NTMobileフレームワーク

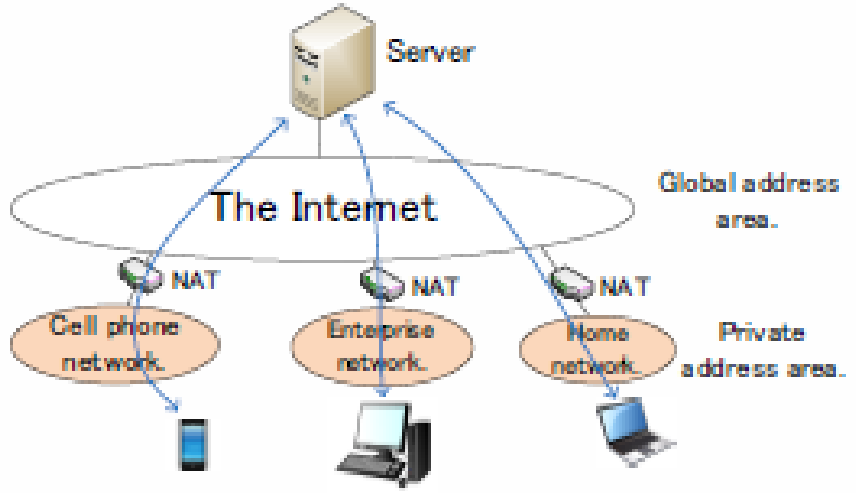
150441159 渡邉憲士

IPネットワークの課題

- NAT越え問題
  - グローバルアドレス空間からプライベートアドレス空間に
    通信を開始できない
- IPv4とIPv6は互換性がない
  - IPv4/IPv6間で相互通信を行うことができない
- 移動透過性がない
  - 通信中にネットワークを切り替えるとIPアドレスが変化するため
    通信を継続できない

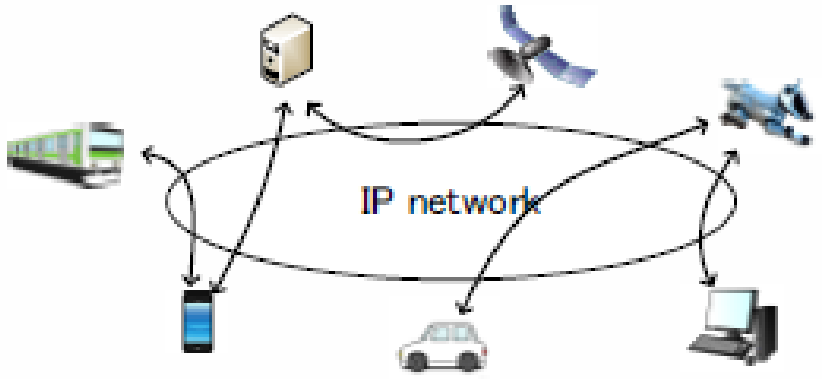
クライアントサーバモデル

- サーバをグローバルアドレス空間に置き、クライアント側から通信を開始するのが前提
- クライアント側がどのようなアドレス空間に存在しても、サーバとの接続性を保証できる
- サーバのセキュリティ対策や二重化対策など、管理不可が大きいという課題がある
- サーバが処理ネックになり、通信遅延が増大するという課題がある



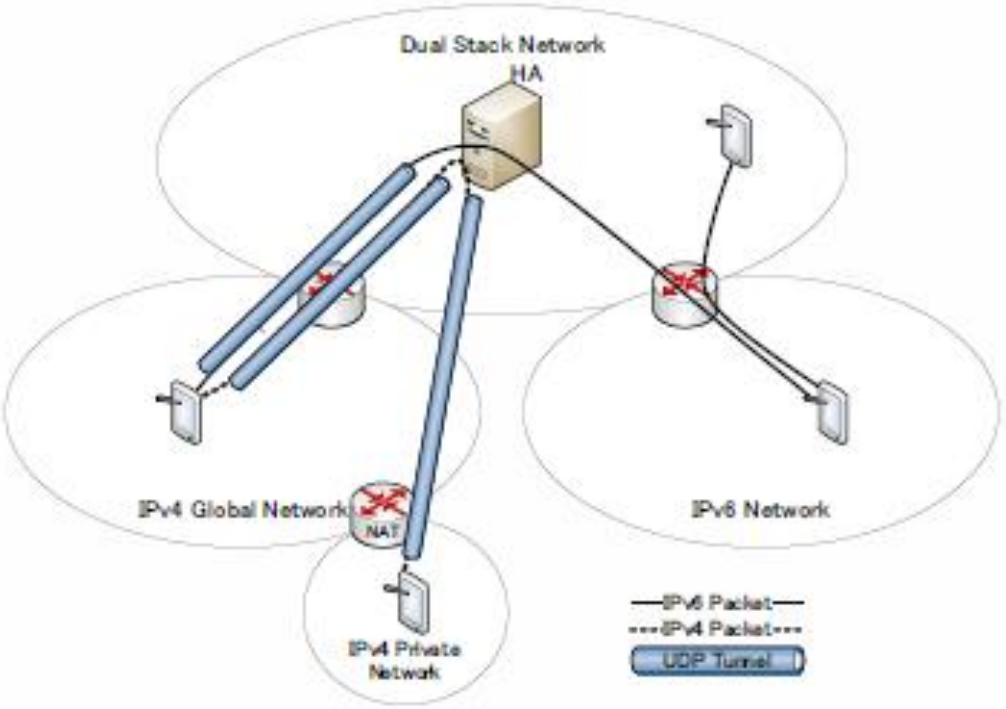
エンドツーエンドモデル

- ネットワークに接続する全ての装置が自由に通信できるモデル
- 任意の装置間で最適経路で直接通信ができ、通信中に任意の場所に移動しても通信が切れることがない
- クライアントサーバモデルを包含することができるためクライアントサーバモデルが適したシステムはそのまま利用することができる
- クラウドサーバにはプライバシー情報を除去した統計情報のみを蓄積し、ビッグデータのみを扱う作業に集中できる



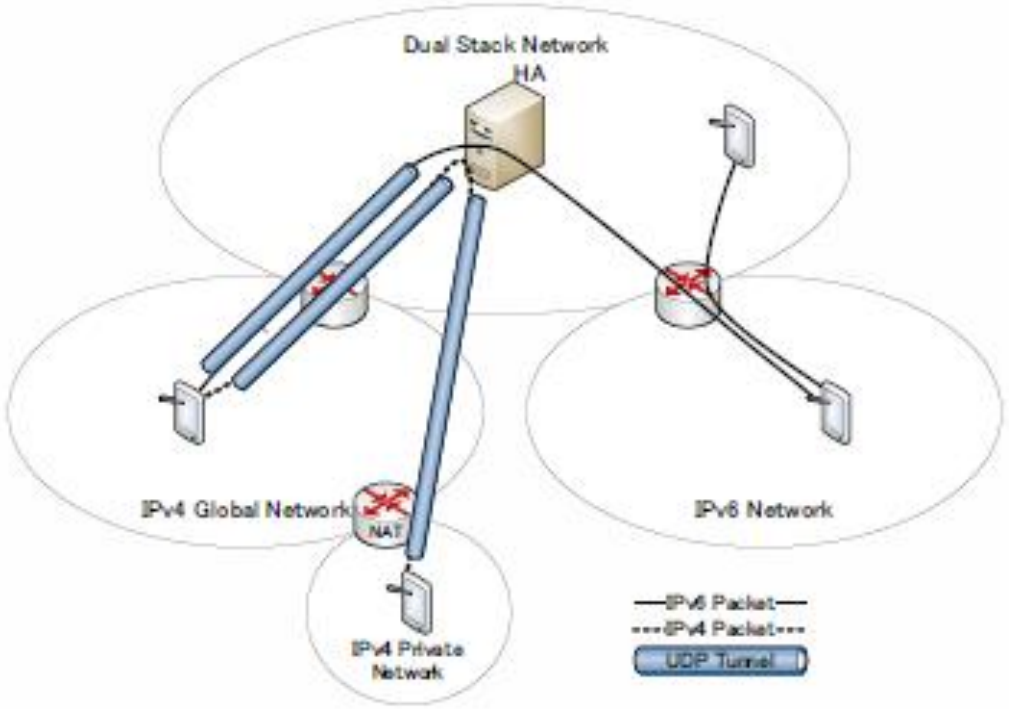
DSMIPv6(Dual Stack Hosts and Routers IPv6)

- MobileIPv6をIPv4/IPv6混在環境に拡張したものであり、IPv6の移動透過性技術をベースにNAT越え、IPv4/IPv6間の通信を可能にした方式である
- MobileIPv4の技術をそのまま利用できるようにしているため、課題がそのまま継承されている
- 全ての移動端末にIPv4グローバルアドレスが必要となるためアドレスの枯渇に逆行している
- カーネル内のIP層を改造するのが前提



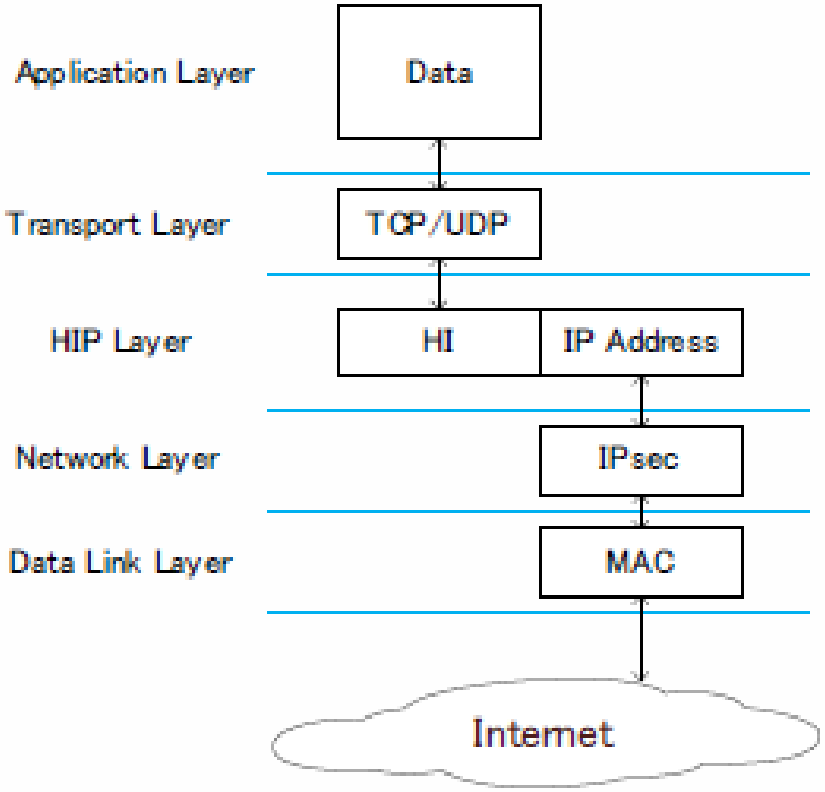
DSMIPv6(Dual Stack Hosts and Routers IPv6)

- MNはHoAとCoAの2種類のアドレスを持つ
  HoAは変化せず、HoA用いて通信を行う
- IPv6オンリーネットワークでは経路最適化により
  直接通信を行う
- IPv4空間では必ずHAを経由した冗長経路で
  通信を行う



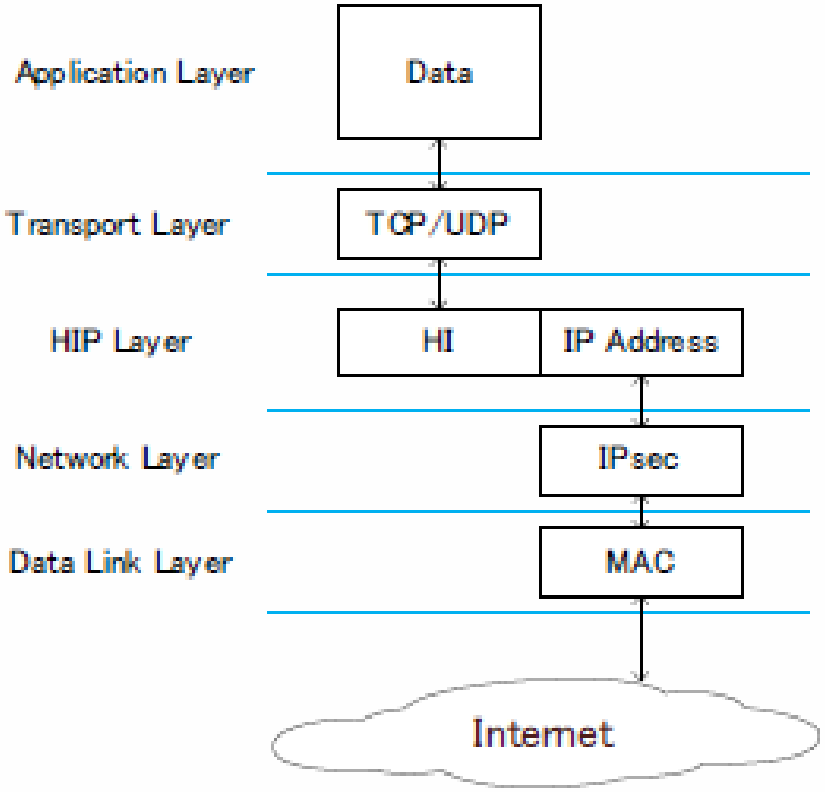
HIP(Host Identity Protocol)

- IPアドレスがもつ端末識別子と位置識別子の役割のうち、端末識別子を分離し、端末識別子としてHIを導入する
- IP層とTCP/UDP層との間に新たにHIP層を定義するHIP層ではIPアドレスとHIのマッピングを管理し、上位層ではHIを用いて通信を識別する



HIP(Host Identity Protocol)

- HIはエンド端末の公開鍵から生成するため、エンドツーエンドのセキュリティが確実で強固あるという特徴がある
- 移動によってIPアドレスが変化してもHIは変化せず移動透過性を実現できる
- NAT越えにはICEを利用する



NTMobileの構成

- DC(Direction Coordinator)
  - NTM端末の実IPアドレスや仮装IPアドレスの関係を管理し、UDP トンネルの構築支持を出す
- AS(Account Server)
  - ユーザの登録と認証を行う
  - NTM端末の認証やDCとNTM端末間等における通信の暗号化に用いる鍵の配布を行う
- RS(Relay Server)
  - NTM端末間で直接通信できない場合にカプセル化パケットを中継する
- NTM端末
  - NTMobileを搭載した端末

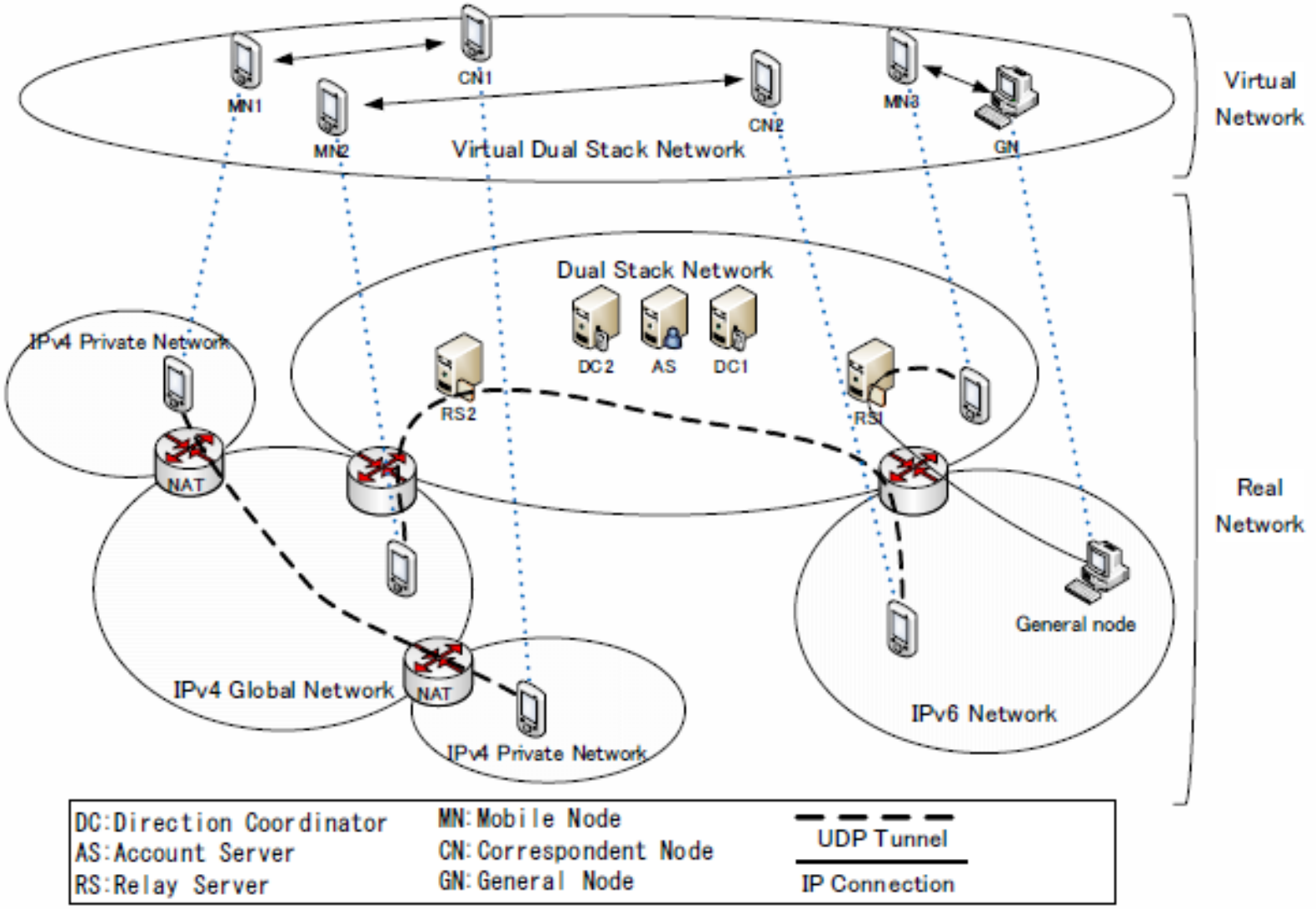
NTMobileの動作手順

- (1)MNがCNに経路指示を要求
- (2)DCが経路を決定し、Ktmp, Ktunを生成
- (3)RSに要求がくることを伝え、Ktunを送信
- (4)CNに経路指示をし、Ktmp, Ktunを送信
- (5)MNに経路指示をし、Ktmp, Ktunを送信
- (6)MNはKendを生成し、Ktmpで暗号化
- (7)MNはKtunで暗号化したトンネル要求とKtmp(Kend)をRSに送信

NTMobileの動作手順

- (8)RSはこれをMAC認証してCNに送信
- (9)CNはKtunでMAC認証後、Ktmpで複合することによってKendを取得
- (10)CNはトンネル応答をKendで暗号化してMN送信
- (11)MNはトンネル応答をMAC認証することで共通鍵を共有できたことを確認
- (12)これ以降MN, CN間は共通鍵Kendを用いて安全に通信することができる

NTMobile


CN1
MN1
MN2
CN2
MN3
GN
Virtual Dual Stack Network
Virtual Network
Dual Stack Network
DC2
AS
DC1
RS2
RS1
IPv4 Private Network
NAT
IPv4 Global Network
NAT
IPv4 Private Network
General node
IPv6 Network
Real Network
DC:Direction Coordinator
AS:Account Server
RS:Relay Server
MN:Mobile Node
CN:Correspondent Node
GN:General Node
UDP Tunnel
IP Connection

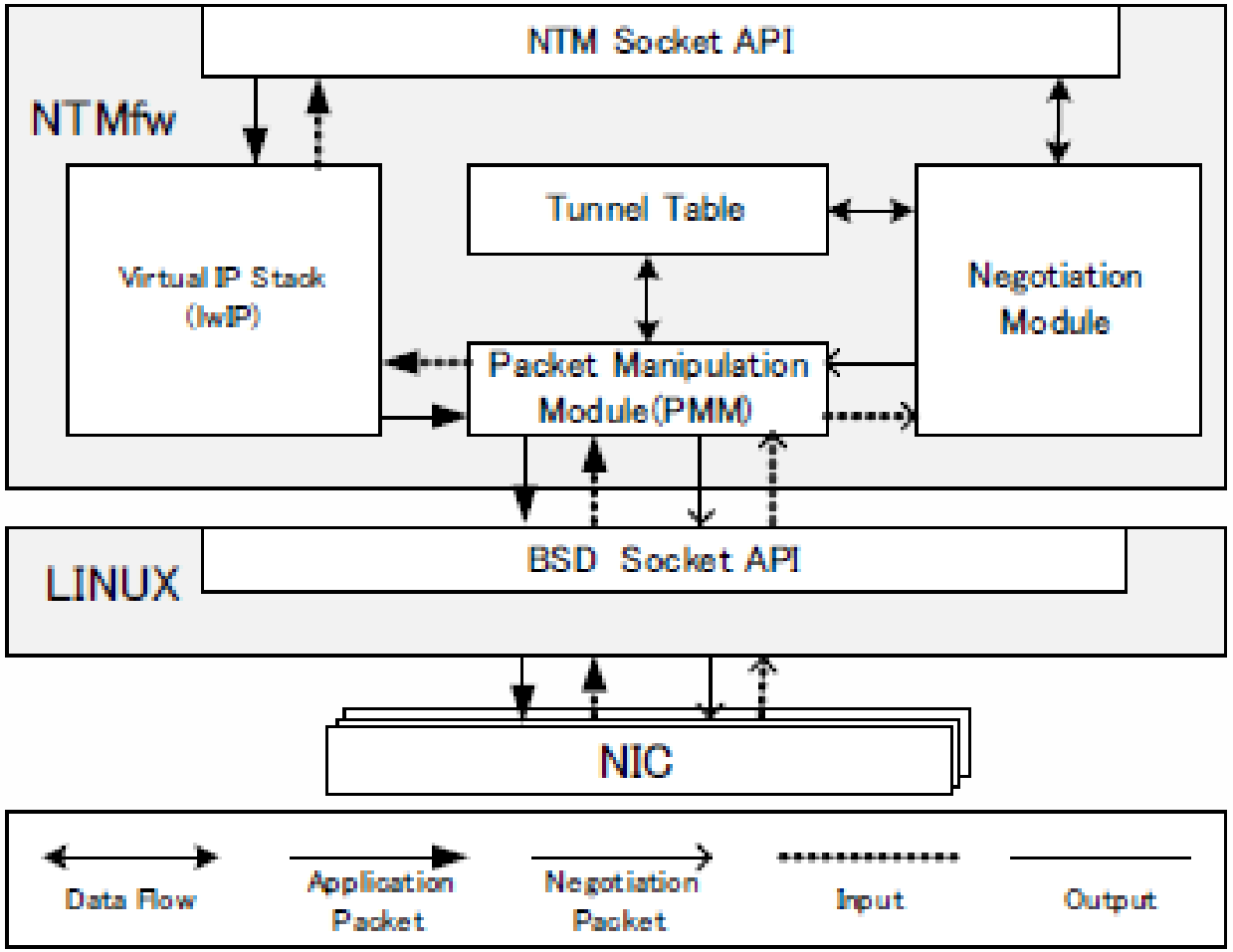
NTMobile framework library

- NTMfwは一般のアプリケーションがカーネルの通信ライブラリを利用するのと同じ容量でNTMfwを呼び出すことにより利用できる
- NTMobileのシグナリング処理はNTMfwが実行するためアプリケーションはこれを意識しない
- DCとNTM端末によるシグナリング処理によりトンネル経路が生成されるとその後の通信すべてUDPカプセル化通信となる
- パケットはトンネル経路を経由して相手に届けられる
- DSとの間でシグナリング処理を行う
  IPアドレスが変化したときには再度シグナリング処理を行う

NTMobile framework library

- NTMソケットAPI
  - BSDソケットAPIに代わってアプリケーションを提供するソケットAPI
- ネゴシエーションモジュール
  - NTMobileの初期化処理とシグナリング処理を行う
- パケット処理モジュール
  - 通信パケット、シグナリングパケットの生成、解析処理を行う
- 仮想IPプロトコルスタック
  - アプリケーション層にてTCP/IPプロトコルを実行
- トンネルテーブル
  - FQDN、仮想IPアドレス、実IPアドレス、共通鍵、識別子等を格納したテーブル

NTMobile framework library



既存技術との比較

	DSMIP	HIP	提案方式
NAT 越え	△	○	○
移動透過性	○	△	○
IPv4/IPv6 相互通信	○	○	○
カーネルの改造	×	×	○
既存アプリケーション	○	○	△

まとめ

- NTMfwによってエンドツーエンド通信をアプリケーションレベルで実現できる
- スループットの向上に向けた実践方式の検討が必要

参考文献

- 納堂博史, 鈴木秀和, 内藤克浩, 渡邊晃：
  エンドツーエンド通信をアプリケーションレベルで可能にする通信ライブラリの実現と評価,
  情報処理学会研究報告