NTT

「IPv6モビリティ技術の動向」

JPNIC Next Generation Task Force 研究会

2003年11月29日

NTT情報流通プラットフォーム研究所

加藤淳也 **<kato@syce.net>**

自己紹介

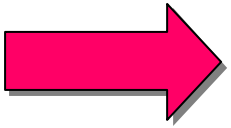
- 所属（2003年11月29日現在）

  NTT情報流通プラットフォーム研究所
  ユビキタスコンピューティング基盤プロジェクト
  ユビキタス方式グループ

- IPv6にかかわる経歴
  - 1997年 はじめてIPv6にふれる。
    - 基礎検証を経て早稲田大学構内へ導入、IPv6接続実験を開始
  - 2000年 7月～ Windows向けIPv6アプリケーション開発を開始
  - 2002年 ユビキタスコンピューティングのため
    Mobile IPv6とネットワークモビリティの研究開発に従事

「ユビキタス」の解釈？

いつでもどこでも（　思い立ったときに）サービスが受けられる



どんなときでもネットワークへ常時接続

研究会の概要

1. IPv6の発展とモビリティ技術へのインパクト
2. Mobile IPv6 プロトコル概要
3. Mobile IPv6 標準化動向
4. Mobile IPv6 の効果と課題
5. Mobile IPv6 以外のモバイル技術
6. ネットワークモビリティへの展望

IPv6の登場とP2P通信へのインパクト

膨大なアドレス空間

→ すべてのデバイスに一意のアドレス

→ デバイス同士が直接通信 (P2P通信)

VoIP, テレビ会議, インスタントメッセージ

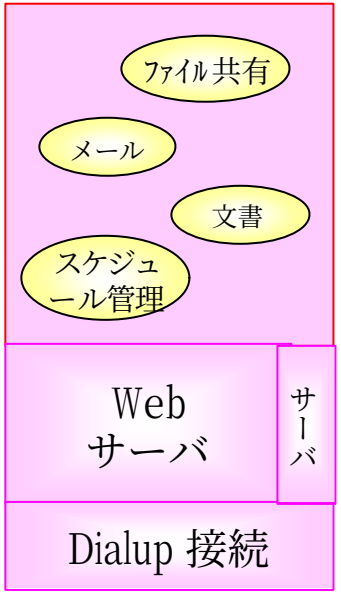
サーバを呼び出す

↓

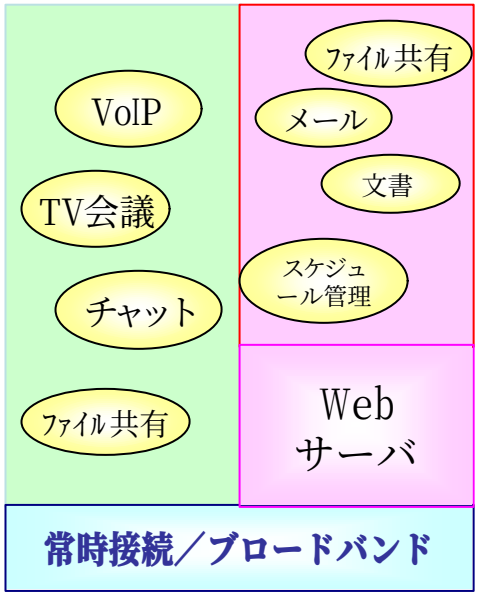
相手を直接呼び出す
相手から直接呼び出される

ヘパラダイムシフト

蓄積配送アプリ
(放り投げ型)



リアルタイムインタラクティブアプリ (割り込み型)



モビリティ技術への注目

ユーザニーズ

- 思い立ったときに使いたい
  - 場所と通信手段を選ばない
- ネットワークの接続を自動化したい
  - 最適なネットワークに自動接続
- アプリケーションを使い続けたい
  - 設定（サーバ）の切り替えたくない

背景

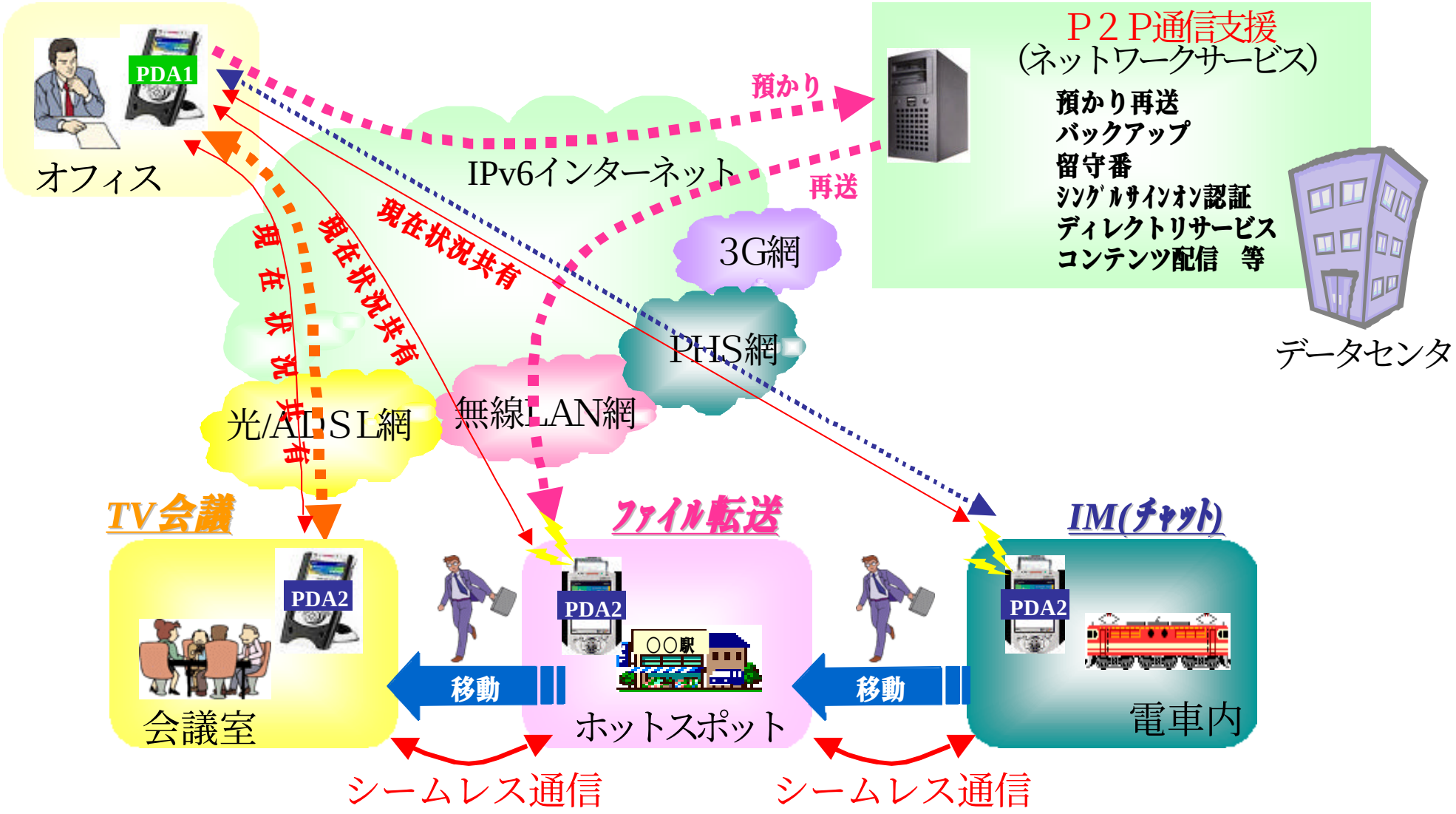
- 端末の小型化・通信I/Fの内蔵（特に無線LAN）
  ノートPCやPDAの小型化／軽量化
- アクセスインフラの整備
  公衆無線LAN
  ブロードバンド, 携帯電話／PHS

例えばNTT Com HotSpot は
全国600ヶ所以上に展開中

ユビキタス時代のモビリティ

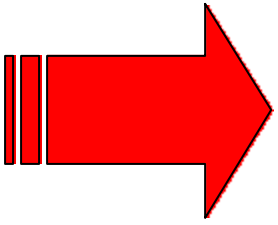
ユビキタスサービスのプロトタイプ

NTT Information Sharing Platform Laboratories



いつでもつながるための技術は？

- いついかなるときでもつながっている必要性
  - インスタントメッセージ
  - 携帯VoIP
  - 携帯ゲーム機？
- レイヤ3（IPv6層）でのモビリティ確保
  - IPv6インターネットの接続性さえあればよい
  - アクセスメディアやISPに依存したくない



Mobile IPv6は有力な手段

IPv6上でモビリティを実現するプロトコル
Mobile IPv6

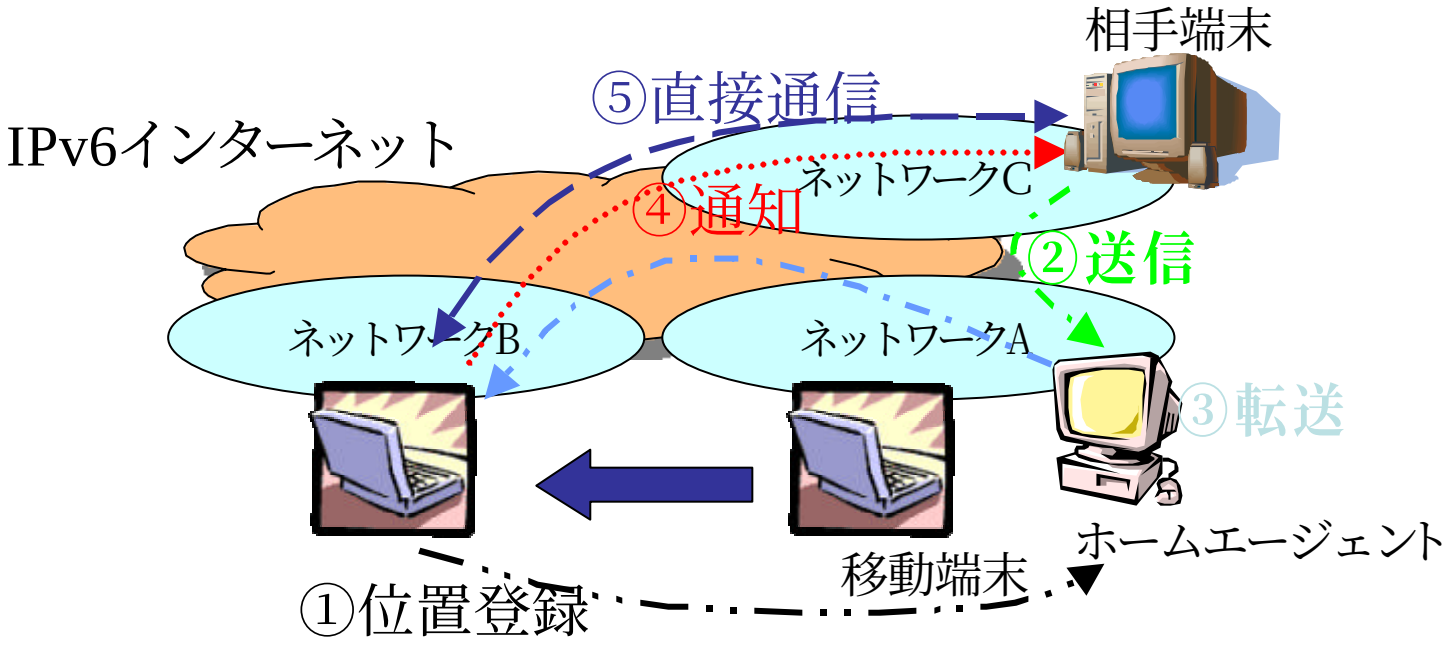
- 位置透過性
  1. 接続リンクが変更になっても同一アドレスでノードを参照できる
  2. 接続リンクが変更になっても進行中の通信（セッション）を維持できる

- IPv6レイヤのみで実現
  - アプリケーションおよびL2のサポートが不要
    （アプリケーションの改造もL2の改造も不要）

⇒ IPv6コネクティビティさえあれば位置透過な通信が可能

- Mobile IPv4からの改善点
  - 経路最適化が標準で定義
  - Foreign Agentの廃止
  - ソースアドレス詐称が無い
    ⇒ ファイヤウォールのingress filterに整合

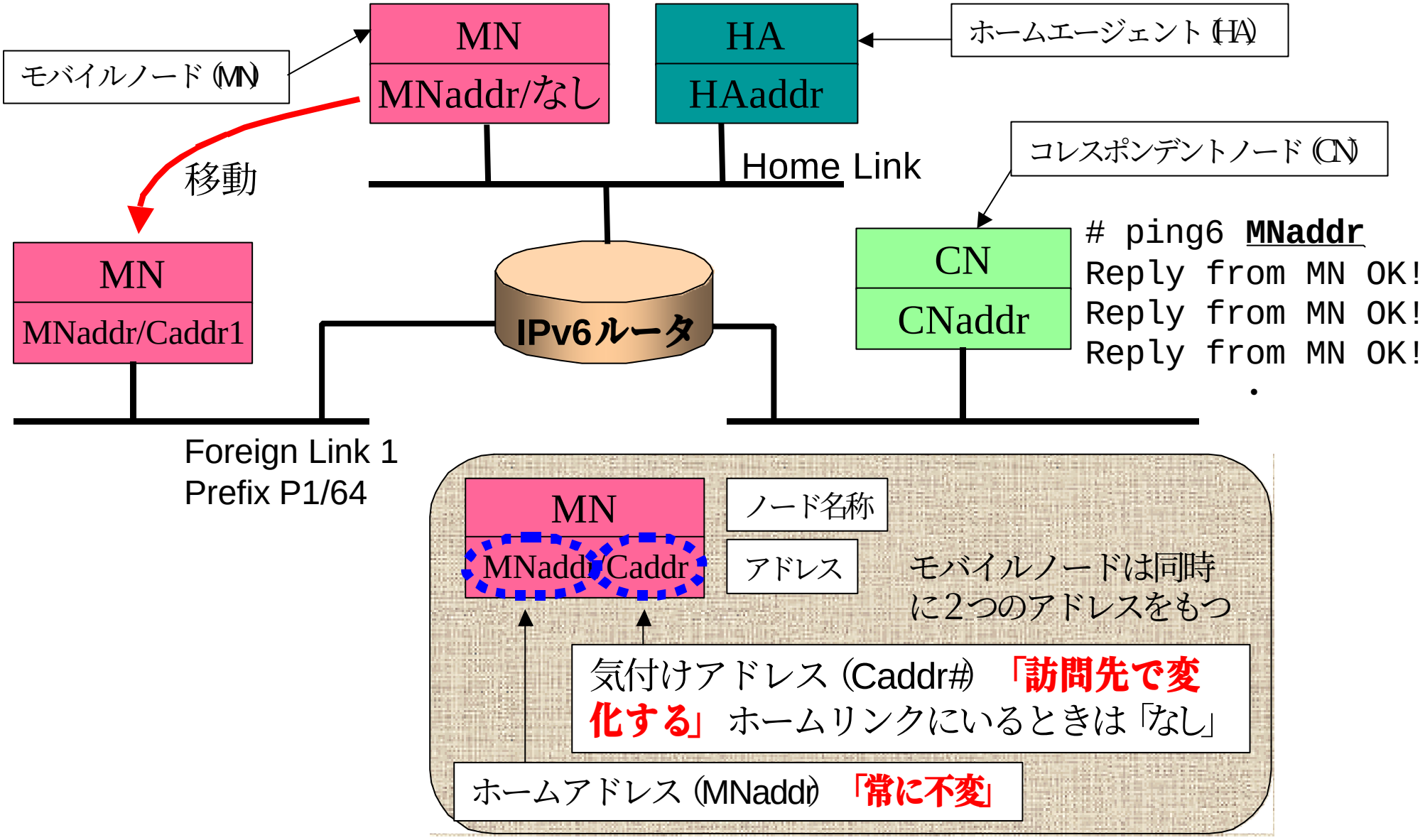
Mobile IPv6 の動作概略



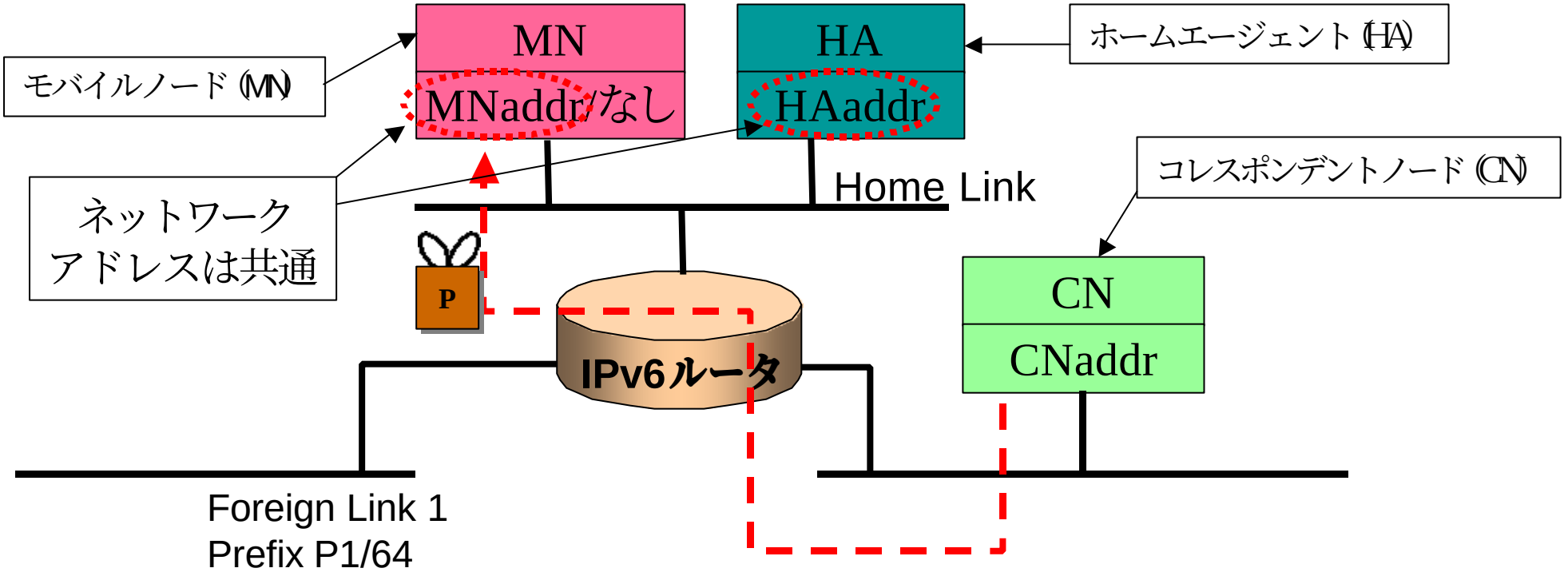
- 移動端末はホームエージェントに位置登録
- 相手端末は、通信開始時のみホームエージェントのサポートを受け、移動端末にパケットを送信
  - ホームエージェントがパケットを転送する
- 移動端末は相手端末にも位置を通知する
  - 通信開始後は、移動端末と相手端末は直接通信

Mobile **IPv6**の特徴

Mobile IPv6を用いた移動通信

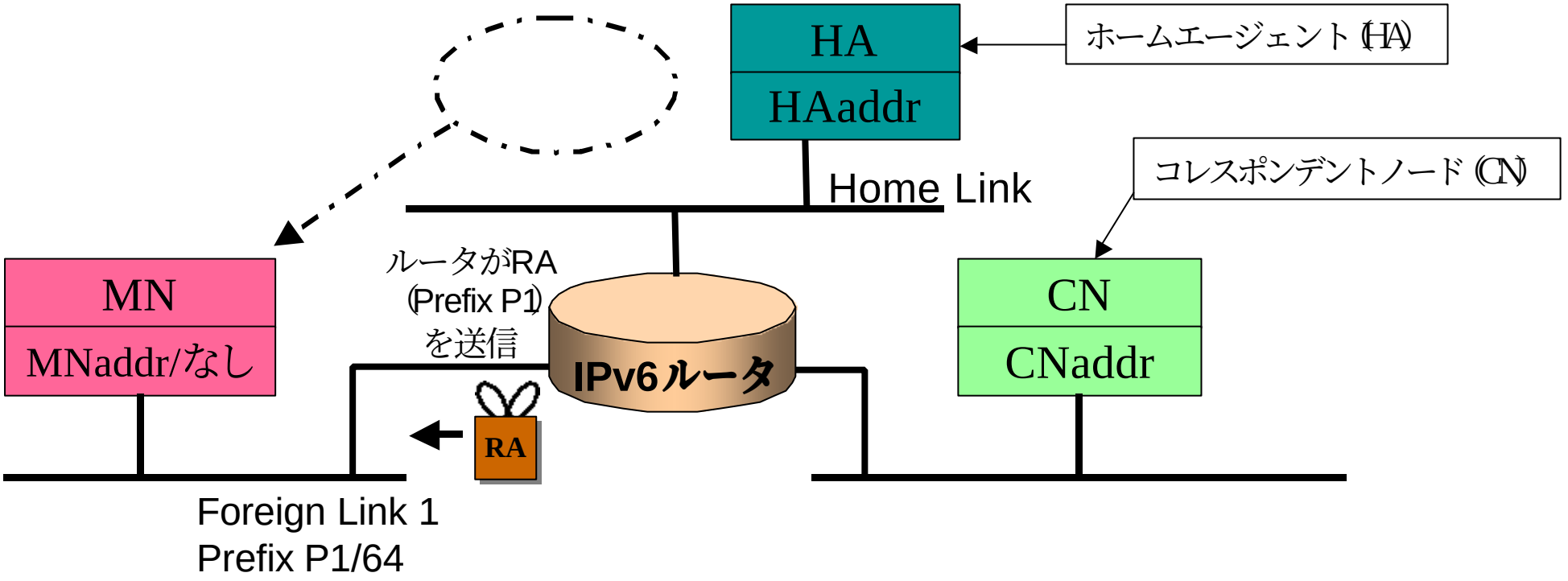


MNがHome Linkに存在



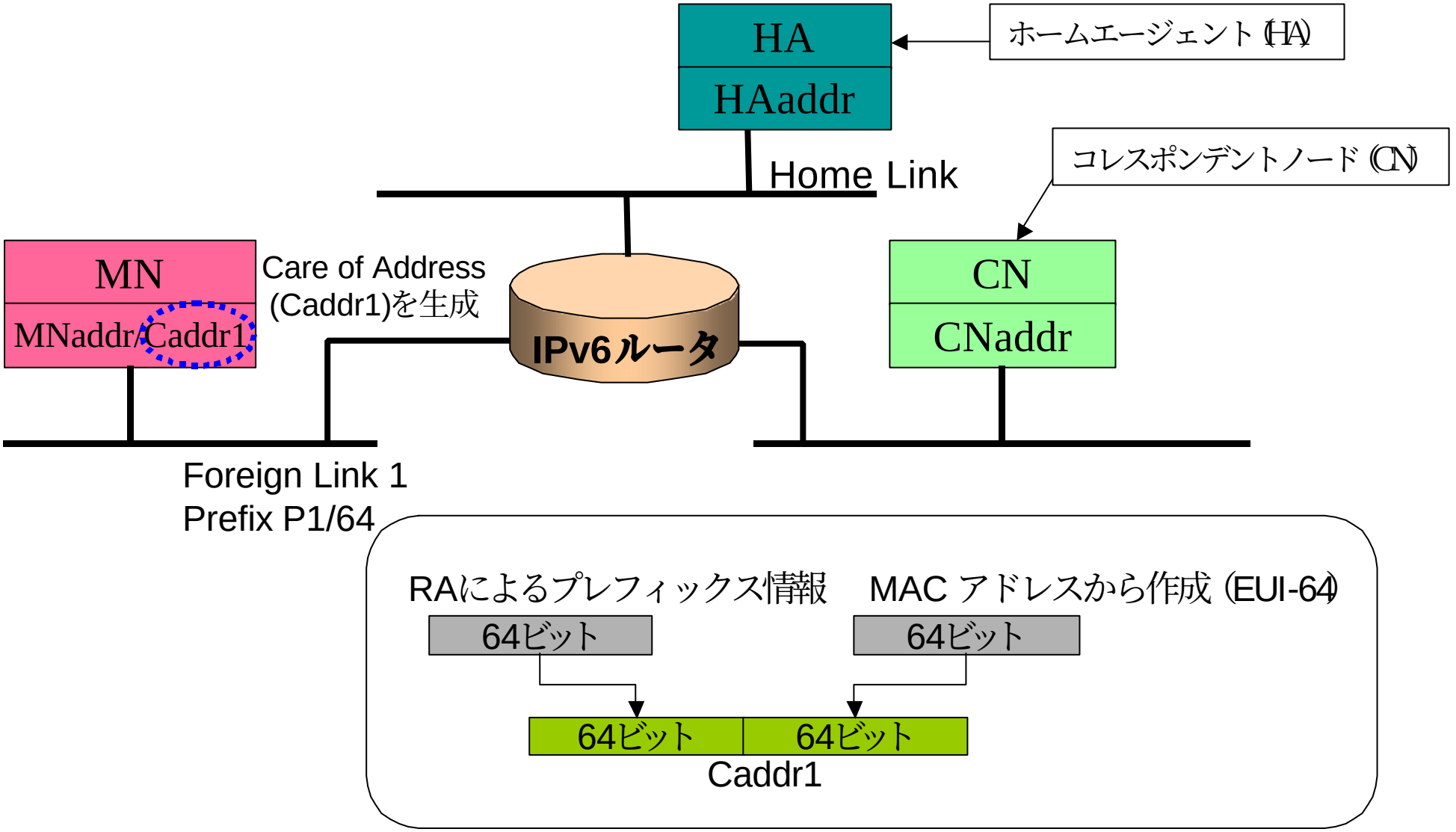
通常のIPv6通信が行われる

MNは自分が移動したことを検出する

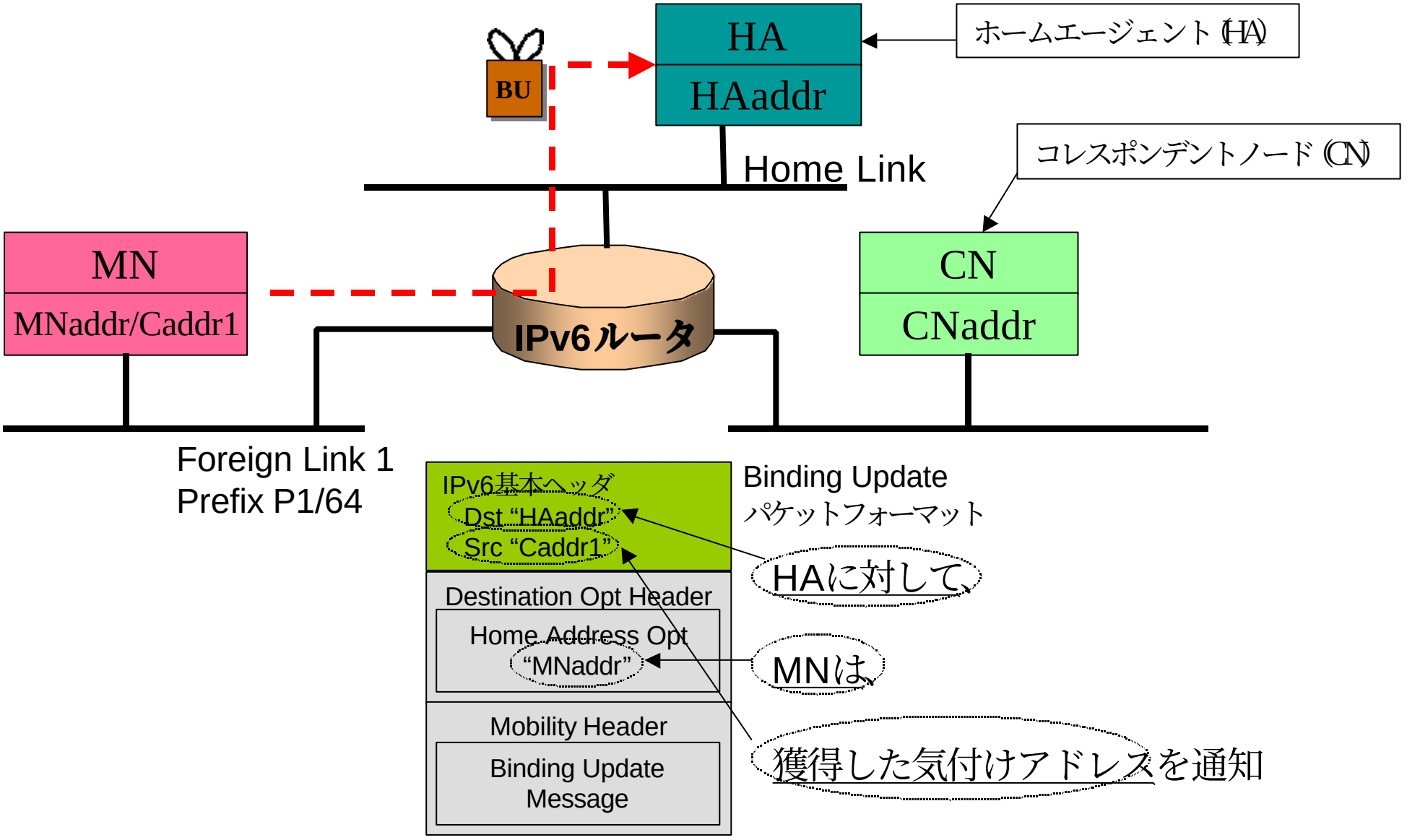


プリフィックスがホームアドレスのものと一致しない
直前に受け取ったプリフィックスと一致しない ⇒ MNは移動したと判断

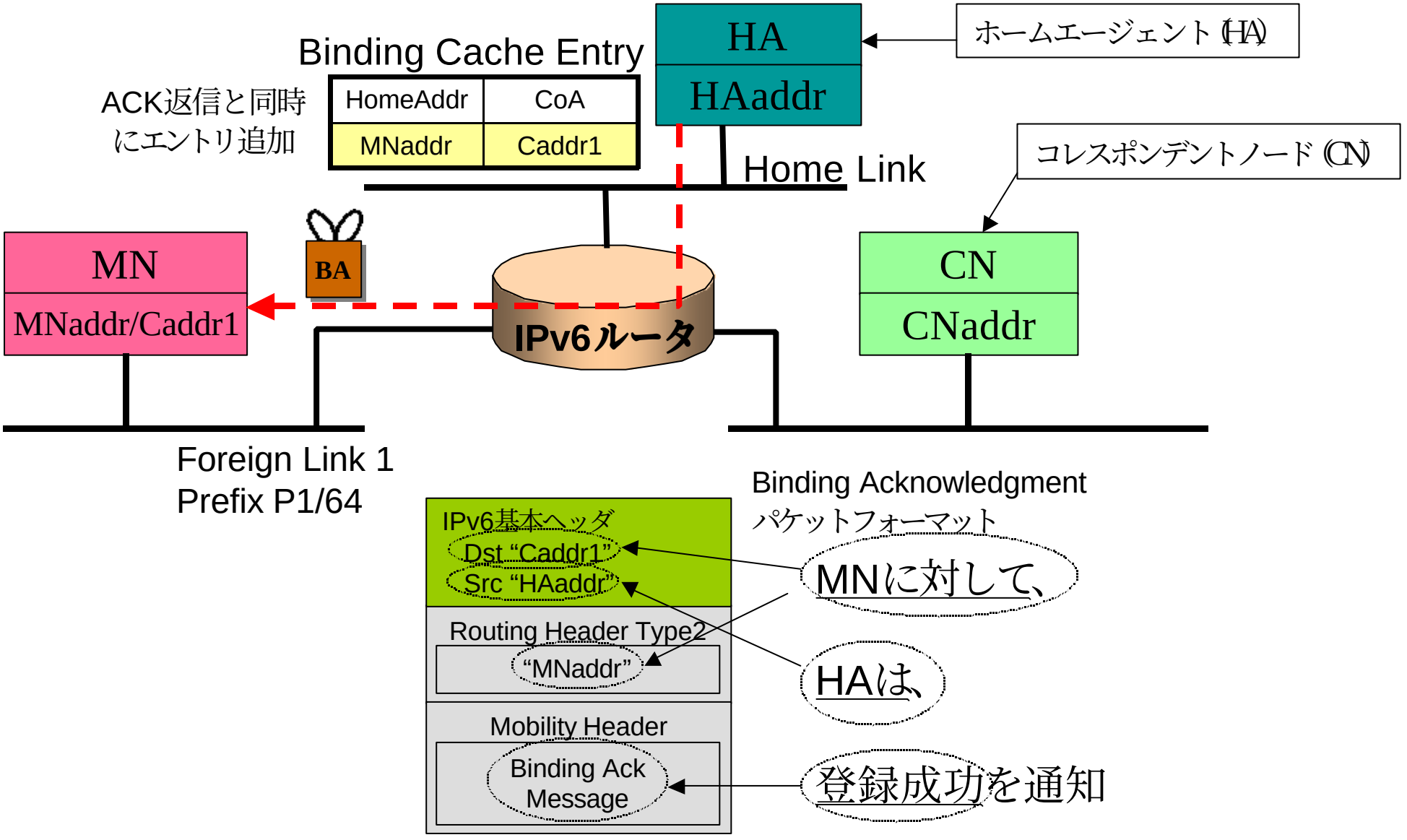
MNは気付けアドレスを生成する



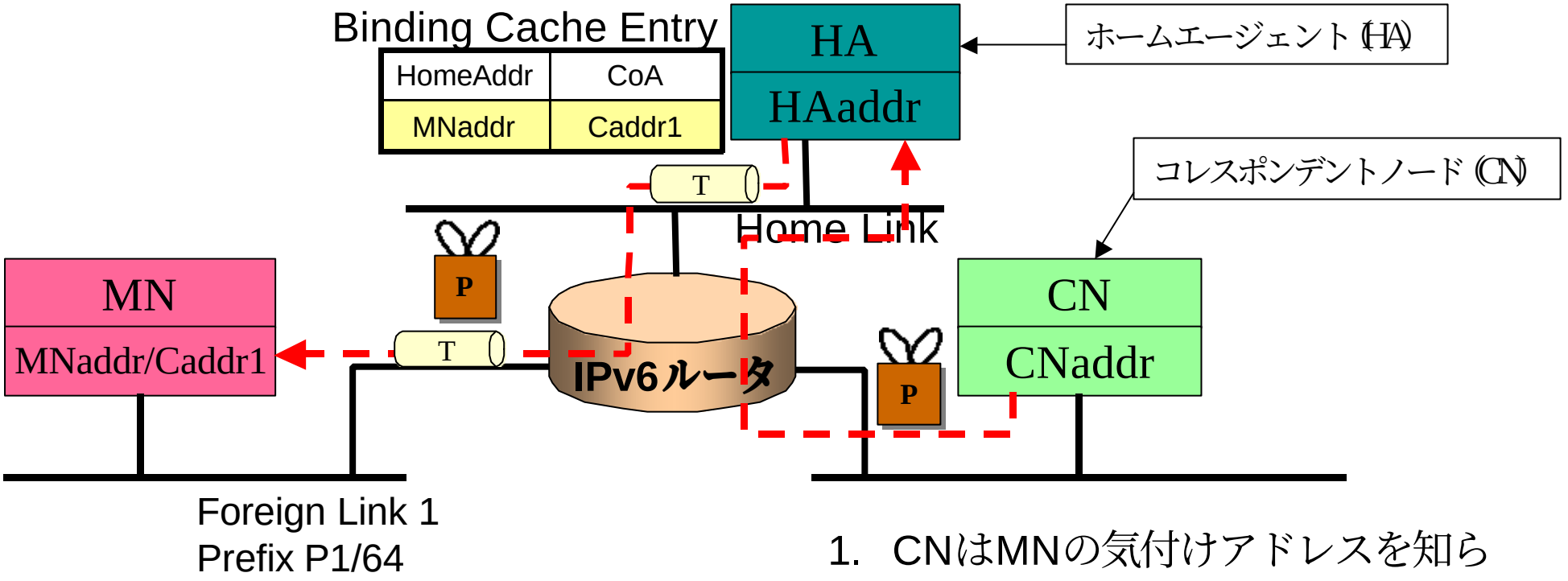
MNがCare-of アドレスをHAに通知(Notification)する HAへのBinding Update



HAがCare-of アドレスを確認(Acknowledge)する Binding Acknowledgment



CNがMNに向かって通信を開始

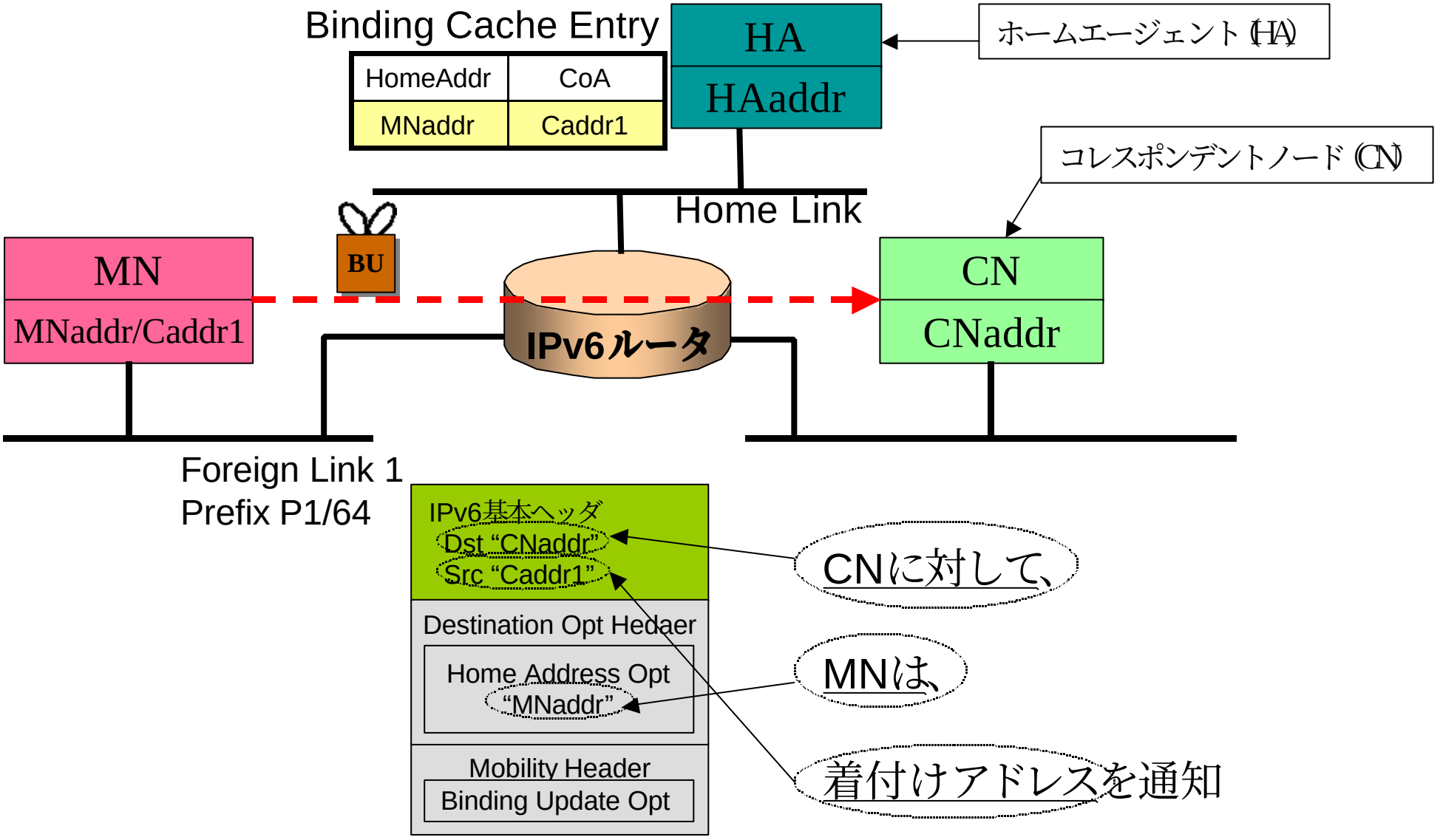


CN発のパケットをHA経由で受け取った場合CNがBinding Cacheを持たないと判断する

1. CNはMNの気付けアドレスを知らないので、HAにパケットを送る
2. HAはBinding Cacheの対応関係を調べ、転送先の気付けアドレス（Caddr1）を発見する。
3. トンネル（カプセル化）によりCNからのパケットを転送する

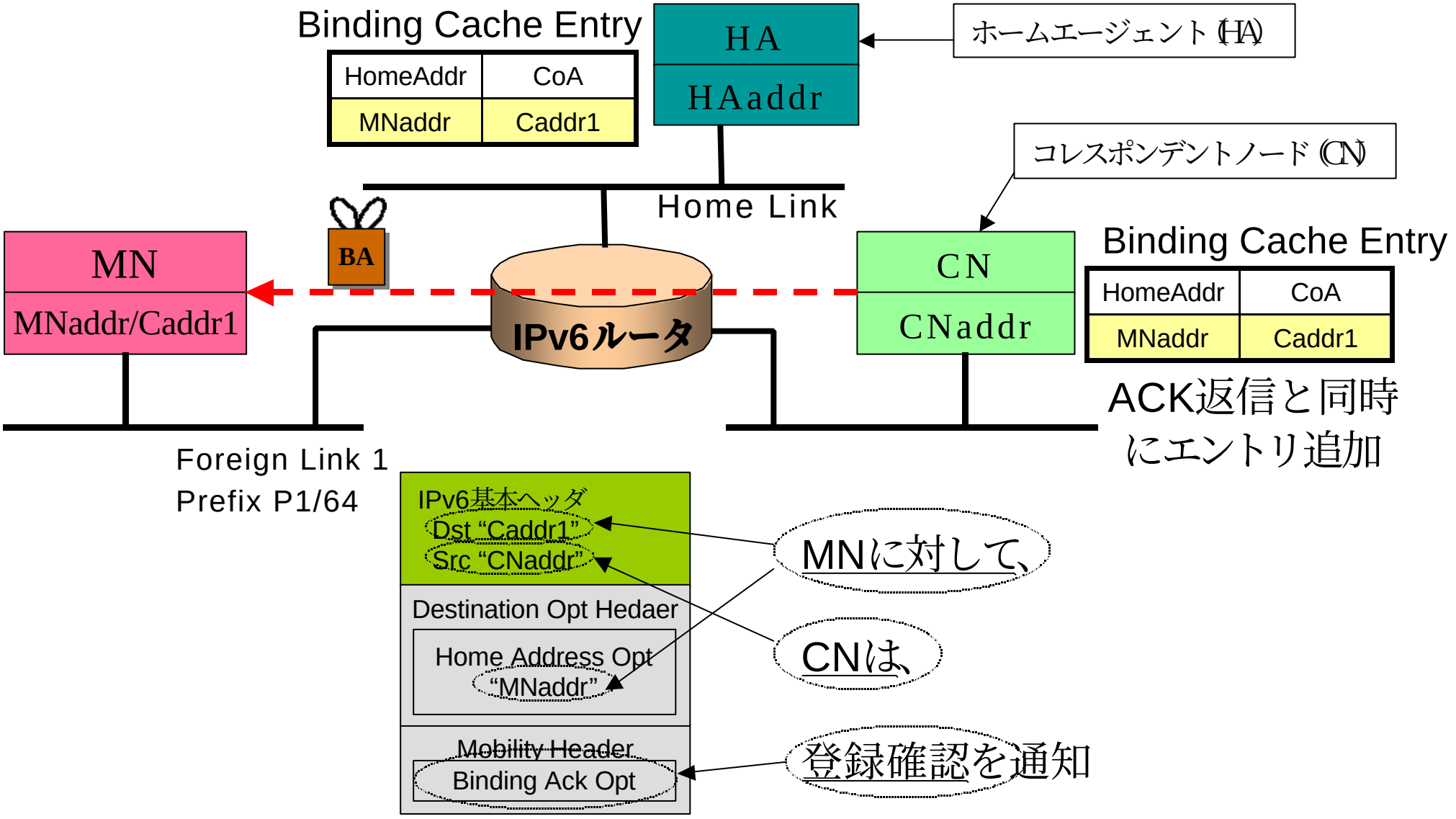
MNがCNに対してCare-of (気付) アドレスを通知する

※通知前にReturn Routability手続きが必要だが説明の簡略化のため別途解説

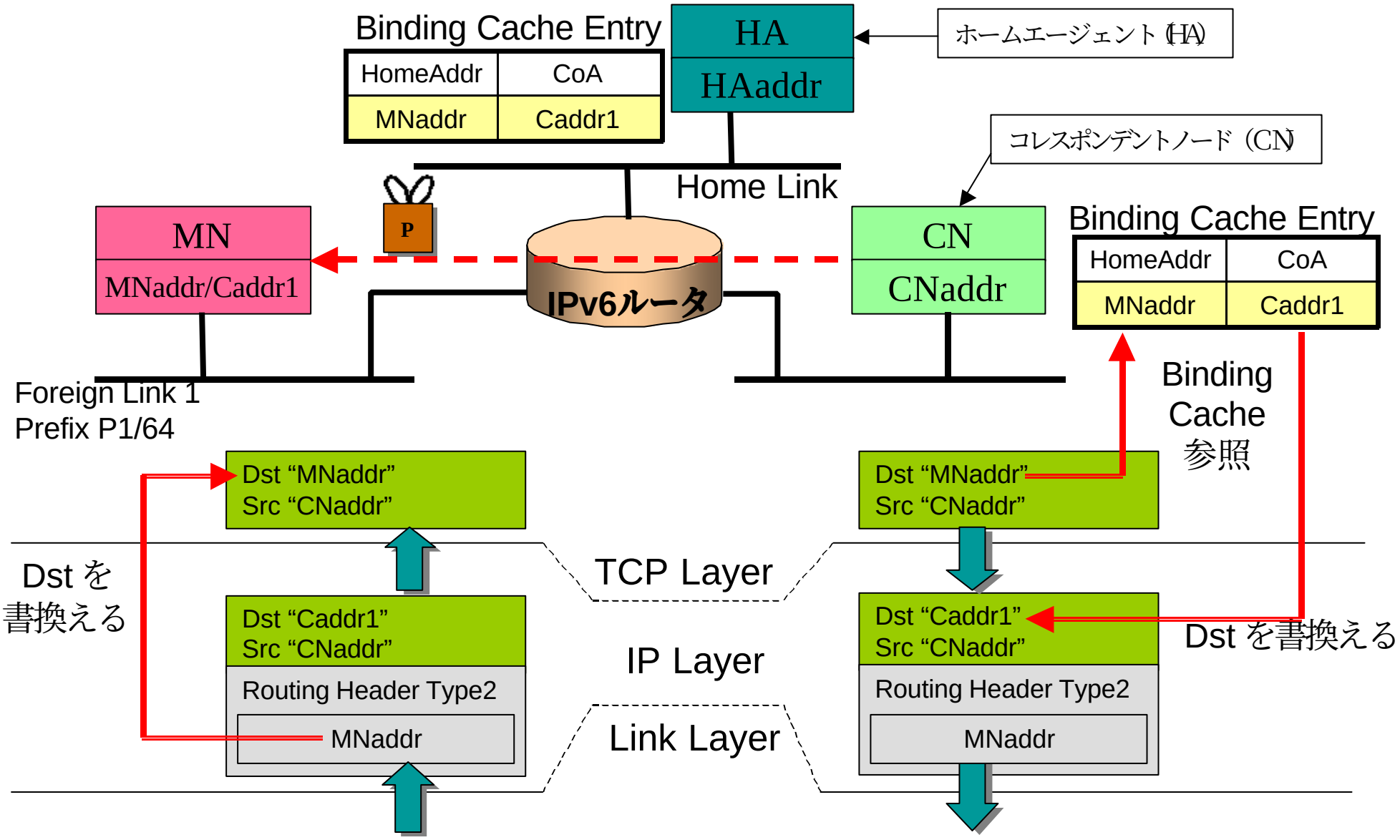


CNがCare-of アドレスを確認(Acknowledge)する

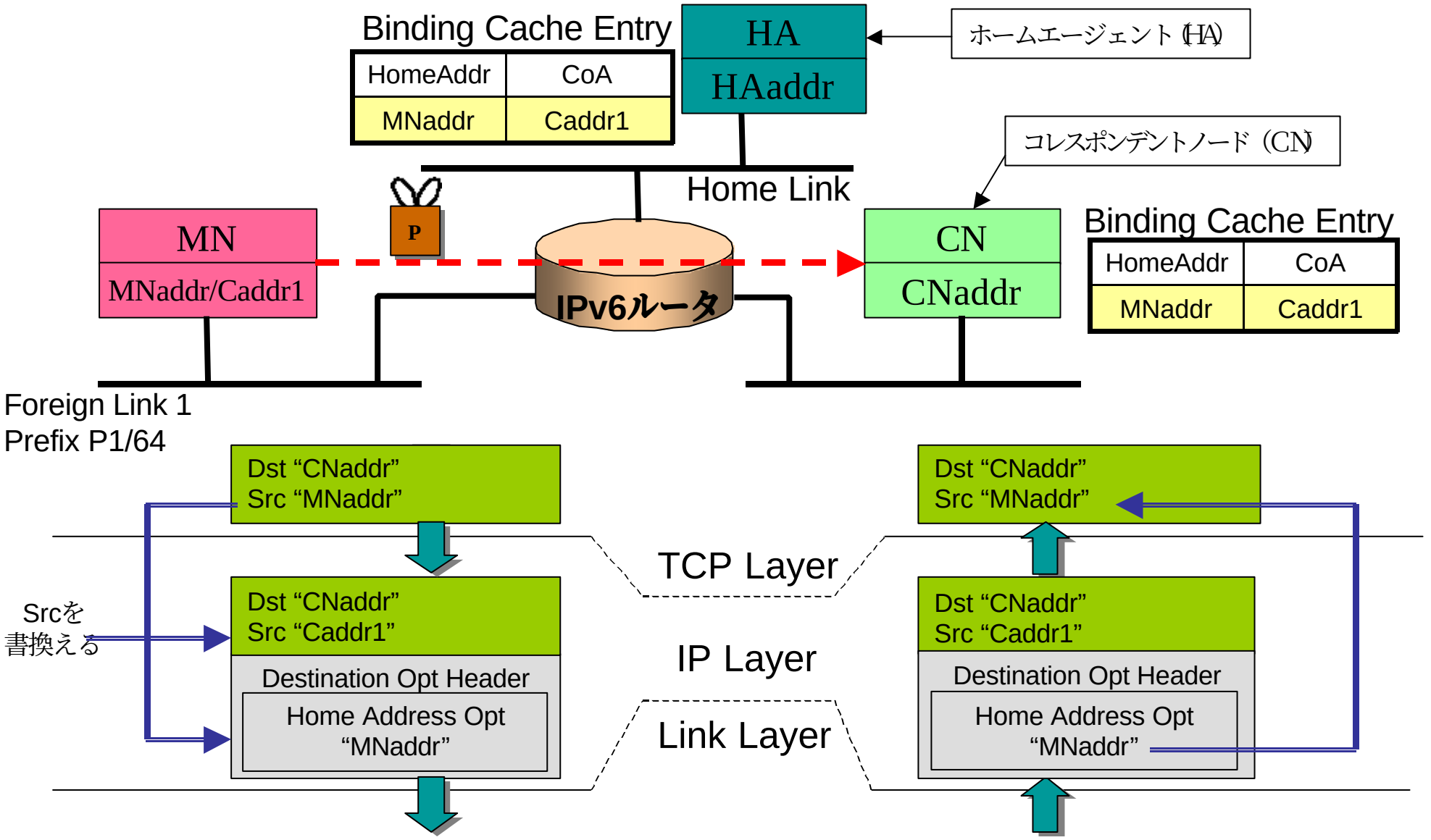
※Return Routability Procedureは別途解説



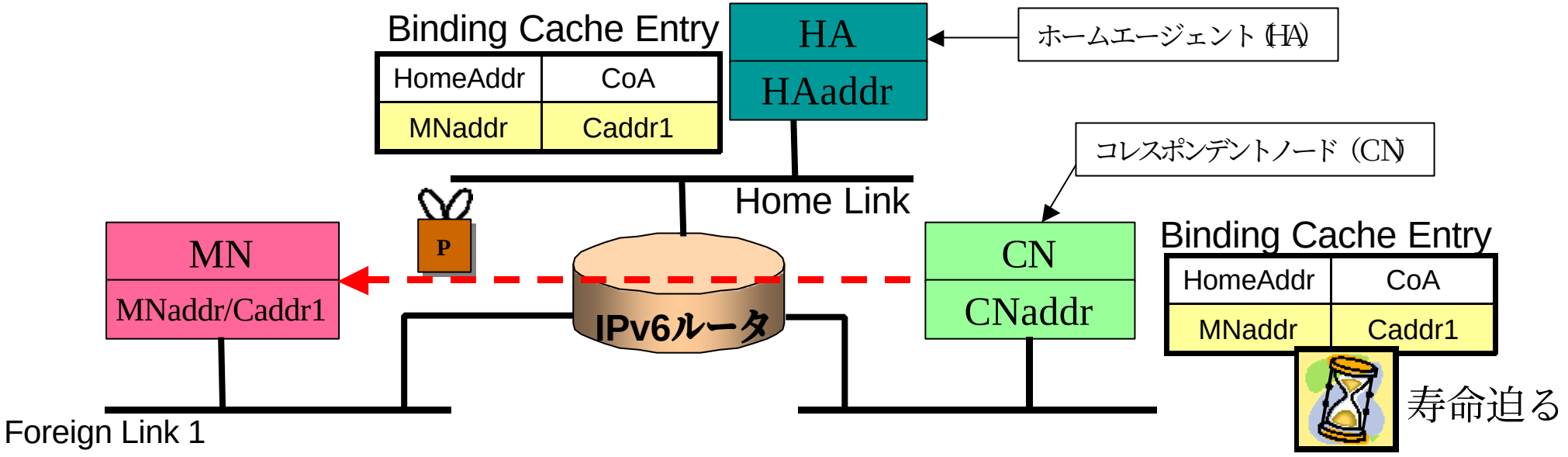
CNはBinding Cache を使いMNにパケットを送信

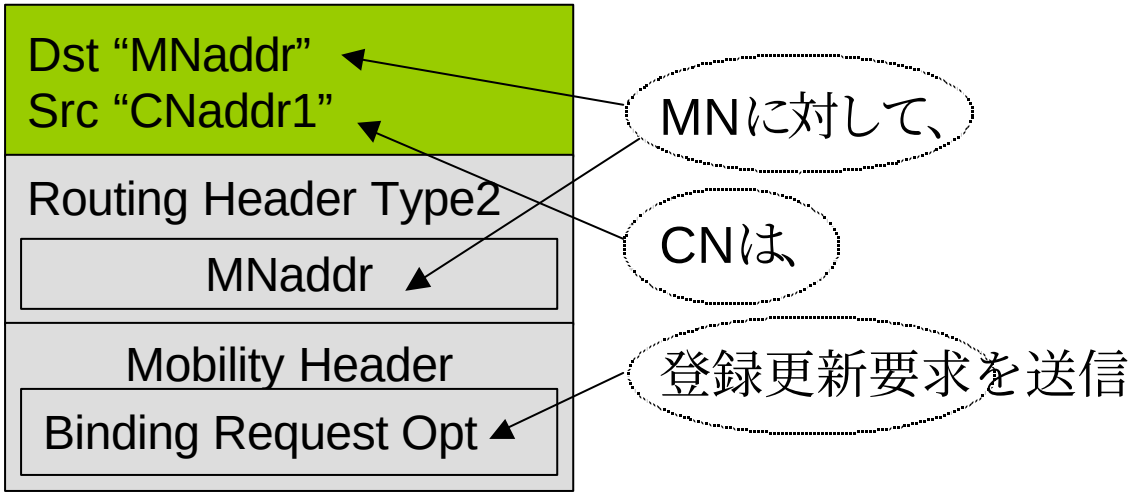


MNはHome Address Optを使いCNにパケットを送信



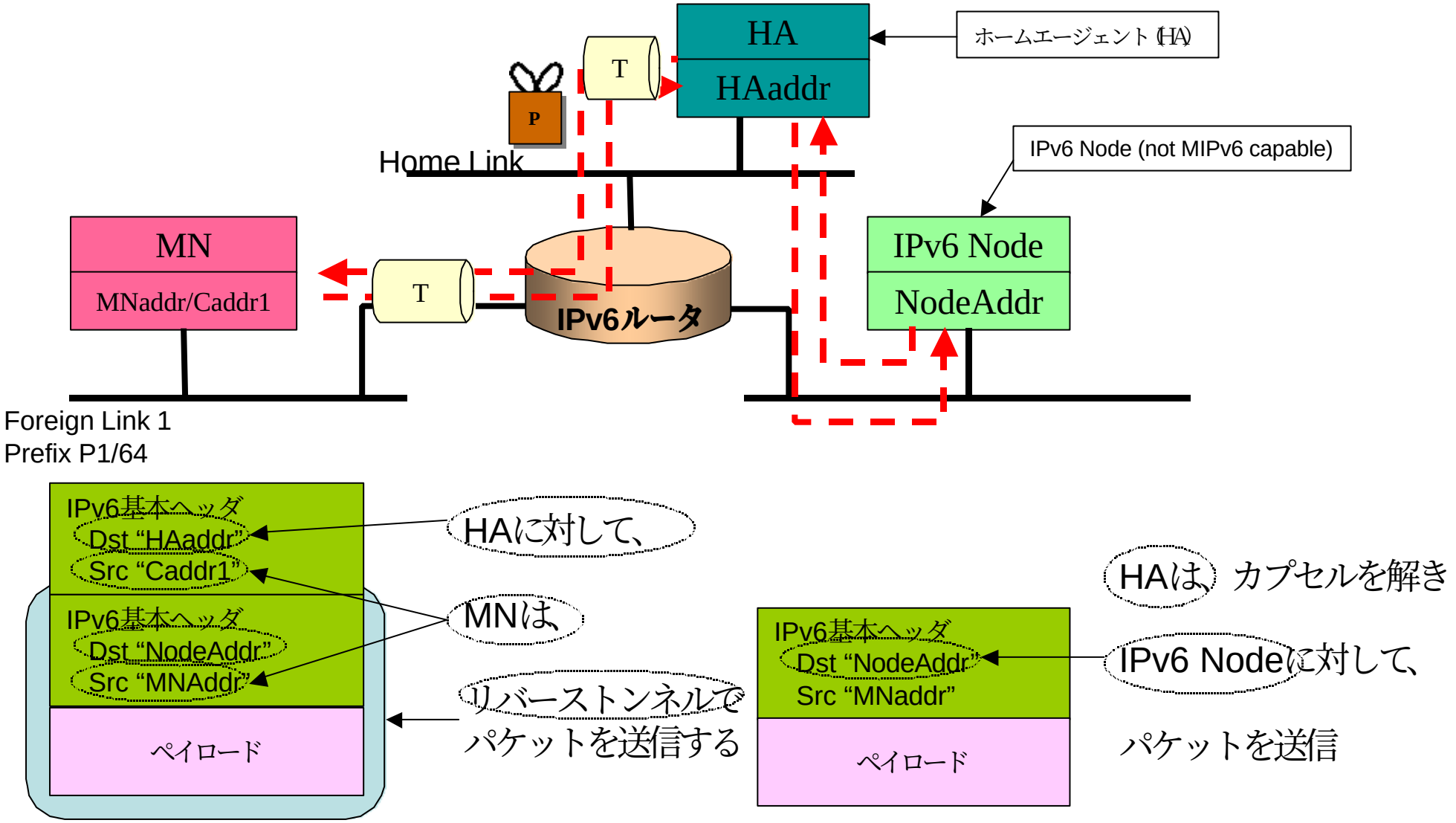
CNはBinding Cacheの寿命が切れそうになったらMNにBinding Request を送信





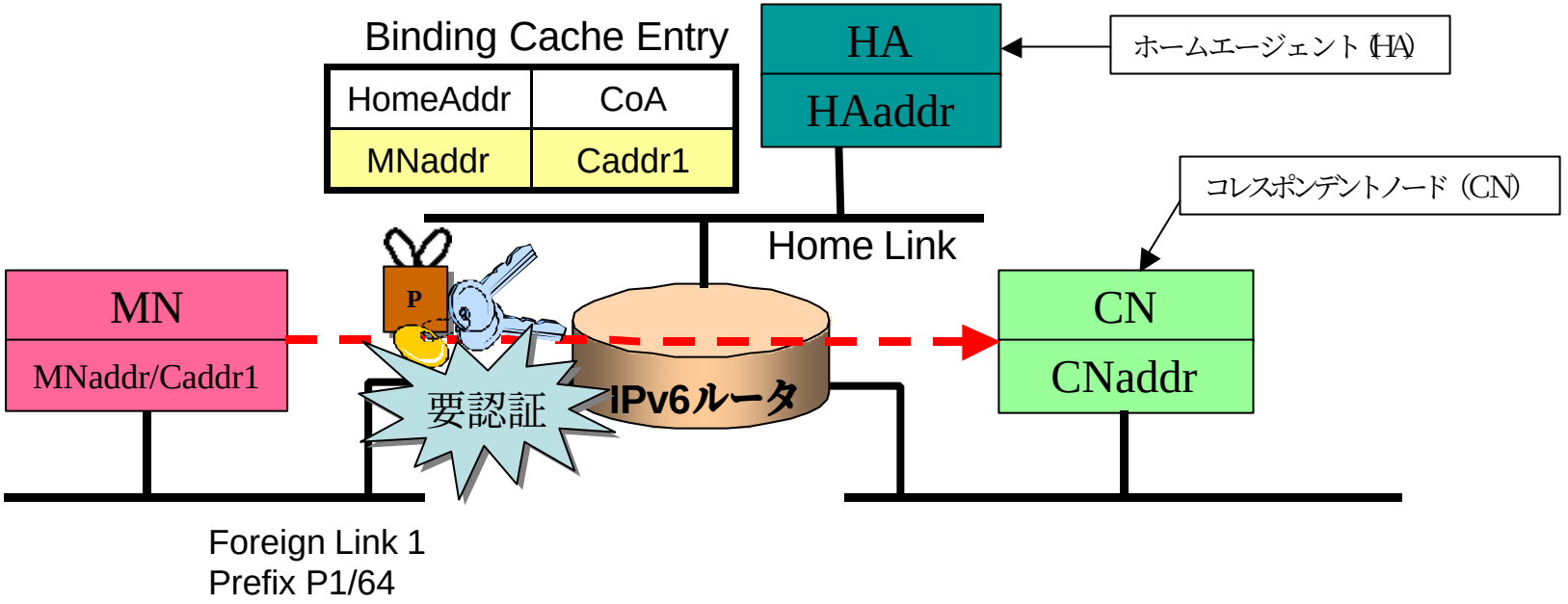
その後
2）MNがCNに対して気付（Care-of Address）を通知する
3）CNがCare-of アドレスを確認（Acknowledge）する

Mobile IPv6 を実装しないノード（Binding Cacheを持たないCN）との通信



MN⇔CN間の認証手続き
Return Routability

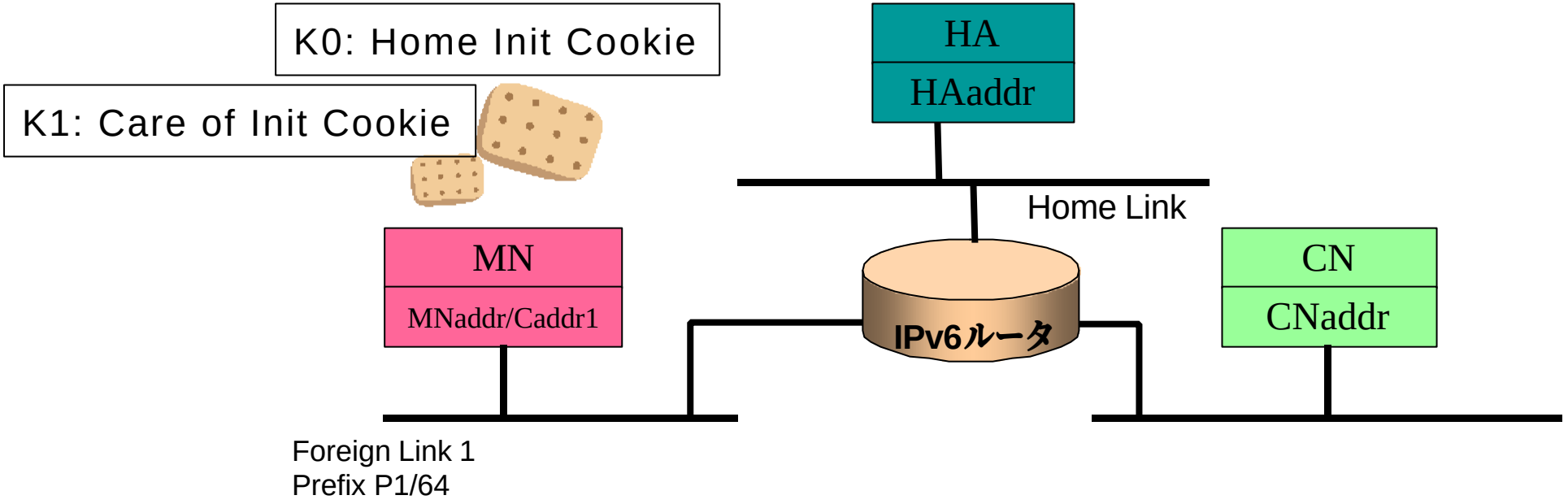
MN⇔CNの直接通信のために
MNがCNに対してCare-of (気付) アドレスを通知する



- 成りすまし防止のためCNはMNを認証する
- (現状では) 一般にCNはMNの認証鍵を持たない
- HA⇔MN間はIPsecにより安全という仮定を置き

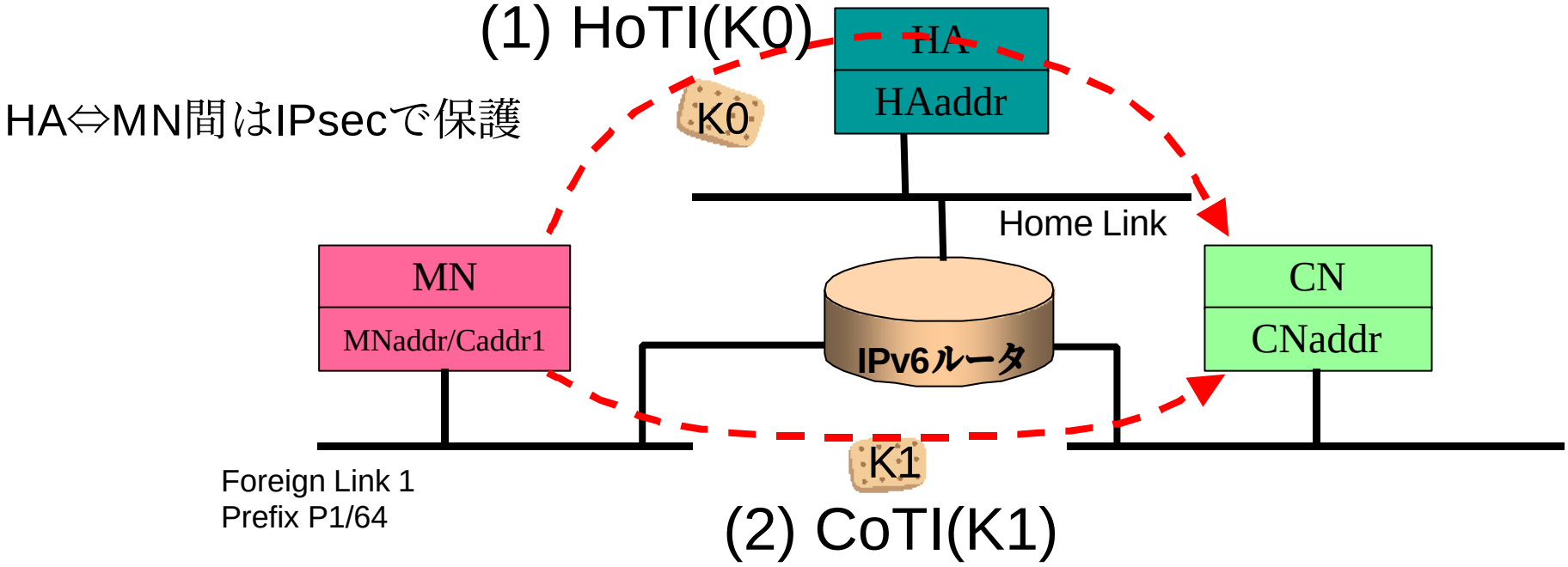
⇒ Return Routability (RR) 手続きを発行

Return Routability手続き STEP 1
MNはクッキー（K0, K1）を生成



- K0: Home Init Cookie
- K1: Care of Init Cookie
  いずれも64ビット長の乱数値

Return Routability手続き STEP 2
MNは2種類のTest Initメッセージを送信

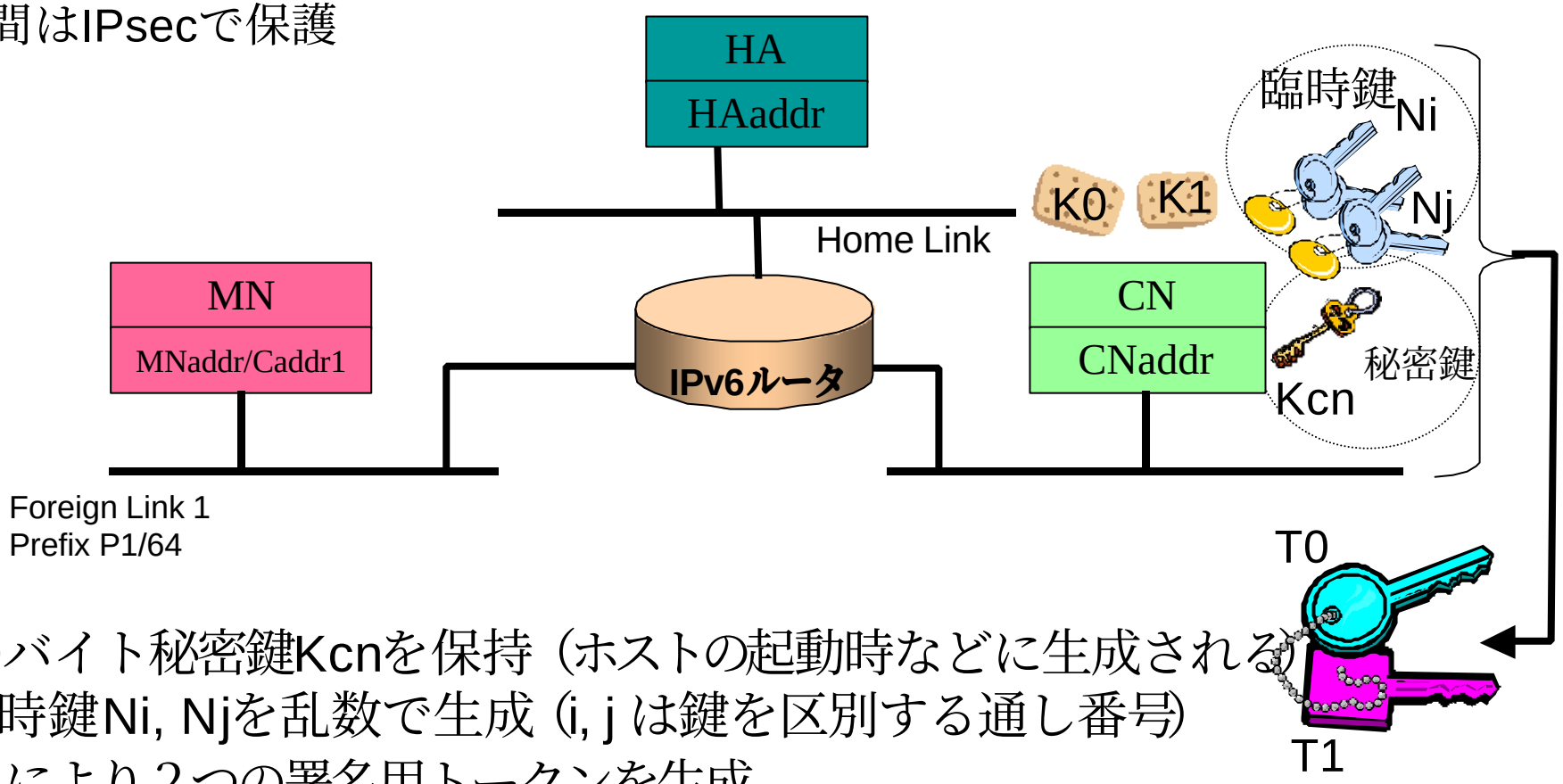


MNはCNへ2種類のメッセージを同時に送信

(1) Home Test Init (HoTI)　（ホームエージェント経由／cookie K0を含む）
(2) Care of Test Init (CoTI)　（CNへの直接配送／cookie K1を含む）

Return Routability手続き STEP 3
CNは署名用トークン（T0,T1）を生成

HA⇔MN間はIPsecで保護

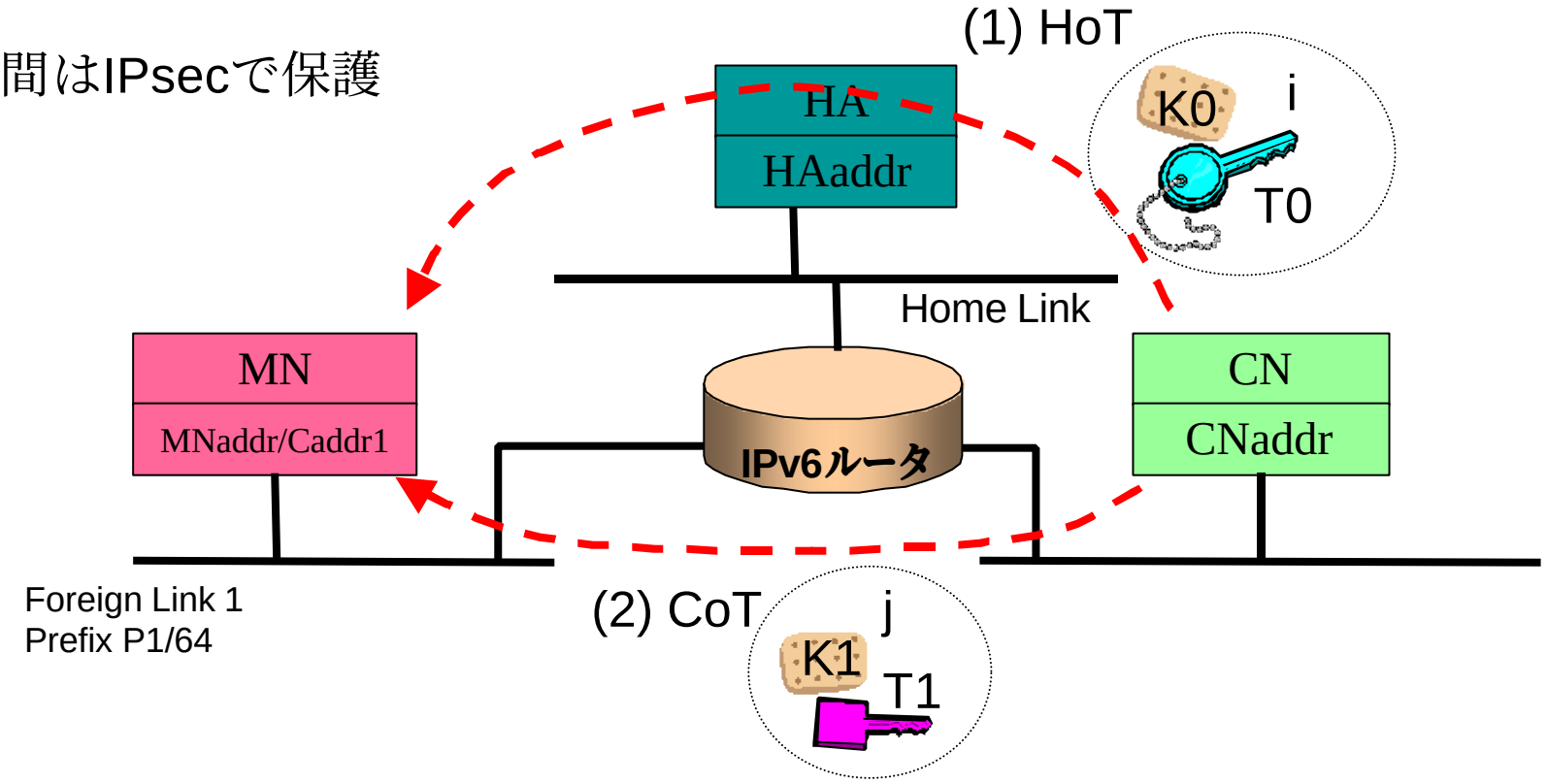


CNは20バイト秘密鍵Kcnを保持（ホストの起動時などに生成される）
CNは臨時鍵Ni, Njを乱数で生成 (i, j は鍵を区別する通し番号)
ハッシュにより２つの署名用トークンを生成

(1) home keygen:　T0 = HMAC_SHA1(Kcn, (MNaddr+Ni+0x00))
(2) care of keygen: T1 = HMAC_SHA1(Kcn, (Caddr1+Nj+0x01))

Return Routability手続き STEP 4
CNはMNへ署名用トークン（T0,T1）を返送

HA⇔MN間はIPsecで保護



CN はMNへ2種類のメッセージを同時に返送

(1) Home Test (HoT)

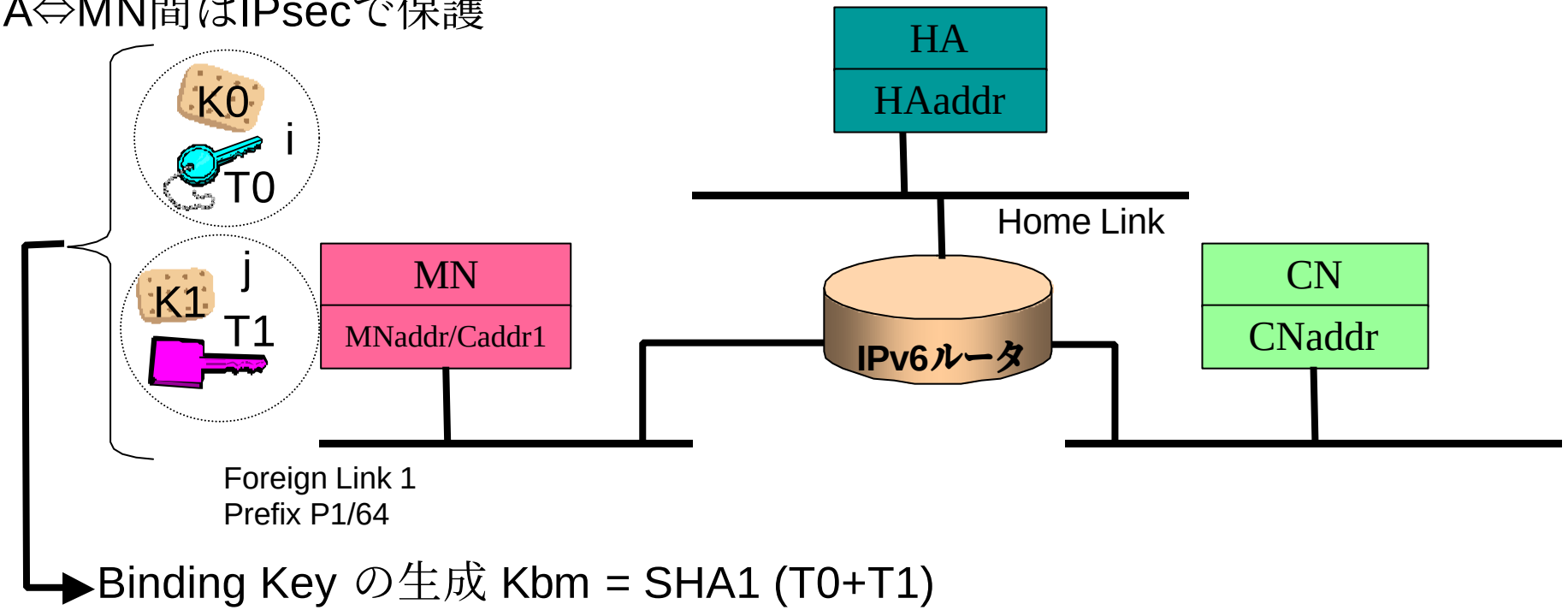
ホームエージェント経由／cookie K0, 署名用トークンT0, 臨時鍵番号 i を含む

(2) Care of Test Init (CoT)

MNへの直接配送／cookie K1, 署名用トークンT1, 臨時鍵番号 j を含む

Return Routability手続き STEP 5
MNは署名鍵（T0,T1）から署名MACを生成

HA⇔MN間はIPsecで保護



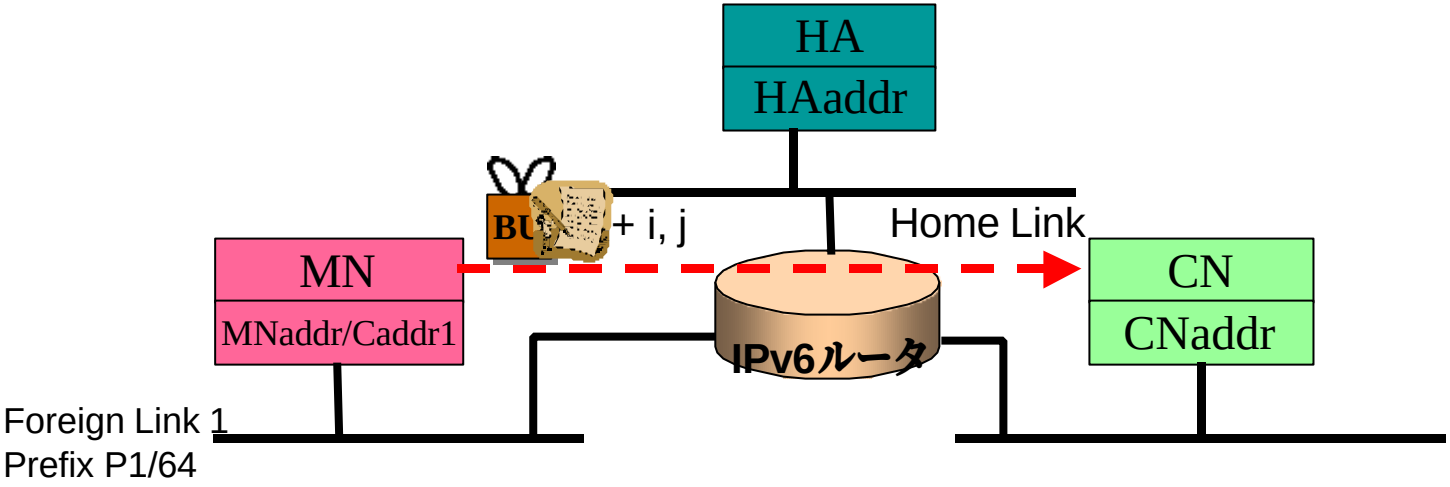
Binding Key の生成 Kbm = SHA1 (T0+T1)

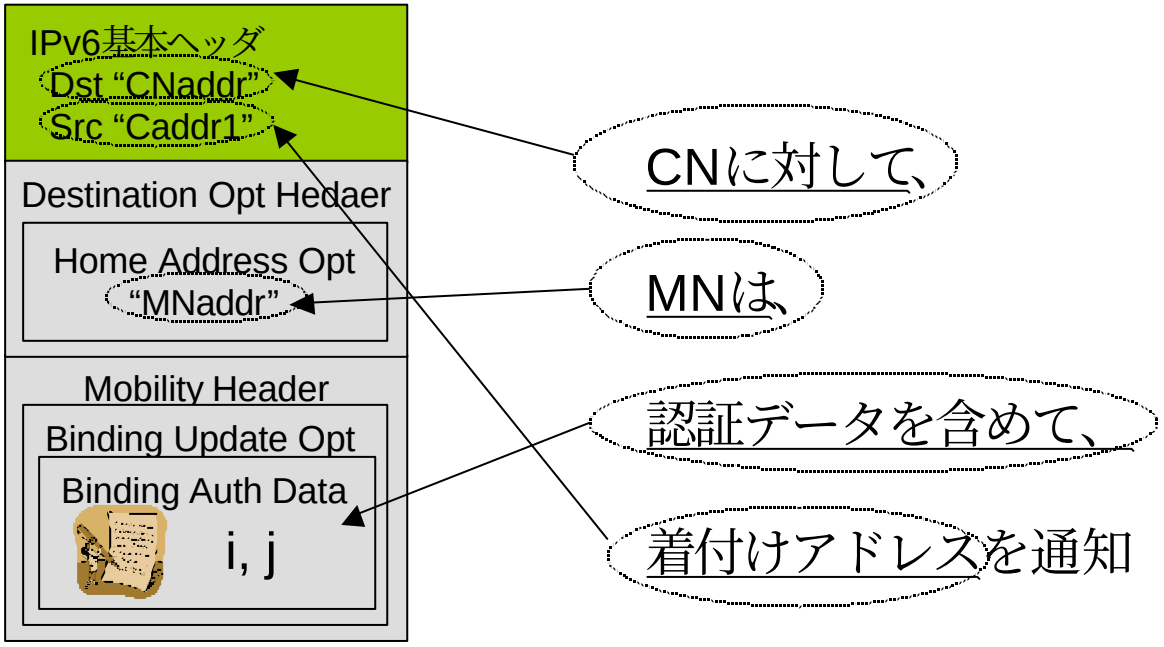
MNはBinding Updateメッセージを生成し、Kbmにより署名(MAC)を計算する

MAC = HMAC_SHA1 (Kbm, (Caddr1+CNaddr+BU))

Binding Updateメッセージのデータ

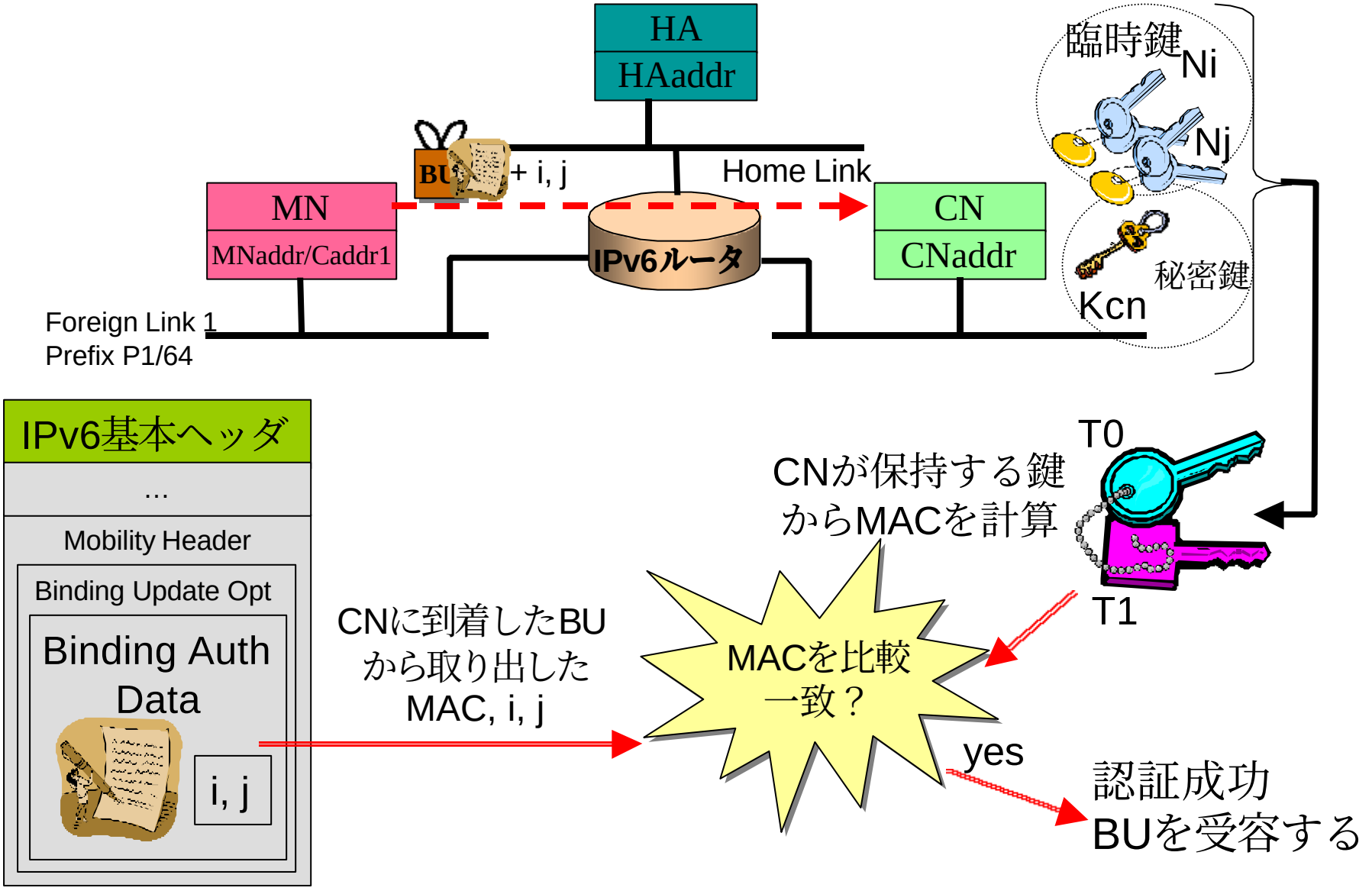
Return Routability手続き STEP 6
MNはCNへ署名つきBinding Updateを送信





Return Routability手続き STEP 7

CNはBUに含まれる署名を検証し正しければ受容



Return Routabilityの特徴と問題点

- 特徴
  - CNにアクセスしてくるMNは不特定多数
    - あらかじめMNの鍵を持つことは困難
    - PKI + IPsec は現状では非現実的
  - HAはMNを認証することを前提にする
    - RRはHA⇔MN間の通信が信頼できることを利用
- 問題点
  - CNの近傍（non-IPsec区間のCN⇔HA通信）の盗聴には無防備

⇒ 不特定多数の認証と不完全な認証の折衷案

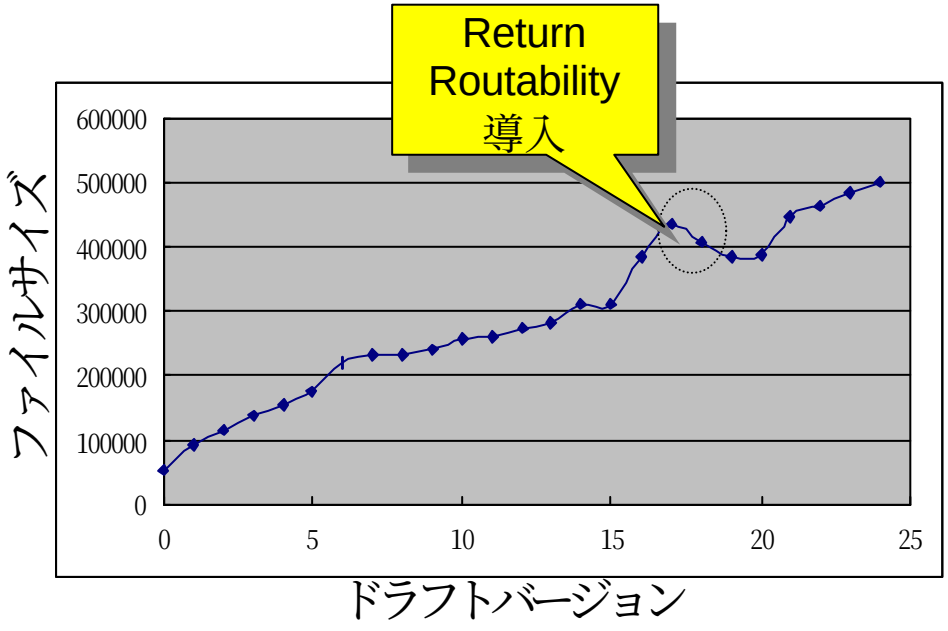
標準化動向

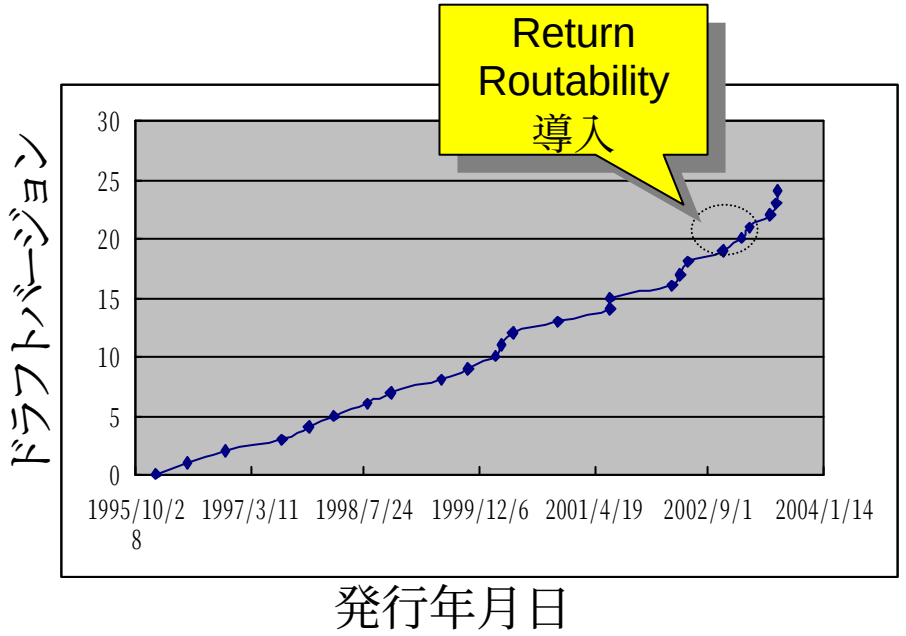
IETFでの標準化経緯

- ベーススペックに関する最新Internet Drafts
  - **draft-ietf-mobileip-ipv6-24.txt**
  - **draft-ietf-mobileip-mipv6-ha-ipsec-06.txt**
    ホームエージェントとモバイルノード間の通信の保護方法を規定

  RFC化に向けて最終調整の段階

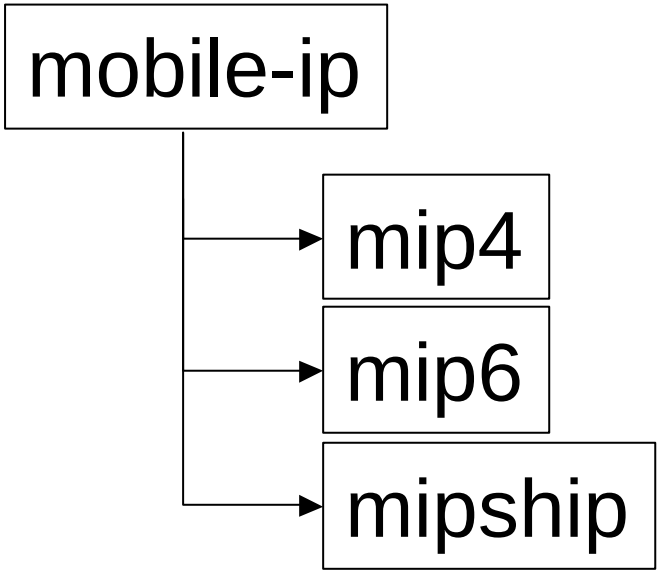
- 1996年から第24版まで議論され続けた長寿命ドラフト
- ID-15でRFC化が決まりかけたがIESGよりセキュリティに関するコメントがつく





標準化の最新動向
IETFにおけるワーキンググループ体制

第５７回ウイーン会合より体制を再編成



MobileIPv4

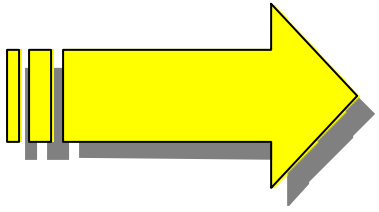
MobileIPv6

MIPv6 Signaling and Handoff Optimization（※）

※高速ハンドオーバ（FMIP, HMIP）に関する方式を議論

標準化の最新動向
第58回IETF mip6 WGでの議論内容 (1)

- ID-24をベースプロトコルとして固める
- 議論はベーススペックから＋αの機能へ
  - MobileIPv6 MIB
  - ホームエージェントの負荷分散／リダンダント化
  - マルチホーミング (MNの複数I/Fの使い分け)
  - プログラミングAPI
  - ファイヤウォールとの共存



実用品としてのチューンナップ
実環境での利用を強く意識した提案

標準化の最新動向
第58回IETF mip6 WGでの議論内容 (2)

- 相互接続性テストに関する提案
  - IPv6のコネクティビティさえあればMobileIPv6は動作する特長を生かす
  - 実網上で遠隔で相互接続試験を実施する枠組み
  - 単なる相互接続性試験ではなくデプロイの一環

- 幕張メッセにてTHAIテストイベント（2004/1）

  http://www.tahi.org/

主要各社の Mobile IPv6 実装状況

ホームエージェント（HA）	コレスポンデントノード（CN）	モバイルノード（MN）

BSD（KAME），Linux（MIPL, USAGI）

ホームエージェント単独
日立, NEC, Cisco

サーバ向けOS
HP（HP-UX, Tru64 UNIX）

Linux Zaurus / HP iPAQ（Linux）

Nokiaなどの携帯端末

Microsoft Windows Server 2003, Windows XP
Windows CE .NET 4.2

Apple（Mac OS）
Sun (Solaris)

携帯電話端末

Mobile IPv6 がもたらす効果

- IPはメディアに非依存の性質を利用すると
  - アクセス統合／ISP統合が実現
- ホームエージェントサービスの可能性
  - IP層の接続性が特定アクセス網／ISPから分離
  - ISPが変わっても同じアドレスを使い続けられる
  - 考え方はMSP（Mail Service Provider）と類似

    xxxxx@hotmail.com はISPに依存しない

Mobile IPv6 の課題

- ハンドオーバ
  - ハンドオーバ時間の短縮
    - FMIP (Fast MIP), HMIP (hierarchical MIP)
  - 異メディア間／異ISP間のハンドオーバ
    - ISPによりアカウントやアクセス方法はまちまち
- ホームエージェントオペレーション
  - 本来のインターネットは自立分散アーキテクチャ
  - Mobile IPv6は超集中型アーキテクチャ
- できないこと
  - セッションの保存
  - 端末間のコンテキスト移送

レイヤ別 位置透過性確保手法

［レイヤ４以上］
- SIP, Dynamic DNS, 各種VPN
- セッションの移送（例 VNC, Windows Terminal Service, SunRay）

○ セッションが保存できる
○ 端末間移動ができる

× 特定アプリケーションやサーバが必要
× 資源利用がサーバに集中

［レイヤ３］ Mobile IP, LIN6 など

○ アプリケーションは変更不要
○ メディアに依存しない（IPはメディア非依存）

× ハンドオーバ時間が長い
× セッション保存や端末間セッション移送は不可

移動に対してシームレス

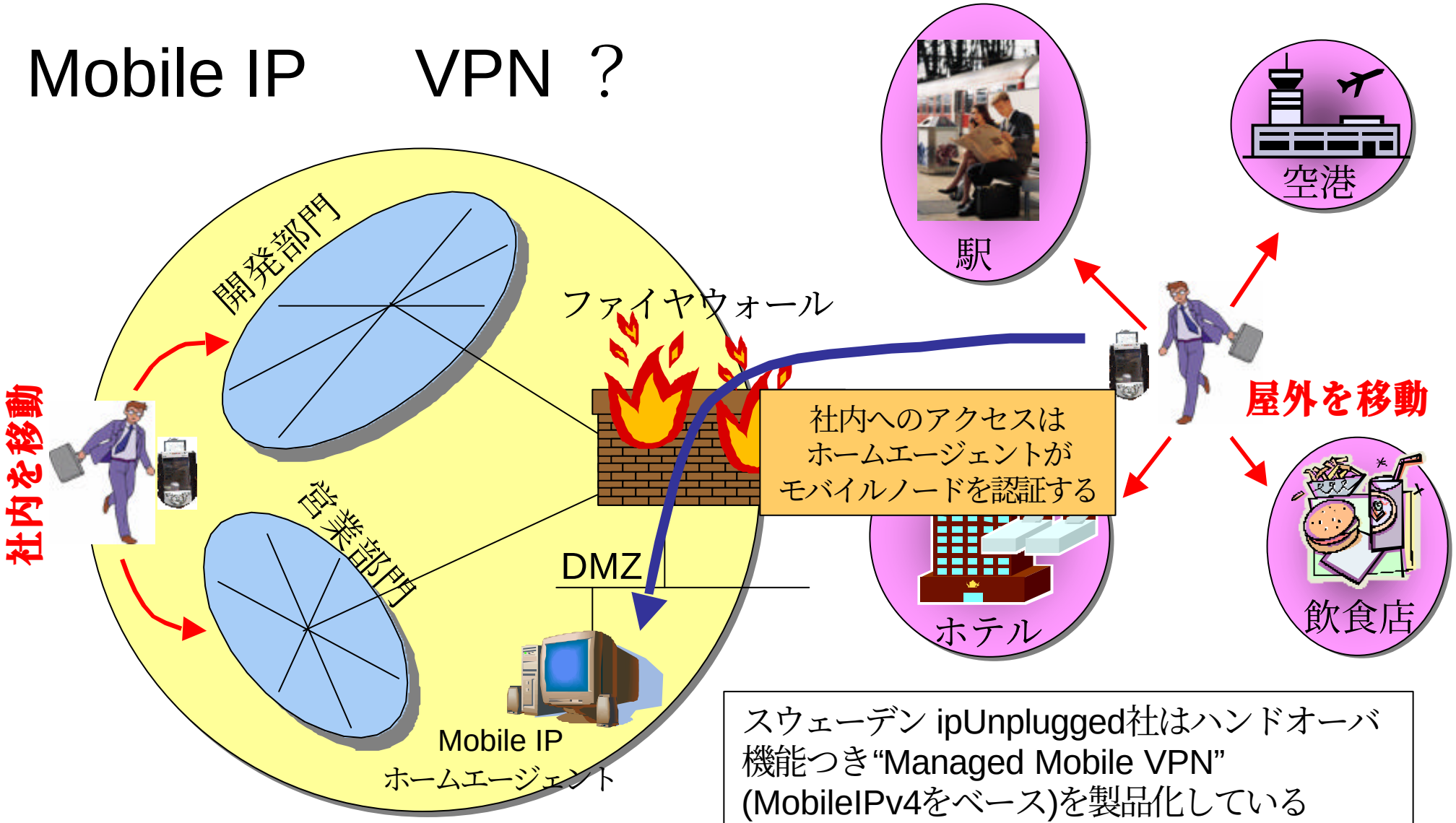
［レイヤ２］ 携帯電話, PHS, 無線LAN（L2）ローミング

○ プロトコルスタック／アプリケーションは変更不要
○ ハンドオーバ時間が短い

× メディアが単一
× 他のメディアに比べて低速

Mobile IP をVPN アクセスの手段として利用

Mobile IP　　VPN ？



スウェーデン ipUnplugged社はハンドオーバ機能つき“Managed Mobile VPN”(MobileIPv4をベース)を製品化している

ネットワークモビリティ

IPv6モバイル技術の新しい展望

標準化中

複数機器（＝ネットワーク）が丸ごと移動する

モバイルルータ 

ネットワークモビリティ （NEMO）

標準へ

機器単体（＝ノード）が移動する

モバイルノード 

ノードモビリティ （MobileIPv6）

確立

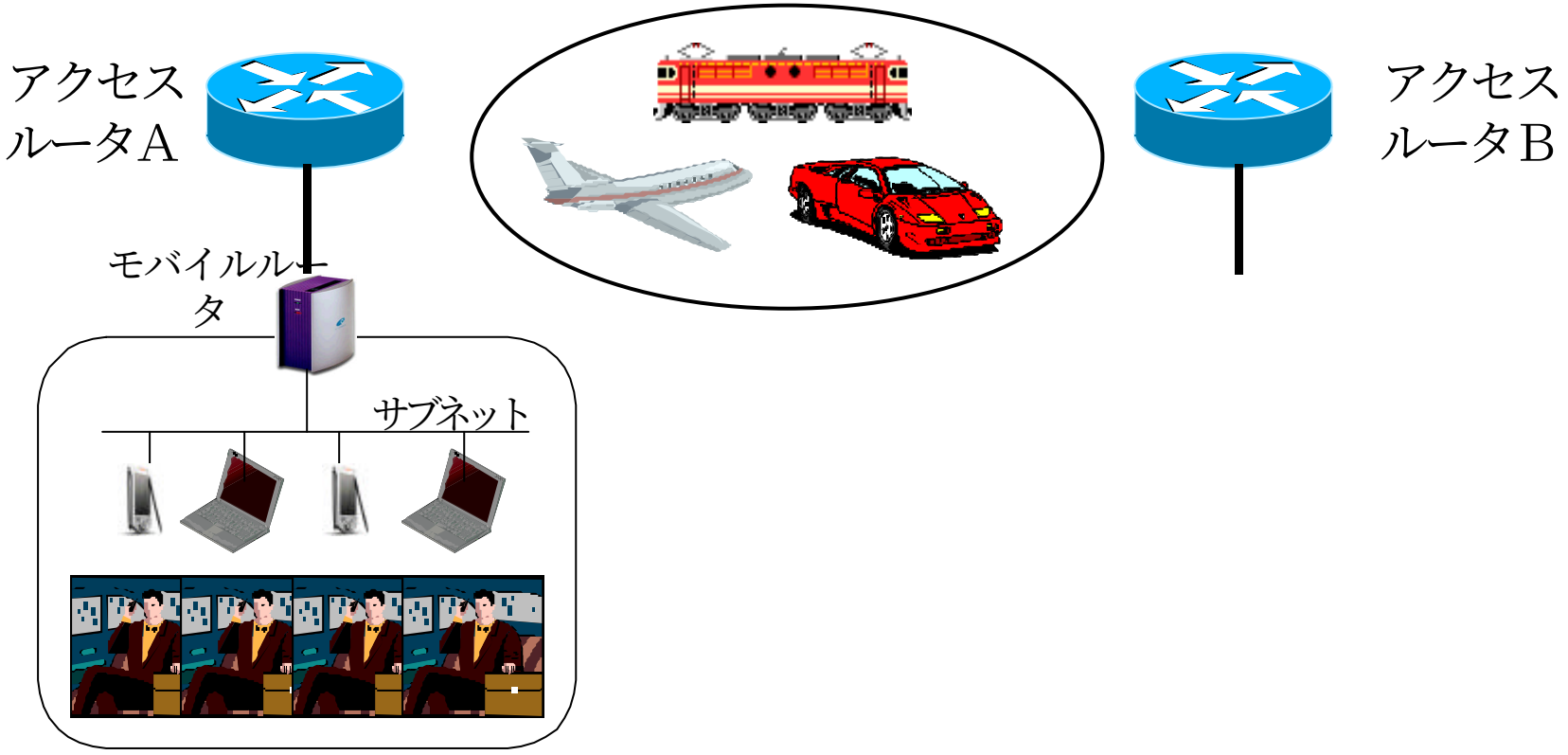
IPv6基礎技術

IPv6黎明期

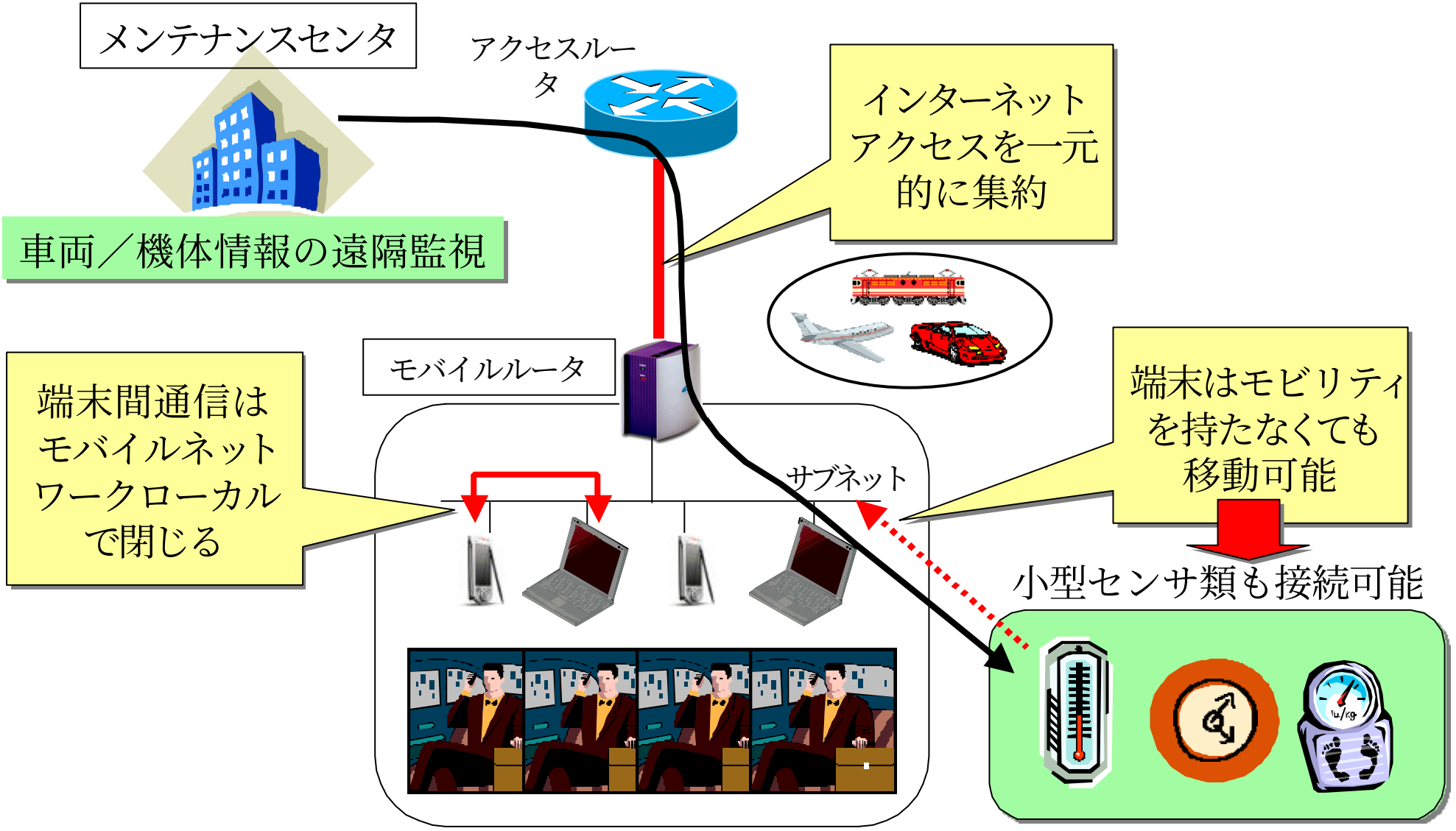
ネットワークモビリティ技術
サブネットワークが丸ごと移動

電車、自動車、飛行機など乗り物では
- 乗客　／センサーなど

複数のデバイスが同時に移動する

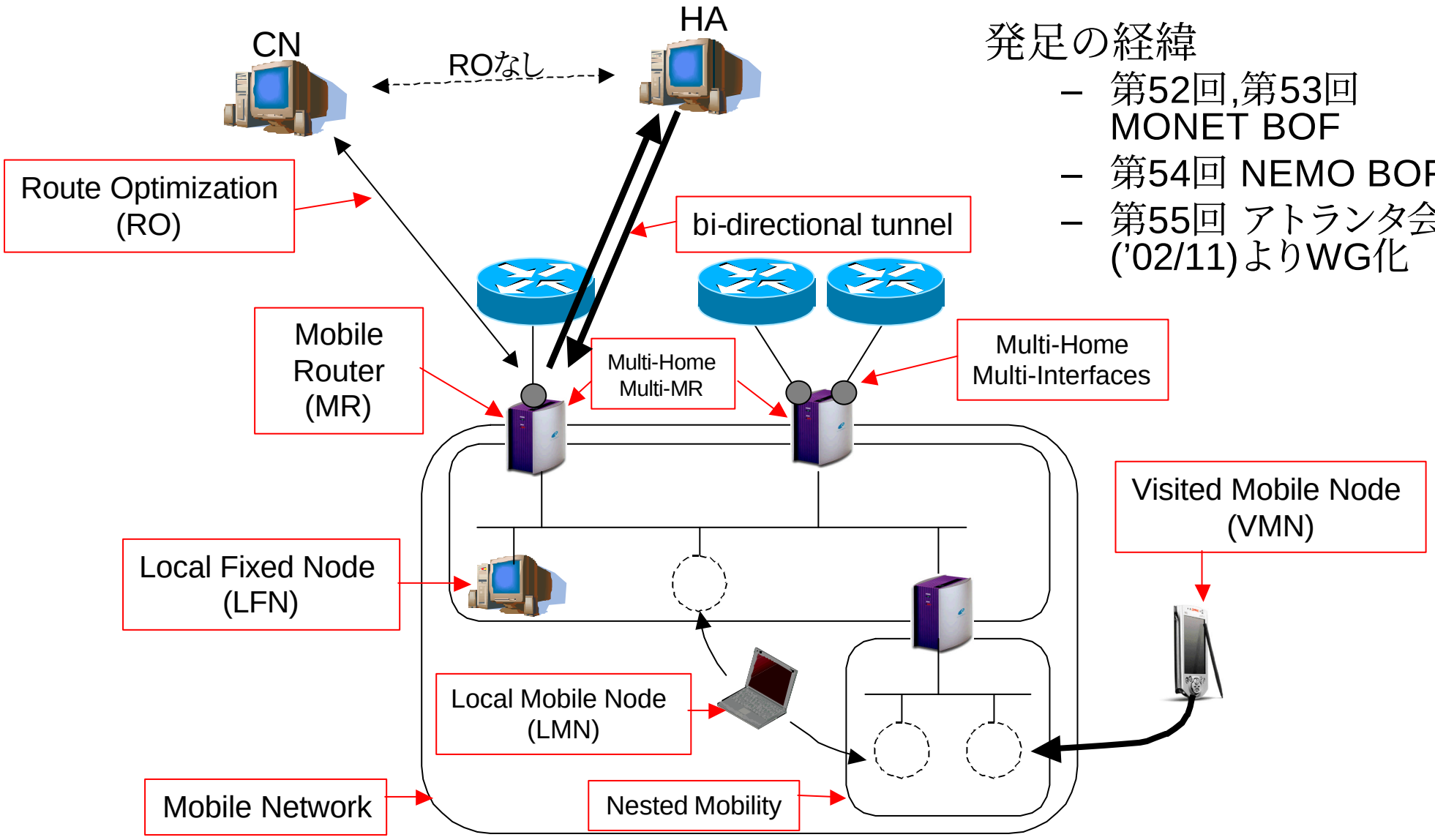


ネットワークモビリティの応用例



標準化動向

IETF NEMO (Network Mobility) ワーキンググループ



発足の経緯

- 第52回,第53回 MONET BOF
- 第54回 NEMO BOF
- 第55回 アトランタ会合 ('02/11)よりWG化

標準化動向
NEMOプロトコル概要

機能ごとにフェーズを分けて方式を検討

1. NEMO Basic Support
   - ホームエージェントと双方向トンネル
   - 実装も比較的容易
2. NEMO Extended Support
   - 経路最適化機能を取り込み

NEMO Basic Support Protocol (1)

draft-ietf-nemo-basic-support-01.txt

NEMOルータの動作例：

Explicit Network mode

② HAで3ffe:1800:01234:4567:/64に対するBinding Cacheエントリが構成される

① Rビットを立てたBinding UpdateによりMNPを通知

③ HAよりBinding Ackを返送

Binging Update

DST: HA SRC: 2001:218:1234::1
Destination Opt Header HoA Option 3ffe:1800:1234::1
Mobility Header Binding Update Mess. Rbit ON MNP Option 3ffe:1800:1234::/64

Binding Cache

Home address	CoA	Life Time
HoA	CoA	XXX

ルーティングテーブル

Destination	Gateway
3ffe:1800:1234::/64	Mobile Router へ

CoA 2001:218:1234::1

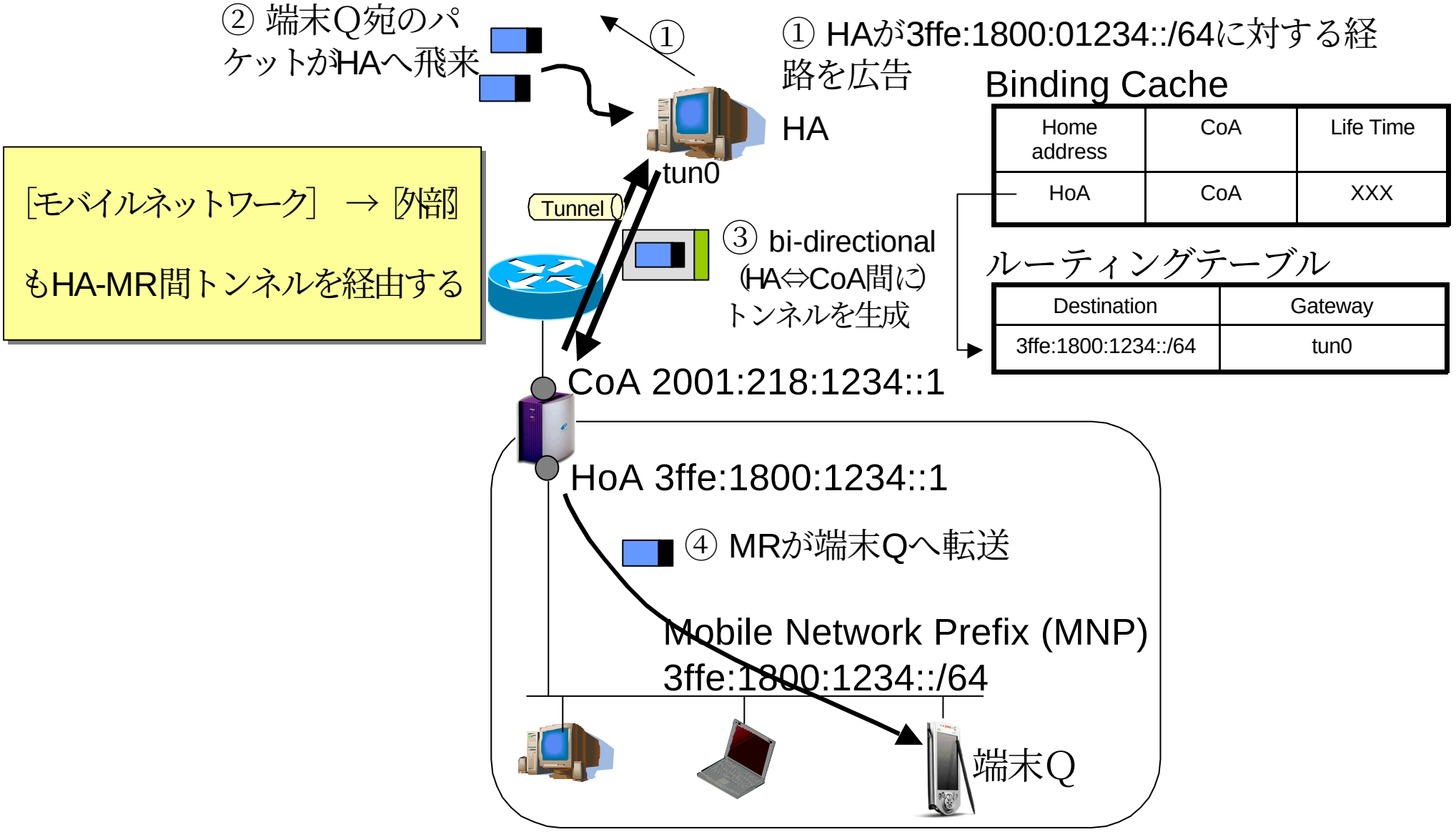
HoA 3ffe:1800:1234::1

Mobile Network Prefix (MNP)
3ffe:1800:1234::/64



NEMO Basic Support Protocol ②

draft-ietf-nemo-basic-support-01.txt



まとめと今後の課題

- IPv6モバイル技術は確立し始めている
  - 実装の出揃い待ち

- 次は新しい利用モデルの創出
  - Mobile IPv6 を実用品としてデプロイするために
    - 運用のための経験値を積む
    - 新しいISPサービスモデルの開発
  - ネットワークモビリティの新たな応用は？

参考文献

- IETF WG
  - mip6 WG
    http://www.ietf.org/html.charters/mip6-charter.html
  - mipship
    http://www.ietf.org/html.charters/mipshop-charter.html
  - nemo WG
    http://www.ietf.org/html.charters/nemo-charter.html
- Mobile IPv6 実装
  - KAME project
    http://www.kame.net/
  - USAGI Project
    http://www.linux-ipv6.org/
  - MIPL Mobile IPv6 for Linux
    http://www.mipl.mediapoli.com/
- ニュース／最新情報
  - v6start.net
    http://www.v6start.net/
  - IPv6style
    http://www.ipv6style.jp/