

GSCIP の Windows への実装

三宅 智朗*, 播磨 宏和, 渡邊 晃(名城大学)

Implementation of GSCIP in Windows

Tomoro Miyake, Hirokazu Harima, 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多く実現が難しい。

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為には、Windows に機能を実装させ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 を実装するにあたっての課題

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ピングを定義でき管理負荷を軽減できる。

GSCIP の機能としては、DPRP (Dynamic Process Resolution Protocol) と Mobile PPC (Mobile Peer to Peer Communication) 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 対応装置の認証や、通信の可否を判断する処理。Mobile PPC は通信中に一方の端末が移動したとき、エンド端末どうしで 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アドレスの変化を隠蔽する。この処理を移動透過性と呼ぶ。現在の GSCIP は FreeBSD の IP 層に実装し、基本動作を確認済みである。GSCIP モジュールは IP 層の適切な場所から呼び出されるサブルーチンとなっている。オープンソースなので、IP 層を改造することにより実現が可能である。Windows は TCP/IP を含む OS がブラックボックスであるが、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 とは 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。しかし、上記で述べた移動透過性を実現するためには、Mobile PPC によって、通信パケット

に対する IP アドレスの変換処理を行うとともに、IP 層内に保持されている IP ルーティングテーブルと ARP キャッシュテーブルの書き換えも同時に必要である。FreeBSD では GSCIP の呼び出し口を変えることにより、両テーブルを自動的に書き換えることができた。しかし Windows ではその方法が取れないため、以下のような実装方法を考案し、実現できる見込みを得ることができた。

3. 実装方法

GSCIP の実装概念を図 1 に示す。GSCIP は NDIS 中間ドライバに実装する。Mobile PPC の処理中にルーティングテーブルと ARP キャッシュテーブルの書き換えを実現するために、GSCIP から一度アプリケーションに制御を渡し、そこから両テーブルを所定の値に書き換える。この処理により課題となっていた Windows における移動透過性の実現が可能となる。他の GSCIP に係る機能については、FreeBSD で実現済みのソースをほぼそのまま流用できる見込みである。

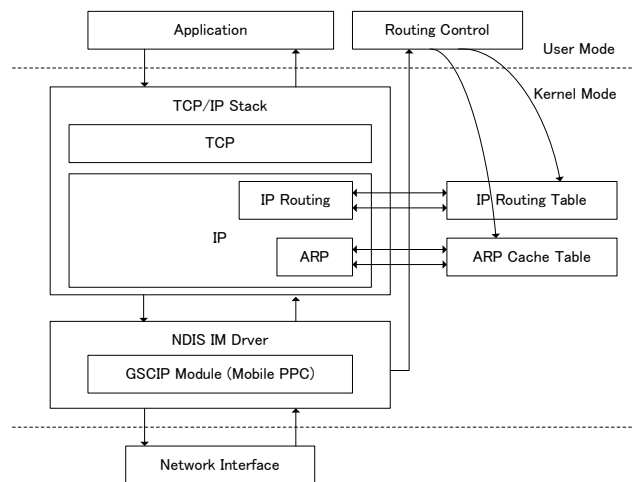


Fig.1. Implementation of GSCIP

4. まとめ

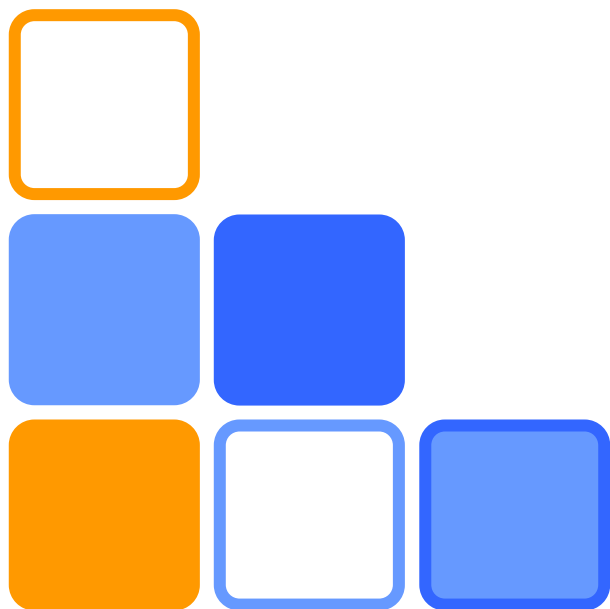
GSCIP を Windows に実装する方法についての検討を行った。今後は実装を完了させ、性能評価を行う。

参考文献

- [1] 鈴木秀和, 渡邊晃, “GSCIP を構成する DPRP の仕組みの検討”, 情報処理学会第 66 回全国大会 講演論文集 3-479, March2004.
- [2] 竹内元規, 渡邊晃, “移動体通信におけるコネクションを維持した通信方式の研究”, 情報処理学会第 66 回全国大会 講演論文集 3-463, March2004.

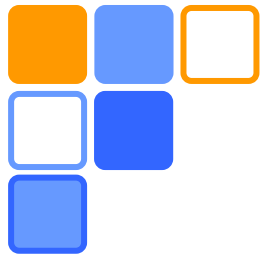
GSCIPのWINDOWSへの実装

- Implementation of GSCIP in Windows -



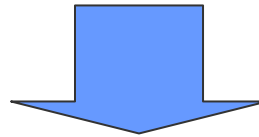
名城大学 理工学部

三宅 智朗 播磨 宏和 渡邊 晃



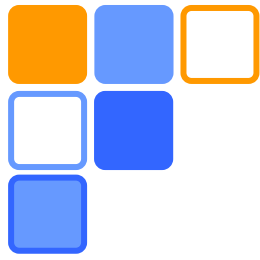
研究背景

- 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)

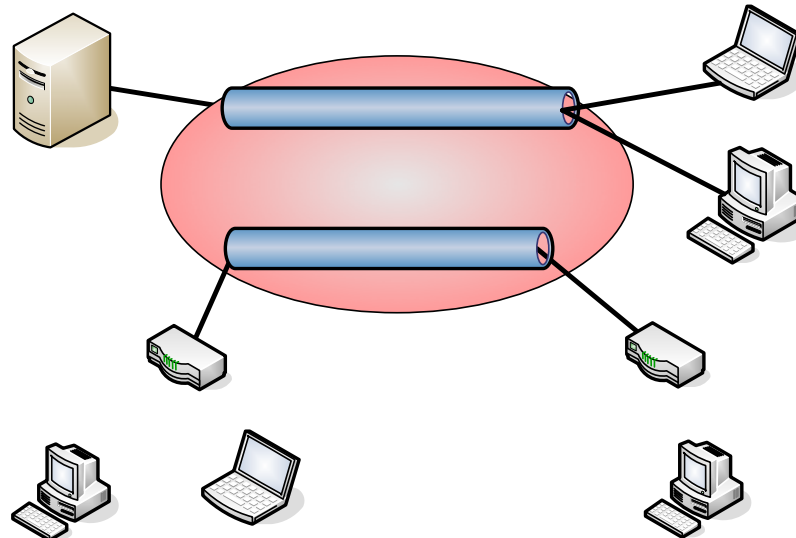
柔軟性とセキュリティを兼ね備えたグルーピング通信を
可能とするネットワークシステム

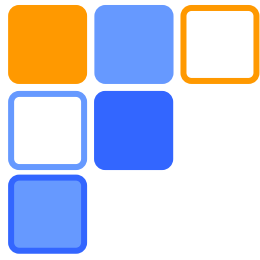


既存技術

VPN (Virtual Private Network)

- ネットワーク同士を安全に接続する手段
- リモートアクセス手段
- ネットワークのインフラを共有する手段としては有効
- VPNの課題
 - サブネット／サーバの位置が固定
 - アクセス開始の方向が固定 (リモートアクセス)
 - ネットワークの多段構成に対応できない

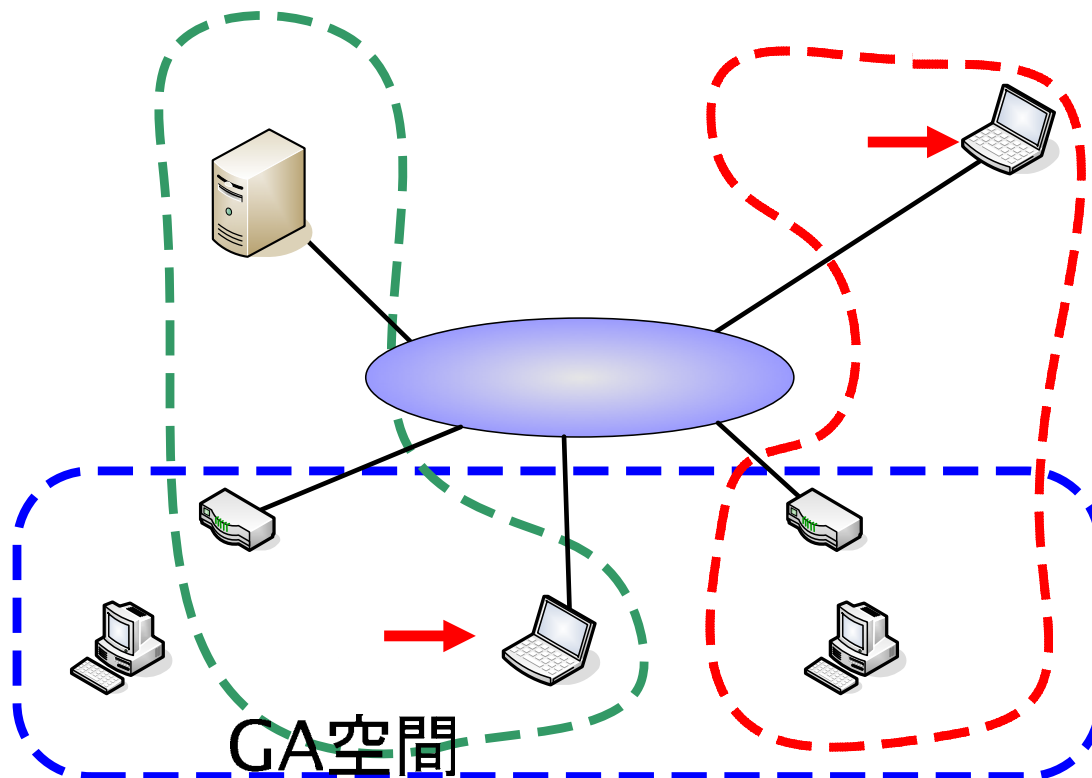




FPN (Flexible Private Network)

□ 特徴

- 全てのホストが動くことを想定
- ネットワークの多段構成に対応



□ 位置透過性

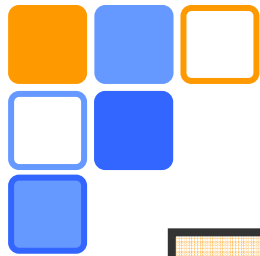
- ネットワークの物理構成が変化してもシステムが動的にその変化を学習して通信グループの関係を維持する

□ 移動透過性

- 通信中に端末が移動してIPアドレスが変化しても、通信を継続する

□ アドレス空間透過性

- GA (グローバルアドレス) 空間と PA (プライベートアドレス) 空間を意識せず通信できる (NAT越え)



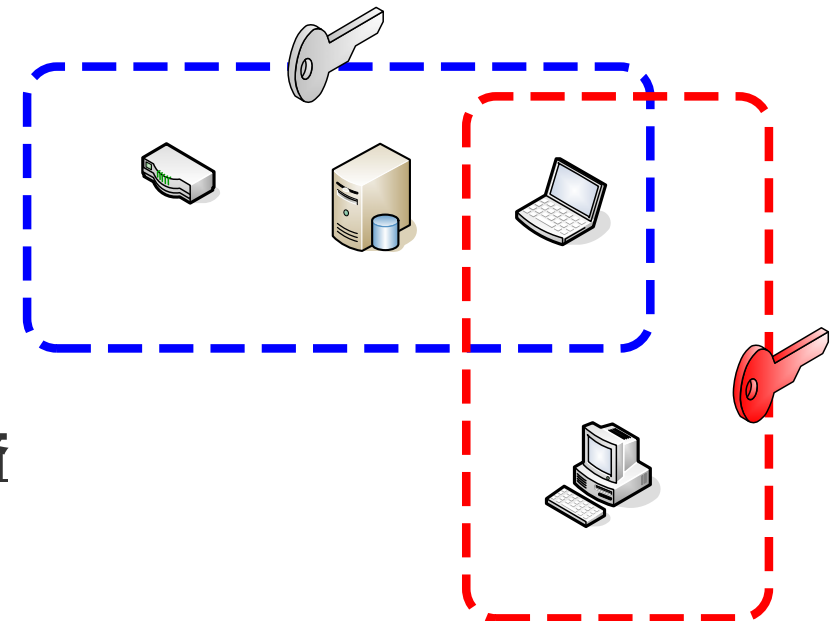
GSCIP (Grouping for Secure Communication for IP)

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

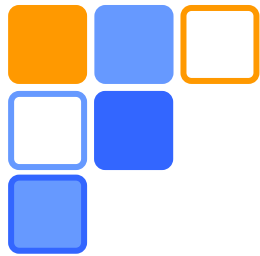
グループ鍵を用いた通信グループの定義
グループ鍵と通信グループが1対1に対応
IPアドレスに依存しないグループ定義

- 現在、GSCIPはFREE BSD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)

└ GSCIP (Grouping for Secure Communication for IP)

└ └ DPRP (Dynamic Process Resolution Protocol)

└ └ Mobile PPC (Mobile Peer to Peer Communication)

└ └ NAT-f (NAT free protocol)

⋮

} プロトコル名称

□ **位置透過性**



DPRP

通信に先立つネゴシエーション
動的処理情報の自動生成

□ **移動透過性**



Mobile PPC

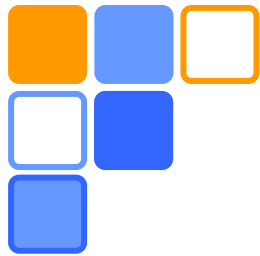
移動時のネゴシエーション
IP層でのアドレス変換

□ **アドレス空間透過性**

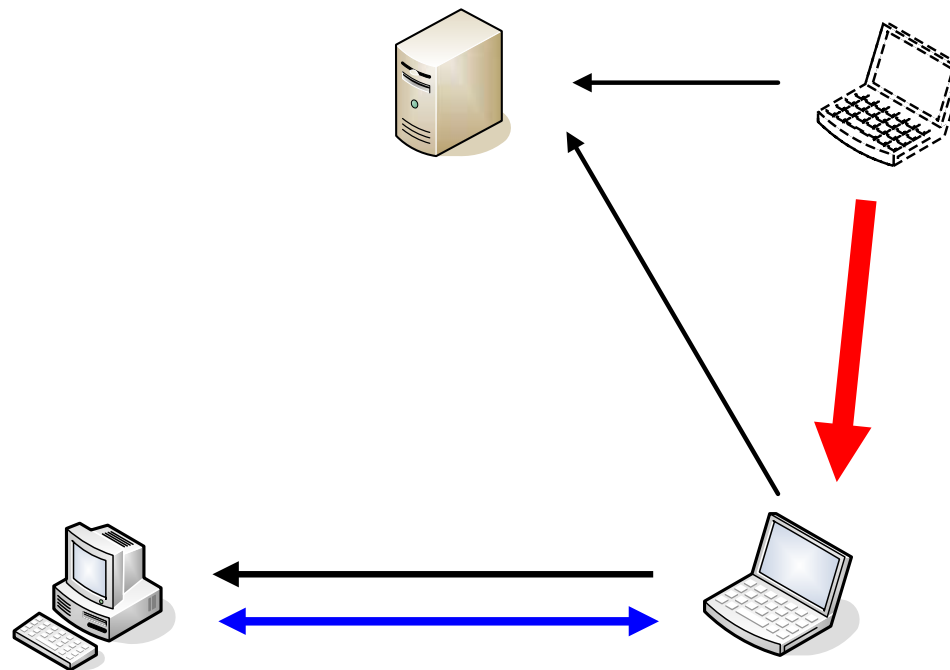


NAT-f

通信に先立つネゴシエーション
NATテーブルの自動生成

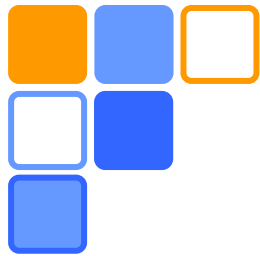


Mobile PPC (Mobile Peer to Peer Communication)

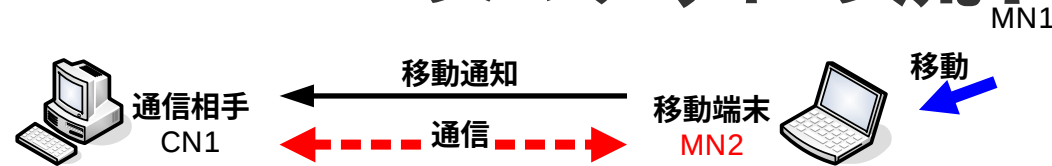


DDNS

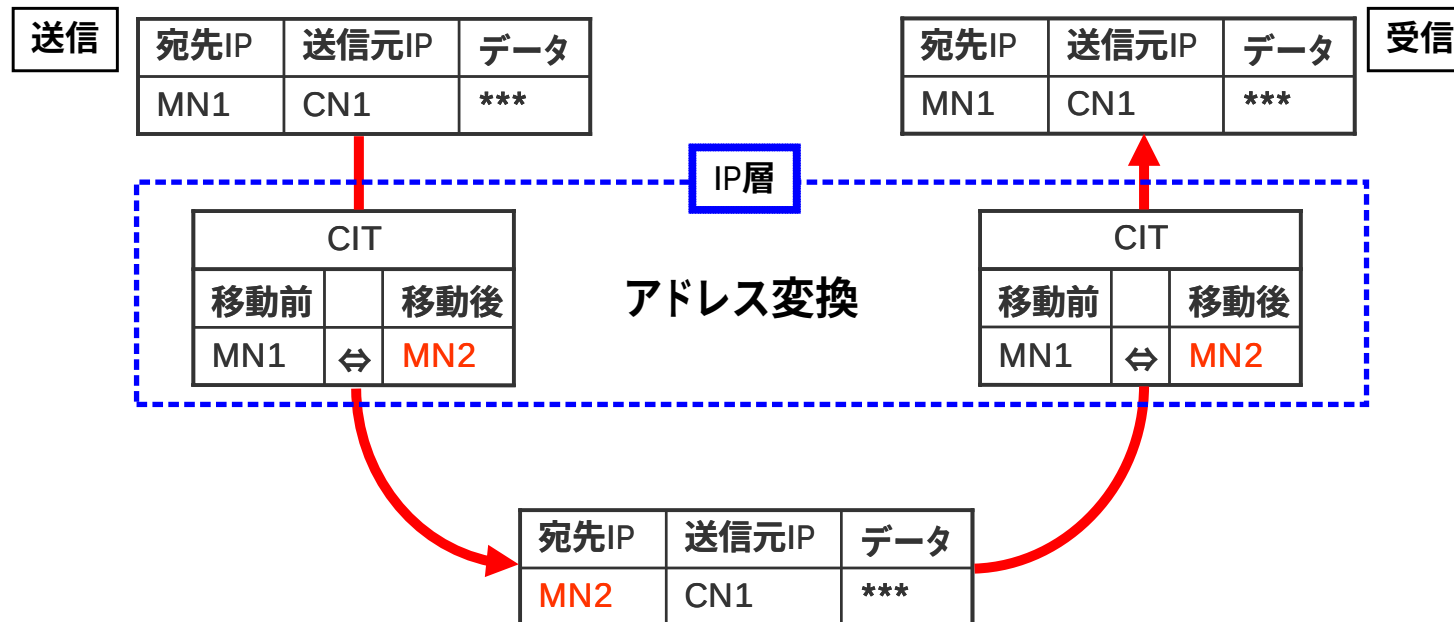
- 初期IPアドレスの解決にはDDNS (Dynamic DNS)を使う
- 移動通知はエンドエンドで通知
- IP層でアドレス変換処理するため, アプリケーションはIPアドレスの変化に気付かない



Mobile PPC のパケットの流れ

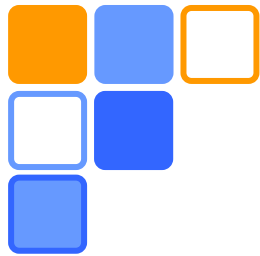


～パケットの流れ～



- 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

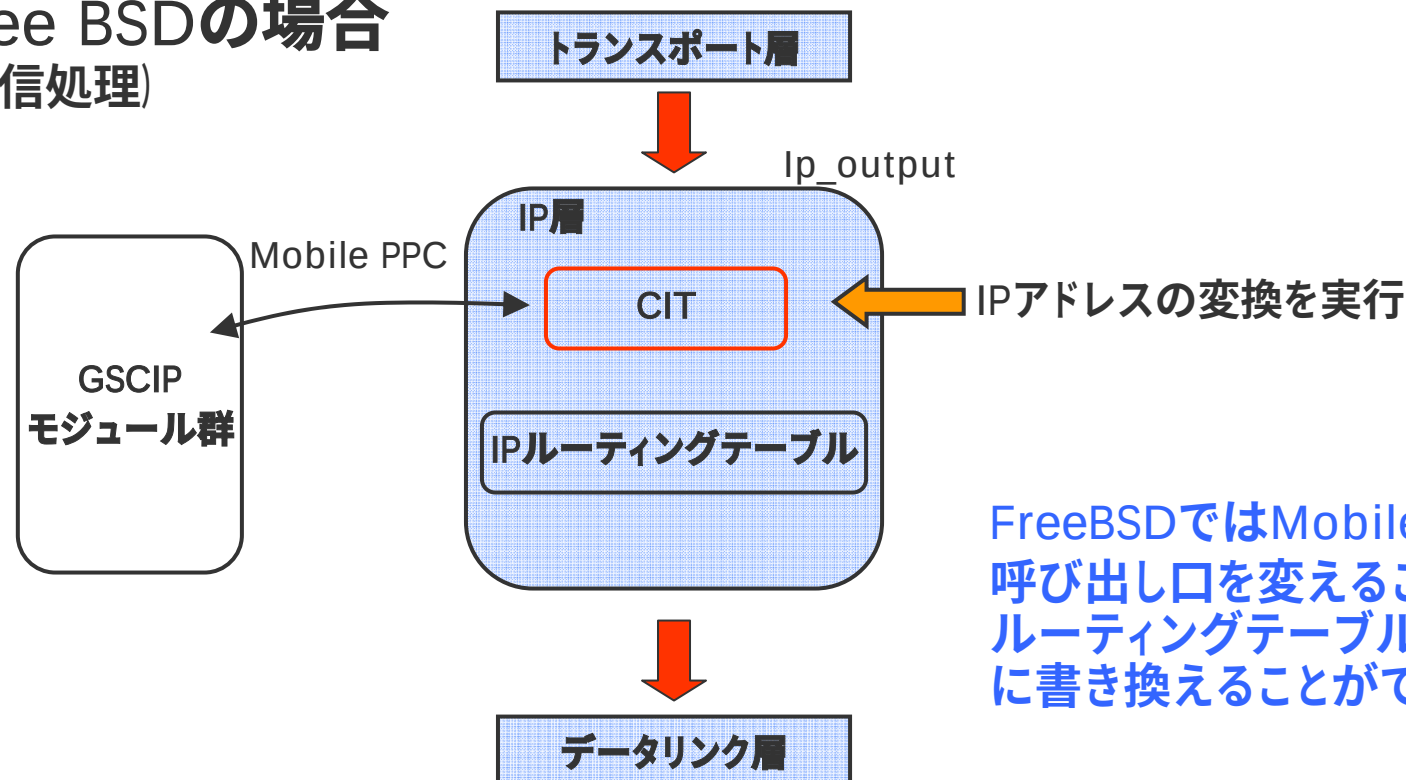
IPアドレスの変化を上位層に隠蔽



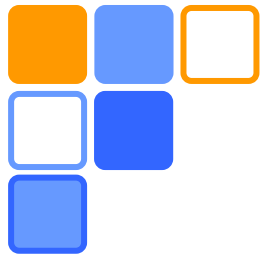
実装にあたっての課題

- 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書き換え

※Free BSDの場合
(送信処理)

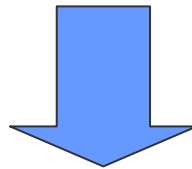


FreeBSDではMobile PPCの
呼び出し口を変えることにより
ルーティングテーブルを自動的に
書き換えることができた

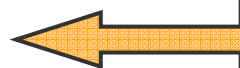


実装にあたっての課題

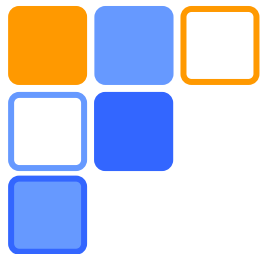
WindowsはTCP/IPを含むOSがブラックボックス



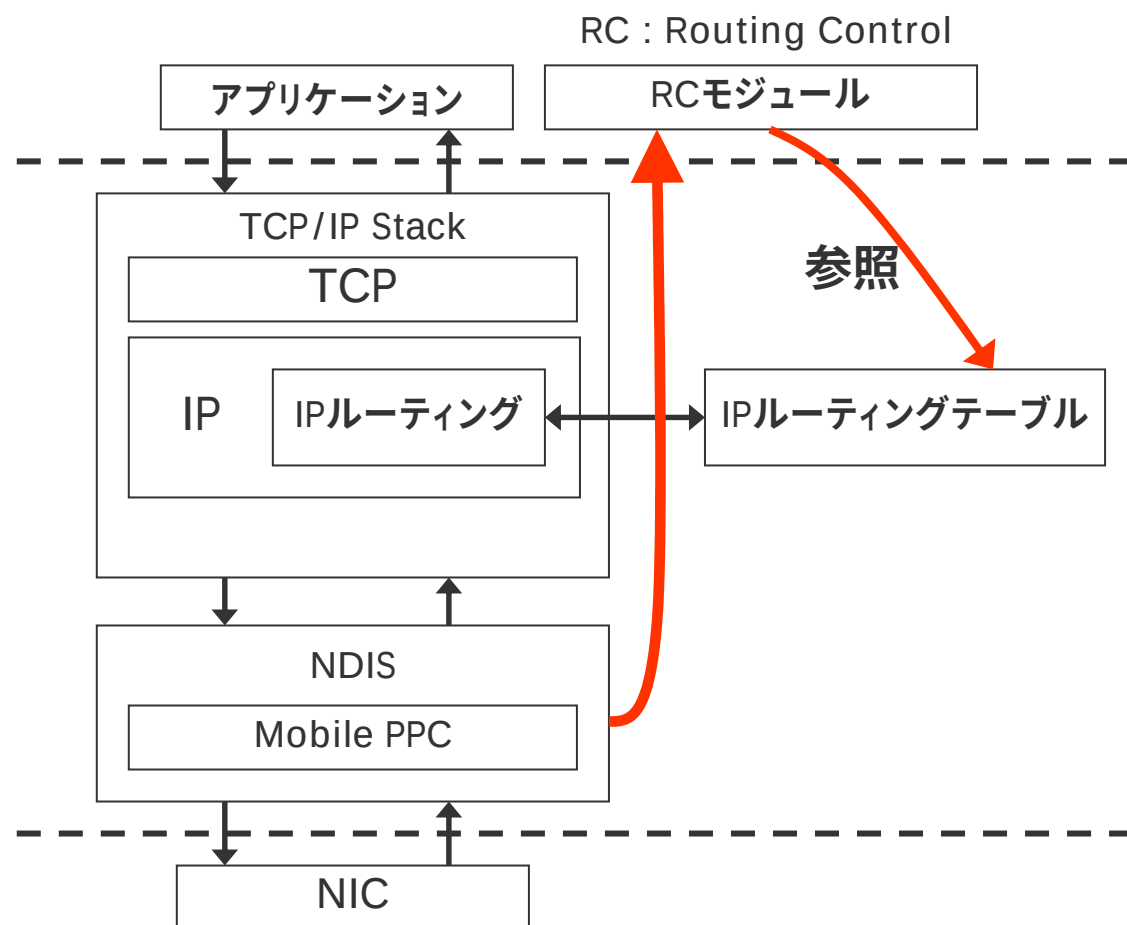
Windowsでは, IP層の改造が出来ない



外部に公開



実装方法



～～流れ～～

Mobile PPC呼び出し

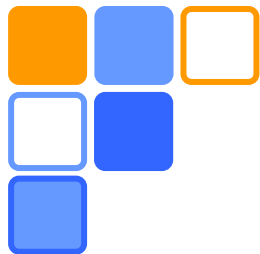
Mobile PPCからRCモジュールに制御を渡す

RCモジュールにて、IPルーティングテーブルの値を参照

参照した値を元にアドレス変換テーブルCITを更新

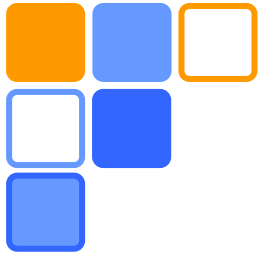
以後の通信はCITを参照しアドレス変換を施す

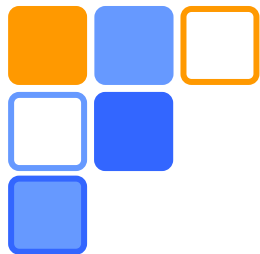
□ Mobile PPC以外の機能はFreeBSDから流用できる見込み



まとめ

- GSCIPをWindowsに実装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、動作検証及び性能評価を行う





ルーティングテーブル

行き先	ゲートウェイ
デフォルト	A.B
A.B	00:0c:29:...
A.C	A.B

