

NTMobileにおけるRSの検討

土井 敏 樹^{†1} 鈴木 秀 和^{†1}
内藤 克 浩^{†2} 渡 邊 晃^{†1}

モバイルネットワークの普及により、自由に通信を開始できる通信接続性と、通信中にネットワークの切り替えが可能な移動透過性が要求されている。我々は、通信接続性と移動透過性を同時に実現できる技術として、NTMobile(Network Traversal with Mobility)を提案している。NTMobileでは、アプリケーションに対して重複しないことが保証された仮想IPアドレスを提供し、実際の通信は実アドレスでトンネル通信を行う。NTMobileでは、あらゆるケースにおける接続性を確実に実現するため、通信パケットの中継を行うRS(Relay Server)と呼ぶ機器が存在する。本論文では、RSを3種類の機能に整理し、実装および動作検証を行った。

Studies on RS in NTMobile

TOSHIKI DOI,^{†1} HIDEKAZU SUZUKI,^{†1} KATSUHIRO NAITO^{†2}
and AKIRA WATANABE^{†1}

Due to the population of mobile networks, both connectivity enabling the start of communication at any time and the mobility enabling the free switching of networks during communications have been eagerly looked for. Under such circumstances, we have been proposing a technology called “NTMobile” (Network Traversal with Mobility) that can realize connectivity and mobility at the same time. Virtual IP addresses are assigned to NTMobile nodes, while actual communications are conducted through a tunnel with real IP addresses. In NTMobile, a device called Relay Server (RS) which relays communication packets is set in order to realize connectivity in every case. In this paper, we categorized RS into three types based on their different functions, and conducted implementation and verification of operability.

^{†1} 名城大学大学院理工学研究科

Graduate School of Science and Technology, Meijo University

^{†2} 三重大学大学院工学研究科

1. はじめに

高速無線技術の発展やスマートフォンなどの携帯情報端末の普及により、ネットワーク利用の需要が劇的に増加している。このようなネットワーク利用状況はIPv4が設計された当時の想定を遥かに超えている。IPアドレス枯渇への長期的解決策としてはIPv6が準備されているが、IPv4とIPv6の互換性が無いことから、移行が殆ど進んでいないのが現状である。そのため、IPv6は必要に迫られ徐々に導入されていくが、IPv4は今後半永久的に存在し続けると言われている。このような背景から、本論文ではIPv4が今後も重要な位置づけを占めることを想定し、IPv4の通信接続性と移動透過性について議論する。

IPv4では、アドレス枯渇対策として、組織内のネットワークをプライベートアドレスで構成し、グローバル空間へのアクセスはNAT(Network Address Translation)を介して行う形態が定着している。しかし、NATはプライベートネットワークをグローバルネットワークから隠蔽する性質を持っており、グローバルネットワーク側から通信を開始することができないNAT越え問題が存在する。既存のNAT越え技術としては、UDP hole punchingを利用したSTUN(Simple Traversal of UDP through NATs)¹⁾、全てのデータ通信を外部サーバ経由で行うTURN(Traversal Using Relay NAT)²⁾、SIPをベースにして複数のNAT越え方式を自律的に選択するICE(Interactive Connectivity Establishment)³⁾などが存在する。これらの技術は既設のNATをそのまま使えるという利点があるが、専用のアプリケーションを利用した通信しか行えないという制約がある。また、これらのNAT越え技術は通信ノードの移動については全く考慮していない。

一方、移動ノードの普及とトラフィック量の増大から、通信しながら場所を移動したり、Wifiを用いてトラフィックを迂回したいという要求が高まっている。しかし、IPネットワークでは、IPアドレスが位置情報と通信識別情報の意味を持っているため、ノードの接続場所が変わると位置情報が変化し、通信を継続することができない。IPv4において、移動しながら通信を継続できる移動透過性技術として、Mobile IPv4⁷⁾、MATv4(Mobile Support Architecture and Technologies v4)⁸⁾などがある。しかし、これらの技術は、基本的にはNATの存在を考慮していない。NATを跨る移動透過性を実現するため、Mobile IPでは、UDPトンネルを使用した手法⁹⁾がある。しかし、必ず中継装置であるHA(Home Agent)を経由した通信となるため、通信経路が冗長化する。また、MATv4についてはNATを跨

Graduate School of Engineering, Mie University

る移動は想定していない。

我々は、NAT 越え問題の解決と移動透過性を同時に実現できる技術として、NTMobile(Network Traversal with Mobility)⁴⁾⁻⁶⁾を提案している。NTMobileでは、アプリケーションに対して重複しない仮想 IP アドレスを提供し、実際の通信は実アドレスでトンネル通信を行うことにより NAT 越えと移動透過性を同時に実現する。

NTMobileでは、基本的にはエンドノード間で直接通信を行うが、それが困難な場合、中継サーバ RS(Relay Server)を介してパケットの中継を行う。RSには用途によって3つの種類がある。すなわち、通信を行う2台のNTMノードが異なるNAT配下に存在する場合に利用するトンネル切り替え型RS-S(RS type-S: Switch), NTMノードとNTMobileを実装していないノード(一般ノード)が通信を行う場合に利用するアドレス変換型RS-N(RS type-N: NAT), および通信パケットのペイロード部分にIPアドレスを含むアプリケーションを利用する場合に利用するアドレス無変換型RS-T(RS type-T: Transparent)である。

本論文では、3種類のRSに対して、それぞれ動作の検討を行った。RSを利用状況に使い分けることによって、あらゆる形態のネットワークにおいて、NTMobileを利用して、NAT越えと移動透過性を同時に実現した通信を行うことができる。また、RSの機能の一部について、実装を終え動作検証を行った。

以降2章では移動透過性とNAT越えを実現している関連技術について、3章ではNTMobileの概要について、4章ではRSについて示す。5章ではLinuxへの実装と動作検証を述べ、6章でまとめる。

2. Mobile IP

Mobile IPで移動透過性とNAT越えを実現出来る技術として、Mobile IP Traversal of NATがある。この手法を用いることにより、MNがNAT配下に移動したとしても通信を継続することが可能である。図1に、Mobile IP Traversal of NATの概要を示す。

MNは移動前に、HAを介してCNと通信を行なっている。ここで、MNがNAT配下のネットワークに移動すると、移動先ネットワークのDHCPによりプライベートアドレスが割り当てられる。このアドレスを、共存気付けアドレス: CCoA(Co-located Care-of Address)と呼ぶ。MNがHAに向けてBUを送信するとき、MNとHA間にUDPトンネルを構築するように指示する。HAはパケットを受信すると、BUに記載されているCCoAと送信元IPアドレスを比較し、アドレスが違うためHAはMNがNAT配下にいると判断する。HAからの応答を受信したMNは、HAへと逆方向トンネルを形成してCN宛のパ

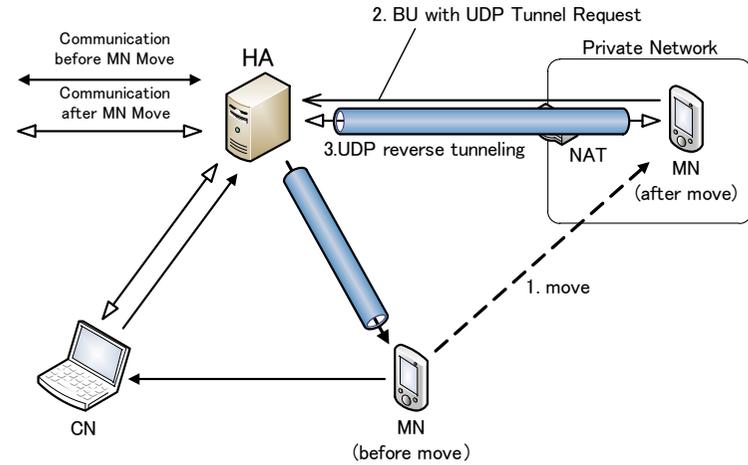


図1 Mobile IP Traversal of NATの概要
Fig. 1 Overview of Mobile IP Traversal of NAT.

ケットをHAへと送信する。

この手法によるとNATが存在する環境において移動透過性を実現することができるが、必ずHAを経由した通信となる。

3. NTMobile

3.1 NTMobileの構成

図2に、NTMobileの概要を示す。NTMobileでは、システムの構成要素として、NTMobileの機能を実装したエンドノード(NTMノード)の他に、NTMノードのアドレス情報を管理するDC(Direction Coordinator), エンドエンドの通信が行えない場合などにパケットを中継するRS(Relay Server)が存在する。DCは、NTMノードに仮想IPアドレスを配布する他、NTMノードとRSに対してはトンネル経路を指示する装置であり、DynamicDNSの機能を包含している。また、NTMノードのアドレス情報をNTMobile専用レコード(NTMレコード)として保持している。NTMobileで使用する仮想IPアドレス等の情報を管理するために、各DCは自身に割り当てられた仮想IPアドレスプールを持ち、NTMノードに重複しない仮想IPアドレスを提供する。なお、DCとNTMノード間、各DC間及び各

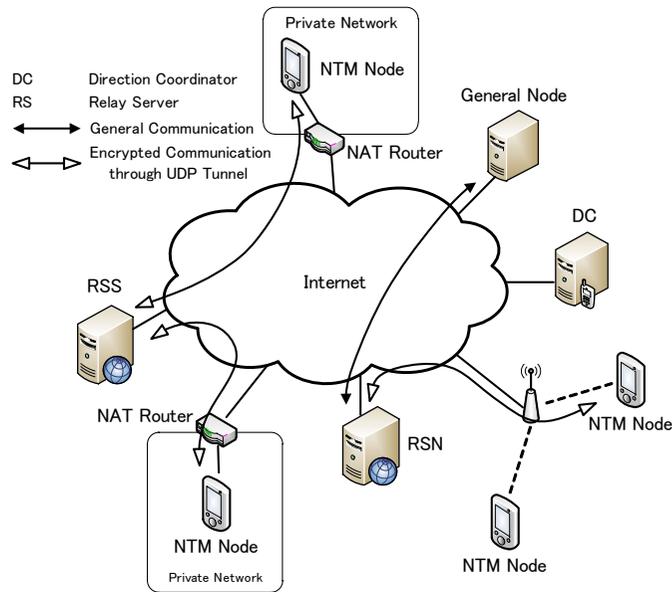


図 2 NTMobile の概要
Fig. 2 Overview of NTMobile.

DC と各 RS との間には信頼関係があるものとする。NTM ノードは、DC からノードを一意に識別できる仮想 IP アドレスを与えられ、NTM ノード同士の通信の識別に使用する。アプリケーションは、割り当てられた仮想 IP アドレスを自身のアドレスとして認識する。

実際の通信は、実 IP アドレスにより仮想 IP アドレスの packets を UDP でカプセル化することにより実現する。DC はエンドノードが存在する位置から通信経路を決定し、NTM ノードにトンネル経路確立手順を指示する。この手法によって、アプリケーションに対して、NAT の存在や移動に伴う実 IP アドレスの変化を隠蔽することができる。

NTM ノードのアプリケーションは、仮想 IP アドレスを利用して通信するため、移動に伴う実 IP アドレスの変化に気づかず、通信を継続できる。エンドエンドの通信が可能な場合は NTM ノード間で直接トンネル構築を行い、エンドエンド通信が行えない場合には RS を経由したトンネル経路を構築する。

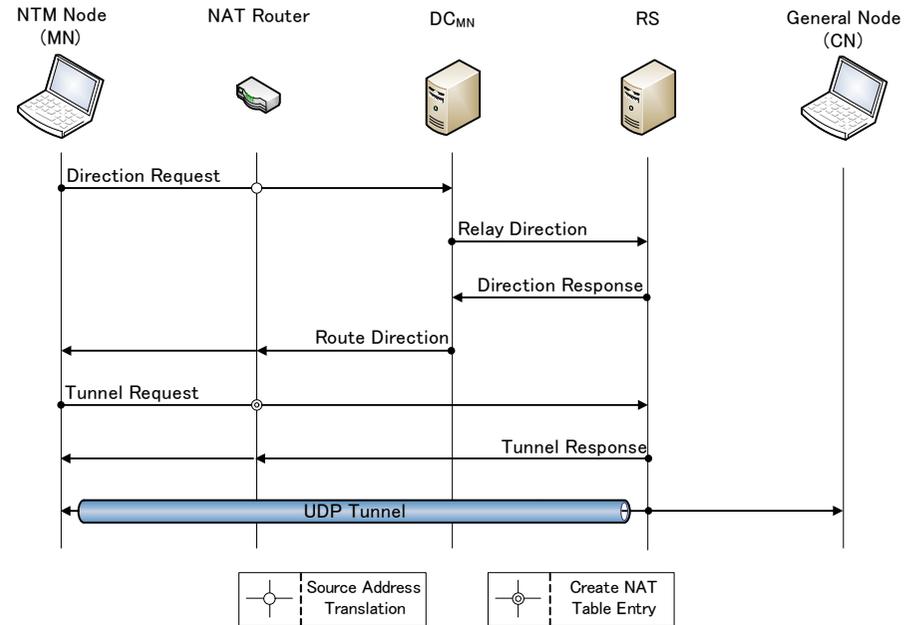


図 3 RS を介した接続確立手順
Fig. 3 Connection procedure via RS.

3.2 NTMobile の動作

図 3 に、NTM ノード (MN) が一般ノード (CN) との間に RS-N を介した接続を確立する手順を示す。以後の説明では、通信開始側のノードを MN (Mobile Node)、通信相手側ノードを CN (Correspondent Node) とする。

3.2.1 ネットワーク接続時

全ての NTM ノードは、ネットワーク接続時に DC に対してアドレス情報の登録処理を行う。この時、NTM ノードは DC から重複しないことが保証された仮想 IP アドレスを与えられる。アプリケーションは仮想 IP アドレスを使用してセッションを確立する。

3.2.2 名前解決

通信開始時、MN は自身のプライマリ DNS に相手ノードの名前解決を行う。このとき、MN では DNS への問い合わせをフックし、CN の NTM レコードの問い合わせを行う。CN

が NTM ノードであれば、CN 側の DC から NTM レコードを入手できるので、MN は入手した情報を記録する。CN が一般ノードの場合は、問い合わせに対する応答を得ることができないため、MN は CN が一般ノードであると認識する。

3.2.3 コネクション確立

MN は DC_{MN} に対して経路指示要求 Direction Request を送信する。 DC_{MN} は、Direction Request に記載されている MN の NTM レコードの情報より、MN がプライベートネットワークに存在すると判断し、トンネル経路を決定する。CN が一般ノードである場合、Direction Request を受信した DC_{MN} は RS に対して Relay Direction を送信し、RS は Direction Response を応答する。Relay Direction には、MN と CN の NTM レコードの情報やノード間のトンネル経路を識別する $PathID_{MN,CN}$ が記載されている。その後、 DC_{MN} は MN に経路指示である Route Direction を送信することにより経路確立手順を指示する。MN は RS に向けて Tunnel Request を送信し、RS は MN に対して Tunnel Response を返す。以上のネゴシエーションによって MN は RS との間に UDP トンネルを構築し、実際の通信では MN から RS までがトンネル通信を行う。RS では受信パケットのカプセル化/デカプセル化、また元パケットのアドレス変換を行う。

3.2.4 トンネル通信

MN は宛先が仮想 IP アドレスであるパケットを送信する際、UDP でカプセル化して暗号化を行い、RS へと送信する。通信経路上に NAT が存在しても、外側 IP ヘッダの IP アドレスが変化するのみであり、オリジナルパケットは変更されない。パケットを受け取った CN は受信したパケットを、デカプセル化してから上位アプリケーションへと渡す。この手法によって、アプリケーションに対して、NAT の存在や移動に伴う実 IP アドレスの変化を隠蔽することができる。

4. Relay Server

本論文では、NTMobile における RS の機能について、整理した。RS は使用用途によって以下の 3 種類に分類できる。

4.1 RS-S(RS type-S : Switch)

RS-S はトンネル切り替え型の RS である。図 4 に、RS-S を用いた通信における通信パケットの遷移の様子を示す。

MN と CN が異なる NAT 配下に存在する場合、NAT 越え問題によって直接通信を行うことができない。このような場合、エンドノードは RS との間に UDP トンネルを構築する。

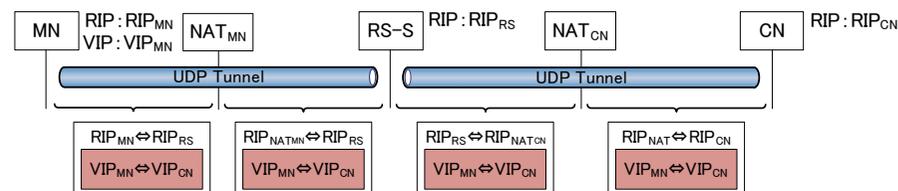


図 4 RS-S を用いた通信のパケット遷移の様子

Fig. 4 Translation state of the packet communication using the RS-S.

このように RS を経由した通信を行うことにより、NTM ノードが異なる NAT 配下に存在しても通信を行うことが出来る。実際の通信では、MN から送信されたパケットは、実 IP アドレスでカプセル化されて RS へと転送される。RS は受信パケットの外側 IP ヘッダのアドレス変換を行なって NAT_{CN} へと転送し、CN はパケットを受信するとデカプセル化を行う。このように、仮想 IP アドレスを実 IP アドレスでカプセル化して通信を行うことで、元パケットが変更されることなく、上位アプリケーションは仮想 IP アドレスを利用した通信を行うことが出来る。

なお、MN と CN は更に自律的に経路最適化処理を行う¹⁰⁾。NAT の種類によっては RS を経由しない経路で通信を行うことが出来る。

4.2 RS-N(RS type-N : NAT)

RS-N はアドレス変換型の RS である。図 5 に、RS-N を用いた通信における通信パケットの遷移の様子を示す。利用例として、NTM ノードがインターネット上の Web サーバにアクセスする場合などが挙げられる。サーバ (一般ノード) への改造を避けるため、また、NTM ノードの移動透過性を実現するために RS-N がデカプセル化とアドレス変換の処理を行う。

NTM ノードと一般ノードと通信を行う場合、NTM ノードは RS-N との間に UDP トンネルを構築する。RS-N は NTM ノードからパケットを受信すると、パケットのデカプセル化を行い、仮想 IP アドレスを実 IP アドレスへとアドレス変換を行なって一般ノードへと転送する。一般ノードは通信相手が RS-N であると認識する。このように RS-N を中継した通信を行うことにより、NTM ノードが移動しても RS が軸となって一般ノードへの中継を行うため、NTM ノードの移動透過性を実現することが出来る。

4.3 RS-T(RS type-T : Transparent)

RS-T はアドレス無変換型の RS である。NTM ノードと一般ノードが通信を行う場合、

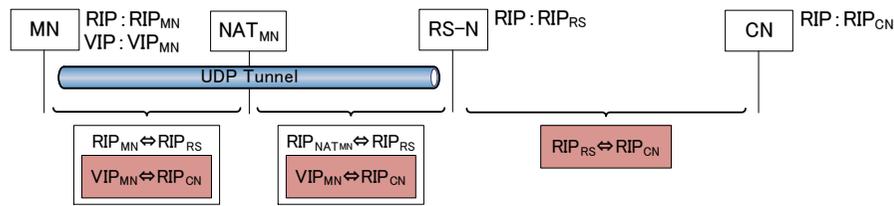


図 5 RS-N を用いた通信のパケット遷移の様子
Fig. 5 Translation state of the packet communication using the RS-N.

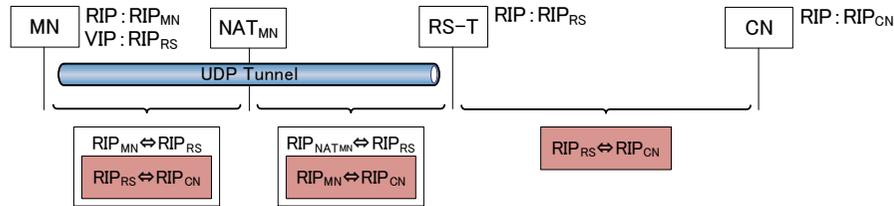


図 6 RS-T を用いた通信のパケット遷移の様子
Fig. 6 Translation state of the packet communication using the RS-T.

RS-N を利用した通信を行い、RS-N において元パケットのアドレス変換が行われる。ここで、パケットのペイロード部分に IP アドレスを含むアプリケーション^{*1}を利用したい通信を行う場合、ペイロード部分の IP アドレスはアドレス変換されない。よって、一般ノードがパケットを受信したパケットでは、ヘッダとペイロードで IP アドレスの相違が生じてしまう。この課題は、RS-T を用いることで解決できる。図 6 に、RS-T を用いた通信における通信パケットの遷移の様子を示す。

RS-T は、予め DC より複数の実 IP アドレスを配布してもらい、NTM ノードは、通常の仮想 IP アドレスの他に、RS が保持している実 IP アドレスの内 1 つを仮想 IP アドレスとして保持する。NTM 端末が SIP 通信などを行う場合は、RS より割り当てられた実 IP アドレスを仮想 IP アドレスとして使用する。RS-T が NTM ノードからパケットを受信すると、パケットのデカプセル化を行う。ここで、元パケットの送信元アドレスはそもそも

*1 主に SIP(Session Initiation Protocol) のことを指す。

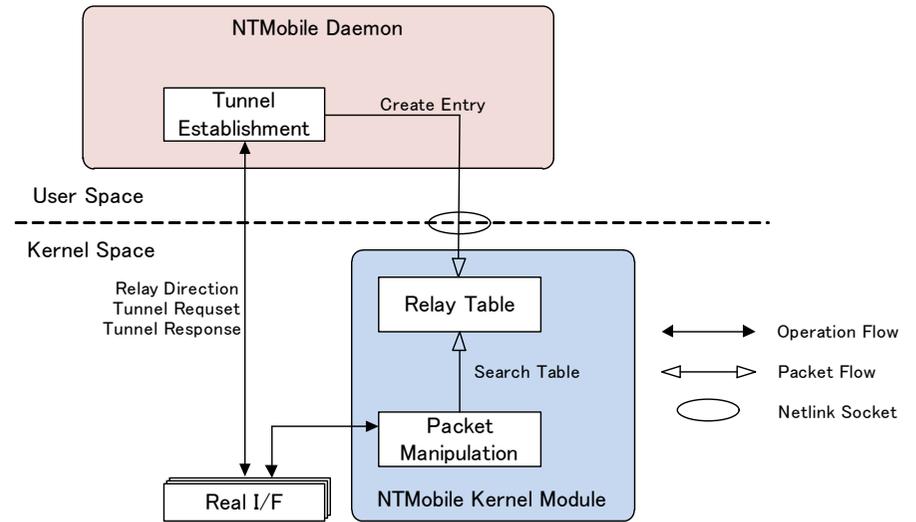


図 7 RS-S のカーネルモジュール図
Fig. 7 Module configuration of Relay Server.

RS の実アドレスであるため、アドレス変換を行わない。よって、デカプセル化したパケットをそのまま一般ノードへと転送する。一般ノードが RS-T から受信したパケットでは、IP アドレスの差異は生じない。

5. 実装と動作検証

今回は、RS のカーネル空間での転送機能の実装と動作検証を行ったのでその結果を報告する。図 7 に RS-S のモジュール構成図を示す。RS-S は NTMobile の機能をユーザー空間とカーネル空間に実装している。なお、ユーザー空間の NTMobile デーモンとカーネル空間の NTMobile カーネルモジュールとのインタフェースは、Netlink ソケットを用いる。

5.1 NTMobile デーモンの実装

NTM デーモンは、ユーザー空間にて、主に制御メッセージの送受信処理を行う。

- トンネル中継情報の登録

DC から Relay Direction を受け取り、パケットに記載されている PathID や、配下ノードへ到達する Tunnel IP/Port などをカーネル空間に実装されている Relay Table に登

表 1 装置仕様
Table 1 Device specifications.

	Hardware	OS	CPU	RAM
DC	EPSON Endeavor NT350	Ubuntu 10.04	Celeron M 380 1.6GHz	256MB
RS	HP s5550j	Ubuntu 10.04	Intel Core i7 2.93GHz	10GB
NTM Node(MN,CN)	HP s5550j	Ubuntu 10.04	Intel Core i7 2.93GHz	10GB

録する。また、Tunnel Request を待機する。

- Tunnel Request の受信と Tunnel Response の送信
NTM ノードから Tunnel Request を受信すると、Tunnel Request を返信し、NTM ノードとの間に UDP トンネルを構築する。

5.2 NTMobile カーネルモジュールの実装

NTM カーネルモジュールは、カーネル空間にて、通信パケットの中継処理を行う。

- Relay Table の管理
Relay Table が保持する情報として、PathID_{MN,CN}、配下ノードに到達する IP アドレス/ポート番号、ノード間の暗号化に使用する共通鍵情報がある。
- カプセル化パケットの中継
NTM ノードからカプセル化パケットを受信したときは、パケットに記載されている PathID_{MN,CN} をキーとして Relay Table を検索し、パケットの宛先をエントリより取得した IP アドレスへ、送信元を RS の IP アドレスへ変換して送信する。

5.3 動作検証

動作検証を行うため、RS におけるパケット中継に要する処理時間と端末間の RTT を計測した。表 1 に各装置の仕様を、図 8 に実機測定のネットワーク構成を示す。比較対象として、ユーザー空間にも Relay Table と転送処理を実装し、カーネル空間との処理時間を比較した。また、図 8 のネットワーク構成ではエンドエンドで通信経路が確立されるが、RS の転送性能を測定するため、ここでは DC の経路指示において RS 経由のトンネル経路を構築するように指示した。

表 2 に RS における転送処理時間の実機測定結果を示す。MN から CN へ ping を実行し、RS で Wireshark を用いてパケットキャプチャを行い、カプセル化されたパケットが到達した時間と宛先にパケットが送信された時間を計測した。なお、ping の送信間隔は Linux における ping 送信間隔のデフォルト値である 1[s] とし、100 回送信して平均値を算出した。

ユーザー空間での転送処理とカーネル空間での転送処理時間の差は明らかであり、約 11.5

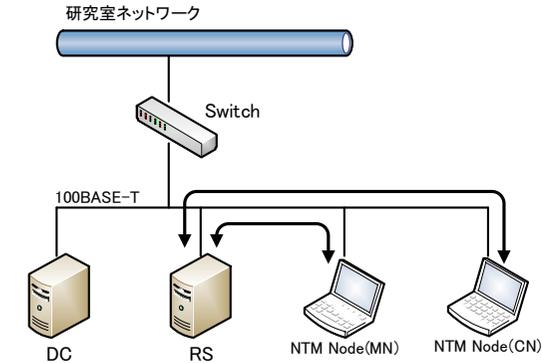


図 8 試験ネットワーク構成
Fig. 8 Test network configuration.

表 2 RS における転送処理時間
Table 2 Transfer processing time in RS.

	ユーザー空間転送	カーネル空間転送
転送処理時間 [ms]	0.15	0.013

表 3 MN-CN 間の RTT
Table 3 RTT between the terminal.

	ユーザー空間転送	カーネル空間転送
RTT[ms]	1.194	0.921

倍の差が出た。ノード間の RTT についても約 1.3 倍の差となった。また、RTT の差は 0.273[ms] となり、転送処理時間の差は 0.137[ms] となった。転送処理時間の差は MN から CN へのパケット中継と CN から MN へのパケット中継においてそれぞれ発生するため、合わせて 0.274[ms] となり、RTT の差とほぼ同じとなった。

6. まとめ

NTMobile では、あらゆるネットワーク形態に対応するため、RS が重要な役割を果たす。本論文では RS を、異なる NAT 配下間での通信に利用する RS-S、一般ノードとの通信に利用する RS-N、SIP 通信などに利用する RS-T の 3 種類に分けて機能の検討を行った。また、RS の転送機能を実装しユーザー空間とカーネル空間での転送性能の比較を行った。今

後は、RS-N と RS-T の実装と動作検証を進める予定である。さらに、IPv4/IPv6 混在環境への適応方法も検討していく予定である。

参 考 文 献

- 1) Rosenberg, J., Mahy, R., Matthews, P. and Wing, D.: Session Traversal Utilities for NAT (STUN), RFC 5389, IETF (2008).
- 2) Mahy, R., Matthews, P. and Rosenberg, J.: Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN), RFC 5766, IETF (2010).
- 3) Rosenberg, J.: Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols, RFC 5245, IETF (2010).
- 4) 西尾拓也, 内藤克浩, 水谷智大, 鈴木秀和, 渡邊 晃, 森香津夫, 小林英雄: NTMobile におけるノードアドレスの移動管理と実装, マルチメディア, 分散, 協調とモバイル (DICOMO2011) シンポジウム論文集, pp.1139-1145(2011)
- 5) 内藤克浩, 西尾拓也, 水谷智大, 鈴木秀和, 渡邊 晃, 森香津夫, 小林英雄: NTMobile における移動透過性の実現と実装, マルチメディア, 分散, 協調とモバイル (DICOMO2011) DICOMO2011 シンポジウム論文集, pp.1349-1359(2011)
- 6) 鈴木秀和, 水谷智大, 西尾拓也, 内藤克浩, 渡邊 晃: NTMobile における相互接続性の確立手法と実装, マルチメディア, 分散, 協調とモバイル (DICOMO2011) DICOMO2011 シンポジウム論文集, pp.1339-1348(2011)
- 7) Perkins, C.: IP Mobility Support for IPv4, Revised, RFC 5944, IETF (2010).
- 8) 関 顕生, 岩田裕貴, 森廣勇人, 前田香織, 近堂徹, 岸場清悟, 西村浩二, 相原玲二: IPv4 拡張した移動透過通信アーキテクチャ MAT の設計と性能評価, 情報処理学会論文誌, Vol.52, No.3, pp.1323-1333 (2011).
- 9) Levkowitz, H. and Vaarala, S.: Mobile IP Traversal of Network Address Translation (NAT) Devices, RFC 3519, IETF (2003).
- 10) 納堂博史, 鈴木秀和, 内藤克浩, 渡邊 晃: NTMobile の経路最適化の検討, 情報処理学会研究報告, 2012-MBL-61, No.33, pp.1-8 (2012).
- 11) 上醉尾一真, 鈴木秀和, 内藤克浩, 渡邊 晃: IPv6 ネットワークにおける NTMobile の検討, 情報処理学会研究報告, Vol.2011-MBL-59, No.9, pp.1-7 (2011).

NTMobileにおけるRSの検討

†名城大学 理工学研究科 ‡三重大学 工学研究科
土井敏樹† 鈴木秀和† 内藤克浩‡ 渡邊晃†

- NTMobileについて
 - 研究背景
 - システムの概要と動作シーケンス
- 中継装置RS(Relay Server)の分類と動作
 - 利用場面別に分類, 動作の検討と整理
 - 動作シーケンス
- 実装と性能評価
 - Linux OS上にRSを実装
 - 転送性能の評価
- まとめ

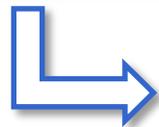
- 移動しながら通信をしたいという要求
 - 公衆無線網や小型端末(スマートフォンなど)の普及
- 移動透過性技術の必要性
 - IPネットワークでは接続場所が変わるとIPアドレスが変化
 - 端末が移動すると通信が途切れてしまう
 - トラフィック量増大によるWIFIへのトラフィック迂回
- NAT越え技術の必要性
 - IPネットワークではNATの利用が一般的
 - NATの外側から内側にアクセスを開始できない

NAT: Network Address Translation

移動透過性とNAT越えを同時に実現する技術
NTMobile(Network Traversal with Mobility)

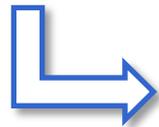
- 目的
 - あらゆるネットワークにおいて, NAT越えを伴った移動通信の実現
- 特徴

仮想アドレスの導入

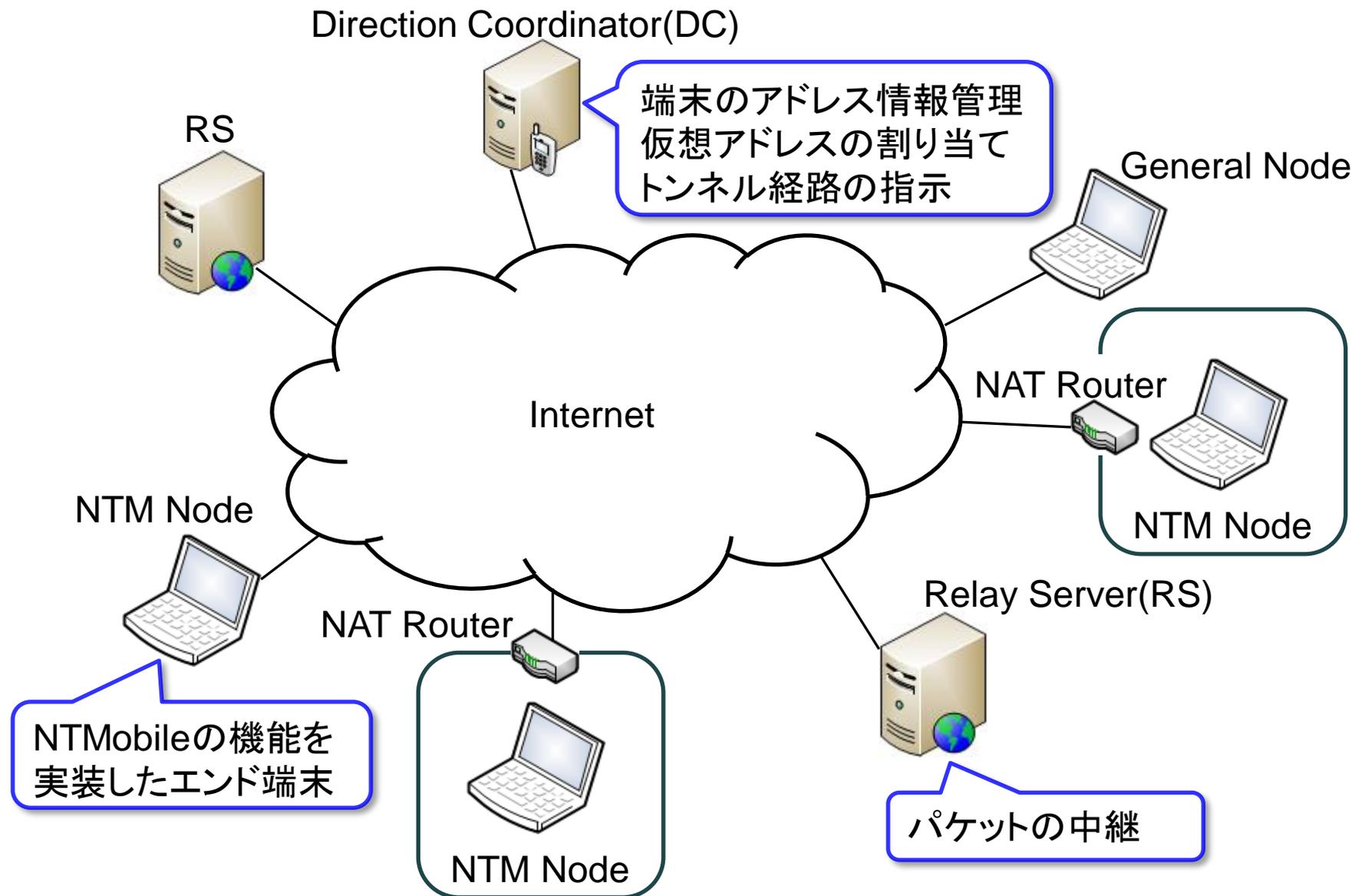


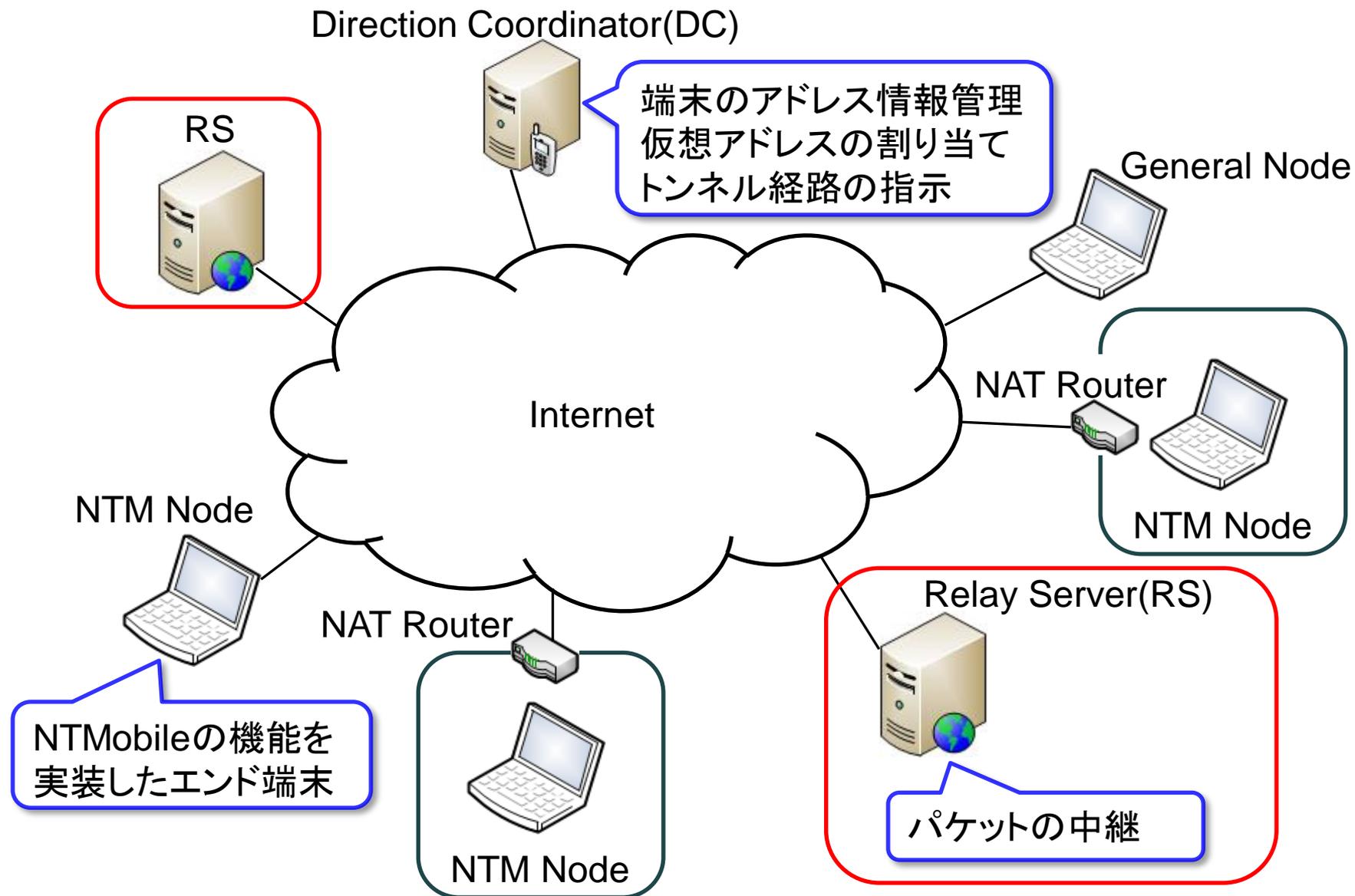
- 端末を一意に識別できる仮想アドレスを提供
- 移動に伴う実アドレスの変化を隠蔽
- アプリケーションは仮想アドレスを使って通信

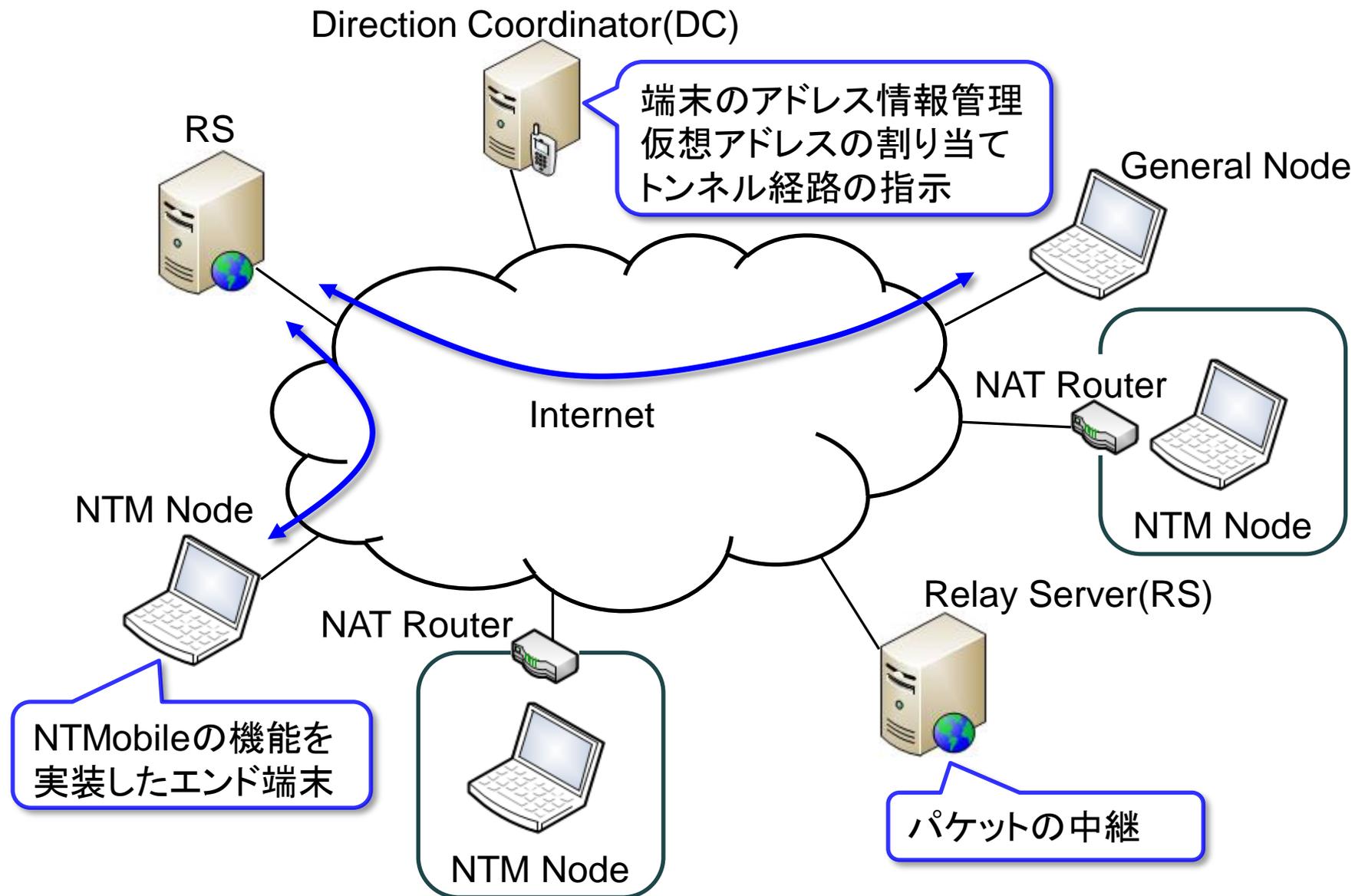
UDPTunnelを使った通信

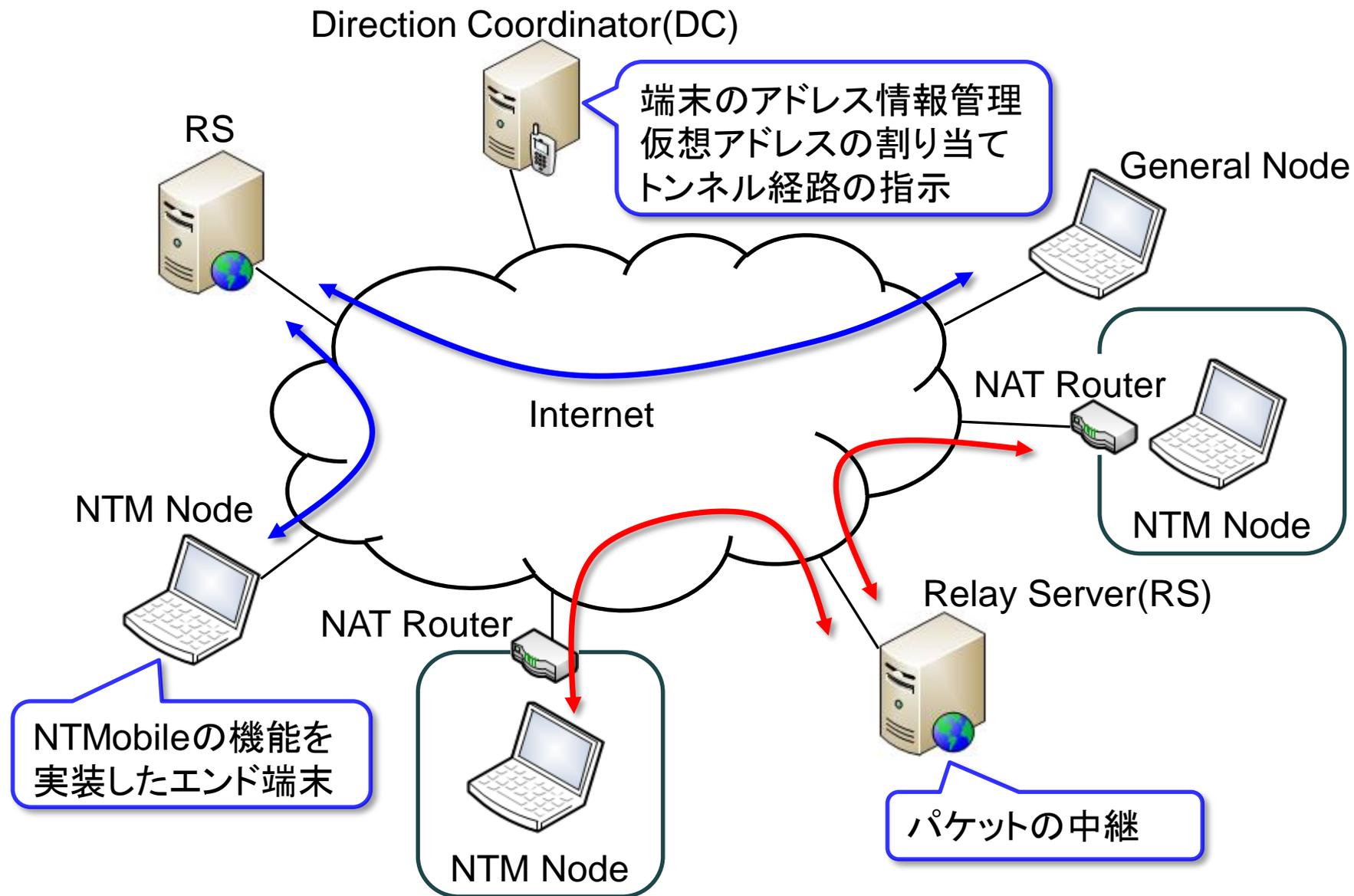


- 通信開始時にUDPTunnelを構築
- 全てのデータパケットをUDPを使ってカプセル化

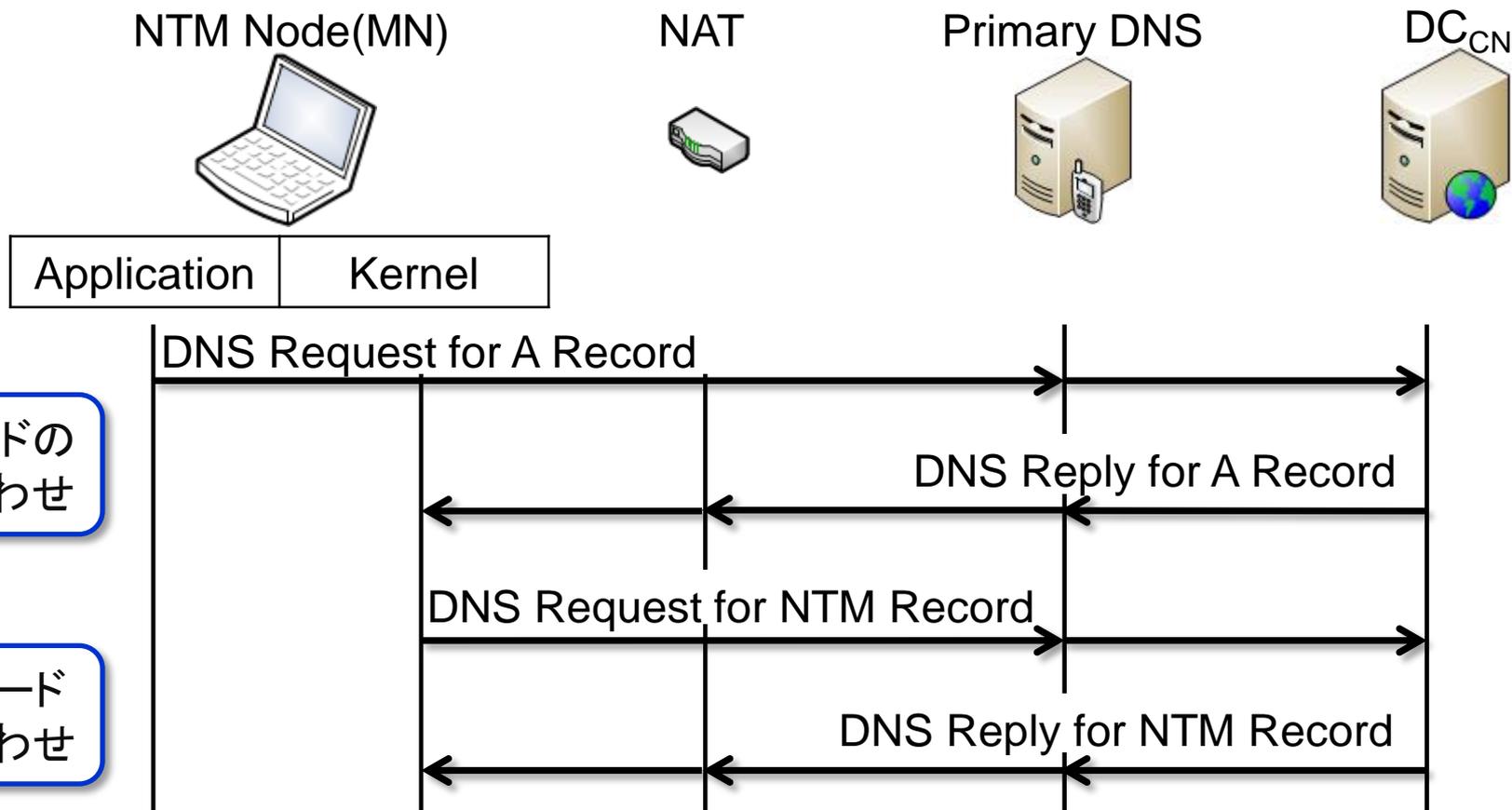




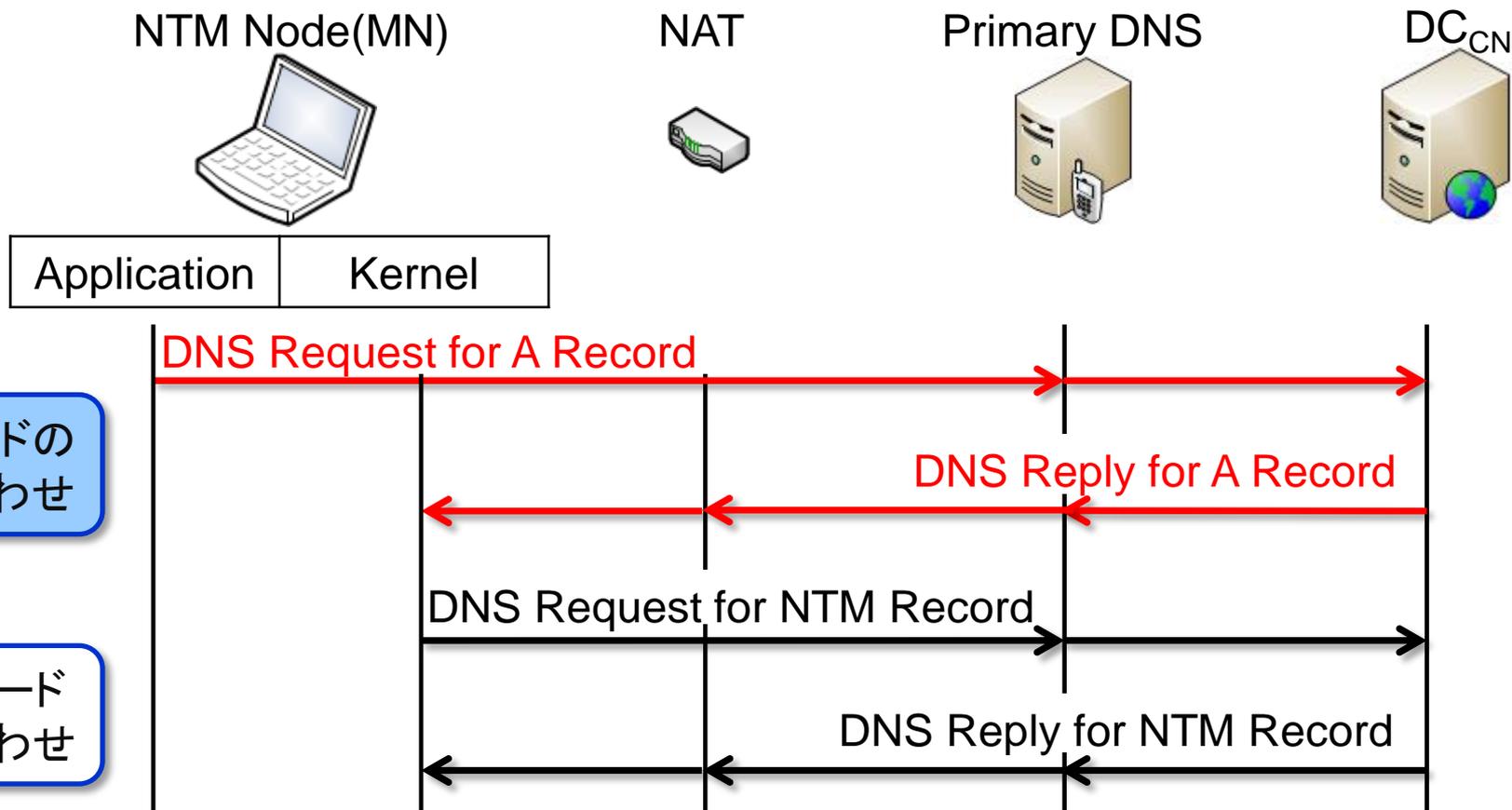




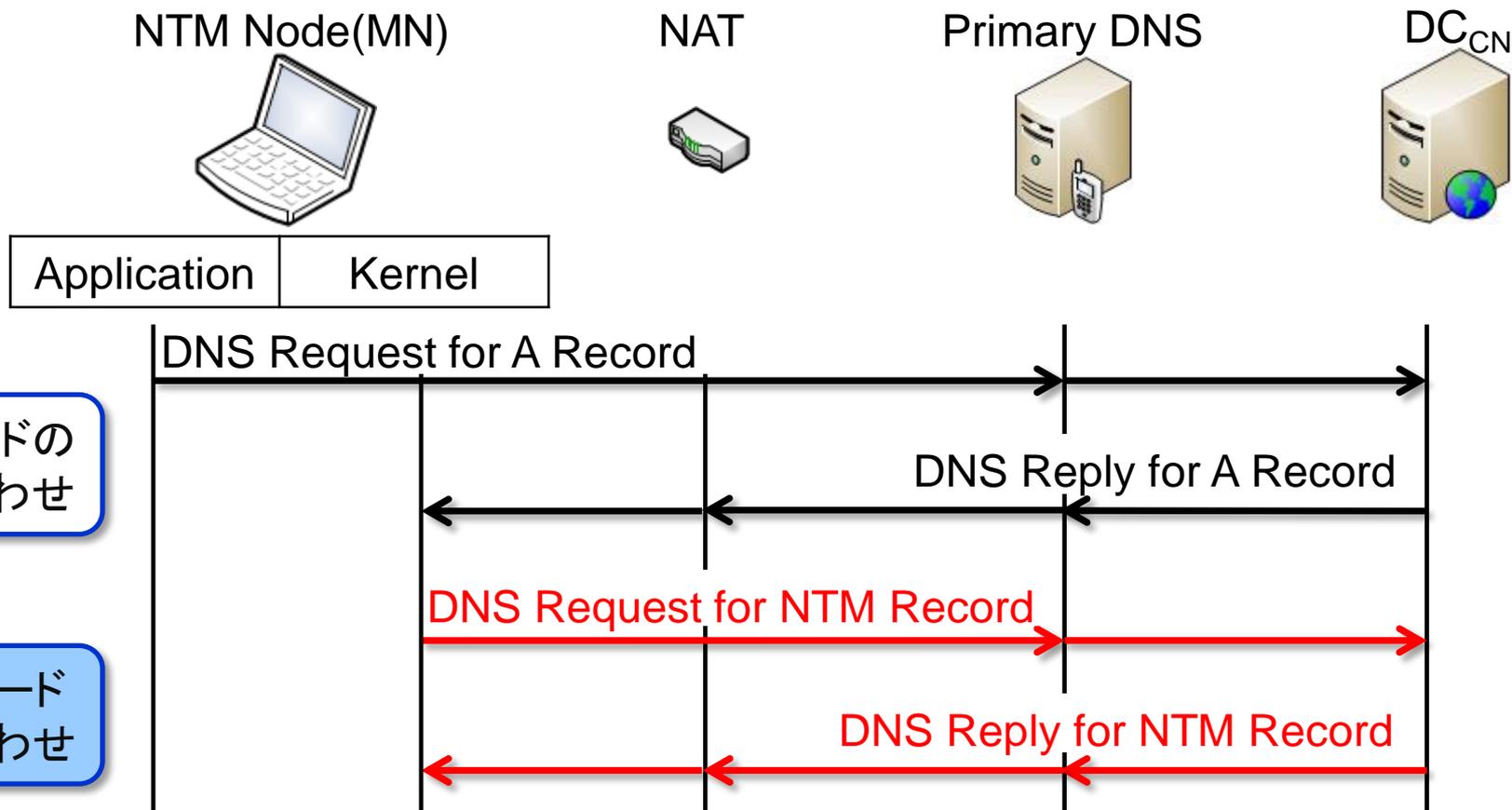
- 通信相手端末の名前を解決する
 - 通信開始時
 - Aレコード問い合わせをフック



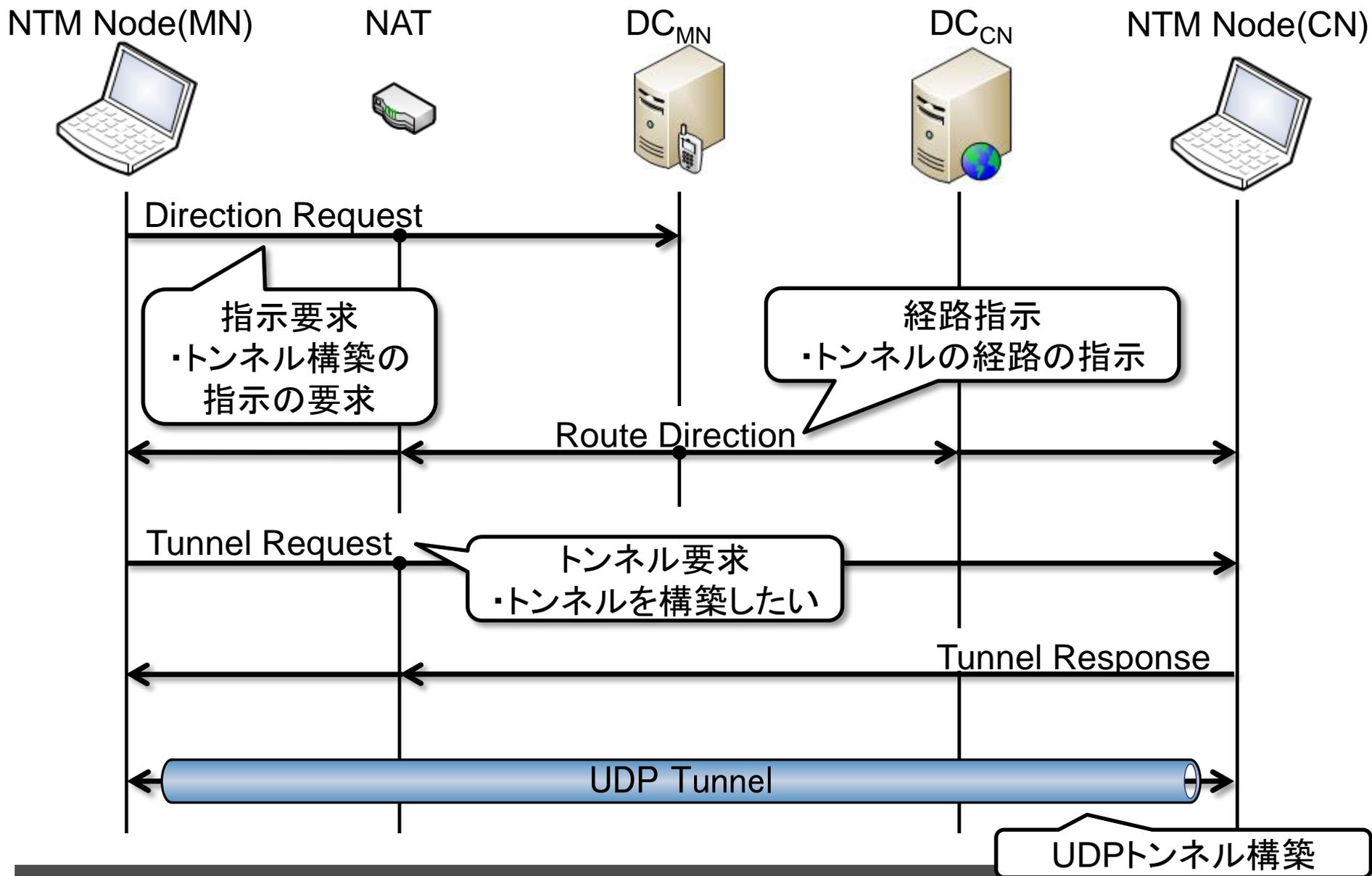
- 通信相手端末の名前を解決する
 - 通信開始時
 - Aレコード問い合わせをフック



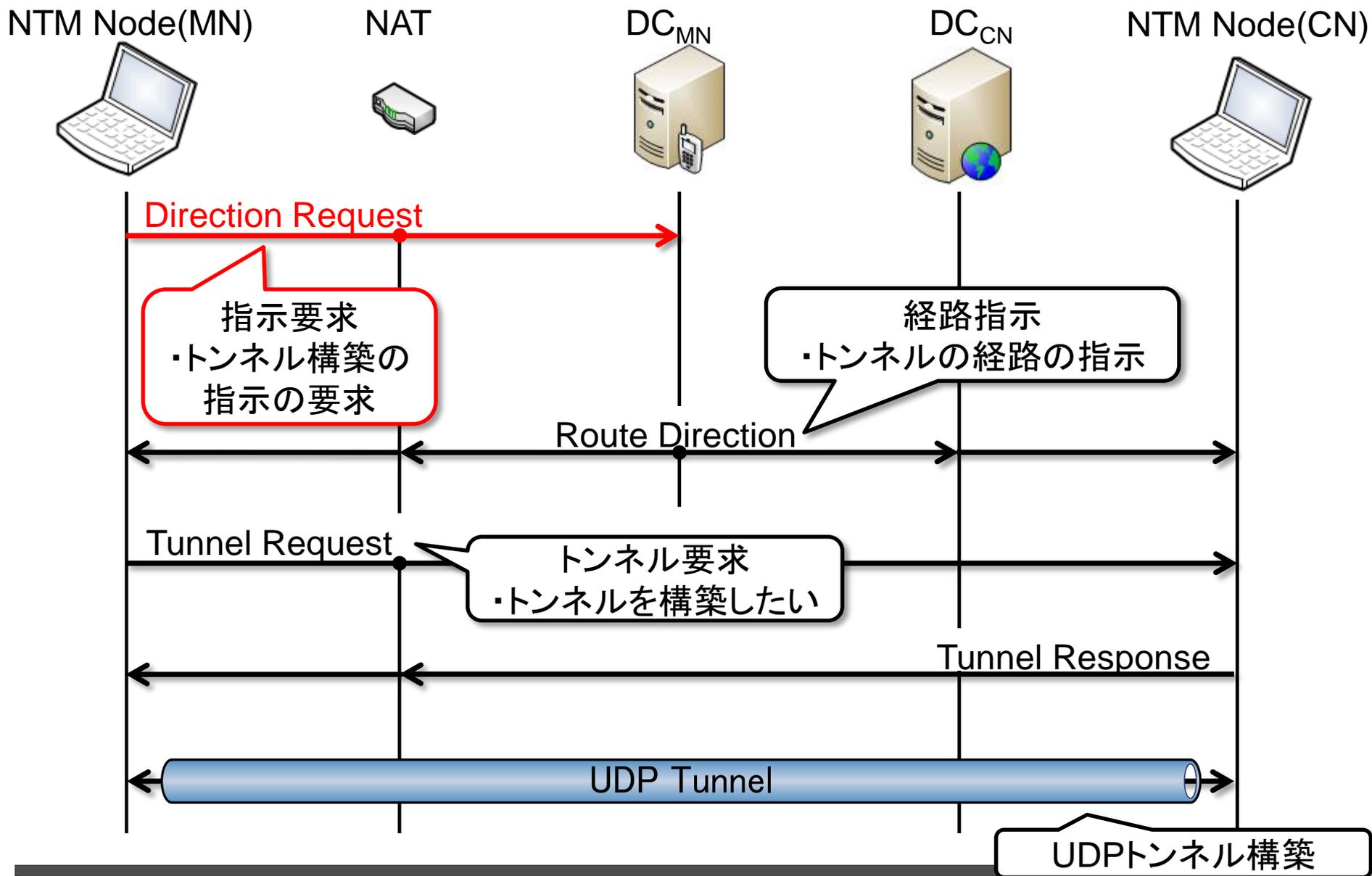
- 通信相手端末の名前を解決する
 - 通信開始時
 - Aレコード問い合わせをフック



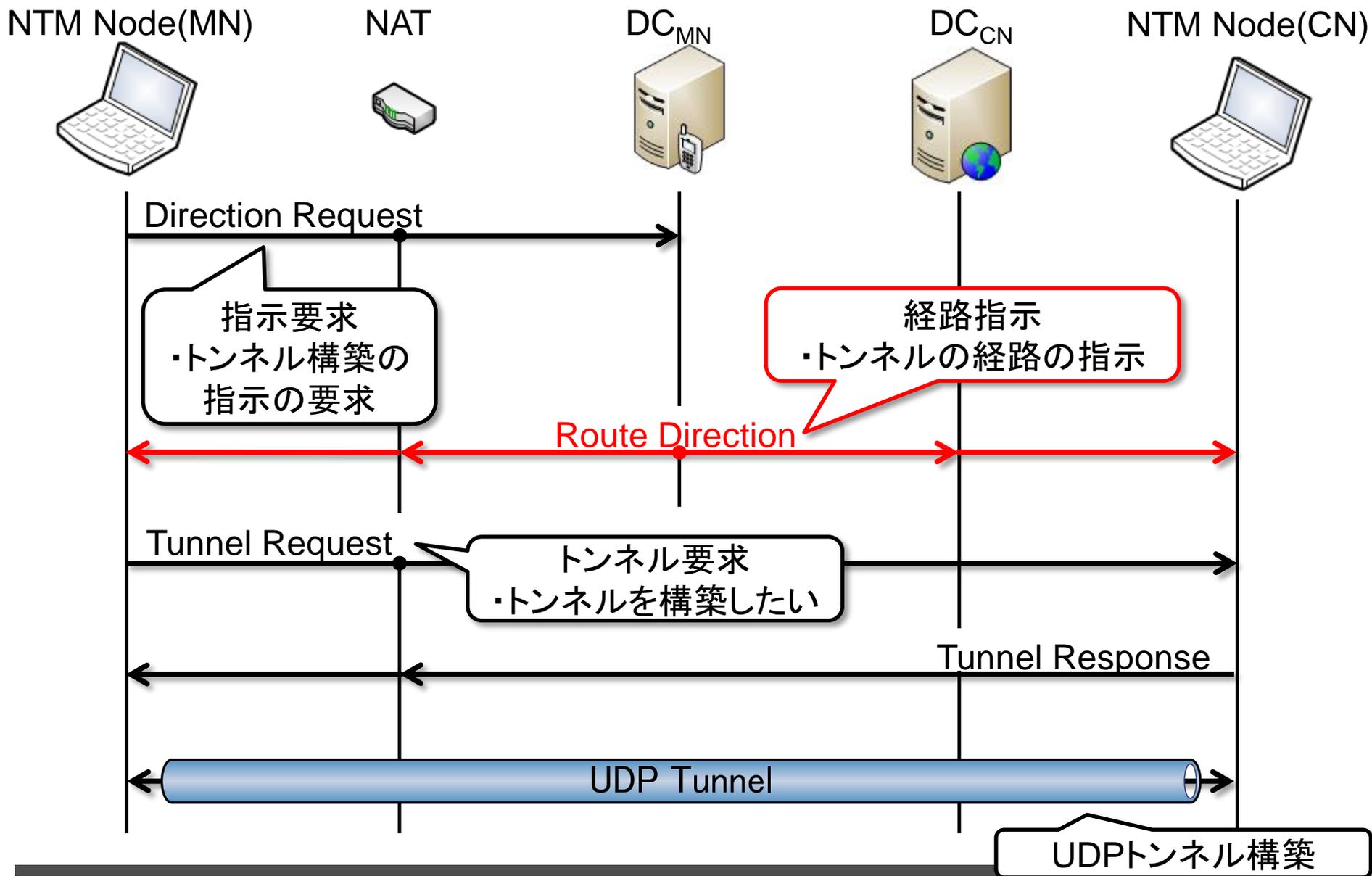
動作シーケンス(2/2) – トンネル構築



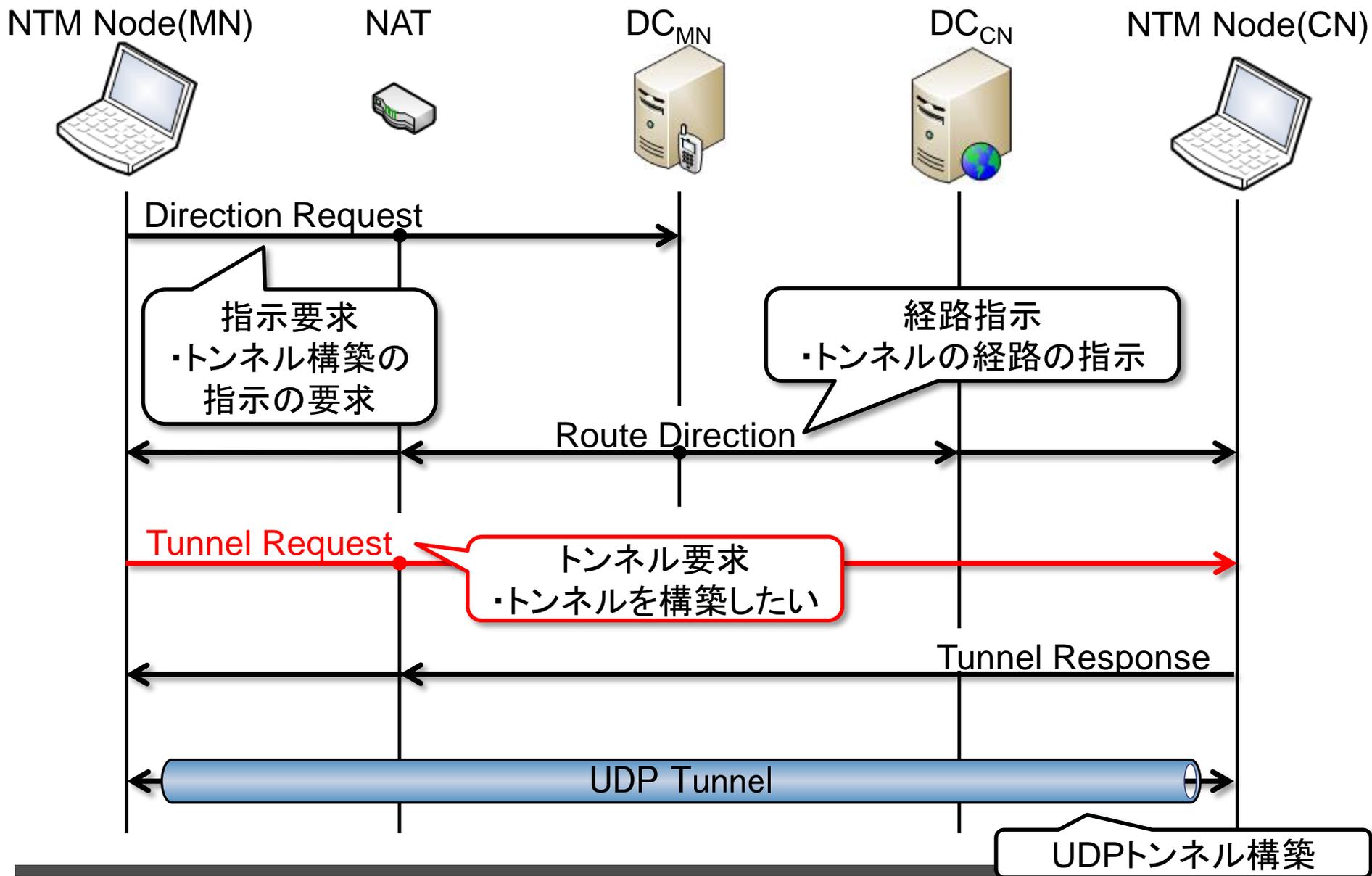
動作シーケンス(2/2) – トンネル構築



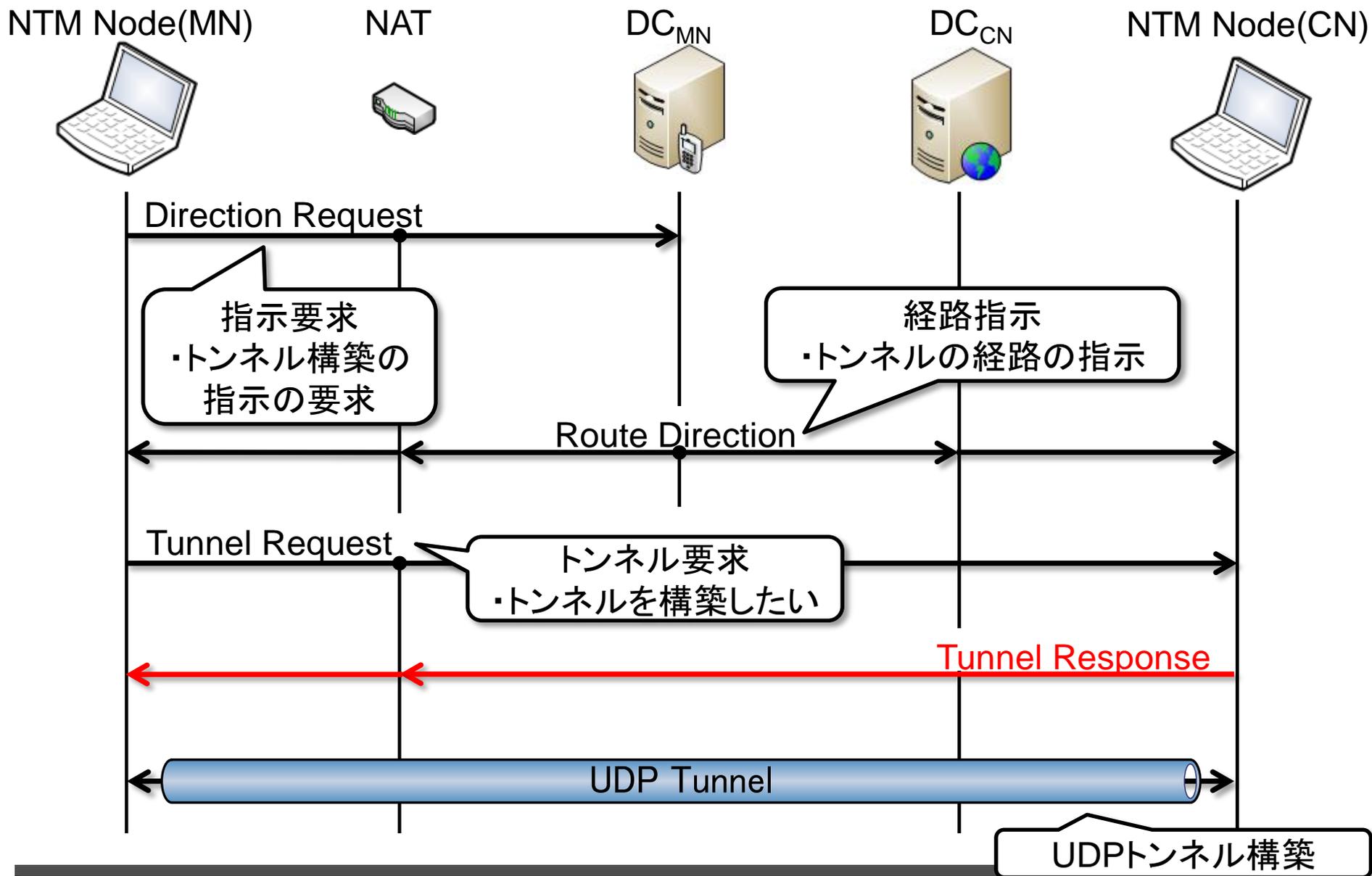
動作シーケンス(2/2) – トンネル構築



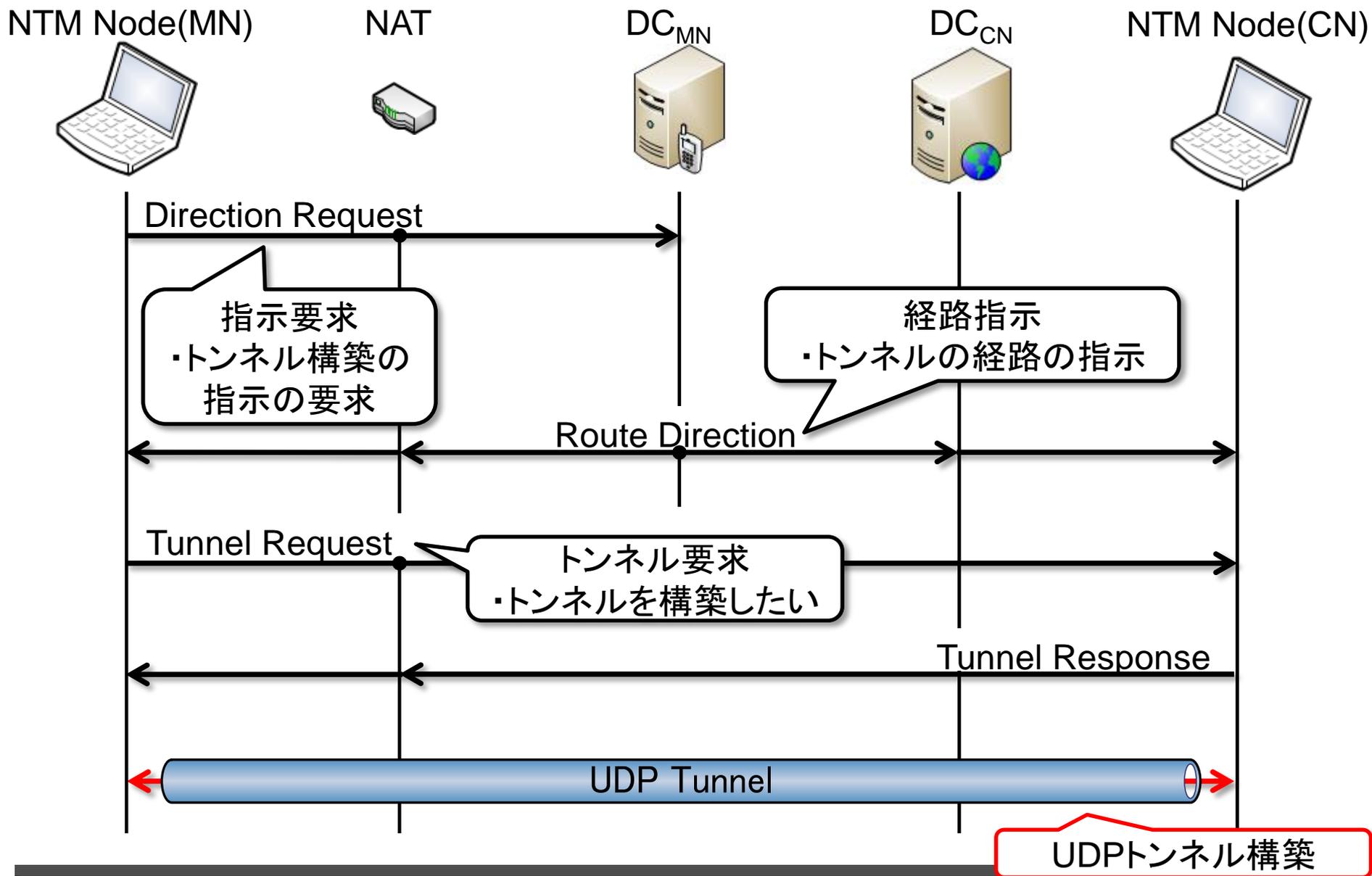
動作シーケンス(2/2) – トンネル構築



動作シーケンス(2/2) – トンネル構築

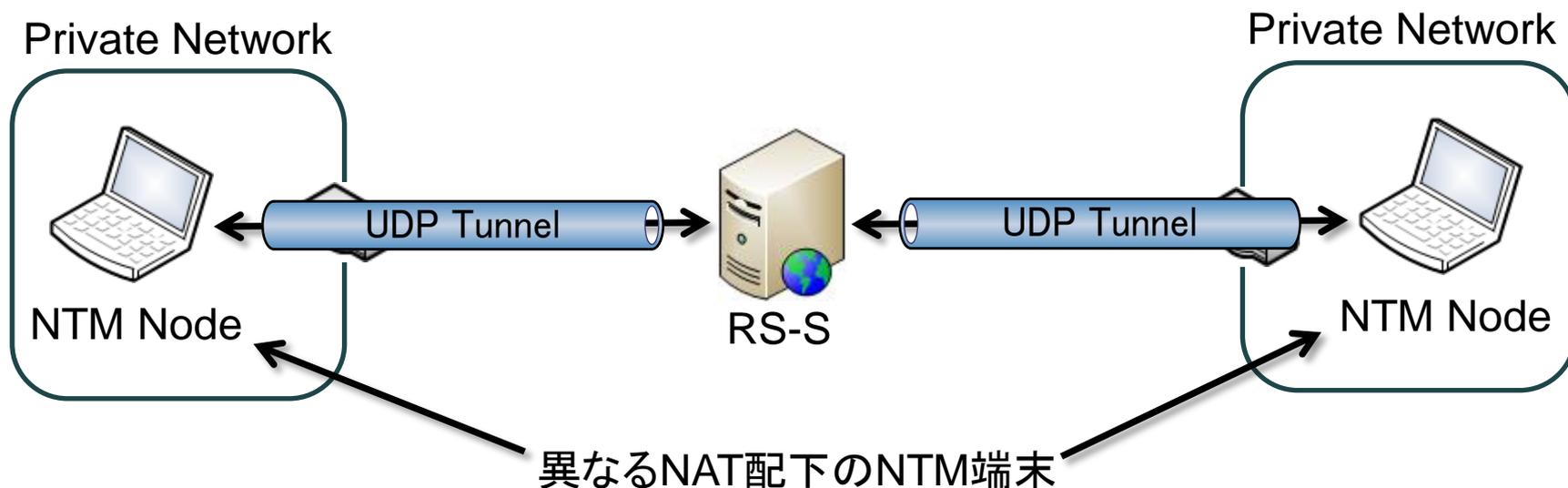


動作シーケンス(2/2) – トンネル構築

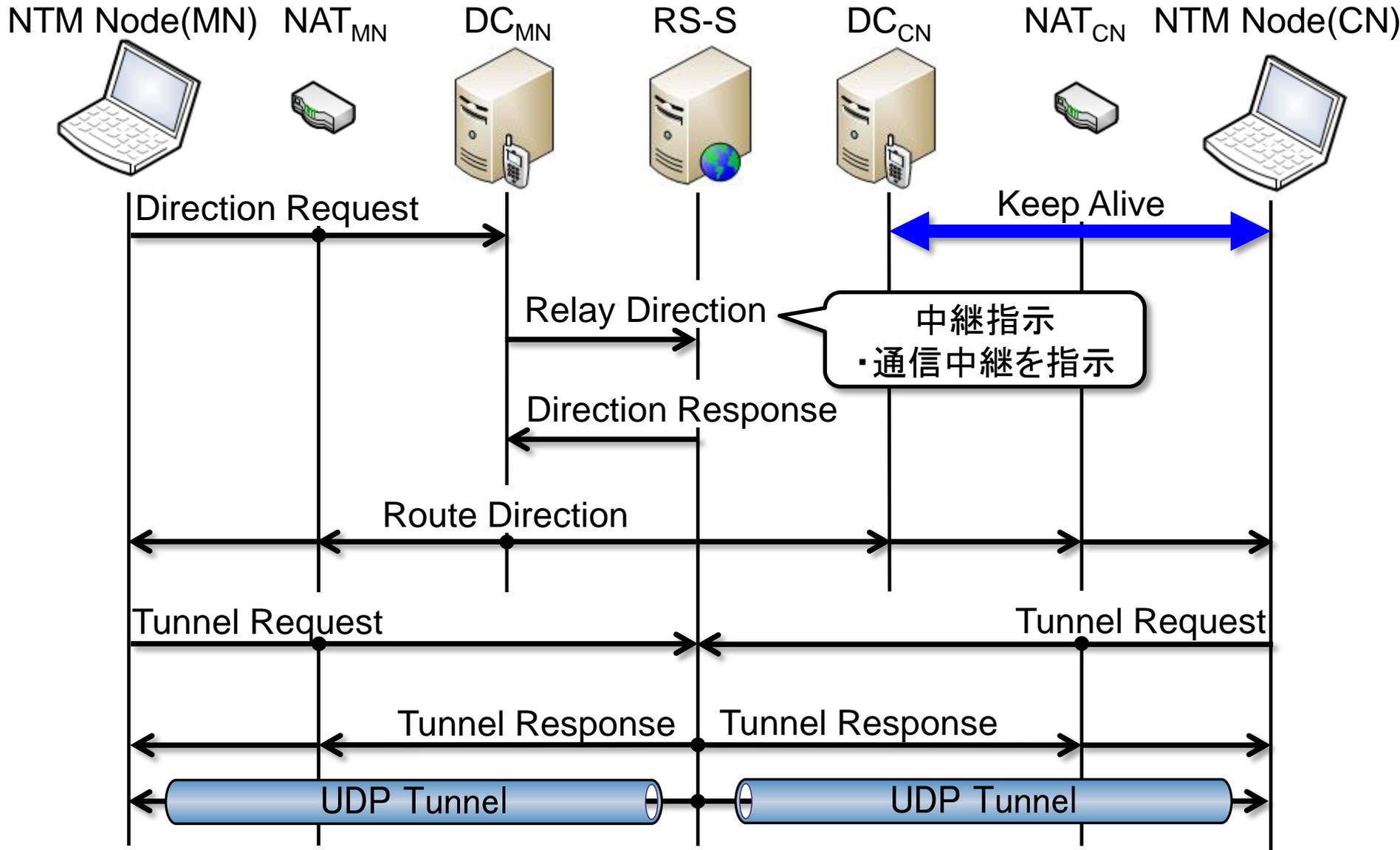


- 特定の条件においてパケットの中継を行うサーバ
- RS-S
 - Relay Server type Switch
 - トンネル切り替え型
- RS-N
 - Relay Server type NAT
 - アドレス変換型
- RS-T
 - Relay Server type Transparent
 - アドレス無変換型

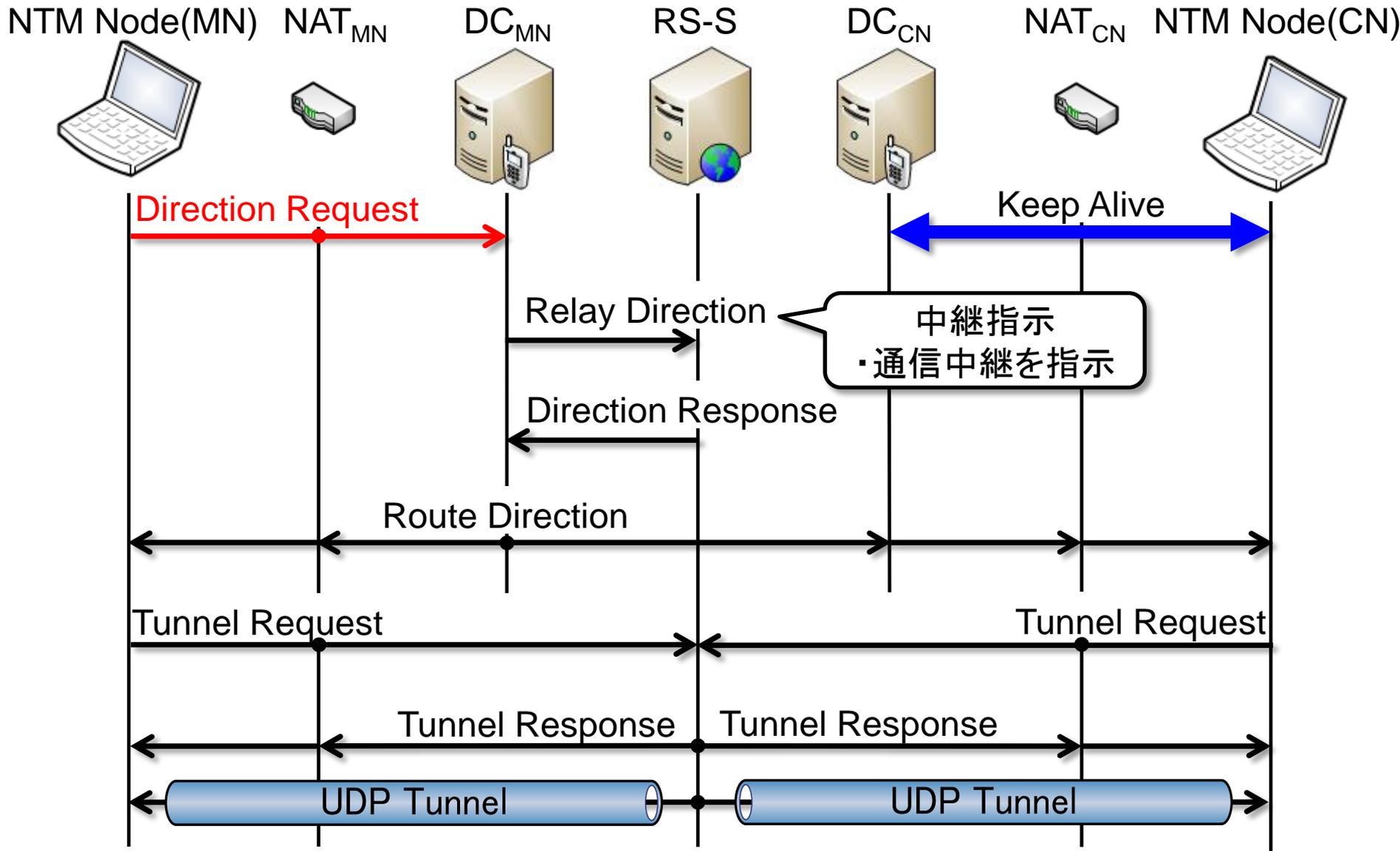
- RS-S(RS type Switch)
 - トンネル切り替え型RS
 - NTM端末が異なるNAT配下に存在する場合に利用
- 双方のNTM端末との間にUDPTunnelを構築
- 直接通信が出来る場合は経路の切り替えも可能



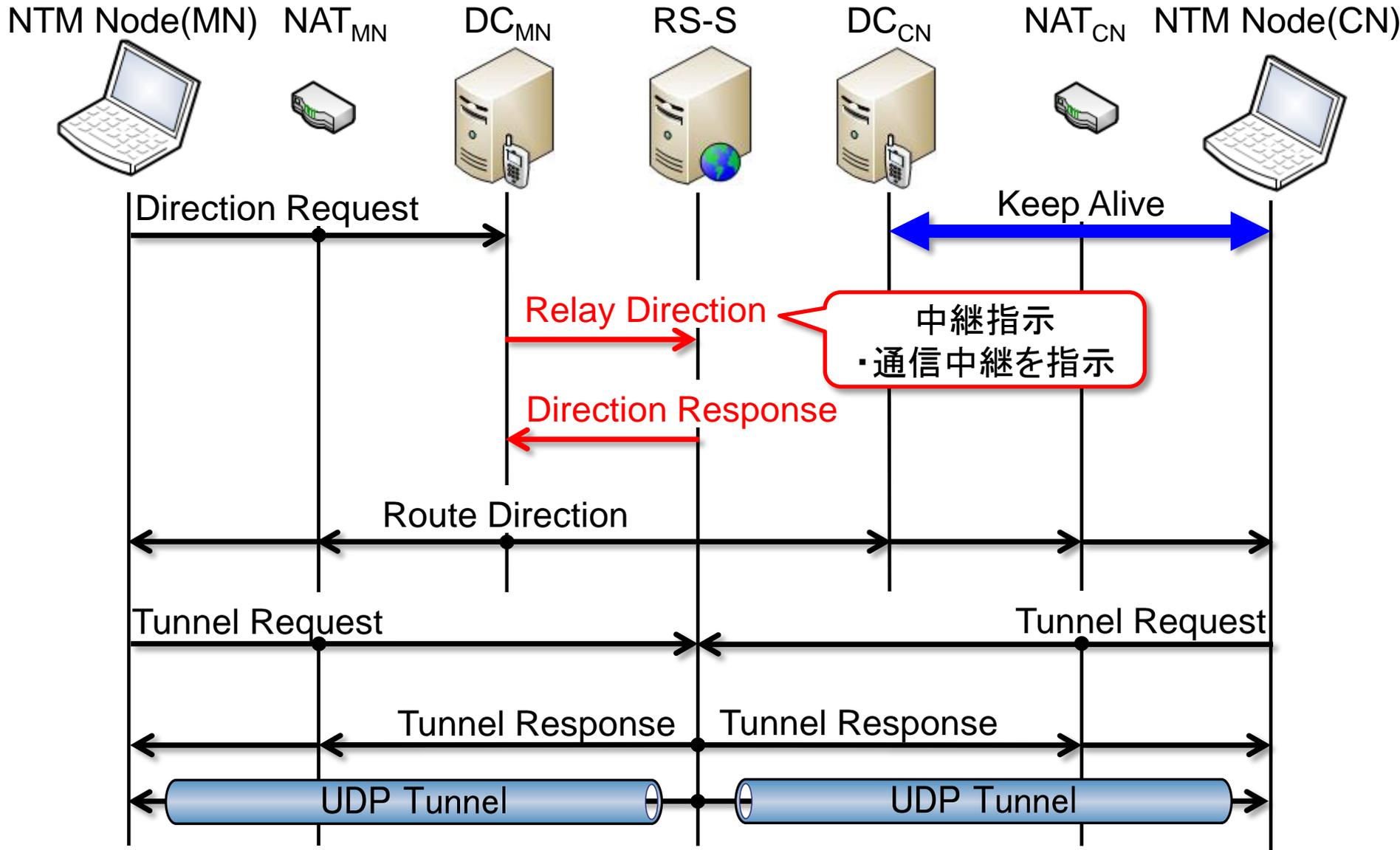
トンネル構築シーケンス



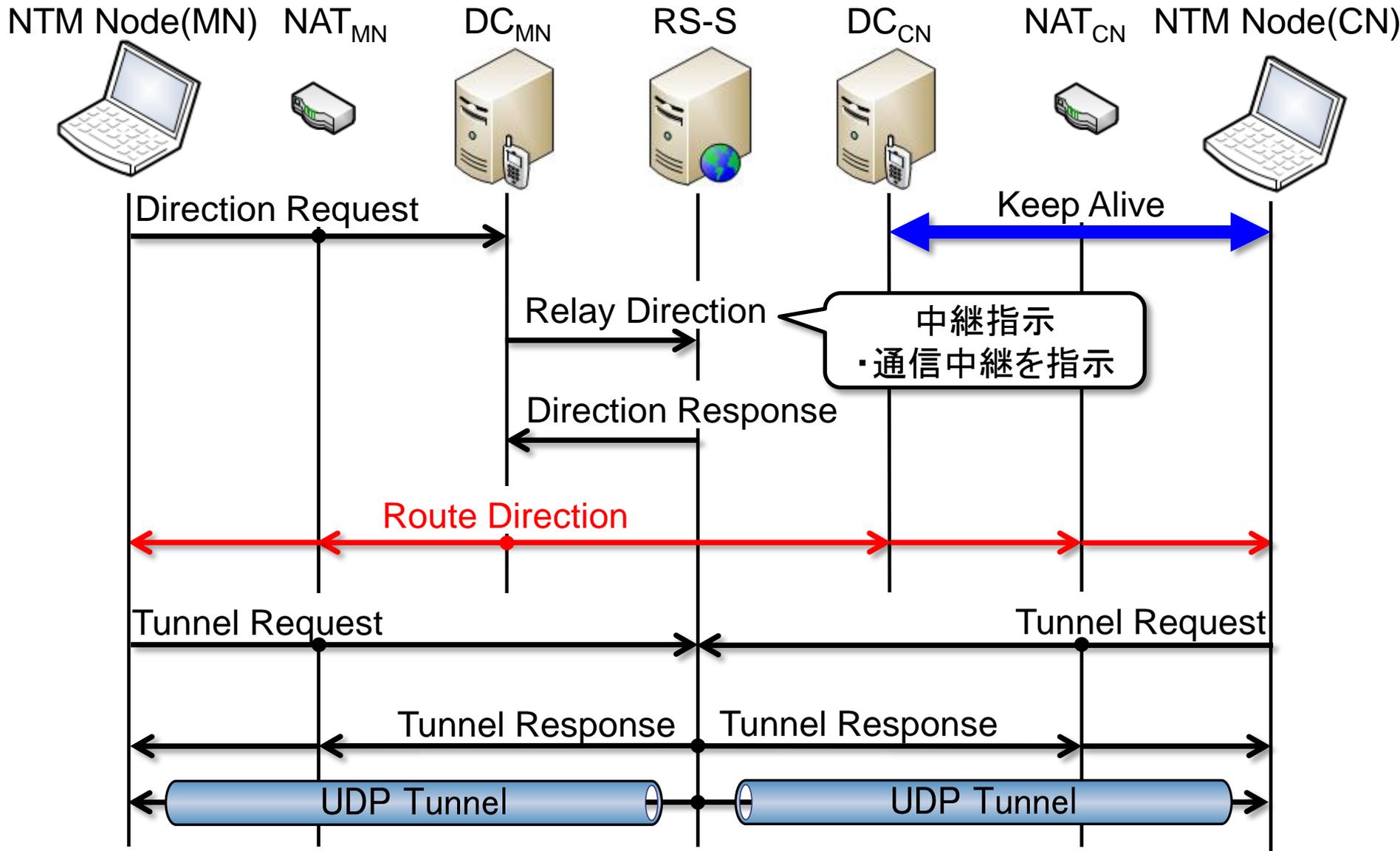
トンネル構築シーケンス



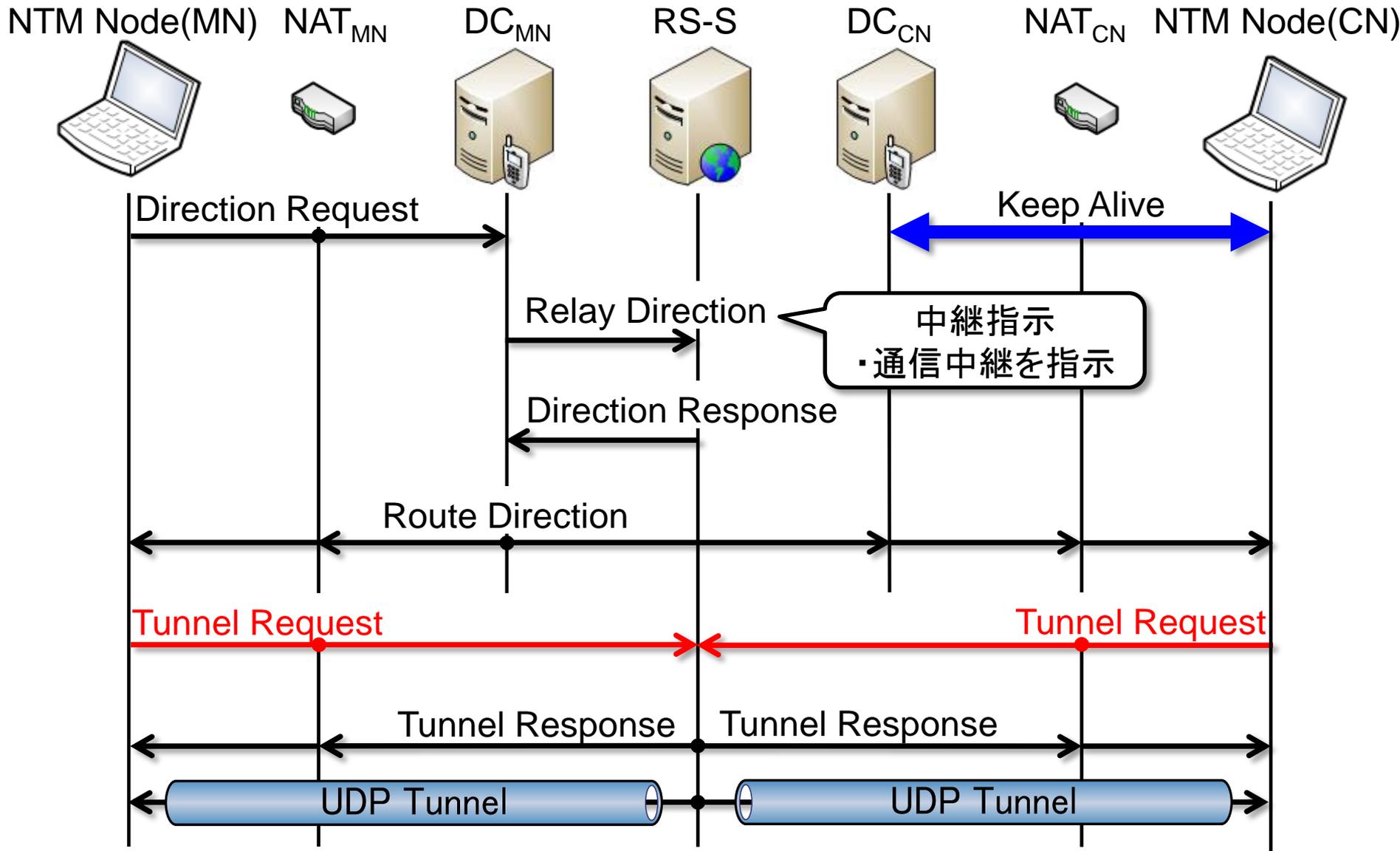
トンネル構築シーケンス



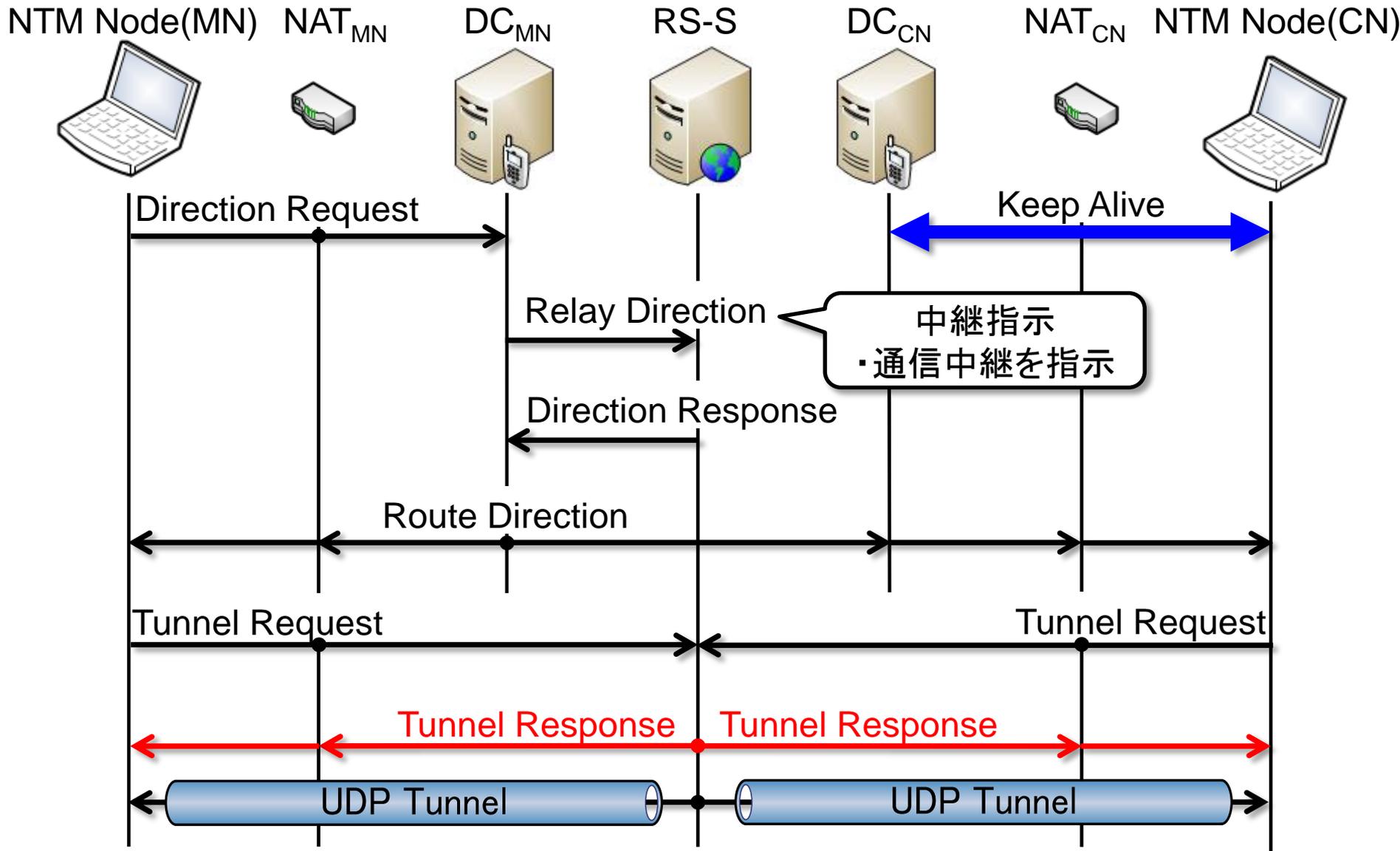
トンネル構築シーケンス



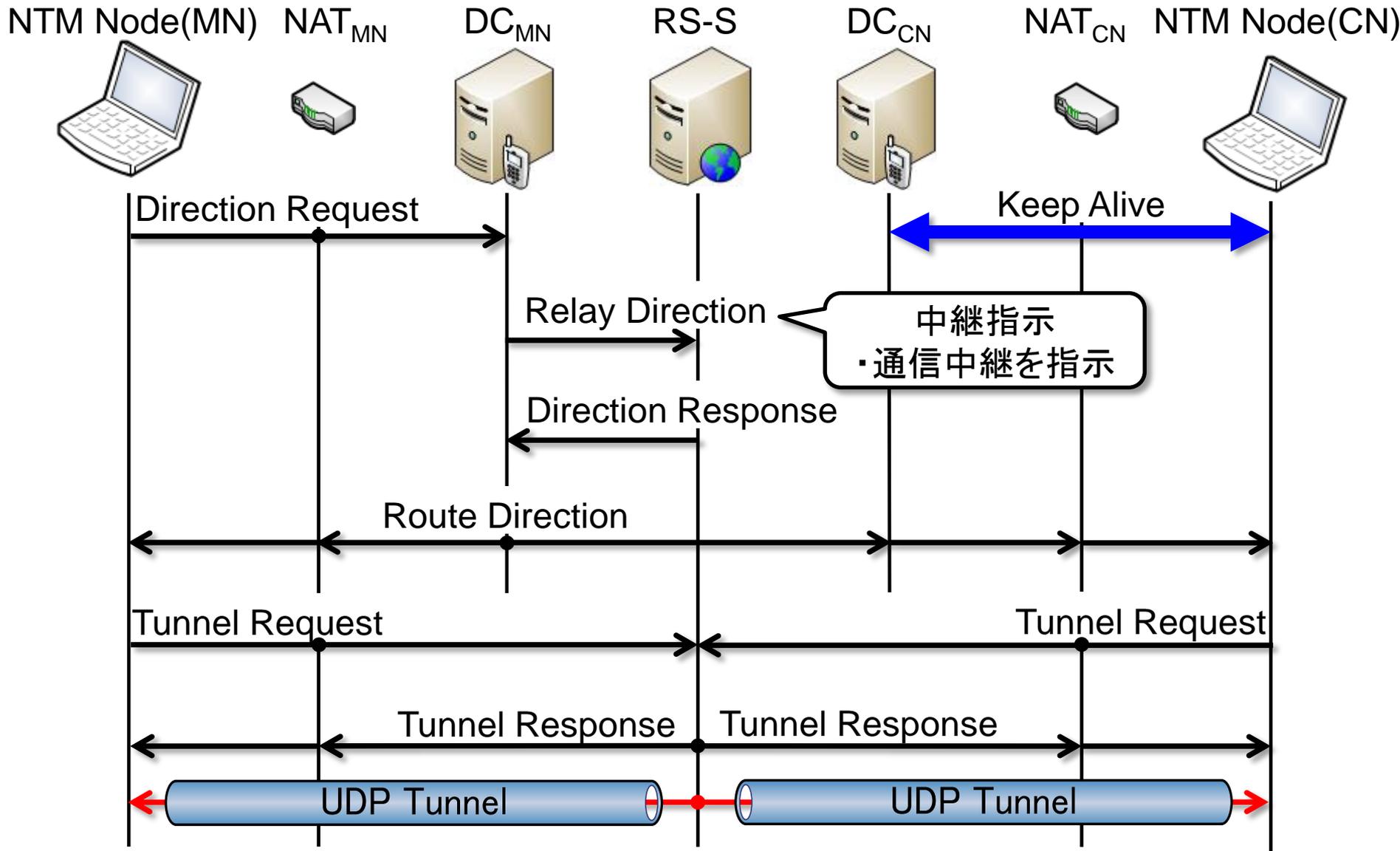
トンネル構築シーケンス



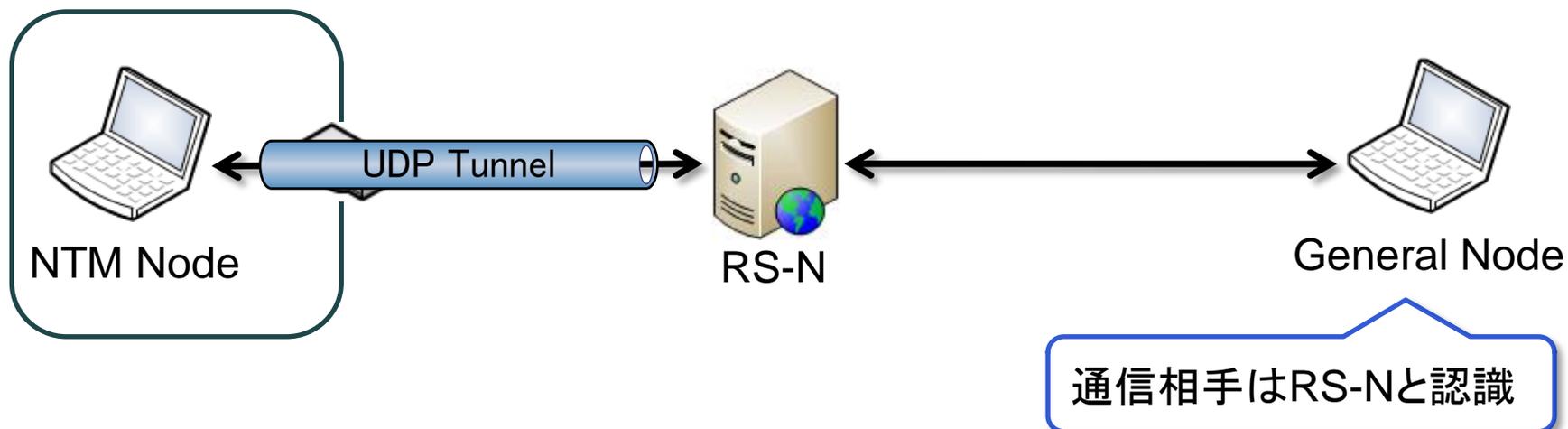
トンネル構築シーケンス



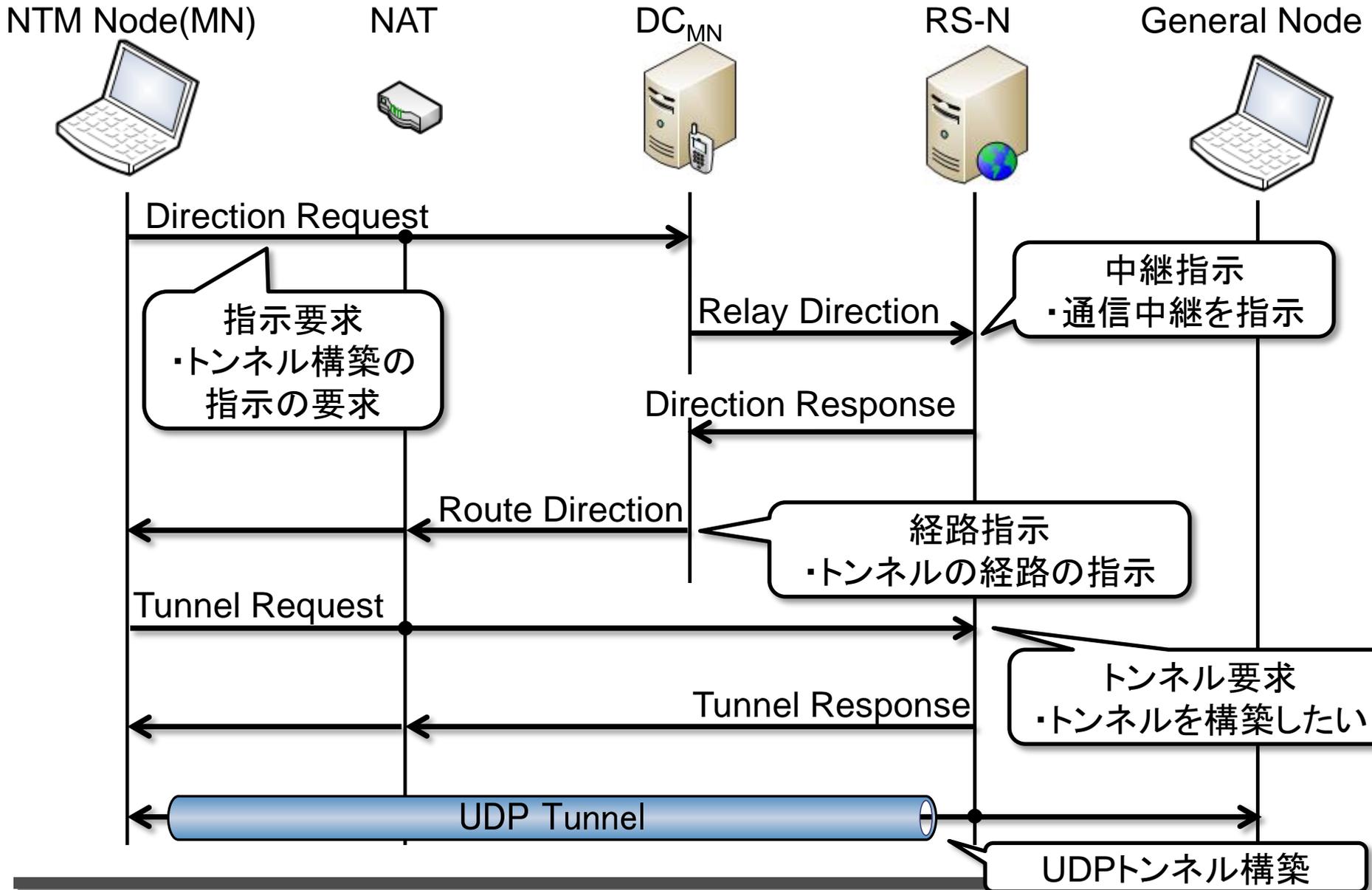
トンネル構築シーケンス



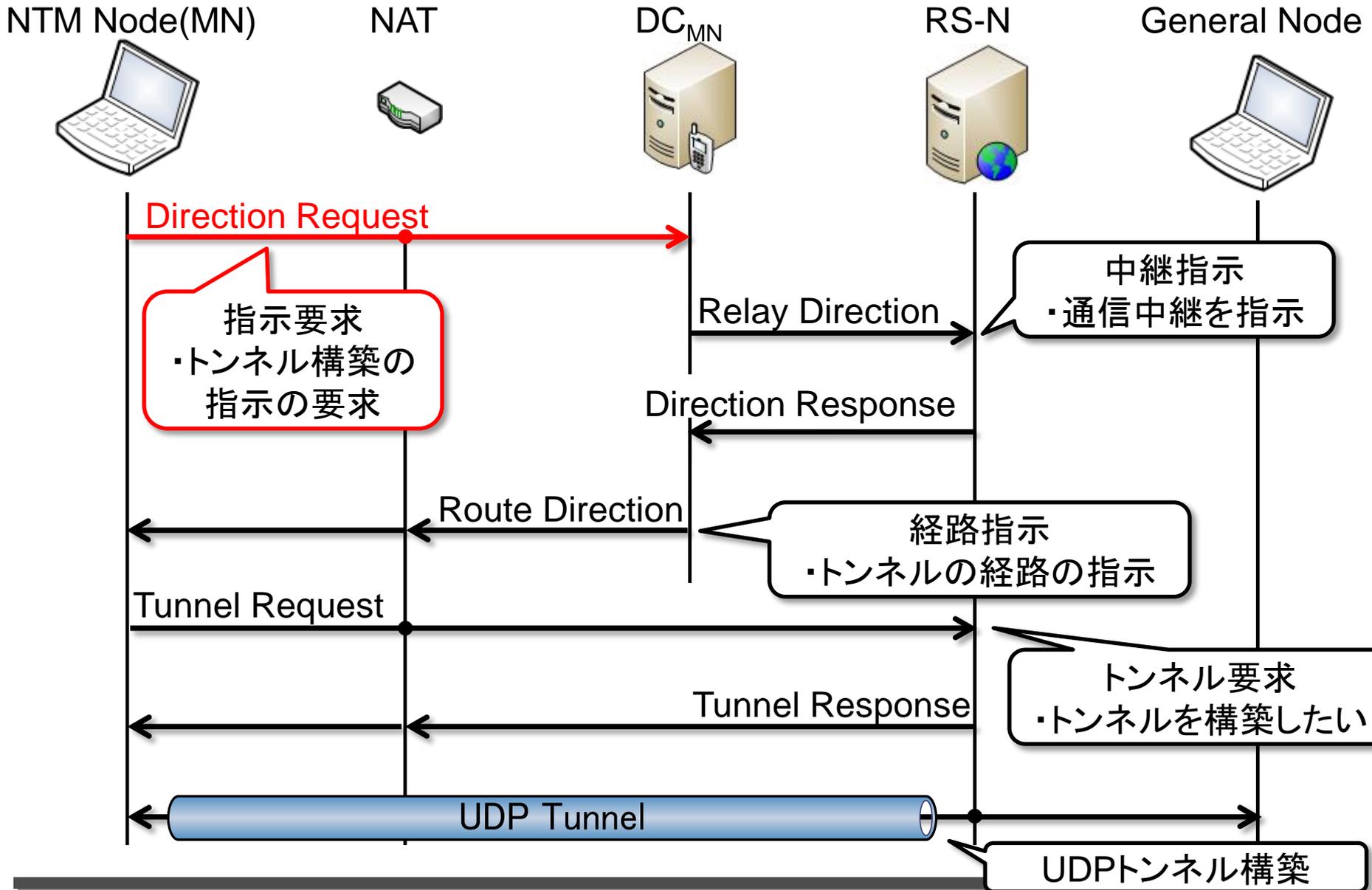
- RS-N(RS type NAT)
 - アドレス変換(NAT)型RS
 - 通信相手端末が一般端末の場合に利用
- NTM端末との間にUDPTunnelを構築
- 一般端末はRS-Nを通信相手と認識



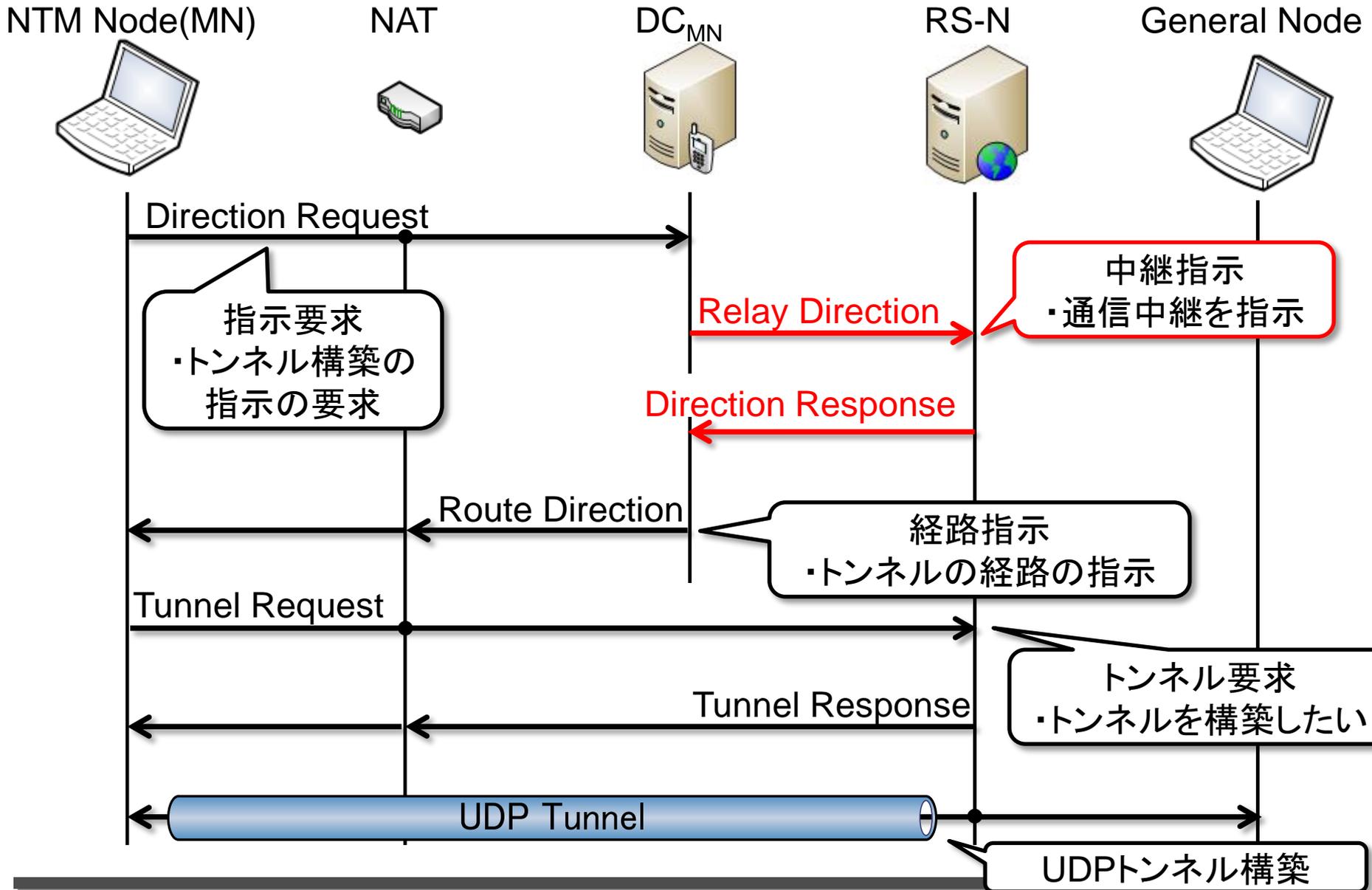
トンネル構築シーケンス



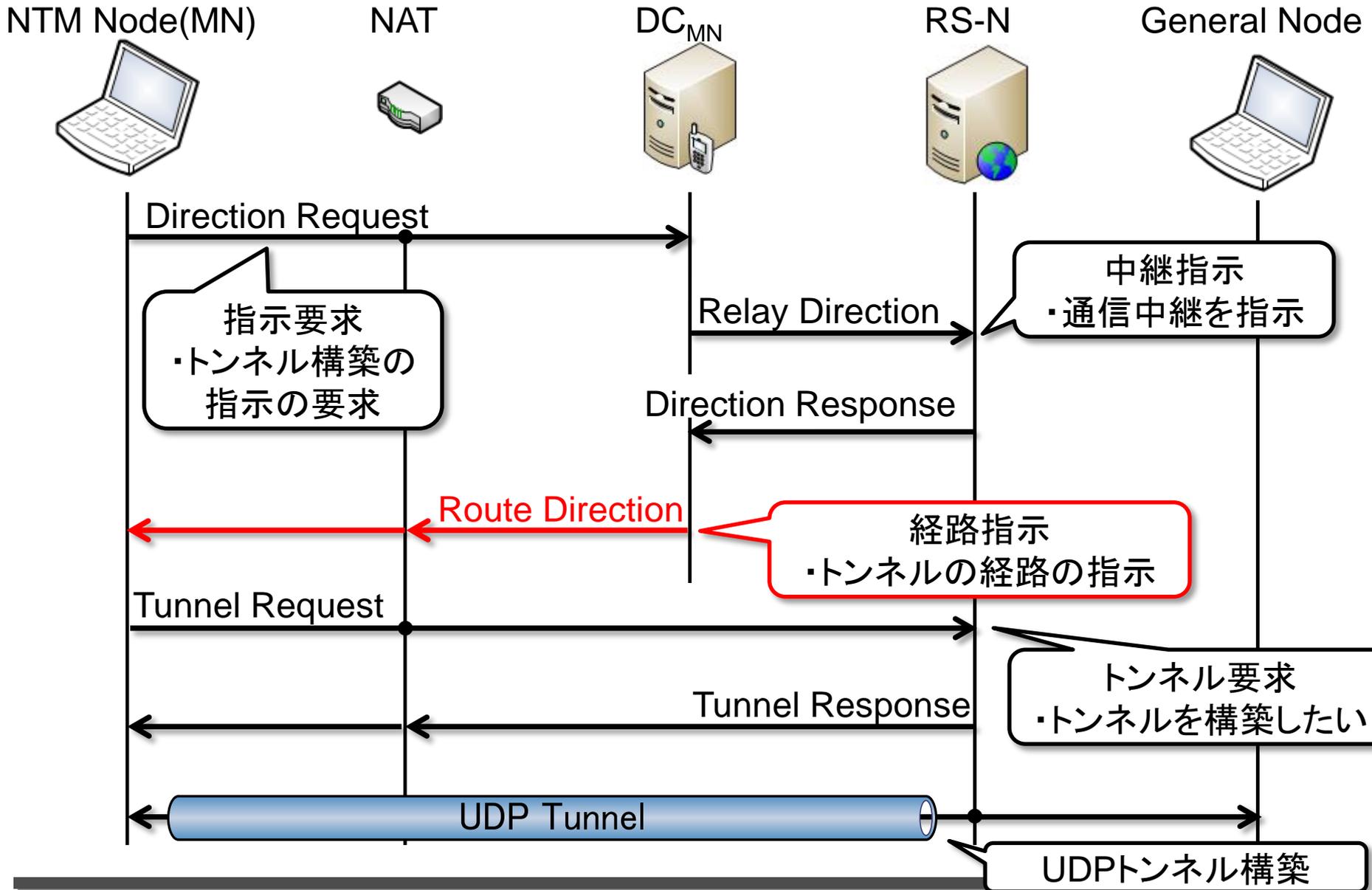
トンネル構築シーケンス



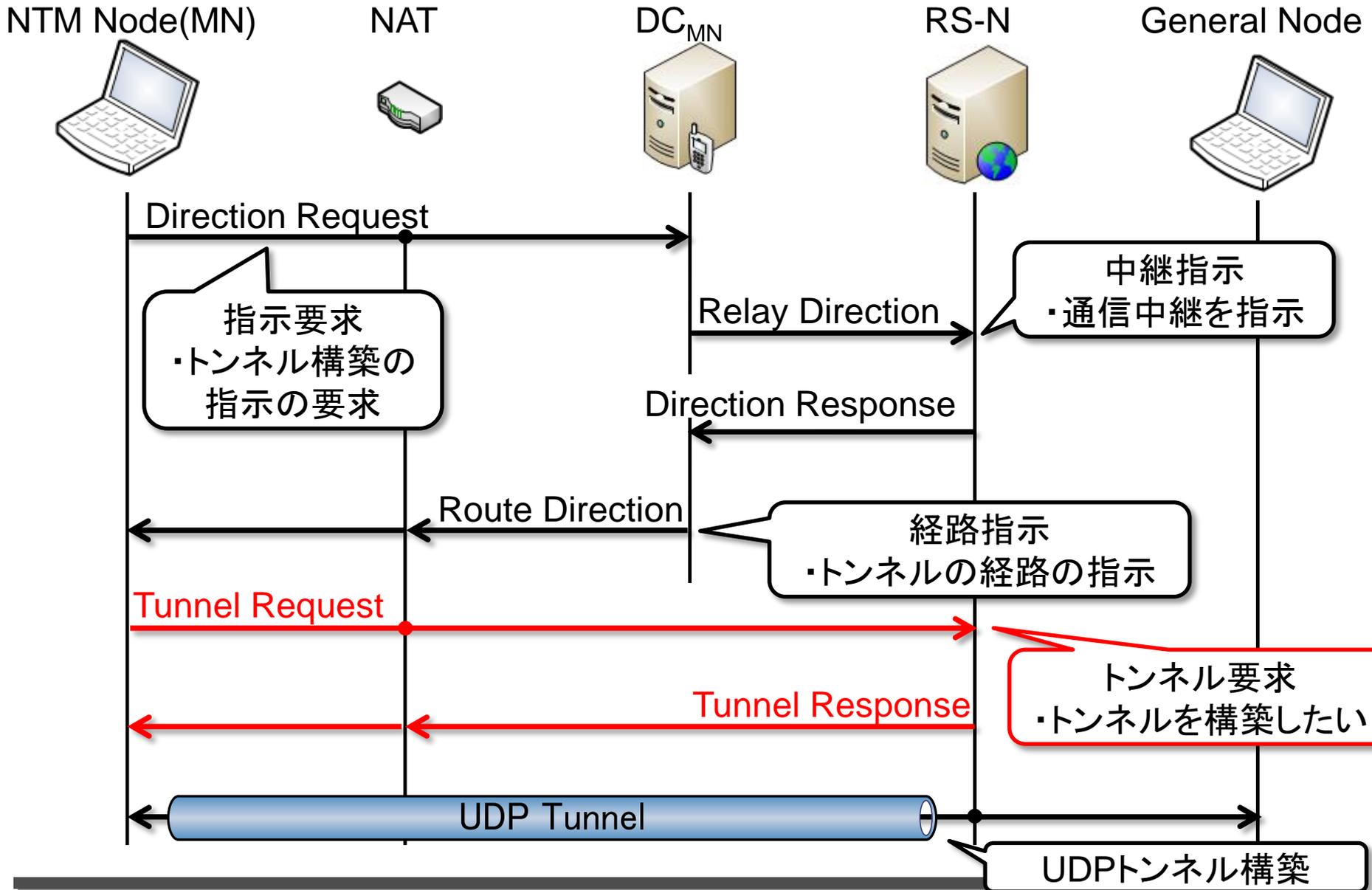
トンネル構築シーケンス



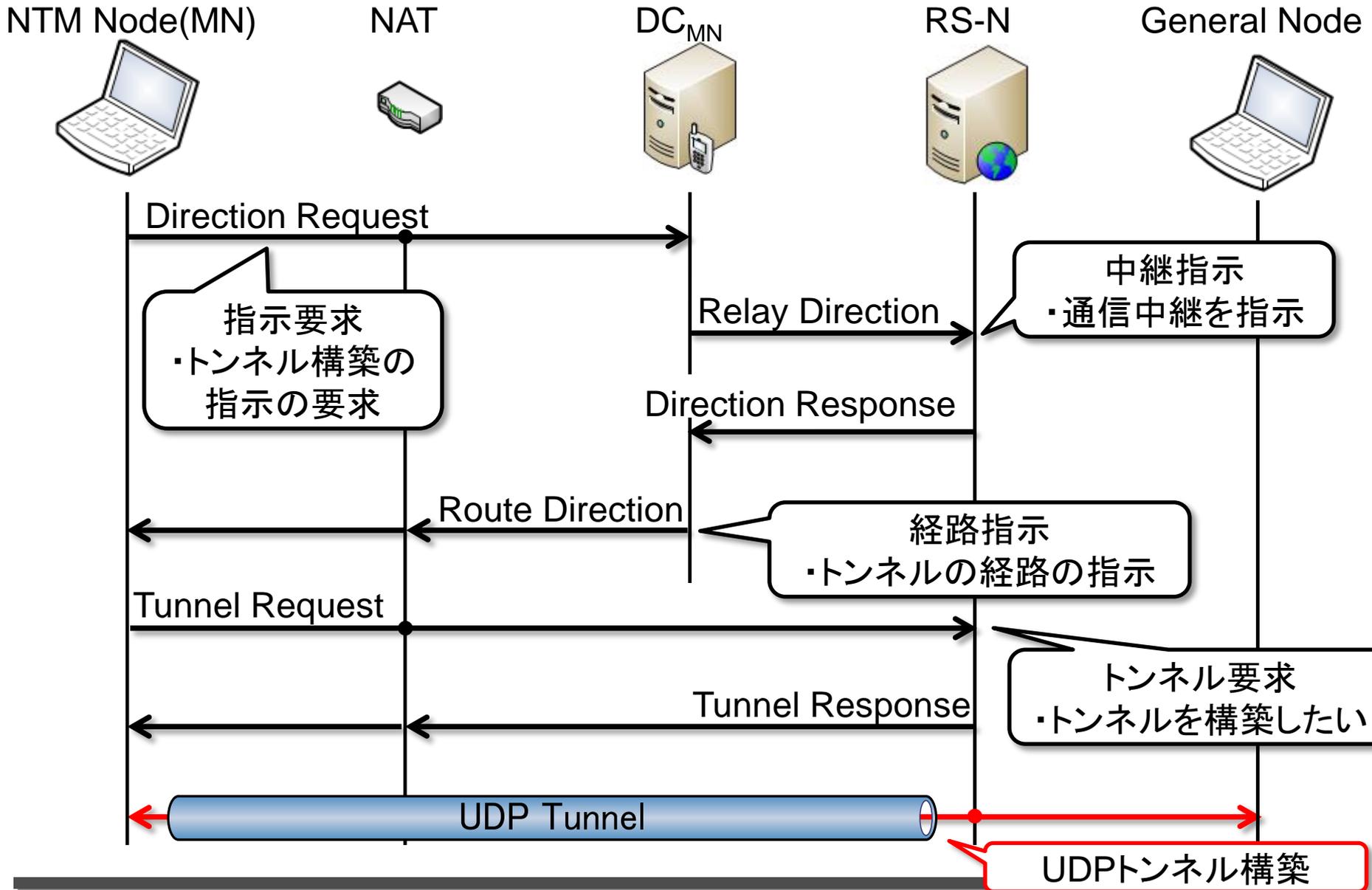
トンネル構築シーケンス



トンネル構築シーケンス



トンネル構築シーケンス

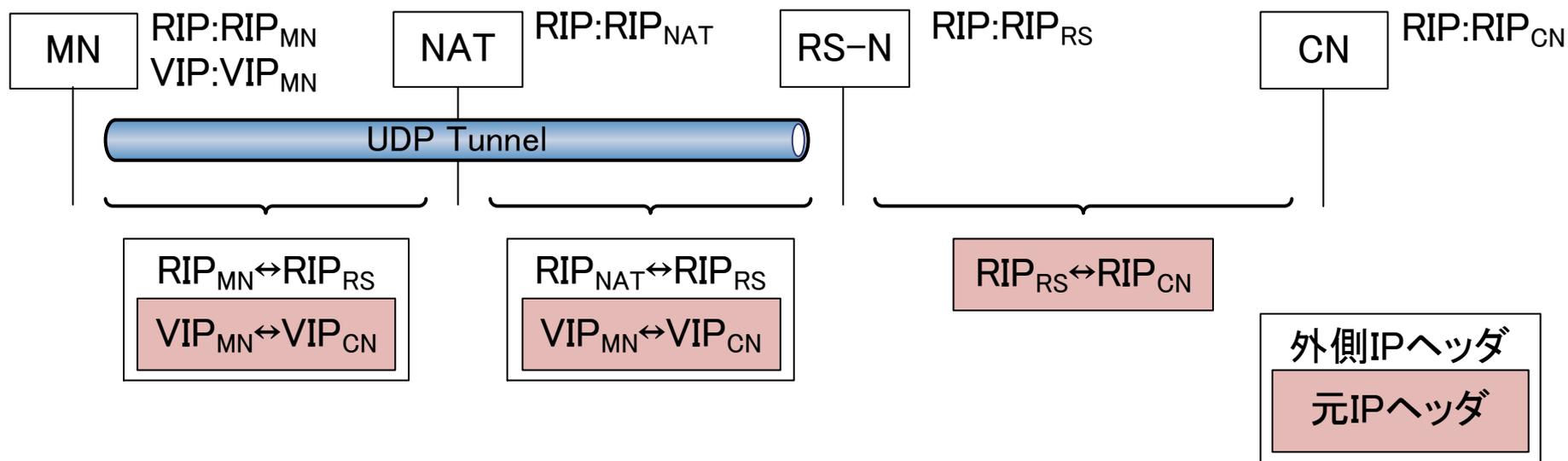


- RS-N(Relay Server NAT type)

- アドレス変換型
- 受信したパケットをデカプセル化 + アドレス変換

MN(Mobile Node)
CN(Correspondent Node)

- MN(NTM端末)からCN(一般端末)への通信開始



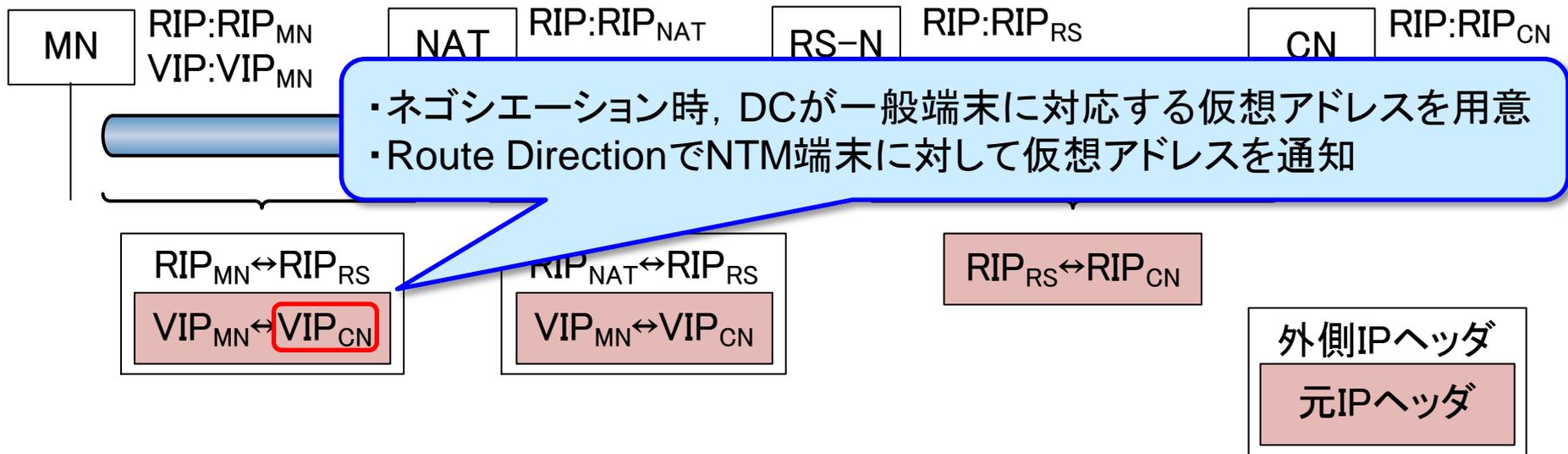
RIP:実IPアドレス VIP:仮想IPアドレス

- RS-N(Relay Server NAT type)

- アドレス変換型
- 受信したパケットをデカプセル化 + アドレス変換

MN(Mobile Node)
CN(Correspondent Node)

- MN(NTM端末)からCN(一般端末)への通信開始



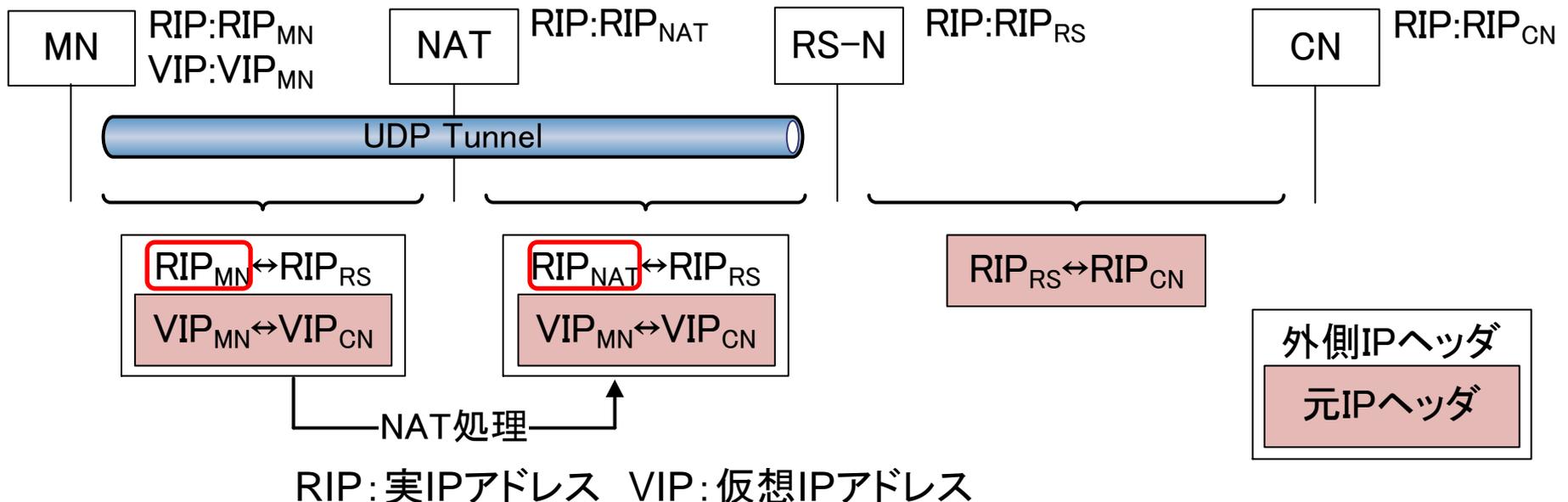
RIP:実IPアドレス VIP:仮想IPアドレス

- RS-N(Relay Server NAT type)

- アドレス変換型
- 受信したパケットをデカプセル化 + アドレス変換

MN(Mobile Node)
CN(Correspondent Node)

- MN(NTM端末)からCN(一般端末)への通信開始

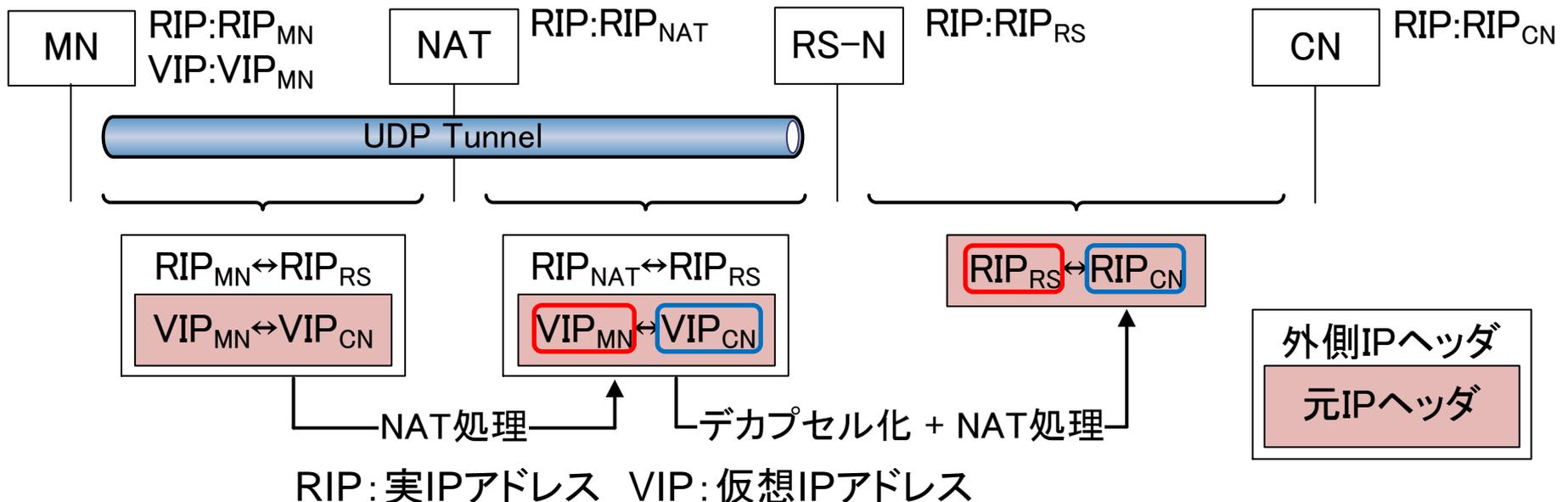


- RS-N(Relay Server NAT type)

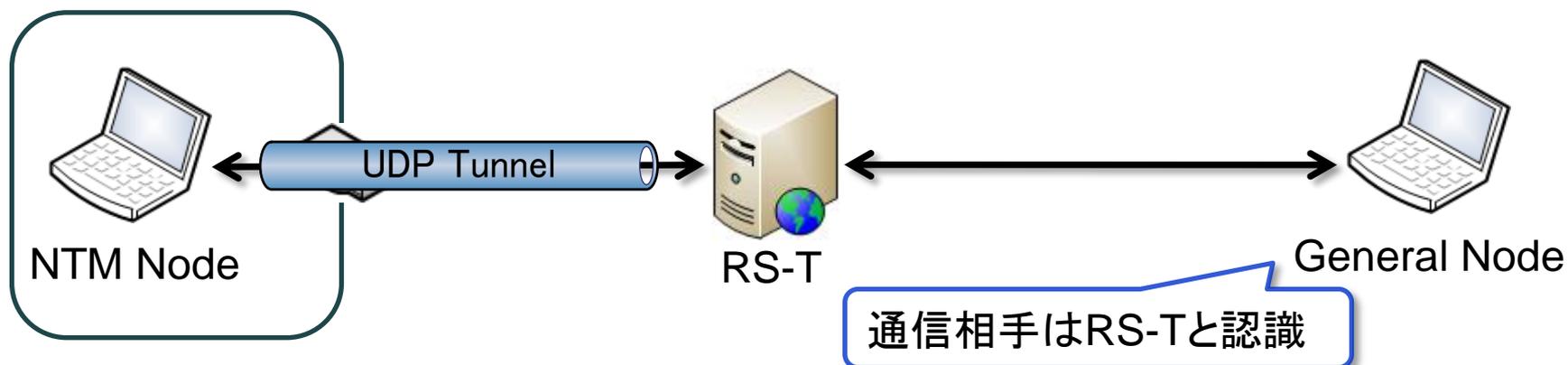
- アドレス変換型
- 受信したパケットをデカプセル化 + アドレス変換

MN(Mobile Node)
CN(Correspondent Node)

- MN(NTM端末)からCN(一般端末)への通信開始

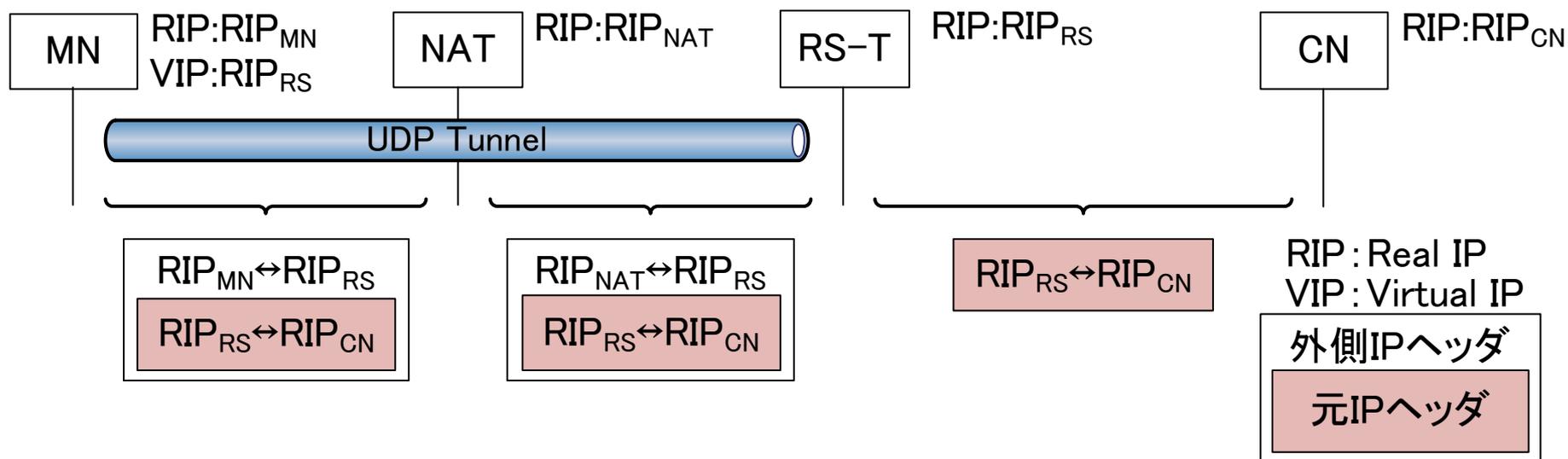


- RS-T(RS type Transparent)
 - アドレス無変換型RS
 - 通信相手端末が一般端末
 - ペイロードにIPアドレスを含むアプリケーションを使用
 - 本発表では主にSIP(Session Initiation Protocol)の事を指す.
- RS-Nでアドレス変換が行われる時
 - ペイロード内のアドレスは変換されない
 - ヘッダのアドレスとペイロードのアドレスが異なる



- MN(NTM端末)からCN(一般端末)への通信開始

MN(Mobile Node)
CN(Correspondent Node)

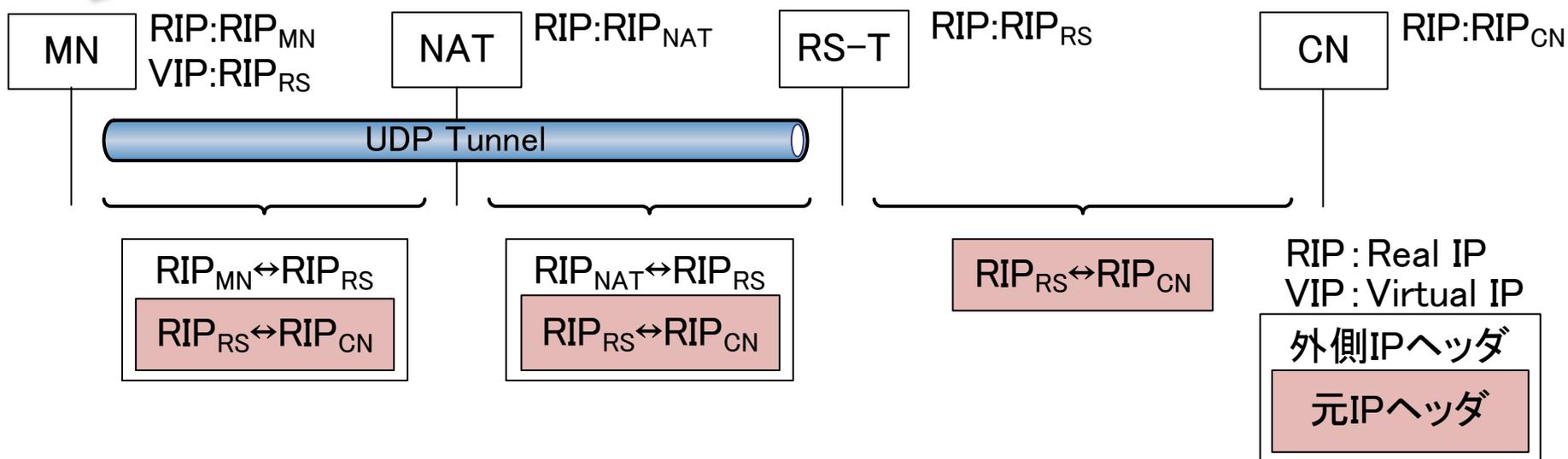


RIP:実IPアドレス VIP:仮想IPアドレス

- MN(NTM端末)からCN(一般端末)への通信開始

MN(Mobile Node)
CN(Correspondent Node)

- ・アプリケーションがパケットを送信
- ・カーネルでパケットをカプセル化

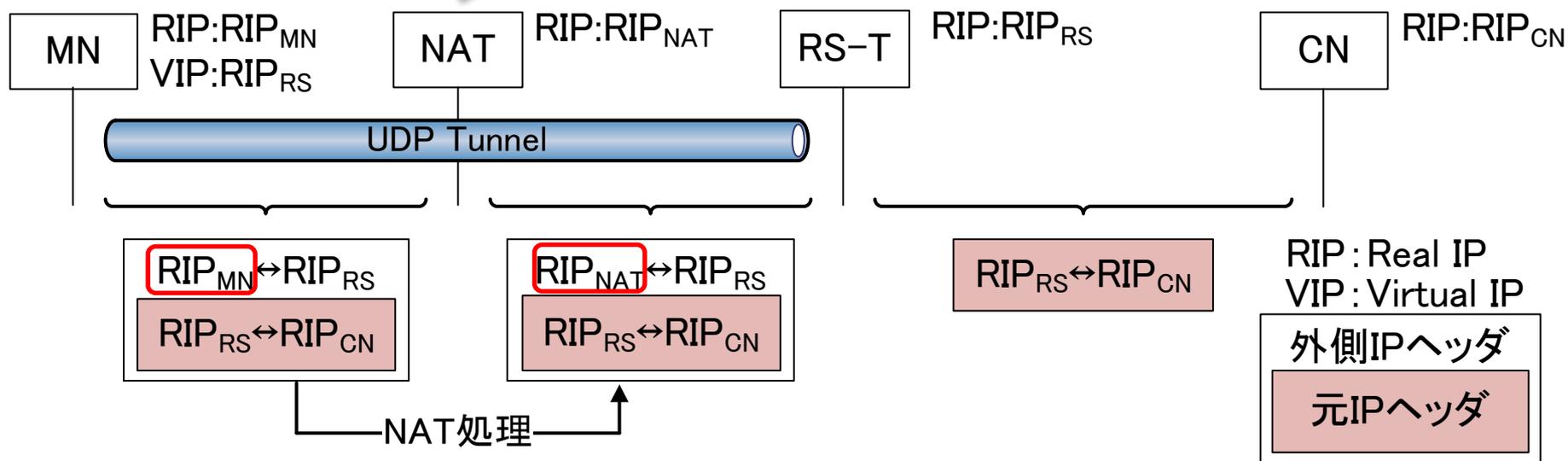


RIP:実IPアドレス VIP:仮想IPアドレス

- MN(NTM端末)からCN(一般端末)への通信開始

MN(Mobile Node)
CN(Correspondent Node)

・外側IPヘッダをアドレス変換

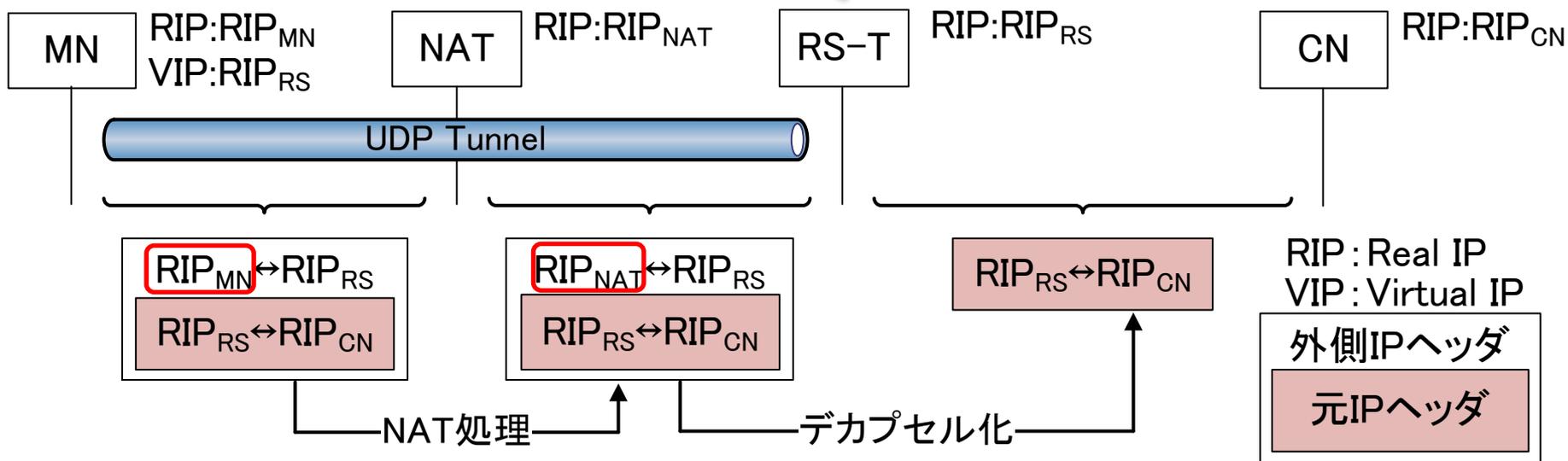


RIP:実IPアドレス VIP:仮想IPアドレス

- MN(NTM端末)からCN(一般端末)への通信開始

MN(Mobile Node)
CN(Correspondent Node)

- 受信したパケットをデカプセル化
- アドレス変換は行わない

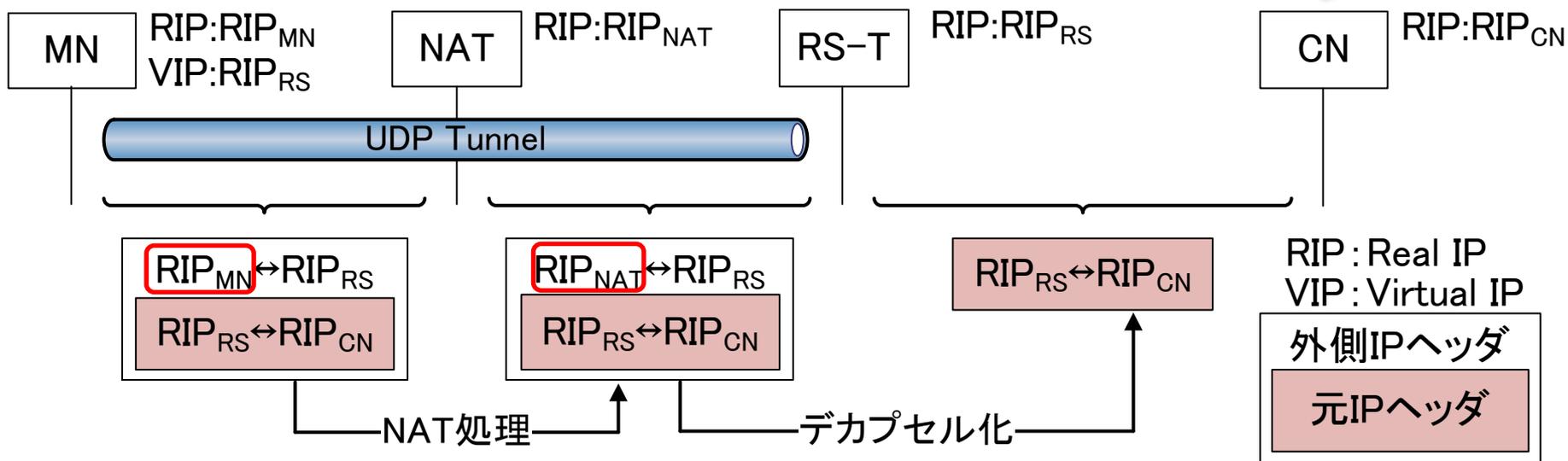


RIP:実IPアドレス VIP:仮想IPアドレス

- MN(NTM端末)からCN(一般端末)への通信開始

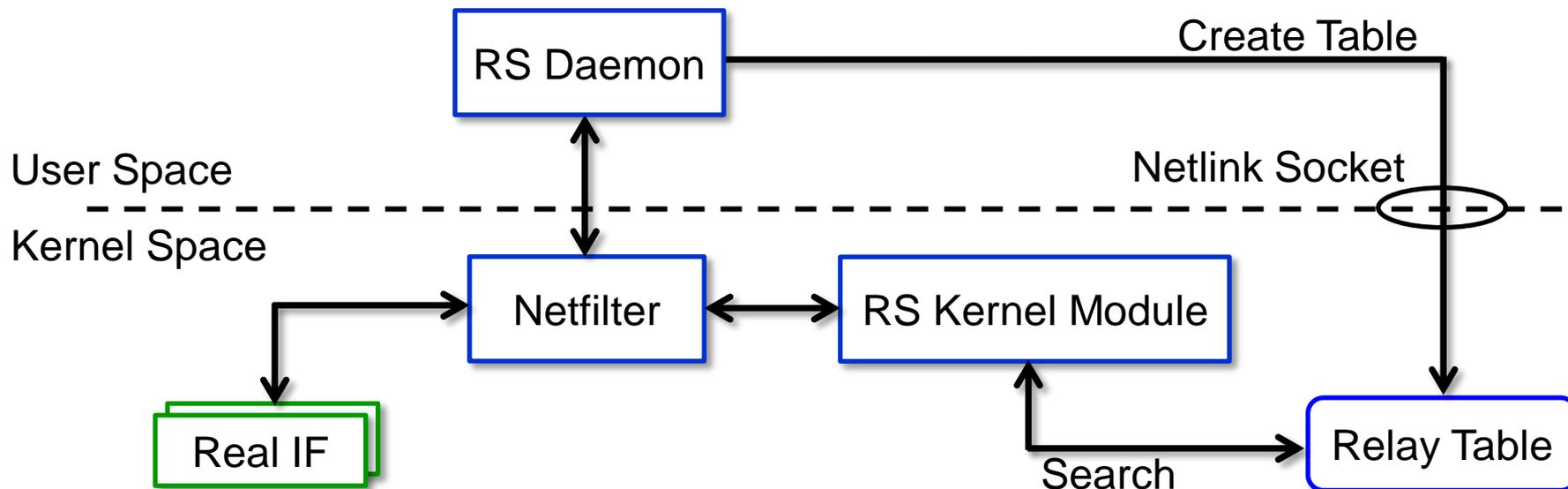
MN(Mobile Node)
CN(Correspondent Node)

- RS-Tからのパケットを受信
- 通信相手はRS-Tであると認識する



RIP:実IPアドレス VIP:仮想IPアドレス

- RSの実装
 - ユーザー空間のRS Daemon
 - カーネル空間のRS Kernel Module
- Relay Table
 - RSが保持しているテーブル
 - 転送に必要な情報(トンネル経路の情報など)が記録されている



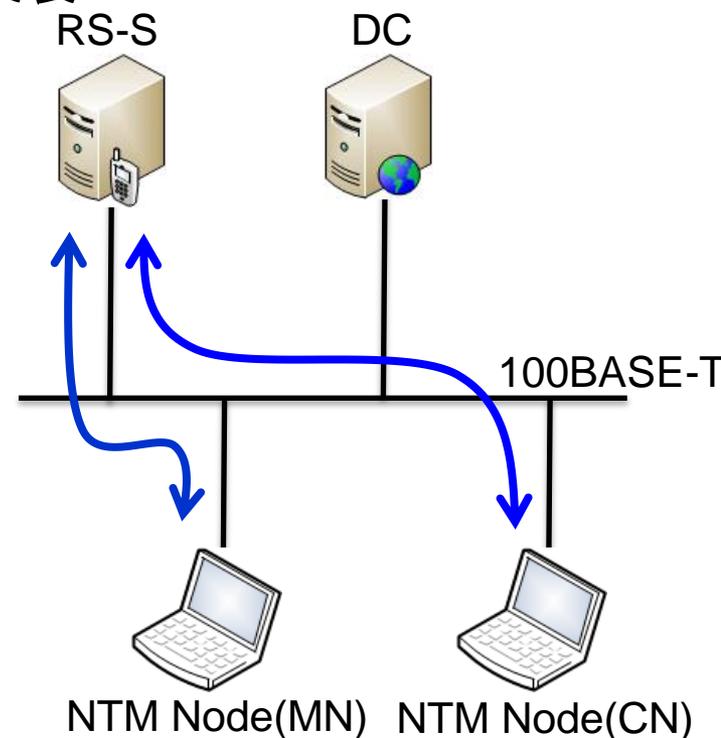
測定環境

- それぞれHost PC上にNTMobileの機能を実装
- RSが転送処理に要する時間を計測
- ユーザー空間にも転送機能とテーブルを実装
 - 転送性能の比較

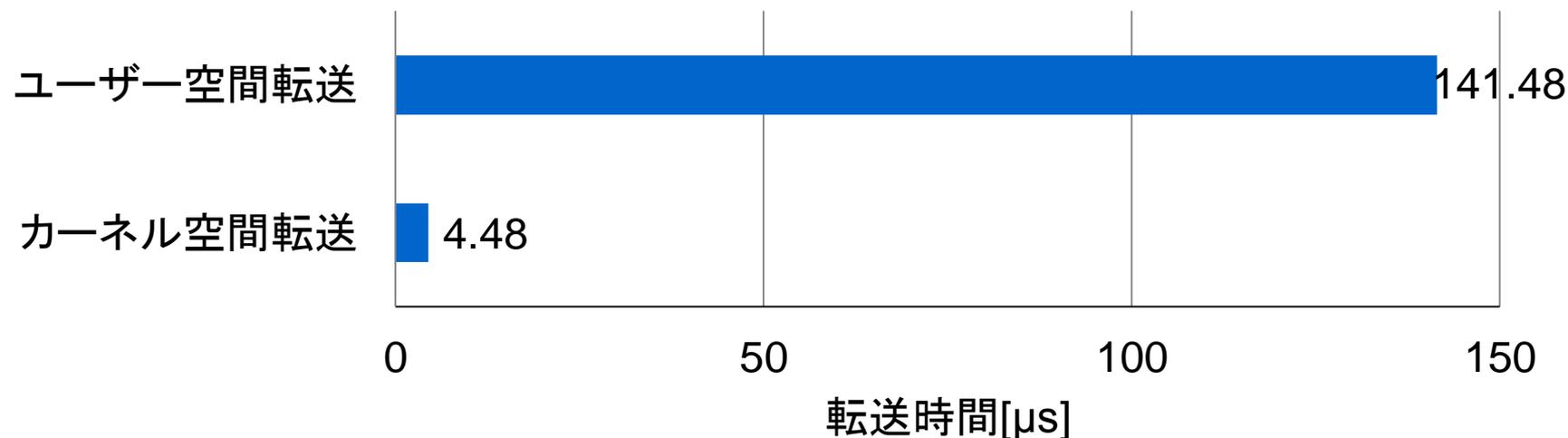
装置仕様

Device	OS	CPU	RAM
DC	Ubuntu 10.04	Celeron M 380 1.6GHz	256MB
RS	Ubuntu 10.04	Core i7 2.93GHz	10GB
NTM Node (MN,CN)	Ubuntu 10.04	Core i7 2.93GHz	10GB

ネットワーク構成



- 測定内容
 - RSがパケットを受信してから送信するまでの時間を計測
 - MNからCNに向けてpingを100回送信, 間隔は1[ms]
- 測定結果
 - 転送時間の差は**31.58倍**となり, 大幅に処理時間を短縮できた



- NTMobile
 - 仮想アドレスとUDPトンネルを使った通信
 - 移動透過性とNAT越えを実現できる技術
- 構成要素RSの分類と動作
 - RS-S(Switch), RS-N(NAT), RS-T(Transparent)
 - 使用用途が異なる
- 実装と評価
 - Linux OSへの実装
 - カーネル空間とユーザー空間での転送性能の比較
- 今後の予定
 - Relay Tableのエントリの整理と検討
 - RS-N, RS-Tの実装

- RSが転送に必要な情報を保持するテーブル
- RS-Sを利用する場合のRelay Tableのエントリー一覧
 - 異なるNAT配下のNTM端末が通信を行う場合

属性名	登録タイミング	内容	備考
Path ID	Relay Direction	PID_{MN-CN}	端末間の経路を示すPath ID
CKey	Relay Direction	K_{MN-CN}	通信に使用する共通鍵
CKey Length	Relay Direction	-	共通鍵の長さ
Tunnel IP	Tunnel Request	RIP_{NAT_MN} RIP_{NAT_CN}	配下ノードに到達するIPアドレス
Tunnel Port	Tunnel Request	m1,m2	配下ノードに到達するポート番号
RefreshTime	-	-	エントリーの生存確認/削除に利用するUNIX時間

NTM Node(MN)



DNS



DC_{CN}



Application

Kernel

DNS Request for A Record

DNS応答を一時退避

DNS Reply for A Record

RIP_{CN}

DNS Request for NTM Record

DNS Reply for NTM Record

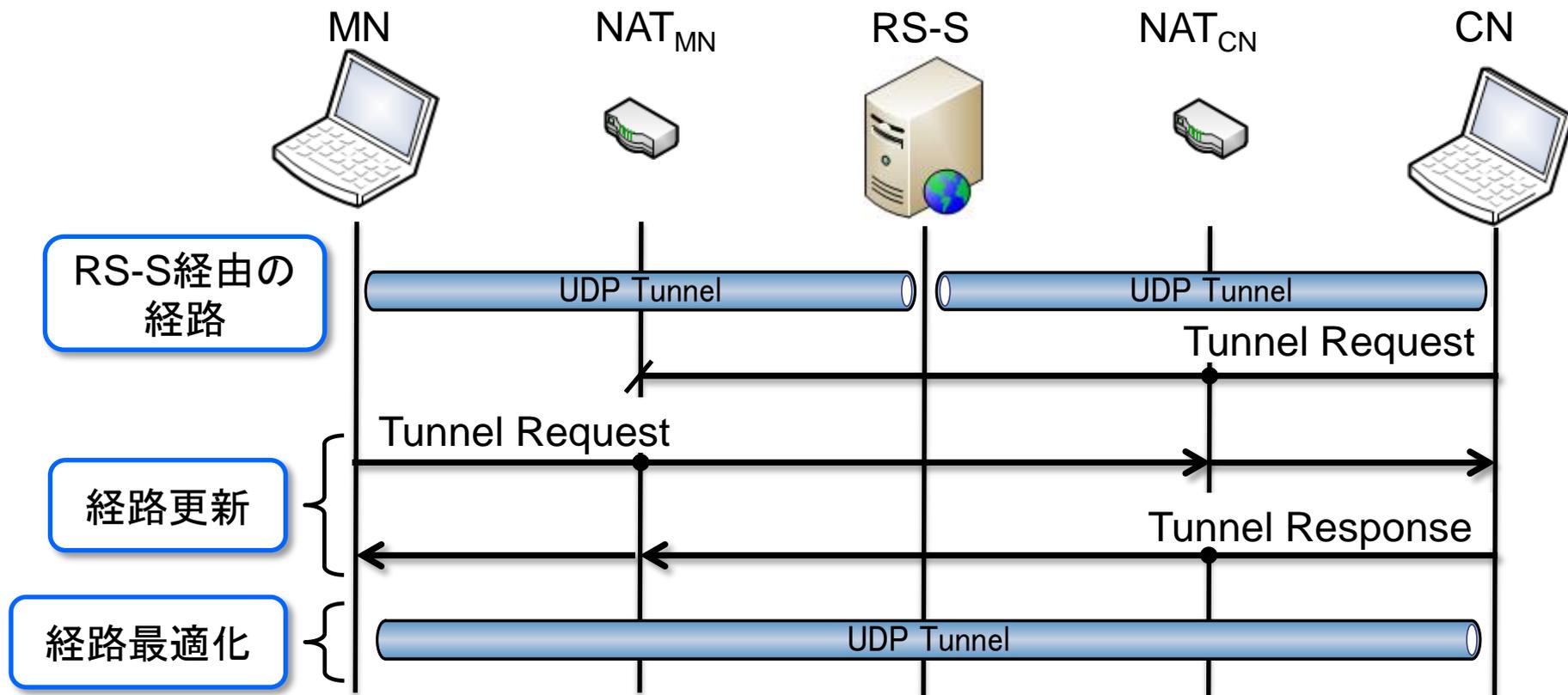
NID_{CN}

RIP_{CN}

RIP_{DC}

VIP_{CN}

- 冗長な経路から最短経路に経路を最適化する
- MNとCNがパケットを投げ合う



納堂博史, 他: NTMobileの経路最適化の検討, 情報処理学会研究報告, 2012-MBL-61, No.33, pp.1—8 (2012).

- NTM端末起動時にDCに対して行われる
- 自身の持つ位置情報を登録する

NTM Node(MN)



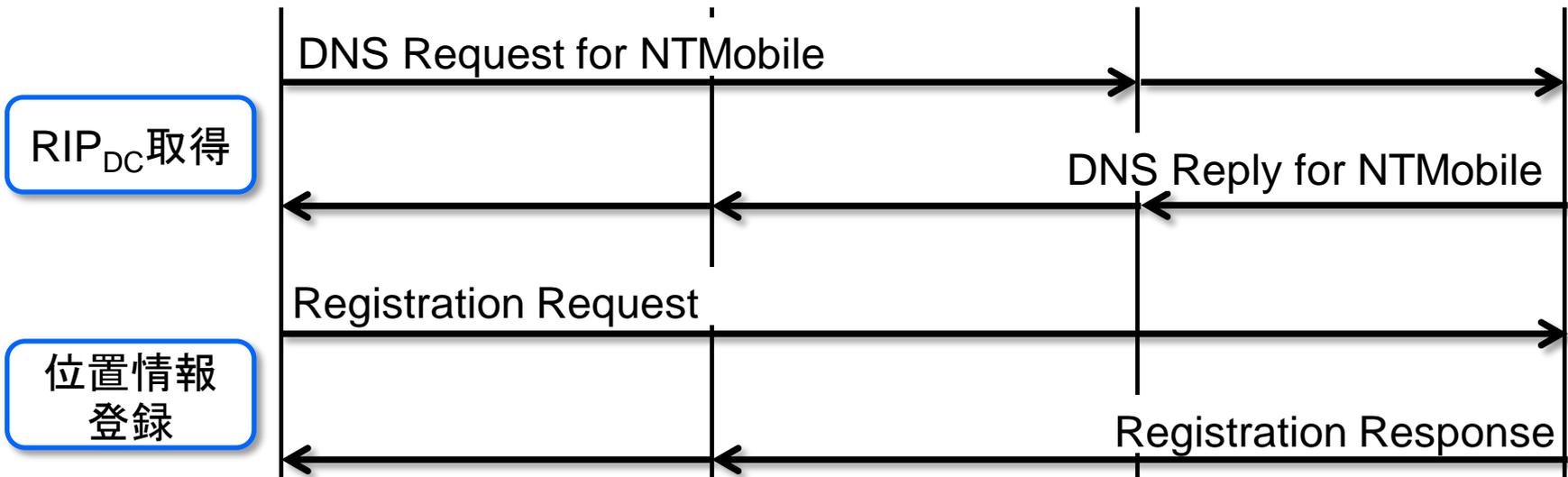
NAT



DNS

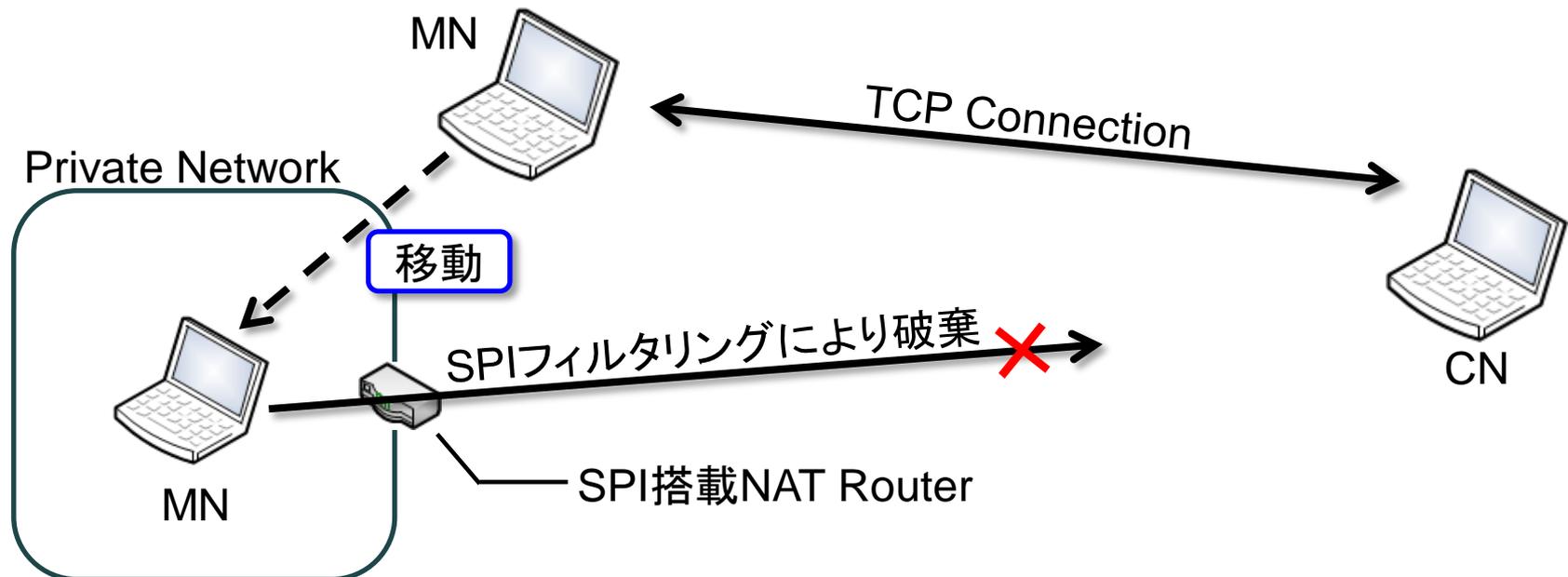


DC_{CN}

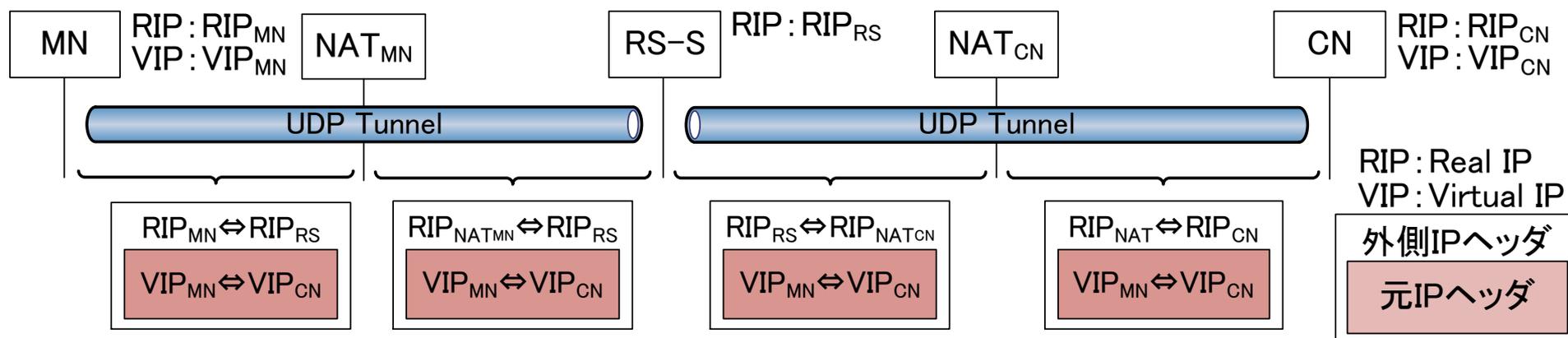


- SPI(Stateful Packet Inspection)

- パケットフィルタリング技術
- 多くのNATルータに実装されている
- TCP通信の場合, シーケンス番号などの整合性によってパケットが破棄される可能性がある

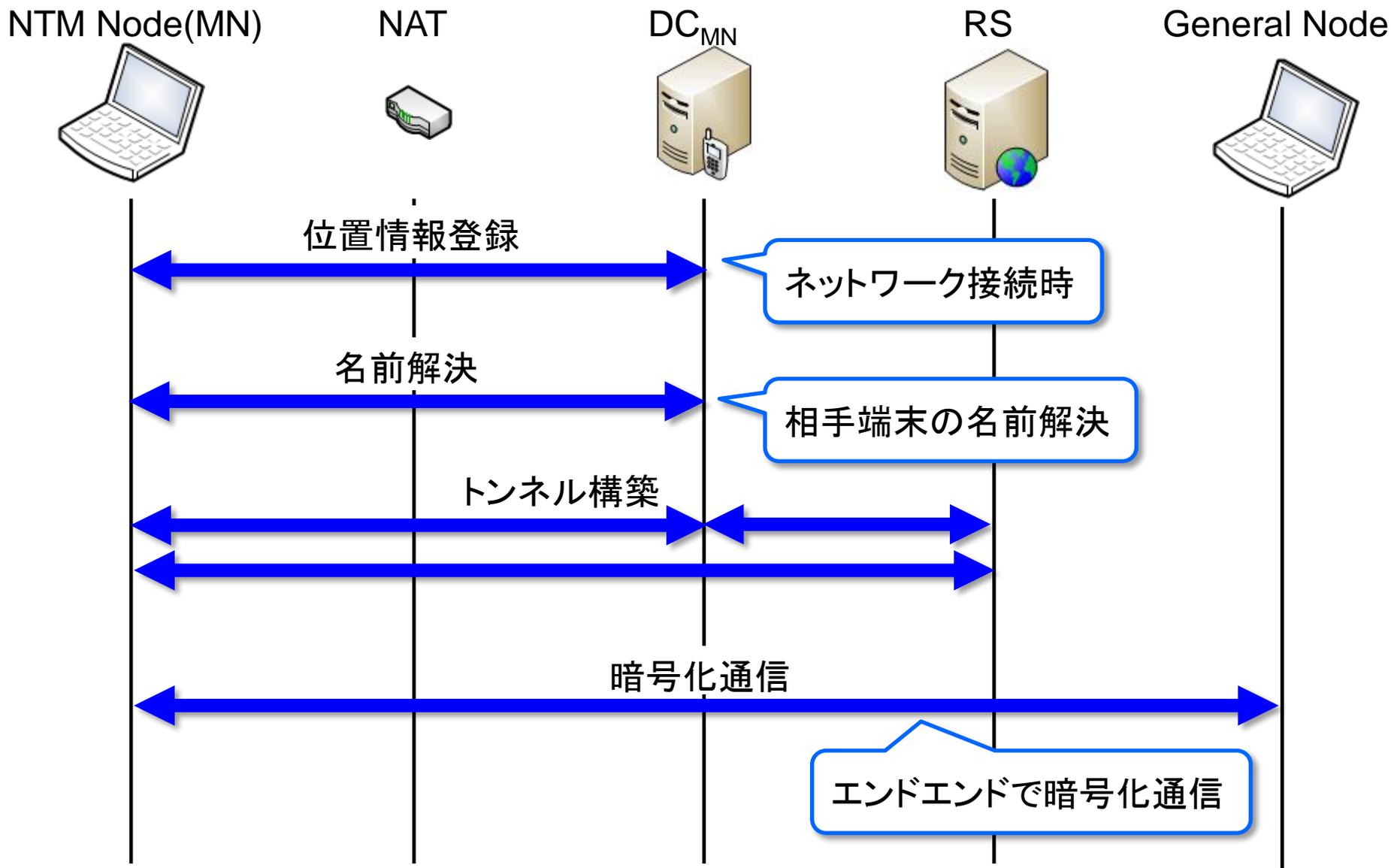


- RS-S(RS type Switch)
 - トンネル切り替え型
 - 受信したパケットをアドレス変換
- MN(NTM端末)からCN(NTM端末)への通信開始

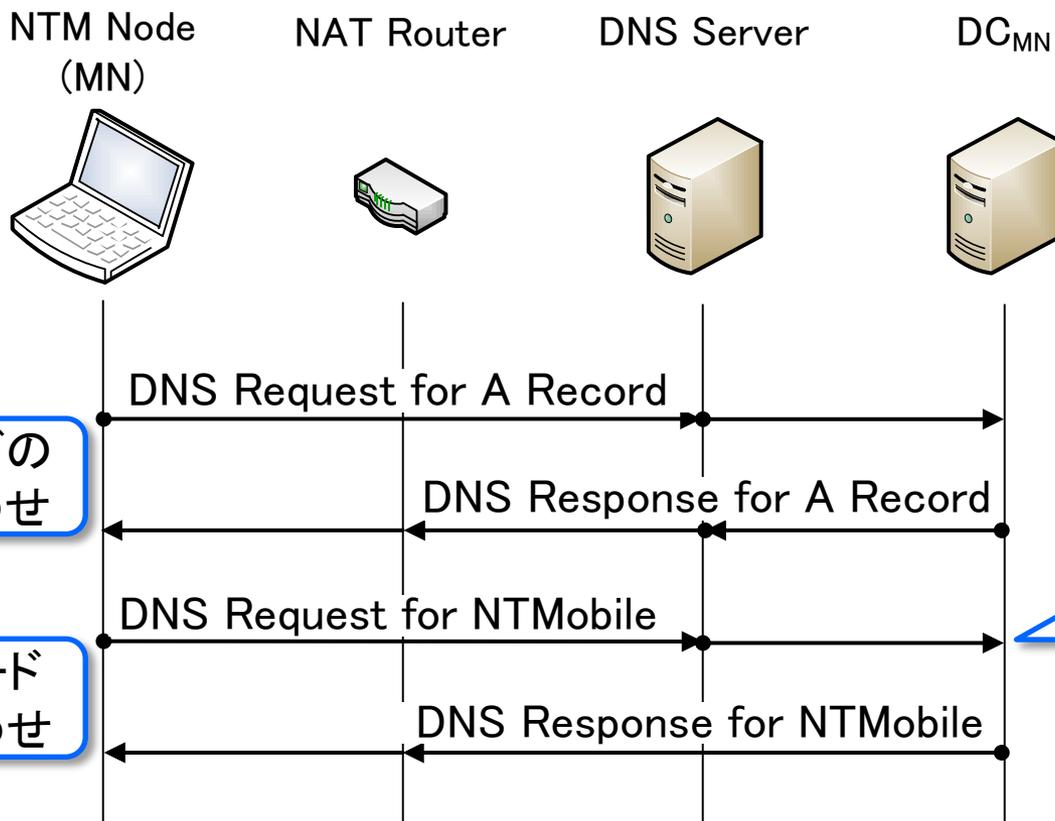


RIP:実IPアドレス VIP:仮想IPアドレス

通信開始までの流れ



- 通信相手端末の名前を解決する
 - 端末のネットワーク接続時
 - Aレコード問い合わせの応答をフックしてネゴシエーションを行う



NTMLレコード

- FQDN
- ノードID
- NATのIP
- 実アドレス
- 仮想アドレス

Aレコードの
問い合わせ

一般端末の場合、NTM
レコードが存在しない

NTMLレコード
の問い合わせ

相手端末は
一般端末である

- Direction Request(経路要求)
 - NTM端末がDCに対して行うトンネル構築指示要求
 - 受信したDCはエンド端末の位置関係よりトンネル構築時手順を判断
- Relay Direction(中継指示)
 - DCがRSに対して行う
 - トンネル経路を示すPath IDを含む
 - 指定したPath IDに関する通信を中継する
- Direction Response(中継指示応答)
 - RSがDCに対して行う
 - Relay Directionに対する確認応答

- Route Direction(経路指示)
 - DCがNTM端末に対して行う
 - トンネル構築に必要な情報(経路情報など)を含む
- Tunnel Request(トンネル要求)
 - エンド端末がDCまたはRSに対して行うトンネル構築要求
 - NAT配下に存在するNTM端末側から送信
- Tunnel Response(トンネル応答)
 - Tunnel Requestに対する応答