NTMobileにおけるアドレス変換型リレーサーバの実装と動作検証

土井 敏樹[1]　鈴木 秀和[1]　内藤 克浩[2]　渡邊 晃[1]

概要：モバイルネットワークの普及によって，自由に通信を開始できる通信接続性と，移動しながら通信を継続できる移動透過性が求められている．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，あらゆるケースにおいて通信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）が存在する．本稿では，一般サーバなど NTMobile の機能が未実装である装置（一般端末）との通信を行うために用いるアドレス変換型 RS（RS-N : Relay Server type NAT）の機能について説明する．RS-N の実装と動作検証・評価を行った結果，RS-N を経由した一般端末との通信が可能であることを確認した．また，NTM 端末どうしの直接通信と比べて 4%程度のスループット低下しか発生しないことがわかった．

1. はじめに

近年，高速無線技術の発展やスマートフォンなどの携帯端末の普及によって，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はるかに超えており，IPv4 アドレスの枯渇が問題になっている．このための長期的解決策として IPv6 が準備されているが，IPv4 と IPv6 に互換性がなく，普及が滞っている．そのため，IPv4 は今後も半永久的に使われていくと考えられる．このような背景から，本稿では，IPv4 が今後も一定の役割を担い続けると想定し，IPv4 の通信接続性と移動透過性に絞って議論する．

IPv4 ネットワーク環境では，組織内のネットワークはプライベートアドレスで構成し，グローバルネットワークへのアクセスは NAT（Network Address Translation）を介して行う形態が一般的である．このようなネットワーク構成では，インターネット側から NAT 配下のネットワークに通信を開始できない NAT 越え問題が発生する．この問題によって通信を開始できる場所が限られてしまうため通信接続性を確保できず，IPv4 の汎用性を損なう大きな要因となる．

一方，移動端末の普及と携帯通信網の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，Wi-Fi にトラフィックを逃す Wi-Fi オフロードの要求が高まっている [1]．しかし，IP ネットワークでは，IP アドレスが位置情報と端末識別情報の意味を持っているため，ネットワークが切り替わると IP アドレスが変化し，そのままでは通信を継続することができない．この課題を解決するために移動透過性技術が今後重要になると考えられる．

移動透過性を実現する既存技術には，特殊な中継装置を必要とするプロキシ型と，中継装置が不要なことを特徴とするエンドエンド型がある．プロキシ型の代表例としては，Mobile IPv4 [2] が挙げられる．Mobile IPv4 は HA（Home Agent）が通信の中継を行い，移動端末の IP アドレスの変化を隠蔽する．Mobile IPv4 は，NAT を跨る移動透過性を実現するため，UDP トンネルを利用した仕様が標準化されている [3]．しかし，必ず中継装置である HA を経由した通信となる．さらに，HA はホームネットワーク上に設置をすることを前提としており，移動端末の移動先によっては，通信経路が冗長になるという課題がある．エンドエンド型の代表例としては，MATv4（Mobile Support Architecture and Technologies v4）[4]，Mobile PPC（Mobile Peer to Peer Communication）[5] などが挙げられる．いずれもエンド端末間で直接通信ができるため，通信経路が冗長になるという課題はない．しかし，MATv4 は NAT を跨る移動を想定しておらず適用範囲が狭いという課題がある．また，相手端末が一般端末である場合は移動通信を実現できず，実現するにはモバイルルータの導入が必要である [6]．Mobile PPC は，一般端末との通信方法が検討されたが，中継装置の設置場所や多重化についての検討はされていな

[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
Graduate School of Engineering, Mie University

© 2013 Information Processing Society of Japan

い [7].

我々は，これまで通信接続性と移動透過性を同時に実現する NTMobile（Network Traversal with Mobility）[8–11] を提案してきた．NTMobile では，NTMobile 対応端末（NTM 端末）のアプリケーションに対して仮想 IP アドレスを提供し，実際の通信は実 IP アドレスでトンネル通信を行うことにより，通信接続性と移動透過性を同時に実現することができる．このとき，NAT の改造が不要であるため，適用範囲は極めて広い．

NTMobile では，NTM 端末が異なる NAT 配下に存在する場合など，エンド端末間で直接通信ができないと判断した場合，中継サーバである RS（Relay Server）を介してパケットの中継を行う．RS には，トンネル切り替え型 RS（RS-S : Relay Server type Switch）とアドレス変換型 RS（RS-N : Relay Server type NAT）の 2 種類が存在する．RS-S は，例えば通信を行う 2 台の NTM 端末が異なる NAT 配下に存在する場合に利用する．RS-N は，NTM 端末と一般端末が通信を行うときに，NTM 端末が移動しながら通信を行いたい場合に利用する．RS-N が一般端末に代わって NTMobile の処理を行い，一般端末が通信相手を RS-N と認識することで，NTM 端末は移動しながら通信を行うことができる．これまでに，RS-S の実装と評価を終えている [12]．RS-N は，これまでに仕様の検討が行われていなかった．本稿では，RS-N の仕様の検討を行い，実装と動作検証・評価を行った．

以後，2 章では NTMobile の概要，**??**章で RS-N の概要と動作について述べる．3 章で RS-N の実装について述べ，4 章で動作検証と評価を行い，5 章でまとめる．

2. NTMobile

図 1 に NTMobile の構成を示す．NTMobile では，構成要素として，NTM 端末，NTM 端末の情報管理とトンネル経路の指示を行う DC（Direction Coordinator），エンドエンドの通信が行えない場合などに通信を中継する RS が存在する．DC や RS はグローバルネットワーク上に設置し，ネットワークの規模に応じて複数台設置することによって処理負荷を分散することができる．

2.1 NTMobile の構成

DC は，NTM 端末に対する仮想 IP アドレスの割り当てなどを行う．DC が各 NTM 端末に割り当てる仮想 IP アドレスは一意な値であり，各 DC に割り振られたアドレス空間から重複が起きないように割り当てる．

RS には，エンド端末間で直接通信が行えない場合に利用する RS-S と，一般端末との通信において利用する RS-N が存在する．本稿では，RS-N を対象として記述する．

NTM 端末のアプリケーションは，仮想 IP アドレスを自身及び相手の IP アドレスとして認識する．仮想 IP アドレスによって生成されたパケットはカーネルでカプセル化され，相手端末へと送信される．

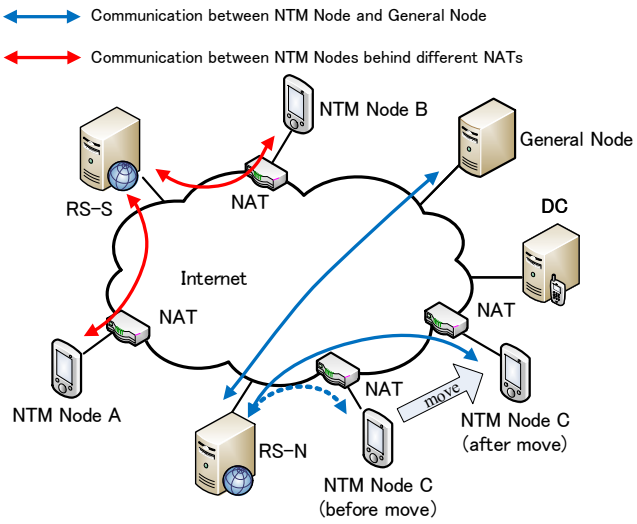


図 1 NTMobile の概要
Fig. 1 Overview of NTMobile.

DC と各端末は信頼関係があることを前提としており，NTMobile で用いる制御メッセージはあらかじめ共有している共通鍵を用いて暗号化される．また，NTM 端末間，NTM 端末と RS 間でやり取りされるメッセージは，トンネル構築時に DC より配布される共通鍵を用いて暗号化される．

2.2 アドレス変換型 RS（RS-N）

RS-N は，アドレス変換型 RS（RS-N : Relay Server type NAT）である．NTM 端末がインターネット上の Web サーバや，NTMobile を実装していない一般端末と通信を行う場合に利用する．NTM 端末の移動透過性を確保するため，RS-N が一般端末との通信を代行し，NTMobile のパケットのカプセル化/デカプセル化，および仮想 IP アドレスと実 IP アドレスのアドレス変換処理を行う．RS-N を設置する場所はグローバルネットワーク上のどこでもよい．RS-N は複数設置が可能であり，トンネル構築ネゴシエーションにおいて，DC が複数の RS-N の中から通信負荷や通信経路を指標として最適な RS-N を選択できる．

2.3 NTMobile の動作

図 2 に，RS-N を経由した通信におけるトンネル構築シーケンスを示す．NTM 端末 X の実 IP アドレスと仮想 IP アドレスをそれぞれ $\mathrm{RIP_X}$，$\mathrm{VIP_X}$ とし，アドレス情報を管理している DC を $\mathrm{DC_X}$ とする．また，通信開始側の NTM 端末を MN（Mobile Node），一般端末を GN（General Node）とし，GN の名前と IP アドレスの対応関係を管理する DNS サーバを $\mathrm{DNS_{GN}}$ とする．

図 2 に RS-N を経由した通信におけるトンネル構築シー

© 2013 Information Processing Society of Japan

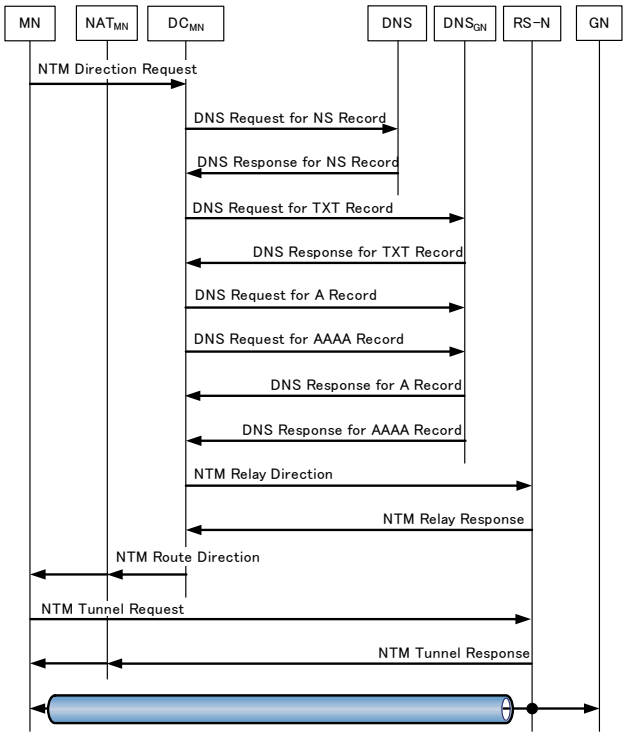


図 2 RS-N を経由した通信におけるトンネル構築シーケンス
Fig. 2 Tunnel establish sequence via RS-N.

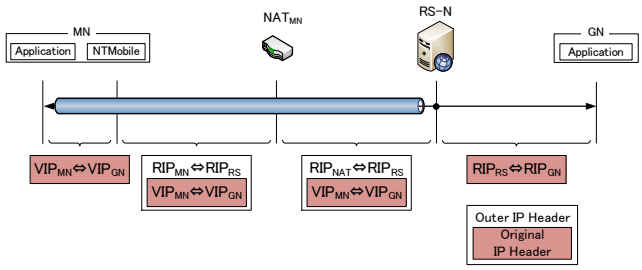


図 3 トンネル通信時におけるアドレス遷移
Fig. 3 Address translation of the tunnel communication.

ケンスを示す.

2.4 端末情報の登録

全ての NTM 端末は，ネットワーク接続時に DC に対して自身のアドレス情報の登録処理を行う．DC$_{MN}$ は自身のデータベースに MN のアドレス情報を登録するとともに，MN に対して仮想 IP アドレスを割り当てる．

2.5 名前解決

MN は，GN の名前解決を行う DNS クエリをトリガーとして，自身を管理する DC$_{MN}$ に対して GN の FQDN（FQDN$_{GN}$）を載せた NTM Direction Request を送信し，名前解決とトンネル構築を依頼する．MN から NTM Direction Request を受信した DC$_{MN}$ は，DNS の仕組みによって DNS$_{GN}$ の NS レコードを取得し，更に DNS クエリによって DNS$_{GN}$ に対して TXT レコードの問い合わせを行う．DC にはあらかじめ，DC であることがわかるような TXT レコードが登録されている．しかし，DNS$_{GN}$ は DC ではなく一般の DNS サーバであるため，DC であることを示す TXT レコードは取得できない．そのため，DC$_{MN}$ は，DNS$_{GN}$ が一般の DNS サーバであると判断し，通信相手端末が一般端末であると判断する．その後，DNS$_{GN}$ に直接 FQDN$_{GN}$ の A/AAAA レコードの問い合わせを行い，名前解決を行う．

2.6 一般端末に対応する仮想 IP アドレス

NTMobile では，DC が一般端末に対応する仮想 IP アドレスを用意し，NTM 端末は仮想 IP アドレスを一般端末の IP アドレスとして認識する．一般端末に対応する仮想 IP アドレスは，NTM Relay Direction 送信前に DC$_{MN}$ によって決定される．DC$_{MN}$ は，自身に割り振られたアドレス空間から一般端末に対応する仮想 IP アドレスを用意し，NTM Relay Direction によって RS-N へ，NTM Route Direction によって NTM 端末へと通知する．

2.7 トンネル構築

DC$_{MN}$ は，RS-N に対して通信の中継を指示する NTM Relay Direction を送信する．次に，NTM Route Direction によって MN に対して RS-N との間にトンネルを構築するように指示する．MN と RS-N は NTM Tunnel Request/NTM Tunnel Response を交換することにより，トンネル経路を構築する．その後，アプリケーションに対して，一般端末に対応する仮想 IP アドレスを通知する．アプリケーションは通知された仮想 IP アドレスを相手端末の仮想 IP アドレスとして認識する．

2.8 トンネル通信

図 3 にパケットのアドレス遷移の様子を示す．MN のアプリケーションでは，仮想 IP アドレスを用いたパケットが生成され，カーネル空間にて実 IP アドレスでカプセル化される．RS-N では，パケットのカプセル化/デカプセル化および仮想 IP アドレスと実 IP アドレスの変換を行う．この時，アドレス変換は送信元/宛先の両方を変換する点が一般の NAT 処理とは異なる．アドレス変換したパケットを GN へ送信することによって，GN は通信相手を RS-N であると認識する．

2.9 NTM 端末のハンドオーバ時の動作

NTM 端末がネットワークを切り替えた場合，変化したアドレス情報を載せた NTM Registration Request を DC$_{MN}$ へと送信し，DC が保持している情報を最新の情報に更新する．その後に，2.7 節で述べたトンネル構築手順をを実行し，RS-N との間にトンネルを再構築する．

© 2013 Information Processing Society of Japan

3. 実装

3.1 RS-N の設計方針

NTMobile では，RS-S の実装と評価を既に終えており，NTMobile の機能をユーザ空間とカーネル空間に実装している．RS-S と RS-N を別の実装としてしまうと複数の種類の RS を設置することになり，実運用上のコストとなってしまう．そのため，RS-N の実装はデーモン/カーネルともに，既存の RS-S を拡張する形態で設計を行う．DC はネゴシエーション時に相手端末を管理する DNS サーバの種類を判断し，RS に動作すべき RS の種類を通知することで，1 台の装置で RS-S と RS-N の双方の機能を実現することを可能とする．

RS-N では，アドレス変換を行うときに Linux の Netfilter[*1] の仕組みを用いる．この仕組みを用いることにより，NTM 端末から受信したパケットの送信元アドレスとポート番号が変換されるとき，使用していないポート番号を自動的に選択することができる．また，FTP などのペイロード部分に IP アドレスを含むプロトコルを用いる場合，Netfilter に存在するモジュールが ALG（Application Level Gateway）の働きをすることでペイロード内の IP アドレスを変換することにより，このようなプロトコルに対応できる．

なお，通信前にデーモンから iptables コマンドを用いて Netfilter の MASQUERADE ルールを設定し，NTMobile が仮想 IP アドレスとして利用している範囲のパケットに対して NAPT 処理を行うように設定する．

3.2 デーモン

RS-N のデーモンでは，通信開始時のネゴシエーションを行う．図 4 に NTMobile のモジュール構成図を示す．NTM Relay Direction/NTM Tunnel Request 受信時には Path ID など，中継に必要な情報をカーネル空間に実装されている Relay Table に登録する．また，NTM Relay Direction 受信時には NTM Direction Response を応答し，NTM Tunnel Request 受信時には NTM Tunnel Response を応答する．

RS が NTM Relay Direction を受信した時には動作すべき RS の種類が通知される．NTM Relay Direction を受信した RS は，パケットに記載されている RS の種類をデーモンから NTMobile カーネルモジュールへと通知する．カーネルモジュールは，受信した RS の種類を元に RS の挙動を確定する．

3.3 NTMobile カーネルモジュール

RS-N のカーネルでは，通信パケットの中継及びカプセル化/デカプセル化を行う．更に，NTMobile で利用する仮想 IP アドレスや端末間のコネクションを識別する PathID などを管理する Relay Table が存在する．通信パケット受信時にはカプセル化/デカプセル化を行い，加えて Netfilter の仕組みを用いた NAPT 処理を行う．

[*1] http://www.netfilter.org/

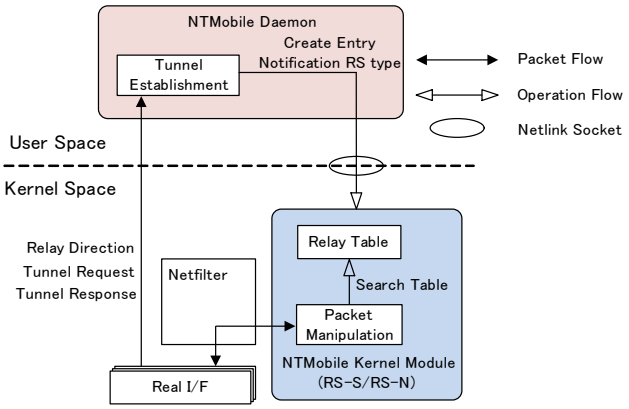


図 4 RS のモジュール構成
Fig. 4 Module configuration of RS.

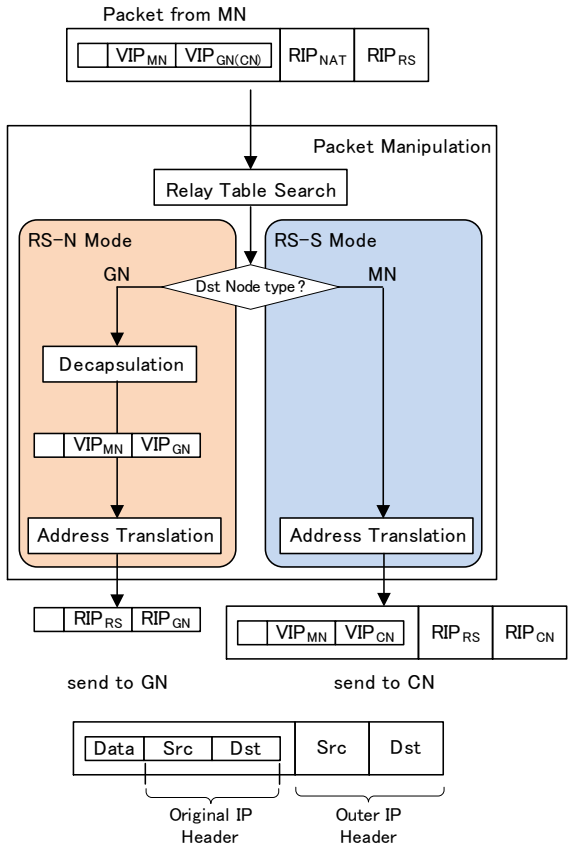


図 5 RS における動作モードとパケット操作
Fig. 5 Behavior Mode and Packet Manipulation of RS.

3.3.1 RS の動作モードとパケットの操作

図 5 に MN からパケットを受信した時の RS の動作モードとパケット操作の様子を示す．なお，通信相手の NTM 端末を CN(Correspondent Node) とする．また，受信パ

© 2013 Information Processing Society of Japan

表 1　装置仕様
Table 1　Device specifications.

	DC, DNS(Virtual Machine)	RS	MN	CN(GN)
Hardware	HP h8-1180jp	Epson Endeavor NT331	Epson Endeavor NT350	Epson Endeavor NA101
OS	Ubuntu 10.04	Ubuntu 10.04	Ubuntu 10.04	Ubuntu 10.04
Linux Kernel	2.6.32-41-generic	2.6.32-38-generic	2.6.32-41-generic	2.6.32-21-generic
CPU	Intel Core i7-2600 (3.4GHz)	Intel Pentium M (1.80GHz)	Intel Pentium M (1.73GHz)	Intel Core Solo U1400 (1.2GHz)
Memory	1GB	512MB	512MB	512MB

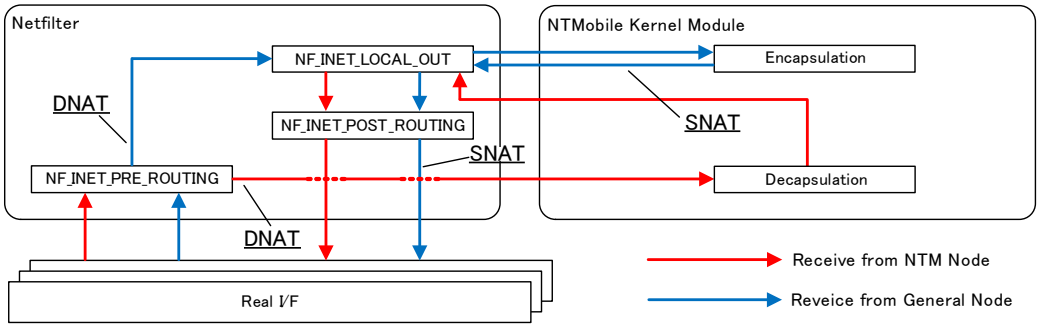


図 6　Netfilter と NTMobile カーネルモジュールの関係
Fig. 6　Relationship of Netfilter and NTMobile Kernel Module.

ケットの元パケットの宛先 IP アドレスは，通信相手端末が一般端末の場合は VIP_{GN}，NTM 端末の場合は VIP_{CN} となる．

RS は MN からパケットを受信すると，パケットに記載されている Path ID をキーとして Relay Table を検索する．ここで，Relay Table には，トンネル構築ネゴシエーション時に取得した相手端末のタイプ（NTM 端末/一般端末）が記載されている．相手端末が GN であれば RS-N として動作し，パケットのデカプセル化とアドレス変換を行う．相手端末が NTM 端末であれば，RS-S として動作し，アドレス変換のみ行う．

3.3.2　Netfilter の仕組みを用いたアドレス変換

図 6 に RS-N の NTMobile カーネルモジュールにおけるアドレス変換と Netfilter の処理フローを示す．MN から受信したパケットは，Netfilter の NF_INET_PRE_ROUTING にてフックを行い，パケットをカーネルモジュールに引き渡す．パケットのデカプセル化を行った後，宛先を Relay Table から取得した RIP_{GN} にアドレス変換し，Netfilter の NF_INET_LOCAL_OUT へ渡す．その後，Netfilter の NF_INET_POST_ROUTING においてフックした後，送信元 IP アドレス/ポート番号を変換し，GN へ送信する．MN から GN に向けての最初のパケットが通過した時，RIP_{RS-N} と VIP_{MN} を関連付けるアドレス変換テーブルが生成される．送信元ポート番号は，Netfilter によって自動的に選択される．

GN から受信したパケットは，Netfilter の NF_INET_PRE_ROUTING にてアドレス変換テーブルに従って宛先を VIP_{MN} に変換し，Netfilter の NF_INET_LOCAL_OUT へ渡す．Netfilter の NF_INET_LOCAL_OUT ではカプセル化とアドレス変換処理を行い，Netfilter の NF_INET_LOCAL_OUT にてパケットをチェインに戻す．その後，MN へと送信する．

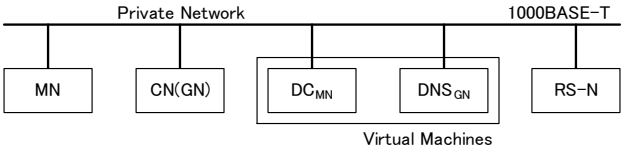


図 7　ネットワーク構成
Fig. 7　Configuration of Network.

Netfilter によるアドレス変換時には，TCP チェックサムの再計算が行われる．この時，送信元アドレスの変換（SNAT）のみ考慮しており，宛先アドレスの変換（DNAT）は考慮されていない．NTMobile カーネルモジュールでは DNAT を行うため，TCP チェックサム再計算時に TCP チェックサムが間違った値となってしまう．そのため，DNAT の処理を行った後チェックサム再計算を行う処理を追加する．

4.　動作検証と評価

動作検証として，RS-N のトンネル構築シーケンスが正常に行われるかどうか検証した．また，RS-N の処理にともなうスループットの低下率を評価した．

4.1　測定環境

図 7 と表 1 に試験ネットワークの構成と各装置の仕様を示す．1 台の実機 PC 上にインストールした VMware

© 2013 Information Processing Society of Japan

表 2　スループット測定結果
Table 2　Results of throughput measurements.

	End to End	via RS-N
Throughput(Mbps)	90.1	86.9

Workstation 8 を利用して，DC と DNS を仮想マシンとして構築し，同一プライベートネットワークへとブリッジ接続した．RS-N と NTM 端末は Linux をインストールした実機 PC に実装し，プライベートネットワークへと直接接続した．接続は 1000BASE-T による有線 LAN である．また，本来はトンネル構築ネゴシエーション時に NTM 端末と RS-N との間で共通鍵の交換を行い，カプセル化通信は暗号化されるが，今回は鍵交換が未実装であるため，暗号化は行わない状態で測定を行った．

4.2　スループット測定

MN と CN 間で iperf を用いた TCP 通信を行い，スループットを測定した．測定対象の構成は，NTM 端末どうしの直接通信，NTM 端末と一般端末との RS-N を経由した通信である．CN を NTM 端末と一般端末の動作をするように切り替え測定は 1 秒間隔のスループット測定を MN から CN に対して 10 回行い，その平均値を算出した．

表 2 に，スループット測定結果を示す．NTM 端末どうしの通信では端末間で直接トンネルが構築されるため最短経路となり，スループットが RS-N 経由の通信より高い値となった．RS-N 経由の通信では経路が冗長になるが，NTM 端末どうしの直接通信に比べて 4%程度のスループット低下しか発生していないことがわかる．この結果より，一般端末との通信において，RS-N のカプセル化/デカプセル化及びアドレス変換の処理が，スループットの低下に大きな影響を及ぼすことはない．

5.　まとめ

本稿では，NTMobile における構成要素の一つであるアドレス変換型 RS（RS-N）の動作と実装及び動作検証について述べた．RS-N を用いることによって，NTM 端末は一般端末との通信においても移動しながら通信を行うことができる．また，既に実装を終了している RS-S に RS-N の機能を統合し，コネクション確立時に RS の種類を選択することにより，1 台の装置で機能を切り替えることが可能となった．そのため，RS-S と RS-N を別の装置として設置する必要はない．

今後は，RS-N を経由した通信における鍵交換の実装を行い，暗号化通信を行った場合の動作検証及び性能評価を行う予定である．また，RS-N の選択手法の検討を進めていく予定である．

参考文献

[1] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012—2017 (2013). http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.pdf.
[2] Perkins, C.: IP Mobility Support for IPv4, Revised, RFC 5944, IETF (2010).
[3] Levkowetz, H. and Vaarala, S.: Mobile IP Traversal of Network Address Translation (NAT) Devices, RFC 3519, IETF (2003).
[4] 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).
[5] 竹内元規，鈴木秀和，渡邊　晃：エンドエンドで移動透過性を実現する Mobile PPC の提案と実装，情報処理学会論文誌，Vol. 47, No. 12, pp. 3244–3257 (2006).
[6] 相原玲二，藤田貴大，岸場清悟，田島浩一，西村浩二，前田香織：常に最適経路で通信を行う移動透過アーキテクチャ MAT の性能評価，インターネットコンファレンス 2006 論文集，Vol. 2006, pp. 13–20 (2006).
[7] 張　冰冰，鈴木秀和，渡邊　晃：プロキシ中継型 Mobile PPC の検討，マルチメディア，分散，協調とモバイル（DICOMO2008）シンポジウム論文集，Vol. 2008, No. 1, pp. 1588–1592 (2008).
[8] 鈴木秀和，上醉尾一真，水谷智大，西尾拓也，内藤克浩，渡邊　晃：NTMobile における通信接続性の確立手法と実装，情報処理学会論文誌，Vol. 54, No. 1, pp. 367–379 (2013).
[9] 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 における端末アドレスの移動管理と実装，Vol. 2011, pp. 1139–1145 (2011).
[10] 細尾幸宏，鈴木秀和，内藤克浩，旭　健作，渡邊　晃：NTMobile における DNS 実装の変更が不要なデータベース型端末情報管理手法の検討，Vol. 2012-MBL-64, No. 6, pp. 1–8 (2012).
[11] 内藤克浩，上醉尾一真，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，情報処理学会論文誌，Vol. 54, No. 1, pp. 380–393 (2013).
[12] 土井敏樹，鈴木秀和，内藤克浩，渡邊　晃：NTMobile における RS の検討，マルチメディア，分散，協調とモバイル（DICOMO2012）シンポジウム論文集，Vol. 2012, No. 1, pp. 1162–1168 (2012).

© 2013 Information Processing Society of Japan

NTMobileにおけるアドレス変換型リレーサーバの実装と動作検証

†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†

研究背景

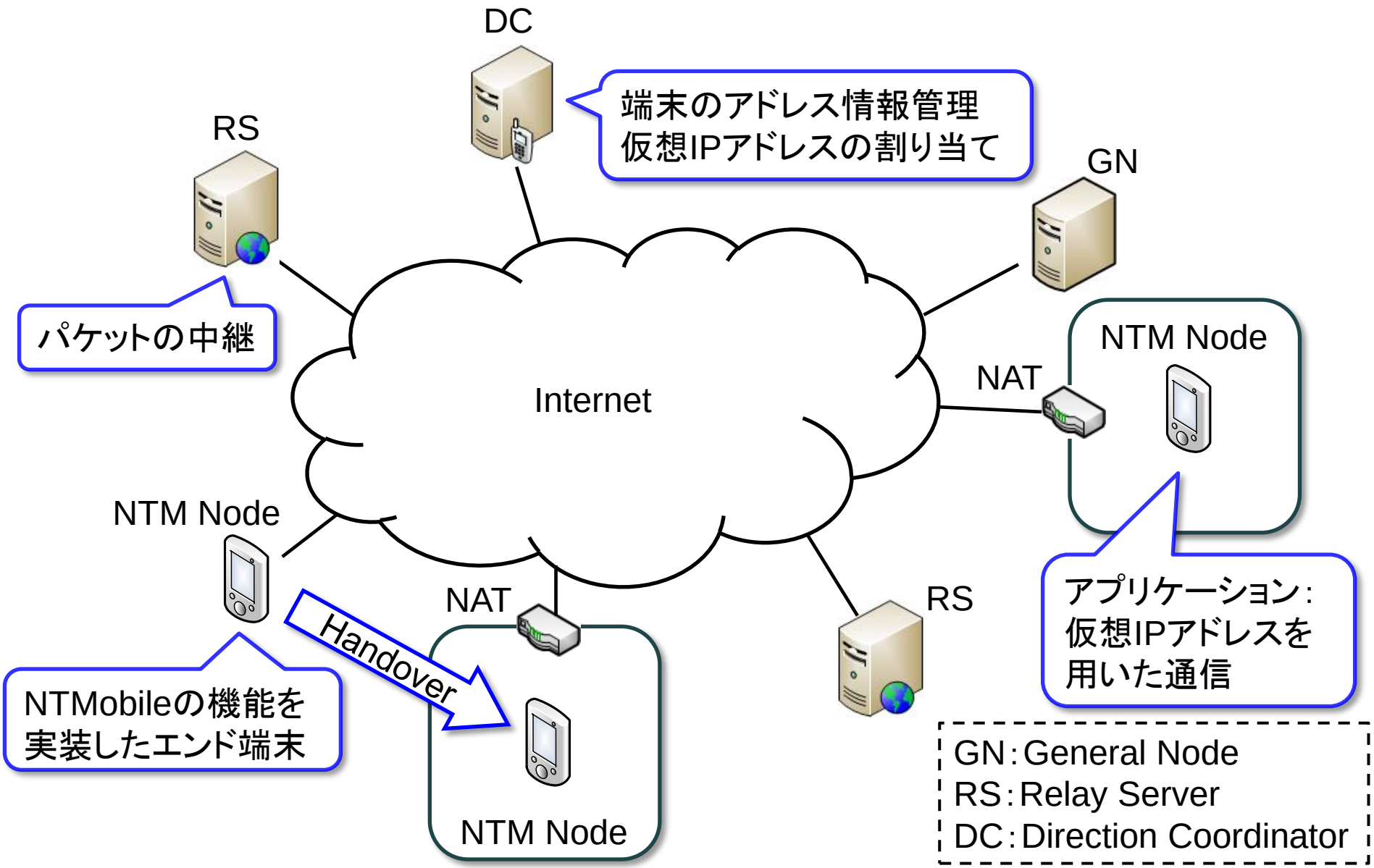
Watanabe Lab.

NAT：Network Address Translation

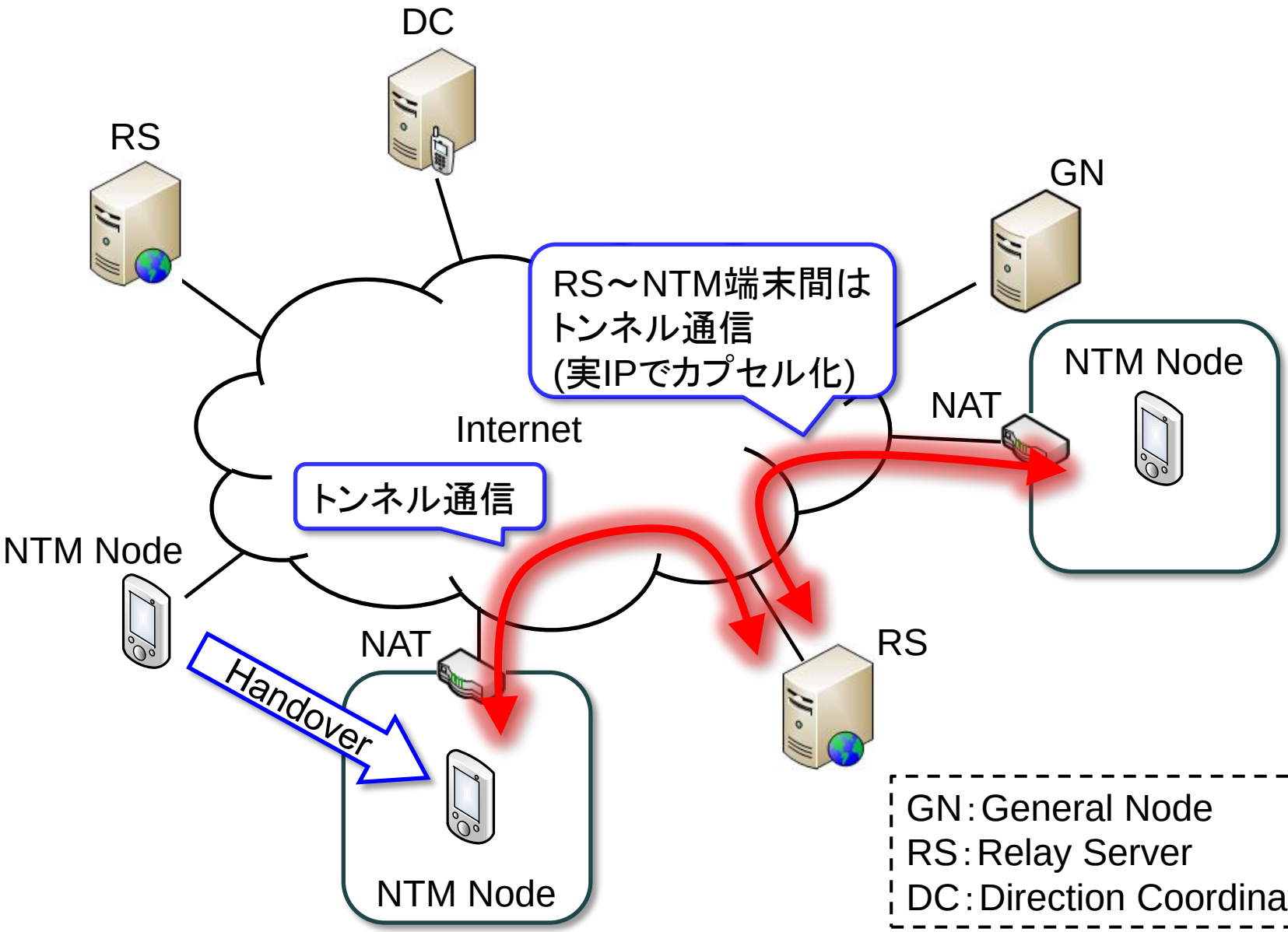
- 移動しながら通信をしたいという要求
  - 公衆無線網や小型端末(スマートフォンなど)の普及
- 移動透過性技術の必要性
  - IPネットワークでは接続場所が変わるとIPアドレスが変化
  - 端末が移動すると通信が途切れてしまう
  - 携帯通信網トラヒック量増大によるWi-Fiへのトラヒック迂回
- NAT越え技術の必要性
  - IPネットワークではNATの利用が一般的
  - NATの外側から内側にアクセスを開始できない

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

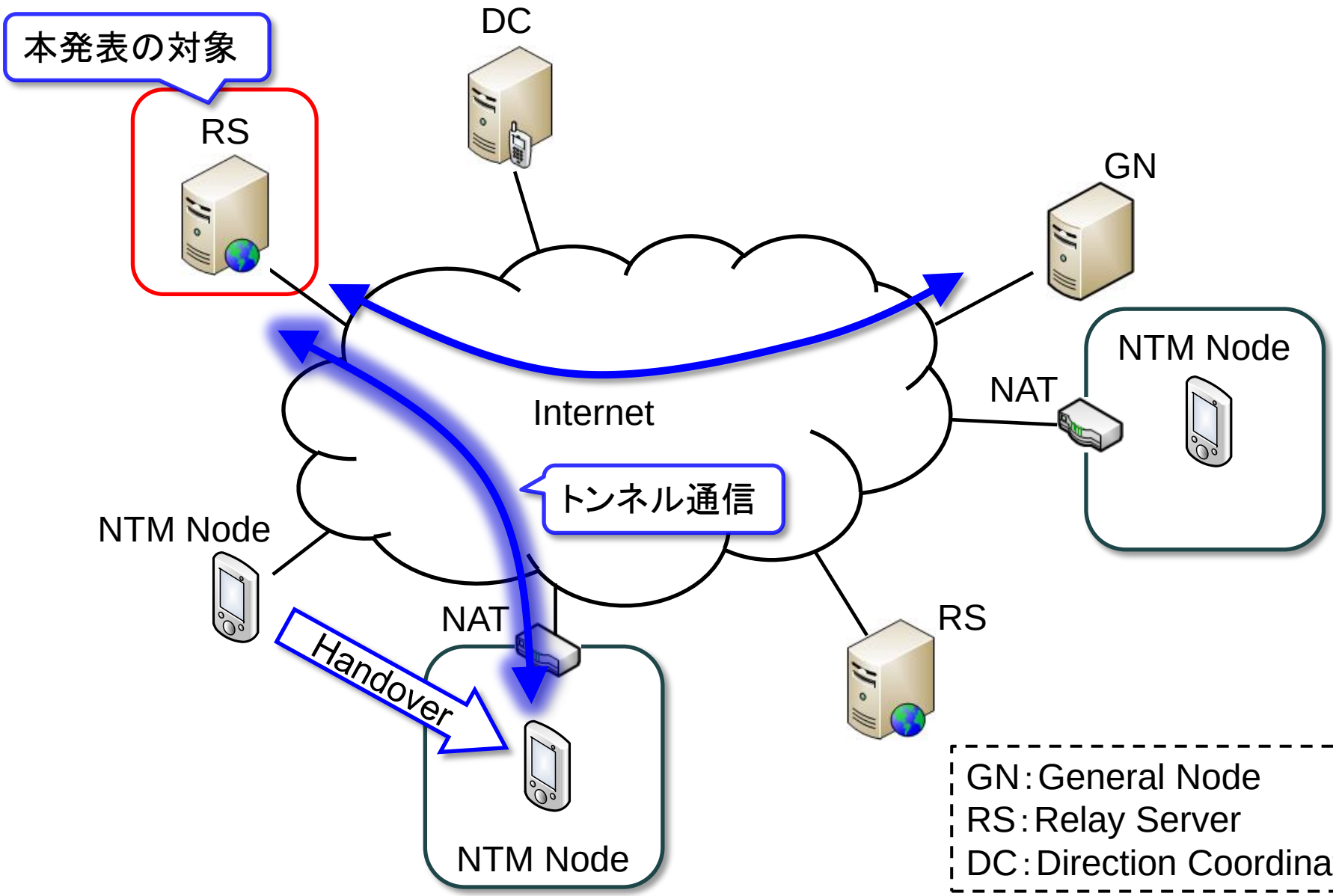
NTMobileの概要



NTMobileの概要



NTMobileの概要



RSの概要

- RS(Relay Server)
  - 特定の条件下においてパケットを中継するサーバ
  - 利用場面によって2つの種類に分かれている
- グローバルネットワーク上に設置し，分散配置が可能
  - 通信負荷等を考慮したRSの選択が可能

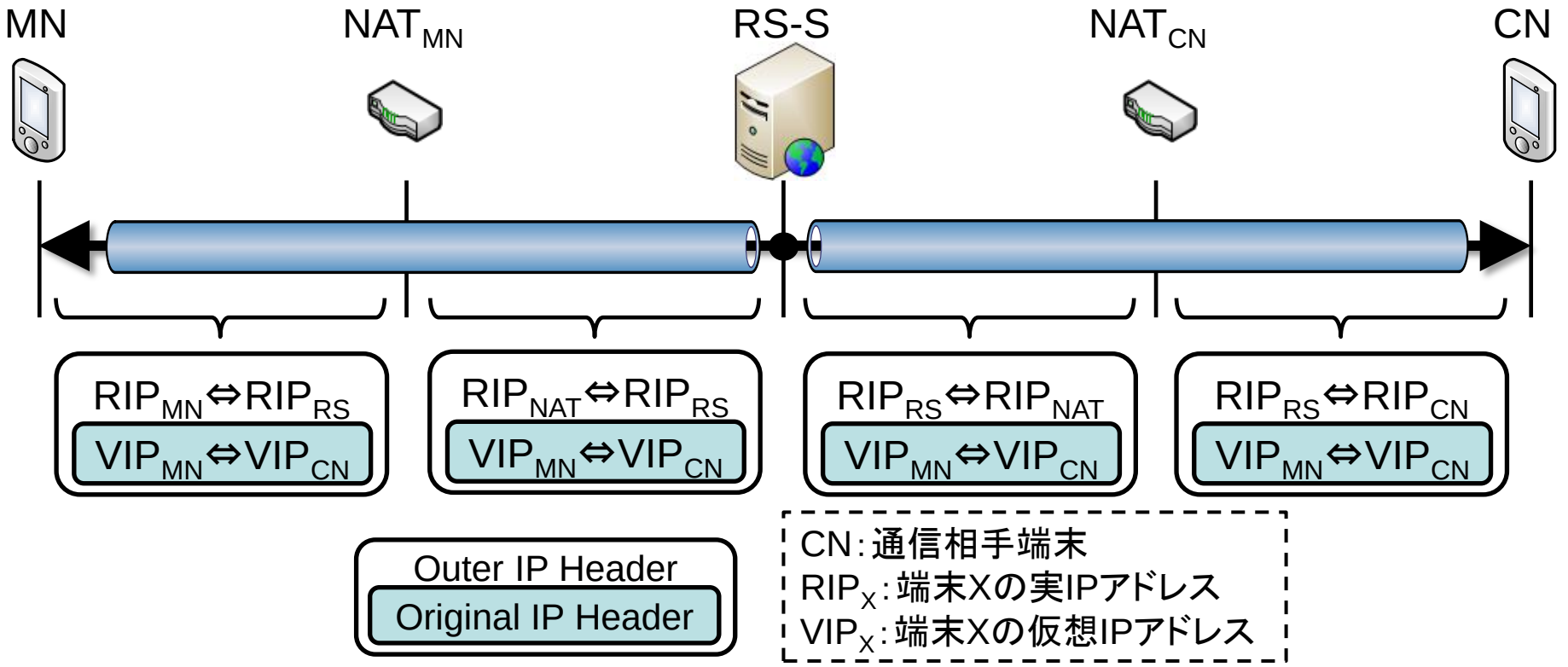
- トンネル切替型RS(RS-S：Relay Server type Switch)
  - 既に実装・評価を行っている
- アドレス変換型RS(RS-N：Relay Server type NAT)
  - 大まかな装置の定義のみで，詳細な仕様などの検討は行われていない

本研究の目的

RS-Nの動作や仕様の検討を行って実装し，動作検証・評価を行う

RS-Sの概要

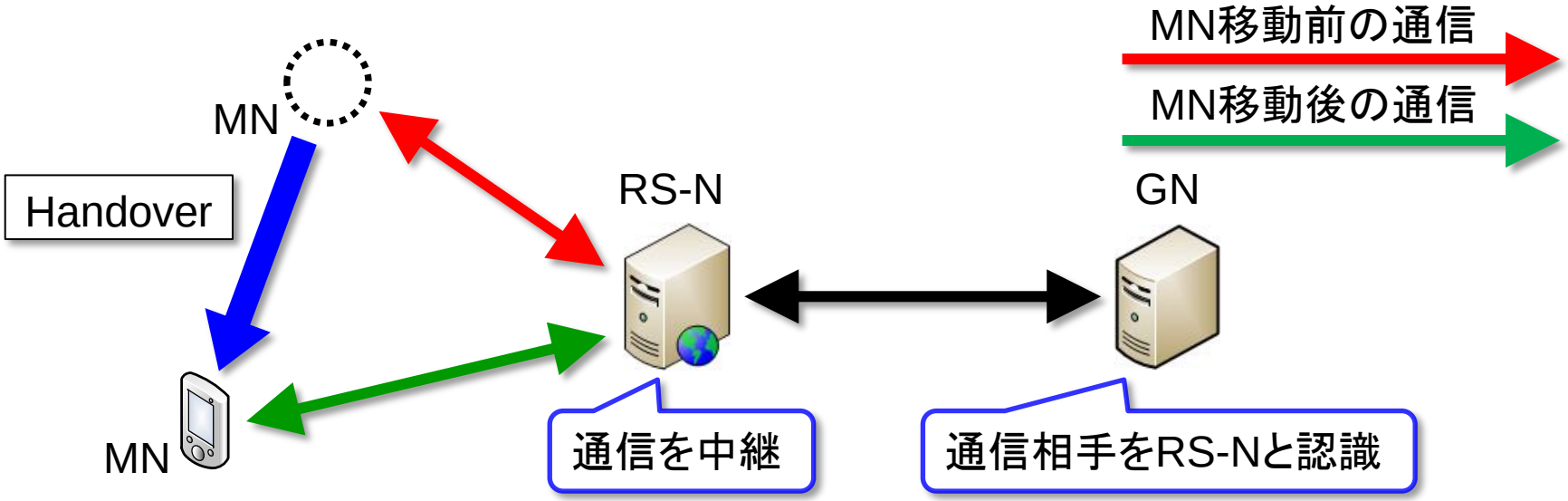
- トンネル切替型RS(RS-S：Relay Server type Switch)
  - 異なるNAT配下に存在するNTM端末が通信したい場合に利用
- MN～RS-S間，RS-S～CN間でトンネルを構築
  - 直接通信できる場合はエンドエンド通信に経路最適化できる



RS-Nの概要

- アドレス変換型RS(RS-N：Relay Server type NAT)
  - 通信相手端末がGNで，MNが移動しながら通信をしたい場合に利用

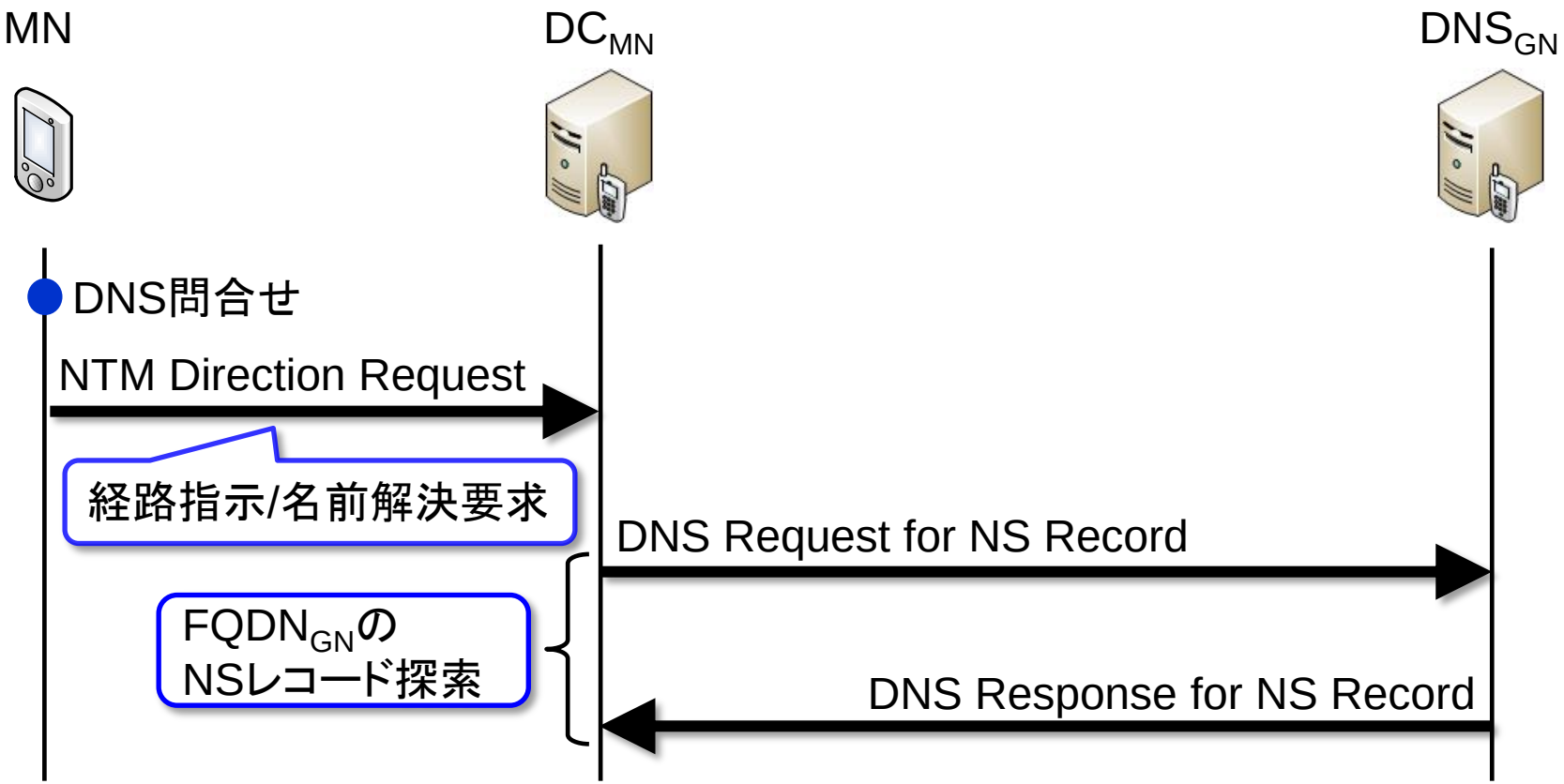
- MN～RS-N間でトンネルを構築
  - MN～GN間の通信はRS-Nを経由
  - MNが移動した場合はMN～RS-N間のトンネルを再構築
  - GNは通信相手をRS-Nと認識することで通信を継続できる



トンネル構築シーケンス(RS-N経由)

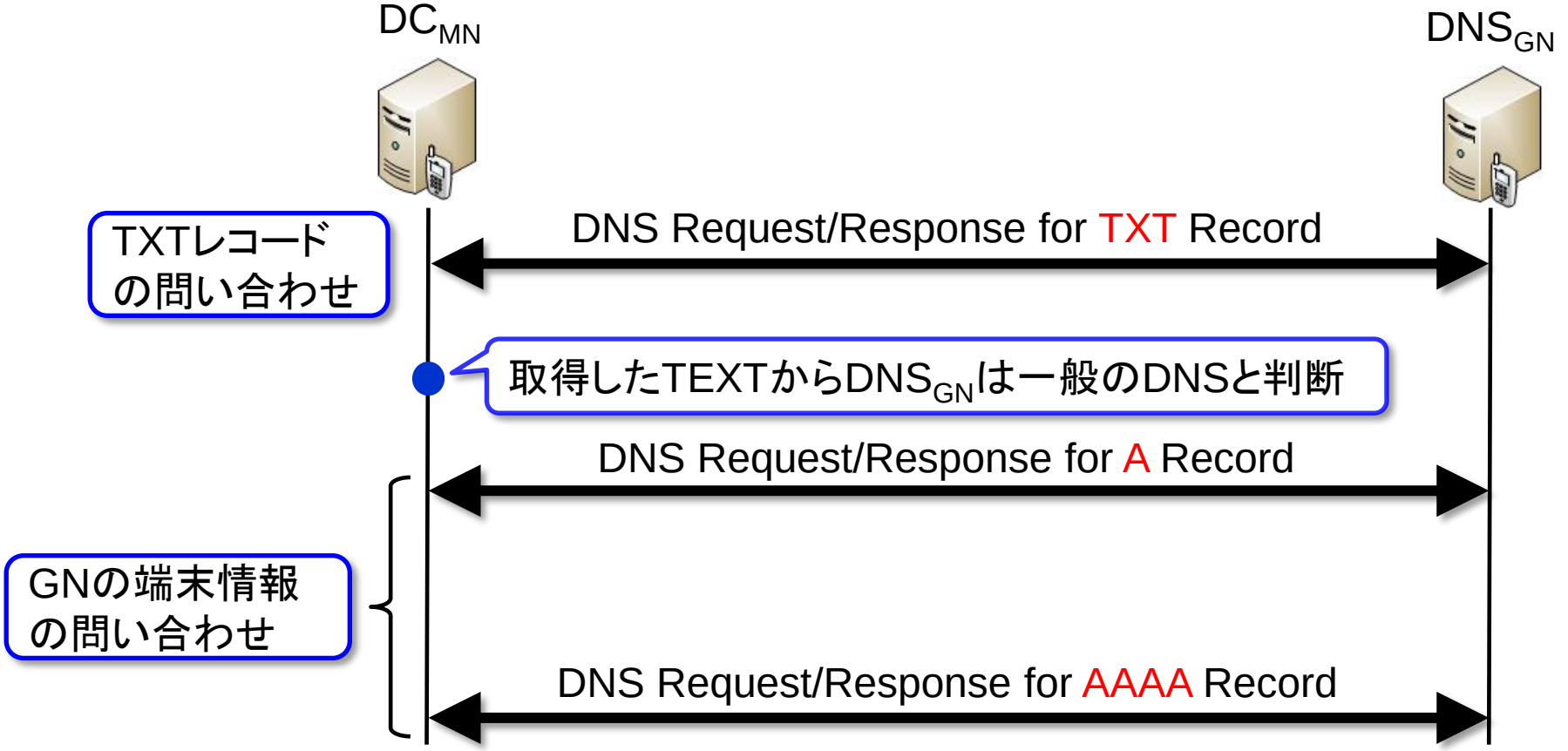
- DNS問合せをトリガーとして動作開始
  - MNがDC_{MN}に経路指示と名前解決を要求
- NSレコードを利用してDNS_{GN}を探索

GN:通信相手の一般端末
DNS_{GN}:GNを管理するDNSサーバ



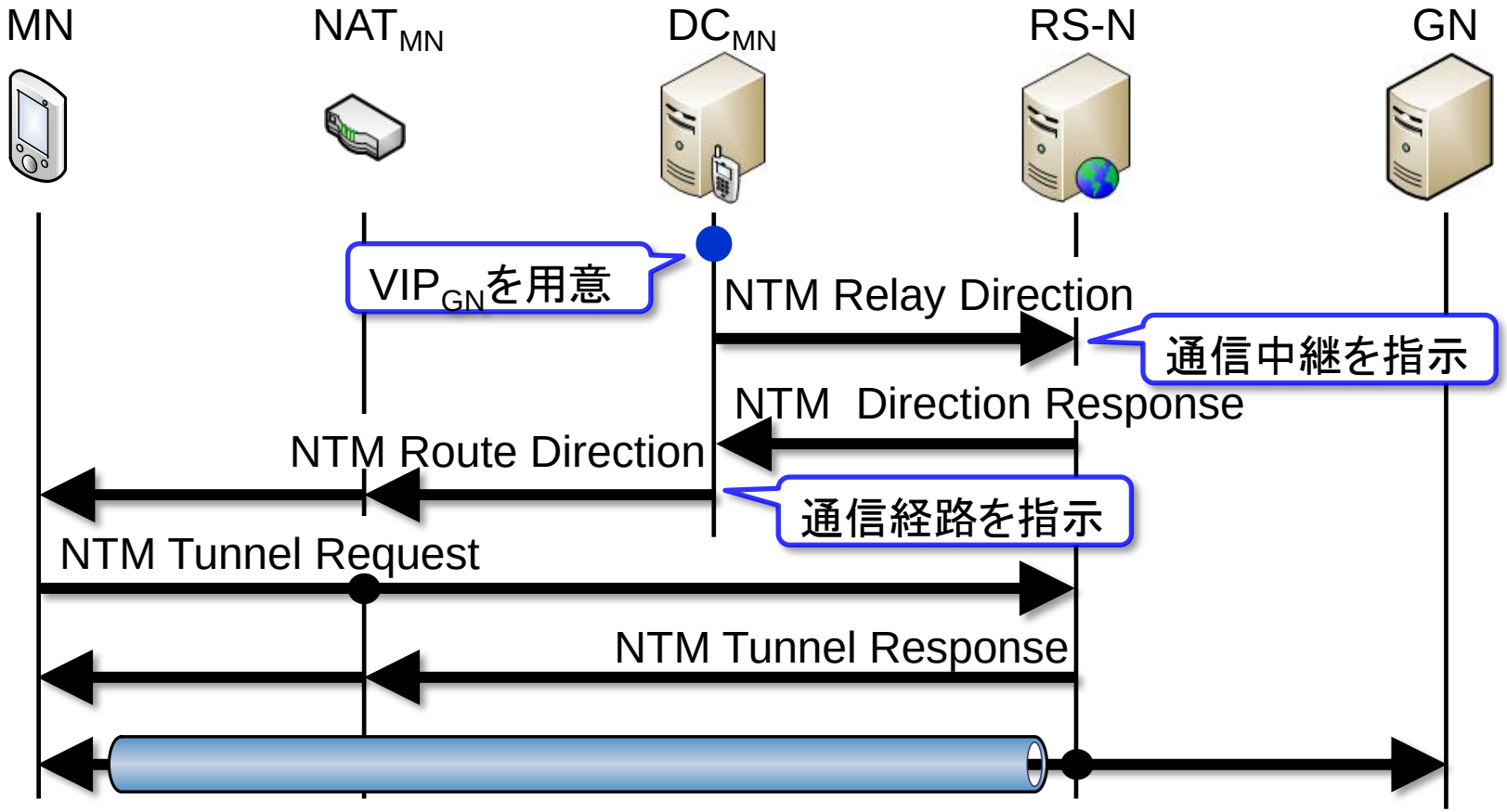
トンネル構築シーケンス(RS-N経由)

- 相手端末を管理するDNSがNTMobileに対応しているか判断
  - DCか一般のDNSサーバを判断
- 直接A/AAAAレコードの問合せ



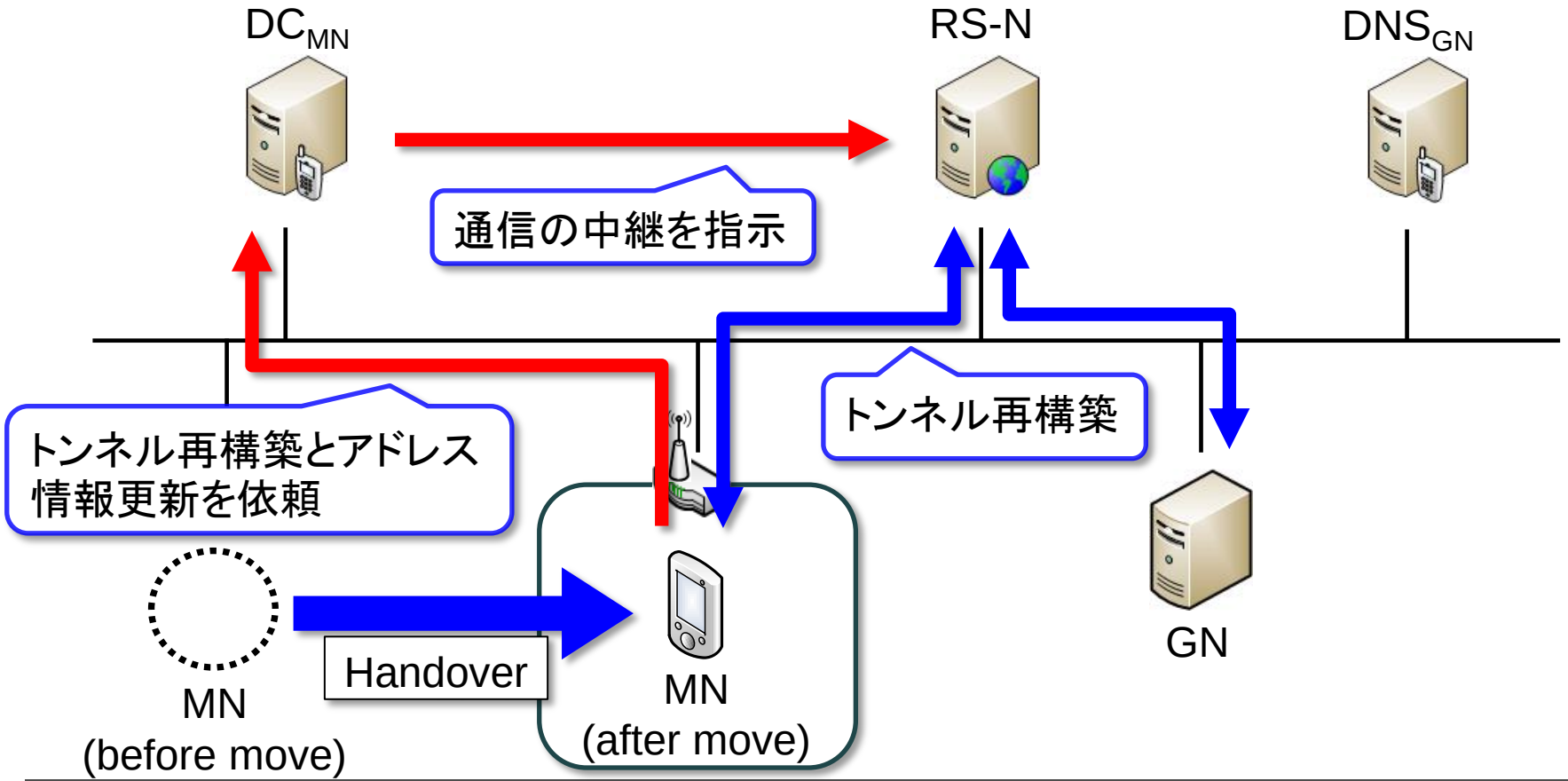
トンネル構築シーケンス(RS-N経由)

- 一般端末に対応する仮想IPアドレス(VIP_{GN})
  - DCに割り振られているアドレス空間の範囲から選択，MNとRS-Nに通知
  - MNはVIP_{GN}を通信相手の仮想IPアドレスとして認識



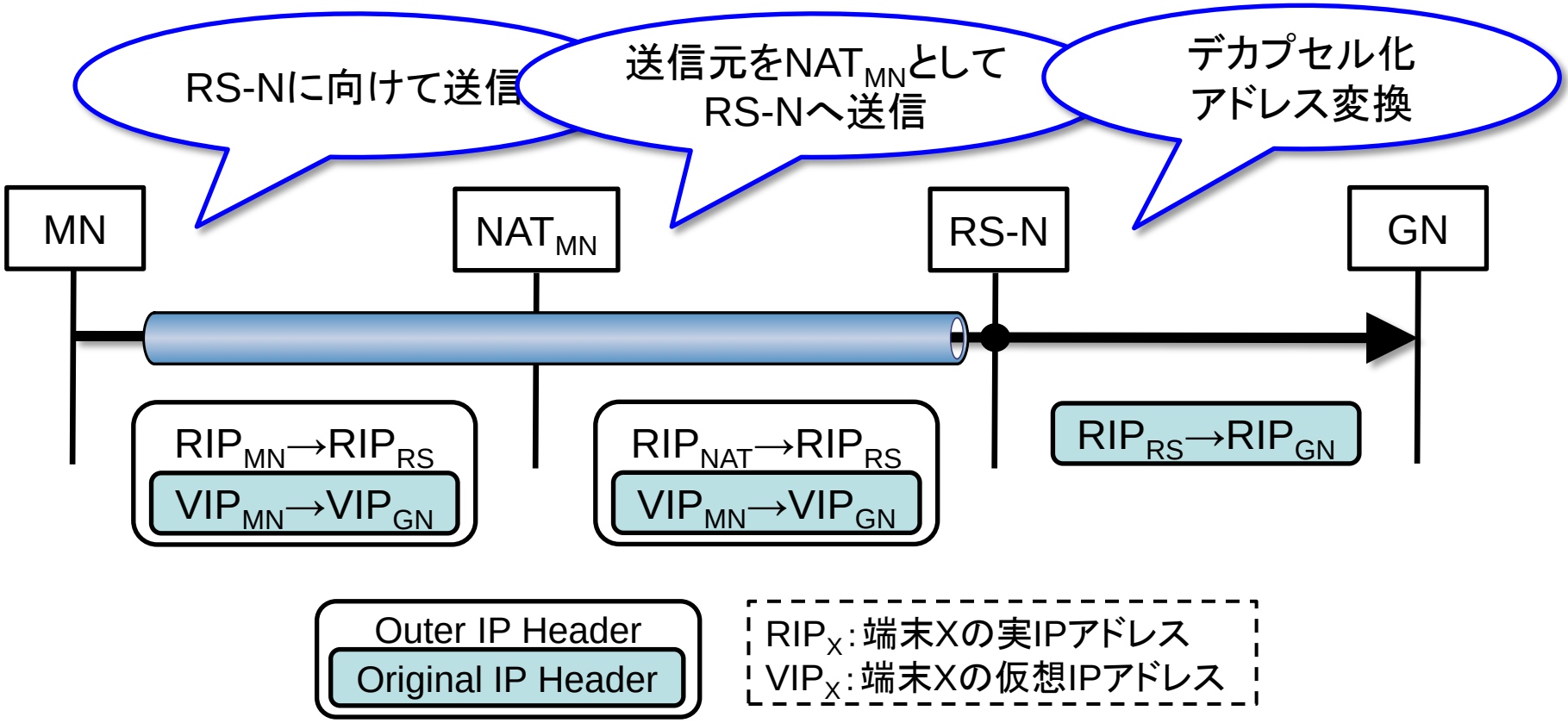
ハンドオーバ時の動作(MNが移動)

- MNが異なるNAT配下にハンドオーバ
  - DC_{MN}に対してアドレス情報更新とトンネル再構築を依頼
- MN～RS-N間でトンネル再構築



トンネル通信の様子(MNからGN)

- MN～RS-N間，RS-N～GN間のパケットの様子
- RS-Nはパケットをカプセル化/デカプセル化+アドレス変換
  - GNは通信相手をRS-Nと認識



RS-Nの実装方針

- Netfilterを利用したアドレス変換
  - Netfilter：Linuxに組み込まれているパケットフィルタリングの仕組み
  - RS-Nのパケット送信時に送信元ポートを自動選択できる
  - ペイロードにIPアドレスを含むプロトコルに対応できる
    - NetfilterのモジュールがALGの働きをしてペイロード内のIPアドレスを変換
  - パケットのフックにも用いる

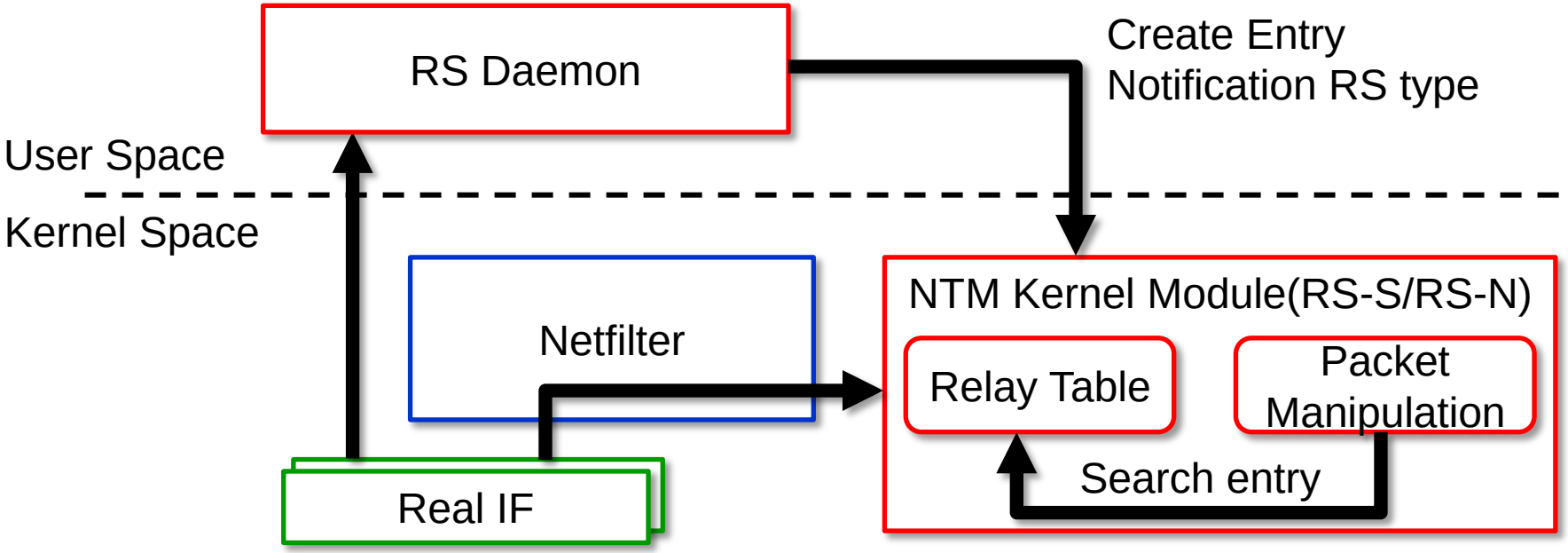
- RS-Sへの統合
  - RS-SとRS-Nを統合すれば1端末でRS-S/RS-Nを実現できる
  - 別の実装とするよりもネットワークに設置するRSの台数が少なくて済む

RS-Nの実装は既存のRS-Sを拡張する形態で設計を行う

ALG：Application Level Gateway

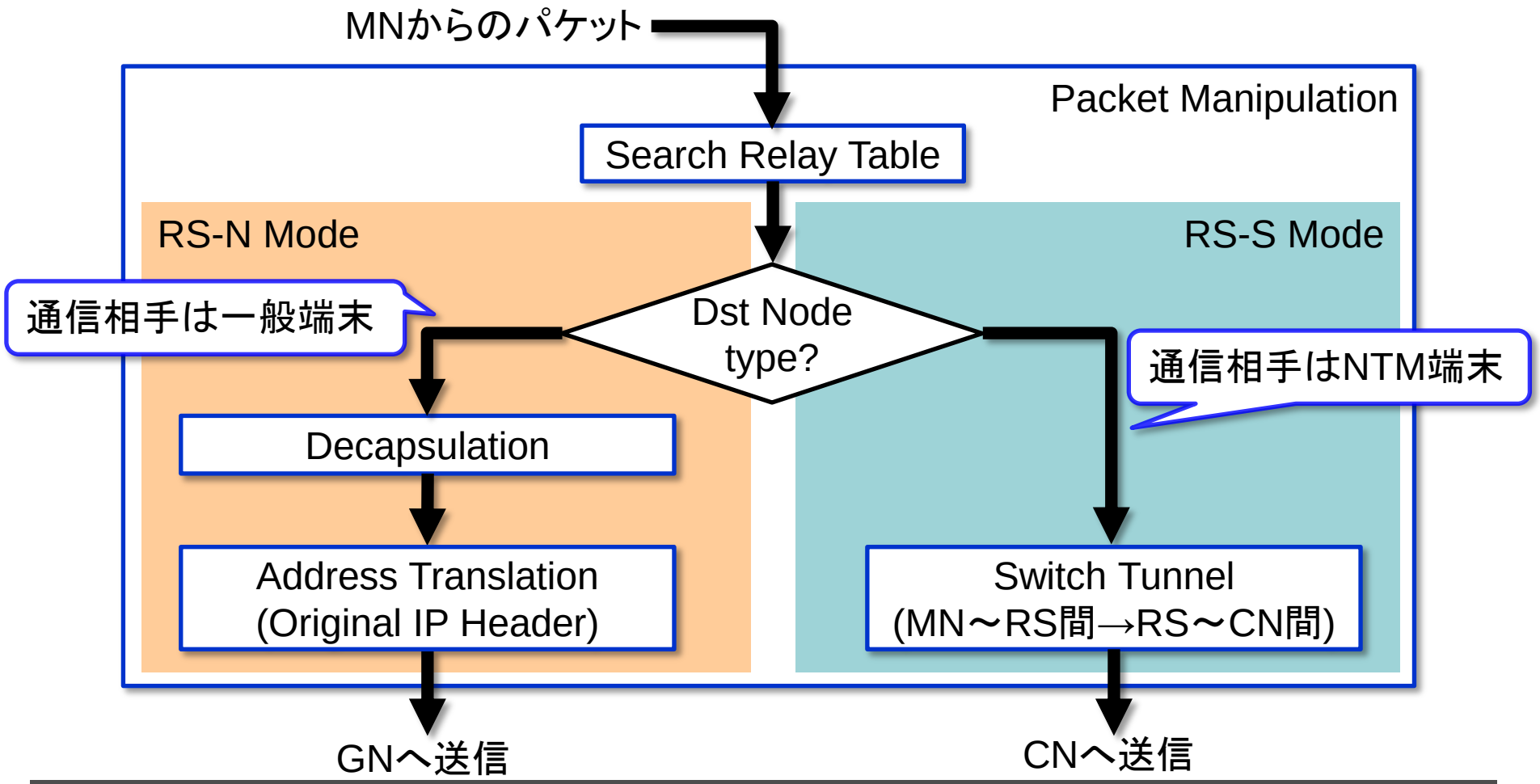
RS-Nの実装

- RSデーモン
  - 制御メッセージの受信/送信処理
  - 転送に必要な情報やRSのタイプをカーネルモジュールに通知
- NTMobileカーネルモジュール
  - Netfilterでパケットをフックしアドレス変換やカプセル化/デカプセル化
  - 転送に用いる情報を記録するRelay Tableを持つ



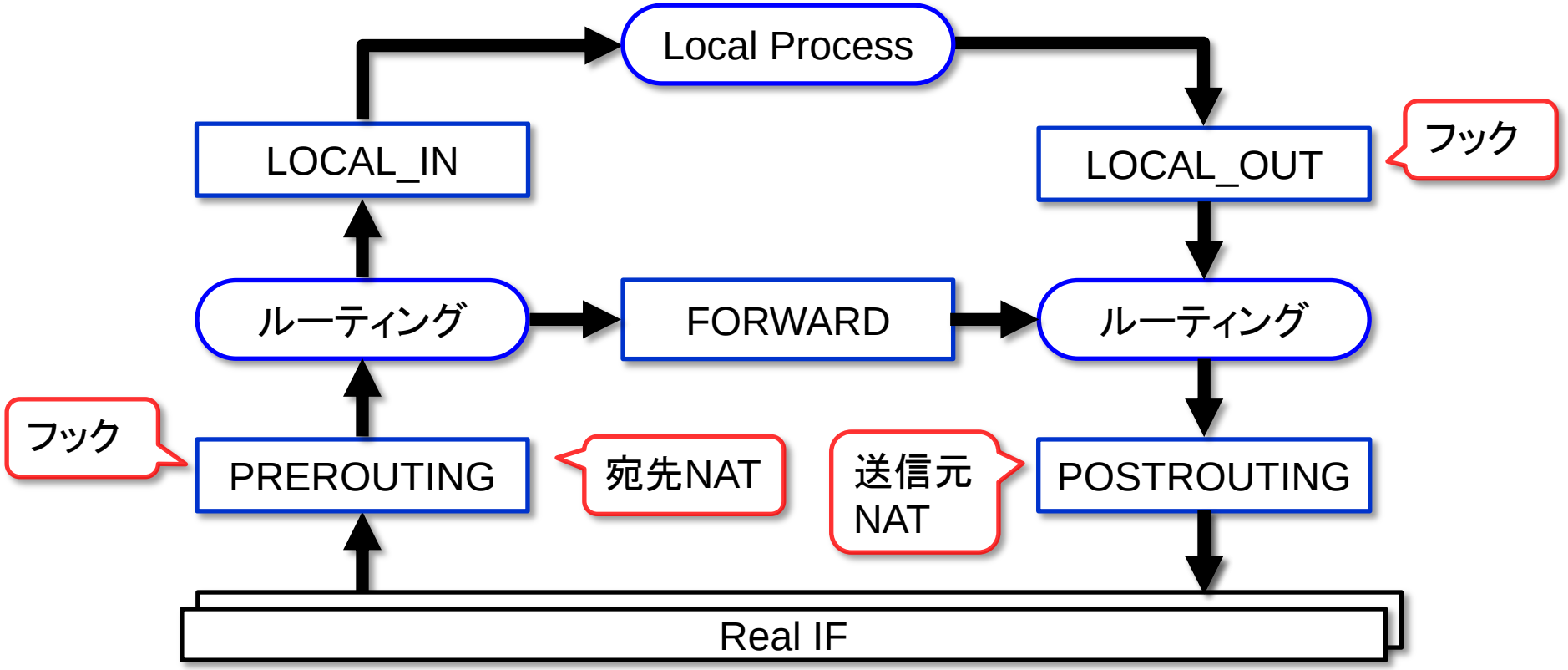
RS-SとRS-Nの使い分け

- RS-Nはパケットを受信するとRelay Tableを検索
  - 相手端末がNTM端末か一般端末かを調べる



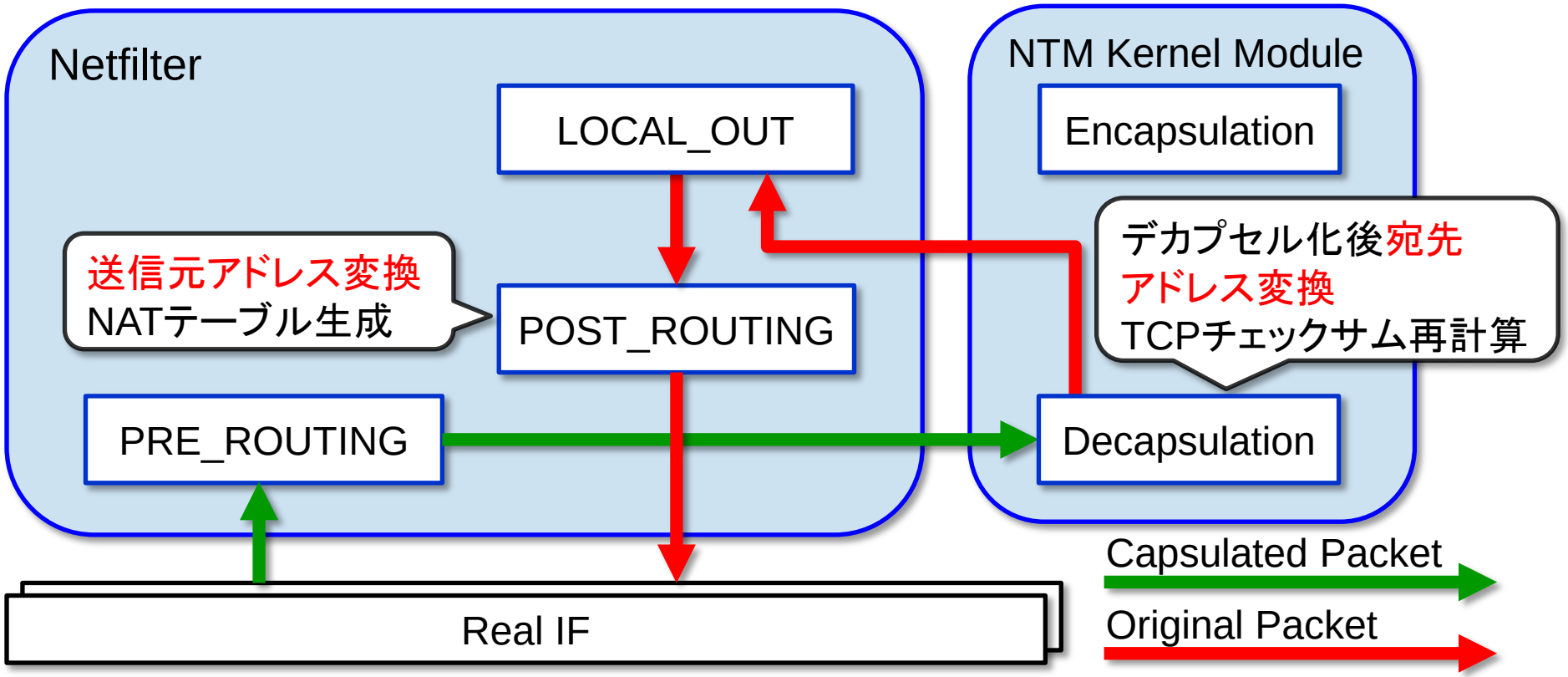
Netfilterの概要

- 複数のチェインで構成
  - チェイン：パケットを操作するルールのリスト
  - 各チェインでルールにマッチするか調べ，次のチェインへ渡す
  - PREROUTINGとLOCAL_OUTでフックし，NTMobileの処理を行う



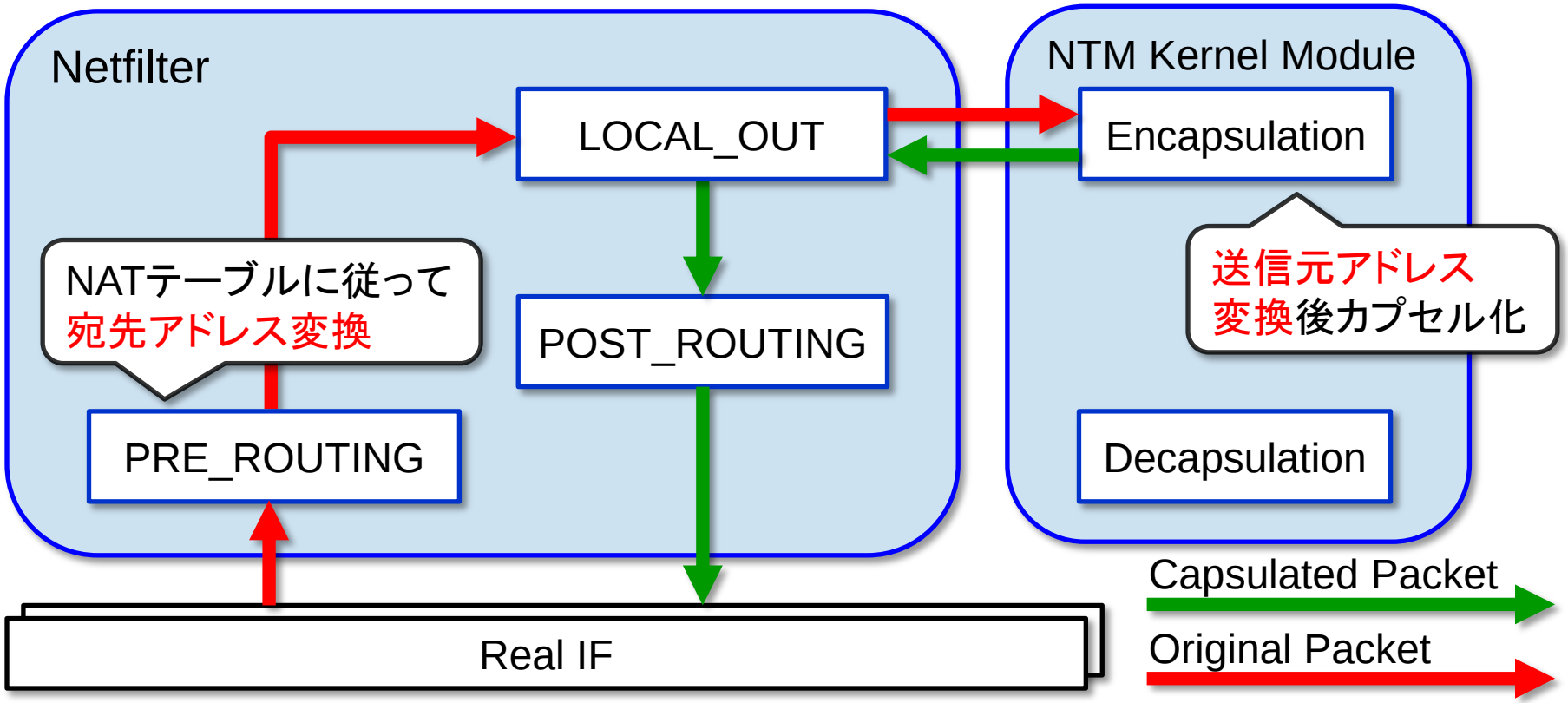
アドレス変換の様子(MNからのパケット)

- 宛先アドレス変換時にTCPチェックサムを再計算
  - Netfilterのチェックサム再計算時に宛先NATが考慮されていないため
- POST_ROUTINGにアドレス変換のルールを設定
  - 送信元が仮想IPアドレスのパケットを送信元NAT



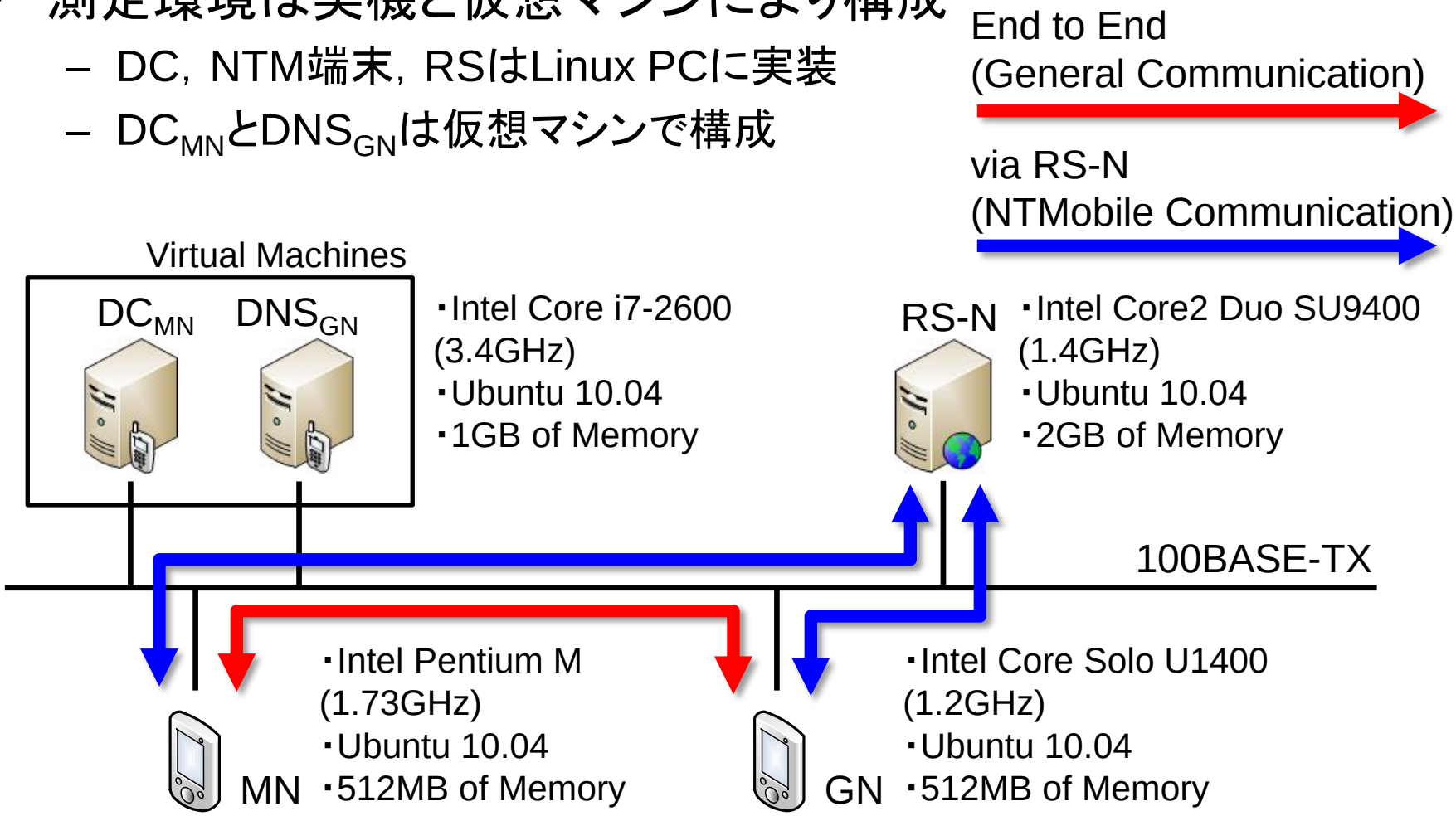
アドレス変換の様子(GNからのパケット)

- 送信時に作られたNATテーブルに従ってDNAT
- LOCAL_OUTで宛先が仮想IPアドレスであるとフック
  - 送信元NATしてカプセル化した後LOCAL_OUTに戻す



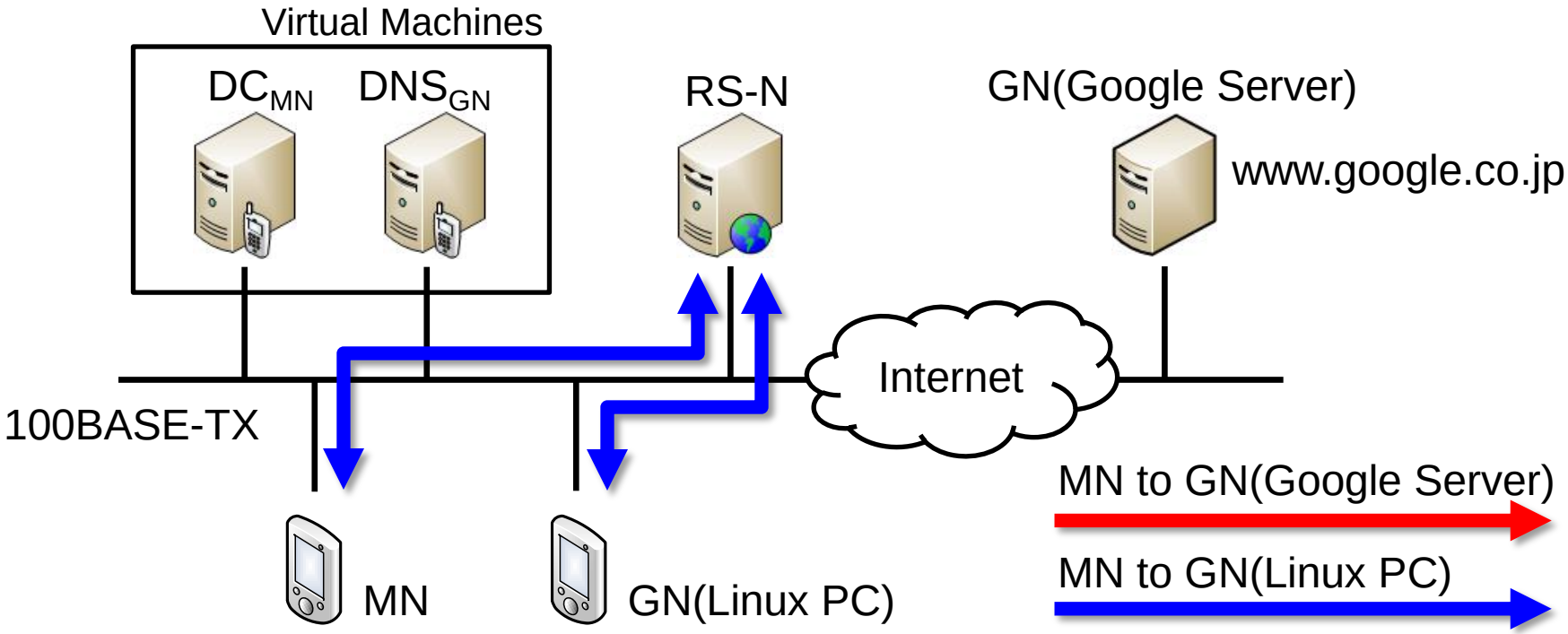
動作検証・性能評価

- 目的：RS-Nの動作検証とスループット低下率の評価
- 測定環境は実機と仮想マシンにより構成
  - DC，NTM端末，RSはLinux PCに実装
  - DC_{MN}とDNS_{GN}は仮想マシンで構成



動作検証

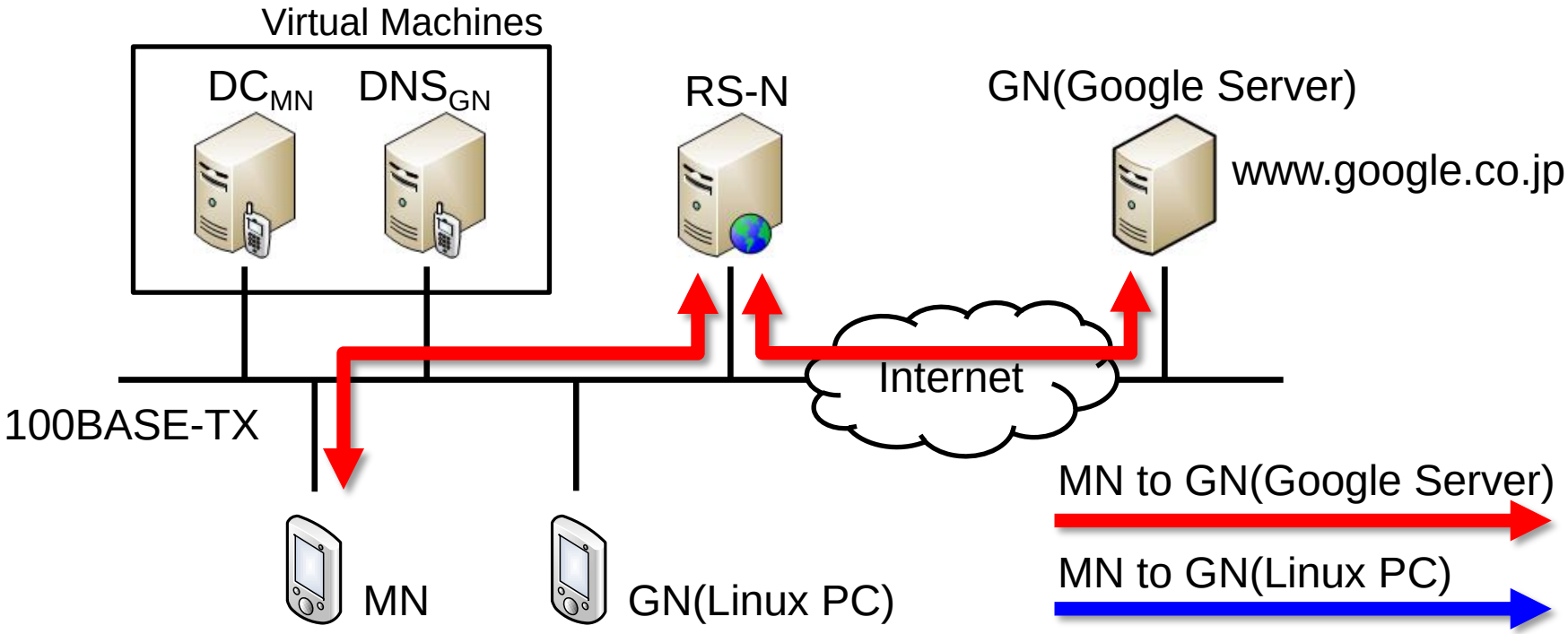
- 検証内容
  - MNからGNに向けてpingを実行
  - トンネル構築，トンネル通信ができるかどうか検証



MN～GN間でRS-Nを経由した通信が行われたことを確認した

動作検証

- 検証内容
  - MNからGNに向けてpingを実行
  - トンネル構築，トンネル通信ができるかどうか検証

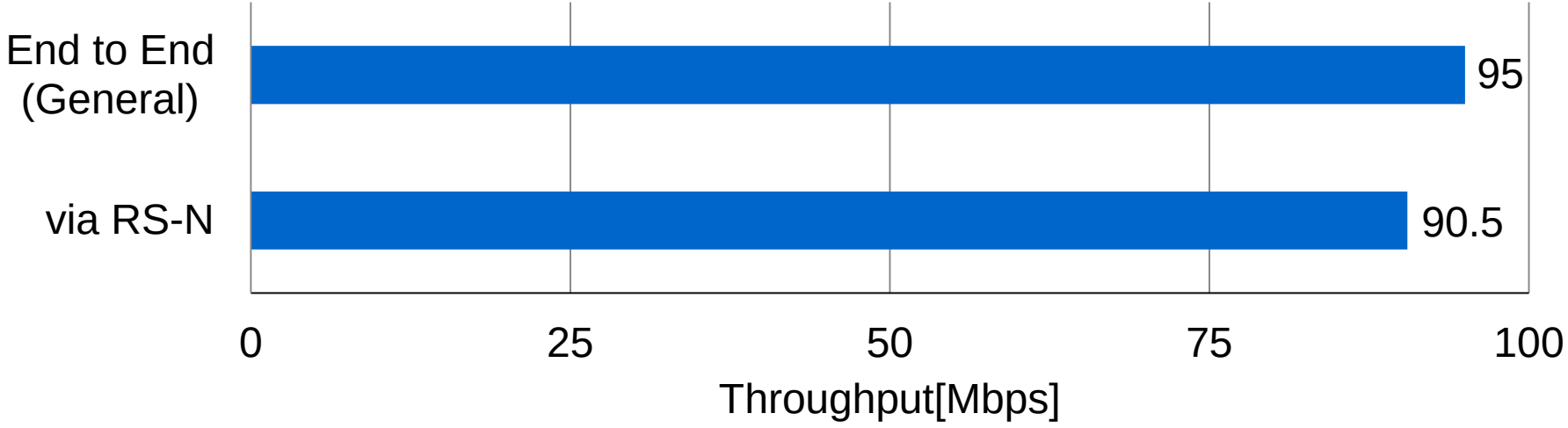


MN～GN間でRS-Nを経由した通信が行われたことを確認した

スループット測定結果

- エンドエンド通信とRS-N経由通信のスループット低下率を測定
  - iperfを用いたTCP通信を行い，MN～GN間のスループットを測定
    - RS-Nを経由したNTMobileの通信と端末間の一般的な通信を比較
  - 共通鍵交換手順は未実装であるため暗号化なしの状態

- スループットの低下率は5%程度となった
  - RS-Nの処理がスループット低下に大きな影響を及ぼさない



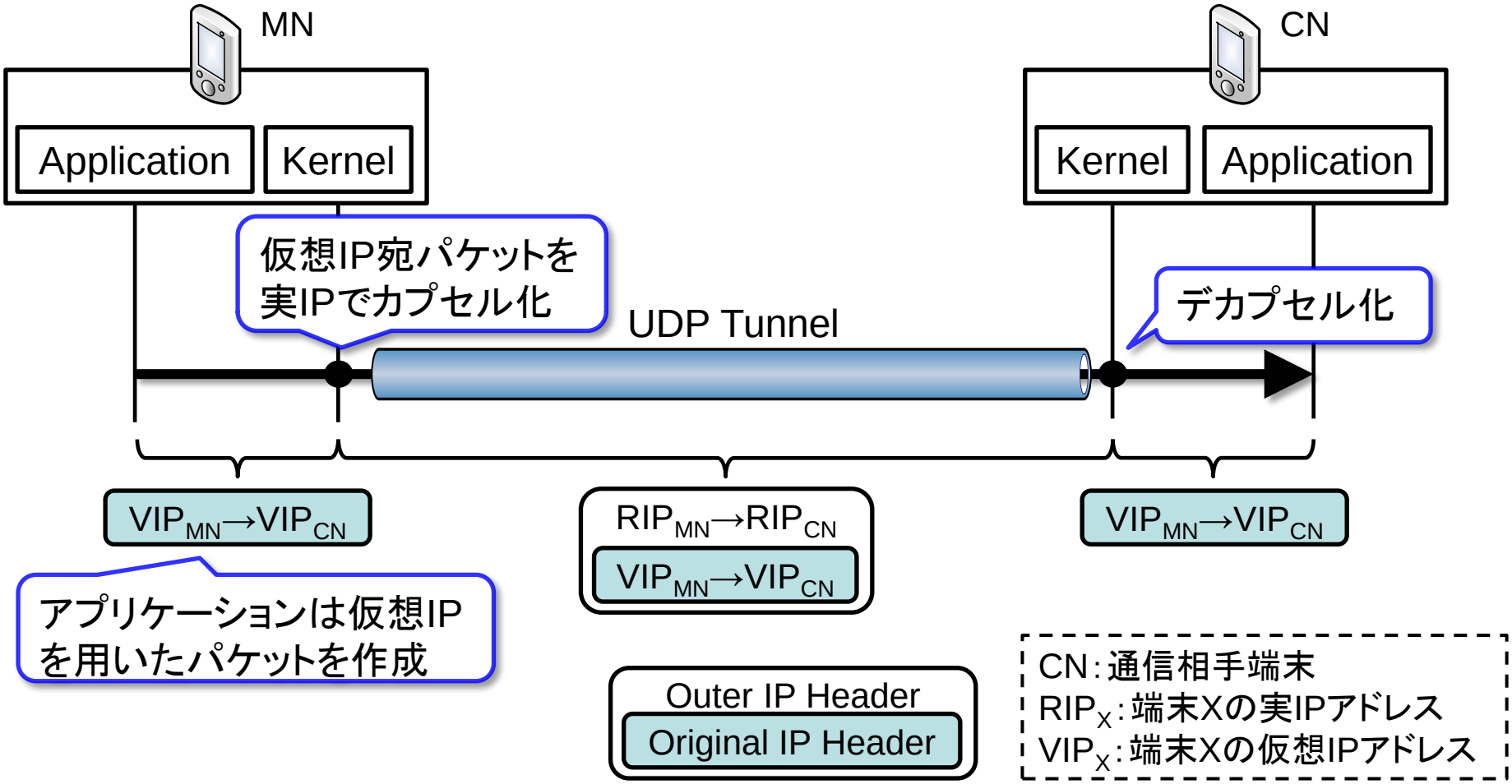
まとめ

- NTMobileの概要と動作
  - 仮想IPアドレスとUDPトンネルを使った通信
  - 移動透過性とNAT越えを同時に実現する技術
- RS-Nの概要と動作
  - 一般端末に対して移動通信を行いたい場合に利用
- RS-Nの実装と評価
  - RSの実装の設計
  - RS-NをLinux OSへ実装
  - エンドエンド通信とRS-N経由の通信におけるスループット評価

- 今後の予定
  - 共通鍵交換手順の実装
  - RS-Nの分散配置，選択手法の検討

トンネル通信の様子(MNからCN)

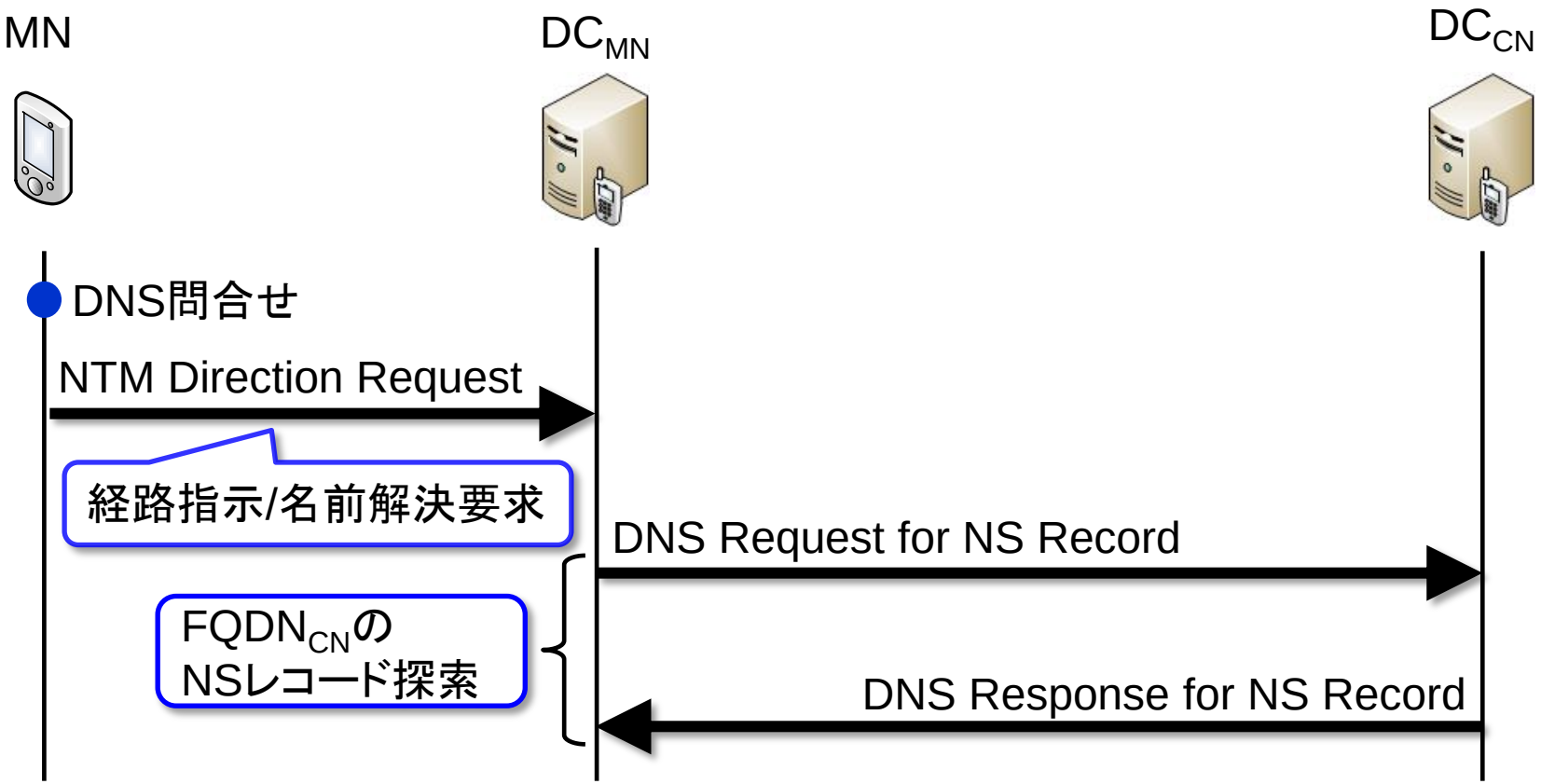
- アプリケーションは仮想IPアドレスを用いて通信
- カーネルではカプセル化/デカプセル化を行う



トンネル構築シーケンス(直接通信)

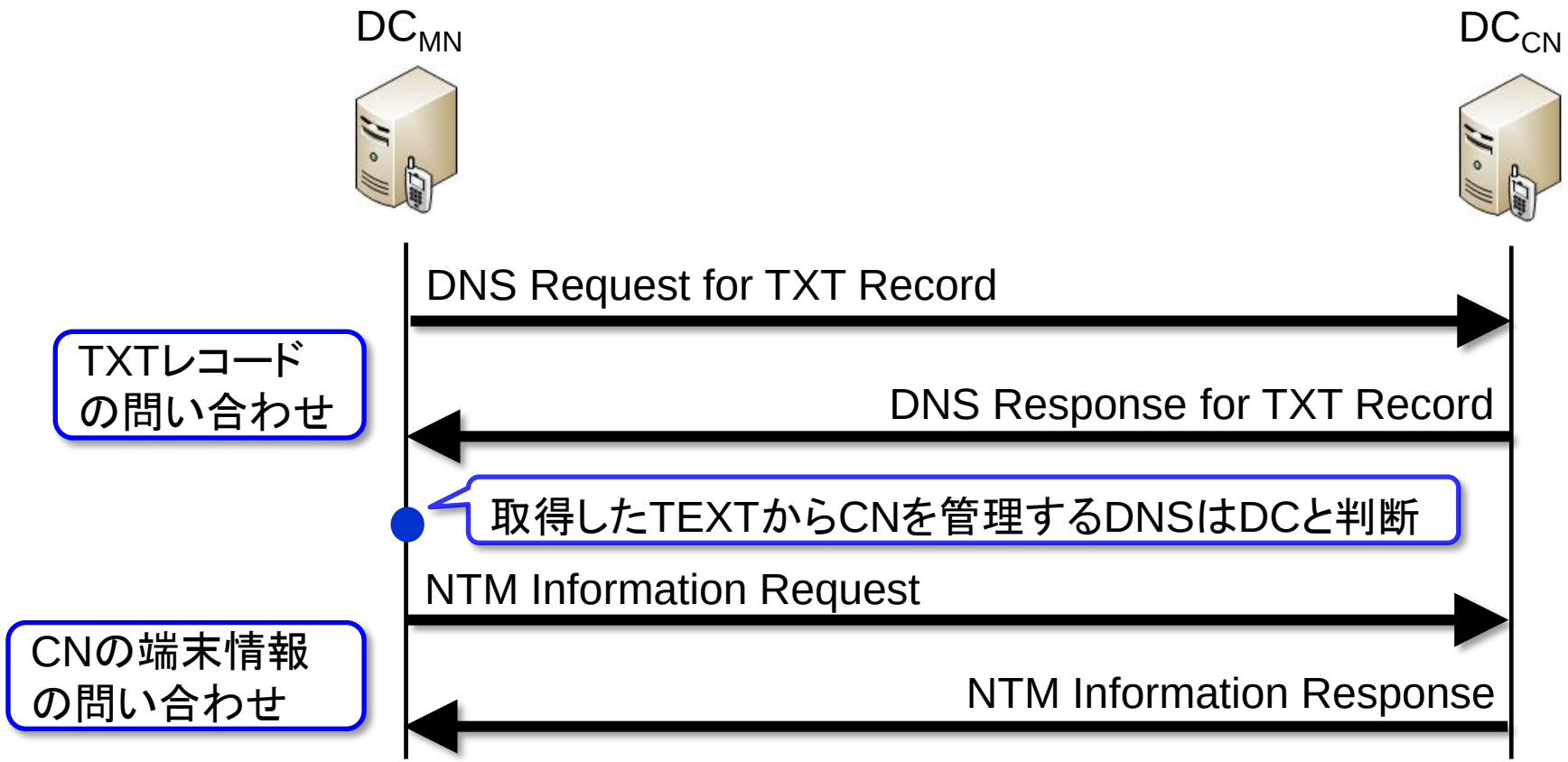
- DNS問合せをトリガーとして動作開始
  - MNがDC_{MN}に経路指示と名前解決を要求
- NSレコードを利用してDC_{CN}を探索

MN:通信開始側NTM端末
CN:通信相手側NTM端末

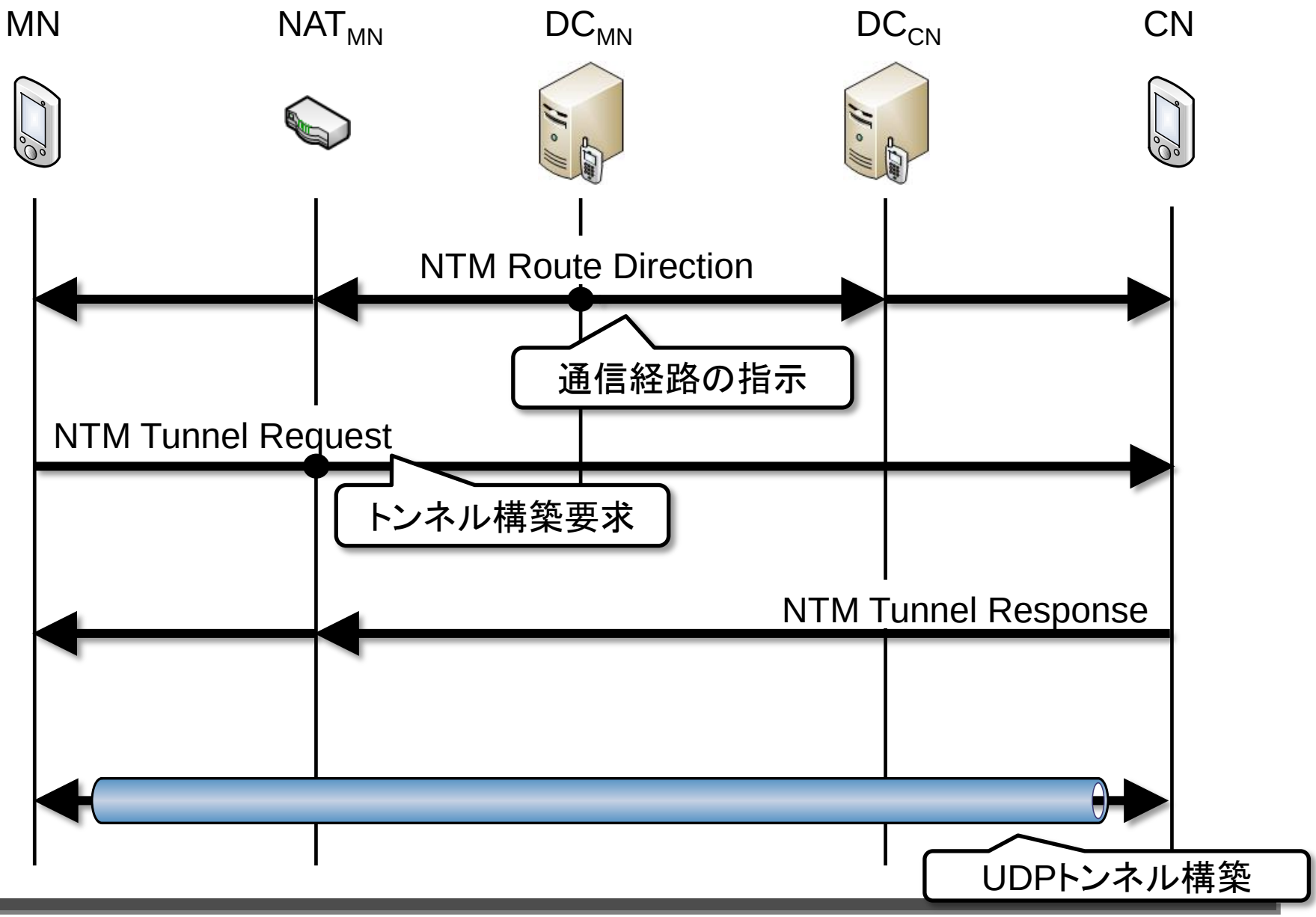


トンネル構築シーケンス(直接通信)

- 相手端末を管理するDNSがNTMobileに対応しているか判断
  - DCか一般のDNSサーバを判断
- DCどうしで直接通信し端末情報を取得



トンネル構築シーケンス(直接通信)



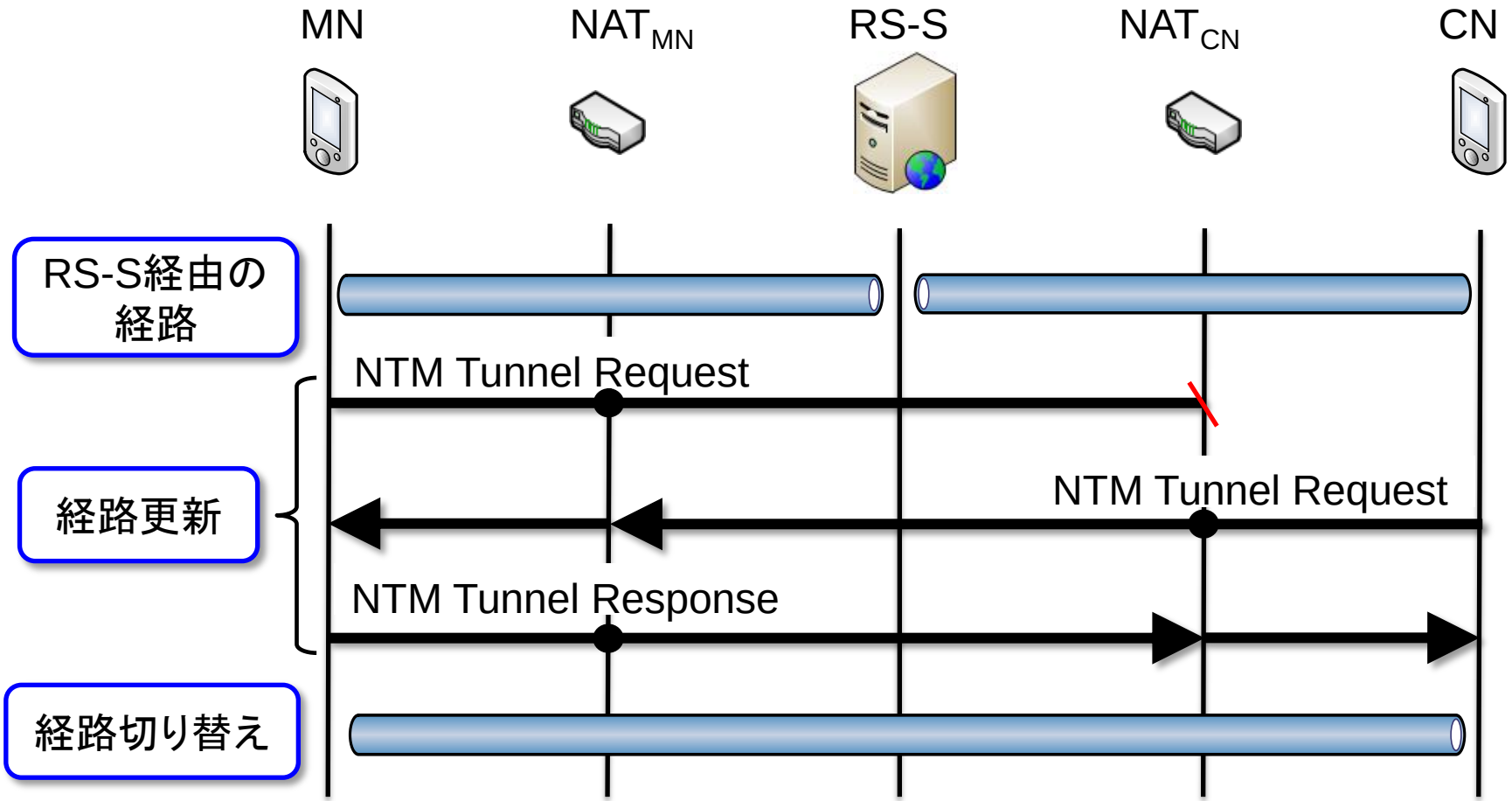
Relay Table

- RSが転送に必要な情報を保持するテーブル
- RS-Nを利用する場合のRelay Tableのエントリー一覧
  - NTM端末が一般端末と通信を行う場合

属性名	登録タイミング	内容	備考
Path ID	Relay Direction	$PID_{MN\text{-}CN}$	端末間の経路を示すPath ID
Common Key	Relay Direction	$Key_{MN\text{-}CN}$	共通鍵情報
Tunnel IP	Tunnel Request	RIP_{NAT_MN}	配下ノードに到達する IPアドレス
Tunnel Port	Tunnel Request	-	配下ノードに到達する ポート番号
Virtula IP			

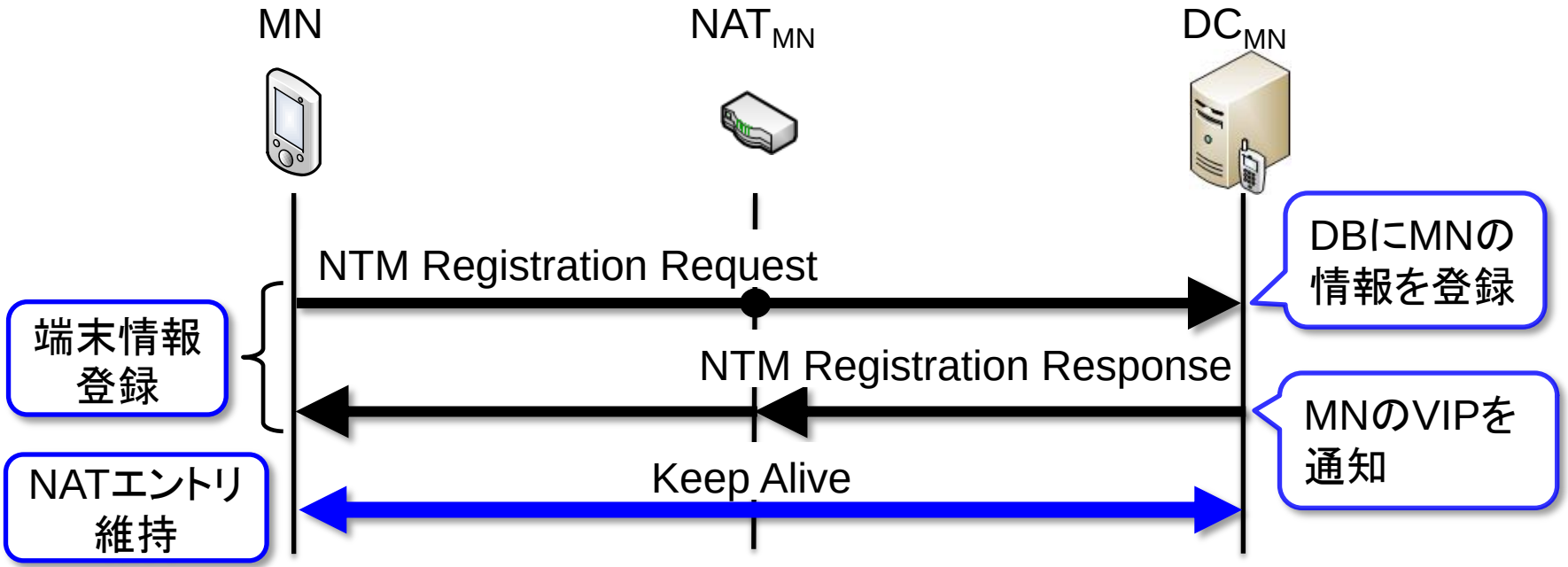
経路最適化

- 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



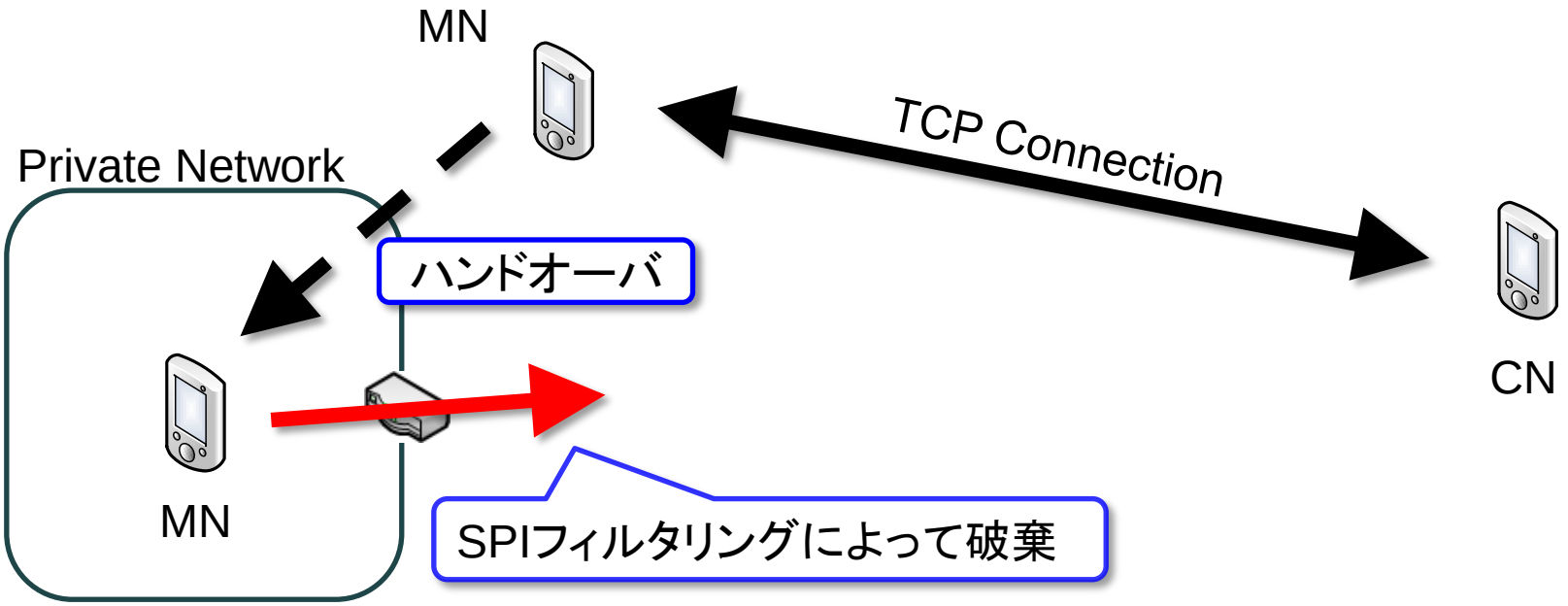
登録処理とKeep Alive

- 登録処理
  - NTM端末の起動時にDCに対して行う
  - 自身の位置情報を登録
- Keep Alive
  - 登録終了後MN～DC_{MN}間で定期的にメッセージのやり取りを行う
  - 制御メッセージ用の通信経路を確保



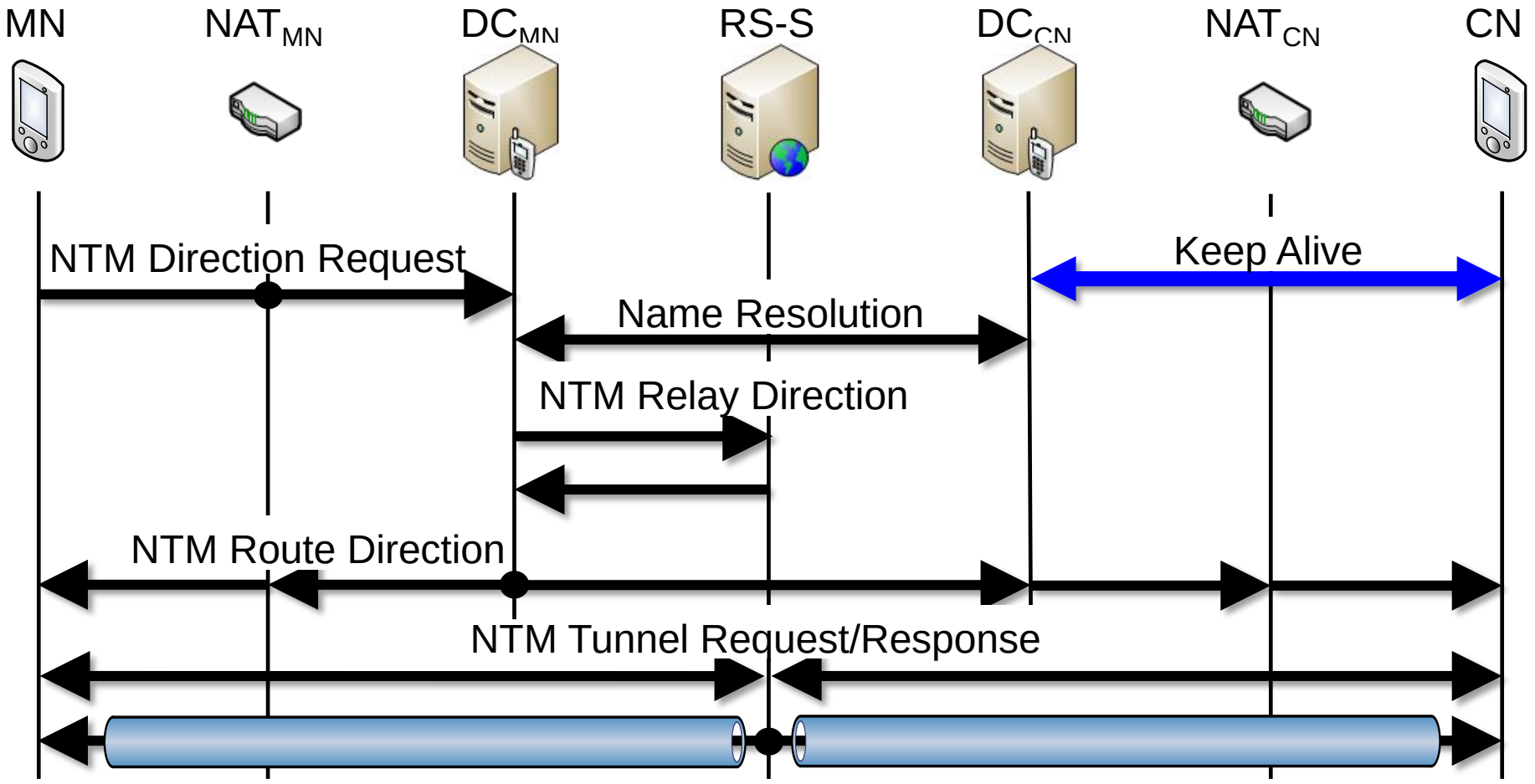
SPI(Stateful Packet Inspection)

- TCPのセッションを監視する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
- NATを跨った移動を行うとパケットが破棄される可能性
  - NTMobileではUDPトンネルを用いてこの問題を解決

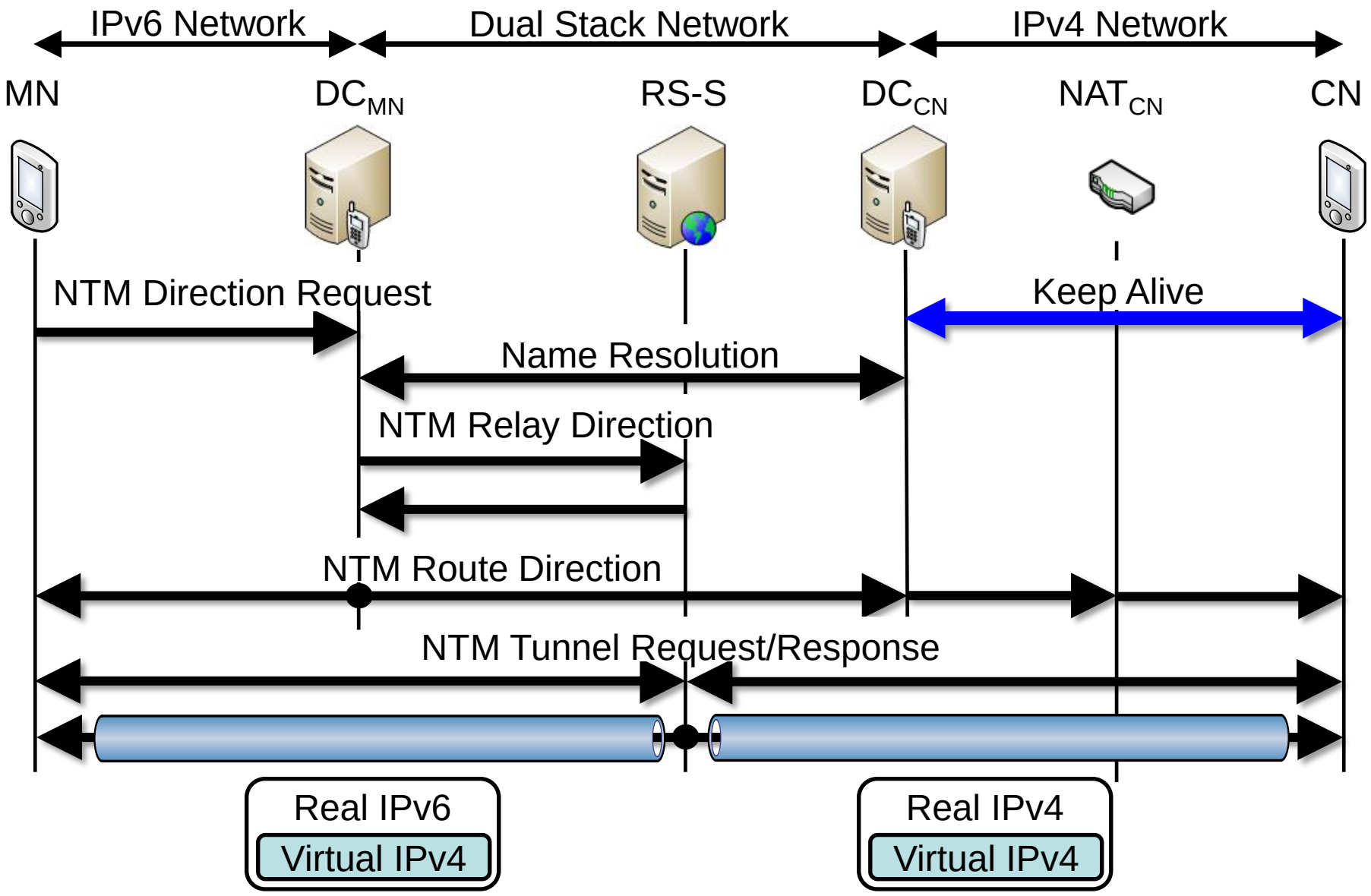


トンネル構築シーケンス(RS-S経由)

- DC_{CN}～CN間はKeep AliveでNATエントリを保持
- MN～RS-S，RS-S～CN間でトンネルを構築

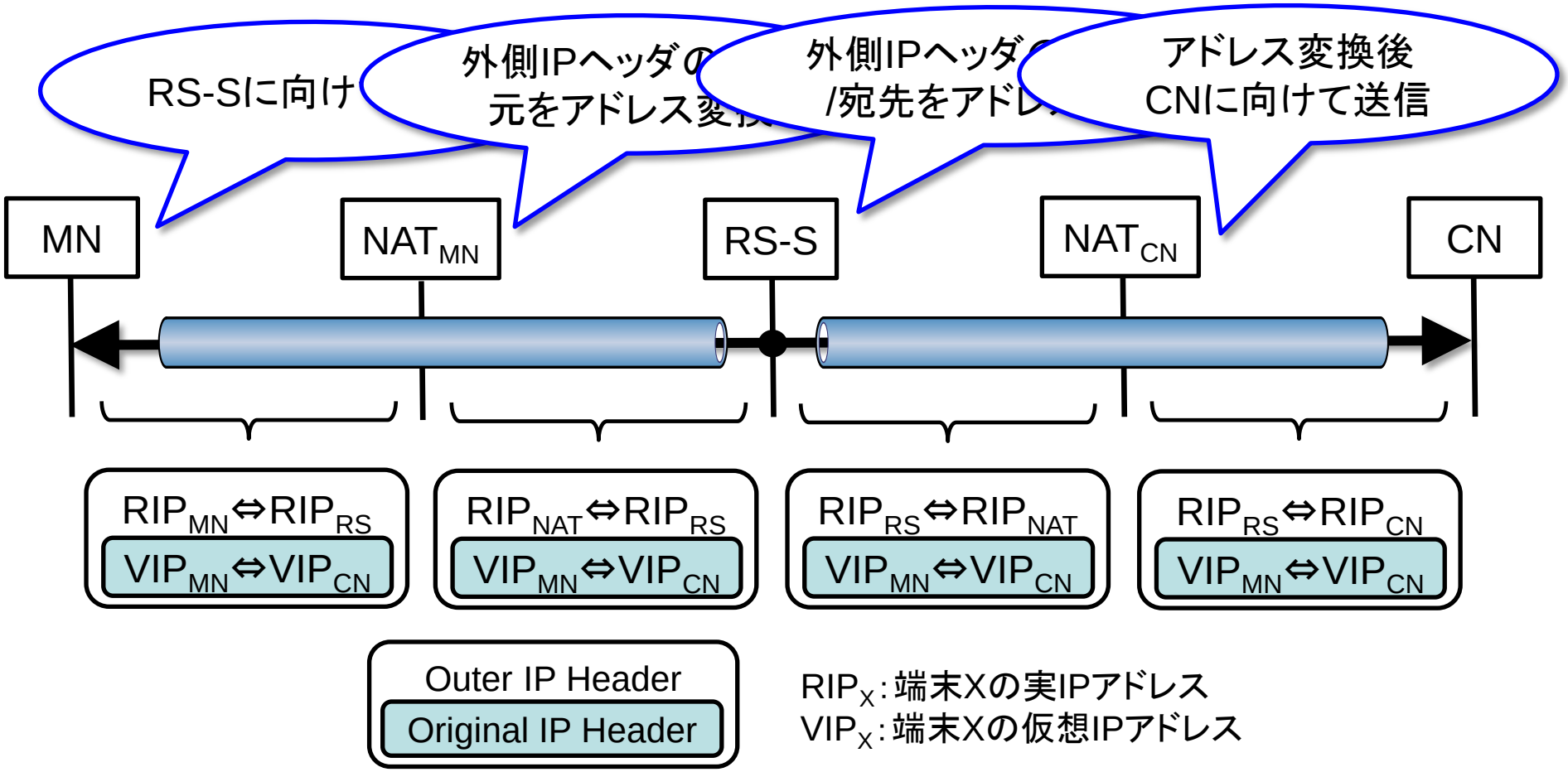


トンネル構築シーケンス(IPv4/IPv6間)



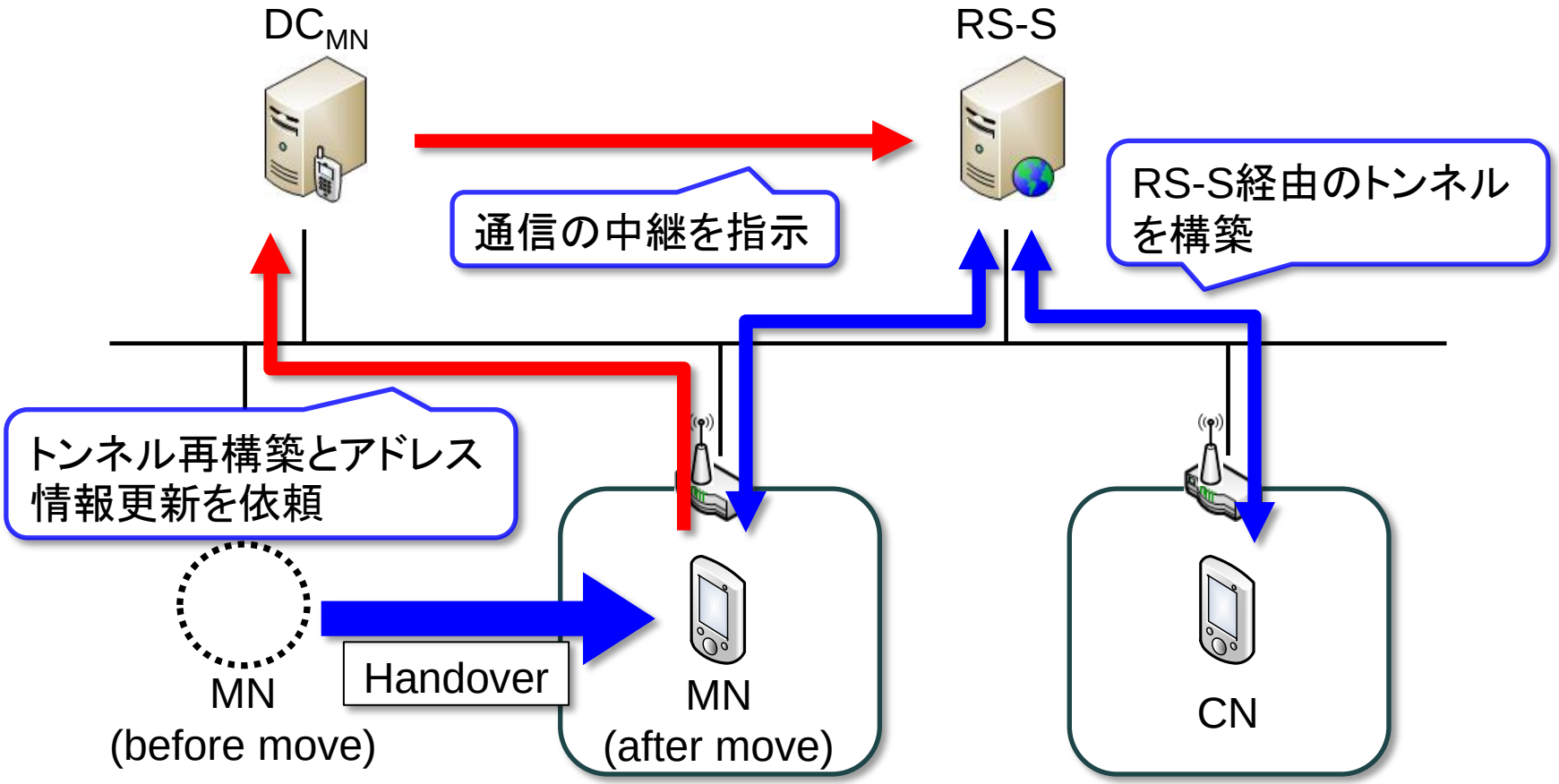
トンネル通信の様子(RS-S経由)

- MN～RS-S間，RS-S～CN間のパケットの様子
- RS-SはIPv4同士の通信の場合アドレス変換のみ



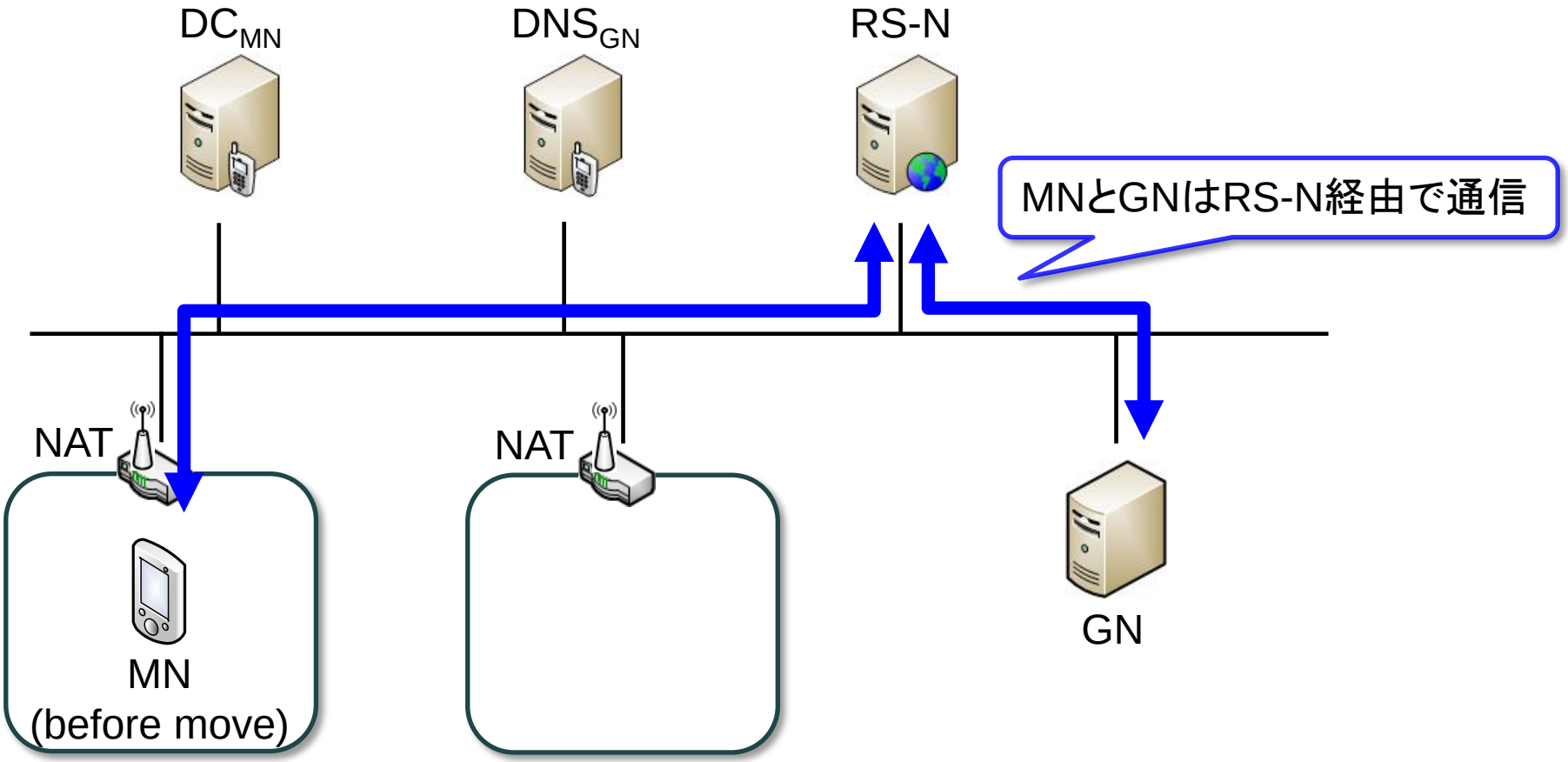
ハンドオーバ時の動作(RS-S経由)

- エンドエンド通信中にMNがNAT配下にハンドオーバ
  - DC_{MN}に対してアドレス情報更新とトンネル再構築を依頼
- MN～RS-S，RS-S～CN間でトンネル構築



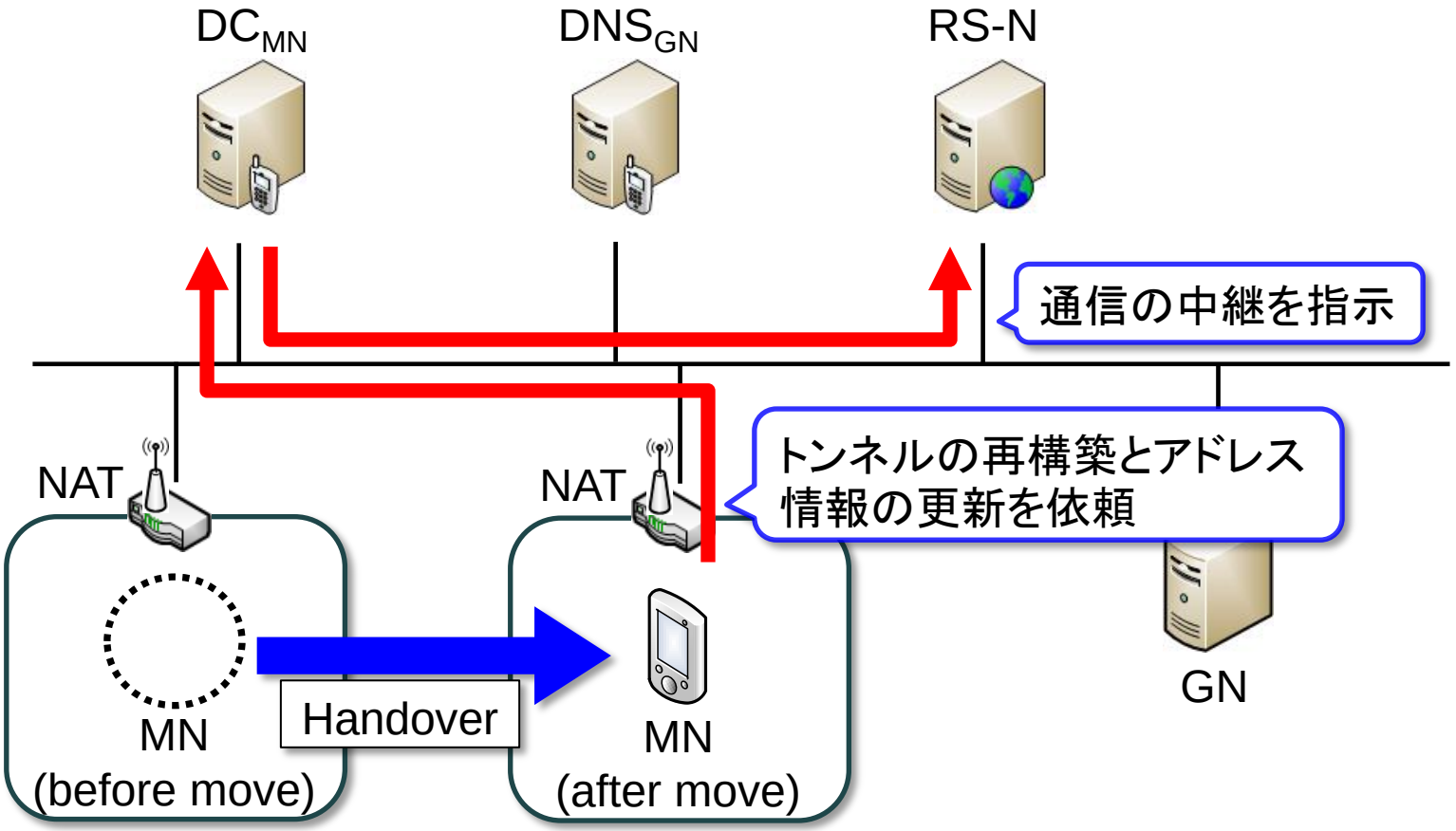
ハンドオーバ時の動作(RS-N経由)

- MNが異なるNAT配下にハンドオーバ
  - DC_{MN}に対してアドレス情報更新とトンネル再構築を依頼
- MN～RS-N間でトンネル再構築



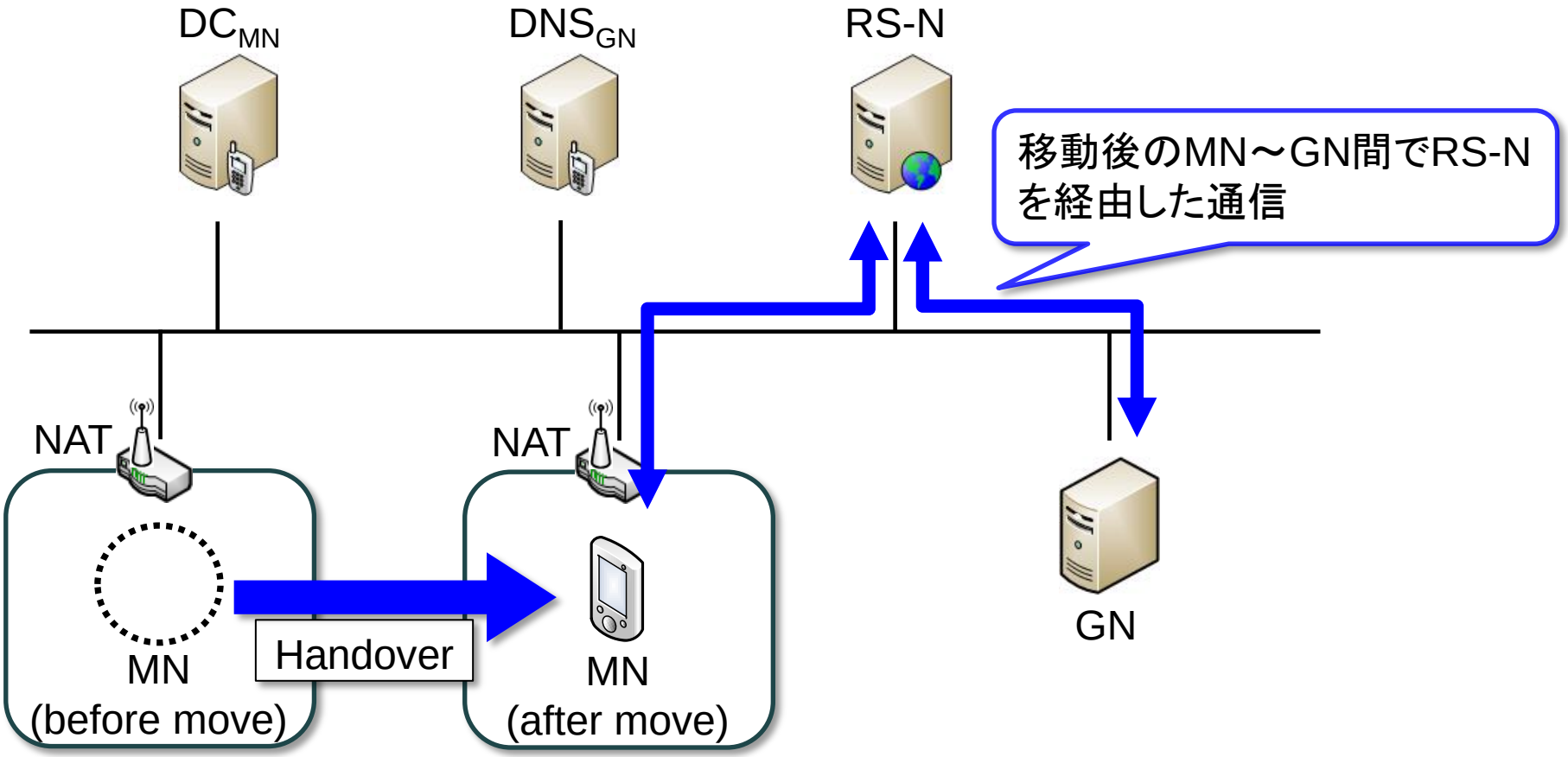
ハンドオーバ時の動作(RS-N経由)

- MNが異なるNAT配下にハンドオーバ
  - DC_{MN}に対してアドレス情報更新とトンネル再構築を依頼
- MN～RS-N間でトンネル再構築

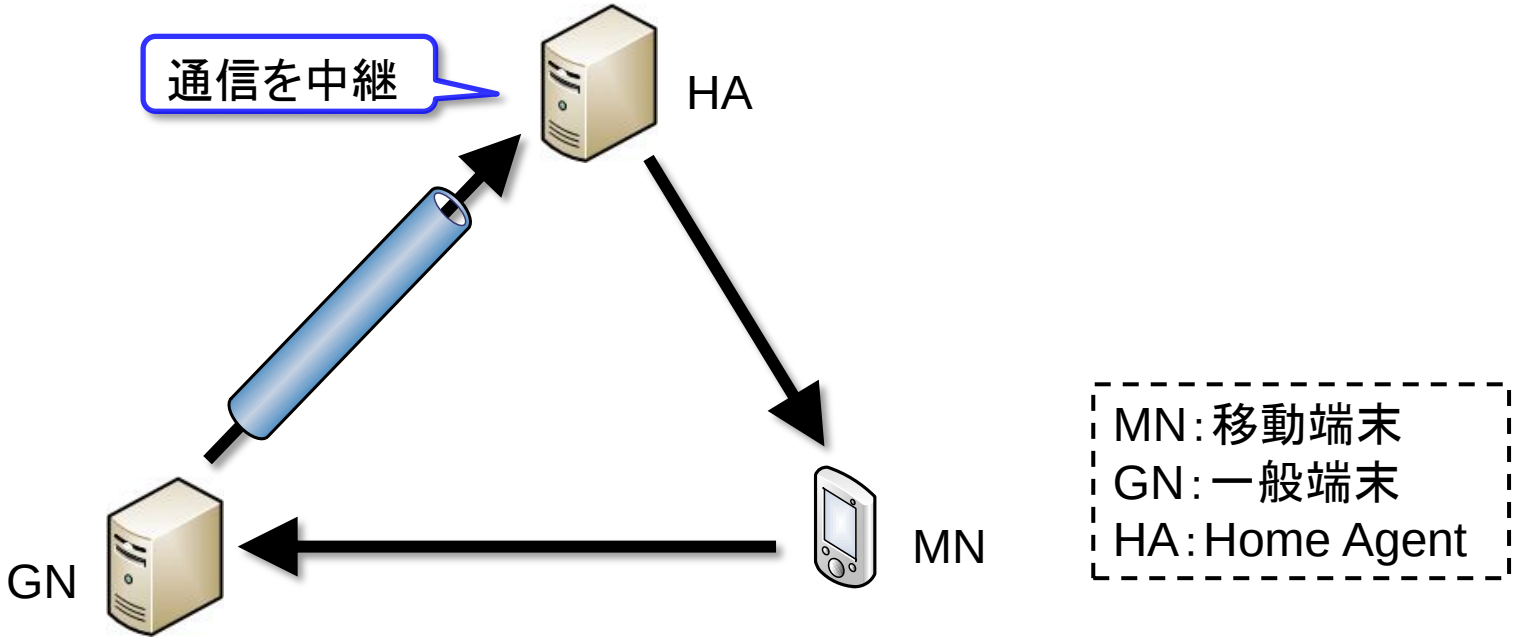


ハンドオーバ時の動作(RS-N経由)

- MNが異なるNAT配下にハンドオーバ
  - DC_{MN}に対してアドレス情報更新とトンネル再構築を依頼
- MN～RS-N間でトンネル再構築



- Mobile IPv4
  - IPv4環境において移動透過性を実現
  - HAを経由することでGNに対してMNの移動を隠蔽
  - 課題
    - HAの設置場所がホームネットワークに限定されるため経路が冗長
    - HAの一点障害問題，負荷分散ができない



関連研究

- LIN6(Location Independent Networking for IPv6)
  - IPv6アドレスをノード識別子と位置指示子の2種類に分離
  - ノード識別子とIPアドレスの対応を位置管理装置で管理
  - 課題点
    - アドレス空間が半分になるためアドレス利用効率が低下
    - アドレス空間不足であるためIPv4に適用が困難

- MAT(Mobile Support Architecture for Technologies)
  - ノード識別子と位置指示子の2つのアドレスを定義
  - 両者の対応関係を管理装置で管理し，両者の間でアドレス変換
  - 課題点
    - NATを跨る移動を想定していないため適用範囲が狭い