNATテーブルを生成

一般NAT装置の場合


Private address area
GES1
IP:G1
一般NAT装置
IP:G2
GES2
IP:P1
P1:X→G1:Y
DDE
NATを通過した
CDN
Binding request(P1:X→G1:Y)
NAT通過後の情報を通知
NATテーブル作成
Binding response(G2:Z→G1:Y)
NAT通過後の情報を利用してPIT生成
DPRP ネゴシエーション
PIT
G2:Z⇔G1:Y
暗号化/復号
NATテーブル
G2:Z⇔P1:X
PIT
P1:X⇔G1:Y
暗号化/復号
変換後のコネクション情報のPIT
変換前のコネクション情報のPIT

仮想IPアドレス

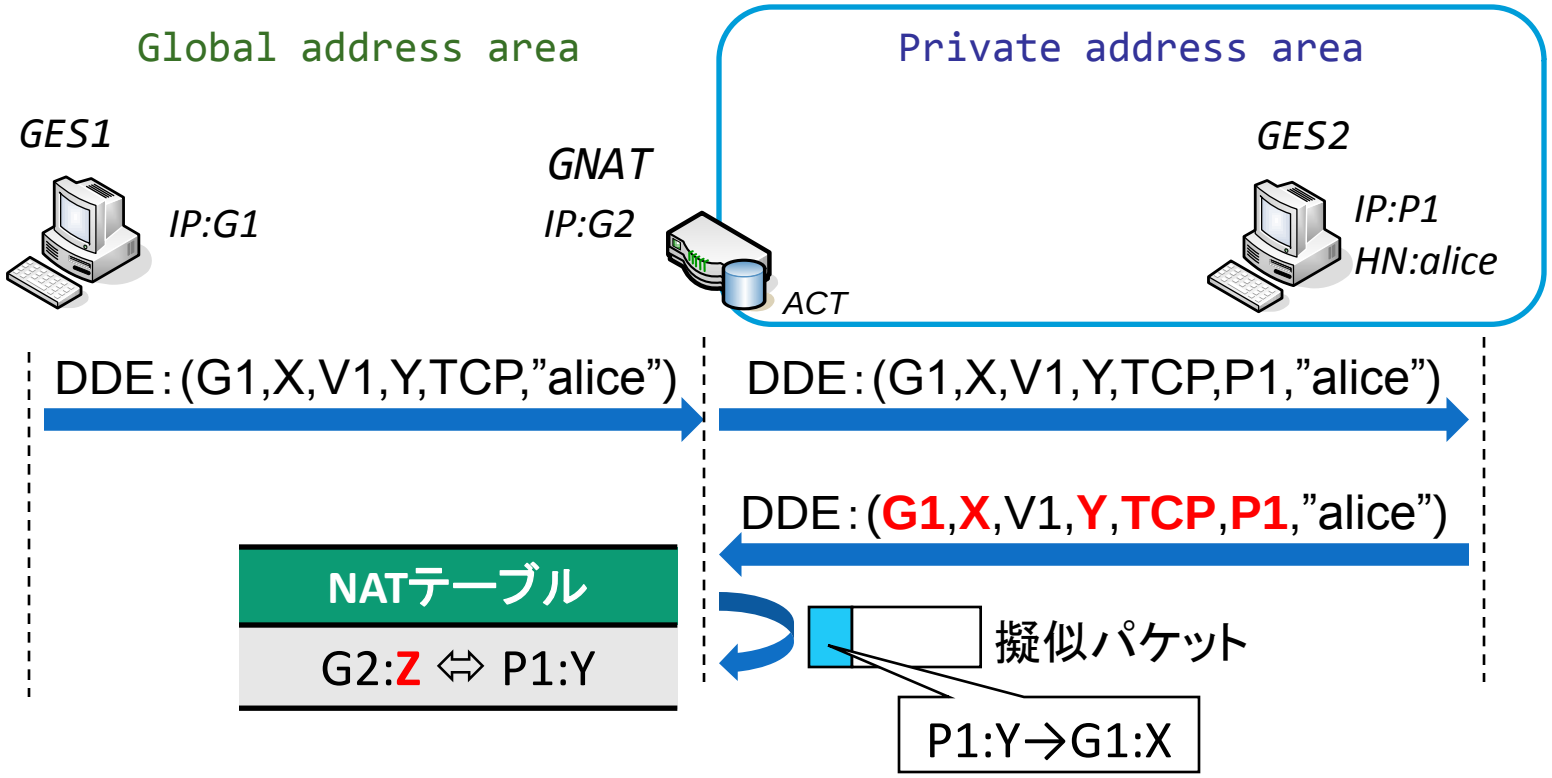
- FQDNに対応して割り当てる



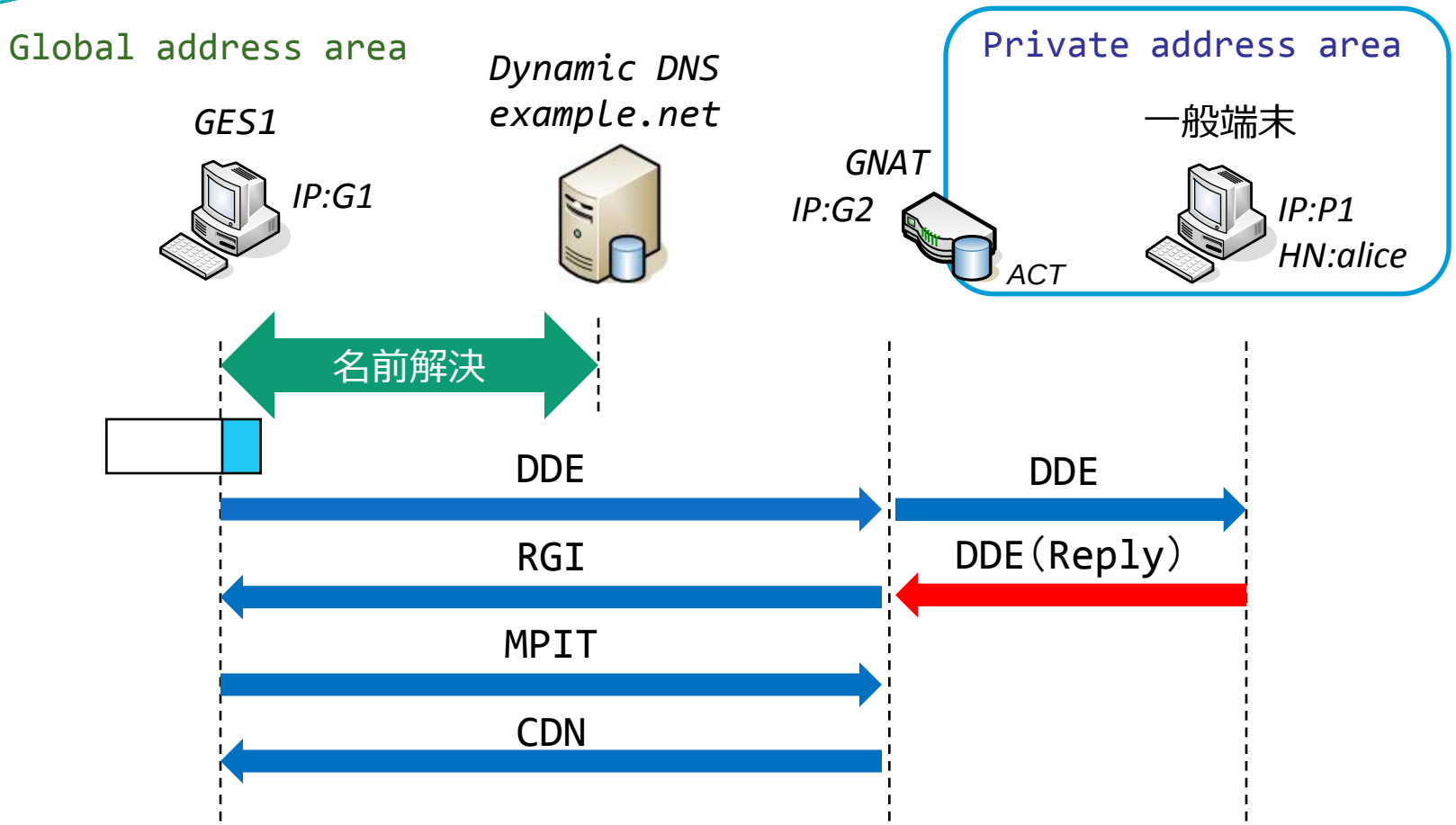
- ハッシュが衝突した場合
  - Xを異なる値に変化

NATテーブル生成方法

- RGIのパケットから擬似パケットを生成
  - GES2からGES1に送信すると見せかけたパケット
  - RGIのコネクション情報とACTで得たIPアドレスから作成

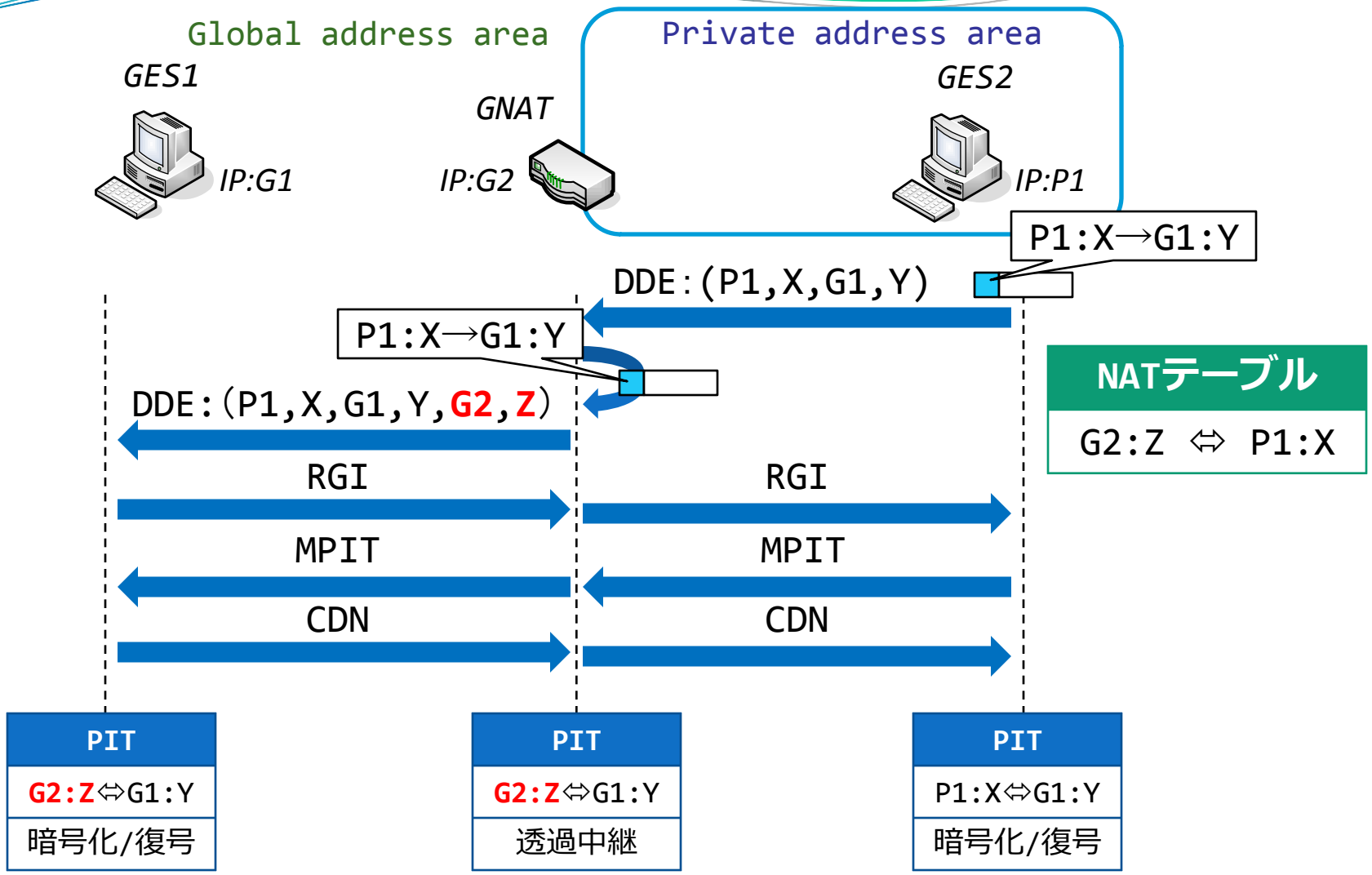


PA空間の端末が一般端末の場合



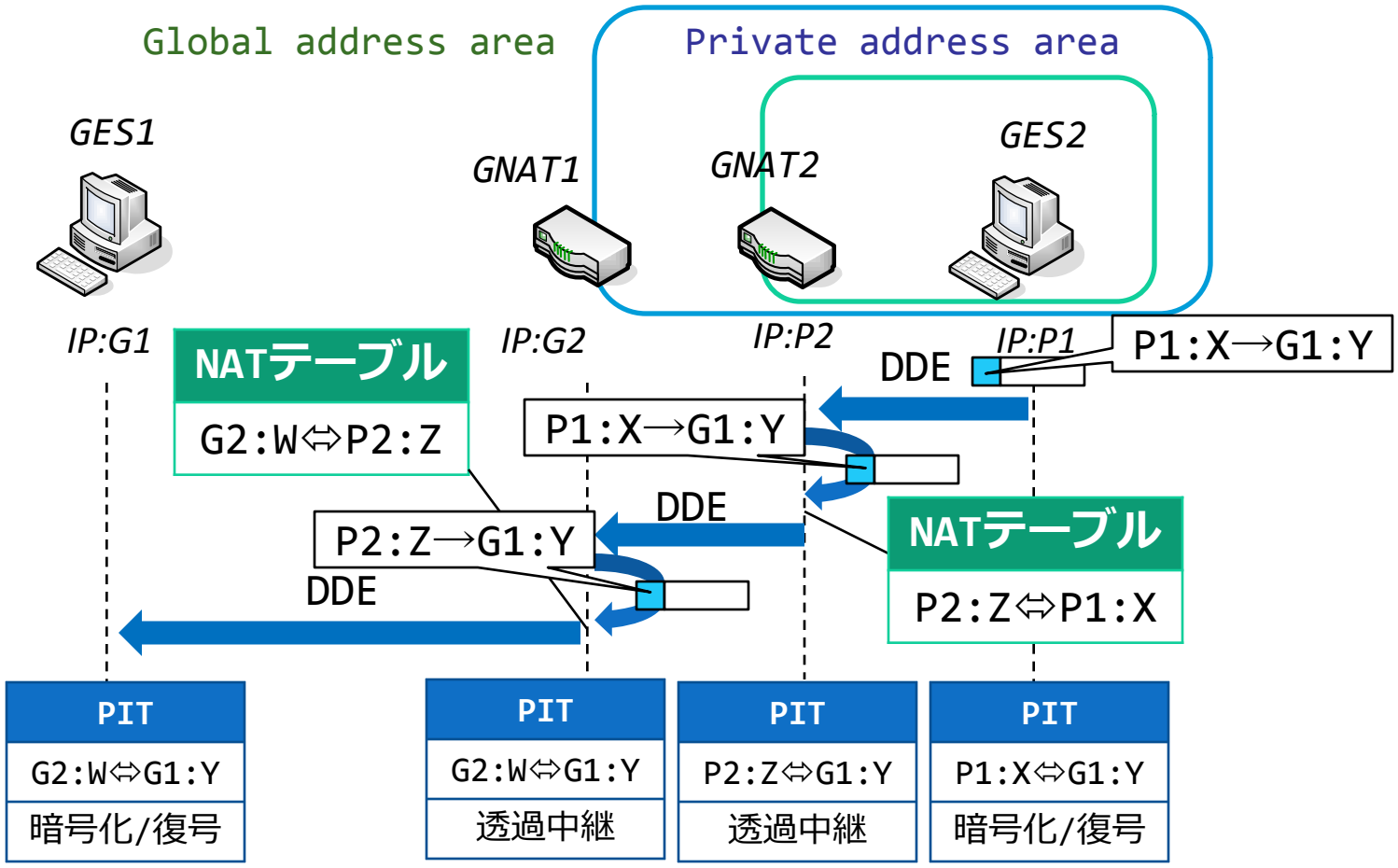
- 一般端末からDDEのReplyが応答される
- その後は，GES1-GNAT間でRGI以降を行う

PA空間からGA空間へのDPRP



- GES2からGES1へ送信すると見せかけるパケットを送信
- GES1-GNAT間では新たなコネクション情報でPITを生成

多段NAT構成の場合



- DDE通過時にNATテーブルを生成
- NAT変換後の情報を使って次のNATテーブルを生成