NATを越えてグループ通信が可能な拡張DPRPの提案

後藤裕司[†1] 鈴木秀和[†1] 渡邊晃[†1]

不正アクセスなどの脅威に対するセキュリティ対策として通信グループを構築する方法は有用である．IPsec は，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，管理負荷が大きいためこのような目的に適していない．そこで，我々はシステム構成が変化しても通信グループを構築する装置がその変化を学習し，通信グループの維持を可能とする動的処理解決プロトコル DPRP（Dynamic Process Resolution Protocol）を提案している．しかし，既存の DPRP は，通信経路上に NAT（Network Address Translation）が介在するような環境には対応できない．そこで本論文では，NAT を越えて DPRP を実行できる拡張 DPRP について検討した．

A Proposal of the extended Dynamic Process Resolution Protocol that group communication is possible exceeding NAT

Yuji Goto,[†1] Hidekazu Suzuki[†1] and Akira Watanabe[†1]

For the security measures against threads such as illegal access, etc. it is useful to define and from communication groups in order to make communication secure. IPsec is not appropriate in the case where system configurations frequently change like intranets, because the management loads of 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.

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おり，ファイアウォール (以下 FW) や IDS(Intrusion Detection System) などと協調するなど，様々な工夫がなされている．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部にも存在しており社員や内部関係者による不正による犯罪が多く報告されている[1)]．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相手認証，アクセス制御しかされていないのが現状であり，有効な対策が今後必要になると考えられている．

このような状況に対応するために，通信グループの構築が有効な方法である．通信グループを構築する代表的なネットワークセキュリティ技術として IPsec がある． IPsec[2)] は通信に先立ち暗号・認証に必要なパラメータを動的に生成して安全な情報の交換を行う．しかし，IPsec はホスト間の通信で利用されるトランスポートモードと，ネットワーク間通信で利用されるトンネルモードで互換性がないため，セキュリティドメインが階層的に構築されていたり，個人単位の通信グループが混在するような環境では利用することが難しい．

そこで我々はイントラネット内のセキュリティ対策と運用管理負荷の低減を両立できる GSCIP（Grouping for secure Communication for IP)[3)] と呼ぶネットワークアーキテクチャを提案している．動的処理解決プロトコル DPRP（Dynamic Process Resolution Protocol）は GSCIP を構成する代表的なプロトコル群の１つである．DPRP[4)] は，通信グループを構成する装置がシステム構成の変化を学習して動的に動作処理情報を生成する．DPRP は，通信に先立って実行され，システム構成が変化しても通信グループの定義が維持される．

†1 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University

一方，企業ネットワークにおいては，内側からの通信開始のみするのが一般的であり，ファイアウォールでもそのような通信のみを許可していた．そのためNAT の制約が表面化することはなかった．しかし，家庭ネットワークにおいては，企業ネットワークのような厳しいセキュリティポリシーは必要とならないため，外出先からホームネットワークのノードに自由にアクセスしたいというニーズがあると考えられる．この様な環境においても GSCIP を運用できると有用である．しかし，既存の DPRP は通信経路上に NAT[5] が介在するような環境には対応できていない．そこで本論文では NAT 越えを可能にする拡張 DPRP の検討を行った．以下に 2 章に GSCIP の概要，3 章で動的解決プロトコル DPRP，4 章で NAT 越えが可能な拡張 DPRP，5 章で NAT 越え DPRP の実装，6 章でまとめを述べる．

2. GSCIP の概要

GSCIP ではサブネット単位とホスト単位の通信グループが混在する環境において柔軟性と安全性を両立したネットワークアーキテクチャである．同一グループ内の端末間通信は暗号化され，異なる通信グループに属する端末からのアクセスを拒否することができる．ホストがサブネット内外を移動しても通信グループの関係は維持される．また，通信に必要な動作処理情報は通信開始時に自動的に生成されるため，管理負荷が軽いという特徴がある．図 1 に GSCIP における通信グループの定義方法を示す．GSCIP では通信グループを構成する装置を GE(GSCIP Element) と呼び，端末にソフトウェアをインストールするタイプの GES(GE realized by Software)，サブネットを構成するルータタイプの GEN(GE for Network) がある．GEN は配下のネットワークに存在する一般端末 (以下 Term) を保護する．

GSCIP では同一の共通鍵 GK(Group Key) を所持する GE の集合を同一通信グループとして定義する．GK を用いて GE 間の認証と通信の暗号化を行う．GSCIP ではこのよう通信グループとグループ鍵 GK を 1 対 1 に対応づけることにより IP アドレスに依存することなく通信グループを定義することができる．個人単位やドメイン単位の通信グループが混在したり重複帰属する通信グループであってもかまわない．グループ鍵 GK は各 GE の立ち上げ時に管理装置 GMS(GSCIP Management Server) から通信グループ情報と共に配送される．この際，GMS と GE 間は公開鍵を用いた確実な認証と暗号化が実行される．グループ鍵 GK は GMS から定期的に更新される．

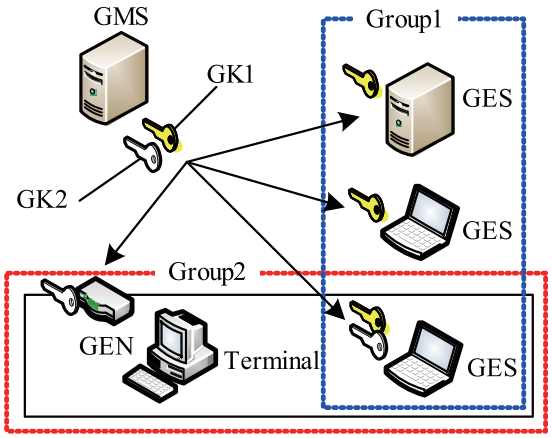


図 1 通信グループの定義方法
Fig. 1 Method to define communication groups.

GE は自身が保持する動作処理情報テーブル PIT(Process Information Table) に従ってパケットの処理を行う．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，廃棄），およびグループ鍵の識別番号が記述されている．PIT の検索には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) を用いる．該当する PIT が無い場合は以下に述べる DPRP を実行し PIT の生成を行う．

3. 動的処理解決プロトコル DPRP

DPRP は GSCIP を実現するプロトコル群の中で最も重要な位置づけを占めるものである．DPRP は端末間の通信開始に先立ち，通信経路上のすべての GE が事前に設定された情報を相互に交換して，各 GE に対応する動作処理情報テーブル PIT を生成する．図 2 に DPRP の動作を示す．GES1 は TCP/UPD パケットの送信時に該当する PIT がない場合は上記の送信パケットを一時的にカーネルに待避し，DPRP を実行して PIT の生成を行う．DPRP は 4 つの ICMP ベースの制御パケットで 2 往復のネゴシエーションを行う．DDE(Detect Destination End GE) は通信相手に最も近い GE を特定する．RGI(Report GE Information) は，通信経路上の各 GE のグループ番号などの情報を収集する．DDE と RGI には DPRP ネゴシエーションのトリガーとなった通信パケットのコネクション識別子 CID の情報が記載される．RGI を受信した GE は収集した GE の情報から GK を用いて

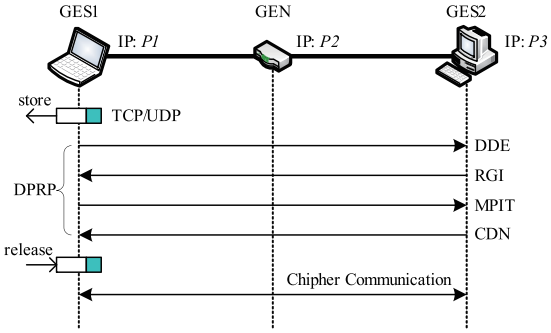


図 2 DPRP ネゴシエーション
Fig. 2 DPRP negotiation.

表 1 動作処理情報テーブル PIT
Table 1 Process Information Table.

Terminal	CID	Process
GES1	P1:s↔P3:d	encrypt/decrypt
GEN	P1:s↔P3:d	relay
GES2	P1:s↔P3:d	encrypt/decrypt

同一グループであるかどうかの確認を行い，動作処理情報を決定する．MPIT(Make Process Information Table) は決定した動作処理情報を各 GE に通知する．CDN(Complete DPRP Negotiation) は DPRP ネゴシエーションの完了を各 GE に通知する．表 1 に図 2 において生成される PIT を示す．各端末には同様のコネクション情報 CID で PIT が生成される．動作処理情報は，GES1,GES2 では暗号化/復号，GEN は透過中継となる．その後，GES1 は待避していたパケットを復帰させ生成した PIT の動作処理情報に従ってパケットを処理し送信する．

現状の DPRP は，通信経路上に NAT が介在するような環境では NAT で IP アドレスが変換されてしまうため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は，NAT の内側から通信が始まる場合，及び NAT の外側から通信が始まる場合の両者について検討する必要がある．本稿では後者の場合を中心に詳細な検討を行った．なお，GSCIP は今後はイントラネット内だけではなく，インターネットとホームネットワークをを組み合わせたシステムにも応用範囲を広げていくことを想定している．そこで，本稿では，NAT の内側はプライベートアドレス（以下 PA），外側はグローバルアドレス（以下 GA）であるものとして記述する．この検討には NAT 越え問題を解決する必要がある．NAT 越え問題とは通信経路上に NAT が介在すると GA 空間側の端末から PA 空間が見えないため通信開始ができないという問題である．そこでこの問題を解決するために GSCIP の枠組の中で別途検

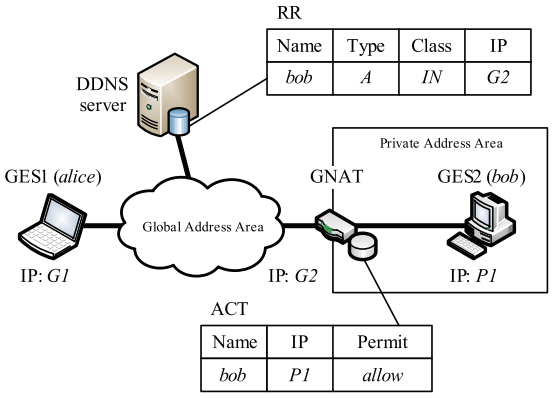


図 3 システム構成と初期情報
Fig. 3 System configuration and initial information.

討中の NAT-f（NAT-free）[6] プロトコルの技術を用いる．NAT-f は外部端末と NAT-f ルータ間のプロトコルで，NAT テーブルを外部端末からの指示で動的に生成する．また，通信経路上に一般 NAT ルータが介在する場合と多段 NAT 環境下においても DPRP が利用できるよう拡張を行った．

4. 提 案 方 式

4.1 NAT 越え DPRP

図 3 に NAT 越え DPRP のシステム構成と初期情報について示す．GA 空間側に GES1,PA 空間側に GES2 が存在する．GA 空間と PA 空間の間には機能を追加した NAT を設置し，これを GNAT と呼ぶことにする．ダイナミック DNS（以下 DDNS）[7] サーバには PA 空間の端末 GES2 のホスト名と GNAT の IP アドレスを関連付けて登録しておく．また，GES2 の名前（bob），プライベート IP アドレス（P1），および外部からのアクセスの可否を GNAT のアクセス制御テーブル ACT（Access Control Table）に登録しておく．

GES1 は GES2 と通信を開始する際に GES2 の FQDN を用いて DDNS サーバに名前解決を依頼する．DDNS サーバは該当するレコードとして GNAT のアドレス “G2” を応答する．GES1 はこの応答を受信するとカーネルにおいて GNAT の IP アドレス “G2” と GES2 のホスト名 “bob” を取得する．さらに GNAT の IP アドレス “G2” を仮想 IP アドレス “V1” に書き換え，これらの関係を名前関連テーブル NRT（Name Relation Table）へ保存する．仮想 IP アドレスとは通信相手となる PA 空間の端末を一意に特定するために割り当てる IP アドレスである．上位ソフトウェアには仮想アドレス “V1” が通知される．その後，

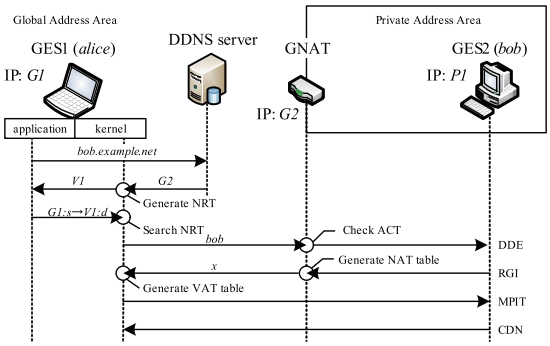


図 4 NAT 越え DPRP の動作
Fig. 4 Extended DPRP negotiation.

上位ソフトウェアから GNAT 宛に最初の TCP/UDP パケットが送信されると，カーネルにおいて上記パケットを待避し拡張 DPRP ネゴシエーションを開始する．図 4 に拡張 DPRP の動作を示す．最初の DDE には NRT から得た通信相手のホスト名 “bob” を追加して GNAT 宛に送信する．GNAT は DDE を受信すると “bob” を検索キーにして ACT の検索を行い通信が許可されているかどうかチェックする．通信が許可されていた場合，“bob” のプライベート IP アドレス “P1” を取得し，DDE を GES2 に転送する．

GES2 は DDE を受信すると DDE に記載されている CID と GES2 のプライベート IP アドレス “P1” より新たに CID1 を定義し，この情報を RGI に追加して GES1 宛に送信する．GNAT は RGI を受信すると，追加した CID1 の情報を元にして NAT テーブルを動的に生成する． GNAT は NAT にマッピングされたポート番号 “x” を RGI に追加して GES1 宛に送信する． GES1 はこれを受信すると，RGI に含まれている情報から GES2 に対応付けられた仮想 IP 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 “x” の相互変換関係が記されたテーブル VAT（Virtual Address Translation table）を生成する．MPIT，CDN の処理は 3 章で述べた内容と同様である．ただし，MPIT で各 GE に指示する PIT の内容は以下に述べる NAT に対応した PIT となる．このようにして生成された各テーブルの内容を表 2 に示す．

4.2 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．このような場合の PIT は，通信相手の見え方によって GE ごと異なる内容となる．これを NAT に対応した PIT と呼ぶことにする．表 3 に NAT に対応した PIT を示す．GES2 は GES1 が通信相手に見える

表 2 NAT 越え DPRP : 各テーブル
Table 2 Extended DPRP:Each table.

名前解決テーブル NRT

Terminal	Name	VIP	IP
GES1	bob	V1	G2

仮想アドレス変換テーブル VAT

Terminal	Target Packet	Translation
GES1	G1:s↔V1:d	G1:s↔G2:x

NAT テーブル

Terminal	Inside	Outside
GNAT	P1:d→G1:s	G2:x→G1:s

表 3 NAT に対応した PIT
Table 3 PIT corresponding to NAT.

Terminal	CID	Process
GES1	G1:s↔G2:x	encrypt/decrypt
GNAT	G1:s↔G2:x	relay
GES2	G1:s↔P3:d	encrypt/decrypt

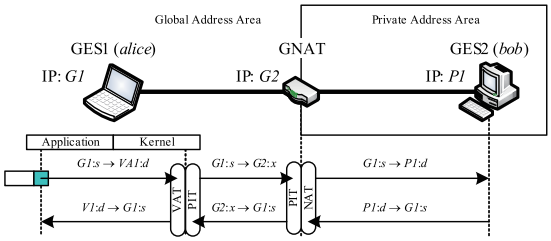


図 5 VAT と NAT によるアドレス変換処理
Fig. 5 Address translation process by VAT and NAT.

ため GES2 と GES1 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 については PIT を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，グローバルアドレス側，すなわち GES1 と GNAT に対応した PIT を生成することとした．

4.3 アドレス変換処理

図 5 に通信パケットが VAT と NAT によりアドレス変換されていく様子を示す．GES1 は TCP/UDP パケットを復帰させ，VAT テーブルに基づいて宛先 IP アドレスとポート番号を “V1:d” から “G2:x” に変換して送信する．GES1 の PIT は VAT で変換後に参照される．GNAT ではパケット受信後まず PIT が参照される．その後，NAT テーブルに従って宛先の IP アドレスとポート番号 “G2:x” を “P1:d” に変換して GES2 に送信する．GES2 ではアドレスの変換処理はなく PIT の参照とその処理だけが実行される．逆方

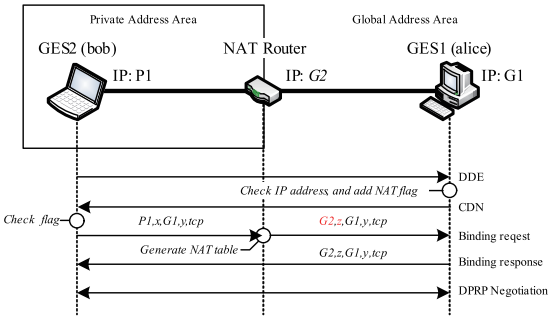


図 6 一般 NAT ルータの場合
Fig. 6 Normal NAT router.

表 4 一般 NAT ルータの場合の PIT
Table 4 Normal NAT router.

Terminal	CID	Process
GES1	P1:s↔G1:y	encrypt/decrypt
GES2	G2:z↔G1:y	encrypt/decrypt

向のパケットは上記と逆の変換を行う．

4.4 一般 NAT ルータを利用した場合

一般 NAT ルータを利用する場合にも GSCIP の構築が可能となるよう検討した．ただし，この場合は NAT 越えが出来ないので，通信の開始は GES2 側からのみという制約が出る．図 6 に一般 NAT ルータの配下の端末から GA 空間の端末へ通信を行う場合の DPRP の処理を示す．GES2 は通信に先立ち DDE を GES1 に送信する．GES1 は DDE を受信するとパケットの送信元 IP アドレスと DDE に含まれている CID の送信元 IP アドレスを比較する．一致している場合は，NAT を経由していないとわかるので，以後の動作はこれまでと変わらない．一致していない場合は，通信経路上に NAT があると判断して CDN を生成する．CDN には通常の CDN と区別するために NAT フラグを付加して GES2 に送信する．GES2 は CDN を受信するとフラグがあるかどうかをチェックする．フラグがある場合は，新たに定義した Binding request によるシーケンスを実行する．通信経路上に一般 NAT ルータしかない場合，ネゴシエーション中に NAT 処理後のコネクション情報が得ることができないため，NAT に対応した PIT を生成することができない．そこで，Binding request を用いて NAT 処理後のコネクション情報を取得する．Binding request は通信パケットのオリジナルのコネクション情報から生成され GES1 に送信される．GES1 は受信後，Binding response を生成する．Binding response には，NAT でアドレス変換処理後の Binding request パケットのコネクション情報を付加して GES2 に送信する．GES2 はこれを

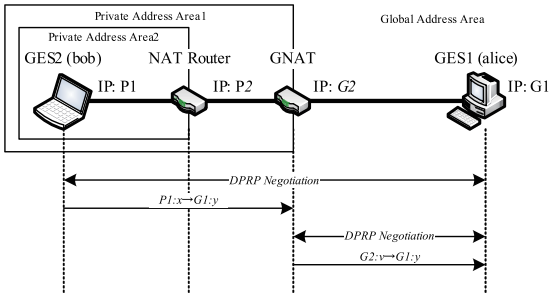


図 7 多段 NAT : PA 空間から GA 空間
Fig. 7 Multistage NAT:PA area to GA area.

表 5 多段 NAT : PA 空間から GA 空間
Table 5 Multistage NAT:PA area to GA area

PIT

Terminal	CID	Process
GES1	G2:z↔G1:y	encrypt/decrypt
	G2:v↔G1:y	encrypt/decrypt
GNAT	G2:z↔G1:y	relay
	G2:v↔G1:y	encrypt/decrypt
GES2	P1:x↔G1:y	encrypt/decrypt

NAT テーブル

Terminal	Inside	Outside
NAT Router	P1:x→G1:y	P2:w→G1:y
GNAT	P1:x→G1:y	G2:z→G1:y
	P2:w→G1:y	G2:v→G1:y

受信後，Binding response に含まれるコネクション情報を DDE に追加して DPRP ネゴシエーションを改めて開始する．この DPRP ネゴシエーションで生成される PIT を表 4 に示す．PA 空間側の GES2 には最初の通信パケットのコネクション情報，GES1 には Binding response で得られたコネクション情報に対応したものとなる．この方法により GES1 には，NAT に対応した PIT が生成される．

4.5 多段 NAT 構成の場合

拡張 DPRP は次の条件の場合に，多段 NAT 環境下においても利用可能である．

PA 空間の端末から GA 空間の端末に通信を開始する場合，GA 空間に接続する NAT 装置が GNAT であれば中間に他の NAT 装置や GNAT が介在していても利用することができる．図 7 の多段 NAT 環境における動作を示す．GES2/GES1 間で拡張 DPRP ネゴシエーションを行うと各 GE の PIT には表 5 の一段目の PIT が生成される．しかし，GNAT と GES1 に生成された PIT は，トリガーとなったパケットのコネクション情報（P1:x→G1:y）をもとに NAT テーブルと PIT が生成されているため，NAT ルータで変換された IP アドレスとポート番号 (P2:w↔G2:v) と

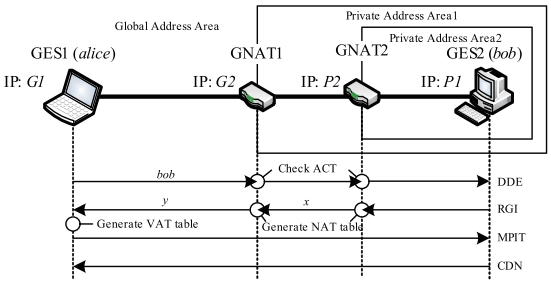


図 8 多段 NAT : GA 空間から PA 空間の場合
Fig. 8 Multistage NAT:GA area to PA area.

表 6 多段 NAT : GA 空間から PA 空間の場合
Table 6 Multistage NAT:GA area to PA area.

VAT

Terminal	Target Packet	Translation
GES1	G1:s↔V1:d	G1:s↔G2:y

NAT テーブル

Terminal	Inside	Outside
GNAT1	P2:x→G1:s	G2:y→G1:s
GNAT2	P1:d→G1:s	P2:x→G1:s

アクセス制御テーブル ACT

Terminal	Name	IP	Permit
GNAT1	bob	P1	allow
GNAT2	bob	P2	allow

一致しない．そのため，GNAT が通信パケットを受信した場合，GNAT の PIT と一致しないため，もう一度 DPRP ネゴシエーションが行われる．GNAT は，NAT で変換後の通信パケットに対して DPRP ネゴシエーションを行うため，GNAT と GES1 には NAT ルータで変換後の IP アドレスとポート番号を考慮した PIT（G2:v↔G1:y）を生成することができる．これにより通信パケットと PIT の内容が一致するためを GES1 に送信することができる．

GA 空間の端末から PA 空間の端末に通信を行う場合，通信相手までの経路上の全ての NAT 装置が GNAT でなくてはならない．拡張 DPRP では外部からの通信に対して ACT を用いてアクセス制御を行っているため，一般 NAT ルータが通信経路上にある場合は外部からの通信を内部に通すことができない．図 8 に多段 NAT 環境で GA 空間から PA 空間へ通信を開始する場合の動作, 表 6 に生成されるテーブルを示す．基本的な動作は 4.1 に示した動作と同じであるが，GNAT1 の ACT には “bob” のプライベート IP アドレスを登録するのではなく GNAT2 の外側の IP アドレス “P2” を登録する必要がある．GES1 は名前解決後，DDE を GNAT1 宛に送信する．GNAT1 では，

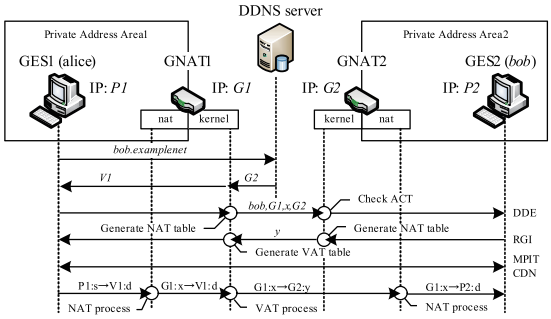


図 9 異なる PA 空間どうしの通信
Fig. 9 Communication between different PA areas.

表 7 異なる PA 空間どうしの通信
Table 7 Communication between different PA areas.

PIT

Terminal	CID	Process
GES1	P1:s↔V1:d	encrypt/decrypt
GNAT1	G1:x↔G2:y	relay
GNAT2	G1:x↔G2:y	relay
GES2	G1:x↔P2:d	encrypt/decrypt

VAT

Terminal	Target Packet	Translation
GNAT	G1:x↔V1:d	G1:x↔G2:y

NAT テーブル

Terminal	Inside	Outside
GNAT1	P1:s→G2:y	G1:x→G2:y
GNAT2	P2:d →G1:x	G2:y→G1:x

ACT

Terminal	Name	IP	Permit
GNAT2	bob	P2	allow

“bob” で検索を行い GNAT2 の IP アドレス “P2” を取得し，GNAT2 宛に DDE を転送する．GNAT2 では，同様に検索を行い “bob” のプライベート IP アドレス “P1” を取得し，DDE を GES2 に転送する．RGI では GNAT2 で NAT にマッピングを行い，マッピングされたポート番号 “x” を RGI に追加して GNAT1 に送信する．GNAT1 では，ポート番号 “x” を用いて NAT にマッピングを行い，マッピングされたポート番号 “y” を RGI に追加して GES1 に送信する．以後の処理は 4.1 に示す動作と同様である．

4.6 異なる PA 空間どうしの通信

拡張 DPRP を更に拡張することにより，異なる PA 空間を跨いだ GSCIP の構築が可能である．図 9 に異なる PA 空間どうしの通信を行う場合の動作を示す．PA 空間 1 を構成する GNAT1 の配下に GES1，PA 空間 2 を構成する GNAT2 の配下に GES2 があるも

のとし，それぞれ異なる PA 空間に存在する．

GES1 は GES2 の “bob” と通信を行うために GNAT1 を経由して DDNS サーバに名前解決依頼を行う．DDNS サーバは該当する GNAT2 のアドレス “G2” を GNAT1 に応答する．GNAT1 は，DNS 応答パケットを受信すると，GNAT1 のカーネルにおいて GNAT2 の IP アドレス “G2” を仮想アドレス “V1” に変換する．GES1 が GA 空間に存在する場合は，アドレス変換処理を GES1 が行っていたが，GES1 が PA 空間に存在し，端末が所属している PA 空間を構成する装置が GNAT の場合は，GNAT が VAT アドレス変換処理を行う．GNAT1 は，アドレス変換処理を行った後，NRT テーブルにホスト名と IP アドレスの関係を保存後，GES1 にパケットを送信する．GES1 には DNS 応答として仮想アドレス “V1” が報告されることになる．GES1 の上位ソフトウェアは通信パケットを仮想アドレス “V1” 宛に送信する．GES1 のカーネルはこれを受信すると，通信パケットを待避して DPRP ネゴシエーションを開始する．GES1 は DDE を仮想アドレス宛 “V1” に送信する．GNAT1 はこれを受信すると，仮想アドレス “V1” で NRT テーブルの検索を行い，該当するホスト名 “bob” と GNAT2 の IP アドレス “G2” を取得する．そして，その情報と DDE に含まれている CID の情報から GES1 と GNAT2 に対応する NAT テーブルを作成する．GNAT2 では DDE を受信すると ACT の検索を行い “bob” のプライベート IP アドレス “P1” を取得し GES2 に転送する．GES2 は DDE を受信後，DDE に記載されている DDE と取得した “P1” で新たに CID を作り，RGI に追加して送信する．GNAT2 はこれを受信すると，追加された CID の情報を元に NAT テーブルを動的に作成する．GNAT2 は NAT にマッピングされたポート番号 “y” を RGI に追加して GNAT1 に送信する．GNAT1 は RGI を受信したら，ポート番号 “y” と RGI に含まれている仮想アドレスなどの情報から VAT を生成する．MPIT では，各アドレス空間に対応した PIT を各端末に生成する．DPRP ネゴシエーション終了後，GES1 は待避していた通信パケットを仮想アドレス “V1” 宛に送信する．GNAT1 はこれを受信すると，NAT によりアドレス変換を行った後に VAT 処理を行うことにより通信パケットを GNAT2 に送信することが出来る．以後の通信は 4.1 と同様である．

5. 実　　装

既存の DPRP モジュールに NAT 越え機能を追加し FreeBSD の IP 層に実装した．図 10 に GES の実装概要を示す．DPRP は IP 層の入出力関数 *ip_input*(), *ip_output*() から呼び出される．DPRP ネゴシエーションのトリガーとなる最初の TCP/UDP パケットは，カーネル内に待避する．このパケットはネゴシエーションが完了した時点で *ip_output*() へ渡すことにより，即座に送信することができる．既存の PIT と新たに追加する NRT,VAT テーブルはカーネル空間に作成して，不要となったら削除する．

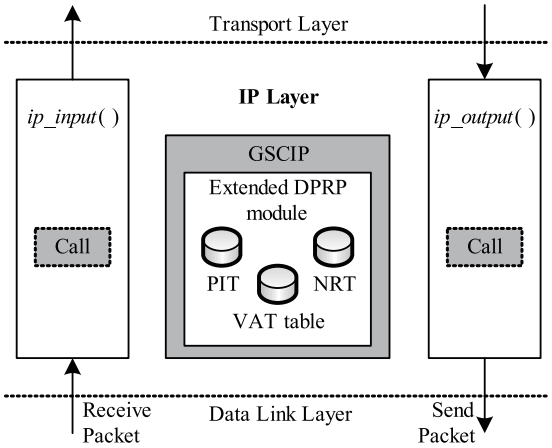


図 10　GES の実装概要
Fig. 10　Implementation of GES.

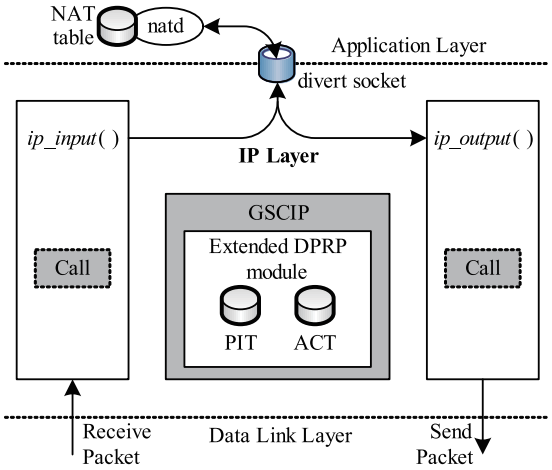


図 11　GNAT の実装概要
Fig. 11　Implementation of GNAT.

図 11 に GNAT の実装概要を示す．GNAT には，GEN に新たに ACT 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．GES と同様にカーネル空間内に PIT と ACT を生成する．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から呼び出される．

6. ま と め

本稿では DPRP を拡張し NAT 越えを可能とする拡張 DPRP を提案した．応用として一般 NAT ルータを利用した場合，多段 NAT 環境下における実現について検討した．拡張 DPRP により，外部から動的に NAT テーブルを生成し，その NAT テーブルに対応した PIT を生成を行う．これにより，グローバルアドレス空間とプライベートアドレス空間の混在する環境においても GSCIP によるグループ定義が可能となった．今後は，本提案の実装を完了させ通信開始時間やアドレス変換処理がスループットに与える影響などの評価を行う．

謝辞 本研究の一部は，日本学術振興会科学研究費補助金（特別研究員奨励費 20・1069）の助成を受けたものである．

参 考 文 献

1) Gordon, L. A., Loeb, M. P., Lucyshyn, W. and Richardson, R.: 2006 CSI/FBI Computer Crime and Security Survey, Technical report, Computer Security Institute (2006).
2) Kent, S. and Atkinson, R.: Security Architecture for the Internet Protocol, RFC 2401 (1998).
3) 鈴木秀和，竹内元規，加藤尚樹，増田真也，渡邊 晃：フレキシブルプライベートネットワークを実現するセキュア通信アーキテクチャGSCIP の提案，マルチメディア，分散，協調とモバイル (DICOMO2005) シンポジウム論文集，pp.441–444 (2005).
4) 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).
5) Egevang, K. and Francis, P.: The IP Network Address Translator (NAT), RFC 1631, IETF (1994).
6) 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).
7) Vixie, P., Thomson, S., Rekhter, Y. and Bound, J.: Dynamic Updates in the Domain Name System (DNS UPDATE), RFC 2136, IETF (1997).

NATを越えてグループ通信が可能な拡張DPRPの提案

名城大学大学院
後藤　裕司
鈴木　秀和
渡邊　晃

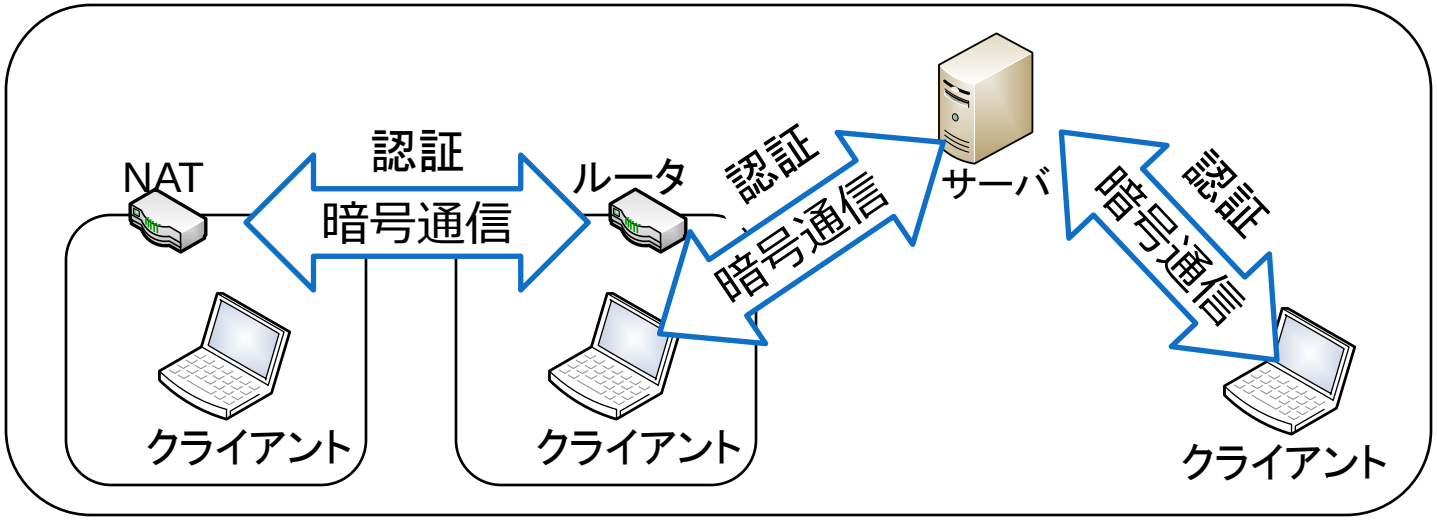
研究背景

- 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
  - 通信の暗号化
  - ディジタル署名，ファイアウォールなど
- 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

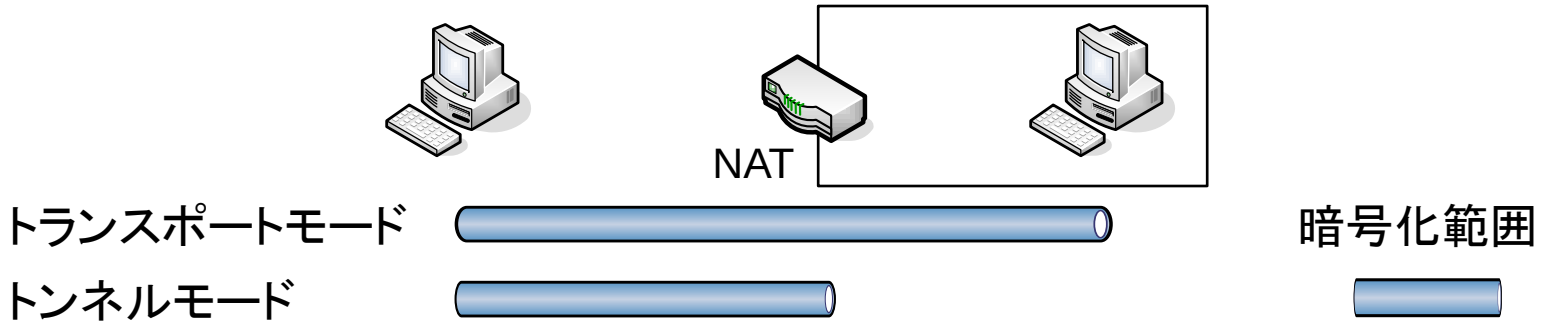
- 通信相手と確実な認証
- 通信内容の暗号化
- あらゆる環境で利用可能
  - 個人単位とドメイン単位が混在
  - 通信経路上にNATがある場合



IPsecで実現しようとすると・・・

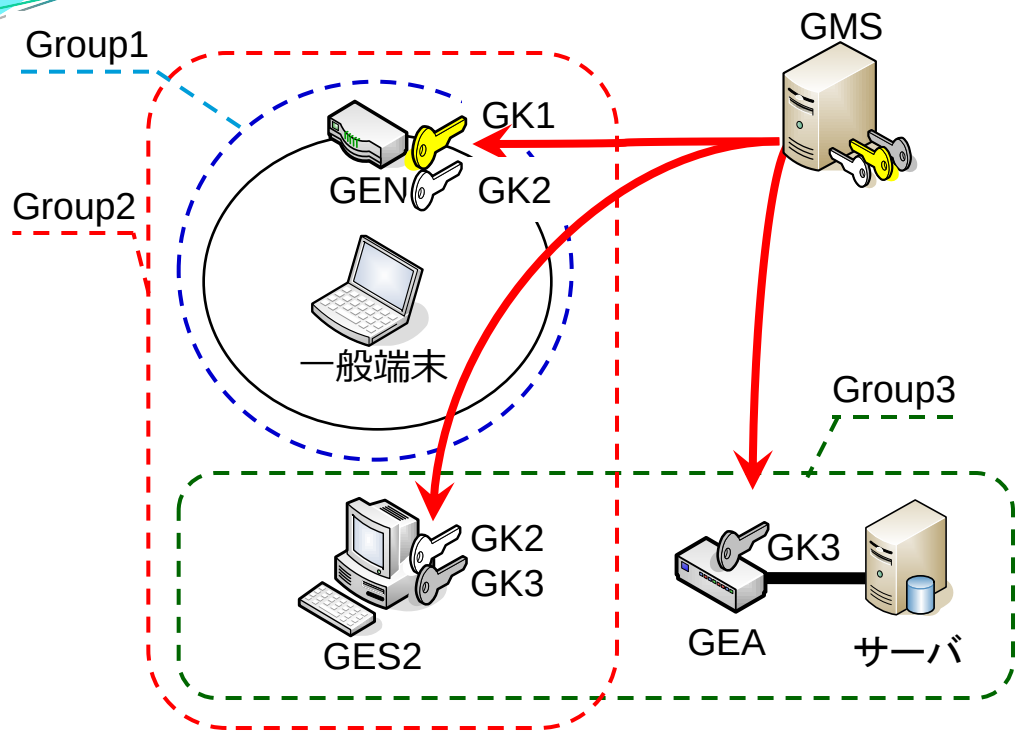
IPsecを利用する場合の問題点

- 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
- NA(P)Tと相性が悪い
  - TCP/UDPチェックサムを更新することが出来ない



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



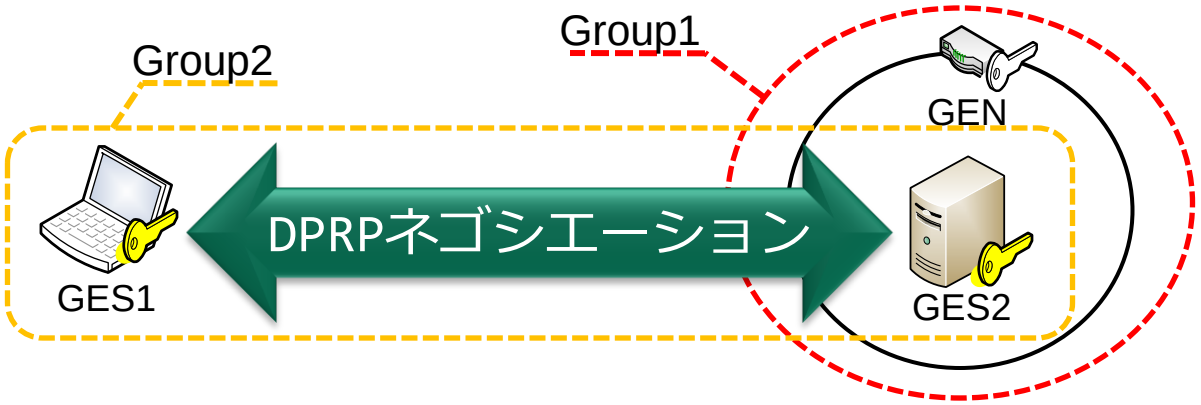
GE：GSCIP対応した装置
GES(Software型):ホストタイプ
GEN(Network型):ルータタイプ
GEA(ブリッジ型)：ブリッジタイプ
GMS：グループ管理装置

- 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

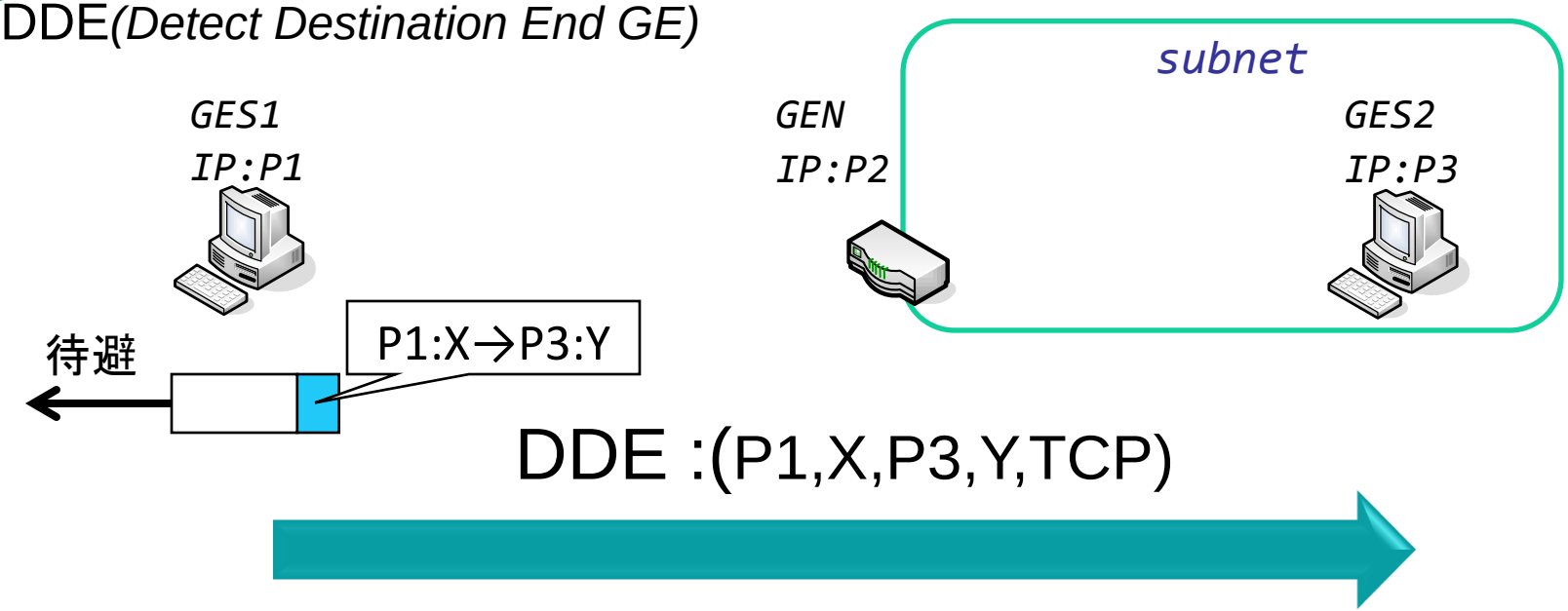
DPRP(*Dynamic Process Resolution Protocol*)

- 通信開始時にネゴシエーションを実行
- 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



DPRPネゴシエーション（1）

DDE*(Detect Destination End GE)*

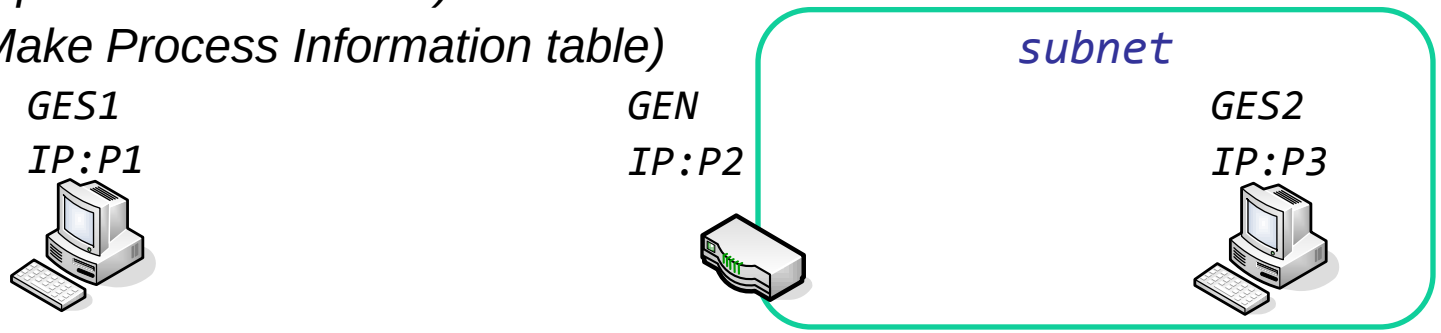


- 通信パケットを待避してから開始
- 終端GEの決定
- 通信パケットのコネクション情報を含む
  - 送信元IPアドレスとポート番号，宛先IPアドレスとポート番号，プロトコル番号

DPRPネゴシエーション（2）

RGI *(Report GE Information)*

MPIT*(Make Process Information table)*



RGI：(P1,X,P3,Y,TCP)＋各GEの設定情報

MPIT :各GEの動作処理情報

PIT
P1:X⇔P3:Y
暗号化/復号

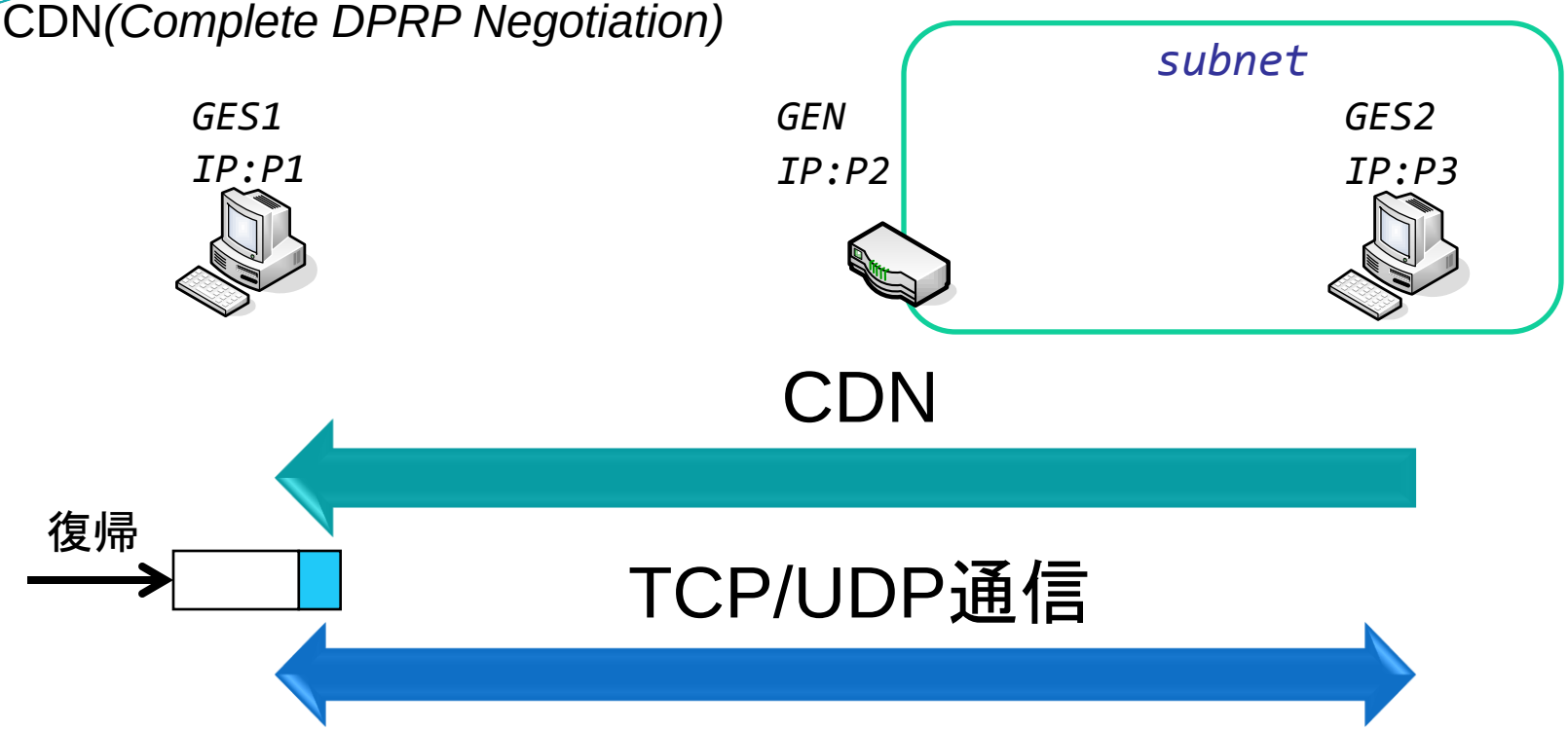
PIT
P1:X⇔P3:Y
透過中継

PIT
P1:X⇔P3:Y
暗号化/復号

- 通信経路上の各GEの設定情報(グループ番号など)を収集
- 決定した動作処理情報の通知
- 動作処理情報テーブルPITの生成

DPRPネゴシエーション（3）

CDN(*Complete DPRP Negotiation*)



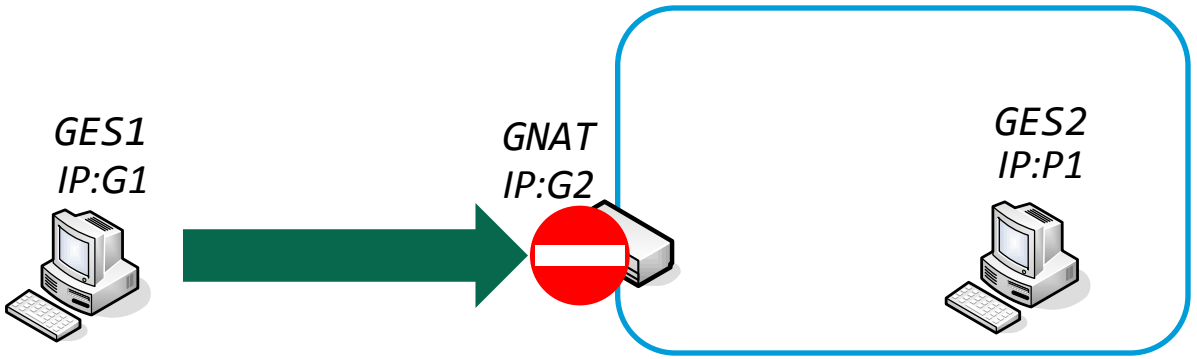
- DPRPネゴシエーションの終了を通知
- 待避させていたパケットを復帰
- 動作処理情報テーブルPITに従ってパケットを処理

DPRPネゴシエーションによってグループ通信が可能に

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)空間側から通信開始できない
  - NATにマッピング情報がないため

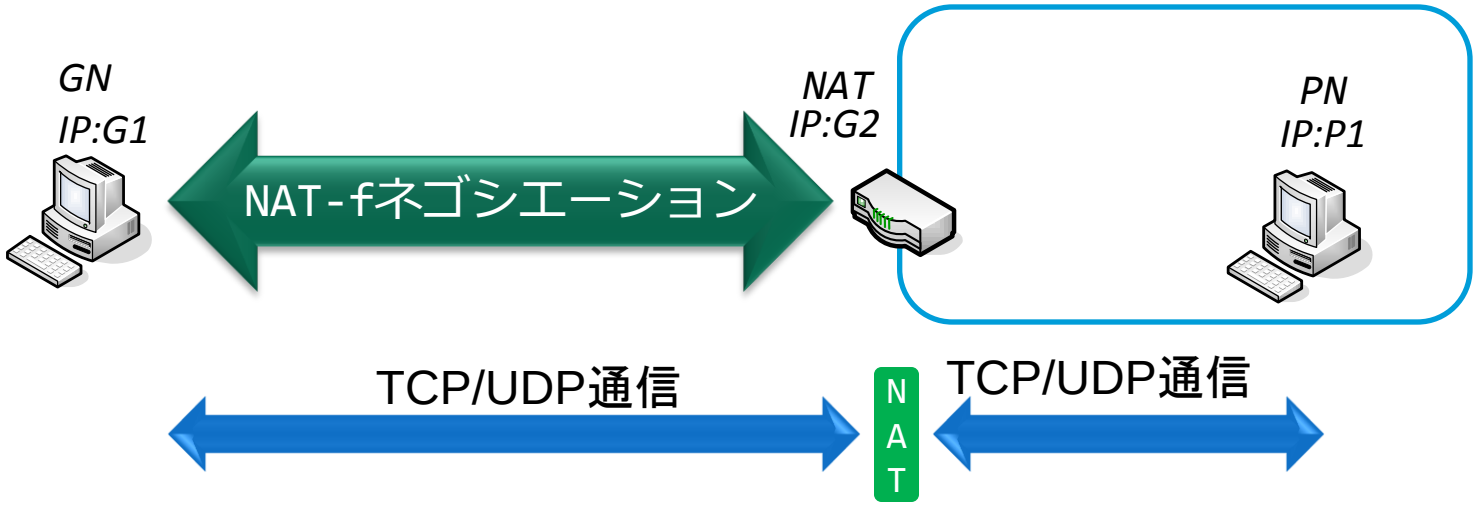
GNAT:GENにNAT機能追加



DPRPに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
  - NAT-fネゴシエーションにより外部から動的にNATテーブルを生成する



DDEとRGIにNAT-fの仕組みを追加

外部動的マッピングによるNAT越えを通信を実現するNAT-fの提案と実装
情報処理学会論文誌，Vol48，No.12，pp.3949-3961，Dec.2007.

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
  - GNATのIPアドレス

Dynamic DNS

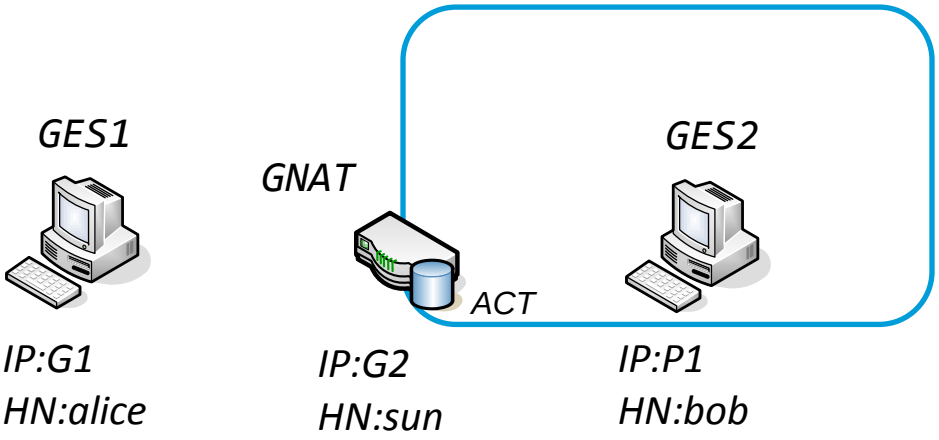
*RR (*Resource Records)

Name	IP
bob	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

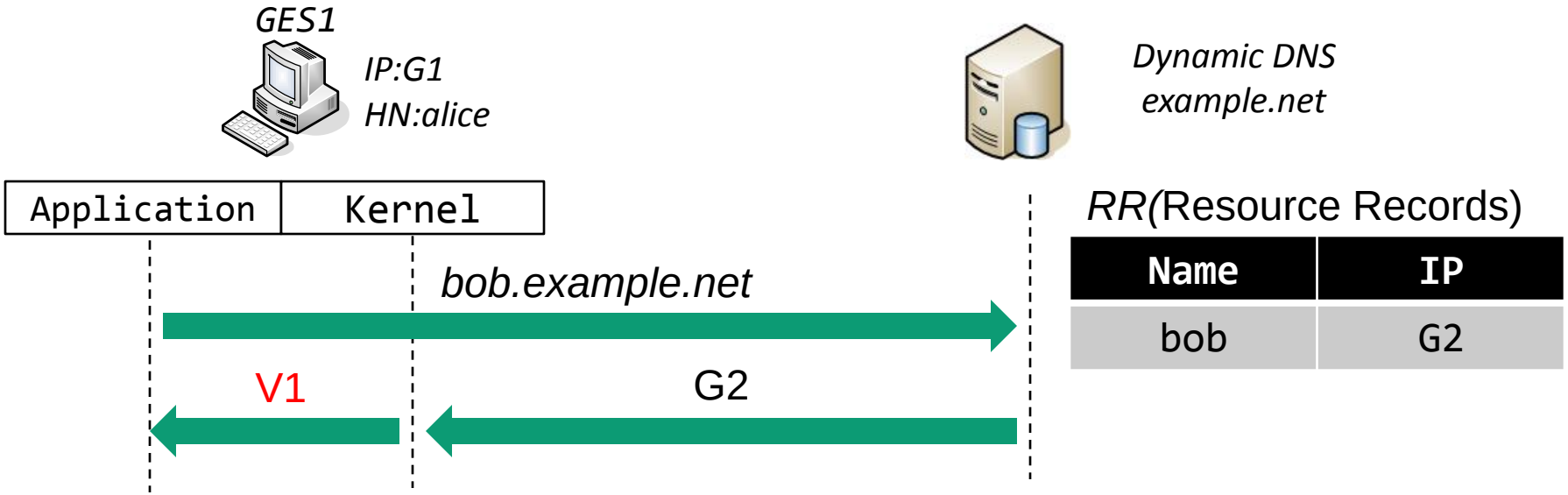
ACT（Access control table）

Name	IP	Authorization
bob	P1	allow



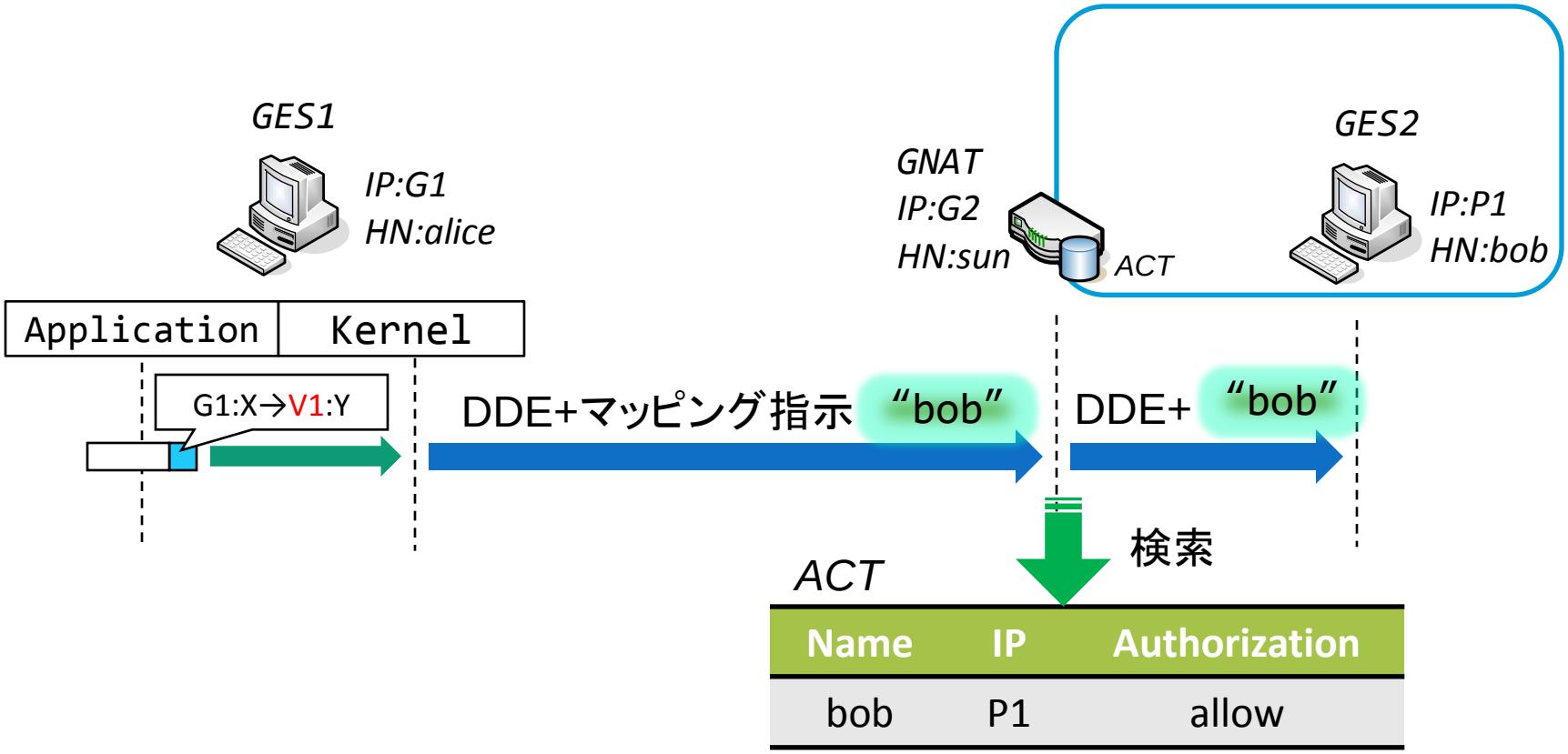
DNS名前解決処理

- 取得IPアドレスを仮想アドレスに書き換え



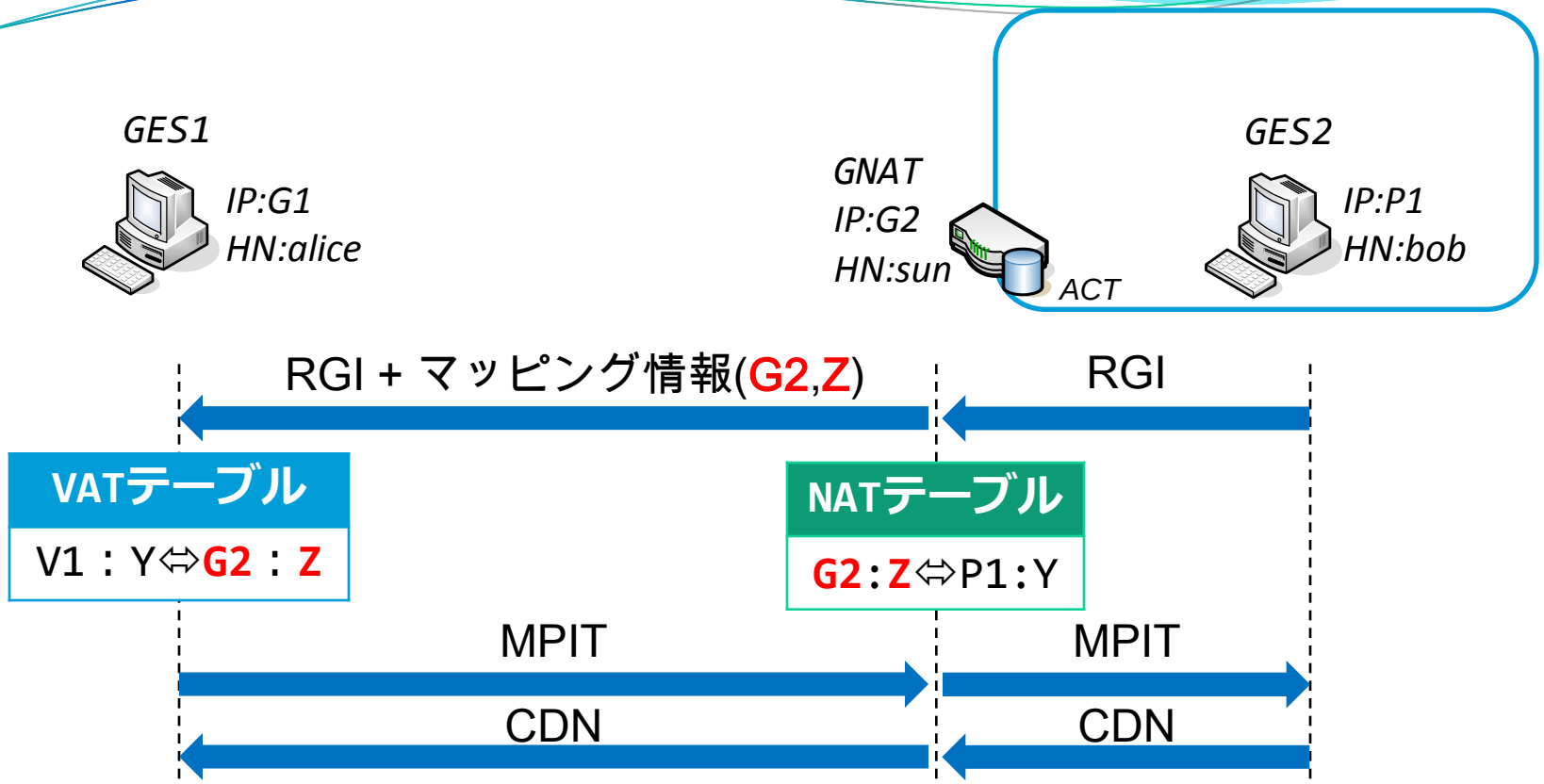
- 仮想IPアドレスはNAT配下の端末を特定するために利用

NAT越えDPRPネゴシエーション



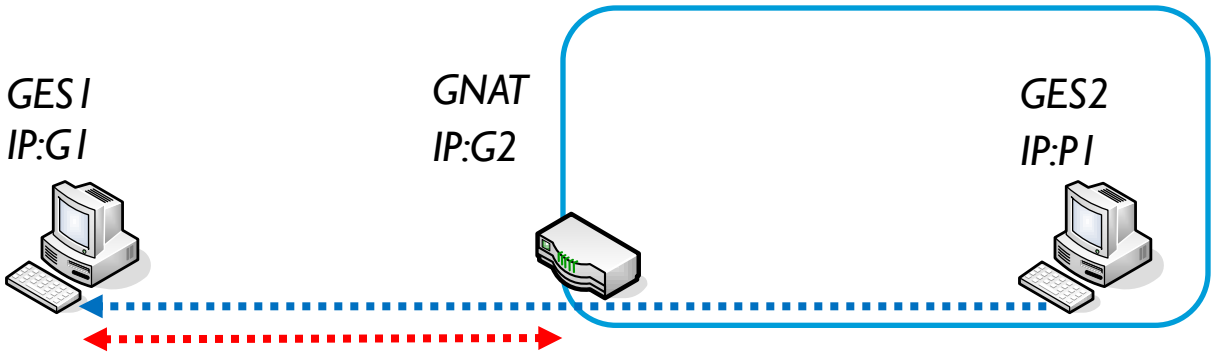
- マッピング指示に必要なホスト名を追加
- ホスト名を用いてACT検索
  - 対応するホスト名のIPアドレスを取得

NAT越え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(Virtual Address Translation)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

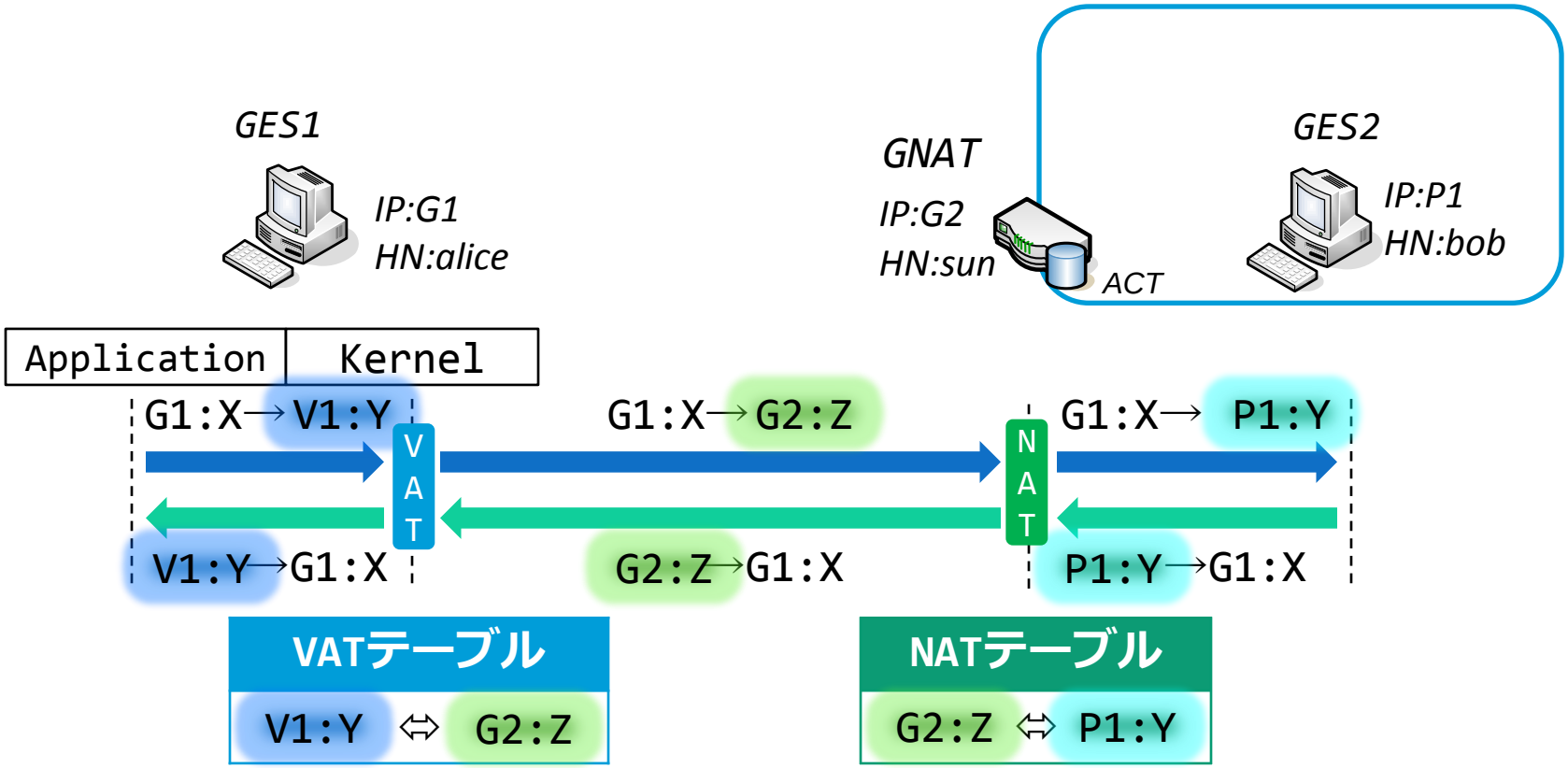
VATテーブル
V1 : Y⇔G2 : Z

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

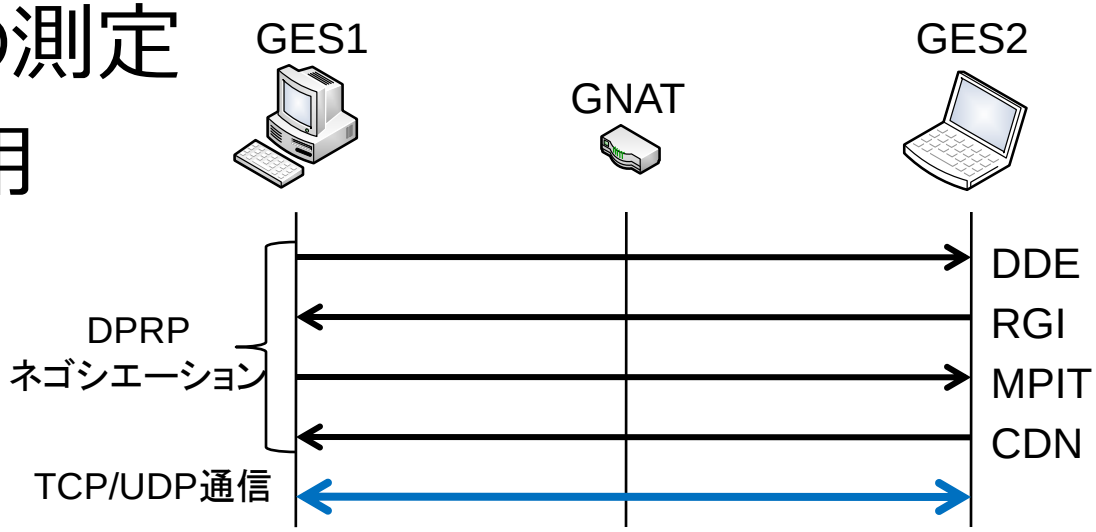


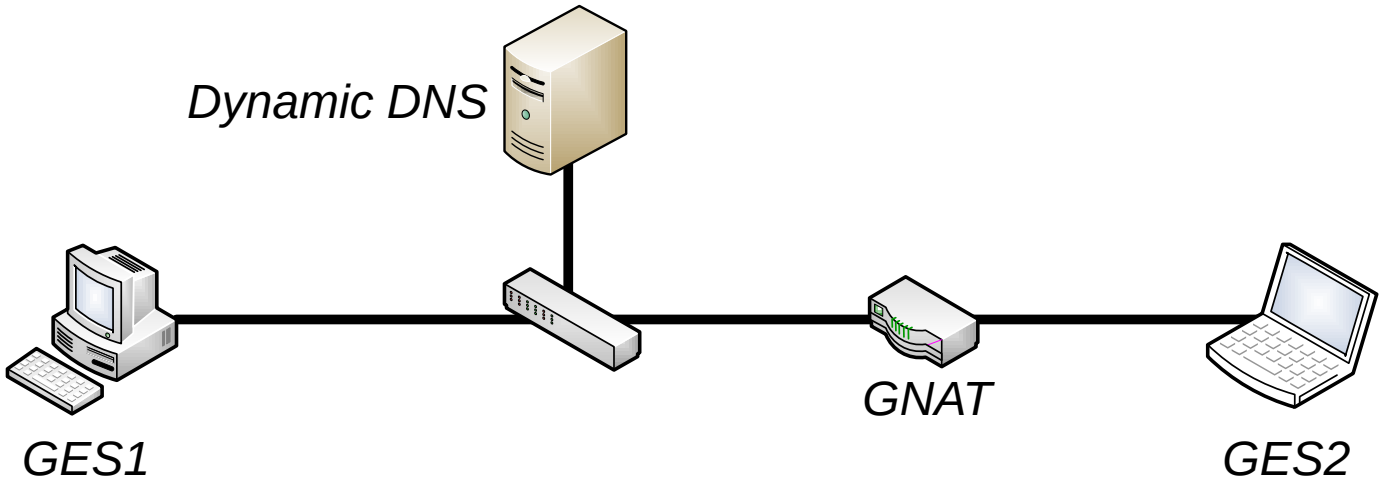
- GES1はNATにマッピング情報に変換して送信
- GA空間側から通信開始が可能になる

性能測定

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

OS:FreeBSD6.1
CPU：Pentium4 3.0GHz
Memory： 1 GB
Ethernet:100BASE-TX





性能測定

- DPRPの処理時間(10回試行の平均値)

DPRPネゴシエーション	1184(μsec)

- スループット(10回試行の平均値)

ポートフォワーディング	93.285Mpbs
暗号化なし	93.458Mpbs
暗号化あり(PCCOM)	93.832Mbps

DPRPが通信に与える影響はほとんどない

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.

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
  - 異なるプライベート空間とのグループ通信

PCCOM (Practical Cipher COMmunication)

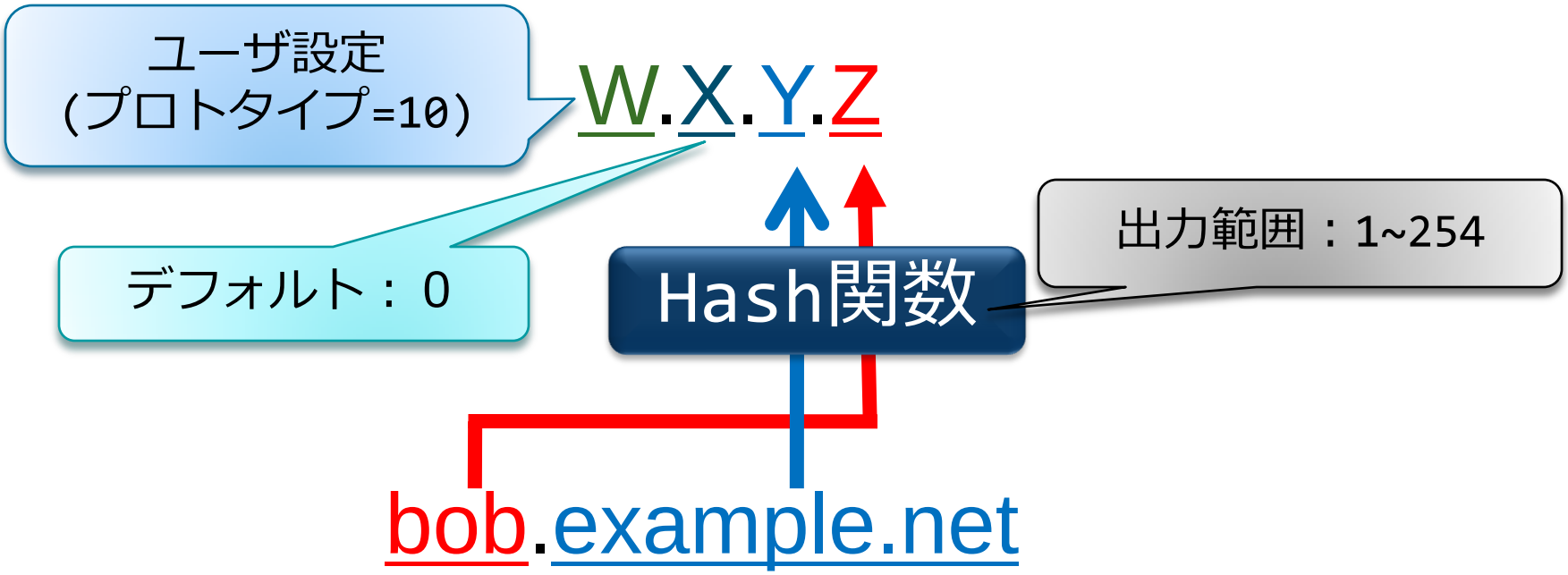
- NA(P)T，ファイアウォールを通過できる
  - 暗号化範囲はユーザデータ部分のみ
  - 完全保証の範囲はIPヘッダから
    - PITの検索過程で保証

- 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のCFBモードを採用

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.

仮想IPアドレス

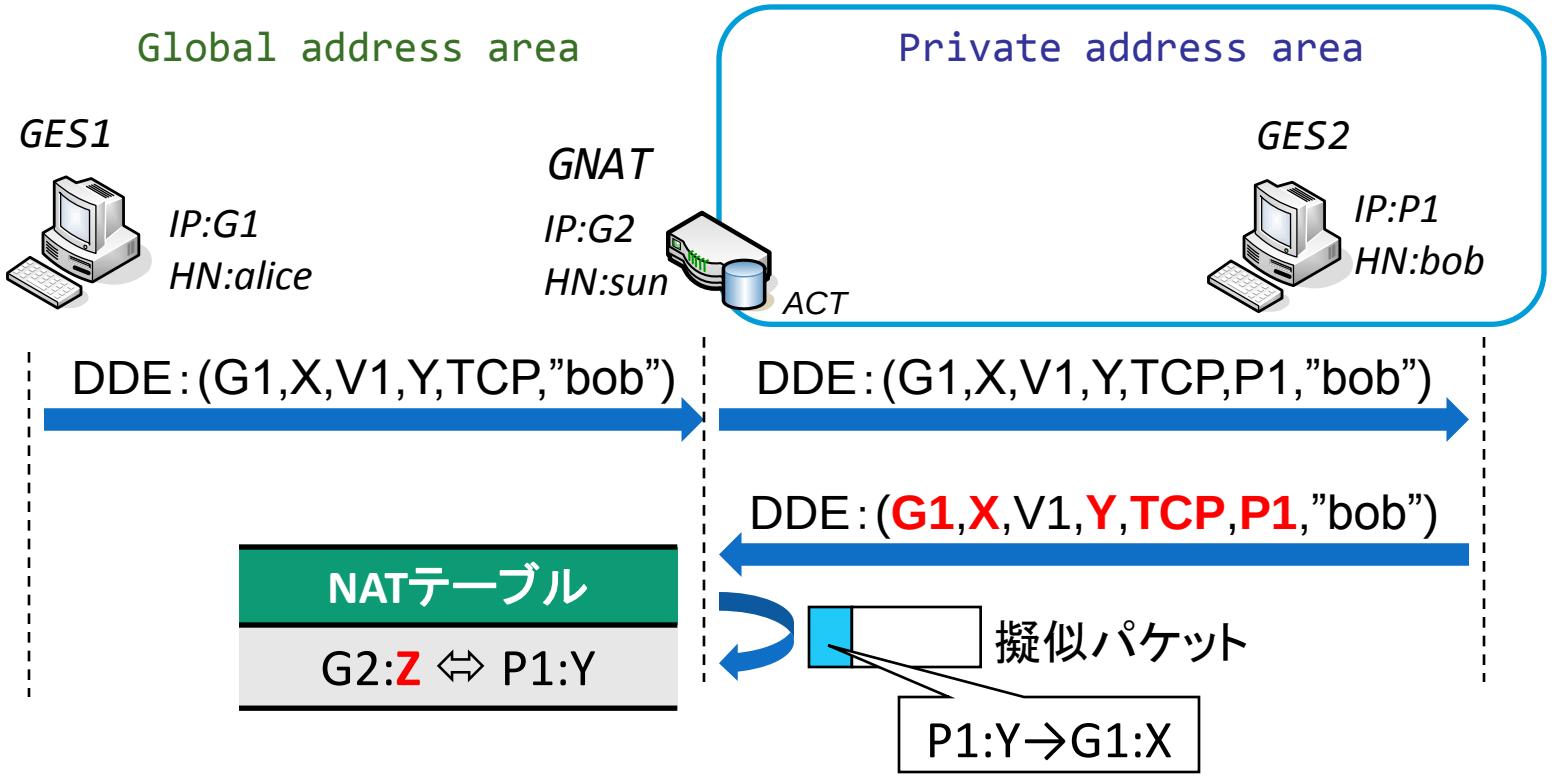
- FQDNに対応して割り当てる



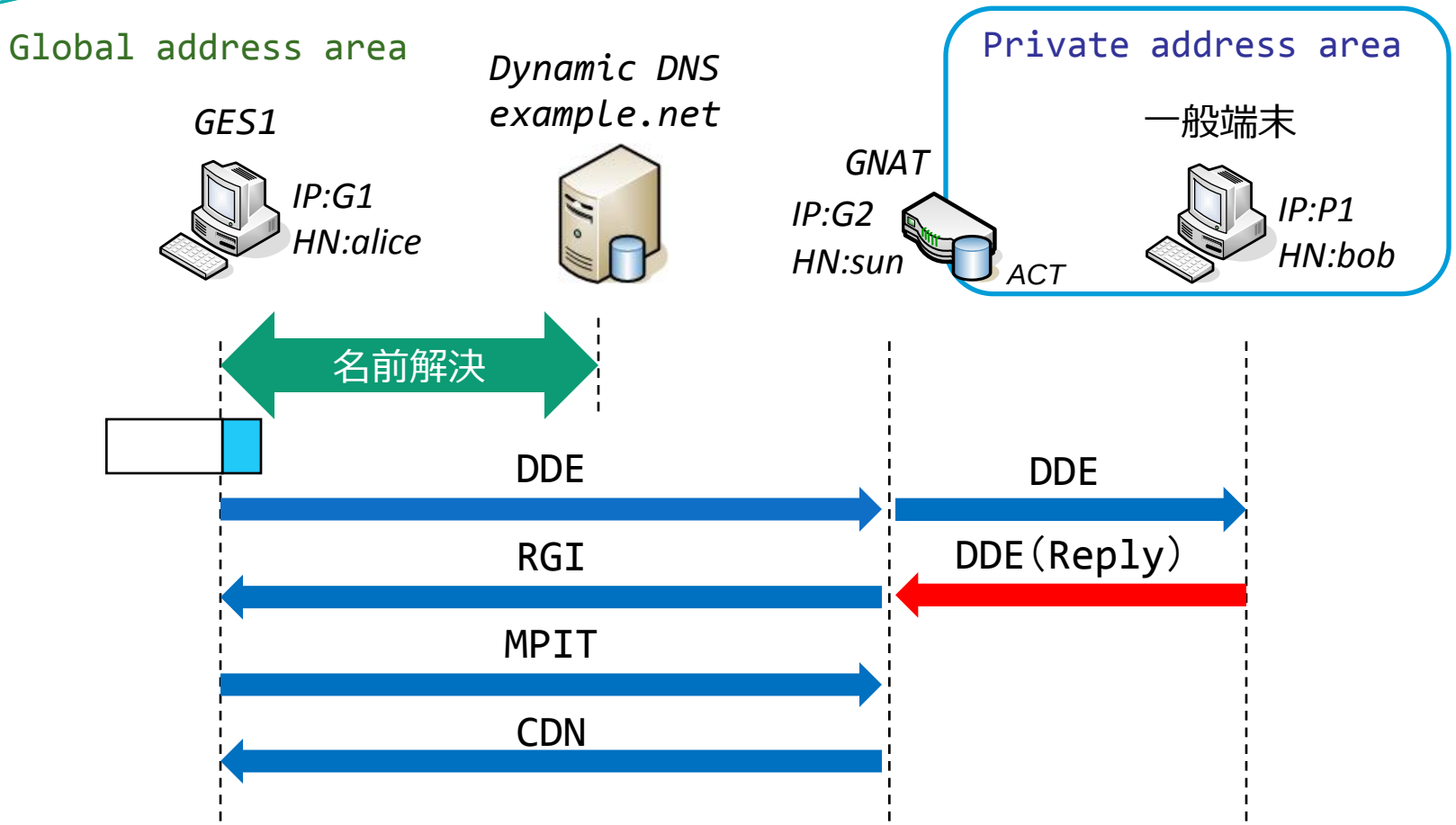
- ハッシュが衝突した場合
  - Xを異なる値に変化

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

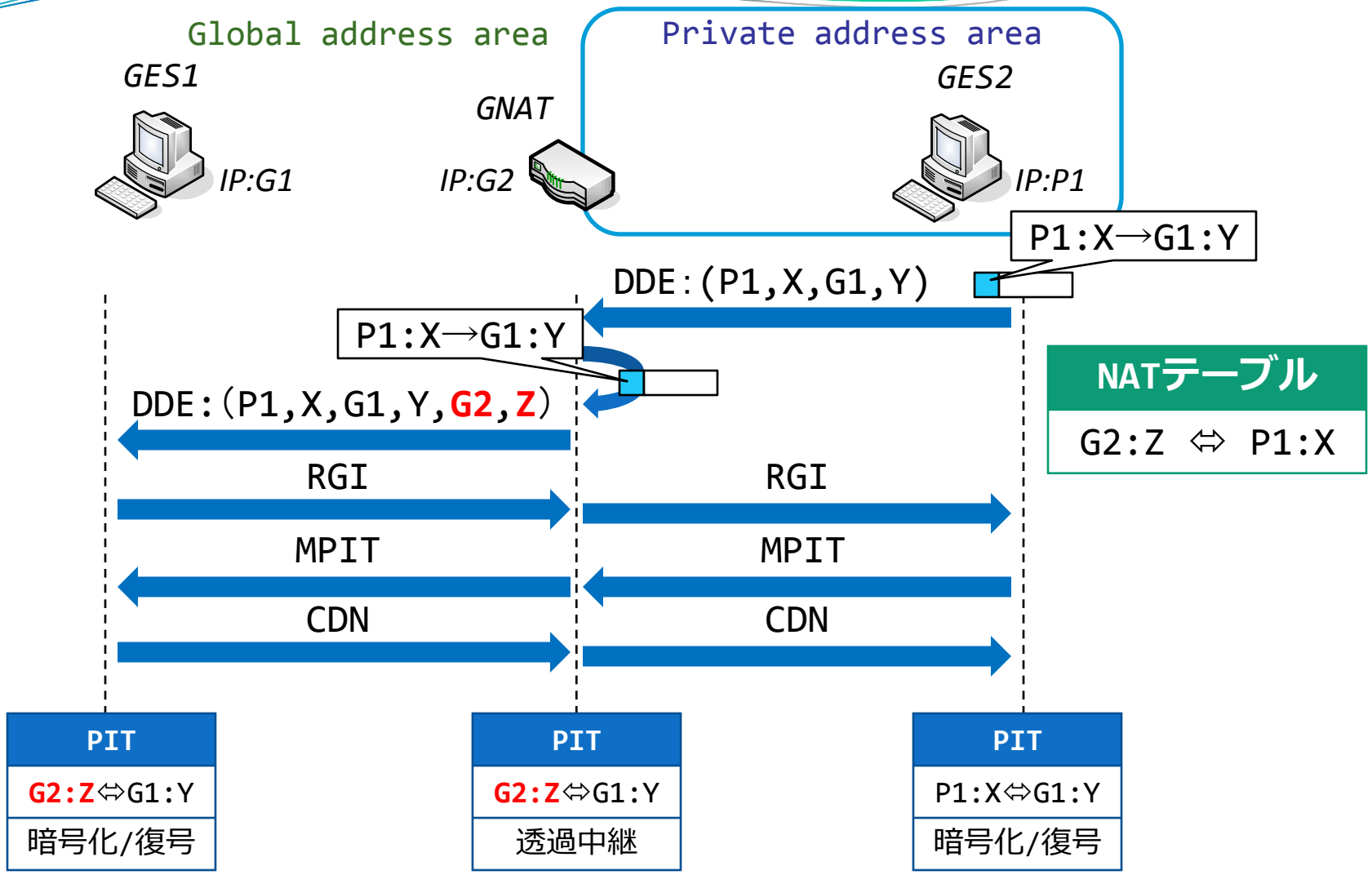


PA空間の端末が一般端末の場合



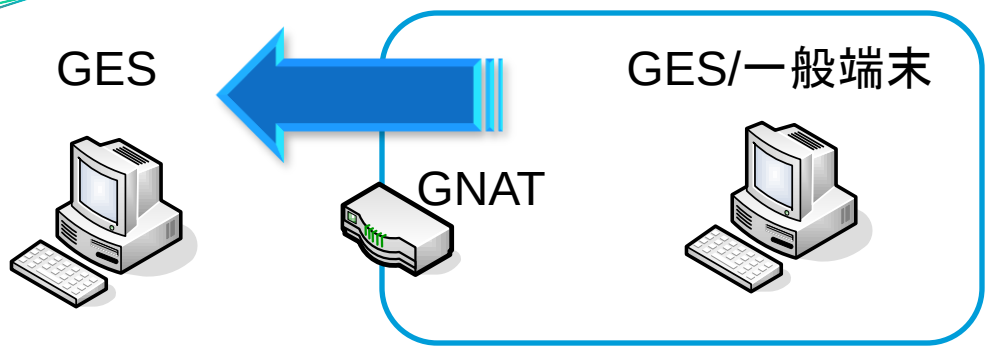
- 一般端末からDDEのReplyが応答される
- その後は，GES1-GNAT間でRGI以降を行う

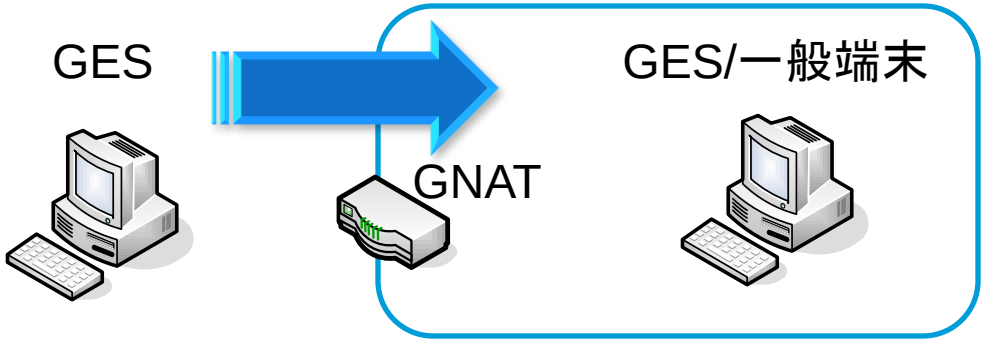
PA空間からGA空間へのDPRP

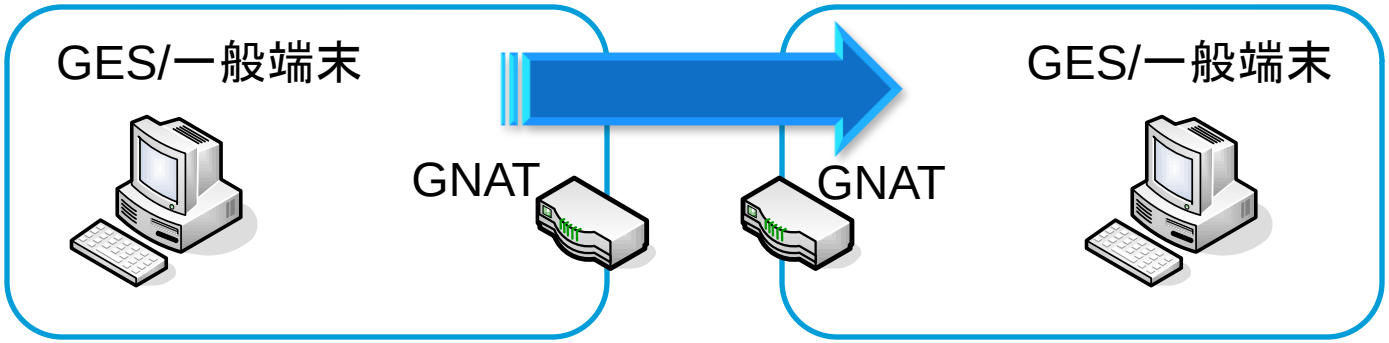


- GES2からGES1へ送信すると見せかけるパケットを送信
- GES1-GNAT間では新たなコネクション情報でPITを生成

DPRPが利用可能な環境

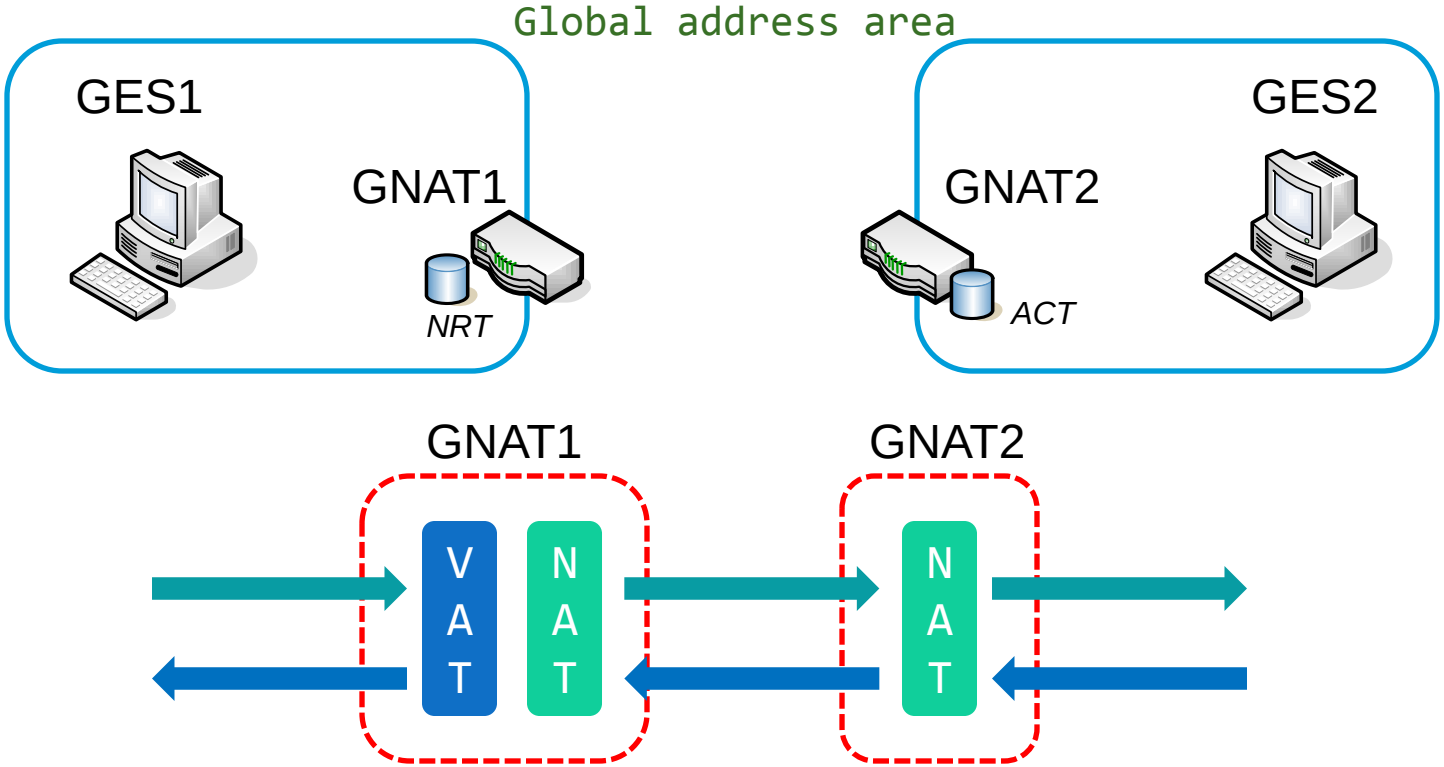






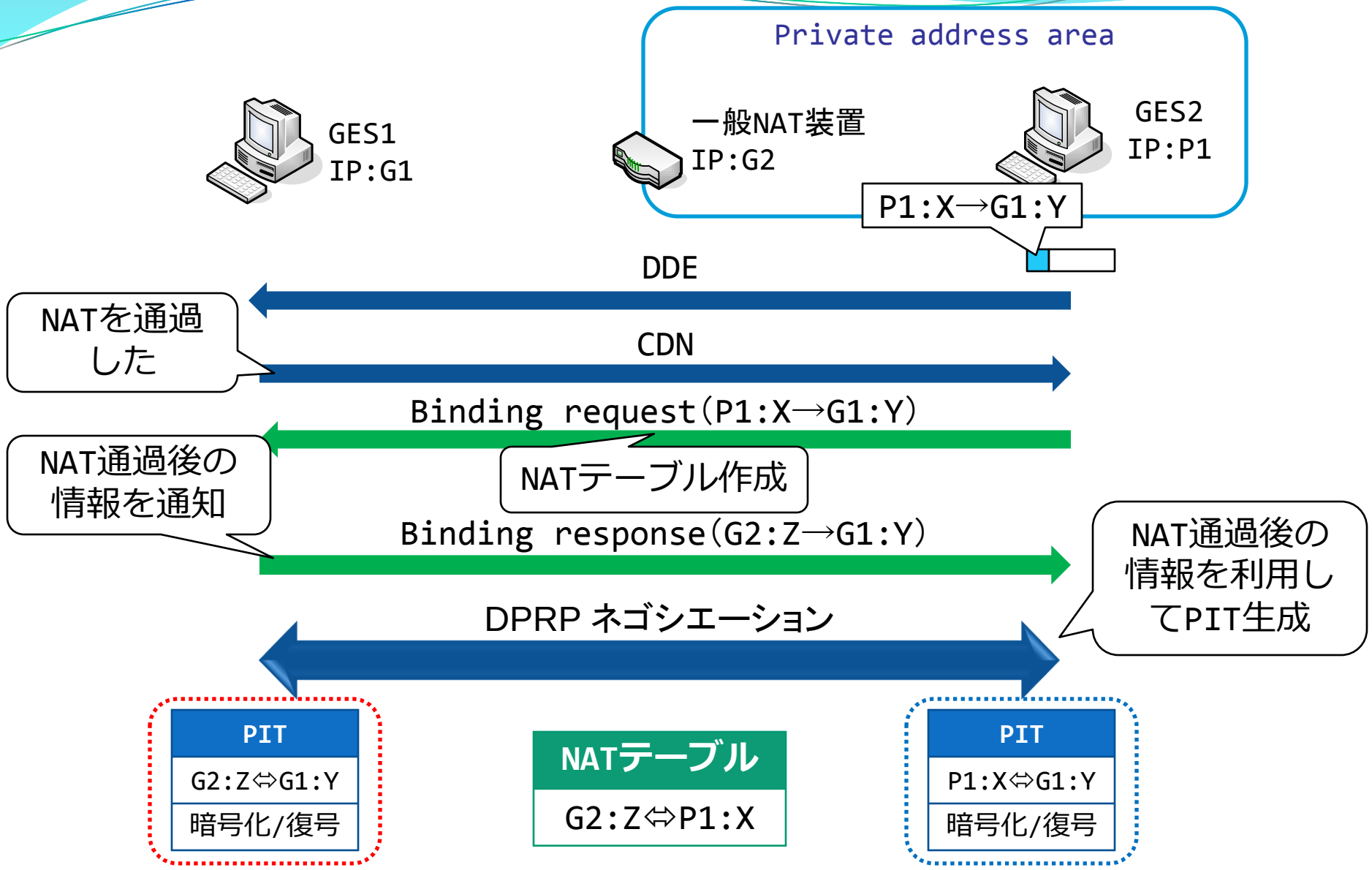
- PA空間の端末は一般端末でも利用可能
- 異なるPA空間同士でも利用可能

異なるPA空間同士の通信

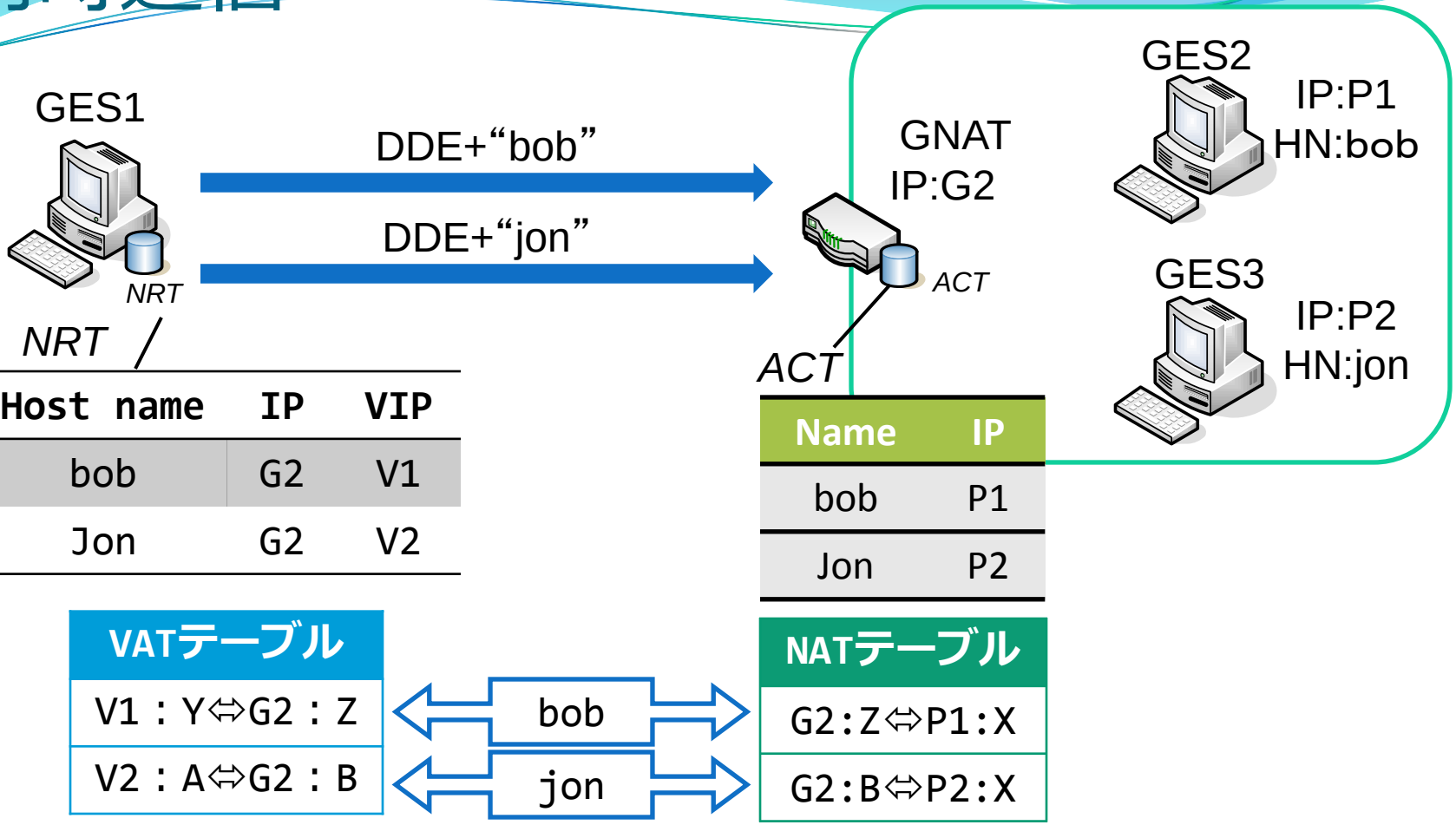


- NRT，VAT処理の位置をGESからGNATに変更
- GNAT 1 とGNAT2でNAT越えに必要な情報を交換

一般NAT装置の場合

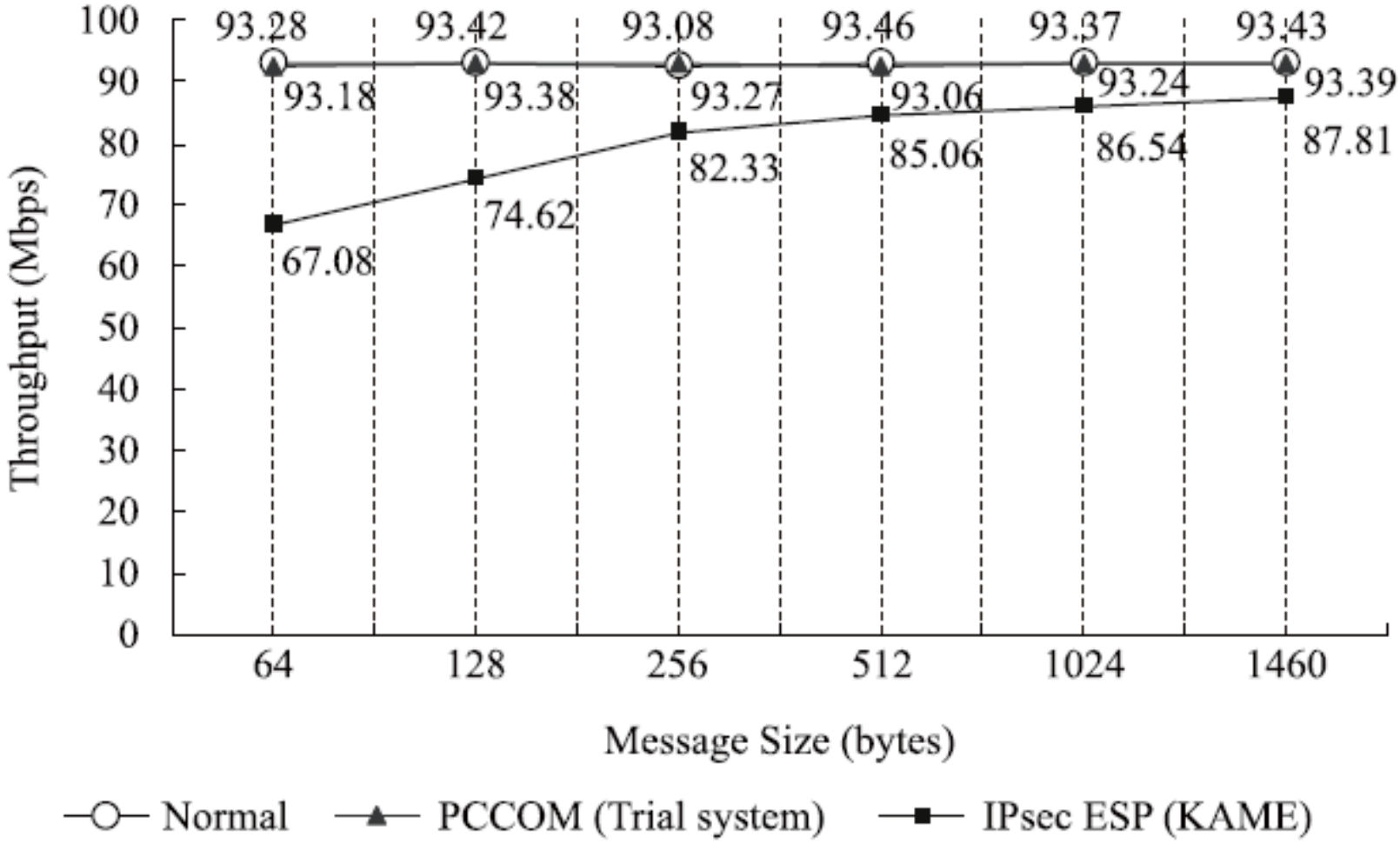

Private address area
GES1
IP:G1
一般NAT装置
IP:G2
GES2
IP:P1
P1:X→G1:Y
DDE
NATを通過した
CDN
Binding request(P1:X→G1:Y)
NATテーブル作成
NAT通過後の情報を通知
Binding response(G2:Z→G1:Y)
NAT通過後の情報を利用してPIT生成
DPRP ネゴシエーション
PIT
G2:Z⇔G1:Y
暗号化/復号
NATテーブル
G2:Z⇔P1:X
PIT
P1:X⇔G1:Y
暗号化/復号
変換後のコネクション情報のPIT
変換前のコネクション情報のPIT

同時通信

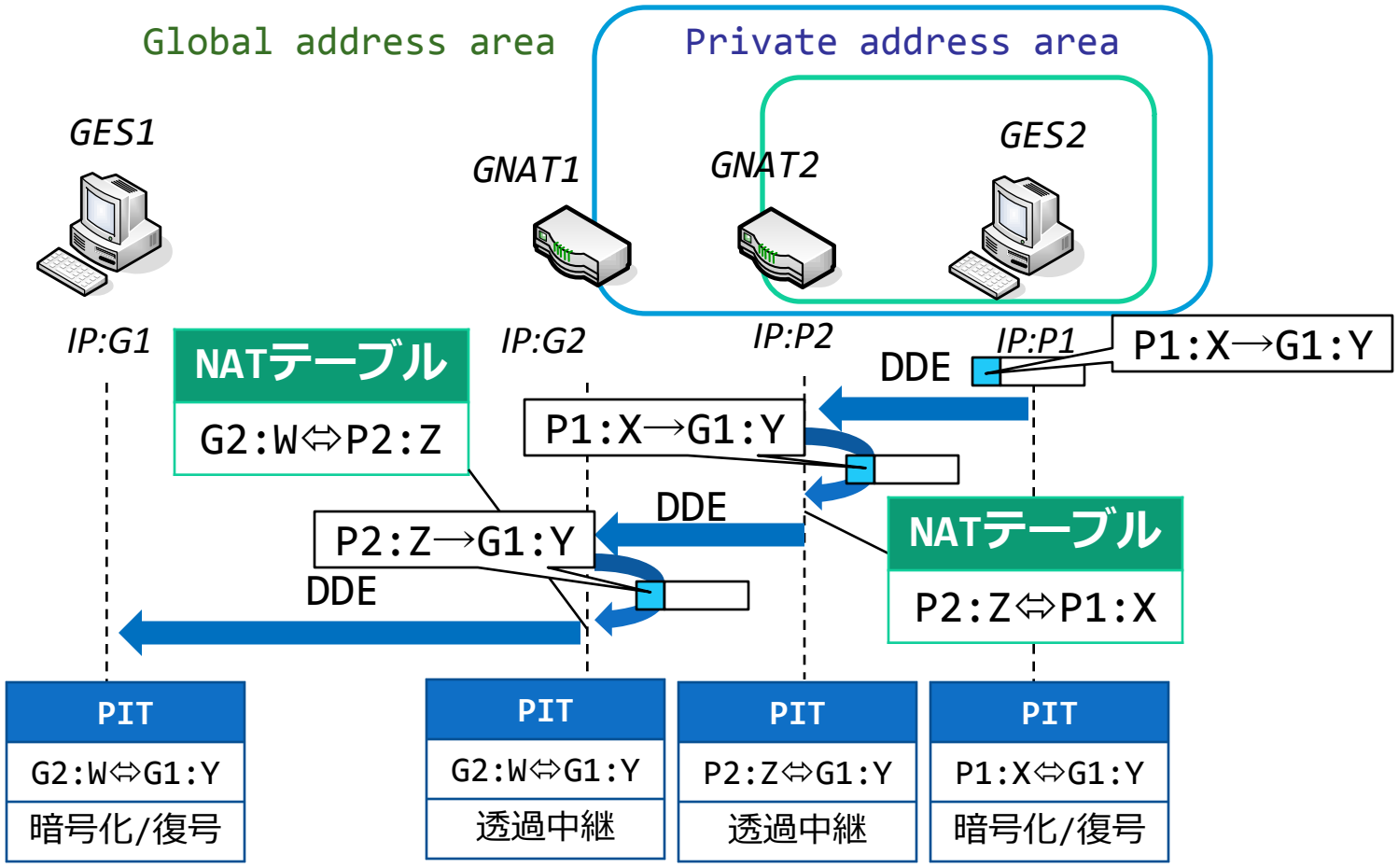


- GES1のアプリケーションは仮想IPアドレスにより NAT配下の端末を区別することが可能
- ホスト名に対応するNATテーブルを生成

PCCOMの性能


Throughput (Mbps)
100
90
80
70
60
50
40
30
20
10
0
93.28
93.42
93.08
93.46
93.37
93.43
93.18
93.38
93.27
93.06
93.24
93.39
67.08
74.62
82.33
85.06
86.54
87.81
64
128
256
512
1024
1460
Message Size (bytes)
Normal
PCCOM (Trial system)
IPsec ESP (KAME)

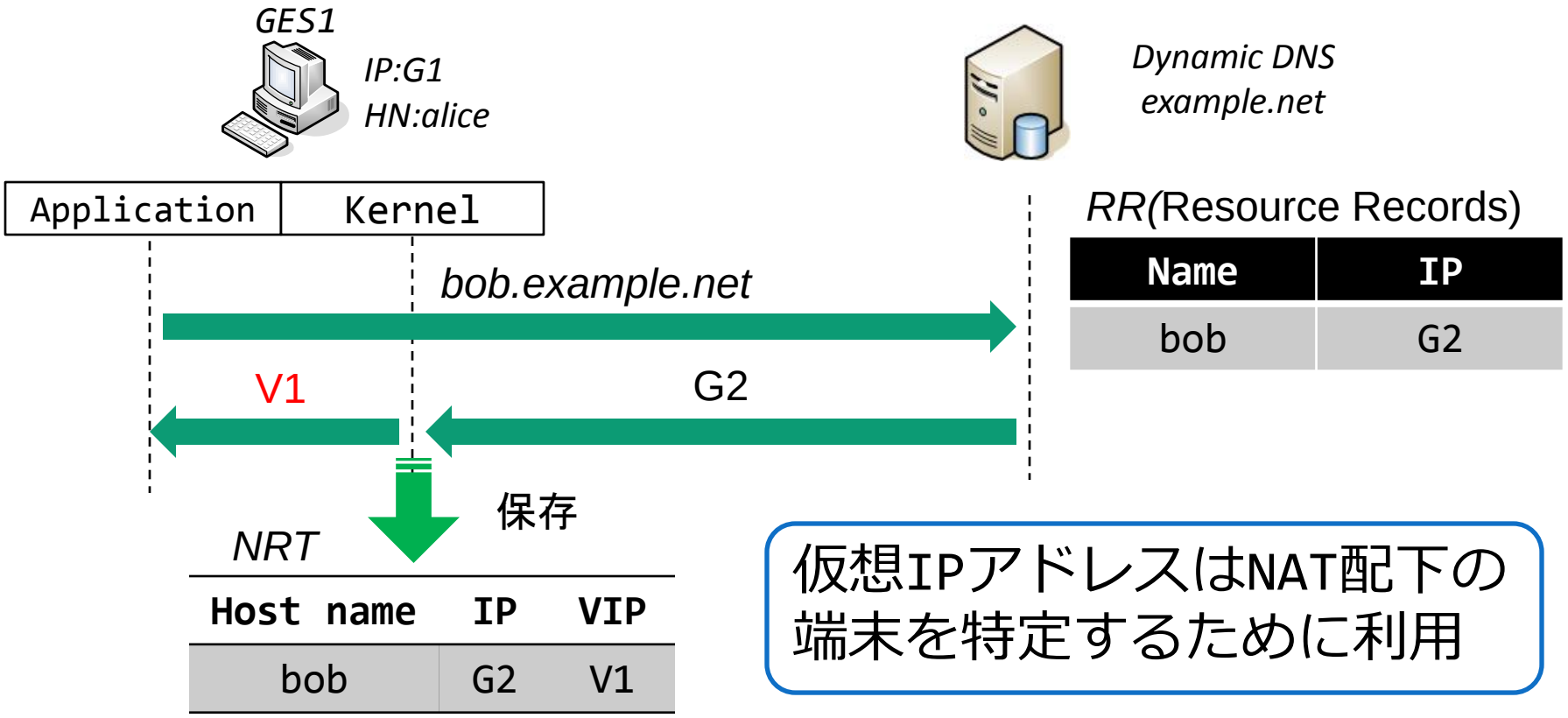
多段NAT構成の場合



- 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

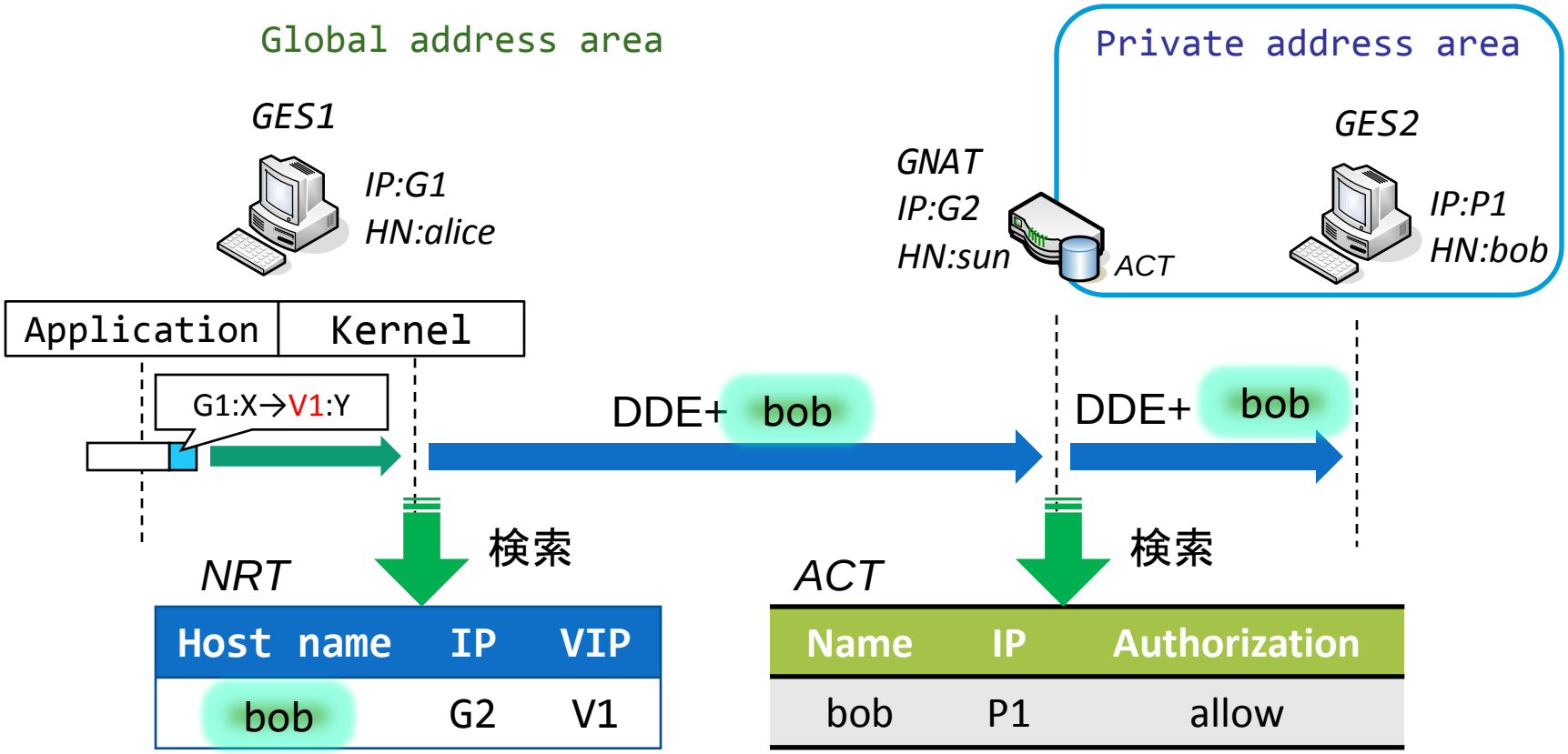
DNS名前解決処理

- 取得IPアドレスを仮想アドレスに書き換え
- 名前関連テーブルNRT（*Name Resolution Table*）
  - ホスト名，IPアドレス，仮想IPアドレスを保存



仮想IPアドレスはNAT配下の端末を特定するために利用

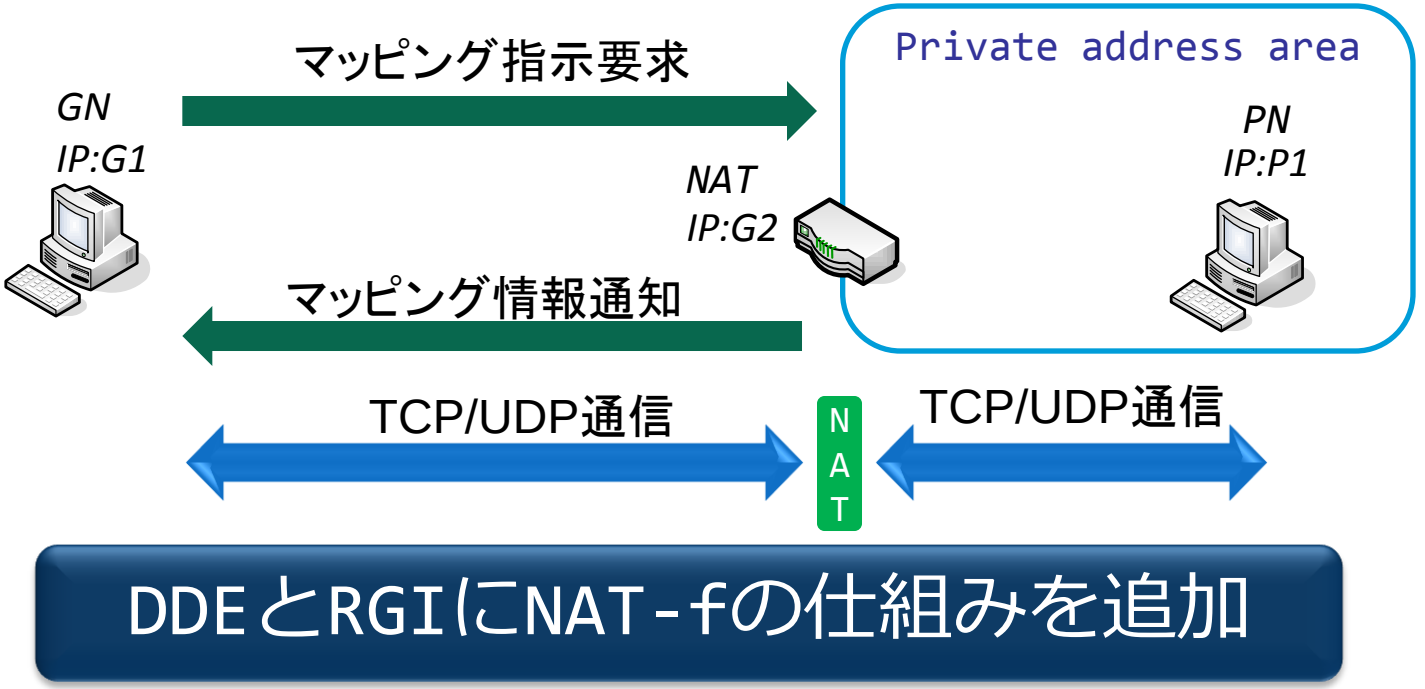
NAT越えDPRPネゴシエーション



- 仮想IPアドレス対応するホスト名をDDEに追加
- 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

NAT-f（NAT-free protocol）

- NAT越えを実現するためのプロトコル
  - 外部ノードからNATに対してマッピング処理を指示
  - マッピング情報の通知
  - マッピングされたポート宛に変換して送信



DDEとRGIにNAT-fの仕組みを追加

外部動的マッピングによるNAT越えを通信を実現するNAT-fの提案と実装
情報処理学会論文誌，Vol48，No.12，pp.3949-3961，Dec.2007.