エンドツーエンド通信を実現するNTMobileのセキュリティ対策

鴨下　友馬[†*]，鈴木　秀和[†]，内藤　克浩[‡]，渡邊　晃[†]
([†]名城大学，[‡]愛知工業大学)

Security Measures of NTMobile that Achieves End-to-end Communication

Yuma Kamoshita[†], Hidekazu Suzuki[†], Katsuhiro Naito[‡], Akira Watanabe[†]
([†]Meijo University, [‡]Aichi Institute of Technology University)

1　はじめに

モバイルネットワークの普及に伴い，通信中にネットワークが切り替わっても通信を継続できる移動透過性や，ネットワーク環境に関わらず通信を開始することができる通信接続性が求められている．NTMobile（Network Traversal with Mobility）は，その両者を同時に実現できる次世代の技術である [1] [2].

NTMobile では端末同士が暗号鍵を共有することにより，安全にエンドツーエンド通信を行うことができる．この暗号鍵は，ネットワーク管理者にもわからないという特徴がある．本稿では，NTMobile のセキュリティがどのように確保されているかを示す．

2　NTMobile の概要

NTMobile は，NTMobile を実装した NTM 端末，NTM 端末のアカウント情報を管理する AS（Account Server），NTM 端末の仮想アドレスなどの管理や通信経路の指示を行う DC（Direction Coordinator），NTM 端末間で直接経路を生成できない場合にパケットを中継する RS（Relay Server）により構成される．NTM 端末は，起動時に AS にログインし，DC から仮想アドレスを取得する．NTM 端末のアプリケーションは仮想アドレスでセッションを確立し，実際の通信はすべて実アドレスによりカプセル化する．

3　セキュリティ対策の実現方式

イニシエータ側の NTM 端末を MN（Mobile Node），レスポンダ側の NTM 端末を CN（Correspondent Node）とする．また，AS，DC，RS はグローバル空間に設置され，それぞれディジタル証明書を保持している．AS・DC 間，DC・RS 間は事前にディジタル証明書を用いて互いに認証し，共通鍵を保持している．さらに，NTM 端末は AS で事前にアカウントを取得しており，パスワードを正しく登録済みであるものとする．

MN は，まず AS に対してログイン処理を行う．AS は MN を認証すると，MN・DC 間の暗号鍵 K_{mndc} を生成し，DC と MN に送信する．以降の MN・DC 間の通信は，この鍵を用いて暗号化する．その後，MN は登録要求／応答（Registration Request/Response）により，DC から仮想アドレス VIP_{mn} を取得する．CN 側でも同様の処理を行い，K_{cndc} を共有し，VIP_{cn} を取得する．

以下では，RS を経由せずに通信が可能な場合と，経由する必要がある場合に分けて説明する．

<3・1>RS を経由しない場合　MN は DC に対して経路指示要求（Direction Request）を送信する．DC が CN までの通信経路を決定すると，一時鍵 K_{tmp} とトンネル鍵 K_{tun} を生成する．K_{tmp} は，エンドツーエンド暗号鍵 K_{mncn} を暗号化するために用いるものであり，K_{tun} はトンネル構築要求（Tunnel Request）パケットの暗号化のために用いられる．DC は経路指示（Route Direction）を CN と MN の両端末に送信し，生成した K_{tmp} と K_{tun} を配布する．

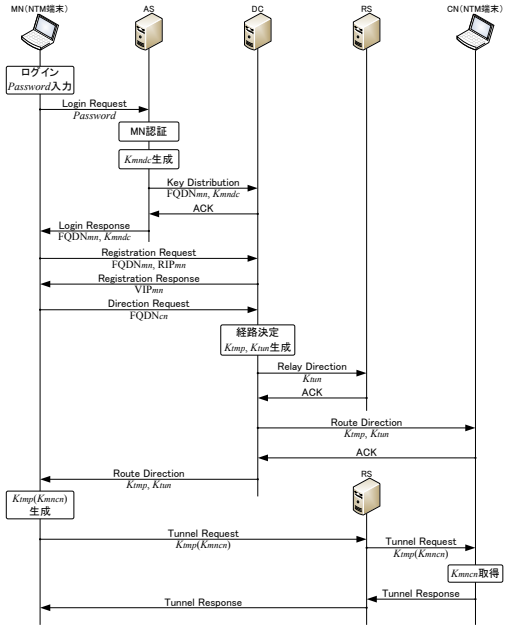


Fig. 1　Sequence of Route Generation via RS

その後，MN は K_{mncn} を生成して K_{tmp} で暗号化する．この K_{tmp} (K_{mncn}) を，Tunnel Request により CN に送信する．Tunnel Request 自体は K_{tun} により暗号化する．CN は K_{mncn} を取得し，トンネル構築応答（Tunnel Response）を送信する．Tunnel Response 自体を K_{mncn} により暗号化することで，MN は K_{mncn} の共有が完了したことを確認する．以降の MN・CN 間の通信は，K_{mncn} を用いて暗号化する．

<3・2>RS を経由する場合　Fig. 1 に，RS を経由した通信を行う場合の経路生成方法を示す．MN と CN が直接経路を生成できない場合は，RS を経由した経路を生成する．DC は K_{tmp} と K_{tun} を生成した後，RS に対して中継指示（Relay Direction）を行う．このとき，MN と CN に対しては K_{tmp} と K_{tun} を両方とも配布する一方，RS に対しては K_{tun} のみを配布する．RS は Tunnel Request を中継するが，K_{tmp} を所持していないため，K_{mncn} を取得することはできない．

4　まとめ

NTMobile では端末間において安全に暗号鍵を共有できることを示した．今後は，各種攻撃への対策などについて検討を行っていく．

文　献

[1] 上酔尾，他：情報処理学会論文誌, Vol.54, No.10, pp.2288-2299, 2013.
[2] 納堂，他：第 82 回 MBL・第 53 回 UBI 合同研究発表会, No.46, pp.1–8, 2017.

エンドツーエンド通信を実現するNTMobileのセキュリティ対策

鴨下　友馬[†]，鈴木　秀和[†]，内藤　克浩[‡]，渡邊　晃[†]
[†]名城大学 理工学部 情報工学科
[‡]愛知工業大学 情報科学部 情報科学科

Watanabe Lab.

研究背景

- モバイルネットワークの普及
- 移動透過性の要求
  - ネットワークが切り替わると通信が継続できない
- 通信接続性の要求
  - ネットワーク環境に関係なく通信することができない
    - NATの外側から内側への通信開始ができない
      （NAT越え問題）
    - IPv4/IPv6の互換性がない

NTMobile(Network Traversal with Mobility)

NTMobileの概要

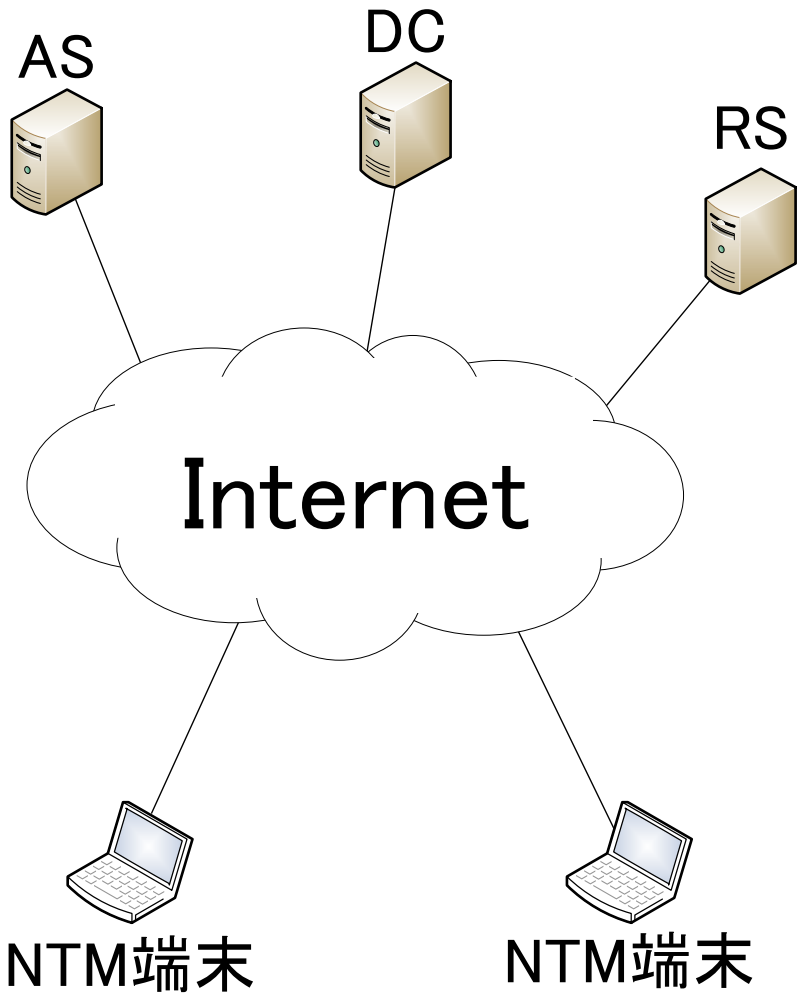
- 移動透過性と通信接続性を同時に実現する技術

- 移動透過性の実現
  - 実IPアドレスの変化に影響されない
    NTMobile独自の仮想IPアドレスを使用

- 通信接続性の実現
  - 通信経路を指示

NTMobileの構成

- NTM端末
  - NTMobileを実装した端末
- AS(Account Server)
  - NTM端末のアカウント情報の管理
- DC(Direction Coordinator)
  - NTM端末の仮想IPアドレスの管理
  - 通信経路の指示
- RS(Relay Server)
  - 端末間で直接経路を生成できない場合にパケットを中継

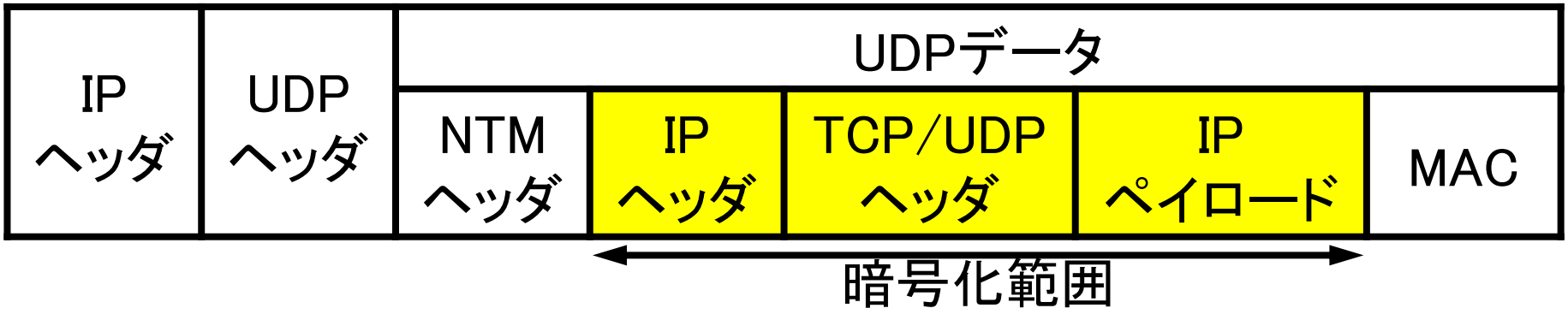


安全性の要求

- 実用化に向けてセキュリティ対策が重要
  - パケットの暗号化
  - 各装置の認証
  - エンドツーエンド暗号鍵の安全な共有

- 情報を漏洩させない
- エンドツーエンド暗号鍵はネットワーク管理者にもわからない

パケットフォーマット

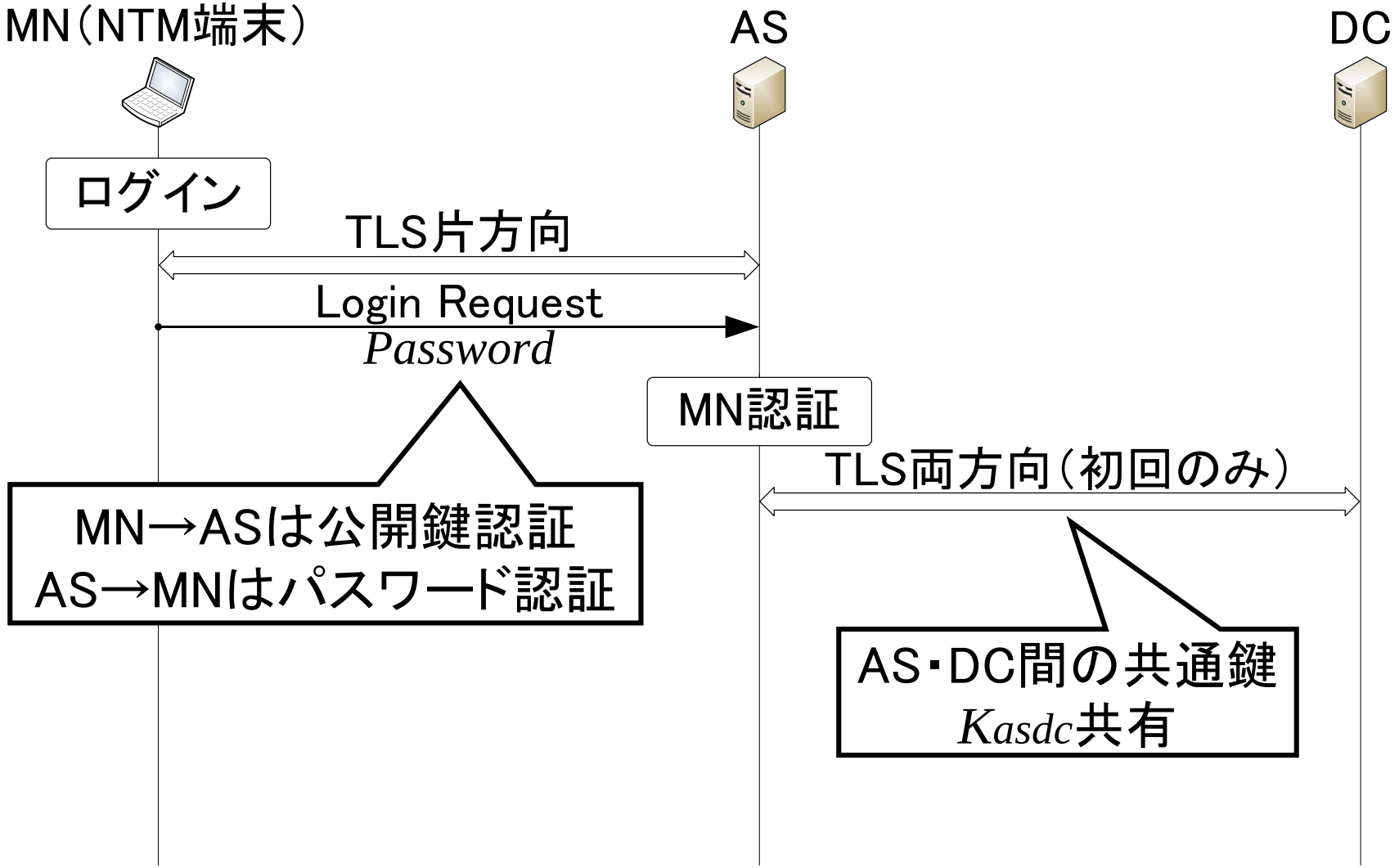


- IPヘッダ：NTM端末の実IPアドレス
- UDPヘッダ：ポート番号4330
- UDPデータ
  - NTMヘッダ：Path ID（通信識別子），シーケンス番号など
  - IPヘッダ：NTM端末の仮想IPアドレス
  - TCP/UDPヘッダ
  - IPペイロード：データ部
- MAC（Message Authentication Code）

各装置の認証方式

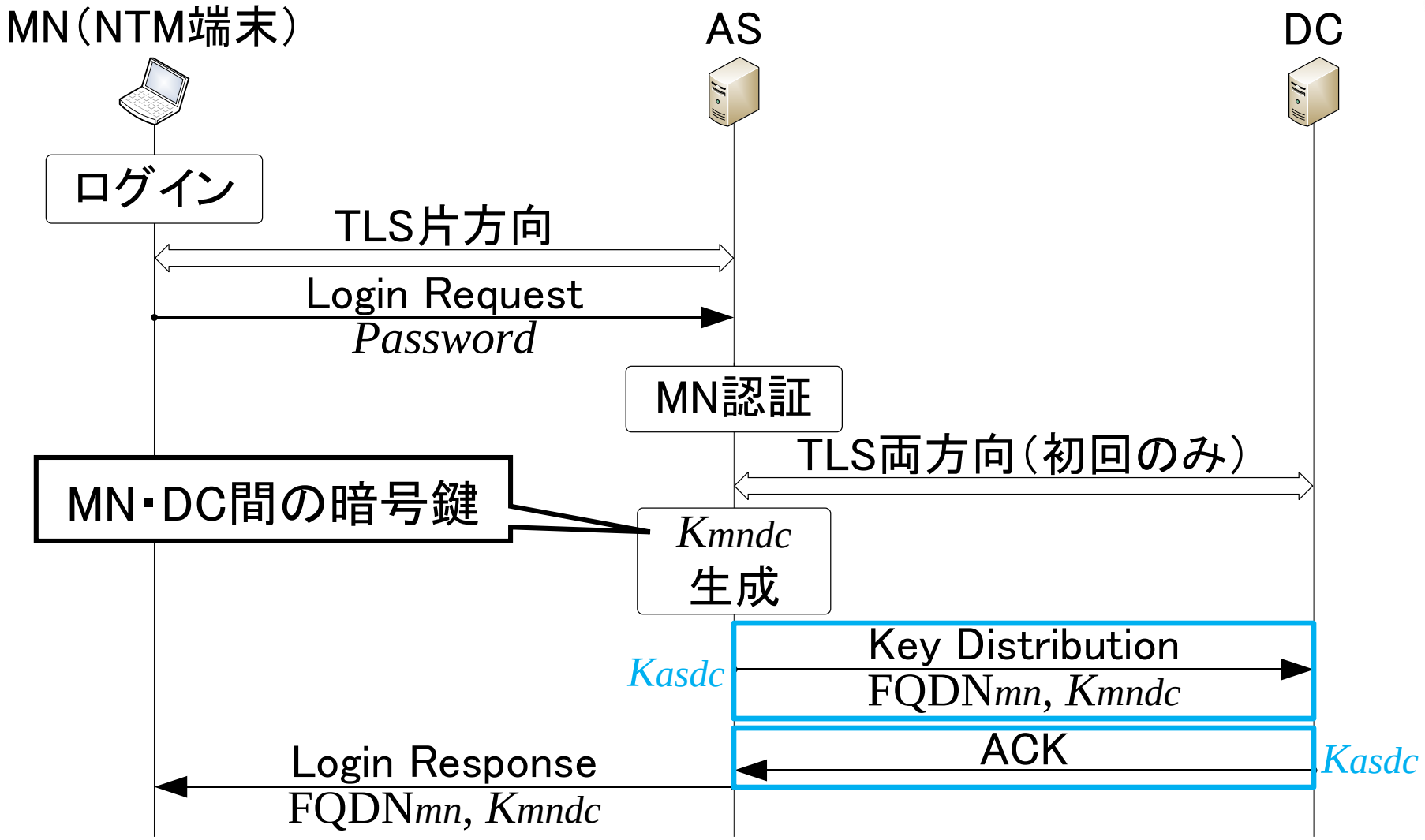
- AS・DC・RSの認証方式
  - 公開鍵認証方式
    - 公開鍵証明書による認証
    - 公開鍵・秘密鍵のペアが埋め込まれ，公開鍵証明書を保持している必要がある
- NTM端末の認証方式
  - パスワード認証方式
    - メールアドレスとパスワードによる認証
    - NTM端末のアカウント情報が，事前にASに正しく安全に登録されている必要がある
  - 公開鍵認証方式

ログイン処理(1/2)



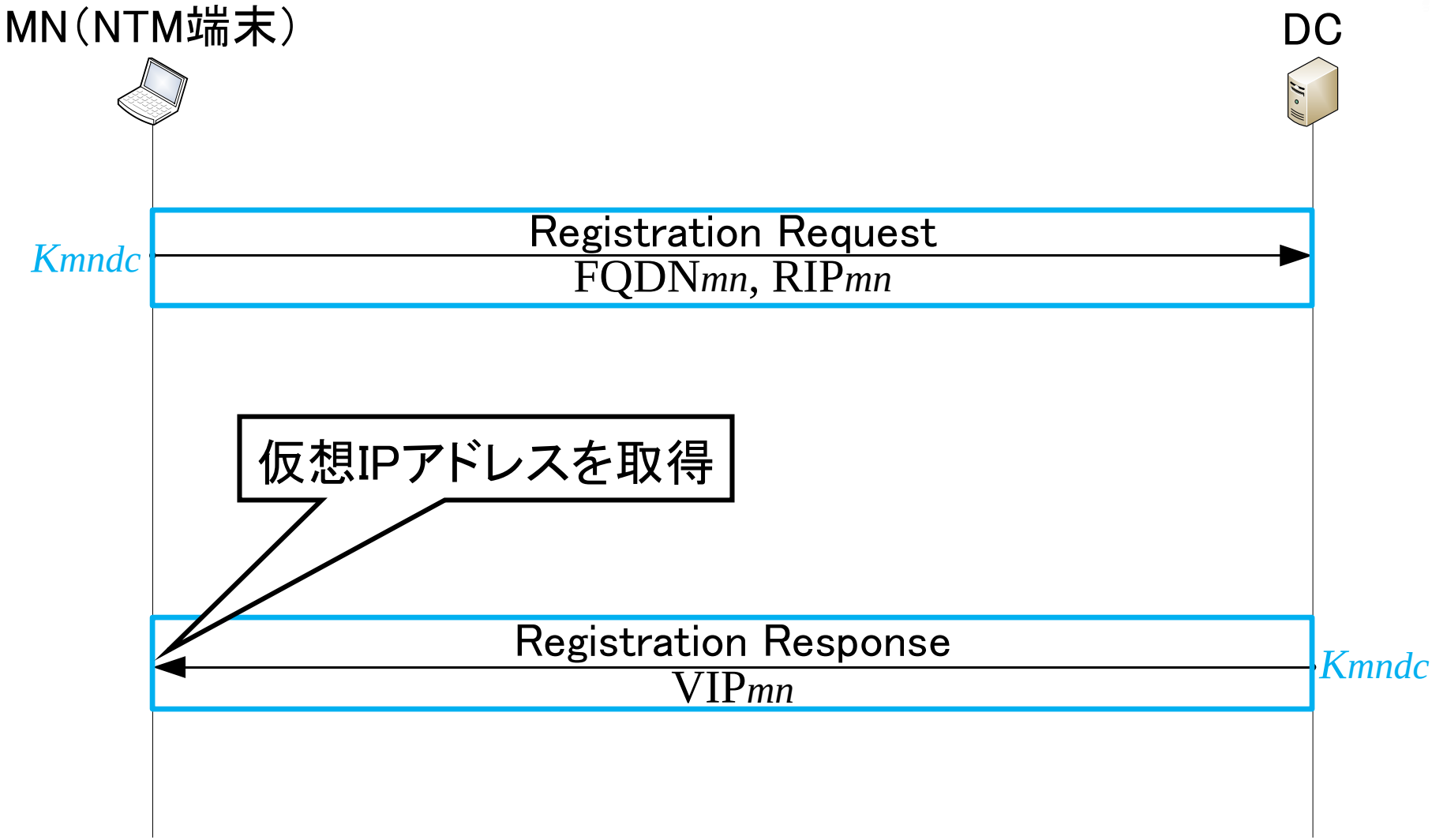
MN : Mobile Node　TLS : Transport Layer Security

ログイン処理(2/2)



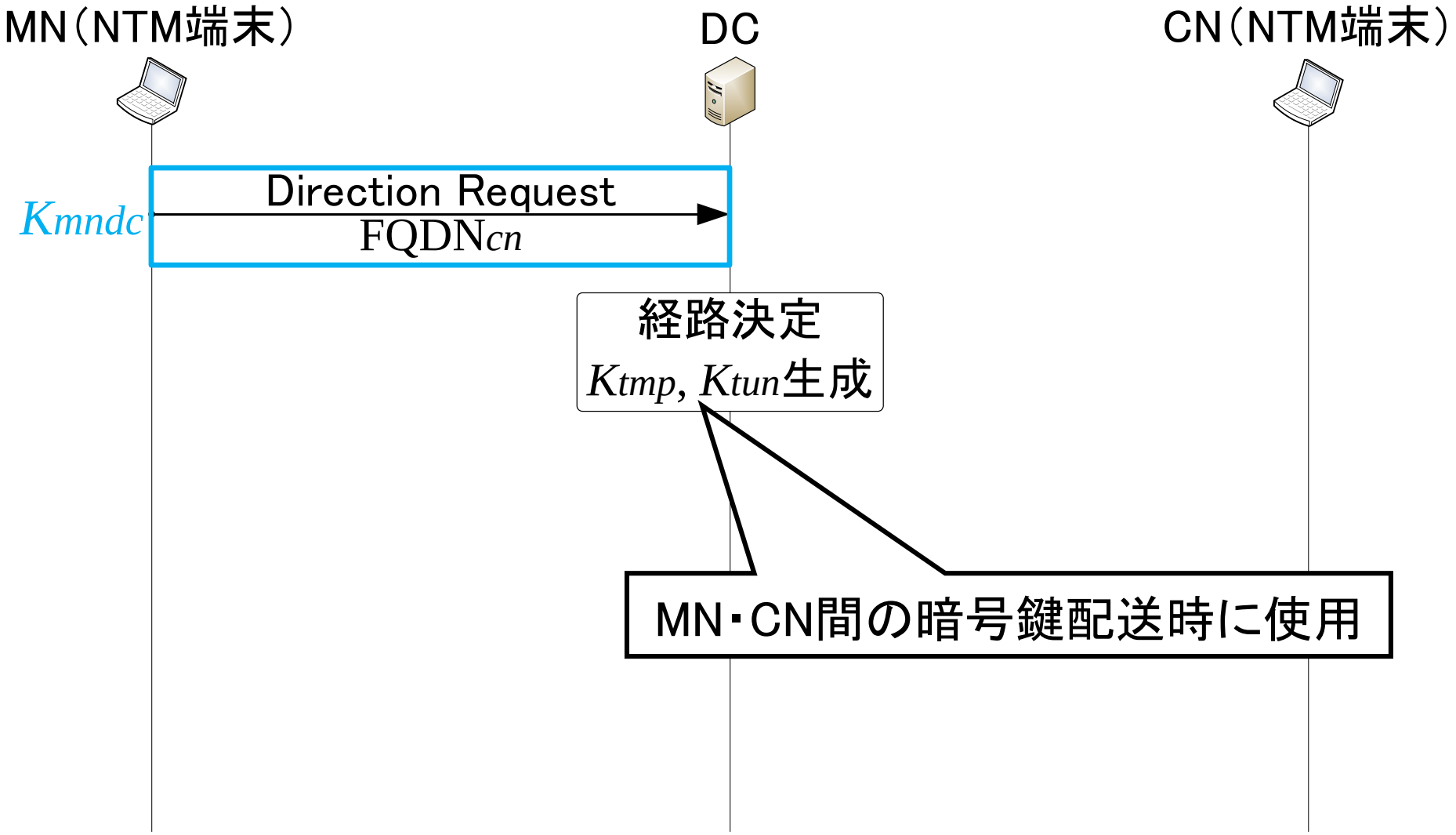
ACK : ACKnowledgement FQDN : Fully Qualified Domain Name

立ち上げ時の処理



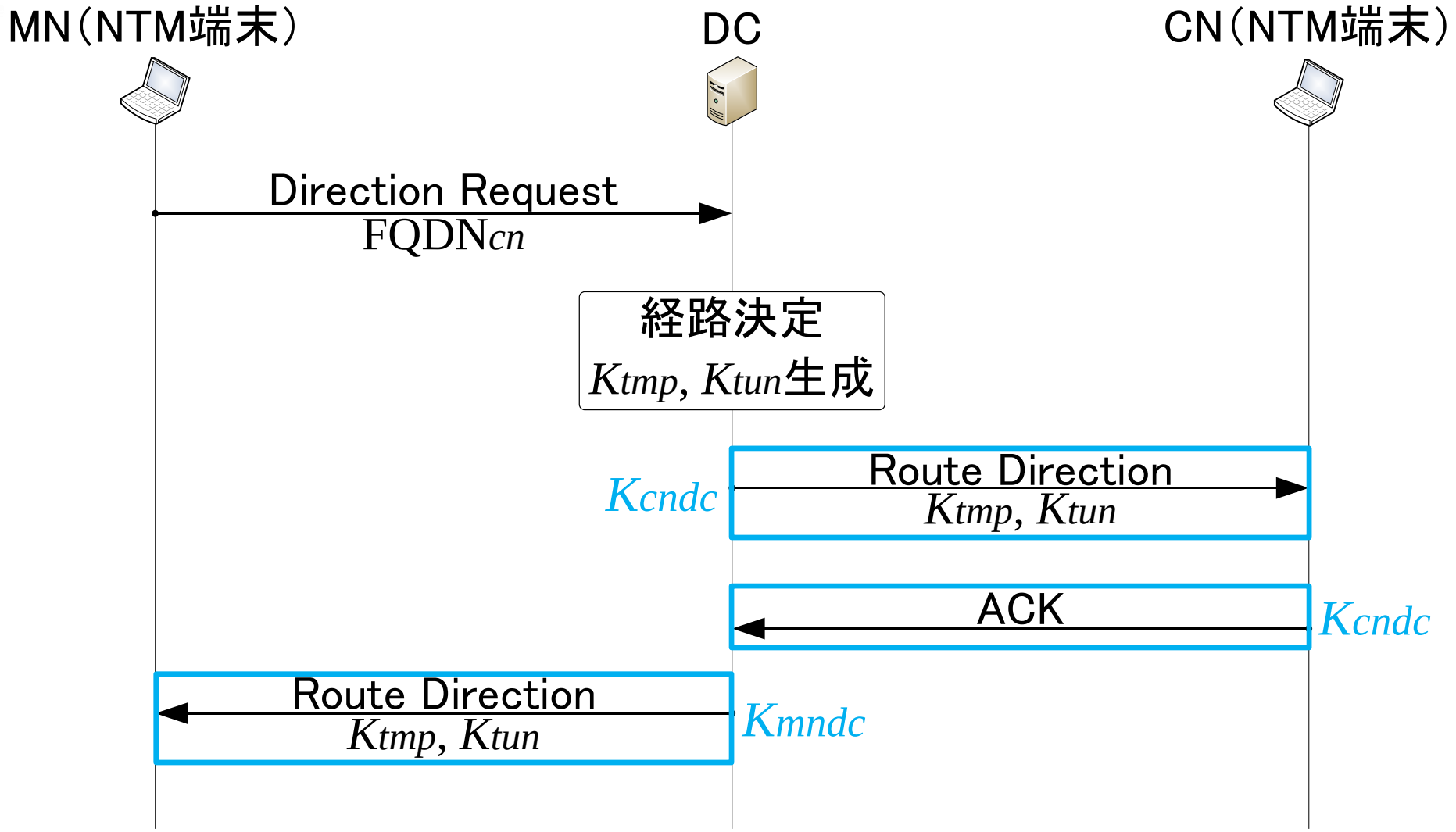
RIP : Real IP Address　VIP : Virtual IP Address

経路生成(1/5)

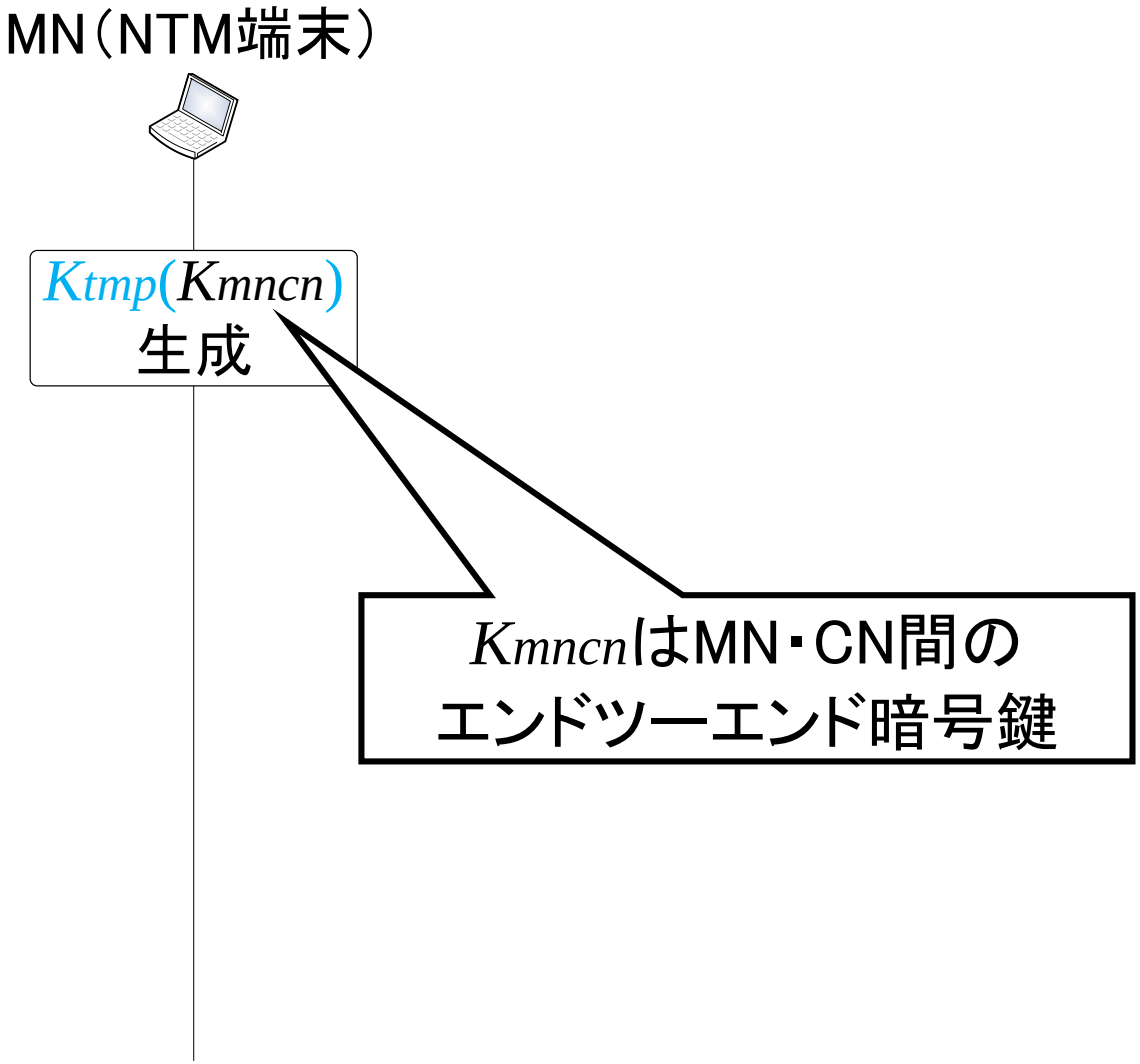


CN : Correspondent Node

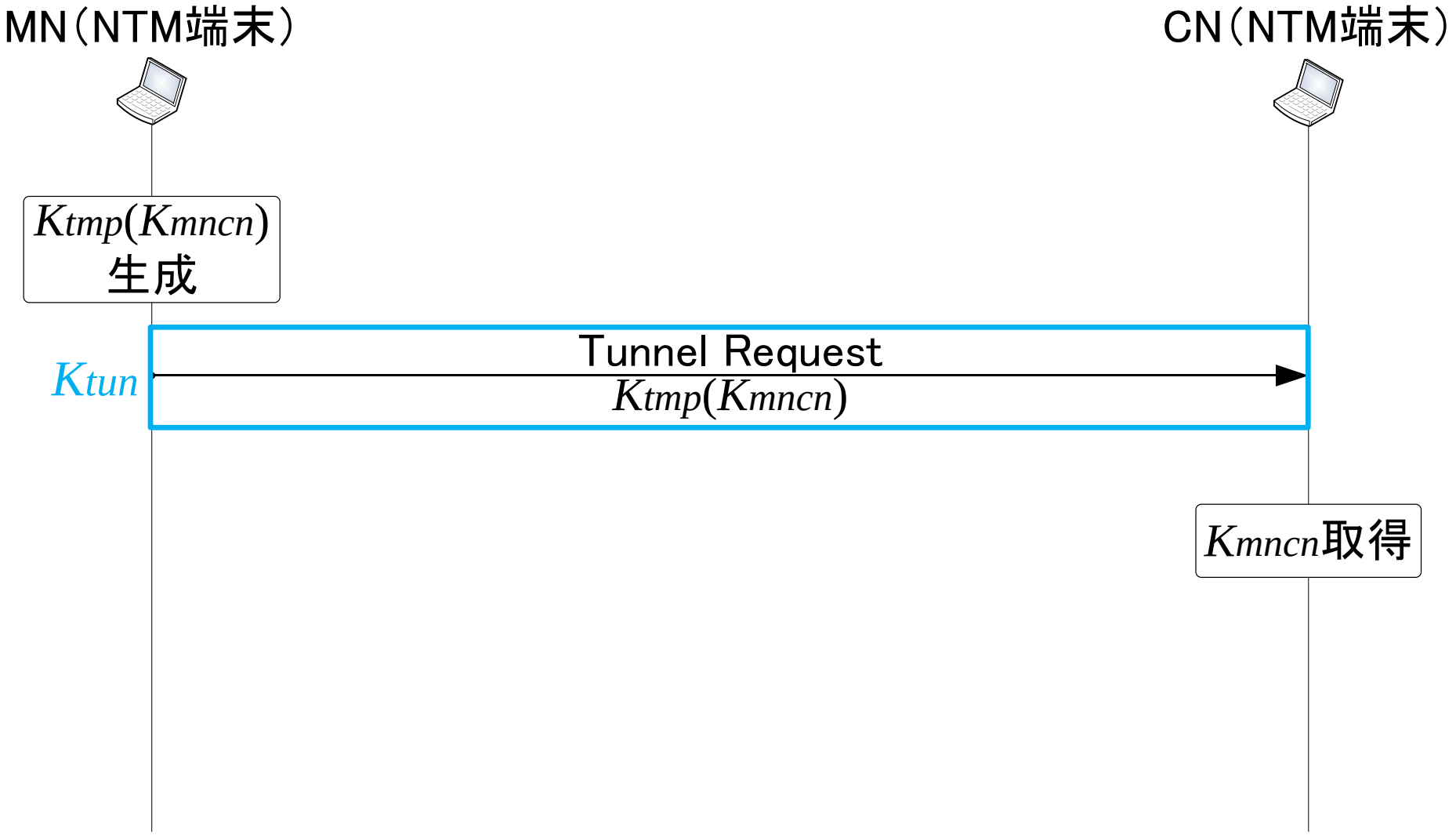
経路生成(2/5)


MN(NTM端末)
DC
CN(NTM端末)
Direction Request
FQDNcn
経路決定
Ktmp, Ktun生成
Kcndc
Route Direction
Ktmp, Ktun
ACK
Kcndc
Route Direction
Ktmp, Ktun
Kmndc

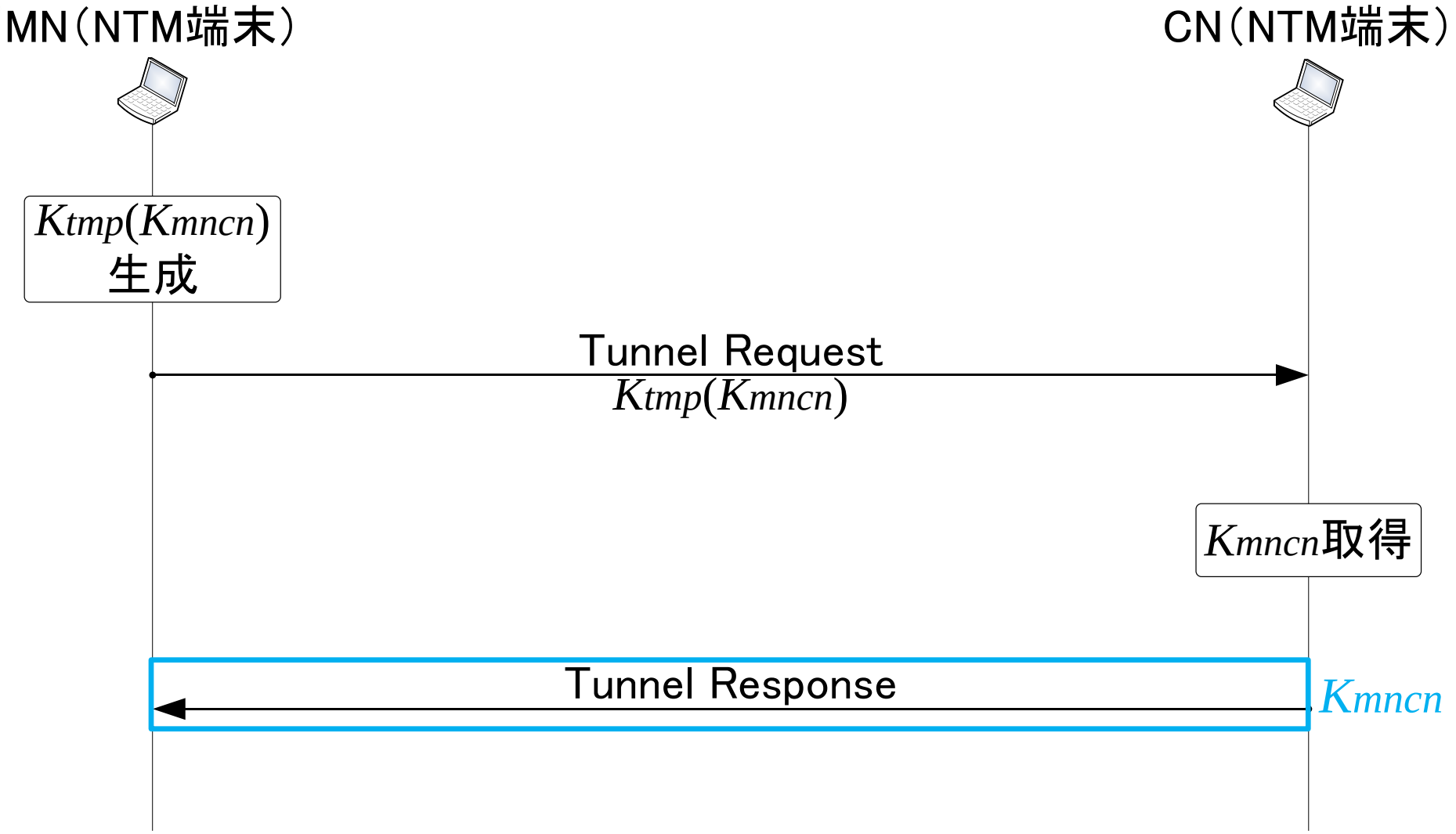
経路生成(3/5)



経路生成(4/5)


MN(NTM端末)
CN(NTM端末)
Ktmp(Kmncn)
生成
Ktun
Tunnel Request
Ktmp(Kmncn)
Kmncn取得

経路生成(5/5)

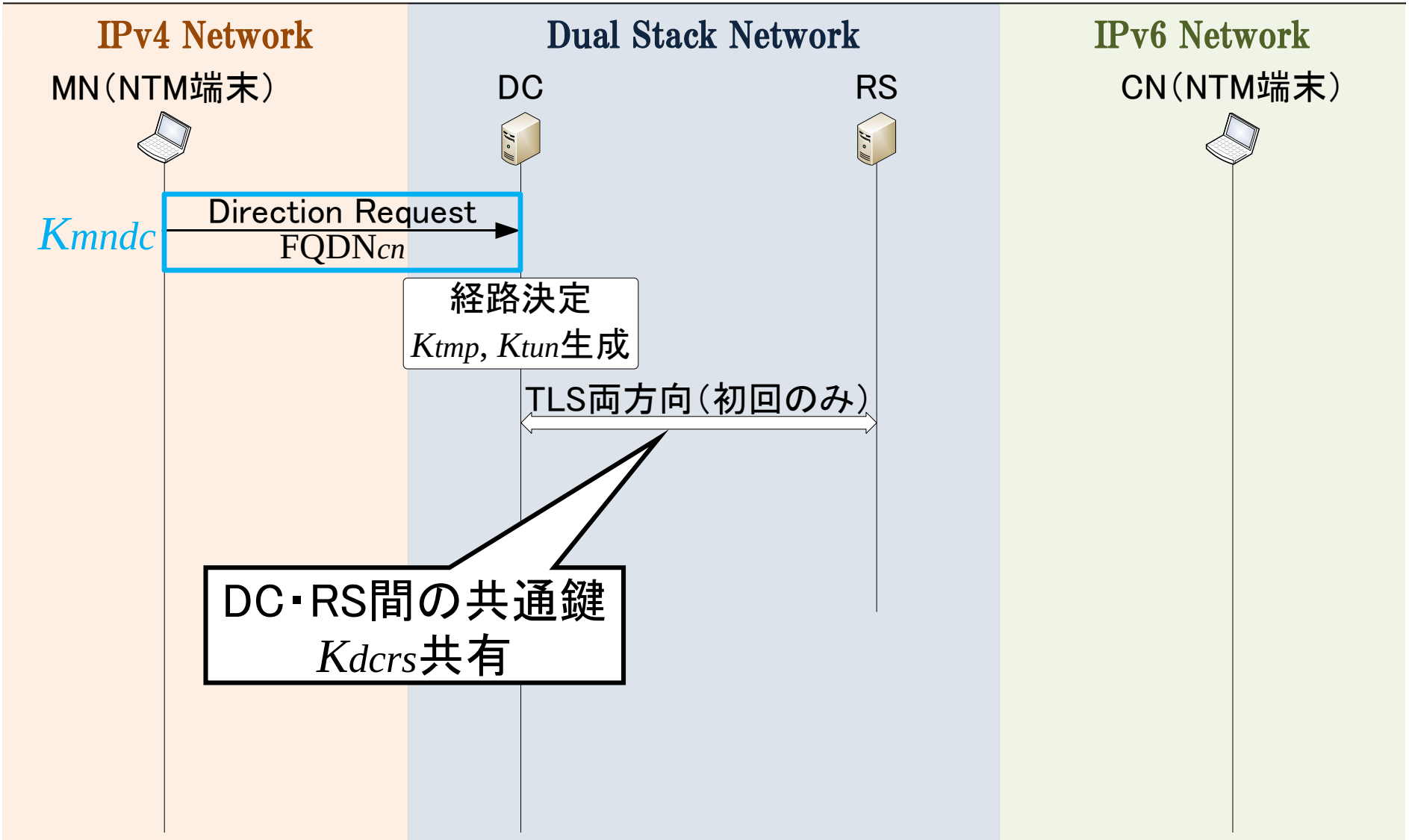

MN(NTM端末)
CN(NTM端末)
Ktmp(Kmncn)
生成
Tunnel Request
Ktmp(Kmncn)
Kmncn取得
Tunnel Response
Kmncn

直接経路生成できない場合

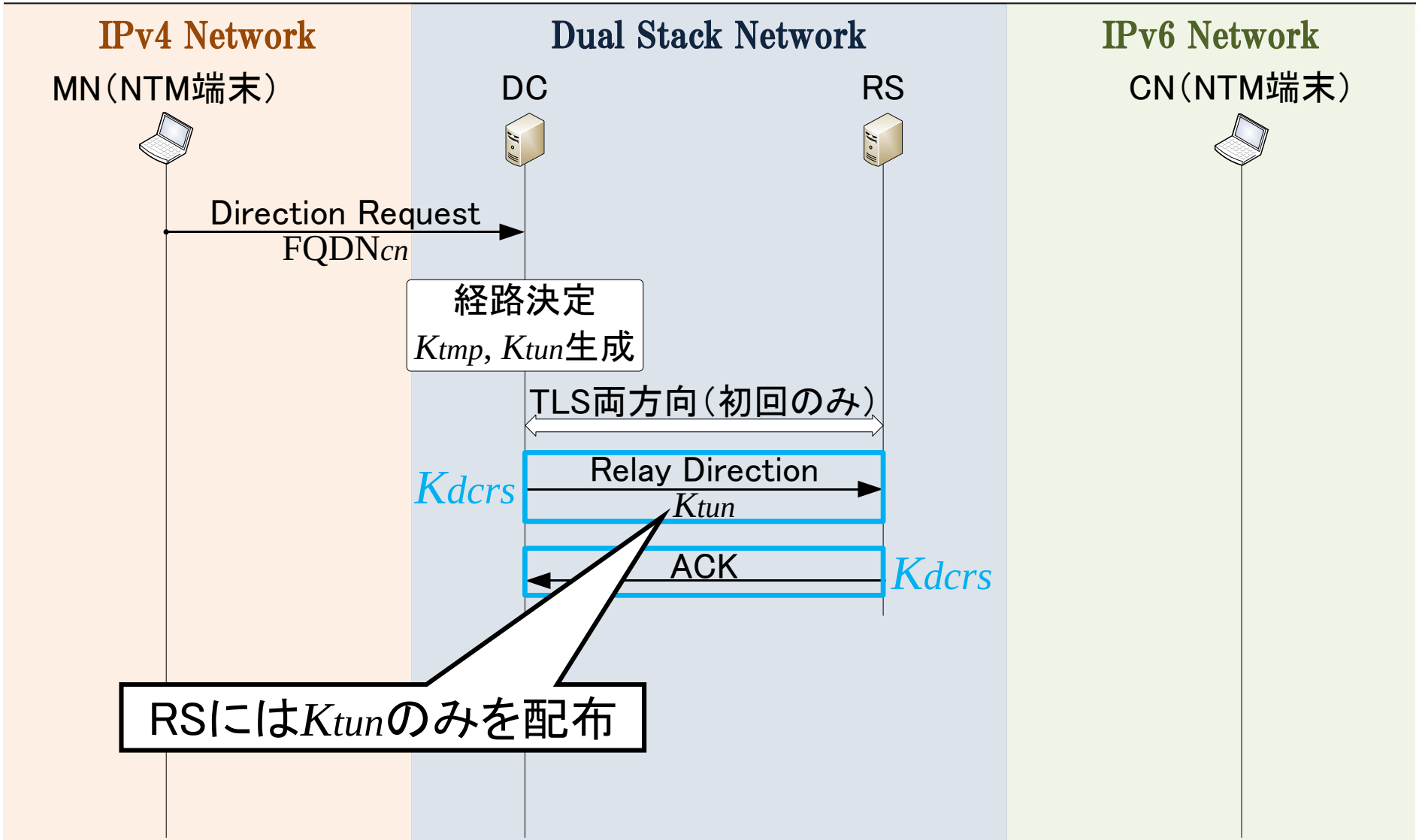
- MNとCNが直接経路を生成できない場合がある
  - 一方がIPv4，他方がIPv6
  - MNとCNが異なるNAT配下にある

- 直接経路を生成できない場合はRS経由の通信
  - この場合にも安全性を確保する必要がある

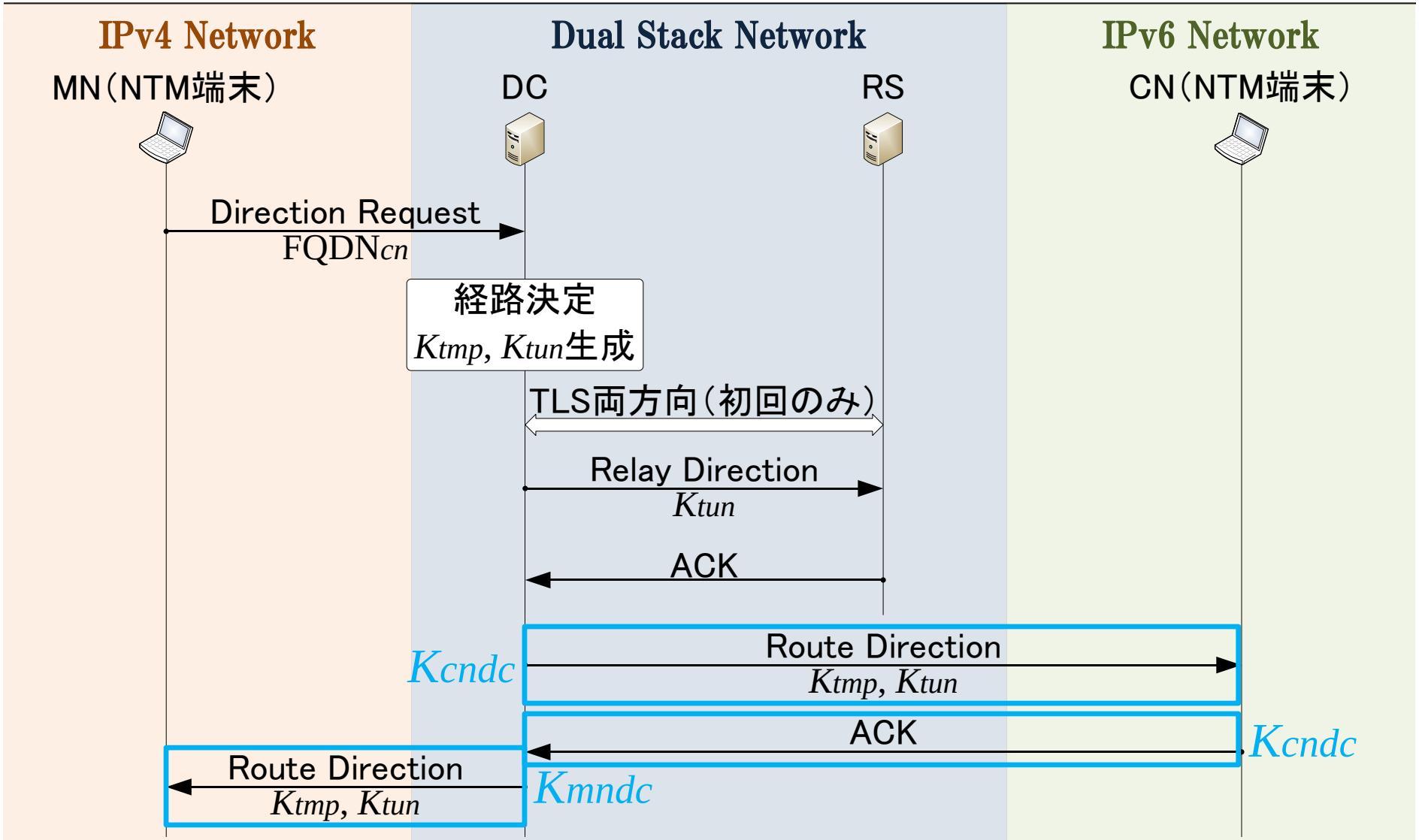
RS経由時の経路生成(1/6)



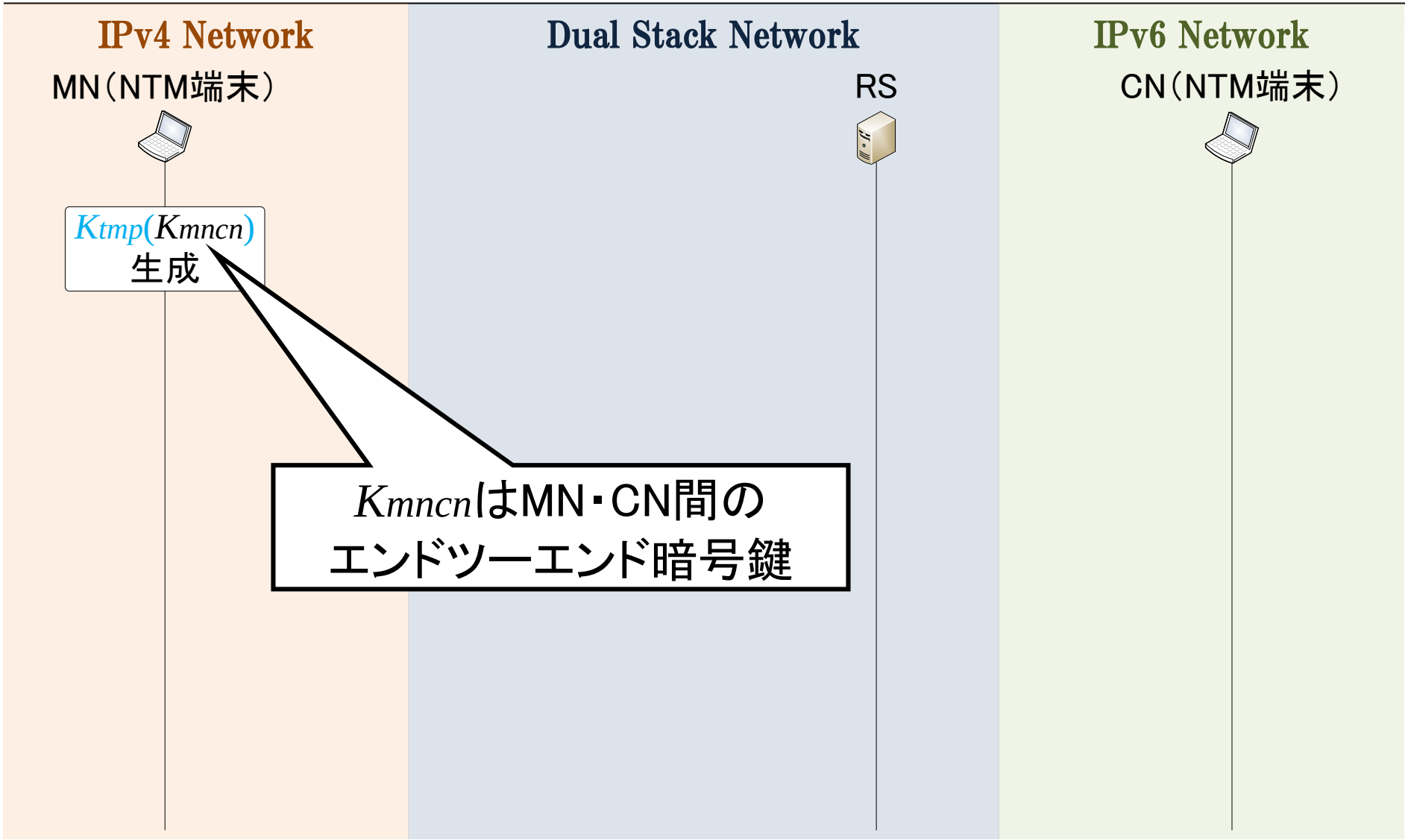
RS経由時の経路生成(2/6)



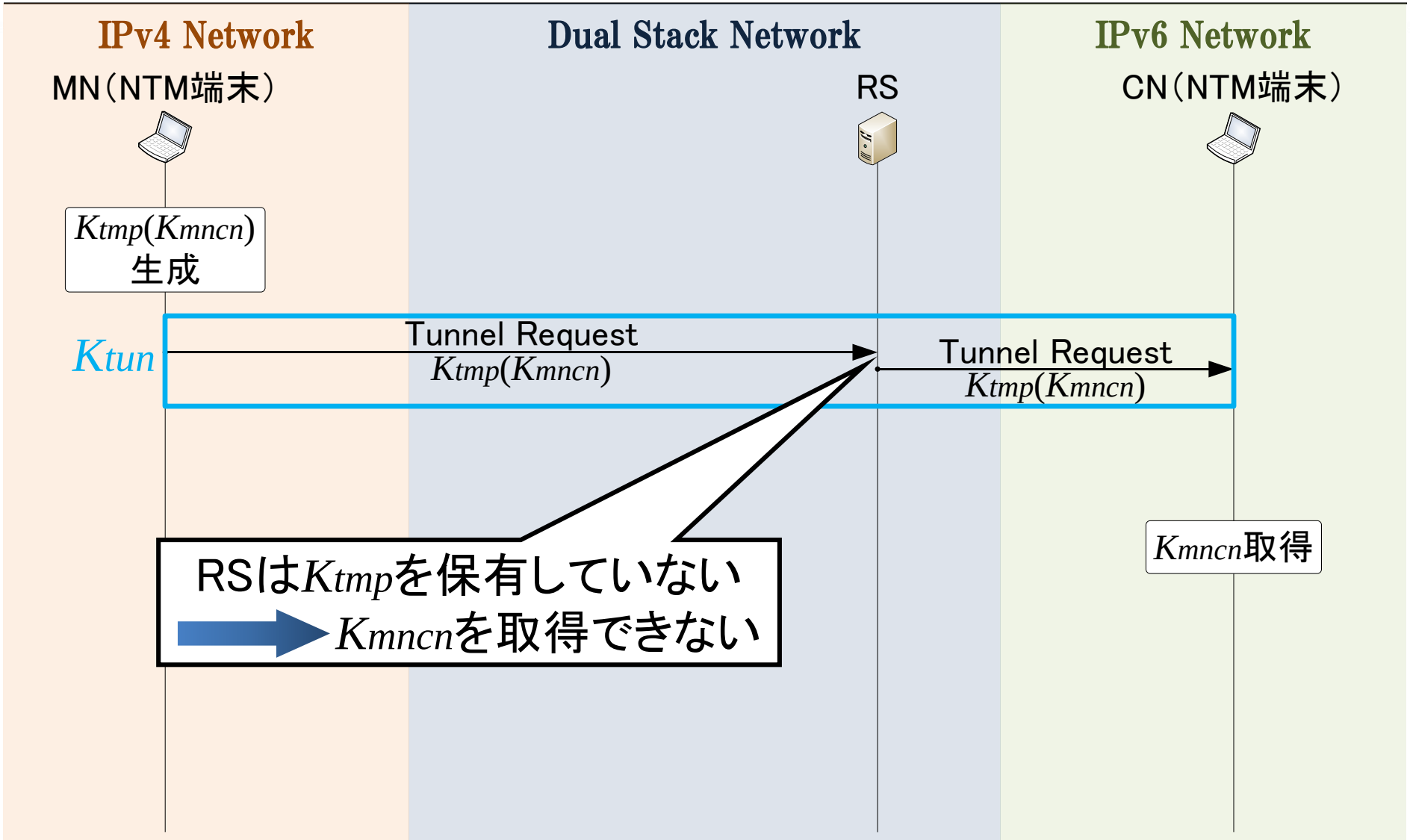
RS経由時の経路生成(3/6)



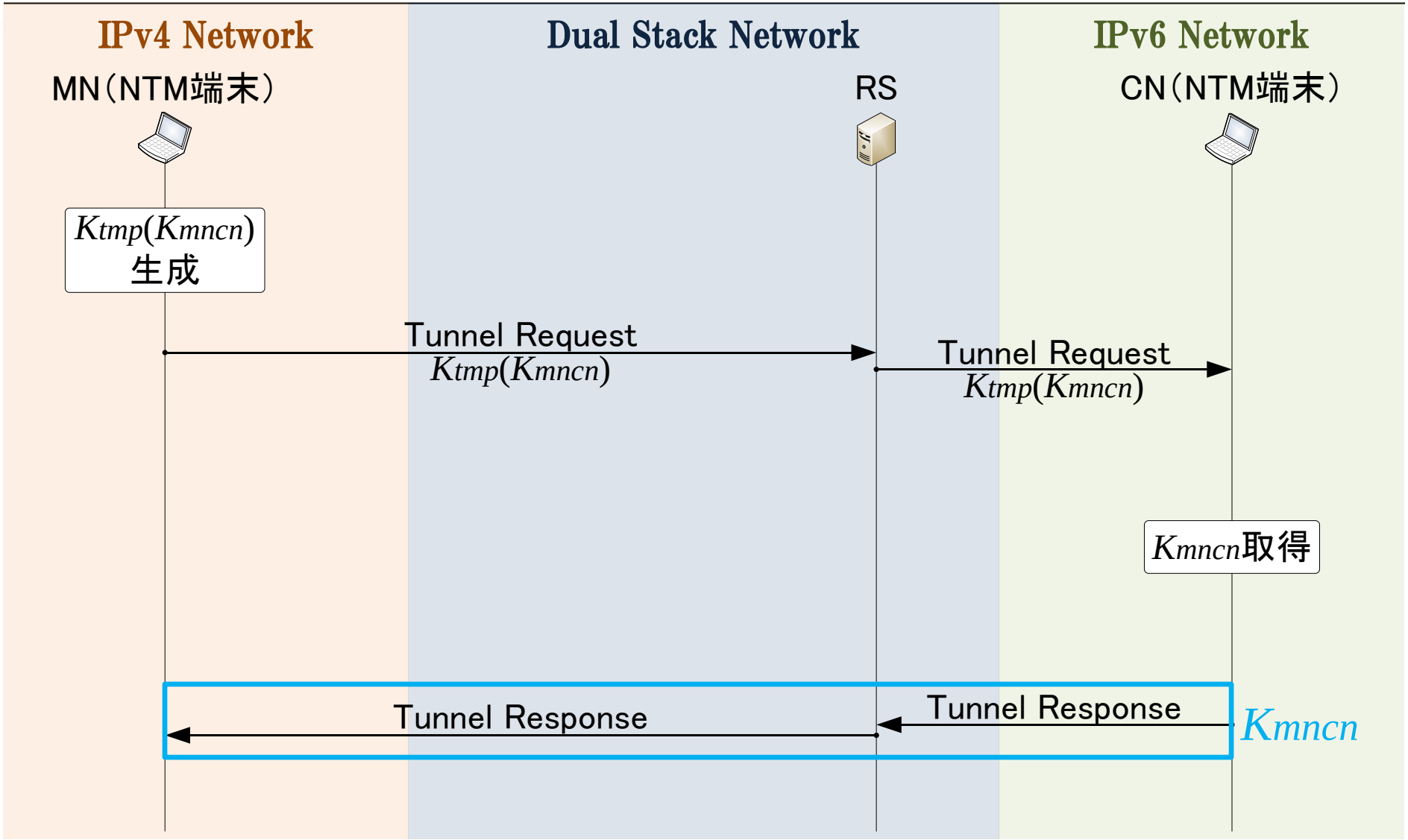
RS経由時の経路生成(4/6)



RS経由時の経路生成(5/6)

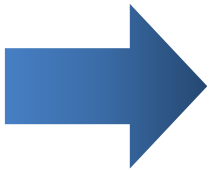


RS経由時の経路生成(6/6)



まとめ

- NTMobileのセキュリティ対策
  - パケットの暗号化
  - 各装置の認証
  - 暗号鍵の安全な共有



エンドツーエンド暗号鍵は
ネットワーク管理者にもわからない

- 今後の方針
  - 各種攻撃への対策方法の検討

付録：ログイン処理（公開鍵認証方式）