# GSCIP における構成要素 GEA の検討

030432057　佐本章悟
渡邊研究室

## 1. はじめに

企業ネットワークにおけるセキュアな通信を実現する技術として IPsec があるが，システム構成が頻繁に変化するような環境では管理負荷が膨大になるため導入が難しく，イントラネットではほとんど利用されていない．そこで我々は柔軟性とセキュリティとを兼ね備えたグルーピング通信を可能とする通信アーキテクチャ GSCIP（Grouping for Secure Communication for IP）[1]を提案している．GSCIP における通信グループの構成要素を GE（GSCIP Element）と呼び，現状では端末にソフトウェアをインストールして実現するホストタイプの 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）の 2 タイプの種類がある．GEN は配下に存在する一般端末を一括して保護する．しかし，各タイプの GE を既存のネットワーク体系に導入することは，既存の端末やルータに手を加える必要があり，容易ではない．本稿では，この課題を解決するためブリッジタイプの GEA（GE realized by Adapter）について検討し，実装したので報告する．

## 2. GSCIP

GSCIP では同一の暗号鍵を所持する GE の集合を同一の通信グループと定義する．この暗号鍵をグループ鍵 GK（Group Key）と呼ぶ．同一通信グループ内の端末間通信は GK により暗号化され，異なる通信グループの端末からのアクセスを拒否することもできる．通信グループと GK を 1 対 1 に対応付けることにより IP アドレスに依存しない通信グループを容易に定義することができる．

## 3. GSCIP における構成要素の検討

図 1 に GES と GEN により構成されるネットワークモデルを示す．GEN は部門単位の通信グループ（Group1）を形成し，配下の端末を保護する．GES1 と GES2 は役職単位の通信グループ（Group2）を形成し，両者の通信は GK2 で暗号化／復号される．

しかし既存のネットワークに GES や GEN を設置することは，サーバソフトウェアの変更やルータの置き換えが必要で許されない場合が多い．そこでブリッジタイプの GEA を既存のサーバやルータの直前に設置することにより GES，GEN を設置したのと同じ役割を果たすことができる．

図 2 に GEA を用いた場合のネットワークモデルを示す．GEA1 と一般のルータにより，図 1 の GEN と同様の機能を提供できる．また GEA2 とサーバにより，図 1 における GES2 と同様の機能を実現できる．スイッチの直前に GEA を設置すれば，スイッチに接続された端末を一括してグルーピングすることも可能であり，柔軟に既存のネットワークに対応することができる．

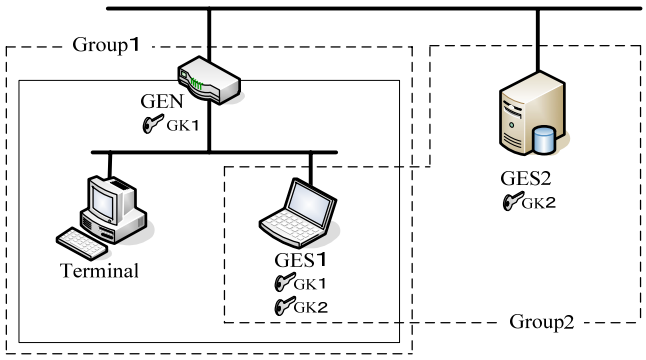



図 1. GES と GEN により構成されるネットワークモデル

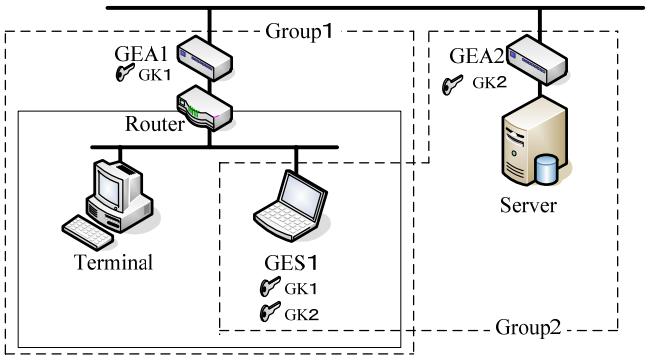



図 2. GEA により構成されるネットワークモデル

GEA の動作はデータリンク層の入力関数である ether_input() でパケットの受信または転送の処理を行なった後，既存のモジュール群の呼び出しを行い，パケットの種類を判別してから適切なモジュールを選択し実行する順序である．各モジュールの処理後に通信を継続するか破棄するかが決定する．

このように GEA の実装はブリッジの処理が行われるデータリンク層で行い，入力関数 ether_input() から既存のモジュール群を呼び出すことで実現した．

## 4. むすび

本稿では GSCIP の構成要素 GEA の必要性とその効果について検討した．今後は GEA の実装を完了させ，実機による動作確認を行う．

### 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 , Nov.2006.

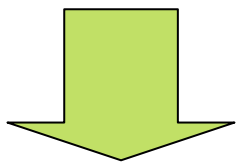
# GSCIPにおける構成要素GEAの検討

渡邊研究室

030432057　佐本章悟

# 研究背景

- ユビキタスな社会に向け
  - 移動が自由
  - 安全な通信
  - ユーザにとって使いやすいネットワーク



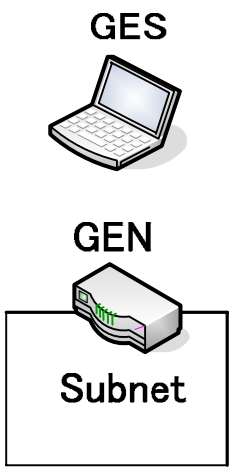
柔軟性とセキュリティとを兼ね備えた通信アーキテクチャ
GSCIP (Grouping for Secure Communication for IP)

# GSCIP

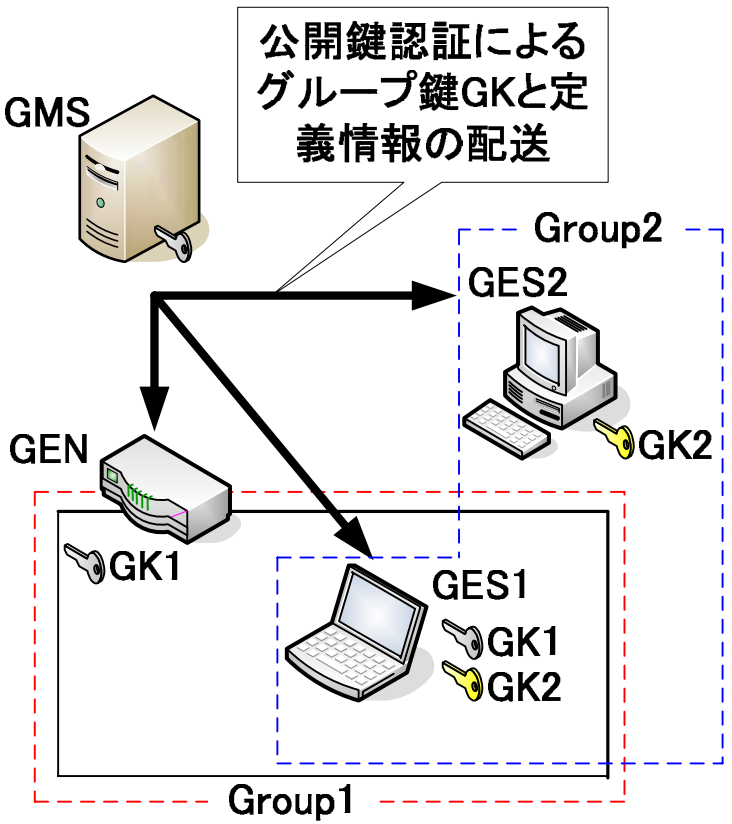
- GSCIPとは・・・
  - 通信グループを構築し，柔軟でセキュアな通信を実現する通信アーキテクチャ
- GSCIPでは・・・
  - 個人単位やドメイン単位の通信が混在した通信グループを定義することが可能
  - 通信グループの位置情報が変化しても動的に通信を維持

# GSCIPの構成要素GE

- GSCIPを実装した装置をGE（GSCIP Element）と呼ぶ
- 現状GEには2タイプの装置がある
  - GES（GSCIP Element realized by Software）
    - 端末にソフトウェアをインストールするタイプ
  - GEN（GSCIP Element for Network）
    - サブネットを構成するルータに適用するタイプ



# GSCIPにおける通信グループの定義方法



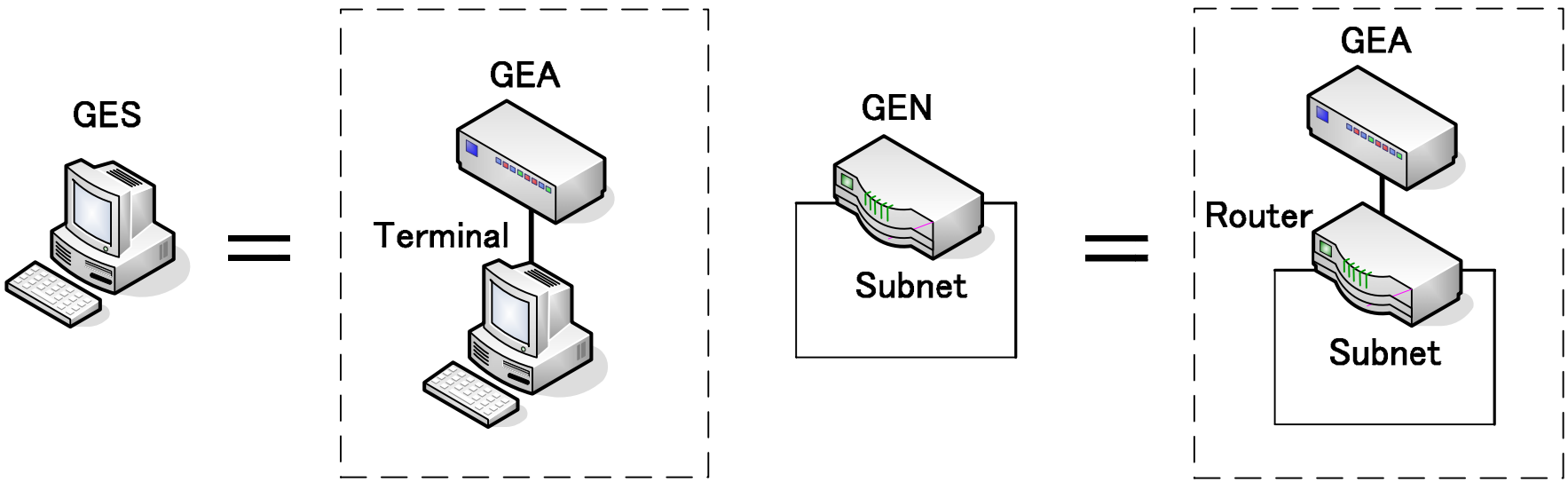

- GSCIPでは同一の暗号鍵を所持するGEの集合を同一の通信グループと定義（この暗号鍵をグループ鍵GKと呼ぶ）
- 管理装置GMSから定期的に鍵を配送し通信グループを形成
- 同一通信グループ内の通信はGKで暗号化
- 通信グループとGKを1対1に対応付けることによりIPアドレスに依存しない通信グループを定義でき，移動してもグループ情報が維持できる

# GEの課題

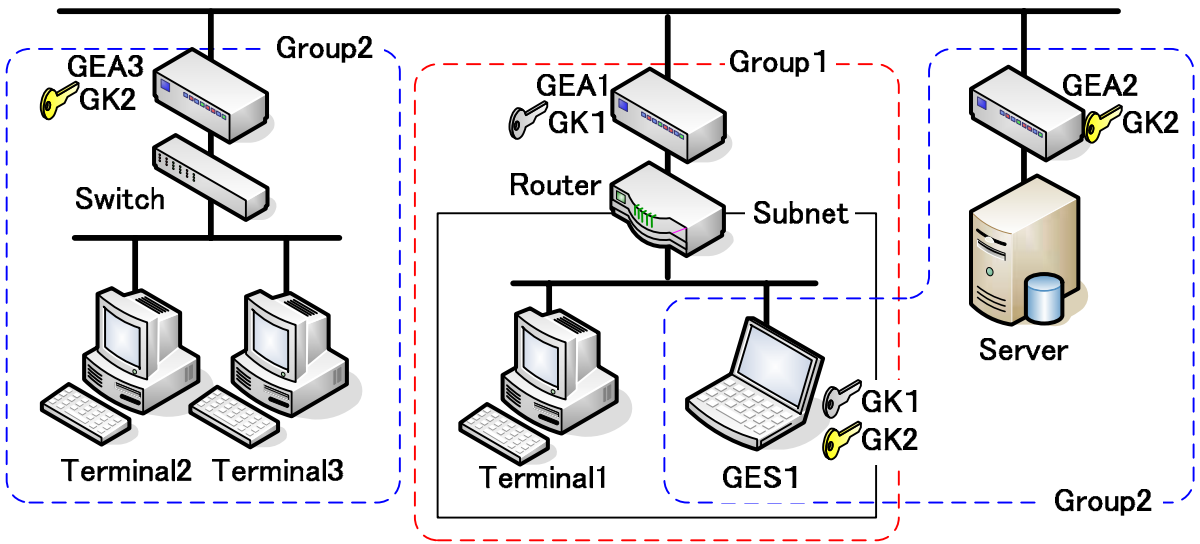
- 既存のネットワークにGESやGENを導入することは，既存の端末やルータに手を加える必要があり困難な場合がある
- 企業ネットワークなどでは新しくルータが入るとアドレス体系が変わり導入が難しい
- 現状のGEはプログラムをIP層で実装しており，既存端末（サーバ等）に変更を加えることはカーネルを操作するのでGES等を導入することは許されない場合がある

# 課題の解決

- **新しいブリッジ型**GE**である**GEA (GE realized by Adapter) **を開発**
- **ブリッジに**GSCIP**の機能を組み込み実現**
- **端末やルータの直前に設置し**GES, GEN**と同じ役割を果たす**

# GEAを組み込んだネットワークモデル

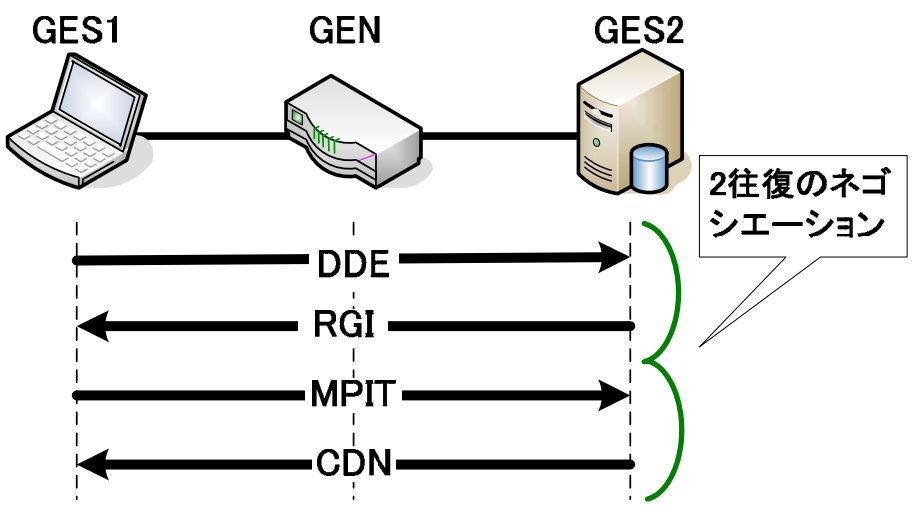



- GEA1により，ルータ配下を保護
- GEA2により，サーバを保護
- GEA3により，スイッチ配下を保護

既存のネットワークにも柔軟に対応できる

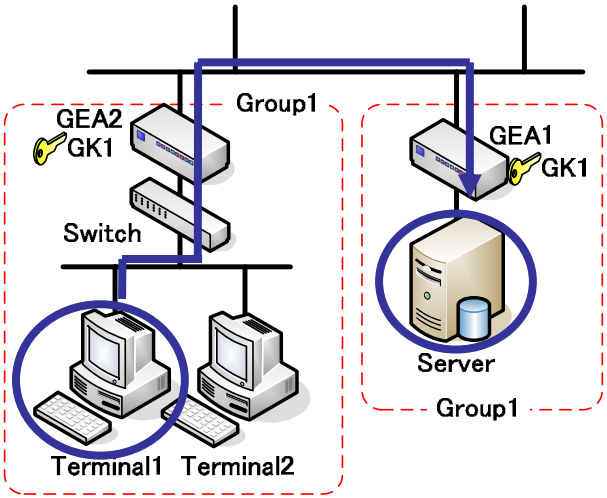
# GSCIPのプロトコルDPRP

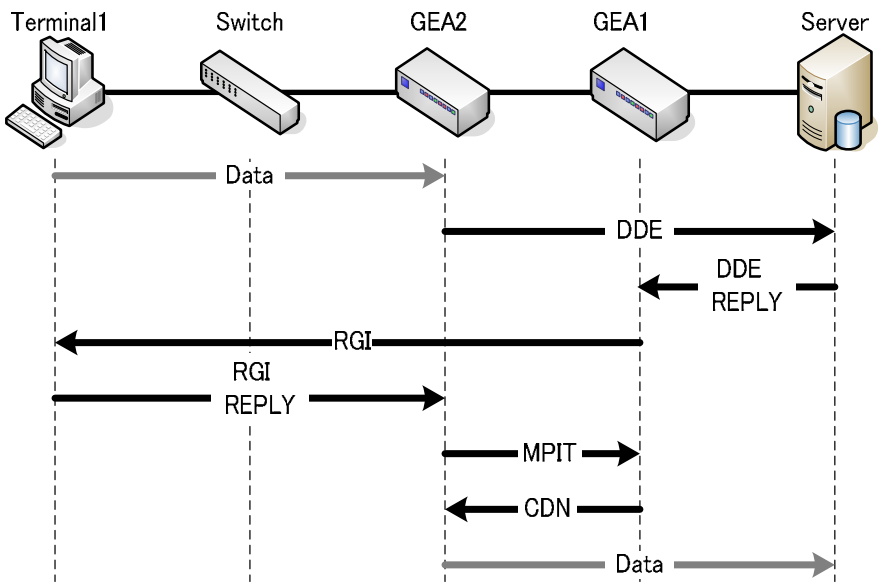
- GSCIPでは，通信を開始する際，各GEの情報を知るため DPRP (Dynamic Process Resolution Protocol) を行う
- 4つの制御パケットを使用し，2往復のネゴシエーションを行い 各GEの情報を取得
- 4つの制御パケットはICMP Echoパケットをベースにしている




DDE ・・・ 終点GEの決定
RGI ・・・ 始点GEを決定し，通信経路上の全GEのグループ情報を収集
MPIT ・・・ RGIで収集した情報を各GEに通知
CDN ・・・ DPRPネゴシエーションの完了の通知

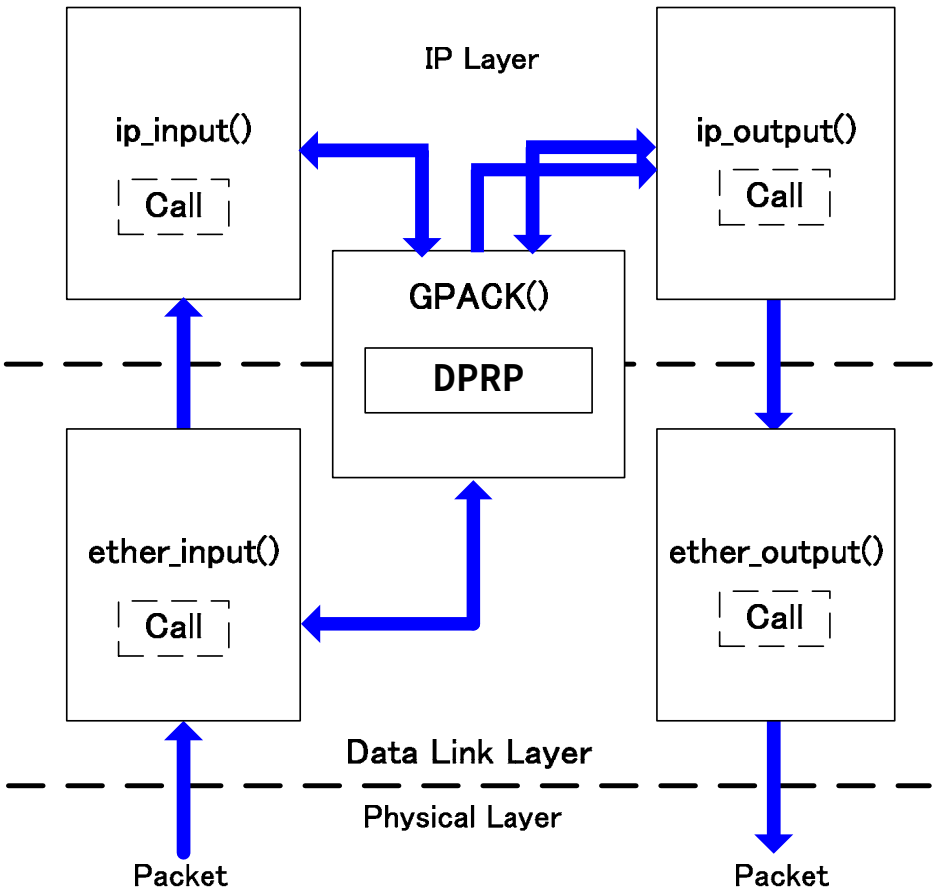
# GEAを含むネットワークの動作




- GEAがデータ受け取るとDPRPネゴシエーションを開始
- DDEを受け取ったサーバは，通常のICMP処理を行いICMP Echo Replyを応答．この応答をDDE REPLYと定義
- DDE REPLYを受け取ったGEAが終点GEとなる
- RGIを受け取った端末1は，通常のICMP処理を行いICMP Echo Replyを応答．この応答をRGI REPLYと定義
- RGI REPLY受け取ったGEAが始点GEとなる

# GSCIPの実装

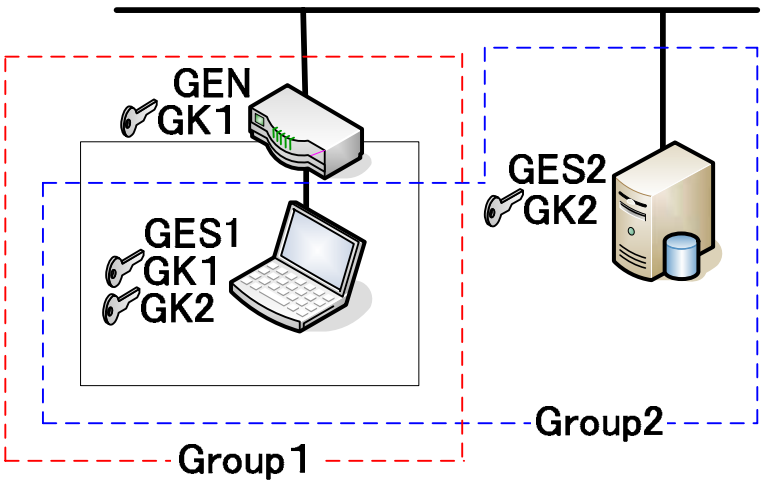


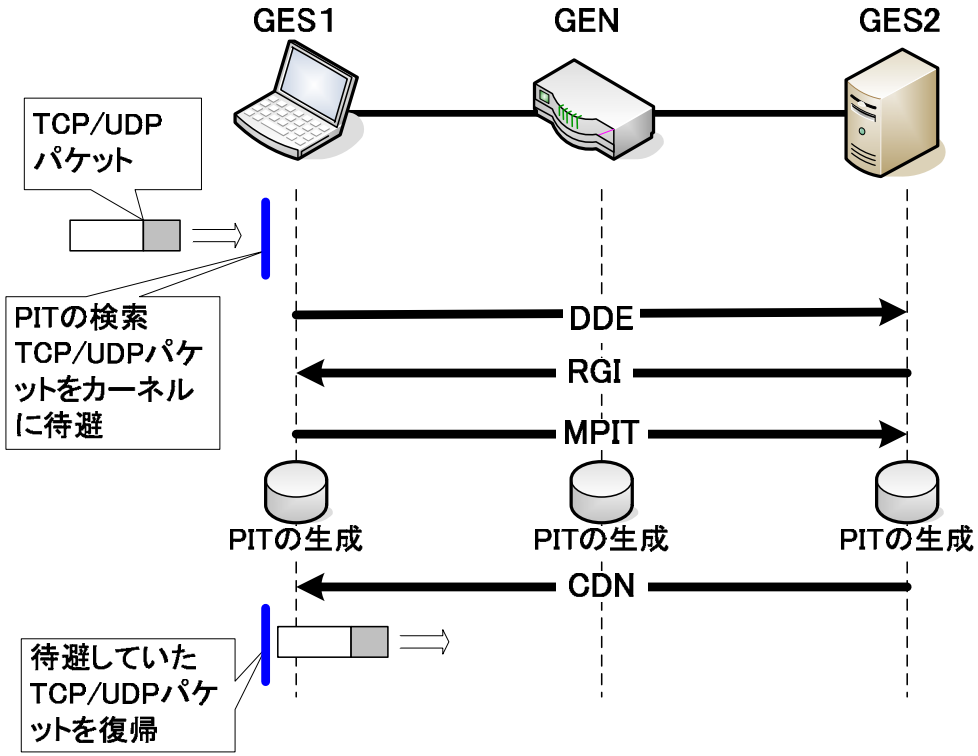

- GSCIPを実現するモジュール群をGPACKと呼ぶ
- 現状のGPACKはIP層から呼び出される
- GEAの場合はブリッジのため，GPACKがData Link層から呼び出される
- GPACKの呼び出し元は，Data Link層の入力関数ether_inputである

# まとめ

- GSCIPにおける構成要素GEAの検討
  - GEの課題とその解決方法
  - ブリッジ型GEAの開発
- 今後の課題
  - 実機による動作確認と評価

# DPRPの動作

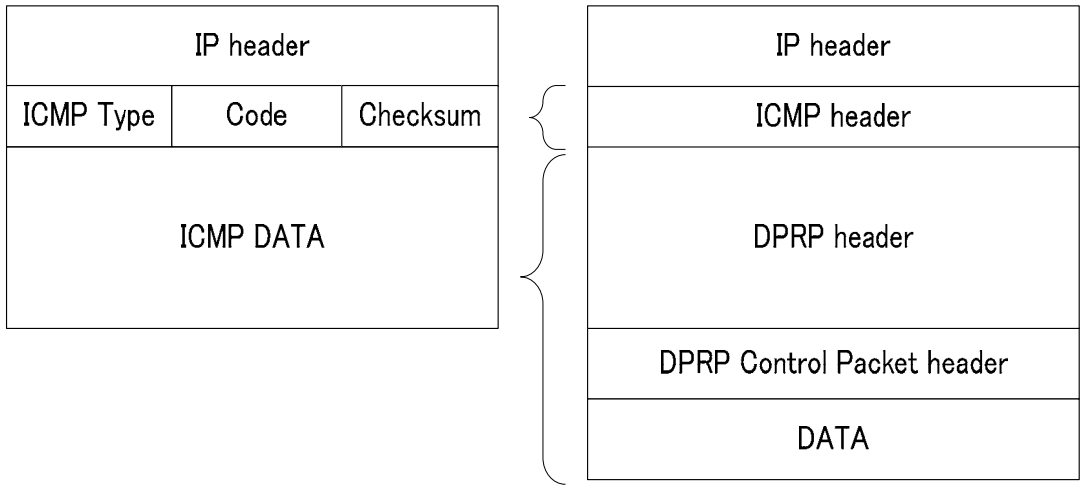



- DDE ・・・終点GEの決定
- RGI ・・・始点GEを決定し，通信経路上の全GEのグループ情報を収集
- MPIT・・・RGIで収集した情報を各GEに通知 動作処理テーブルの生成
- CDN ・・・DPRPネゴシエーションの完了の通知

# ICMP

- **ICMPとは通信したい端末やルータにIPパケットが到達するかどうかを確認したいときに利用されるプロトコル**
- **代表的なコマンドに“Ping”がある**




| DPRP制御パケット | ICMPタイプ |
|---|---|
| DDE | Echo Request(タイプ：8) |
| RGI | |
| MPIT | |
| CDN | Echo Reply(タイプ：0) |

# PIT（Process Information Table）

- PIT・・・**動作処理情報テーブル**

  **DPRP開始時にPITが作成される．初めPITはDDE，RGIのネゴシエーションの際の各GEのCIDが記録される場所となる．その後RGIにより収集された動作処理情報を各GEにMPITで通知することでPITが生成される**

- **構成内容**
  - **送信元 / 宛先IPアドレス**
  - **送信元 / 宛先ポート番号**
  - **トランスポート層のプロトコル番号**

  } CID（Connection Identification）

  - **動作処理内容**
    - **暗号化 / 復号 / 中継 / 破棄**
  - **グループ鍵情報**

  } **動作処理情報**