NTMobileの実用化に向けた統合的枠組みの検討について

名城大学 理工学部 情報工学科
渡邊研究室 130441077 清水 一輝

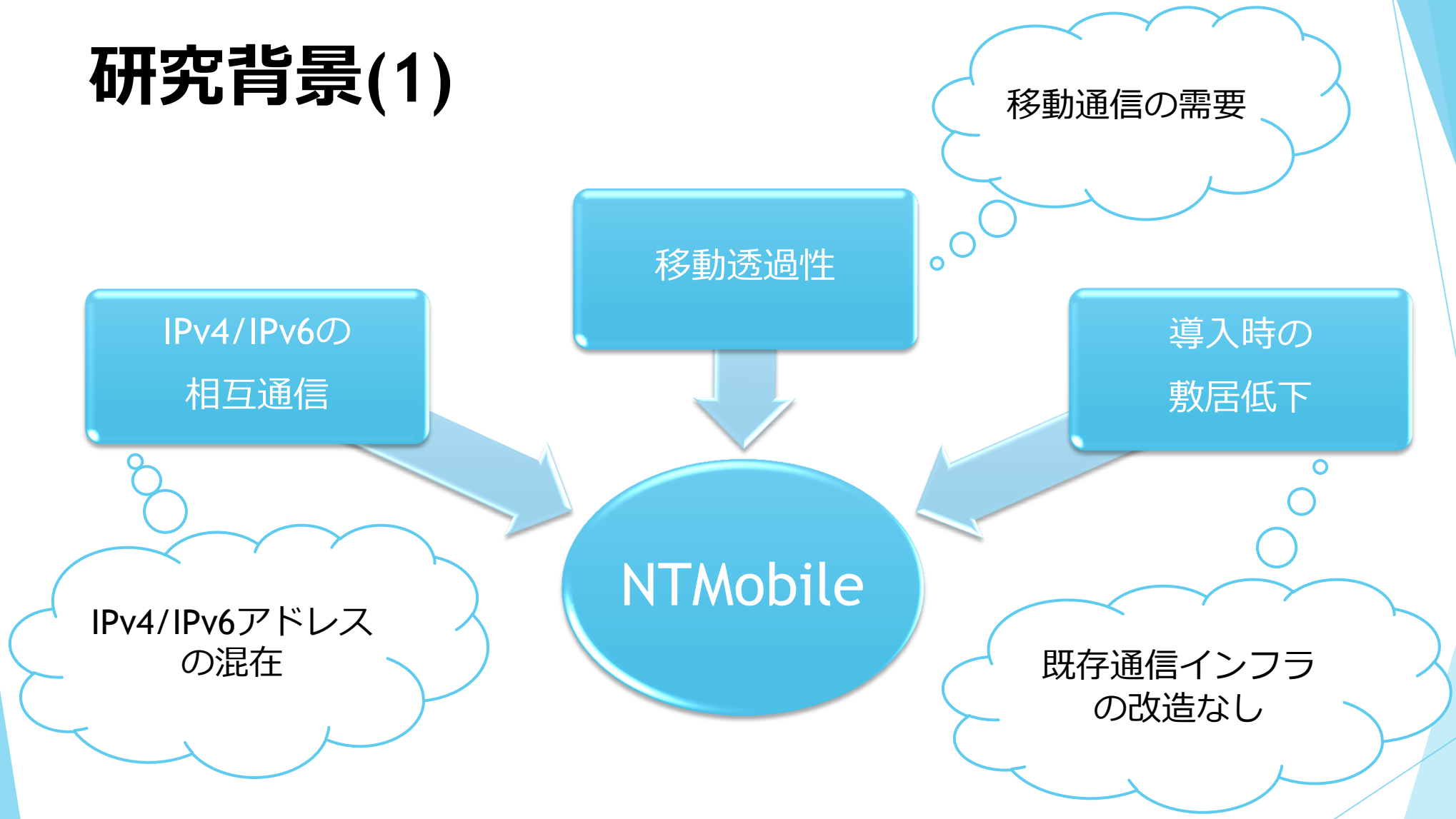
輪講原稿

- 『NTMobileの実用化に向けた統合的枠組みの検討』
  - 納堂 博史
  - 杉原 史上
  - 鈴木 秀和
  - 内藤 克浩
  - 渡邊 晃

目次

- 研究背景
- NTMobileについて
  - 概要
  - 実装方式
  - NAT越え方式
  - トンネル構築
- 新たな要求仕様
- 動作シーケンス
- まとめ

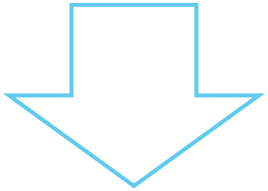
研究背景(1)



IPv4/IPv6混在環境において，既存のインフラで通信の持続性と移動透過性を実現

研究背景(2)

- 実用化に向けて新たな要求仕様の浮上
  - サーバー間の信頼関係
  - OpenIDへの対応
  - 公開鍵への対応
  - 動作シーケンスの統一
  - 実装方式によらない相互互換性



これらを全て満たす1つの統合的な枠組みを再設計

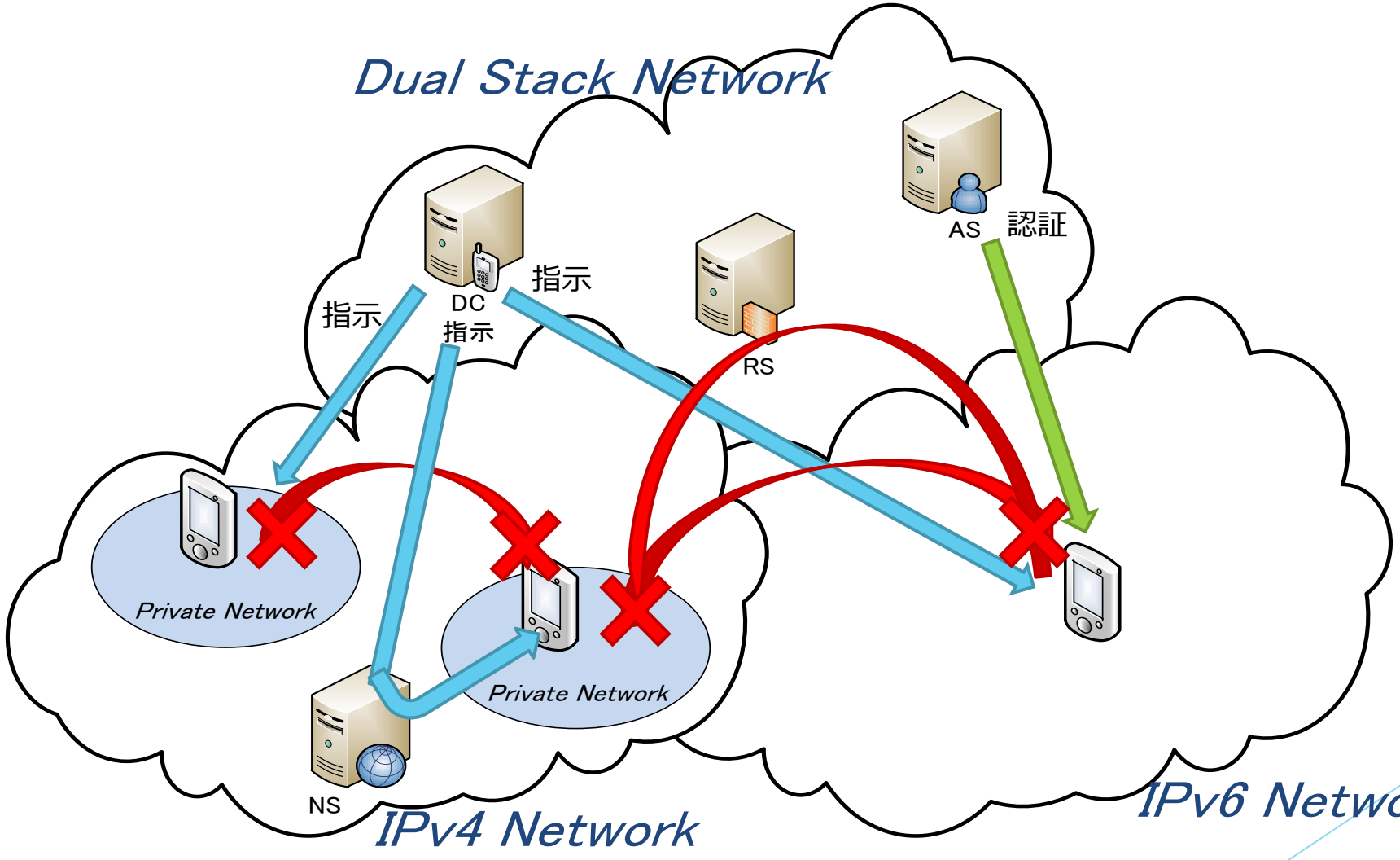
NTMobileの概要(1)

- DC(Direction Coordinator)
  - NTMobile端末の端末情報の管理
  - トンネル経路指示
- RS(Relay Server)
  - IPv4/IPv6間の通信，一般端末との通信，NTMobile端末が互いに異なるNAT配下にいる場合に通信を中継
- AS(Account Server)
  - NTMobile端末の認証
- NS(Notification Server)
  - NAT越えに関するオプション装置

NTMobileの概要(2)

- DC, RS, NSは複数台設置可能
  - 負荷の分散が可能
- ASはNTMobileにおいて1台のみ存在
  - 一定時間内の再認証はDCで可能
    - 大きな負荷がかからない
- NTMobile端末のアプリケーションは仮想IPアドレスで通信
  - 実際の通信は実IPアドレスを用い, UDPでカプセル化される

NTMobileの概要(3)



DC:Direction Coordinator　RS:Relay Server　NS:Notification Server　AS:Account Server

NTMobileの実装方式

- Linuxカーネル実装型
  - LinuxOS対象
  - 高速
  - アプリケーションの改造不要
- フレームワーク組込型
  - Unix対象
  - アプリケーションの改造不要
- VPNサービス利用型
  - Android対象
  - アプリケーションの改造不要

NTMobileのNAT越え方式

- UDPキープアライブ
  - PC対象
  - 20秒間隔
- TCPキープアライブ
  - LinuxBox対象
  - 1時間間隔
- プッシュ通知サービス
  - スマートフォン対象
  - GCM/APNSを利用
  - キープアライブが不要

GCM:Google Cloud Messaging
APNS:Apple Push Notification Service

NTMobileのトンネル構築

- 一方の端末がNAT配下
  - NAT配下端末からトンネル構築要求パケットを送信
- 両方の端末がNAT配下またはIPv4-IPv6間
  - 両方の端末からRSにトンネル構築要求パケット送信
  - 両端末宛にトンネル構築応答を返送

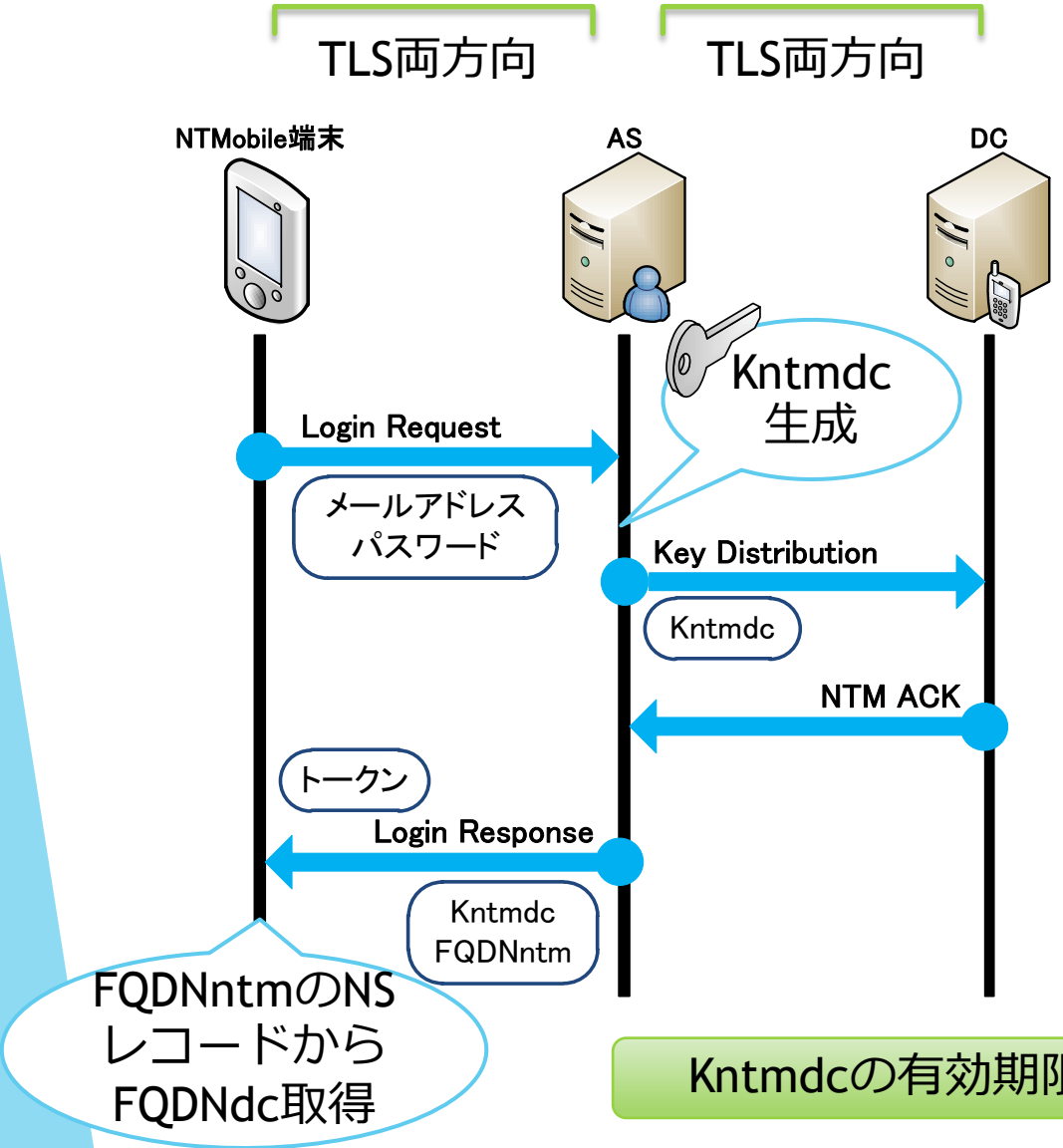
新たな要求仕様(1)

- サーバー間の信頼関係
  - NTMobile端末を除く装置群に公開鍵証明書を持たせる
    - 初回通信時に，相互認証により共通鍵を共有し，以降の通信ではこの共通鍵を利用することで装置間の信頼を実現
- OpenIDへの対応
  - NTMobile端末の認証をNTMobileから分離して対応
  - ASに個人情報を登録する必要がなくなりセキュリティ向上

新たな要求仕様(2)

- 公開鍵への対応
  - NTMobile端末が公開鍵を持たせる場合，持たせない場合でシーケンスを統合
  - アプリケーションパケットの暗号化に用いる共有鍵の共有を公開鍵でも実現
- 動作シーケンスの統一
  - NAT越え手法の違いによる部分を除き統一
  - NTMobile端末の動作仕様をRSの利用の有無に関係なく統一
- 実装方式によらない相互互換性
  - 実装方式に依存しない部分をNTMobile Libraryとして、切り離して実装
    - 全ての実装方式において相互互換性が保たれる設計

動作シーケンス(NTMobile端末の認証)



ASへログイン要求

TLS両方向通信

NTMobile端末とDC間の鍵を生成

メールアドレス, パスワード認証

DCへ鍵を送信

NTMobile端末とDC間の通信で利用

確認応答

NTMobile端末へログイン応答

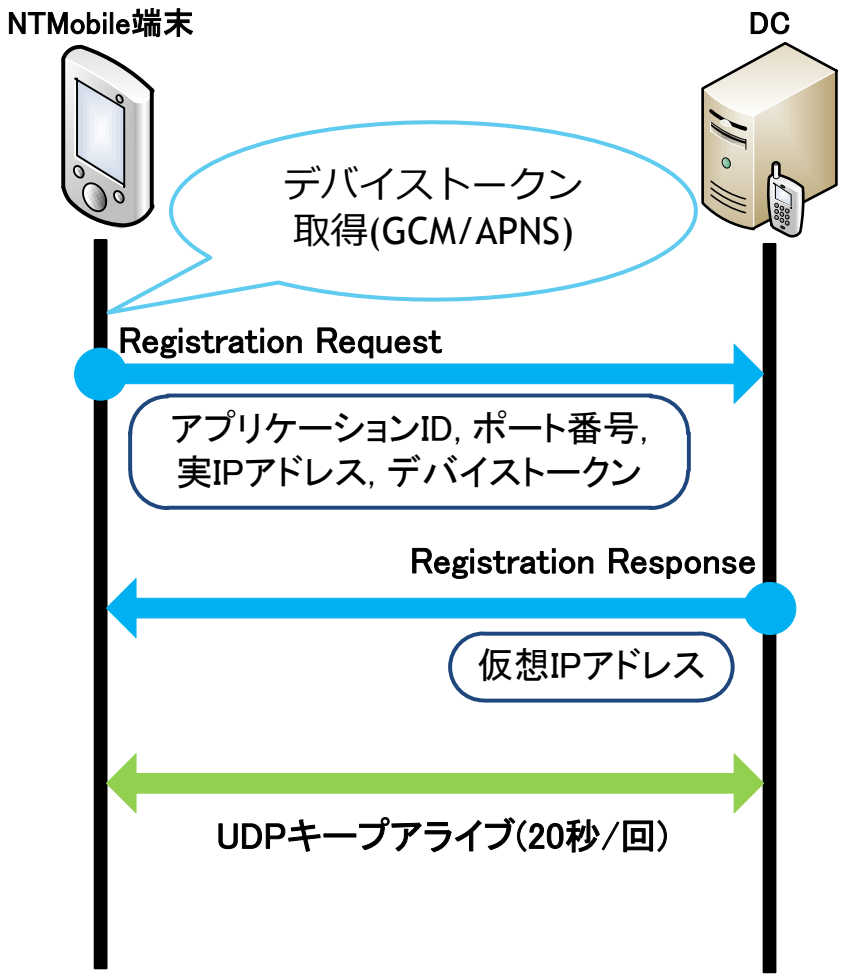
FQDNntmとKntmdcを通知

DCのFQDNを取得

FQDNntmのNSレコードから取得

Kntmdcの有効期限までは再認証が不要

動作シーケンス(ネットワーク情報登録)



情報登録の要求

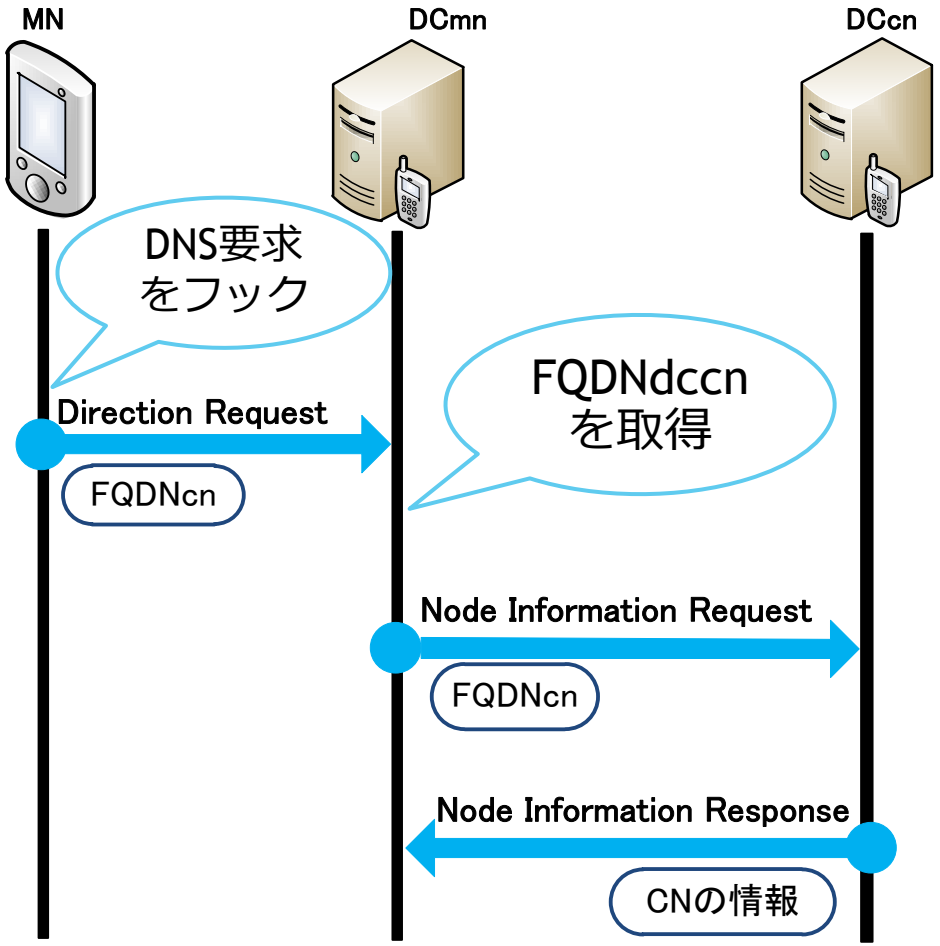
アプリケーションID, ポート番号,
実IPアドレス, NATのIPアドレス

情報登録の応答

仮想IPアドレスを通知

端末起動時と移動時に実行

動作シーケンス(名前解決)



FQDNcnの名前解決をフック

DNS要求をフック

DCmnへ経路指示を要求

トンネル構築の指示要求

FQDNcnからFQDNdccnを取得

FQDNcnのNSレコードを探索

DCcnへCNの端末情報を要求

CNの情報を要求

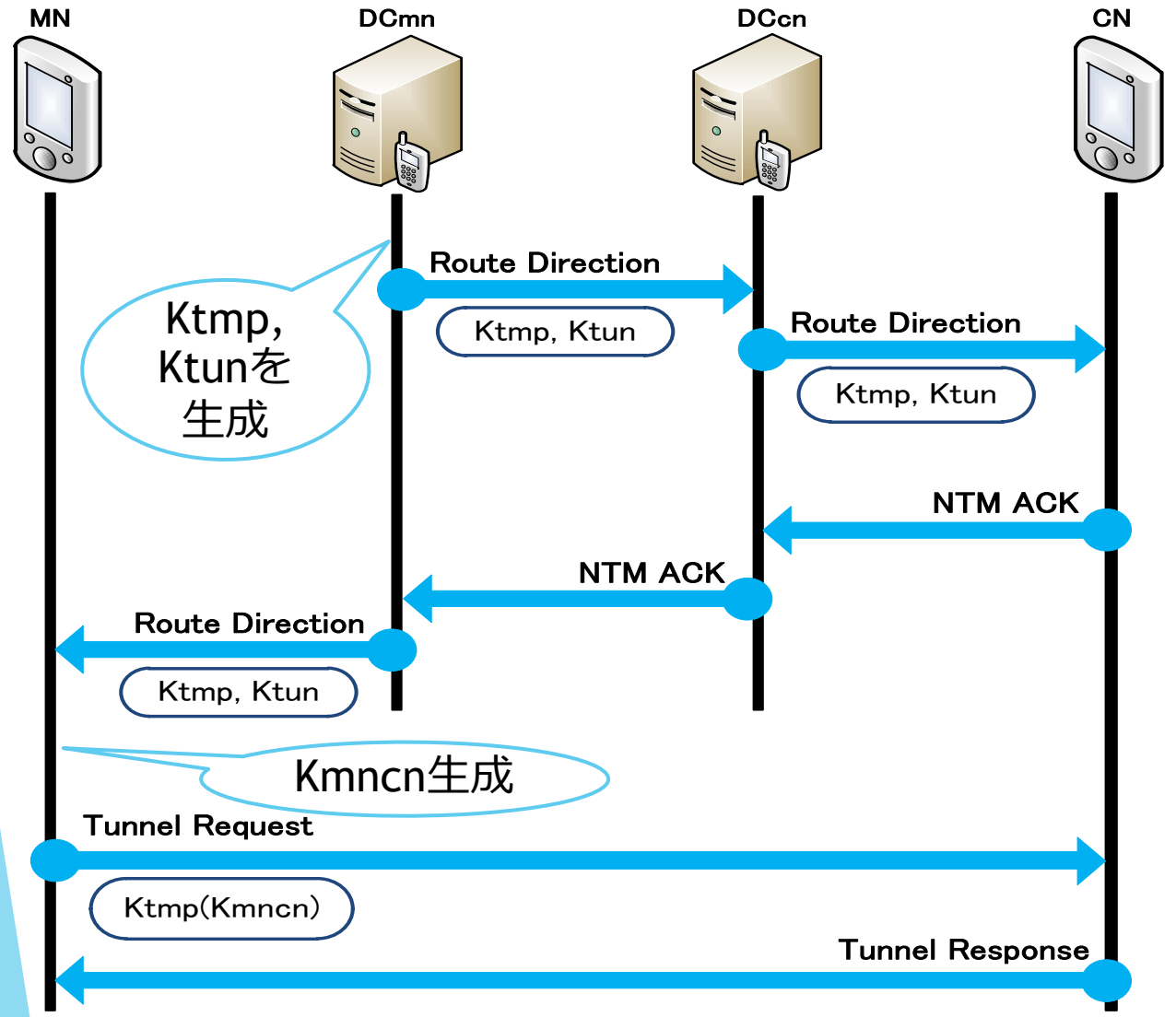
DCmnへCNの端末情報を応答

CNの仮想IPアドレス等を応答

MNとCNの情報を取得したので
トンネル構築指示へ

MN:Mobile Node　　CN:Correspondent Node

動作シーケンス
(通信経路生成-CNがNAT配下-)



経路生成用の共通鍵を生成

トンネル構築を要求

CNへ経路を指示

DCcnを経由

確認応答

DCcnを経由
CNの公開鍵を格納

MNへ経路を指示

通信用の共通鍵を生成

KmncnはKtmpで暗号化

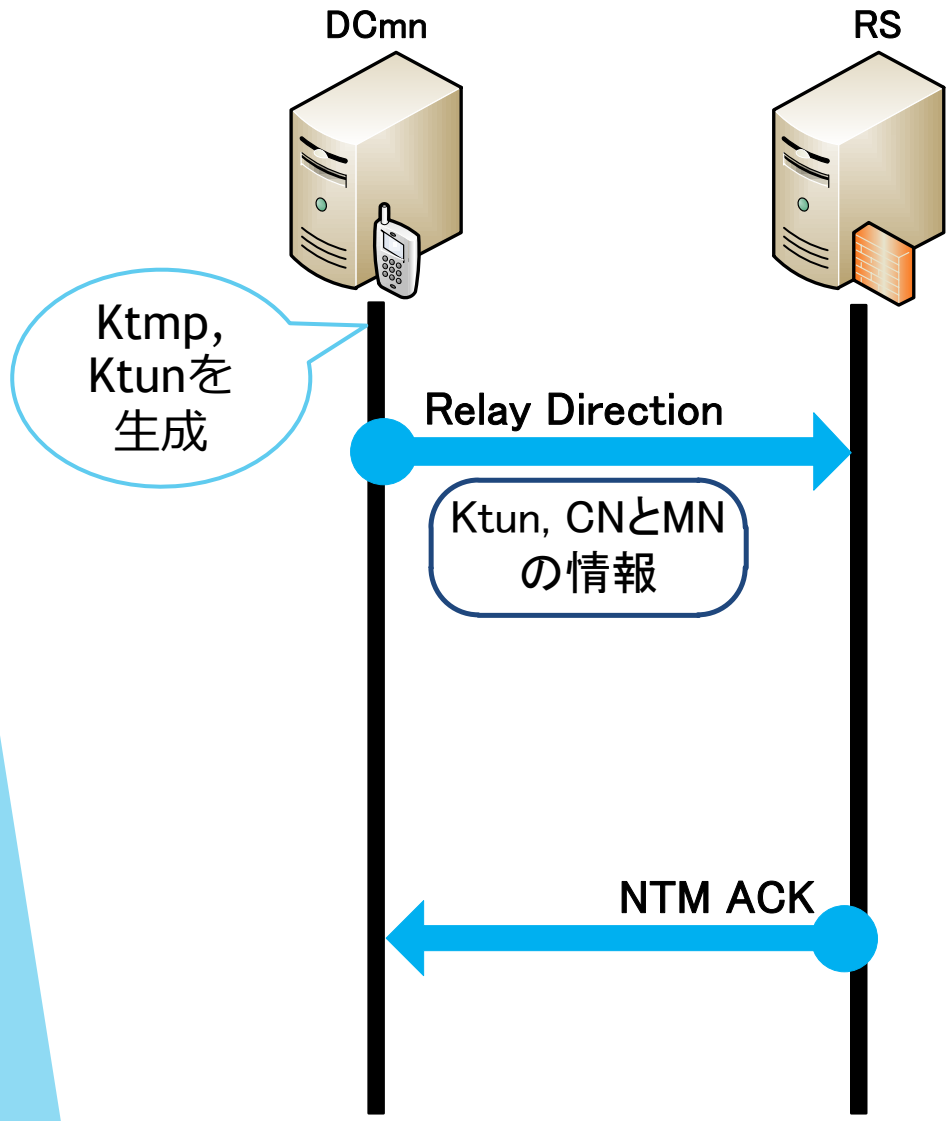
トンネルを要求

メッセージはKtunで暗号化

トンネル応答

Kmncnで暗号化(鍵の共有確認)

動作シーケンス
(通信経路生成-MNとCNがNAT配下①-)



経路生成用の共通鍵を生成

Ktun:Tunnel Request暗号化用

Ktmp:Kmncnの暗号化用

RSへ中継指示

Ktunのみを送信

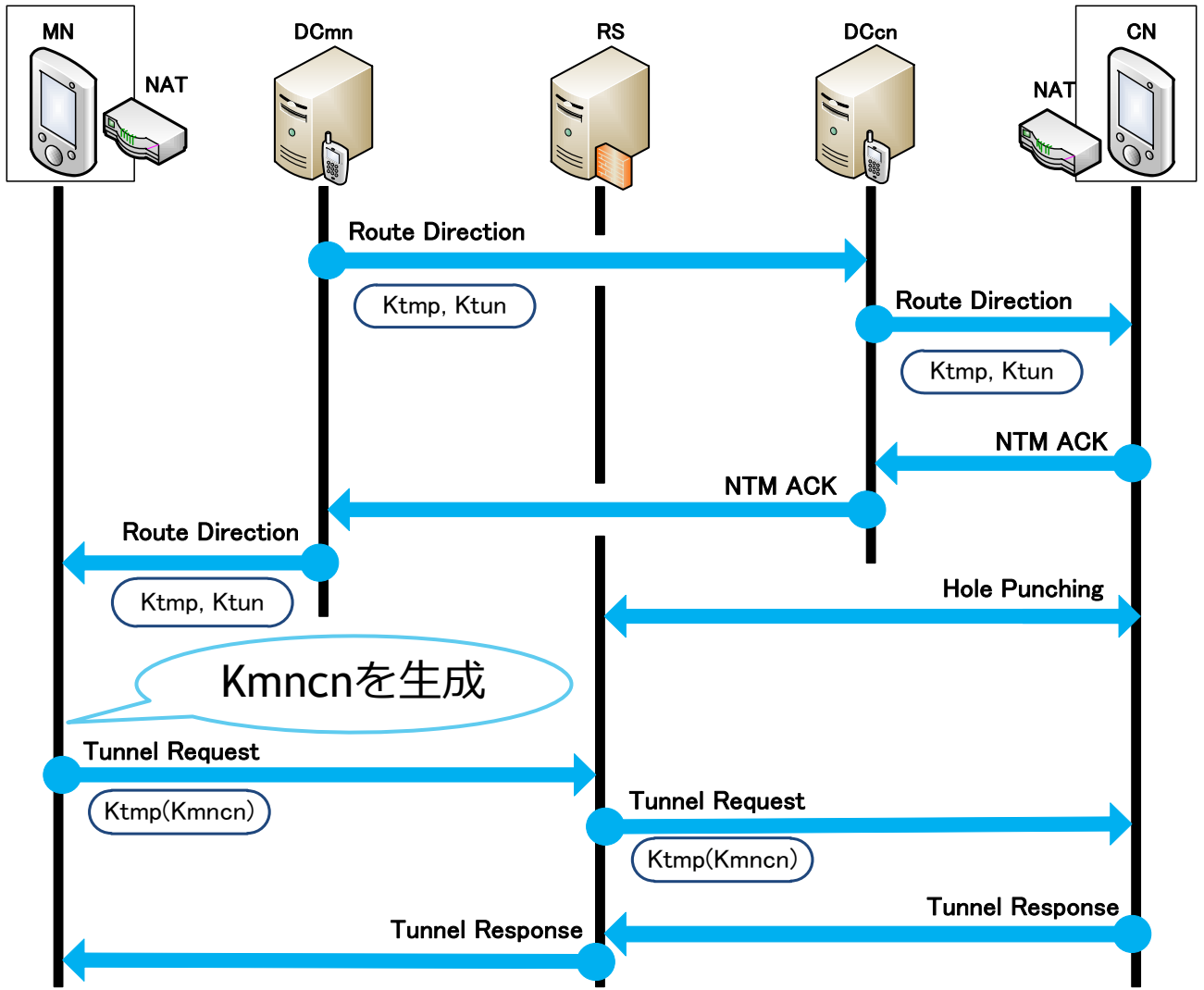
Ktmpは送信しない

Tunnel Request格納のKmncnを
複合できない

確認応答

中継指示が完了後, 経路生成指示へ

動作シーケンス
(通信経路生成-MNとCNがNAT配下②-)



CNへ経路を指示

Ktmp，Ktunを配送

確認応答

CNの公開鍵を配送

MNへ経路を指示

Ktmp，Ktunを配送

UDPホールパンチング

RSからの通信経路を確保

通信用の共通鍵を生成

KmncnをKtmpで暗号化

トンネルを要求

メッセージをKtunで暗号化

トンネル応答

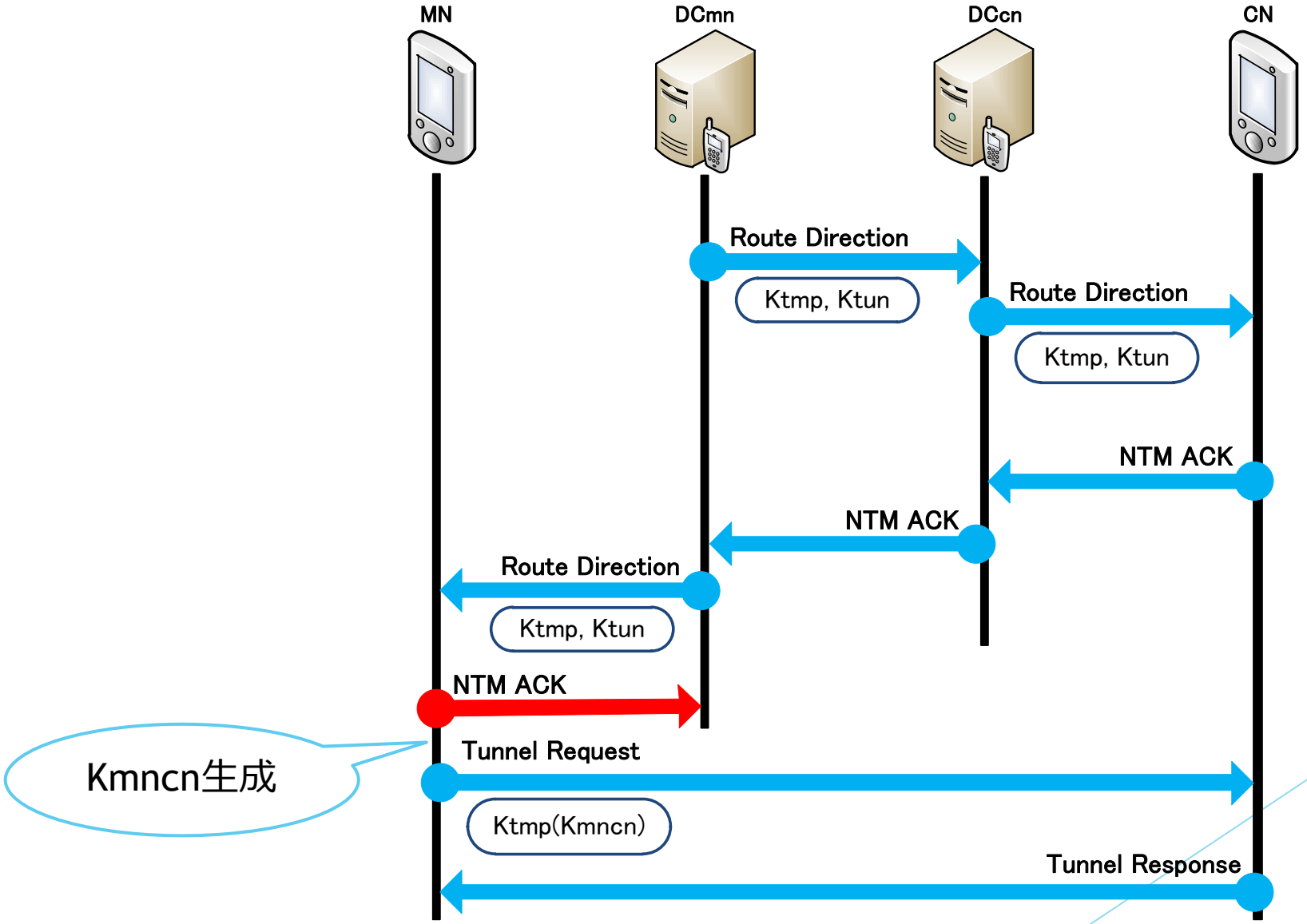
Kmncnで暗号化

まとめ

- NTMobileの実装・動作方式に依存しない枠組みを設計
  - OpenIDへの対応に対する拡張
  - 公開鍵への対応に対する拡張
  - 動作シーケンスの統一
- 今後の予定
  - 32bit/64bitの両OSへの対応
  - OSのクロスプラットフォーム化

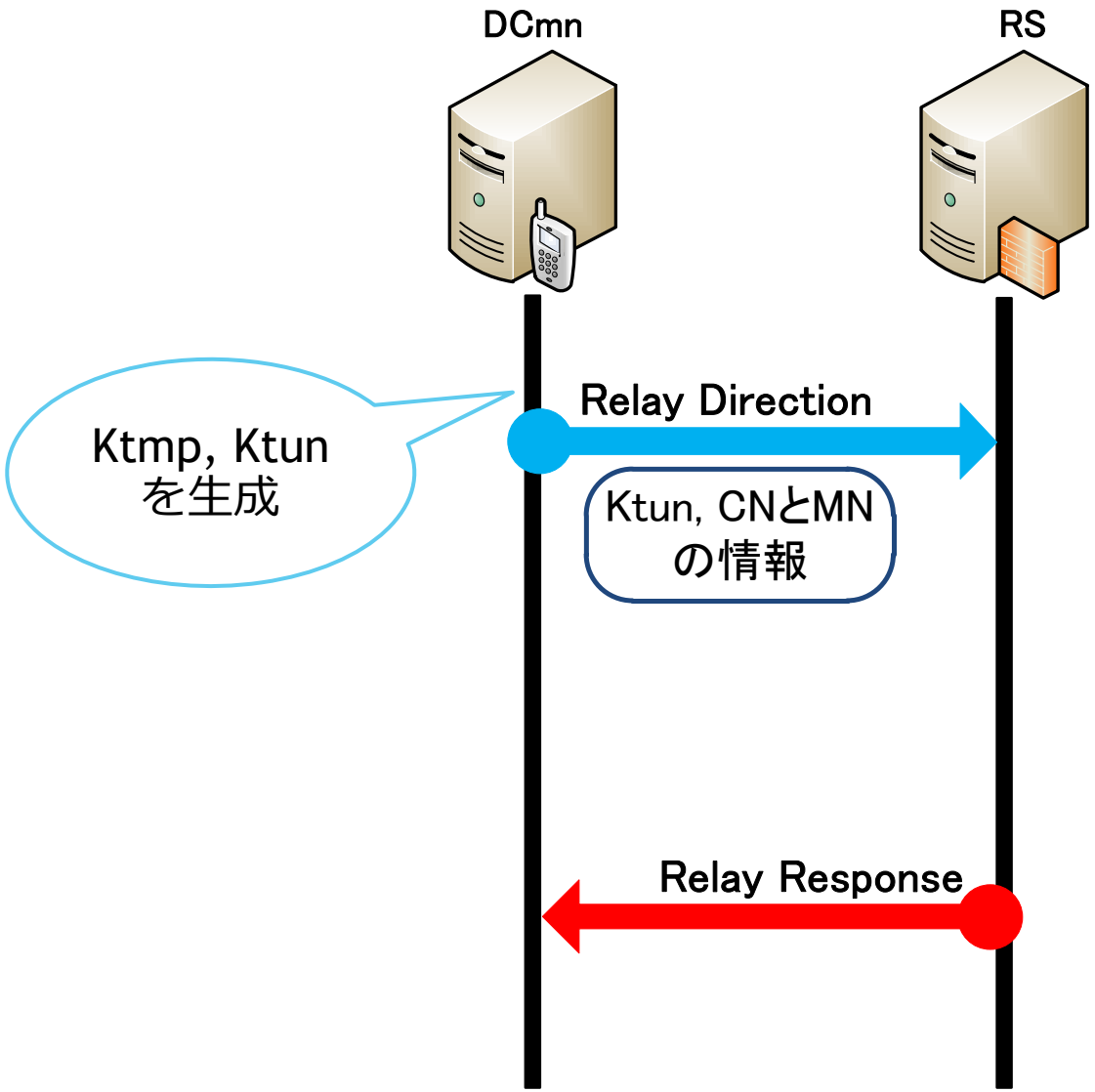
補足資料

従来の通信経路生成-CNがNat配下-



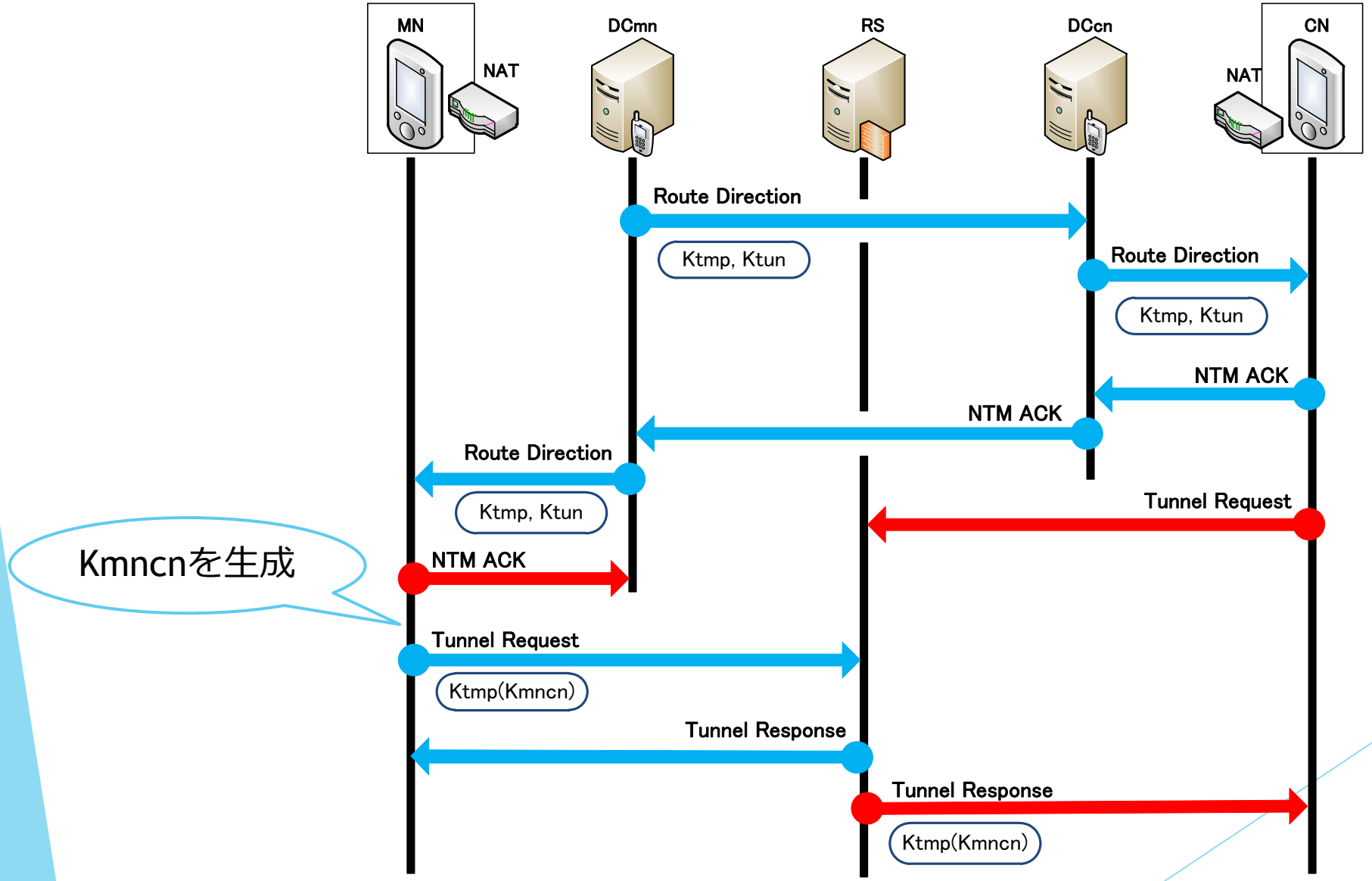
補足資料

従来の通信経路生成-MNとCNがNAT配下①-



補足資料

従来の通信経路生成-MNとCNがNAT配下②-



補足資料
共通鍵について

	共通鍵の名前	生成装置	配送先	
①	Kntmdc	AS	NTMobile端末, DC	NTMobile端末とDC間の通信を暗号化
	Kdcns	DC	DC, NS	DCとNSの間の通信を暗号化
	Kntmns	DC	NTMobile端末, NS	NTMobile端末とNSの間の通信を暗号化
	Kdcdc	DCmn	DCmn, DCcn	DC間での通信を暗号化
	Kdcrs	DCmn	DCmn, RS	DCとRSの間の通信を暗号化
②	Ktun	DCmn	MN, CN, RS	Tunnel Requestを暗号化 RS宛てのHole Punching/ACKを暗号化
	Ktmp	DCmn	MN, CN	Kmncnを暗号化
	Kmncn	MN, CN	MN, CN	MNとCNの間の通信を暗号化

①は共通鍵を共有後は共通鍵の有効期限まで，再共有は不要
②は通信する毎に生成する必要あり