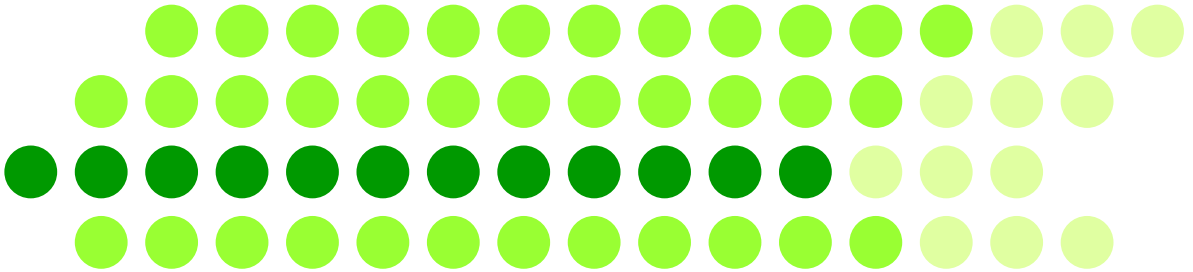
GSCIPのWINDOWSへの実装

-Implementation of GSCIP in Windows-

渡邊研究室

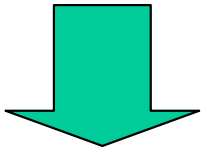
030432105　三宅 智朗



研究背景

- ユビキタスネットワーク環境の整備
  - 安全に通信したい
  - 自由に移動しながら通信したい

というニーズの増加



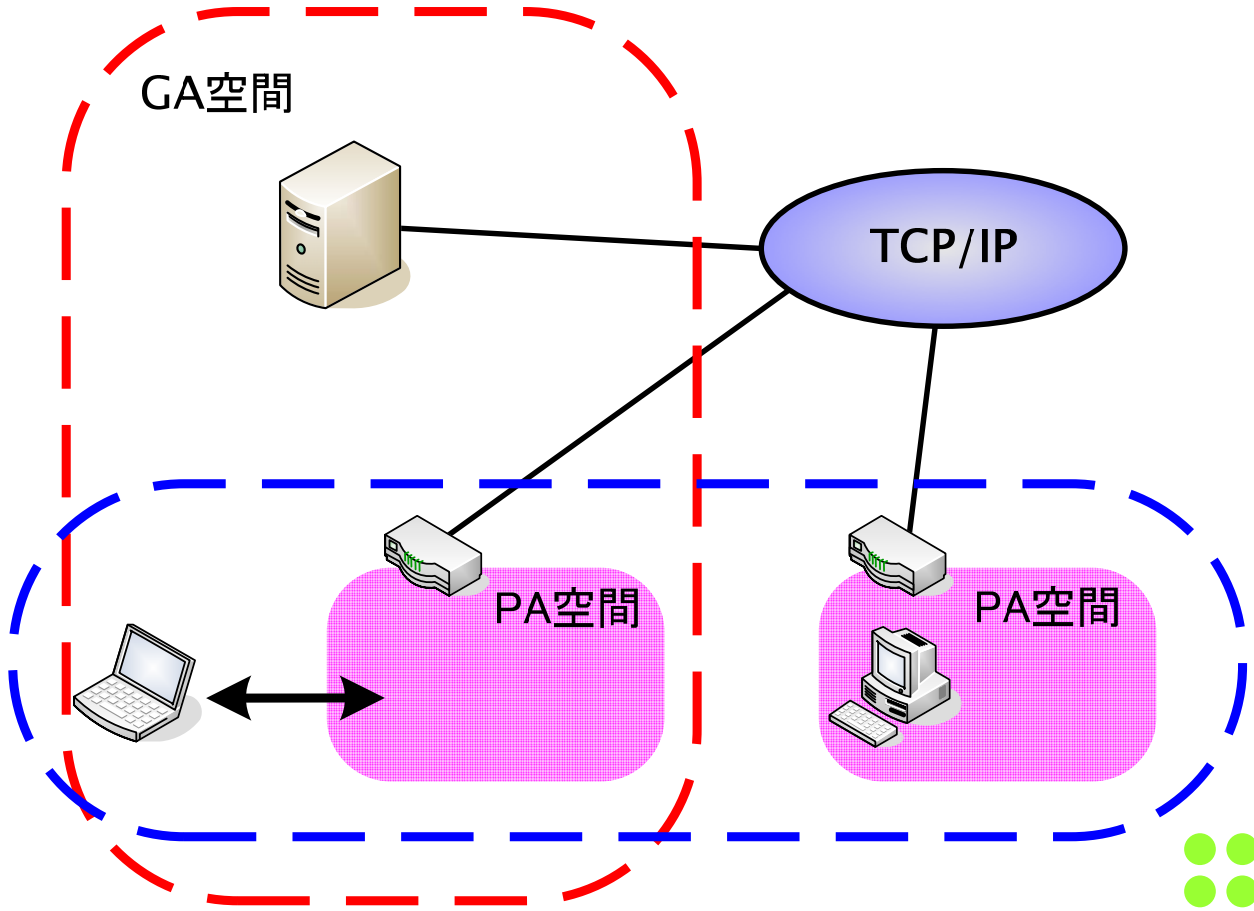
FPN（Flexible Private Network）

柔軟性とセキュリティを兼ね備えたグルーピング通信を可能とするネットワークシステム

FPN（Flexible Private Network）

特徴

- 全てのホストが動くことを想定
- サブネットの内外を自由に移動してもグループの定義を維持
- 端末及びドメインは，複数のネットワークに重複帰属可能
- 個人単位とサブネット単位の要素が混在した環境でも通信グループの定義ができる

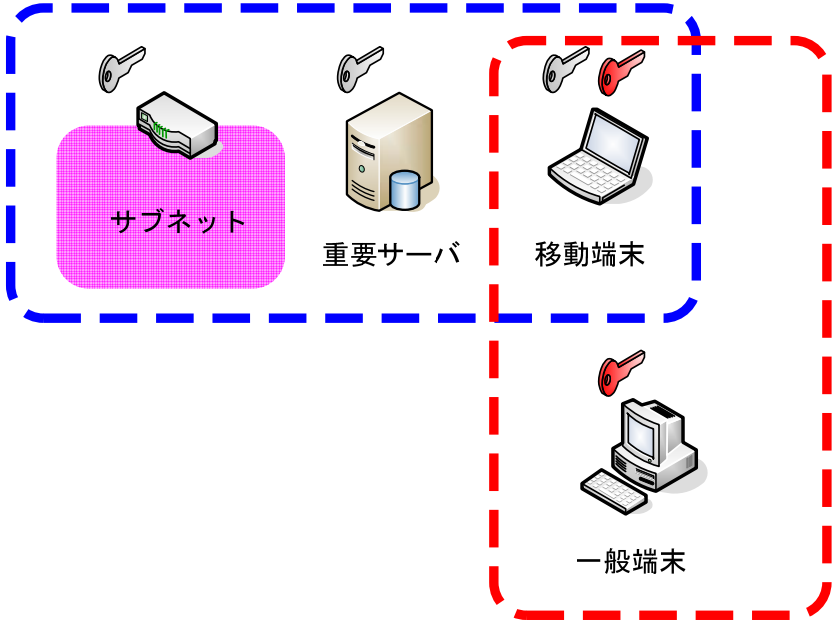


GSCIP (Grouping for Secure Communication for IP)

FPNを実現するためのセキュア通信アーキテクチャ

GSCIP（ジースキップ）の機能

グループ鍵を用いた通信グループの定義
グループ鍵と通信グループが1対1に対応
IPアドレスに依存しないグループ定義



- 現在、GSCIPはFreeBSDのIP層に実装済
- 動作確認済

研究の狙い

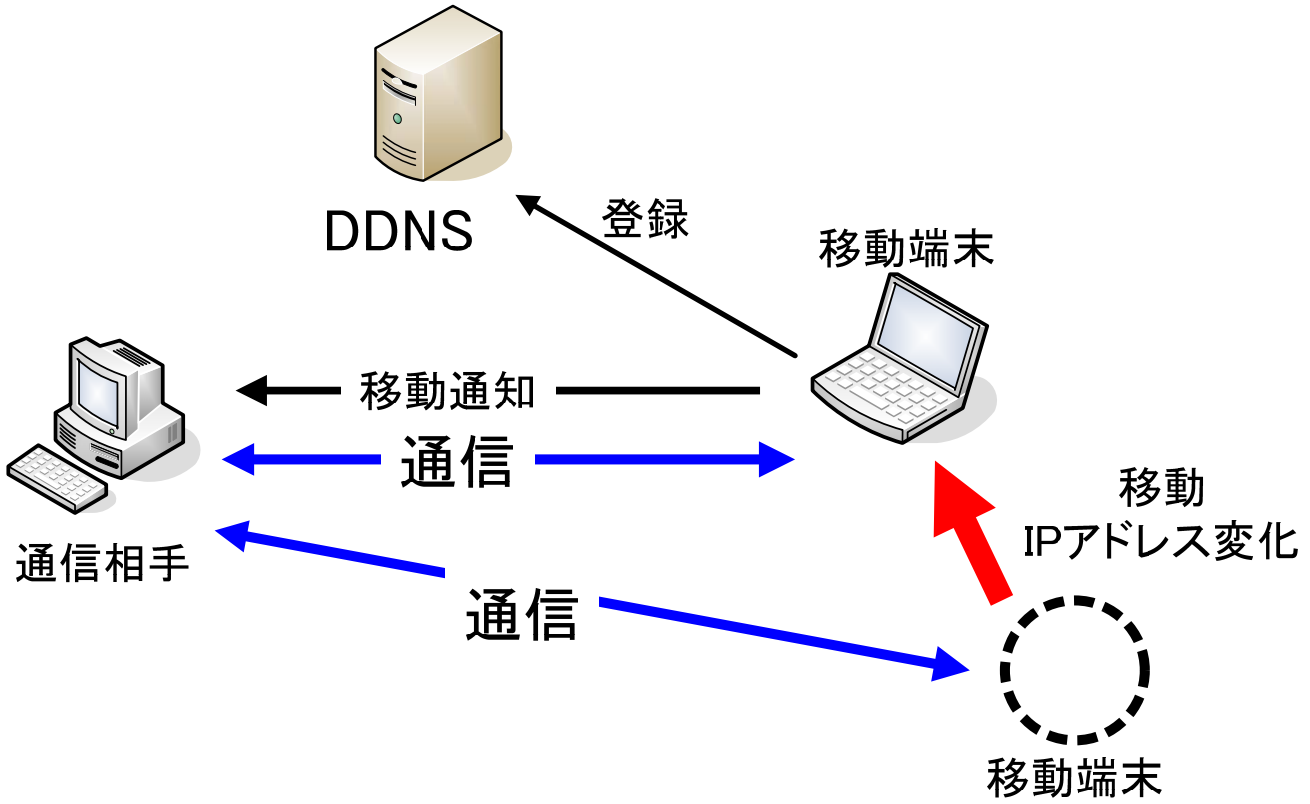
Windowsに実装することにより，GSCIPの普及をはかりたい

GSCIPの実現

FPN (Flexible Private Network)

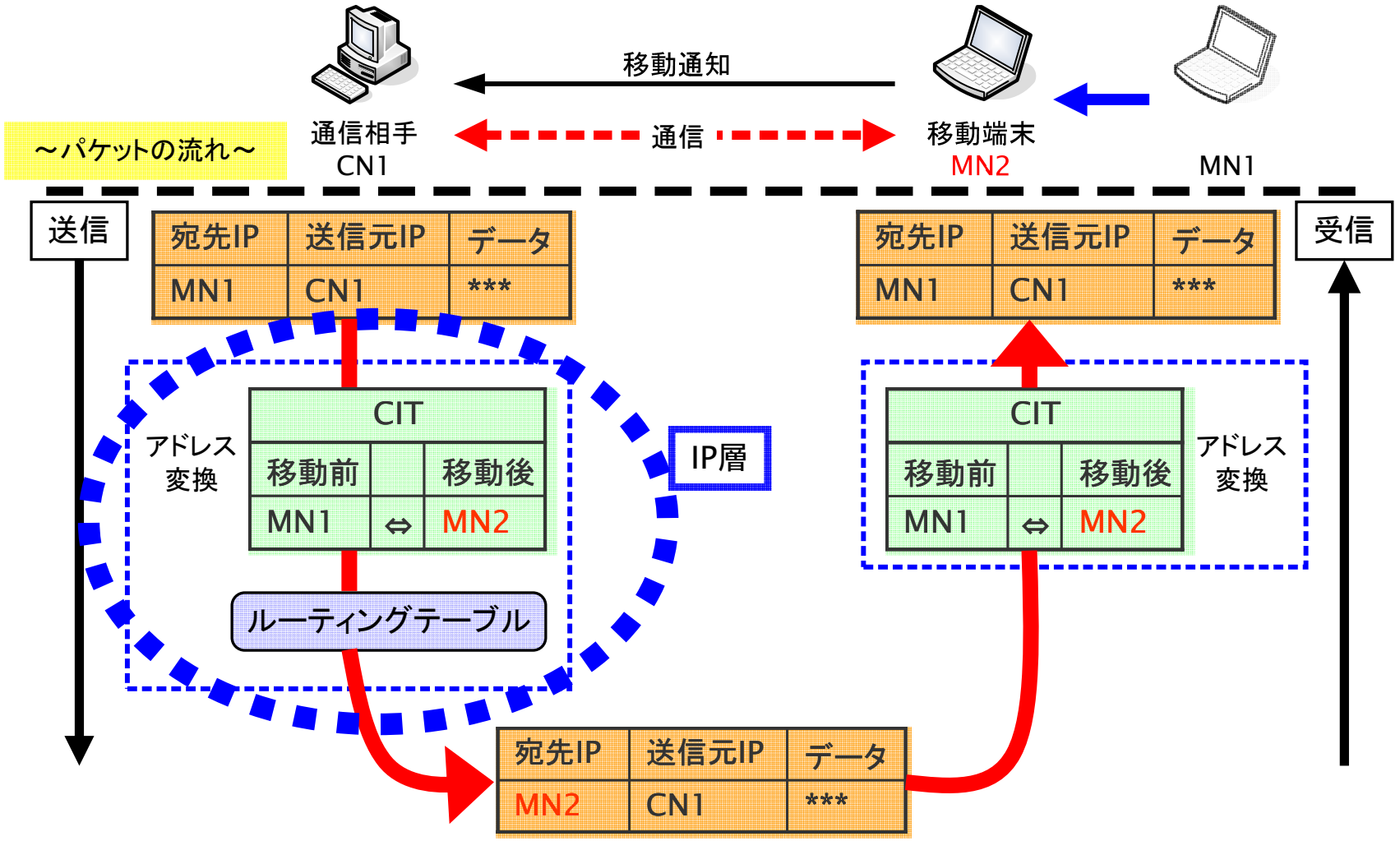
- アーキテクチャ
- GSCIP (Grouping for Secure Communication for IP)
  - プロトコル群
    - DPRP (Dynamic Process Resolution Protocol)
    - Mobile PPC (Mobile Peer to Peer Communication)
    - NAT-f（NAT free protocol）
    - PCCOM（Practical Cipher COMmunication protocol）
    - SPAIC（Secure Protocol for Authentication with IC Card）

Mobile PPC (Mobile Peer to Peer Communication)



- 通信開始時に相手のIPアドレスを知る方法としてDDNS (Dynamic DNS)を使う
- 移動通知はエンドエンドで行う
- IP層でアドレス変換処理するため，アプリケーションに対してIPアドレスの変化を隠蔽

Mobile PPC のアドレス変換の流れ



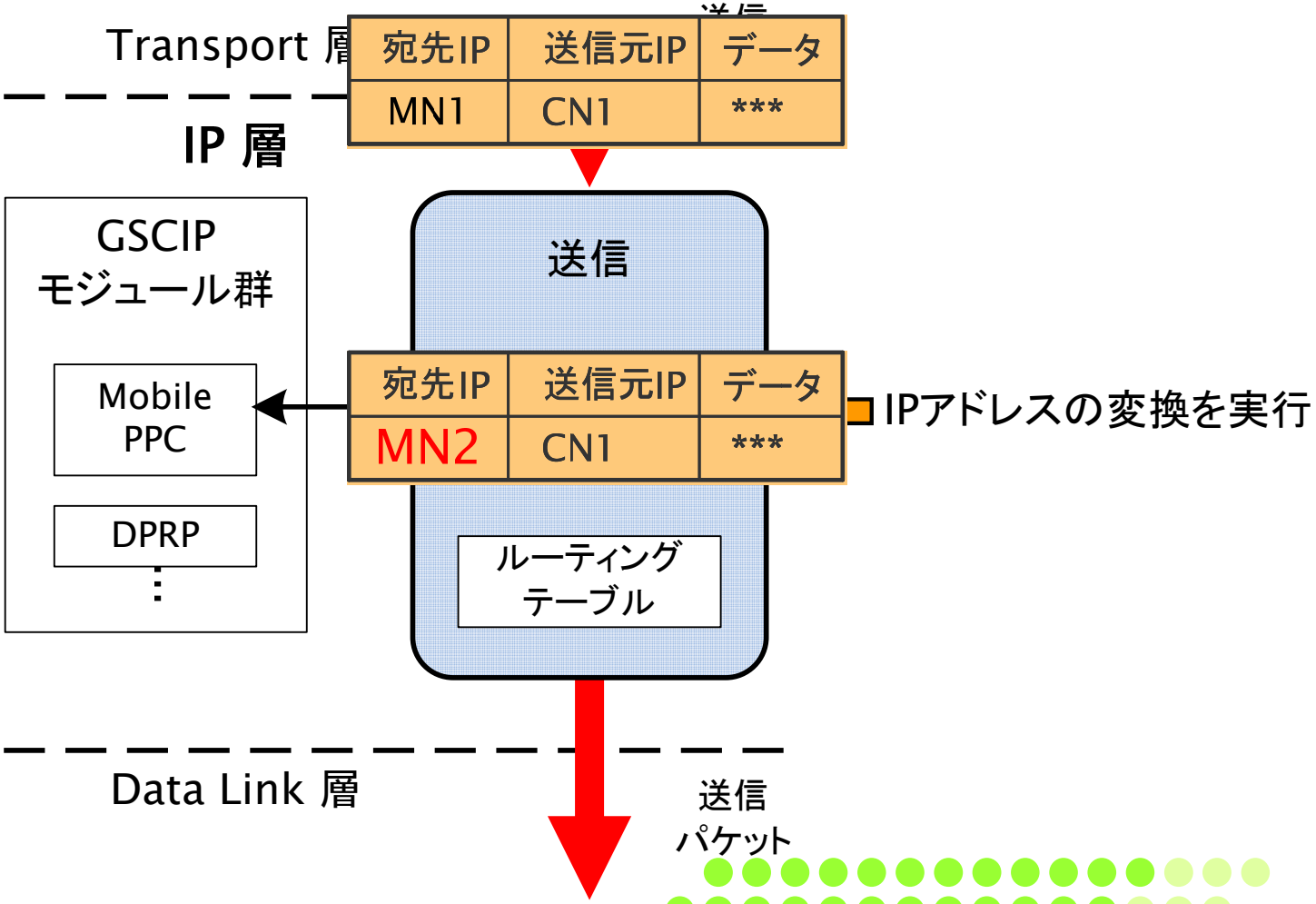
- 移動通知を受けたらアドレス変換テーブルCIT（Connection Id Table）を更新し，その後の通信はCITを参照しIP層においてアドレス変換を施し

IPアドレスの変化を上位層に隠蔽

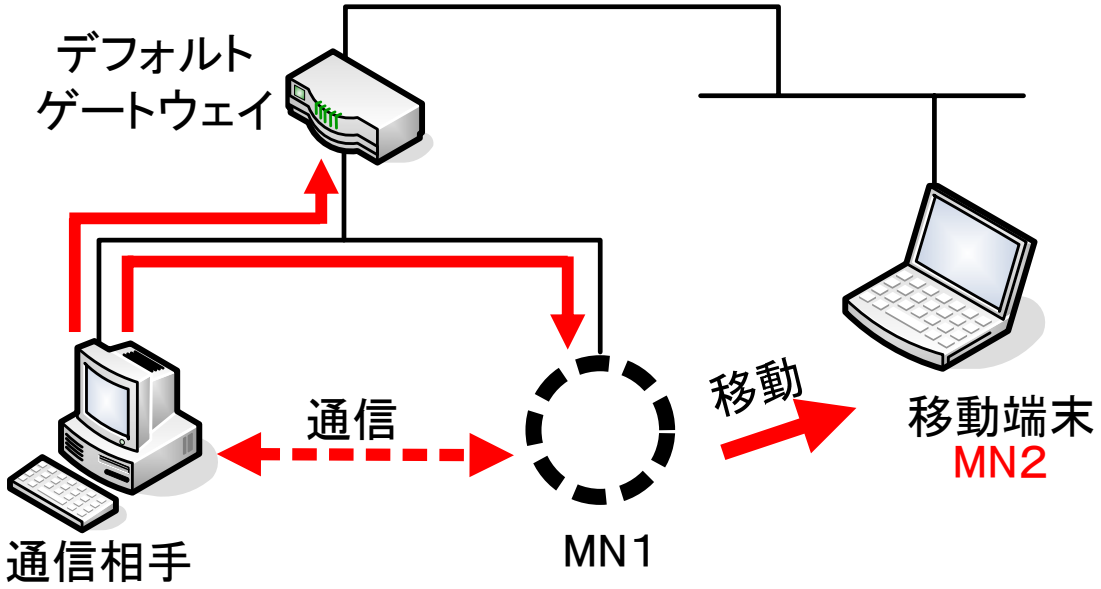
ルーティング

- Mobile PPCによるパケット送受信時の処理
  - 通信パケットに対するIPアドレスの変換処理
  - IP層内に保持されているIPルーティングテーブルの参照

※FreeBSDの場合
（送信処理）



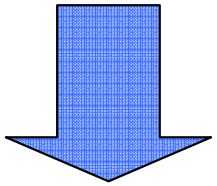
ルーティングテーブル



宛先	ゲートウェイ
デフォルト	Z. Z
MN1	A. A
MN3	B. B

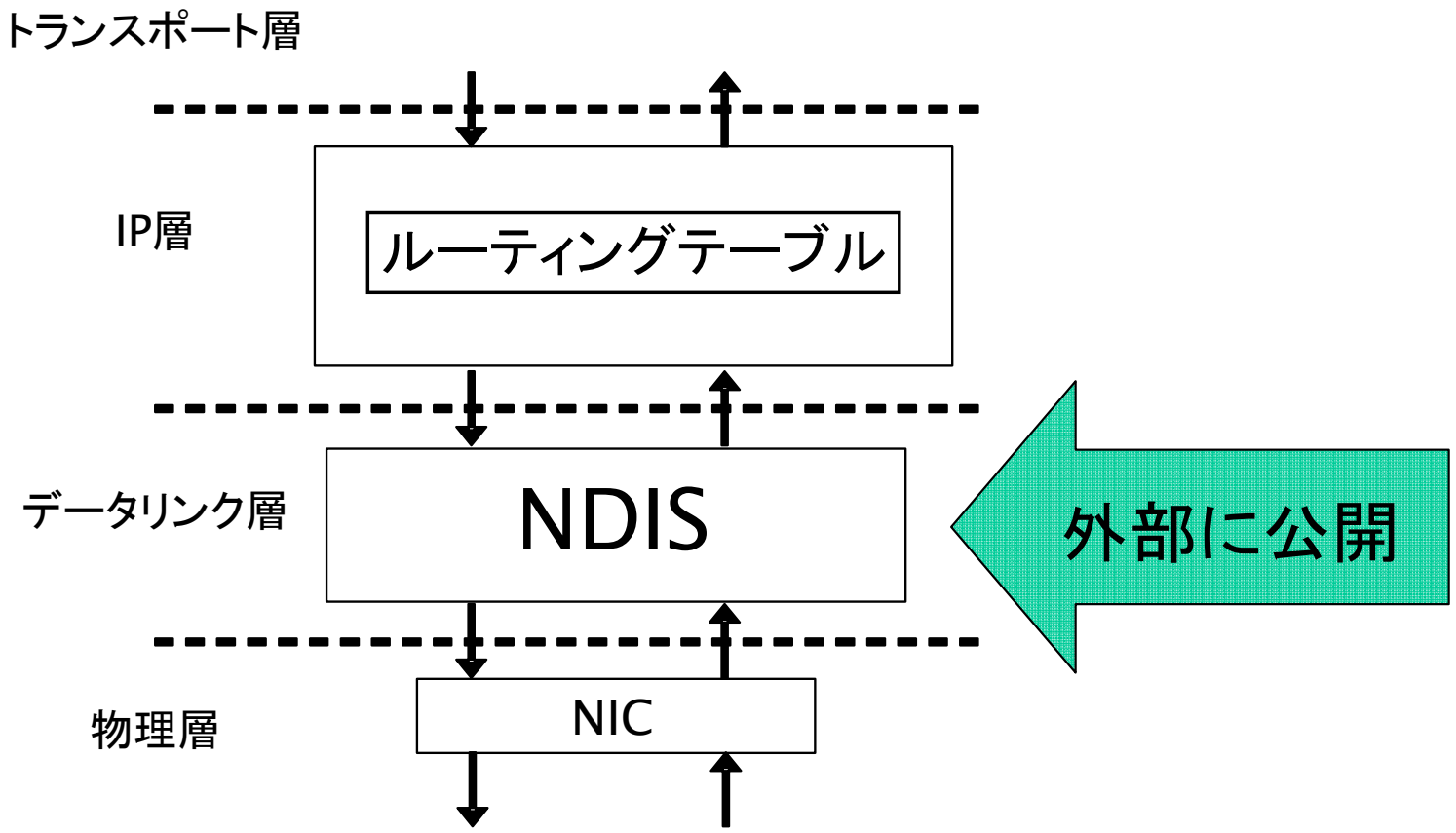
実装にあたっての課題

WindowsはTCP/IPを含むOSがブラックボックス



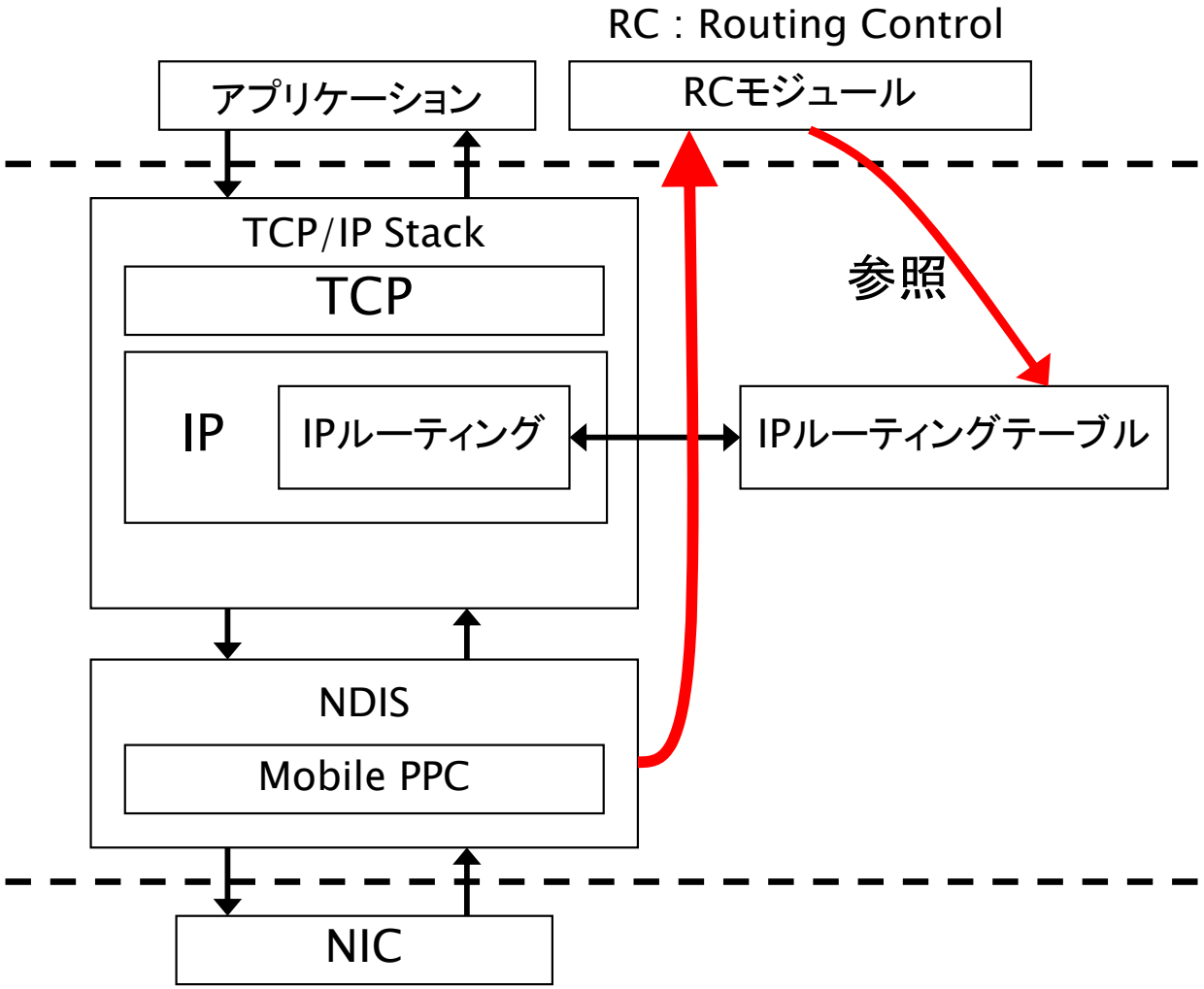
Windowsでは，IP層の改造が出来ない

実装にあたっての課題



- NDIS (Network Driver Interface Specification)
  - Microsoft社が定めたネットワークドライバの仕様
  - ネットワークドライバに機能を追加できるように規定

実装方法



～～流れ～～

Mobile PPC呼び出し

NDIS内で，アドレス変換テーブルCITを基にアドレス変換を施す

Mobile PPCからRCモジュールに制御を渡す

RCモジュールにて，IPルーティングテーブルの値を参照

参照した値を基にMACアドレスを書き換えてルーティング

- Mobile PPC以外の機能はFreeBSDから流用できる見込み

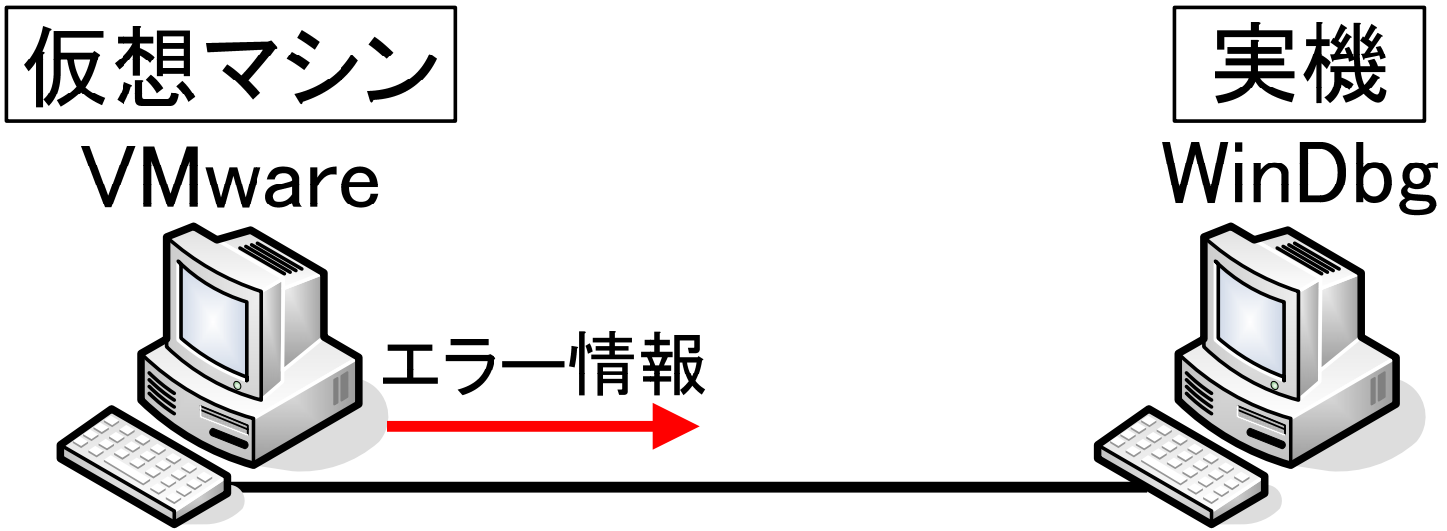
実装環境

- 仮想マシンVMware
  - カーネル領域に手を加えるため
  - 実機で行うより，スムースなプログラミング
- 開発ツール
  - Windows DDK
  - Microsoft Visual Studio 6.0
- デバッグツール
  - WinDbg 6.3

デバッグ・検証

デバッグ手法：リモートデバッグ

- 再起動に要する時間的コスト
  - リアルタイムにエラー情報の取得
- ダンプに関する問題
  - OS が停止してしまうとエラー情報が取得できない



実装状況

- NDIS内を流れるパケットの解析・書き換え・追加
- FreeBSDの関数をWindowsの対応する関数にリプレイス
- OpenSSLのインストール
- DPRPの実装中

まとめ

- GSCIPのWindowsへの実装
  - NDIS内に実装
  - DPRPを実装中
- 今後
  - 実装を完了させ，動作検証及び性能評価

付録