NAT越えを可能にするDPRPの検討

後藤裕司[†]　鈴木秀和[†]　渡邊　晃[†]

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．

Researches on Extended Dynamic Process Resolution Protocol that Can Traverse NAT

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

As the security measures against threads 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.

1. はじめに

近年企業ネットワークでは不正侵入，データの盗聴や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に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．

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

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．この結果，プライベートアドレス空間とグローバルアドレス空間を跨る通信グループの定義が可能となった．本論文の NAT 装置は IP アドレスに加えポート番号の変換を行う NAPT（Network Address Port Translator)[6] のことも含む．

以下に第 2 節に GSCIP の概要，第 3 節に動的解決プロトコル DPRP，第 4 節に NAT 越えが可能な NAT 越え DPRP，第 5 節に NAT 越え DPRP の実装，第 6 節にまとめを述べる．

2. GSCIP の概要

GSCIP ではサブネット単位とホスト単位のセキュリティが混在する環境においてセキュリティと柔軟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 realize for Software)，サブネットを構成するルータタイプの GEN(GE realize 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．各ホストが所持する GK を用いて GE 間の通信を暗号化する．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を容易に定義することができる．グループ鍵 GK は各 GE が起動時に管理装置 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．

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

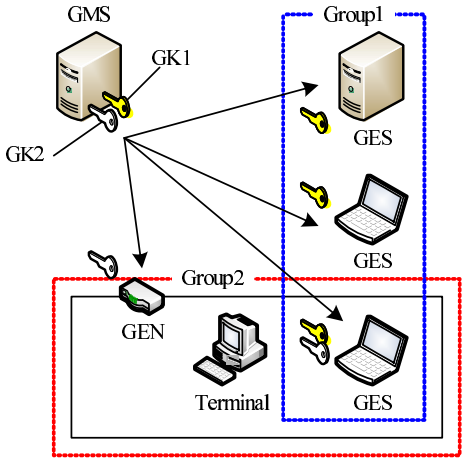


図 1 通信グループの定義方法

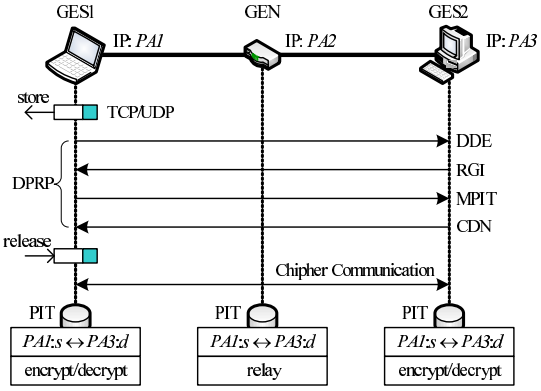


図 2 DPRP ネゴシエーション

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，これらに一致した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），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しめるものである．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

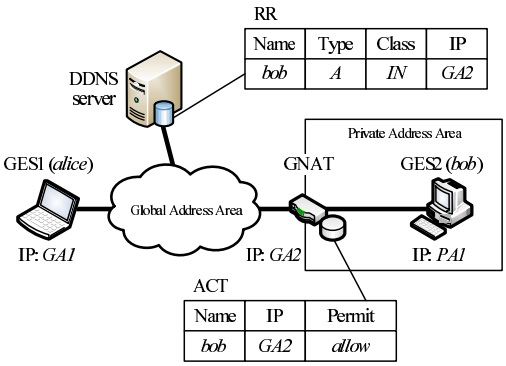


図 3 システム構成と初期情報

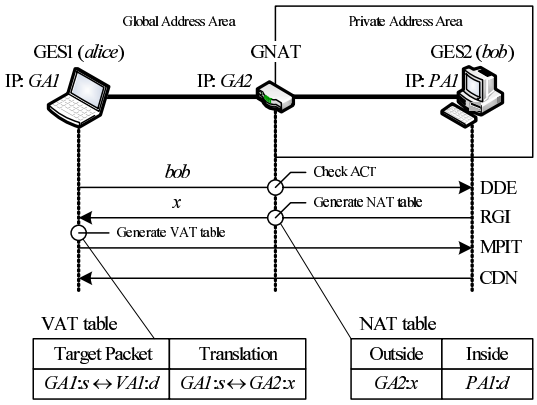


図 4 NAT 越え DPRP の動作

ケットを一時的に待避し，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．図 2 において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，すべての装置がグローバルアドレス空間あるいはプライベートアドレス空間に存在する場合に有効であり，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，プライベートアドレス (以下 PA) 側から通信が始まる場合，及びグローバルアドレス (以下 GA) 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．前者については検討を既に終え実現方法が明確になっている[7]．本稿では後者の場合について詳細に検討を行った．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 ICE[8],UPnP[9],AVES[10] のような NAT 越え通信を実現する我々が提案しているプロトコル NAT-f（NAT-free)[11] の技術を用いることにより DPRP の拡張を行った．

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 が存在し，NAT 機能を追加した GEN を GNAT と呼ぶことにする．ダイナミック DNS（以下 DDNS)[12] 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（PA1），および外部からのアクセスの可否を GNT 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をとして GNAT のアドレス GA2 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 アドレスと GES2 のホスト名を取得する．さらに GNAT の IP アドレスを仮想 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 ”を通知する．その後，上位ソフトウェアから GNAT 宛に TCP/UDP パケットを送信すると，カーネルにおいて上記パケットを待避して拡張 DPRP ネゴシエーションを行う．図 4 に拡張 DPRP の動作を示す．最初の DDE には NRT テーブルから得た通信相手のホスト名“ bob ”を追加して GNAT 宛に送

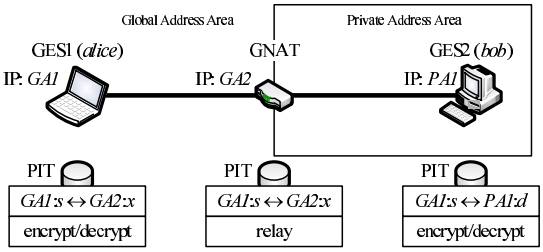


図 5 NAT 環境に対応した PIT

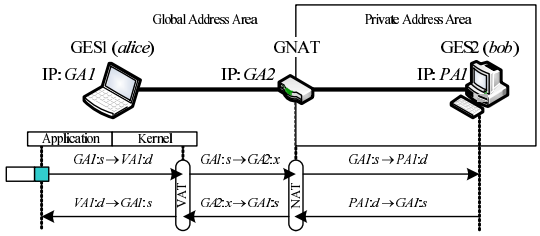


図 6 アドレス変換処理

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 PA1 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“ PA1 ”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，ポート番号と GNAT の IP アドレス，ポート番号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．その後の処理は従来の DPRP と同様である．

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．そこで NAT に対応した PIT は，通信相手の見え方によって異なる内容となる．図 5 に NAT に対応した PIT を示す．GES2 は GES1 が通信相手に見えるため GES2 と GES1 に対応した PIT の生成を行う．GES1 は通信相手が GNAT に見えるため，GES1 と GNAT に対応した PIT の生成を行う．GNAT は NAT で変換後のコネクション情報を用いて PIT の生成を行う．

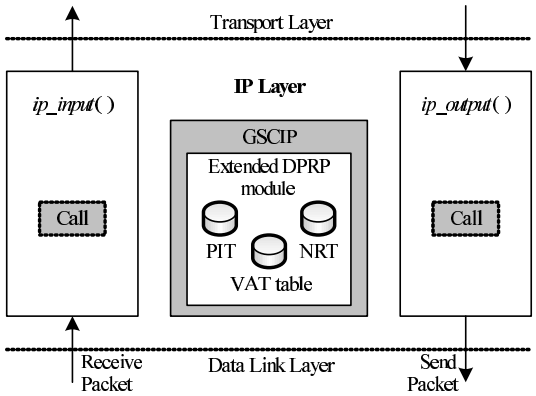


図 7 GES の実装概要

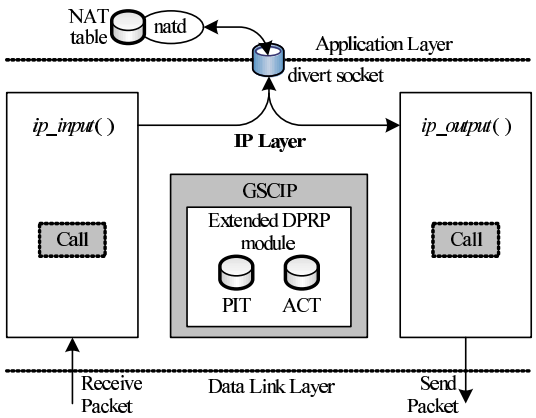


図 8 GNAT の実装概要

4.3 アドレス変換処理

図 6 に通信パケットがアドレス変換されていく様子を示す．GES1 は DPRP ネゴシエーション終了後，一時的に待避していた 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 GA2:x に変換して送信する．GNAT では NAT テーブルに従って宛先の IP アドレスとポート番号“ GA2:x ”を“ PA1:d ”に変換して GES2 に送信する．逆方向のパケットは上記と逆の変換を行う．

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 7 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．PIT，NRT，VAT テーブルはカーネル空間に作成して，不要になったら削除する．図 8 に GNAT の実装概要を示す．GNAT には DPRP モジュールに加えて 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 DPRP のを可能とする方式を提案した．この結果，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評価を行う．

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) Srisuresh, P. and Holdrege, M.: IP Network Address Translator (NAT) Terminology and Considerations, RFC2663, IETF (1999).
7) 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，情報処理学会第 68 回全国大会講演論文集 (2006).
8) Rosenberg, J.: Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offer/Answer Protocols, Internet-draft, IETF (2006). draft-ietf-mmusic-ice-12.txt.
9) UPnP Forum: *Internet Gateway Device (IGD) Standardized Device Control Protocol V 1.0* (2001). http://www.upnp.org/standardizeddcps/igd.asp.
10) Ng, T., Stoica, I. and Zhang, H.: A Waypoint Service Approach to Connect Heterogeneous Internet Address Spaces, *Proc. USENIX Annual Technical Conference*, pp.319–332 (2001).
11) 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，マルチメディア，分散，協調とモバイル (DICOMO2006) シンポジウム論文集，pp.453–456 (2006).
12) Vixie, P., Thomson, S., Rekhter, Y. and Bound, J.: Dynamic Updates in the Domain Name System (DNS UPDATE), RFC 2136, IETF (1997).

NAT越えを可能にするDPRPの検討

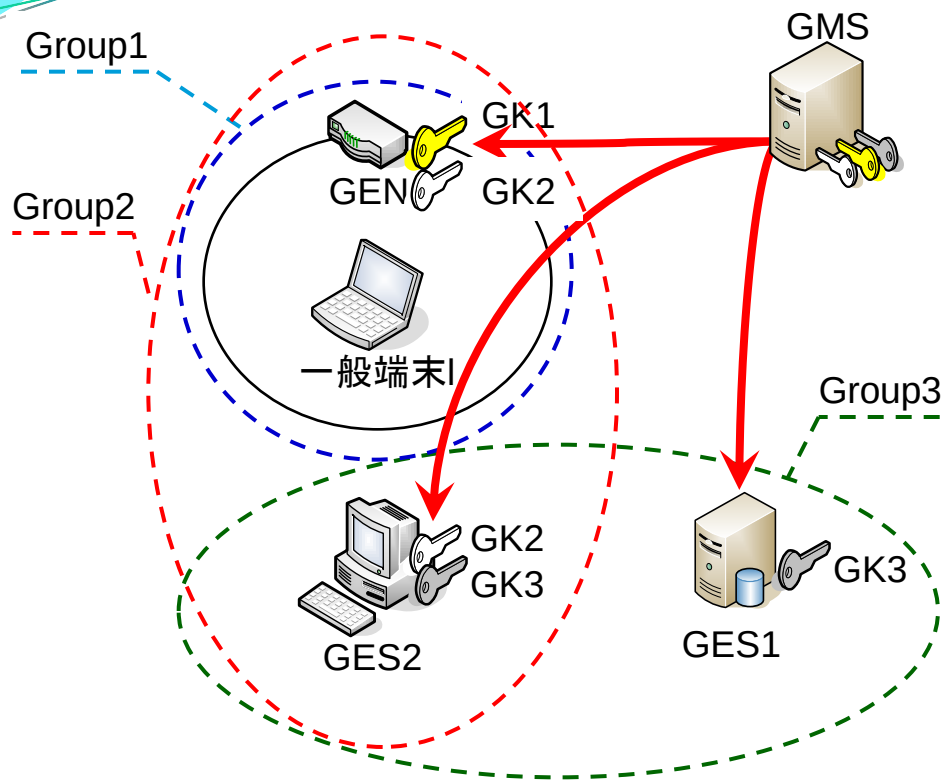
名城大学大学院
後藤　裕司
鈴木　秀和
渡邊　晃

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

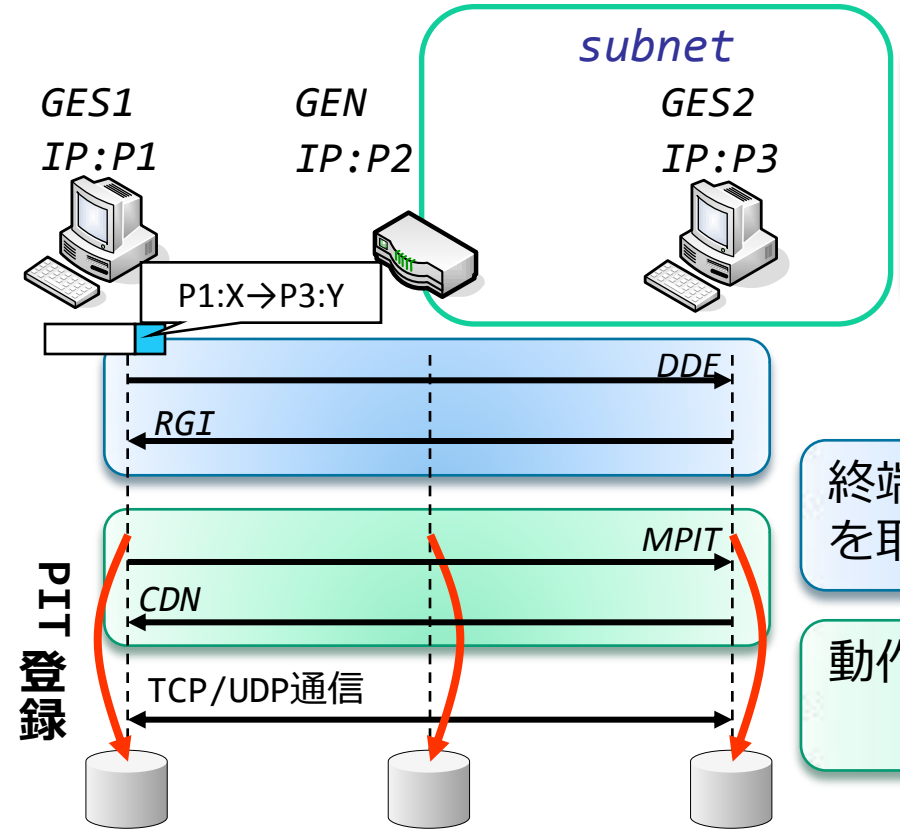


GE：GSCIP対応した装置
✓GES（Software型）:ホストタイプ
✓GEN（Network型）：ルータタイプ
GMS：管理装置

- GMSは各GEにグループ番号とグループ鍵GKを配送
- 同一グループ間は暗号化

- 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

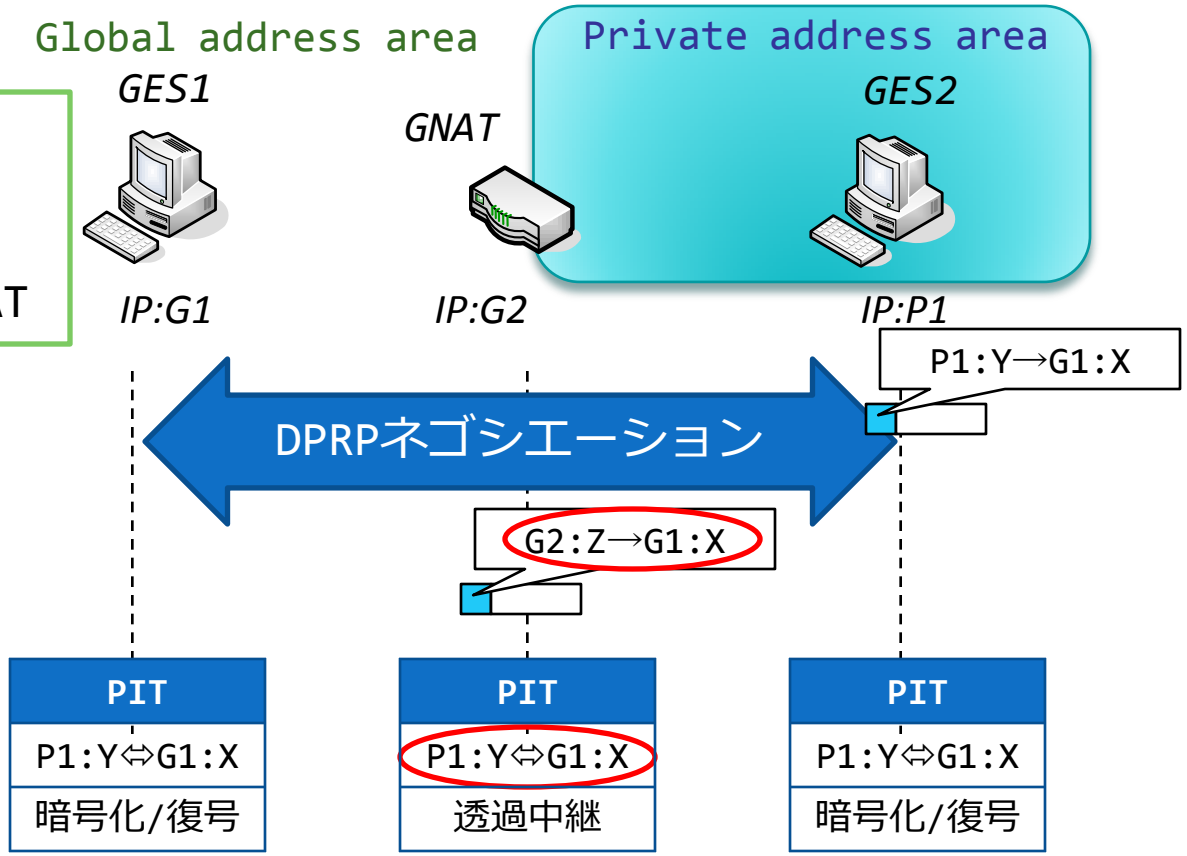
通信経路上にNATが存在する場合

Private→Global

GA空間：*GES1*

PA空間：*GES2*

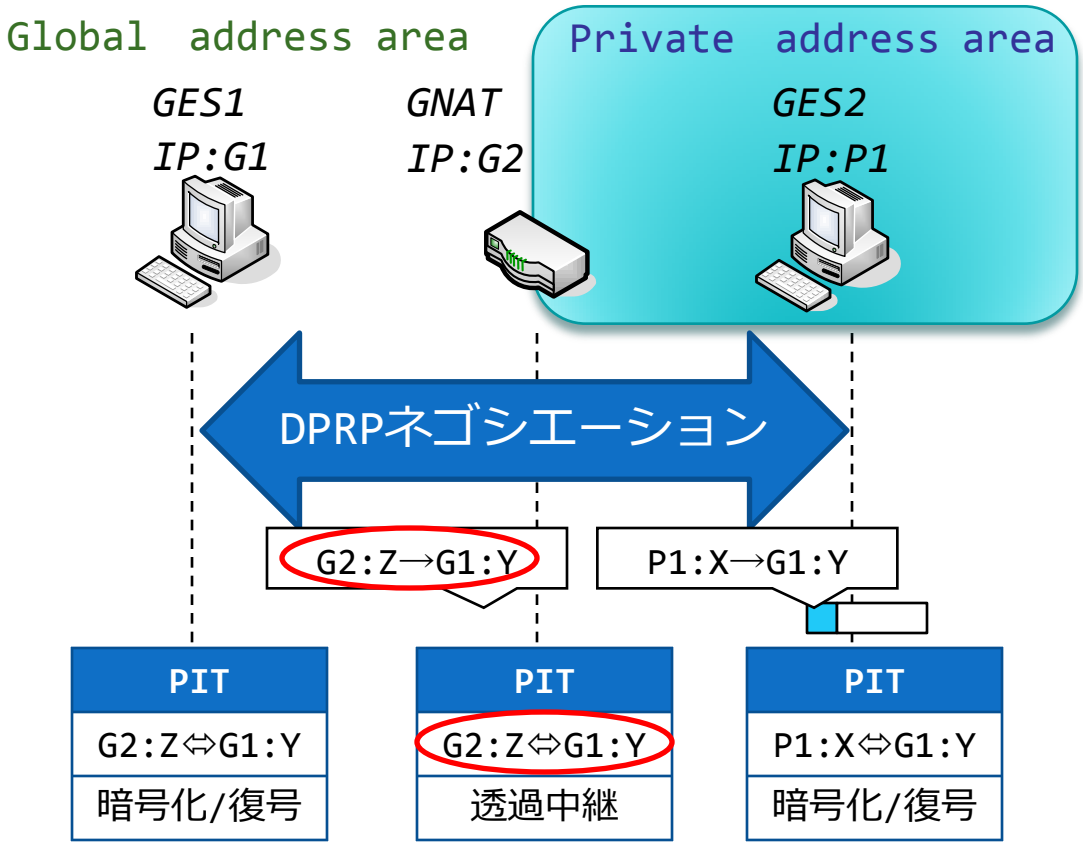
NAT機能を追加：GNAT



- パケットのコネクション情報とPITの内容が一致しない
  - 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が変換される

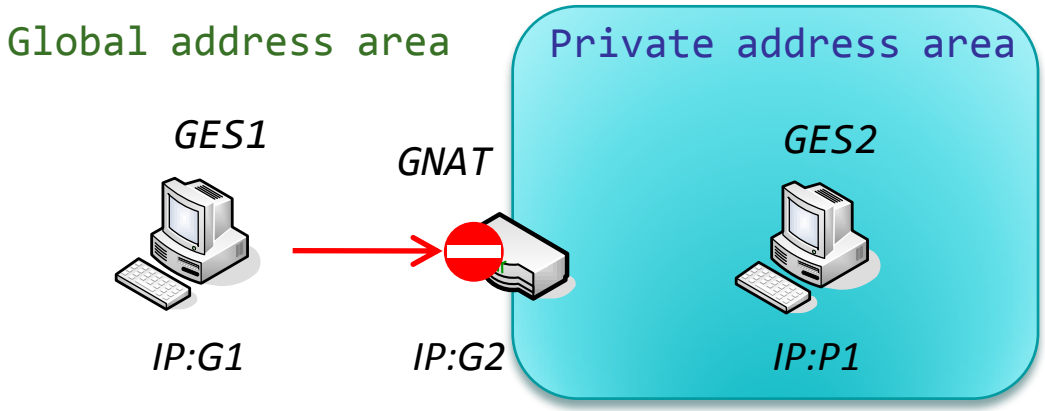
PA空間からGA空間へのDPRP

実装済み



- GES1とGNAT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

GA空間からPA空間へのDPRP



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
  - GNATのIPアドレス

Dynamic DNS

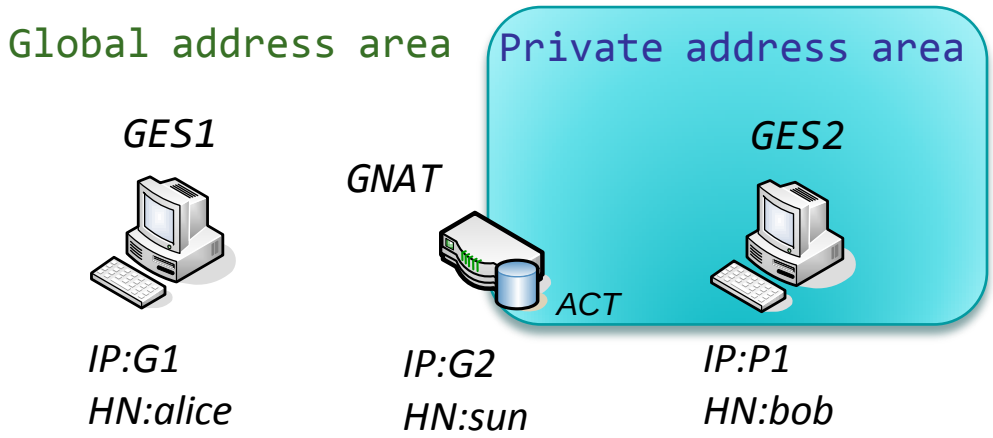
RR (Resource Records)

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

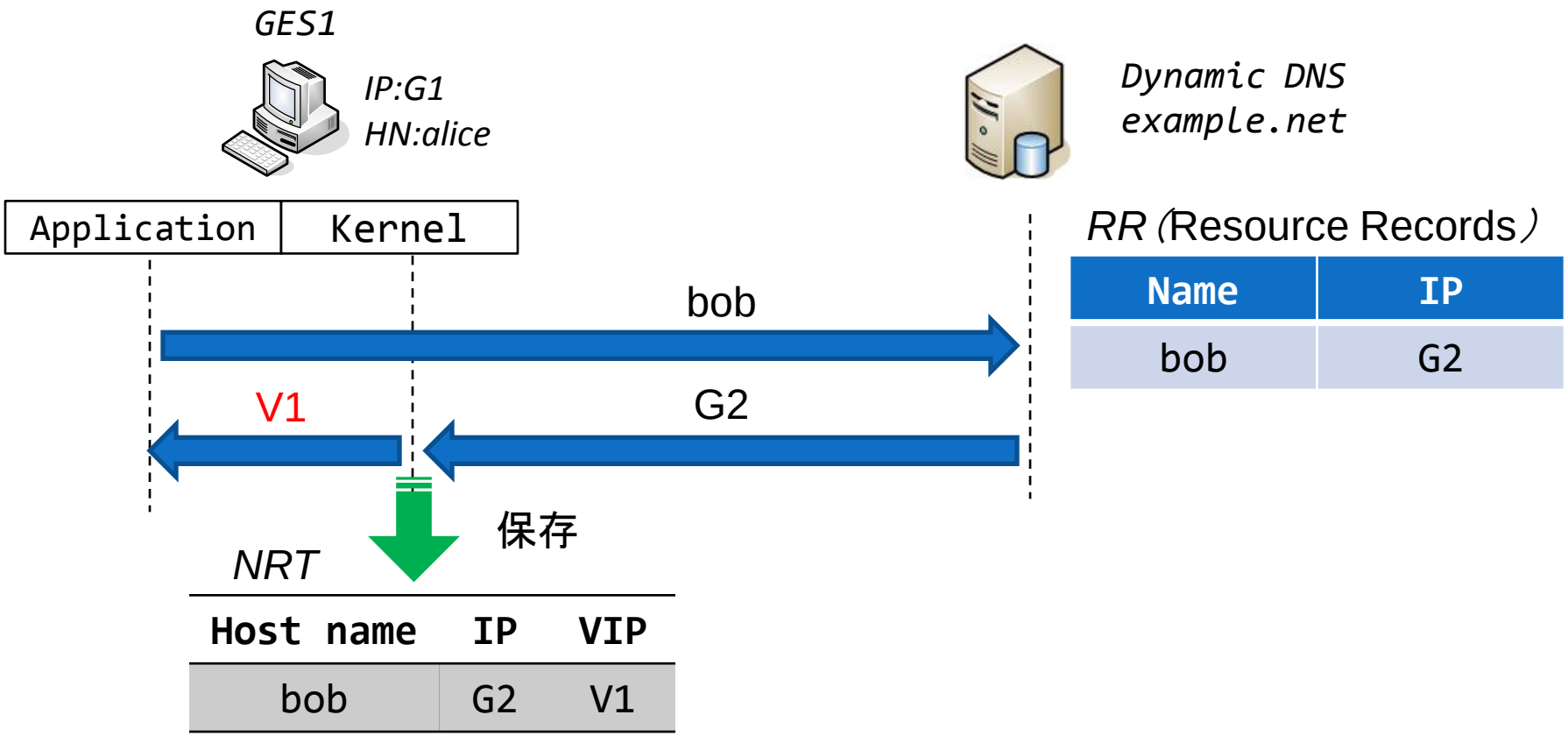
ACT (Access control table)

Name	IP	Authorization
bob	P1	allow

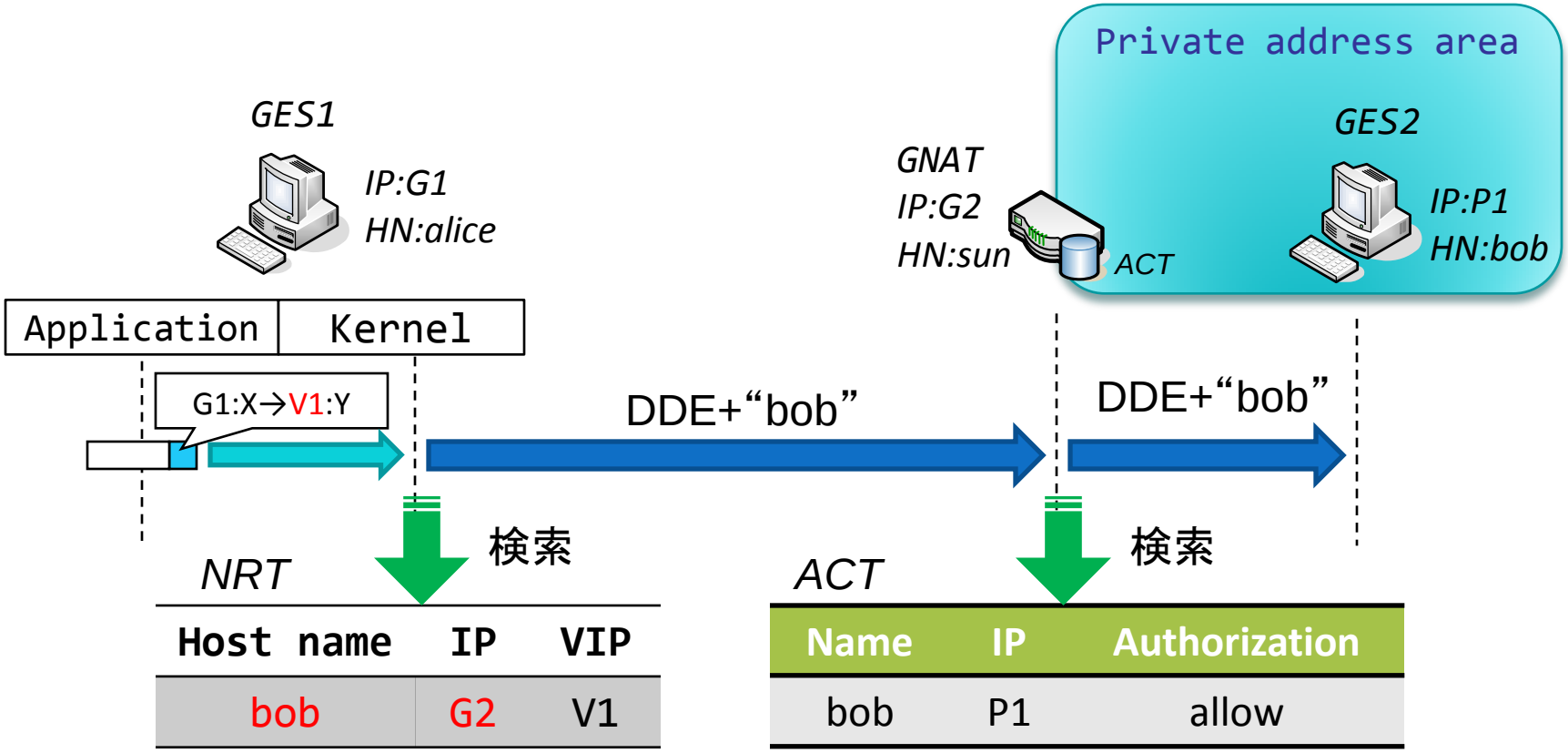


DNS名前解決処理

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

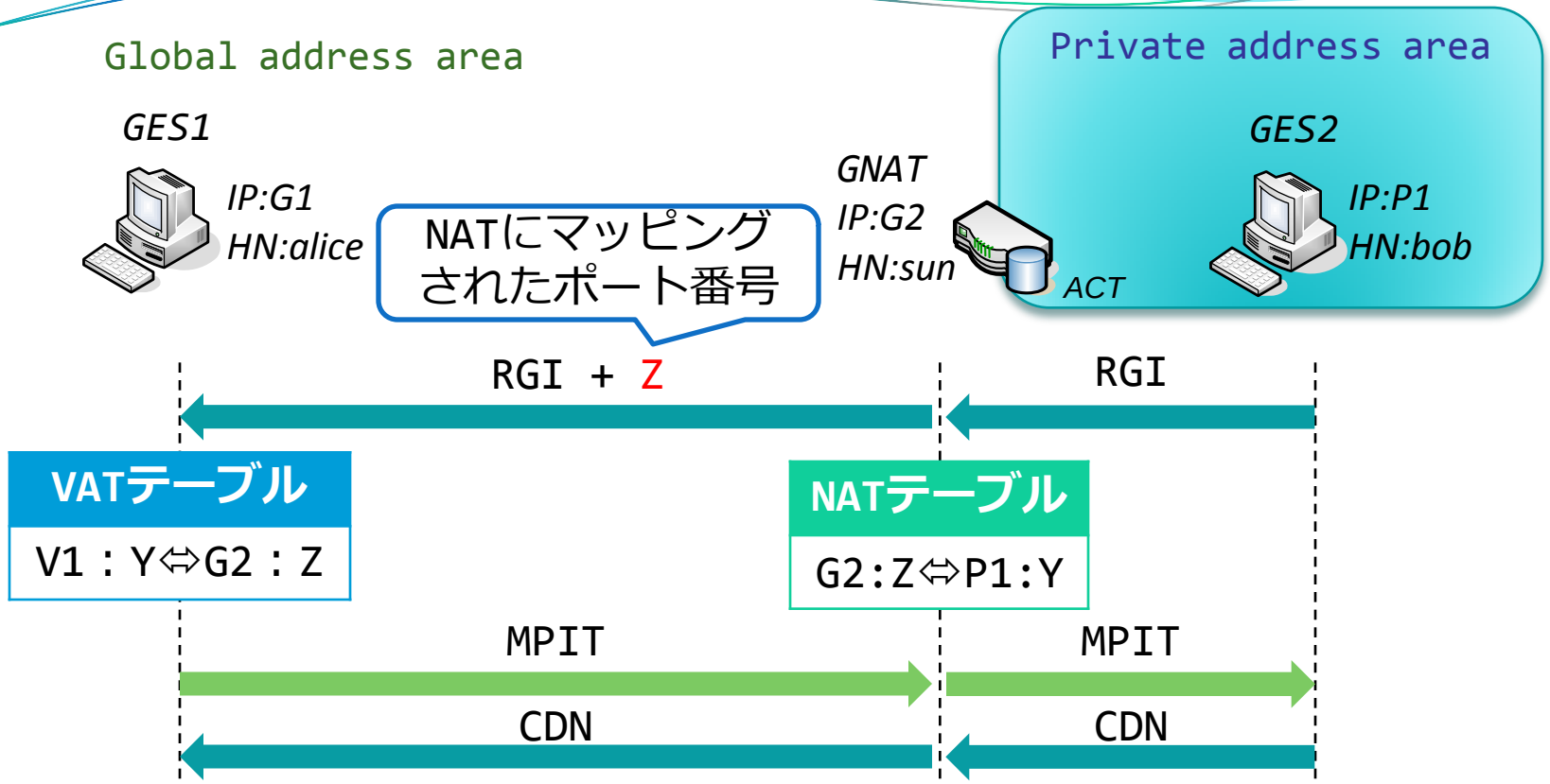


NAT越えDPRPネゴシエーション



- 仮想アドレス対応するホスト名をDDEに追加
- ACT検索
  - P1を取得，DDEをGES2に転送

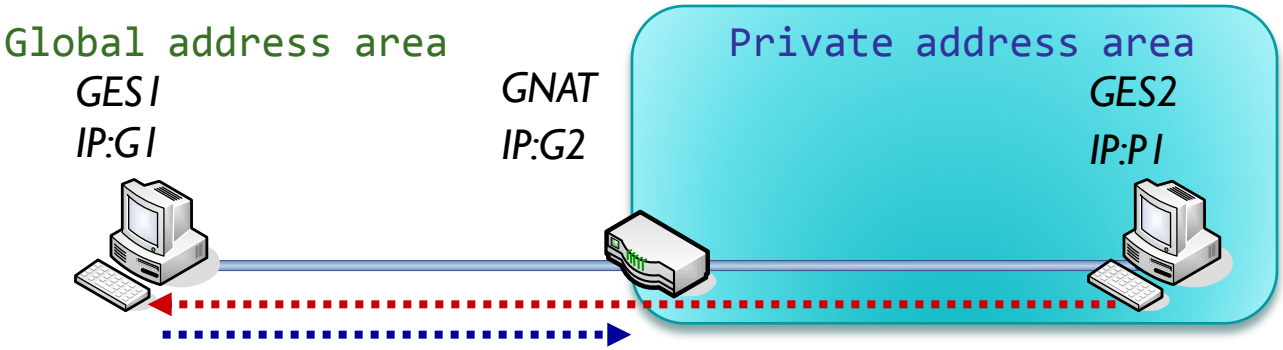
NAT越えDPRPネゴシエーション



- GES1とGES2に対応するNATテーブルを生成
  - RGIに含まれるコネクション情報とACTで取得したP1を利用
- 仮想アドレス変換テーブルVAT(Virtual Address Translation)を生成

NATに対応したPIT

通信経路上にNAT



PIT
G1:X⇔G2:Z
暗号化/復号

PIT
G1:X⇔G2:Z
暗号化/復号

PIT
G1:X⇔P1:Y
暗号化/復号

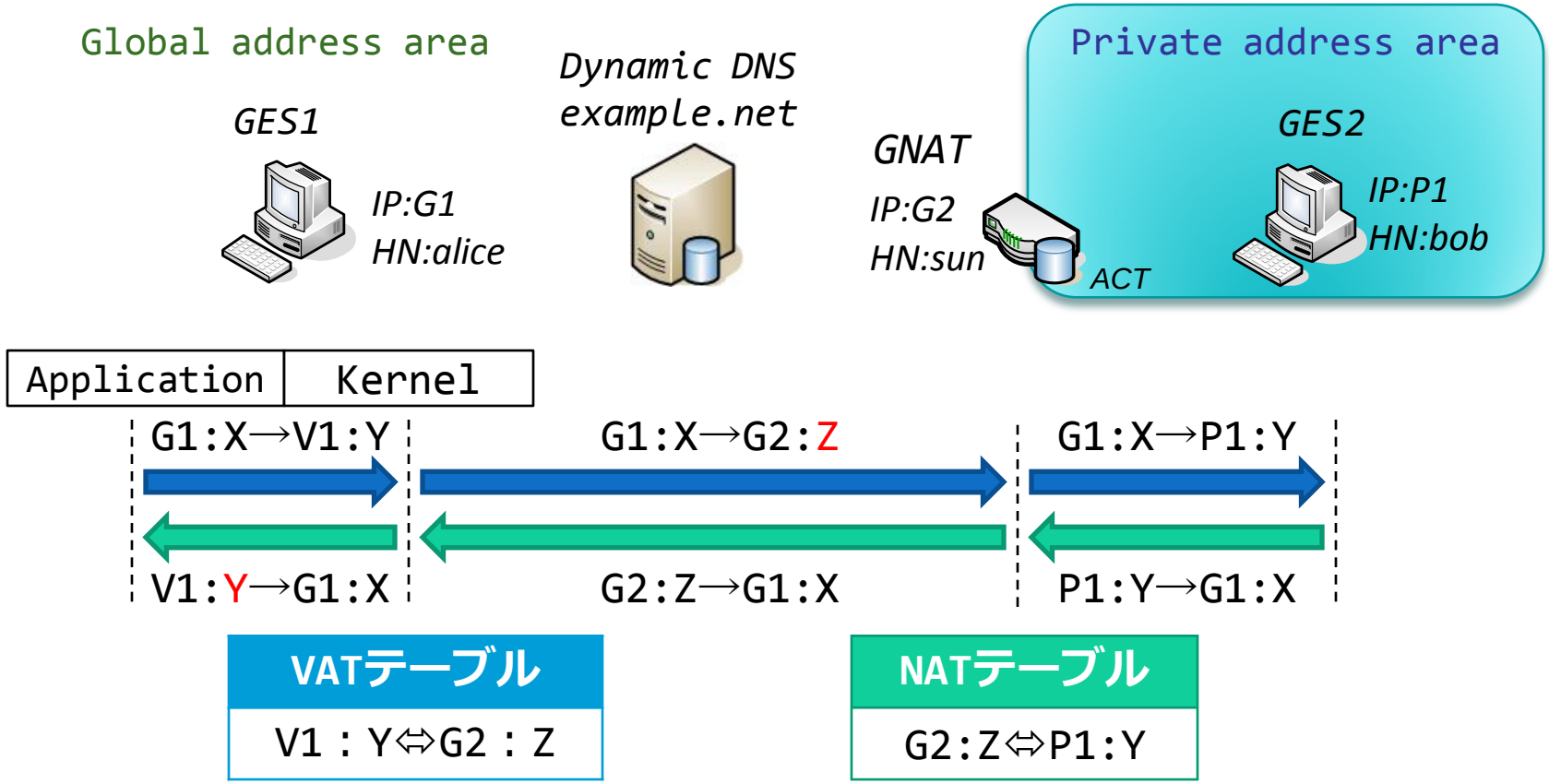
VATテーブル
V1：Y⇔G2：Z

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が生成される

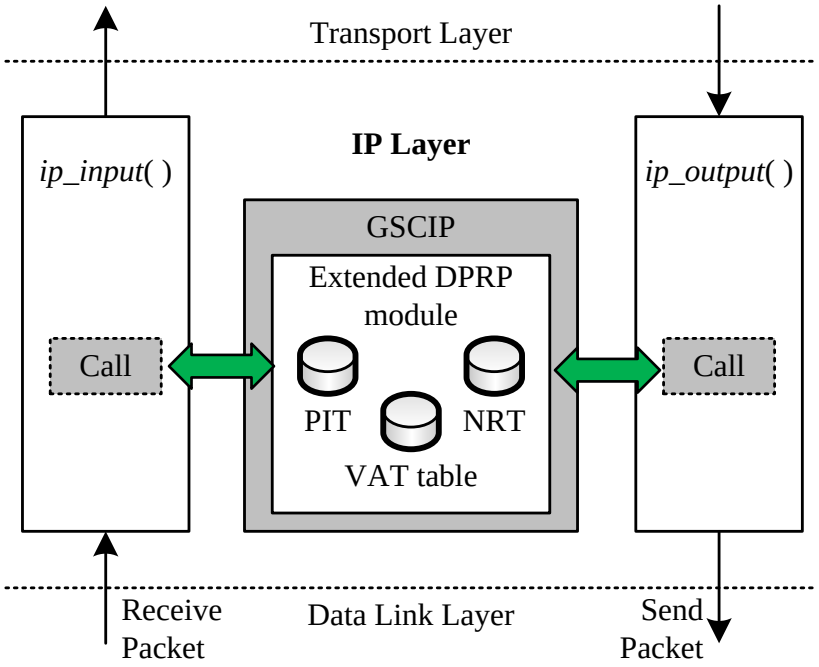
アドレス変換処理



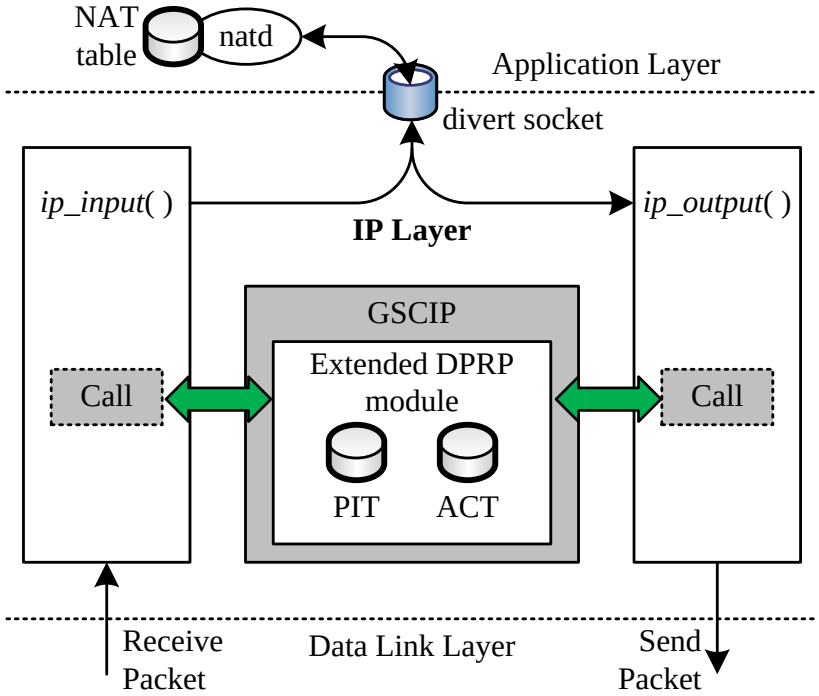
- GES1はNATにマッピングされたポート番号に変換して送信
- GA空間側から通信開始が可能になる

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
- DPRPは実装済み
- 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

まとめ

- DPRPの概要
- 経路上にNATがある場合の問題点
  - コネクション情報とPIT内容が一致しない
  - NAT越え問題
- NAT越えDPRPの提案
  - 双方向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
  - 実装完了・性能評価