GSCIP における構成要素 GEA の検討

佐本　章悟*，鈴木　秀和，渡邊　晃（名城大学）

Researches on GEA; an element of GSCIP

Shogo Samoto ， Hidekazu Suzuki ， Akira Watanabe （Meijo University）

１．はじめに

企業ネットワークにおけるセキュアな通信方式技術として 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ための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，ホストタイプの GES（GE for Software)，ルータタイプの GEN（GE for Network）がある．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 for Adapter）について検討した．

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し, 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定義することができる．

３．GSCIP における構成要素の検討

GE には, 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 と，サブネットを構成するルータタイプの GEN がある． GEN は配下に存在する一般端末（以下 Term）を一括して保護する．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 Term1 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体系に GES や GEN を組み込むことは，ルータの置き換えやサーバソフトウェアの変更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 を既存の一般端末やルータの直前に設置することにより GES，GEN 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 に

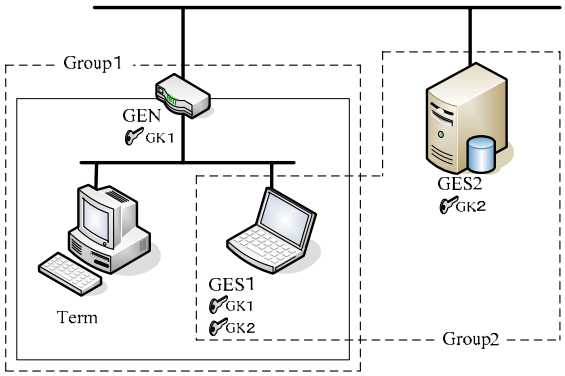


Fig.1. Network model consisted of GESs and GENs

より，ルータ配下のネットワークを部門単位の通信グループ（Group1）として定義できる. 同様に GEA2 により, Term2 は図 1 における GES2 と同様の機能を実現できる．

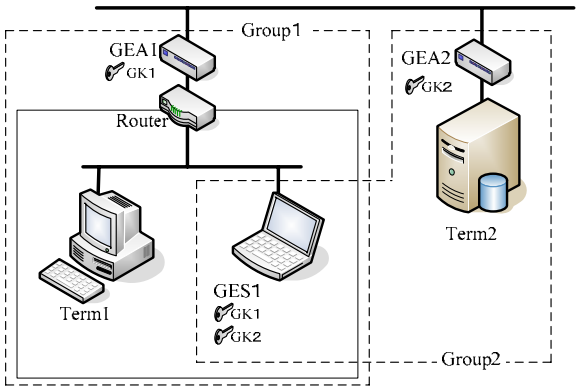


Fig.2. Network model consisted of GEAs

またスイッチの直前に GEA を設置することにより，スイッチに接続された Term を一括してグルーピングすることも可能であり，より柔軟に既存のネットワークに対応することができる．

GEA を設置することで既存のネットワーク機器やサーバを変更せず GSCIP のアーキテクチャを導入することができる．

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 の実装を行う．

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，情報処理学会研究報告，2004-CSEC-28，pp.199-204，2005.

GSCIPにおける構成要素GEAの検討

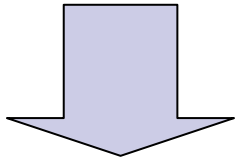
Researches on GEA ; an element of GSCIP

名城大学 理工学部

佐本章悟 鈴木秀和 渡邊晃

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



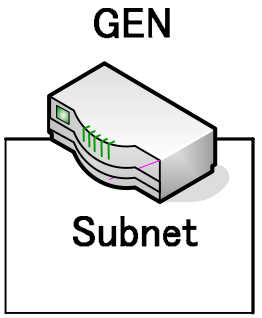
柔軟性とセキュリティとを兼ね備えた通信アーキテクチャ
GSCIP（Grouping for Secure Communication for IP）

GSCIP

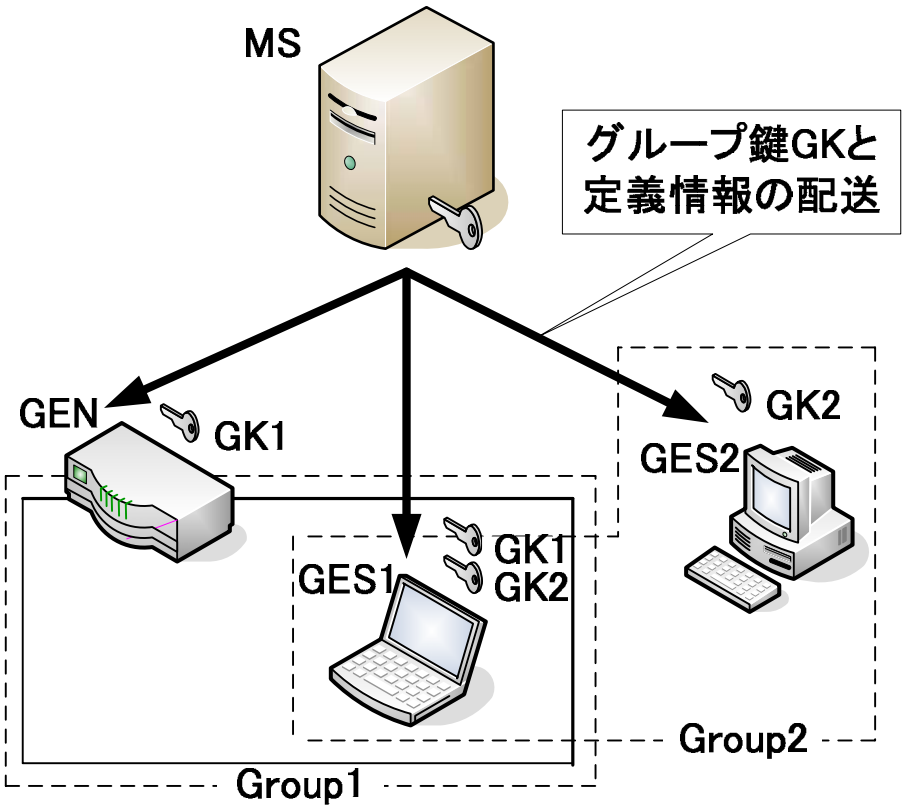
- GSCIPとは・・・
  - 通信グループを構築し，柔軟でセキュアな通信を実現する通信アーキテクチャ
- GSCIPでは・・・
  - 個人単位やドメイン単位の通信が混在した通信グループを定義することが可能
  - 通信グループの位置情報が変化しても動的に通信を維持
  - 既存のネットワークにも対応したプロトコル群をもつ

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（GE 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（GE 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



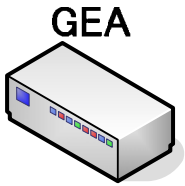
- GSCIPでは同一の暗号鍵を所持するGEの集合を同一の通信グループと定義
  （この暗号鍵をグループ鍵GKと呼ぶ）
- 管理装置MSから定期的に鍵を配送し通信グループをグルーピング
- 同一通信グループ内の通信はGKで暗号化
- 通信グループとGKを１対１に対応付けることによりIPアドレスに依存しない通信グループを定義でき，移動してもグループ情報が維持できる

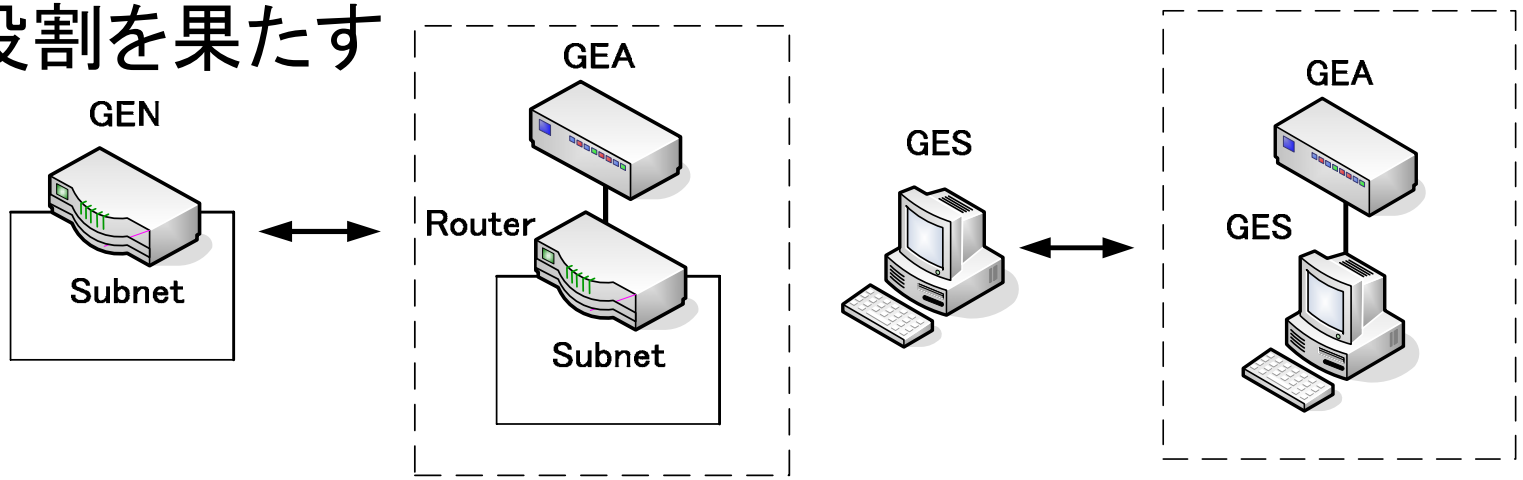
GEの課題

- 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

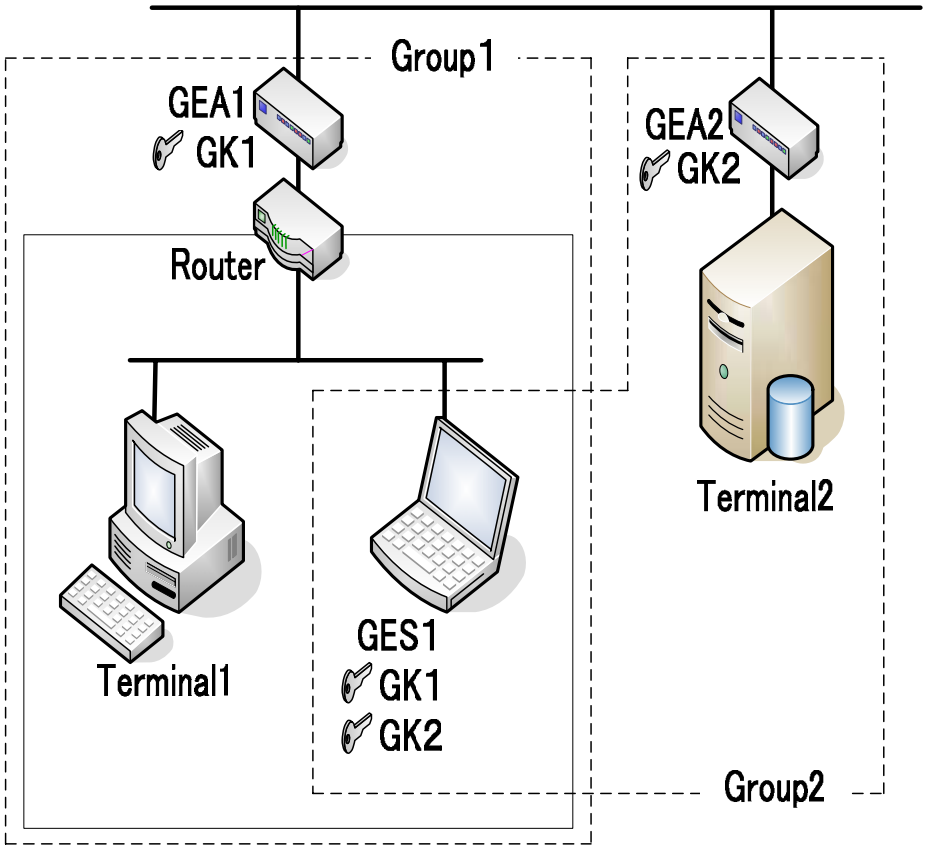
課題の解決

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





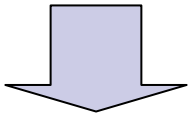
GEAを組み込んだネットワーク



- GEA1により，ルータ配下のネットワークを部門単位の通信グループとして定義，GENのように振舞う
- GEA2により，Terminal2を保護しGESのように振舞う

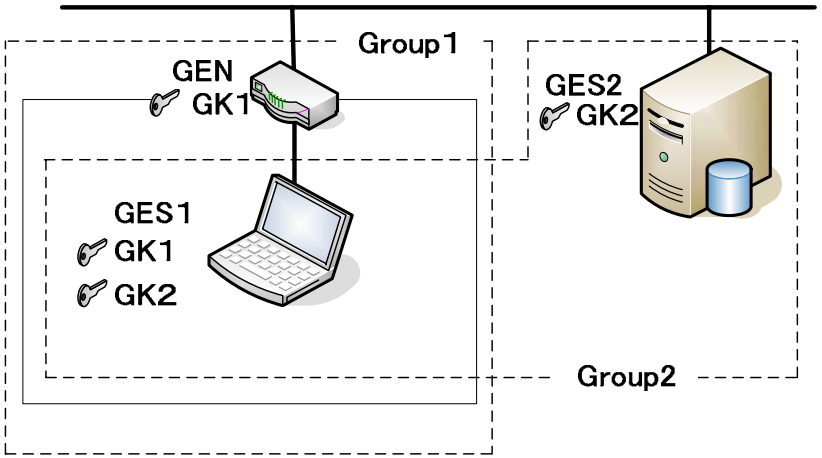
GSCIPのプロトコルDPRP

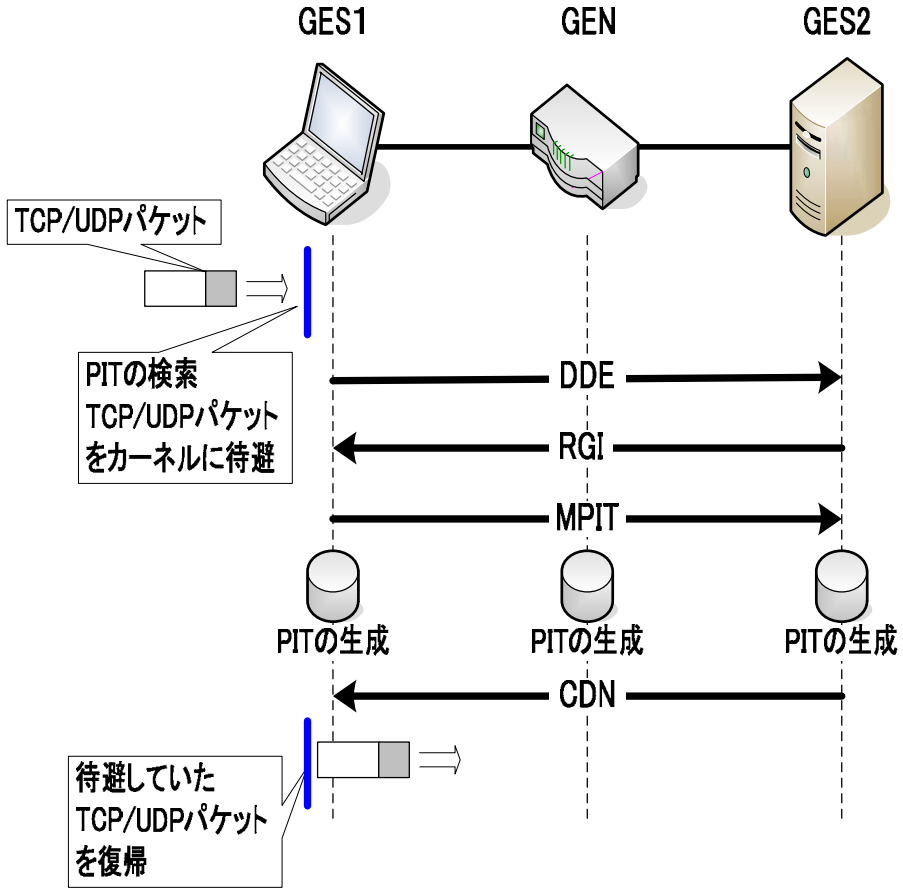
- GSCIPでは，通信を開始する際，各GEの情報を知るためDPRP（Dynamic Process Resolution Protocol）を行う
- DPRPでは4つの制御パケットを使用し，各GEの情報を取得，動作処理テーブルPIT（Process Information Table）を生成，記憶する



ネットワークの物理的構成に変化があっても，
システムが動的にその変化を学習し通信グループの関係を維持できる

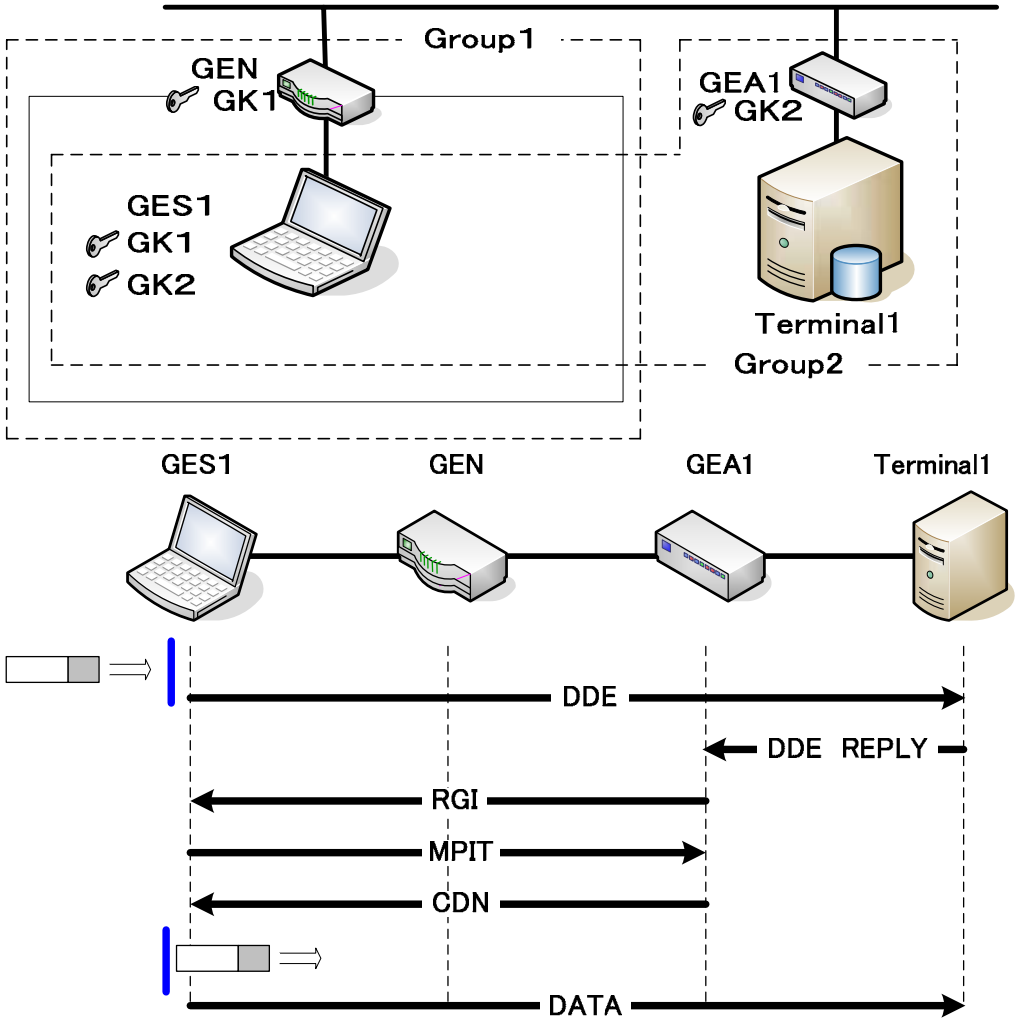
DPRPの動作





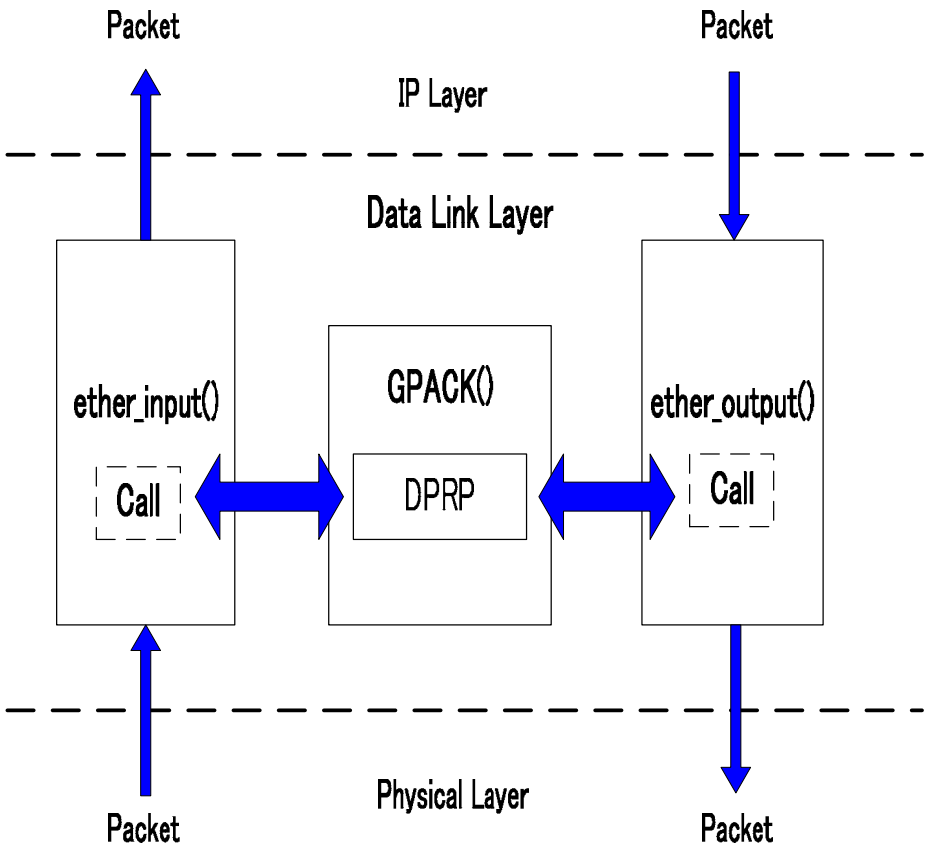
・DDE ・・・終点GEの決定
・RGI ・・・始点GEを決定し，通信経路上の全GEのグループ情報を収集
・MPIT・・・RGIで収集した情報を各GEに通知 動作処理テーブルの作成
・CDN ・・・DPRPネゴシエーションの完了の通知

GEAを含むネットワークの動作



- DPRP制御パケットはICMPをベースに定義されている
- DDEを受け取ったTerminal1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となり，残ったネゴシエーションを行う
- GEA1がTerminal1を保護し，GESと同じ役割を果たす

GSCIPの実装



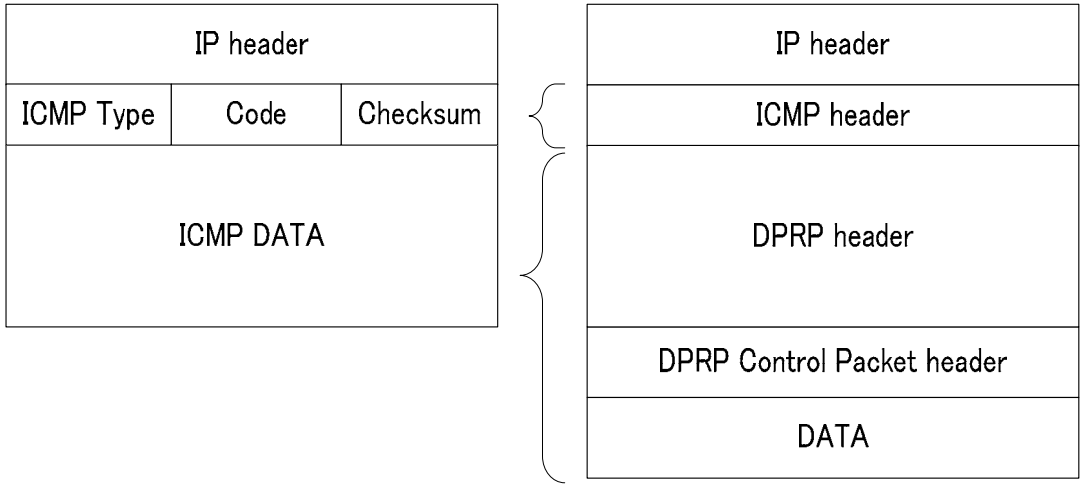
- GSCIPを実現するモジュール群をGPACKと呼ぶ
- 現状のGPACKはIP層から呼び出されるが，GEAはブリッジ機能を含むのでData Link層から呼び出される.
- GPACKの呼び出し元は，Data Link層の入出力関数ether_input,ether_outputである

まとめ

- GSCIPにおける構成要素GEA
  - GEの課題とその解決方法
  - ブリッジ型GEAを開発することで解決
- 今後の課題
  - 実装と評価

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)