GSCIP の Windows への実装に関する検討

細尾　幸宏*，鈴木　秀和，渡邊　晃（名城大学）

A Study of the Implementation of GSCIP on Windows

Yukihiro Hosoo, Hidekazu Suzuki, Akira Watanabe (Meijo University)

１．はじめに

企業ネットワークのセキュリティを確保するために通信グループを定義することは有効な手段である．しかし，IPsec のような既存の技術では部門単位と個人単位の通信グループが混在した場合や，システム構成の変化が多い場合は管理負荷が大きく，実現が難しい．

我々は FPN （Flexible Private Network）と呼ぶ柔軟性とセキュリティを兼ね備えたネットワークの概念を提唱し，FPN を実現するためのアーキテクチャとして GSCIP（Grouping for Secure Communication for IP）を提案している[1]．現在，GSCIP は FreeBSD に実装して動作検証を行っており，有効なアーキテクチャであることが確認されている．今後，GSCIP をより多くの人に評価してもらうためには Windows に機能を実装することが必須である．そこで本稿では，GSCIP を Windows に実装する方式について検討を行った．

２．GSCIP

GSCIP では，共通暗号鍵と通信グループを 1 対 1 に対応づけることにより，IP アドレスに依存しないグループを定義することができ，IPsec に比べ大幅に管理負荷を軽減することができた．

GSCIP を構成するプロトコル群として，DPRP（Dynamic Process Resolution Protocol），Mobile PPC（Mobile Peer to Peer Communication）および NAT-f（NAT-free Protocol）がある．DPRP は通信に先立って通信経路上の GSCIP 対応装置が情報を交換し，GSCIP 対応装置同士の認証や，通信の可否を判断する処理を行う．Mobile PPC は通信中に一方の端末が移動した場合，エンド端末同士で IP アドレスの変化情報を交換し，端末の上位ソフトウェアに対して IP アドレスの変化を隠蔽し，通信継続性を実現する．NAT-f はプライベートアドレス空間にいる相手と通信を開始するとき，NAT-f 対応 NAT ルータに NAT テーブルを強制的に生成することにより，プライベートアドレス空間とグローバルアドレス空間の違いを意識することの無い通信を実現する．現在，GSCIP は FreeBSD の IP 層に実装されており，基本動作を確認済みである．GSCIP モジュールは IP 層の一部を改造し，適切な場所から呼び出すサブルーチンとして実現されている．

３．NDIS を利用した GSCIP の実装

Windows では TCP/IP を含む OS の標準的な機能がブラックボックスとなっているが，NDIS（Network Driver Interface Specification）と呼ぶインターフェースが外部に公開されており，これを利用することができる．NDIS は Microsoft 社が定めたネットワークドライバの仕様であり，ネットワークドライバに機能を追加できるように定められている．ドライバは処理を行うモジュールを登録し，NDIS Interface が必要時に対応するモジュールを呼び出す構造になっている（図 1）．FreeBSD で開発した GSCIP のモジュールはほぼそのまま Windows への流用が可能であるが，Windows と FreeBSD では提供されている API が異なるため，処理内容が等しくなるように API に係わる部分を置き換える必要がある．また，NDIS はデータリンク層でのヘッダ処理より下層で動作するため，IP 層で実装されている FreeBSD のモジュールに対して MAC ヘッダに対する処理を追加する必要がある．GSCIP モジュール内で独自に生成するパケットの送受信は上位プロトコルへ通知しないように NDIS の通知処理を改造する必要がある．また，送受信モジュールと完了通知モジュールは独立しているため，モジュール間で連携してパケットの送受信完了処理を行うかどうか判断することが必要になる．

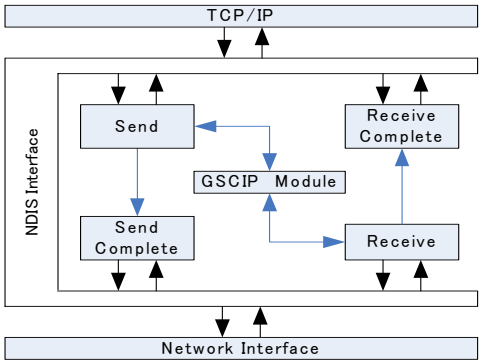


Fig. 1 Implementation of GSCIP using NDIS

４．まとめ

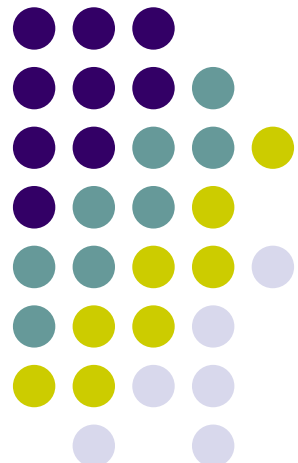
FreeBSD に実装された GSCIP を Windows に移植する方法についての検討を行った．今後は実装を完了させ，性能評価を行う．

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 の実装と評価，情報処理学会論文誌，Vol.47，No.11，pp.2976-2991，Nov.2006.

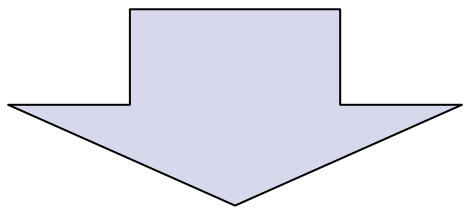
GSCIPのWindowsへの実装に関する検討

名城大学　理工学部
細尾 幸宏　鈴木 秀和　渡邊 晃



研究背景

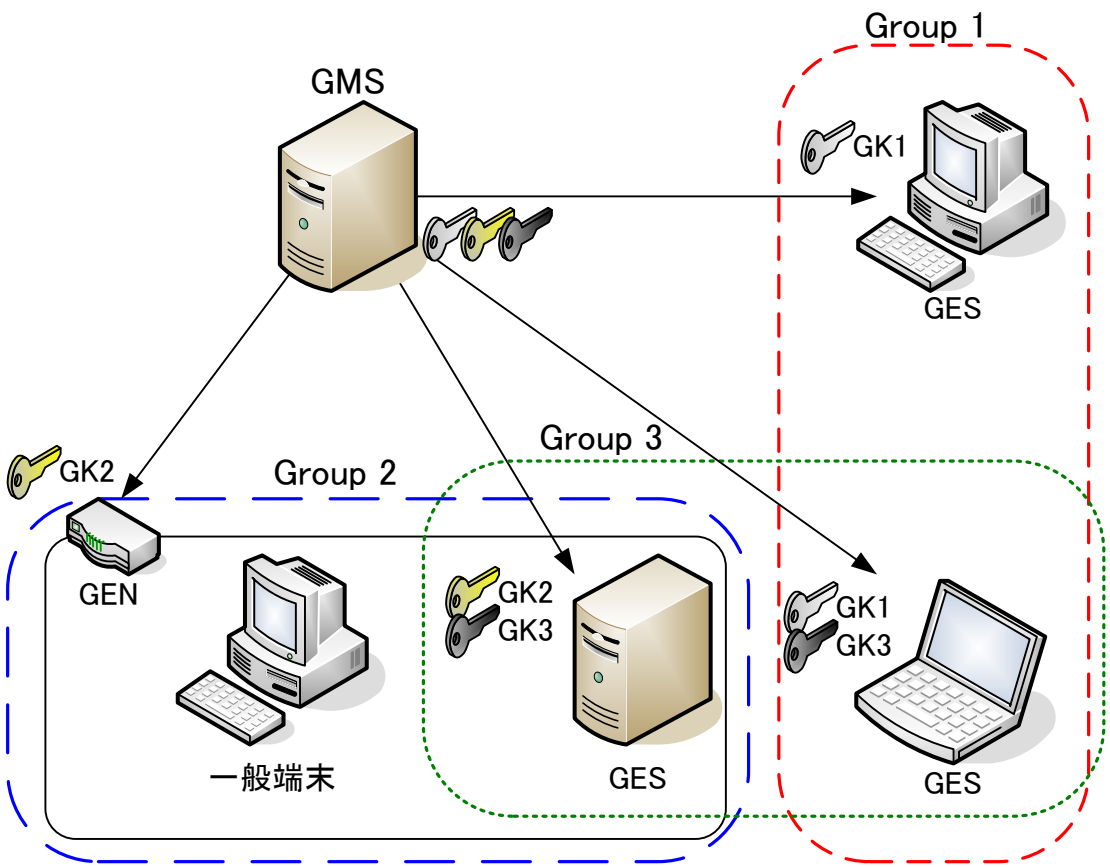
- ユビキタスネットワークの普及
  - 移動しながらの通信
  - 安全な通信
  - アドレス空間の違いを意識しない通信



柔軟性とセキュリティを兼ね備えたグループ通信を実現する
GSCIP（Grouping for Secure Communication for IP）

GSCIPの概要

GE　:GSCIP対応装置
GES:ソフトウェア型
GEN:ルータ型
GMS:管理装置



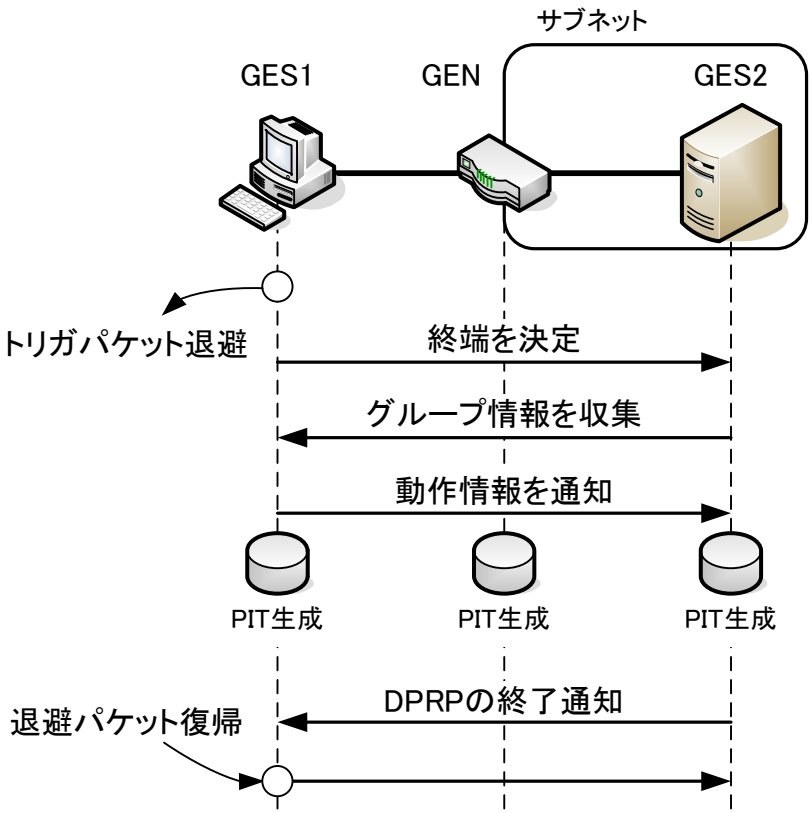
- MSがグループ鍵GKを各GEへ配送
- GKによって通信グループを構築
- 定義された同一グループ間の通信は暗号化される
- GKと通信グループを1:1に対応付け
- IPアドレスに依存しないグループを定義

GSCIP

- GSCIP構成プロトコル
  - DPRP (Dynamic Process Resolution Protocol)
    - ネットワークの構成変化に動的に対応
    - 通信相手と経路上にあるGEに対してネゴシエーションや認証を行う
  - Mobile PPC (Mobile Peer to Peer Communication)
    - IPアドレスの変化を隠蔽し，移動通信をエンドエンドで実現
  - NAT-f (NAT – free Protocol)
    - 対応NATルータに強制的に外部からNATテーブルを生成し，アドレス空間の違いを意識しない通信をエンドエンドで実現

DPRP (Dynamic Process Resolution Protocol)

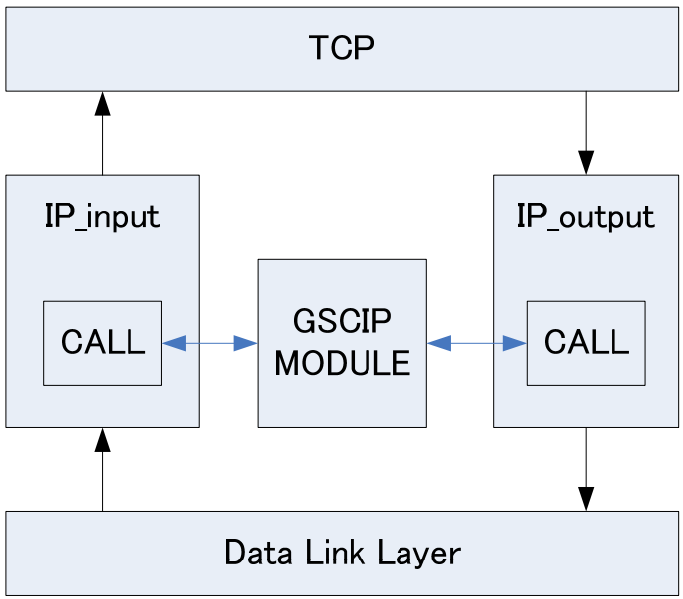
- 通信開始の際に各GEの情報を知るためにDPRPを行う



PIT（Process Information Table）
通信パケットに対する処理を定義する動作処理情報（暗号化/復号，透過中継，破棄）を格納

- 終端GEを決定
- 経路上の各GEのグループ情報を収集し，動作処理情報を決定
- GKによって通信相手が同一グループであるか確認
- 動作処理情報テーブルPIT を生成
- 以降の通信はPITに定義された動作処理情報に従って動作

GSCIPの現状

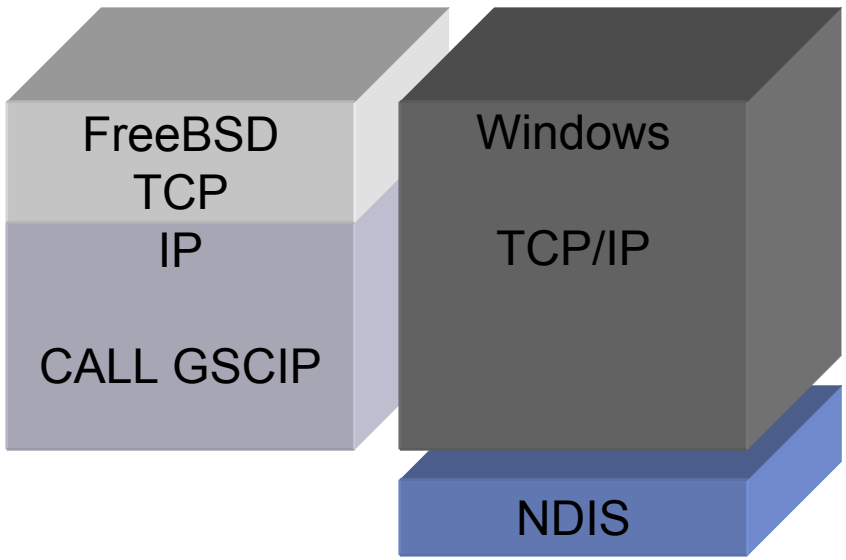


- FreeBSDではIP層にモジュール呼び出しを追加
- 動作確認済み

GSCIPの評価や普及にはWindowsへの実装が必要

Windows

- WindowsはTCP/IPなどのOSがブラックボックス
  - FreeBSDのようにIP層を直接改造できない

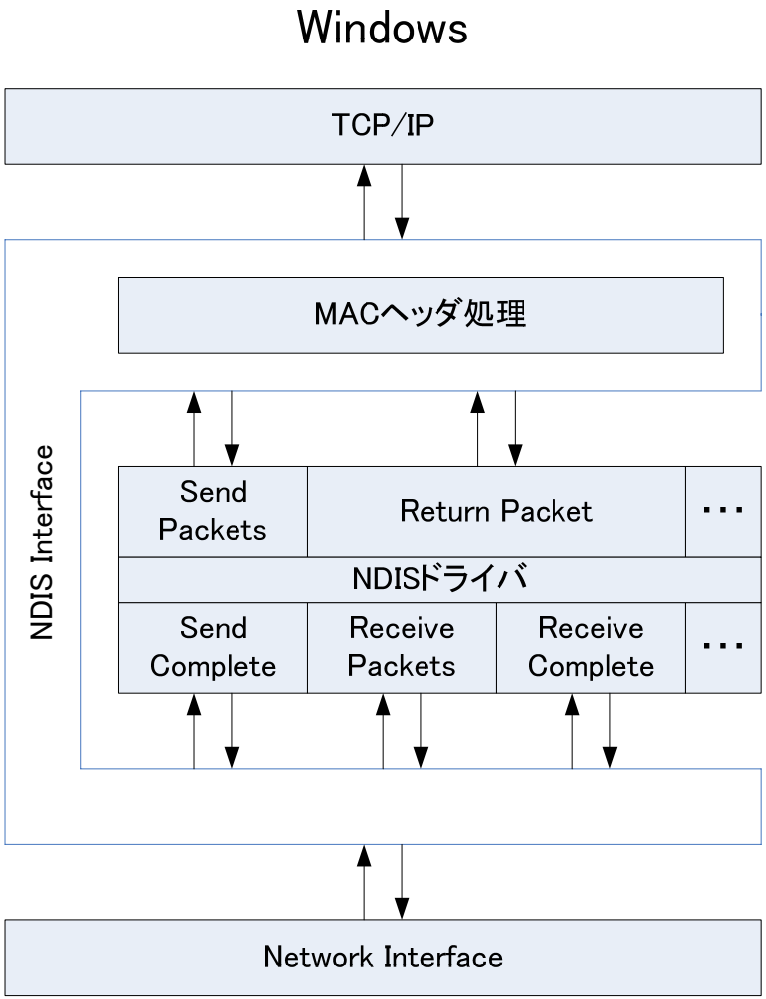


外部に仕様が公開された
インタフェース

ネットワークの機能拡張ができるインタフェース

NDIS (Network Driver Interface Specification)

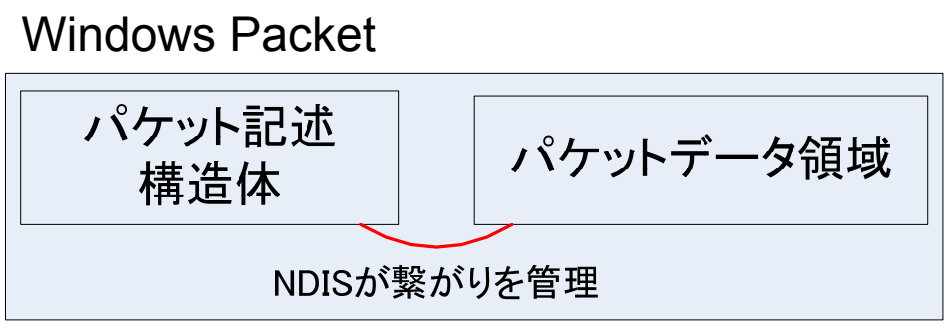
NDISの動作概要



- NDISはネットワークに機能を追加できるインタフェース
- NDISでの機能追加はTCP/IPやデータリンク層の処理より下層
- NDISドライバは仕様として公開された機能を実行するモジュール群として作成し，NDIS Interfaceに登録
- NDISは各モジュールを必要に応じて呼び出す

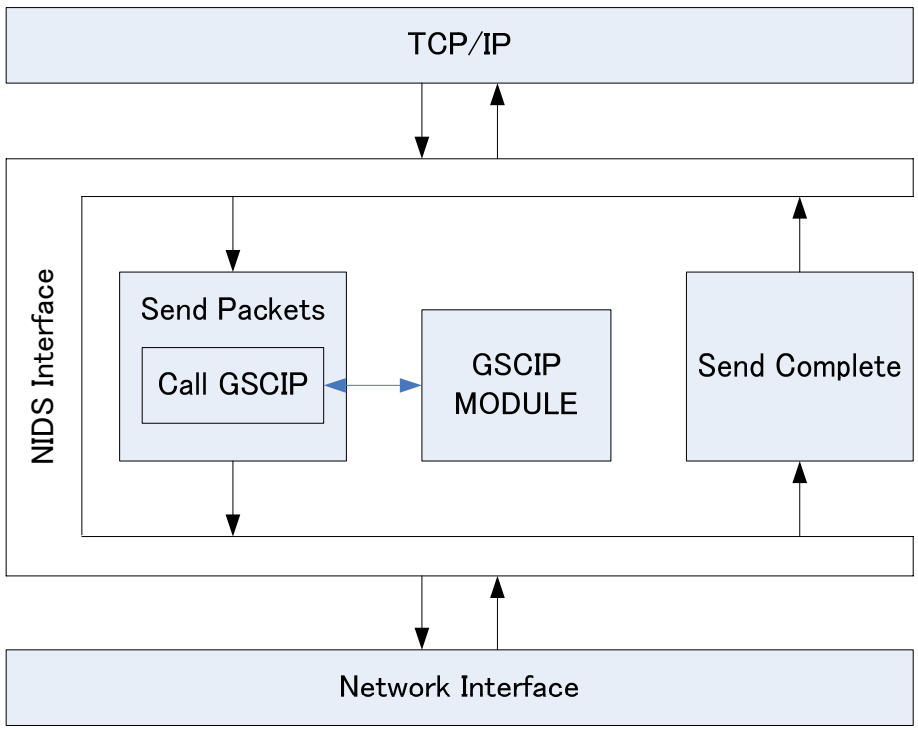
Windowsへの移植

- API (Application Programming Interface)の違い
  - OSが違うため，APIを同等の処理になるように置き換え
- MACヘッダの処理を追加
- パケットの形式
  - FreeBSDでは構造体でパケットを表現
  - NDISでは構造体とメモリ領域の接続で表現



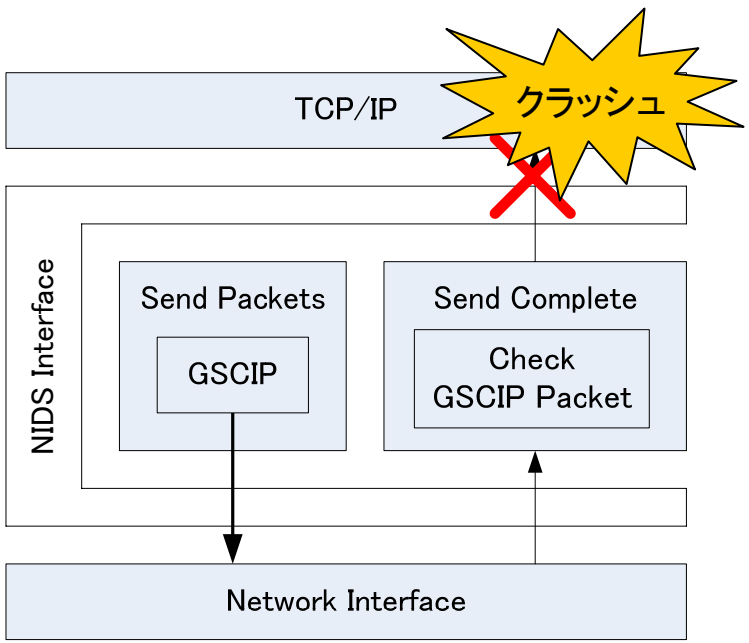
NDIS送信動作

1. Send Packets
   - 上位から下位へ送信パケットを渡す
   - このモジュールからGSCIPを呼び出す
2. Send Complete
   - 下位から上位へパケット送信処理の結果を通知



送信処理完了通知
Send Complete

- GSCIPのプロトコルには独自のパケットを作成し，通信を行う動作がある
  - TCP/IPが関与しないパケットのSend Completeが行われるとシステムが不安定になる

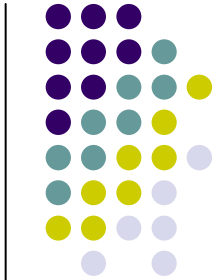


- Send Completeモジュールに GSCIP独自パケットの判断処理を追加
- TCP/IPが関与しないパケットを通知しない

まとめ

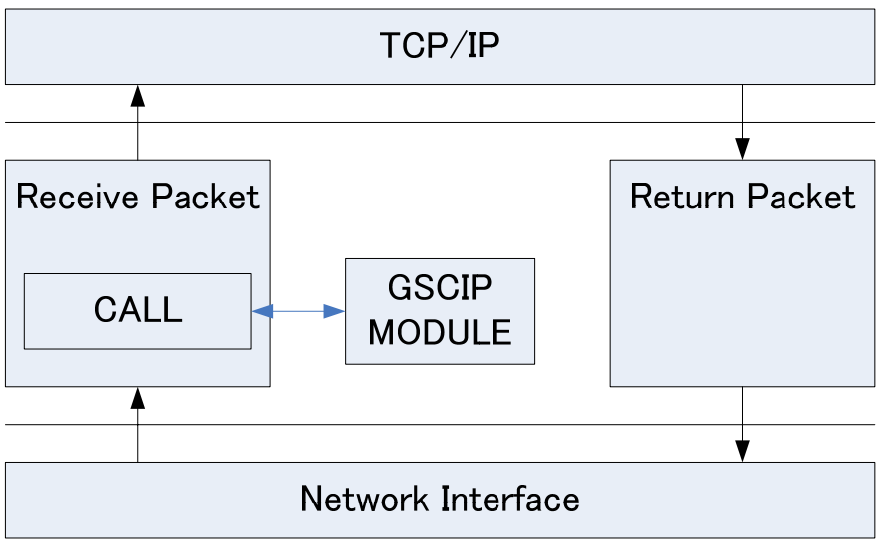
- GSCIPをWindowsに実装する方法についての検討を行った

- 現在パケット送受信動作を含む一部機能の動作確認済み
- 今後は実装を完了させ，性能評価を行う



NDIS受信動作

1. Receive Packet
   - 下位から上位へ受信パケットを渡す
   - このモジュールからGSCIPを呼び出す
2. Return Packet
   - 上位から下位へ処理がすべて終了したパケットを通知
   - 最下層のモジュールは通知を受けたパケットデータを破棄できる



受信

- GSCIP独自のパケットがTCP/IPに渡されるとICMPパケットが送信される
  - GSCIP独自のパケットはICMPベース