IPv6 におけるネットワーク内部の隠蔽方式の提案

060427466 久保敷 透
渡邊研究室

1. はじめに

インターネットの普及に伴い IPv4 アドレスの枯渇が予測されており，根本的な解決策として IPv6 アドレスへの移行が必須である．IPv4 では NAT を利用することで，アドレスの枯渇対策に寄与していた．その結果，NAT 配下のネットワークが隠蔽されるという利点があった．しかし，IPv6 ではすべての端末に一意なアドレスが割り当てられるため，端末が特定されたり，ネットワーク構成が予測されたりする可能性がある．そのため，IPv6 を使用した場合においてもネットワーク内部を隠蔽したいという要求がある．そこで本稿では，IPv6 におけるネットワーク内部の隠蔽方式を提案する．

2. 既存技術

IPv6 にはプライバシー問題を解決するアドレスとして TA（Temporary Address）[1] がある．TA は IPv6 アドレスの下位 64 ビットのインタフェース ID をランダムに生成することで，端末の特定を防ぐ．しかし，TA ではサブネット ID からネットワーク構成が予測されてしまう可能性がある．

そこで，ネットワーク構成を隠蔽する方式としてホストルートを設定する方式が提案されている [2]．この方式ではサブネット ID を任意に設定したアドレスを使用する．しかし，サブネット ID が任意な値であるため，ルータがパケットをルーティングすることができない．そのため，ルータにホストルートを設定する．しかし，この方式では IPv6 アドレスの重複検出がルータを越えて行えないことや，ルータのエントリー数が膨大になることが問題となっている．

3. 提案方式

提案方式では，端末が 2 つのアドレスを持ち，通信相手の位置によってアドレスを使い分ける．一つのアドレスにはランダムに生成したアドレスを用い外部端末と通信を行う．もう一つのアドレスはネットワーク内でのみ有効なアドレスを用い，内部端末と通信を行う．

3.1 アドレス定義

内部端末との通信には ULA（Unique Local Unicast IPv6 Address）[3] を用いる．ULA は高い一意性を持っており，ネットワーク内でのみ有効なアドレスとされている．

一方，外部端末と通信を行う場合は，使用しているアドレスからネットワーク構成が予測されないようにしなければならない．そこで，新たにサブネット ID を含めた下位 80 ビットまでをランダムに生成した CA（Concealed Address）を導入する．

3.2 通信概要

図 1 に提案方式の概要を示す．内部端末である INa（Internal Node）には外部通信用の CA1 と内部通信用の ULA1 の 2 つのアドレスが割り当てられている． INa は通信相手の位置を判断し，内部端末である INb ならば ULA1 を，外部端末である EN（External Node）ならば CA1 を送信元アドレスとして通信を行う．CA1 を用いた通信を可能とするため， CA1 のホストルートをルータに設定する．

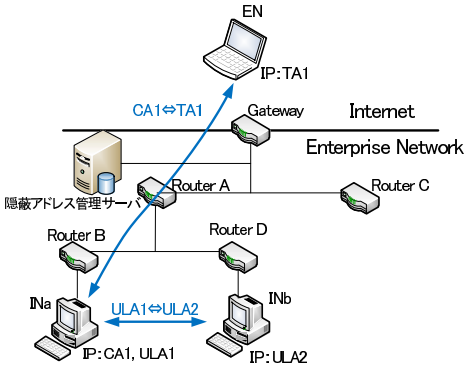


図 1: 動作概要

3.3 隠蔽アドレス管理サーバ

ホストルートで問題となる IPv6 アドレスの重複検出やエントリー数が膨大になるなどの問題を解決するため，新たに隠蔽アドレス管理サーバを設置する．以下に必要とする機能を述べる．

(1) CA の管理
端末からアドレスの要求があった場合に，部通信用アドレス CA を生成し，端末に割り当てる．すべての CA は隠蔽アドレス管理サーバで管理し，どの端末にどの CA が割り当てられているのかを把握する．

(2) ホストルートの自動設定
ホストルートの設定をゲートウェイルータから外部と通信を行いたい端末までのルータに設定する．これにより，ルーティングテーブルのエントリー数の増大を抑える．

(3) ネットワーク構成の把握
隠蔽アドレス管理サーバはホストルートの設定のために，ネットワーク構成を把握する必要がある．その方法として SNMP（Simple Network Management Protocol）を利用し，ルータが所持する管理情報である MIB（Management Information Base）を参照することでネットワーク構成を把握する．

4. まとめ

IPv6 におけるネットワーク内部の隠蔽方式として，通信端末が外部と内部の場合で 2 つのアドレスを使い分ける方式を提案した．今後は実装と評価を行っていく．

参考文献

[1] T. Narten R. Draves S. Krishnan：Privacy Extensions for Stateless Address Autoconfiguration in IPv6, RFC4941, (2007)

[2] G. Van de Velde T. Hain R. Droms B. Carpenter E. Klein“ Local Network Protection for IPv6 ”RFC4864 May 2007

[3] R. Hinden B. Haberman“ Unique Local IPv6 Unicast Addresses ” RFC4193 October 2005

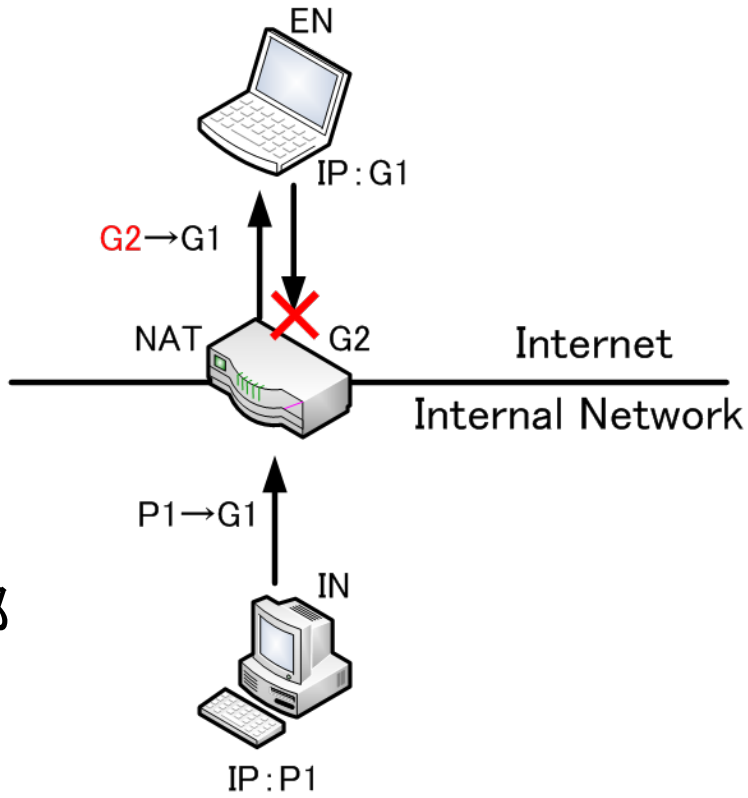
IPv6におけるネットワーク内部の隠蔽方式の提案

渡邊研究室
060427466
久保敷透

Watanabe Lab.

研究背景

- グローバルIPv4アドレスの枯渇
  - 短期解決策
    - プライベートアドレスの利用
- NATの特徴
  - NAT越え問題
  - 外部にはNATのアドレスしか見えないため副次的にネットワーク内部が隠蔽される



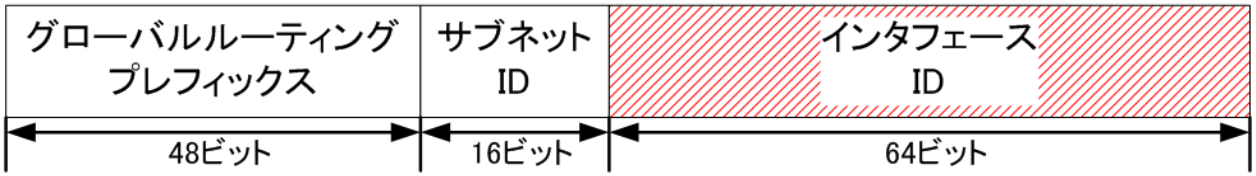
IPv6アドレスへの移行

NAT: Network AddressTranslation
IN:Internal Node
EN:External Node

研究背景

- IPv6アドレス
  - アドレスが十分確保されるためNATが必要ない
  - IPv6アドレスは一意なアドレスが割り当てられる

- 一時アドレス（TA：Temporary Address）
  - インターフェースIDをランダムに生成する
    ⇒ネットワーク構成までは隠蔽できない

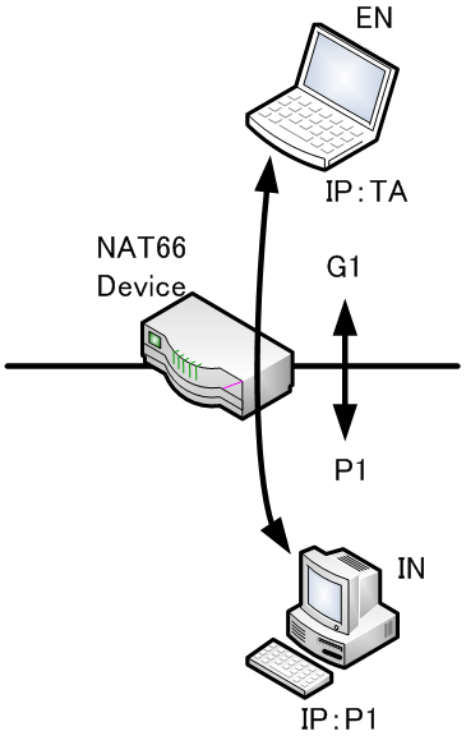


ネットワーク内部を隠蔽する方法

Watanabe Lab.

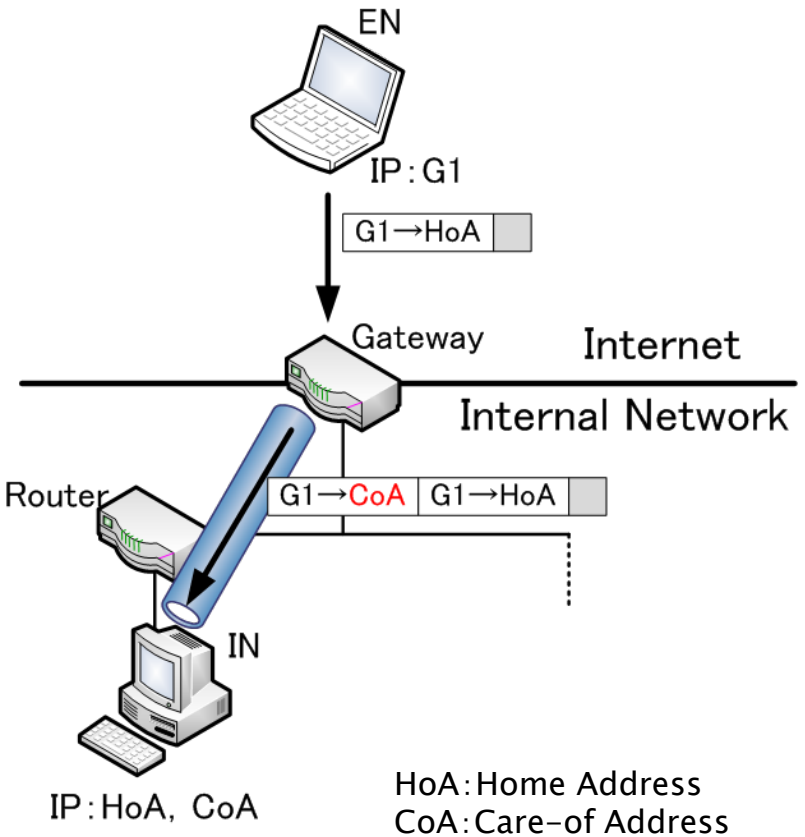
既存技術(1)

- NAT66(IPv6-to-IPv6 Network Address Translation)
  - IPv4におけるNATと同様にアドレス変換する
  - 一対一に対応させて変換
  - 双方向で通信を開始できる
  - ペイロード内にアドレスが含まれるアプリケーションは通信ができない



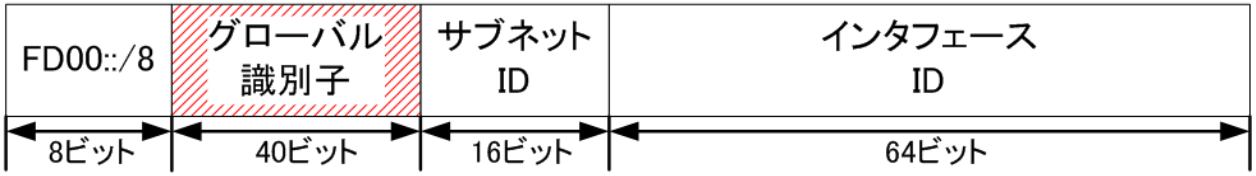
既存技術(2)

- Mobile IPv6を用いたネットワーク内部隠蔽
  - ゲートウェイがホームエージェントの役割を果たす
  - ホームアドレス(HoA)
    - 任意のサブネットID
  - 気付けアドレス(CoA)
    - ネットワーク構成に応じたアドレス
  - 内部端末同士の通信⇒経路の冗長
  - カプセル化⇒オーバーヘッド

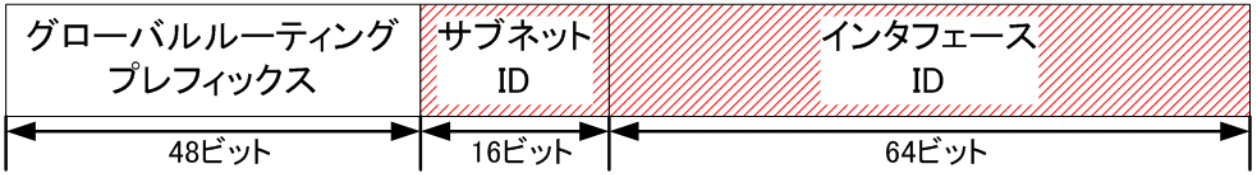


提案方式

- 内部端末には2つアドレスを割り当て，相手端末の位置によりアドレスを使い分ける
  - 内部通信用アドレス
    - ULA（Unique Local Unicast IPv6 Address）



  - 外部通信用アドレス
    - 隠蔽アドレス（CA：Concealed Address）



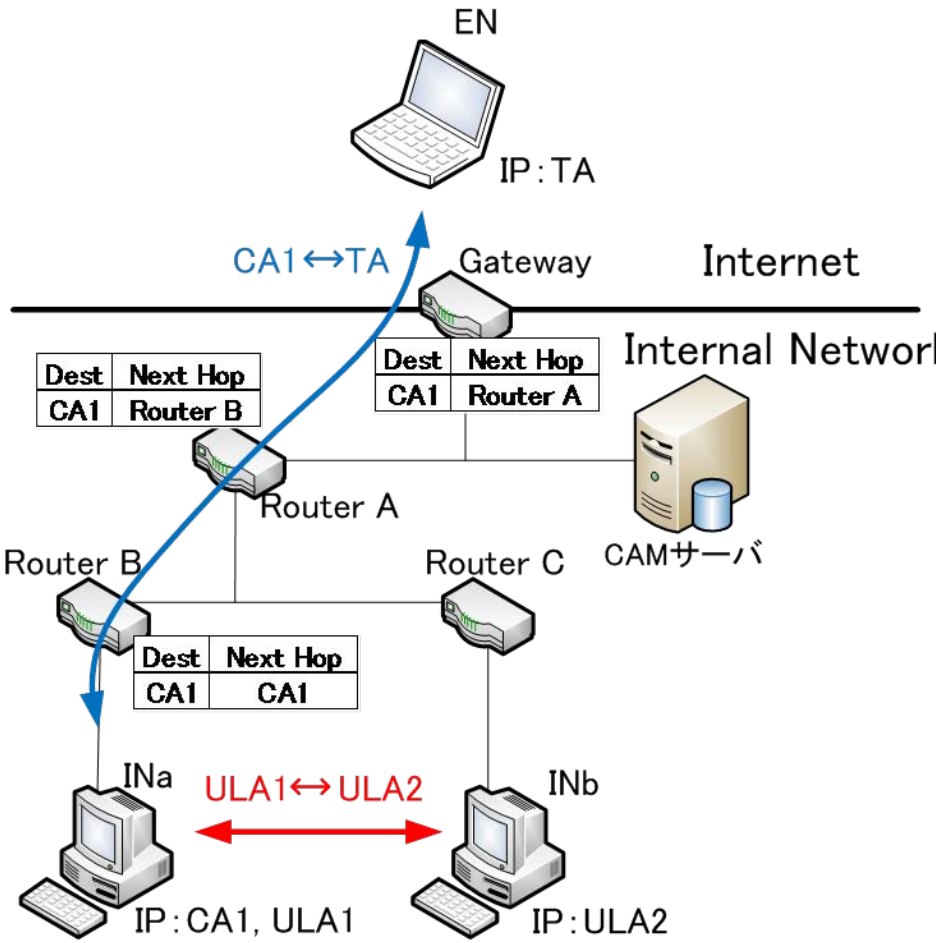
ホストルートによるルーティング

- ホストルート
  - 端末までのルートをルータに一意に設定する
  - サブネットIDがランダムであってもルーティングが可能

- 問題点
  - 端末ごとにホストルートを設定するためルーティングテーブルが膨大になる
  - アドレス重複検出が行えない

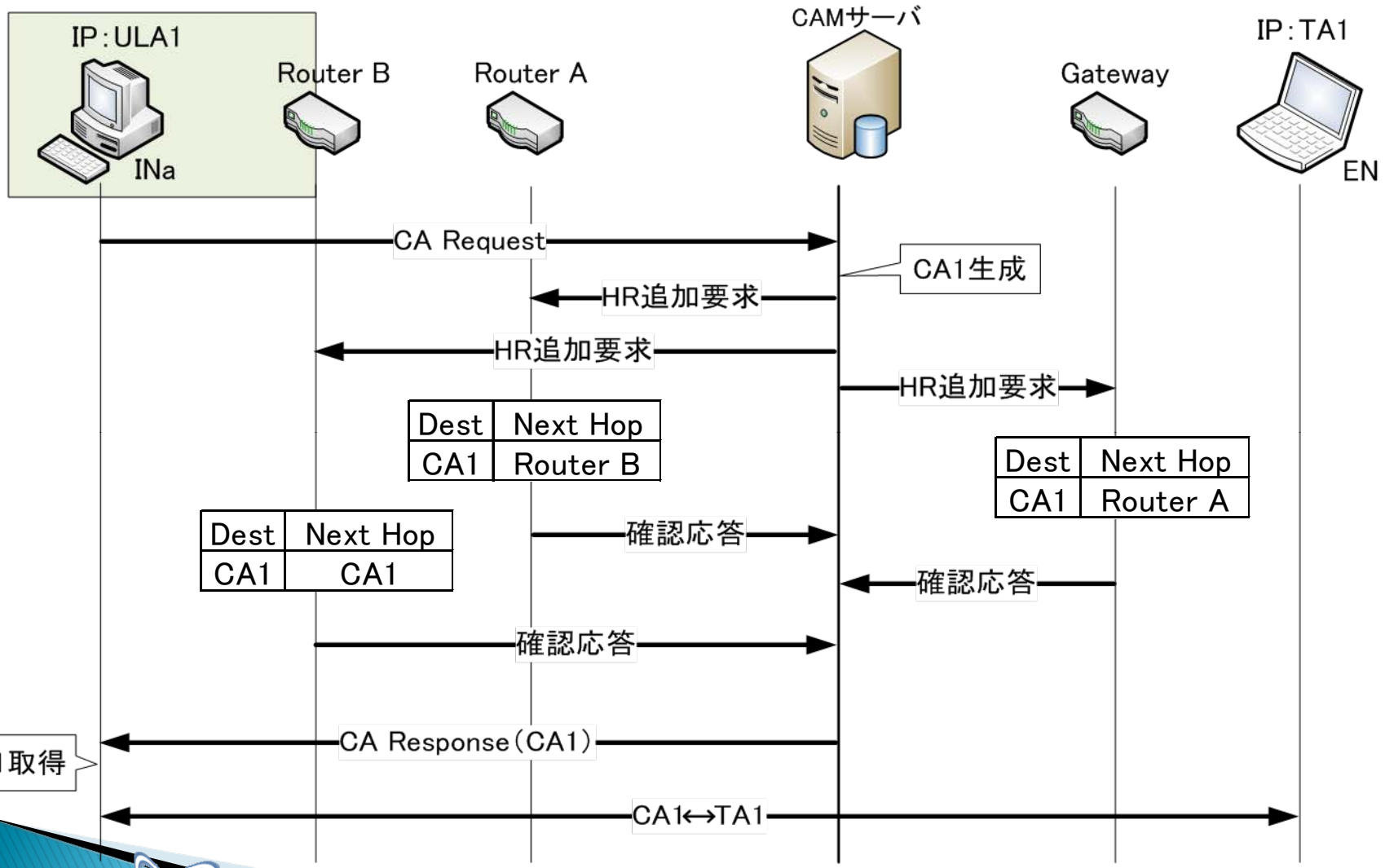
通信概要

- CAMサーバの機能
  - CAの管理
    - 生成、割り当て
  - ネットワーク構成の把握
  - ホストルートの設定
    - 必要なルータにのみホストルートを設定



CAMサーバ：Concealed Address Management Server

CAの取得動作

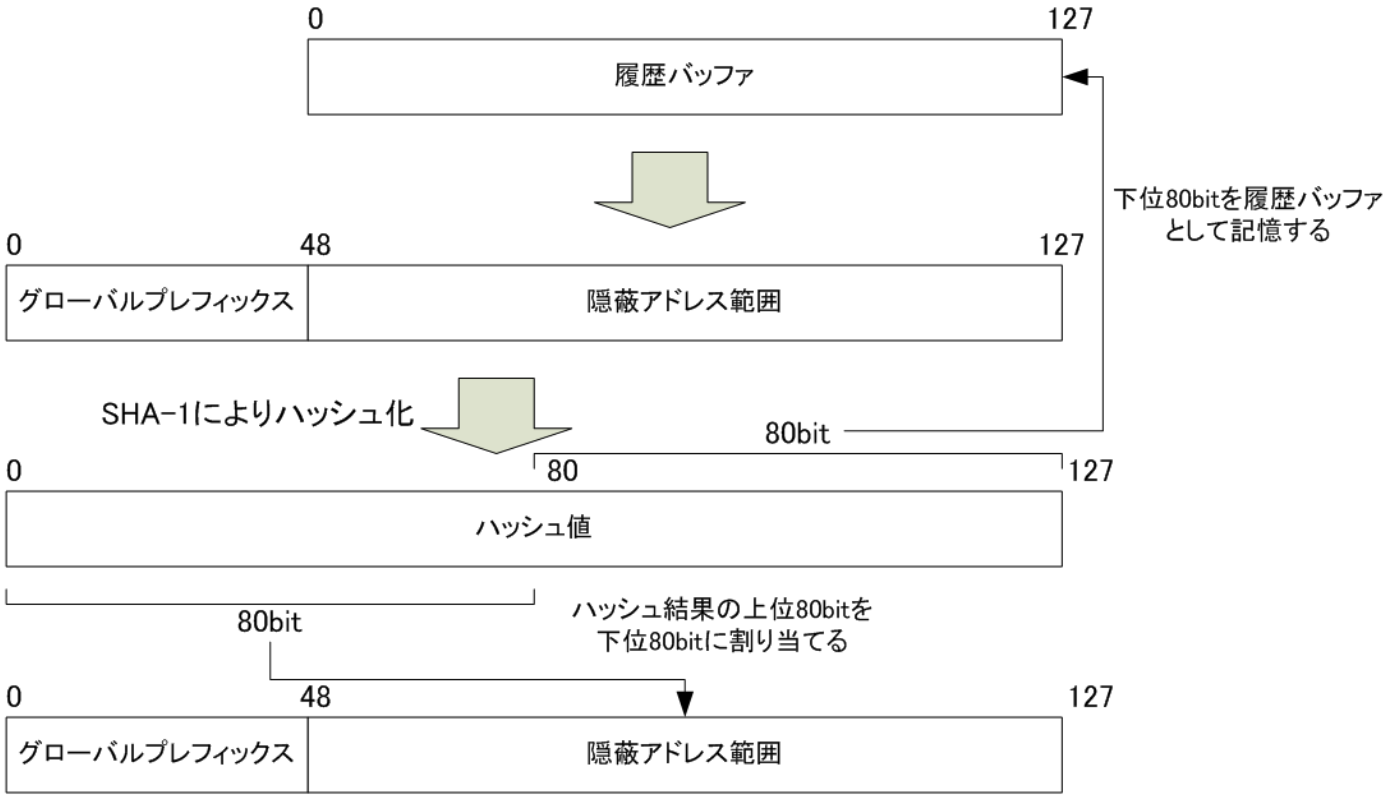


HR:Host Route

まとめ

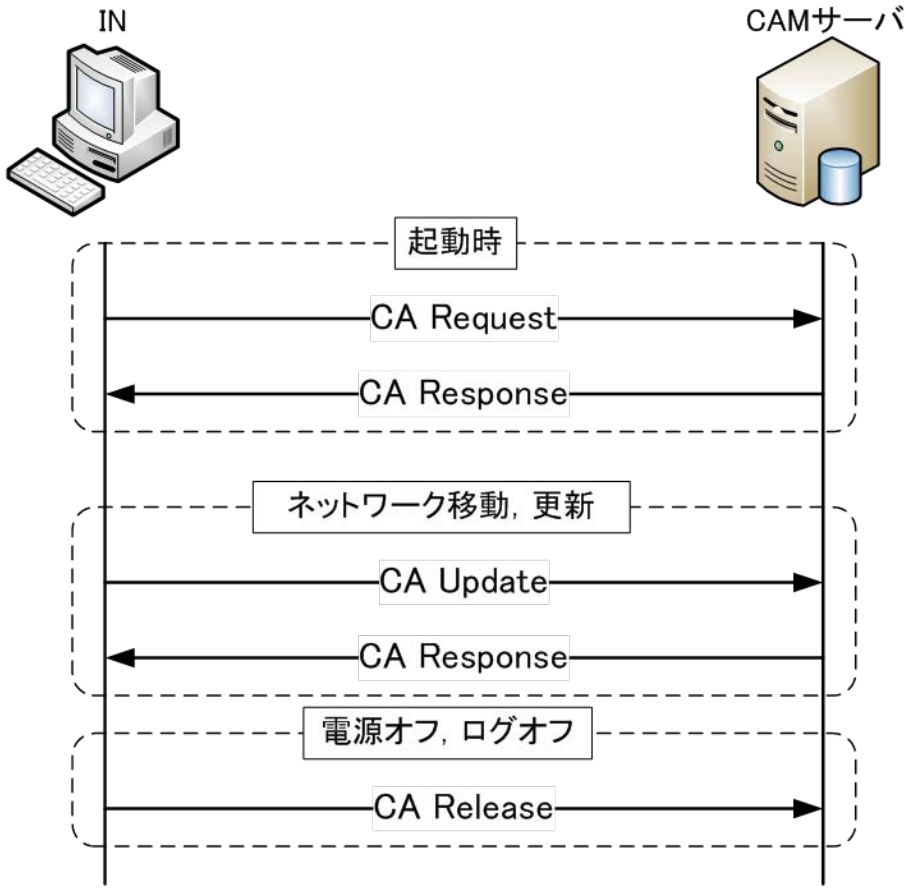
- 提案
  - 端末に2つのアドレスを割り当て，通信相手によって使い分ける
  - CAMサーバの設置によりホストルートの問題を解決
- 今後
  - 実装と評価

CA生成

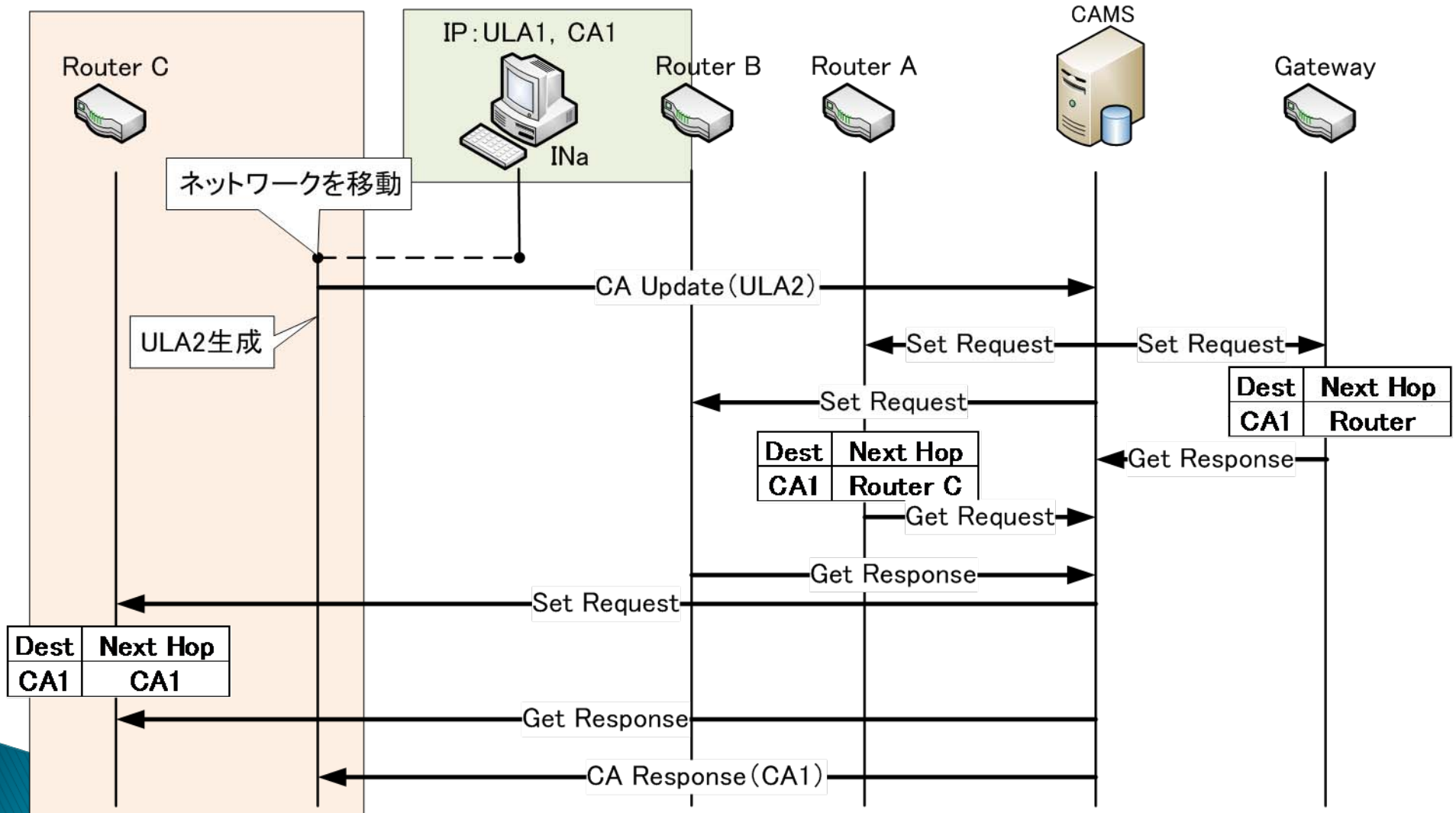

0
127
履歴バッファ
下位80bitを履歴バッファ
として記憶する
0
48
127
グローバルプレフィックス
隠蔽アドレス範囲
SHA-1によりハッシュ化
80bit
0
80
127
ハッシュ値
80bit
ハッシュ結果の上位80bitを
下位80bitに割り当てる
0
48
127
グローバルプレフィックス
隠蔽アドレス範囲

CAの取得と解放

- 起動時
  - CAの取得，ホストルートの設定
- ネットワーク移動，更新
  - CAの取得，ホストルートの再設定
- 電源オフ，ログオフ
  - CAの解放，ホストルートの削除

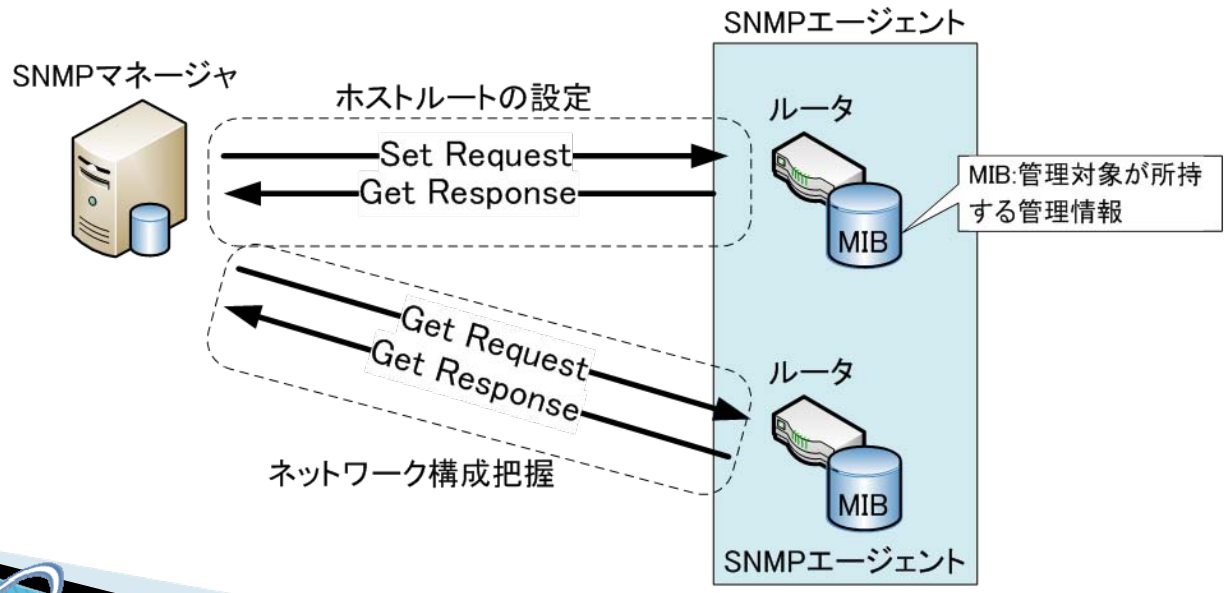


ネットワークを移動したときの動作



SNMP

- SNMP(Simple Network Manegement Protocol)
  - ネットワークを管理するプロトコル
  - 管理対象が所持するMIB(Manegement Information Base)を参照することにより，機器の状態を知ることができる
  - MIBの変更も可能



隠蔽アドレス管理サーバ

- 隠蔽アドレス管理サーバ(CAMサーバ:Concealed Address Management Server)の機能
  - CA管理
    - CA生成，割り当て，有効期限のチェック
  - ホストルートの設定
    - ルータのエントリー数を抑えるため端末から外部ネットワークまでのルート上のルータにのみホストルートを設定する
  - ネットワーク構成把握
    - ネットワーク構成把握のためネットワーク管理プロトコルであるSNMPを利用する

提案方式の比較

	NAT66	Mobile IPv6	提案方式
導入コスト	○	×	△
アプリケーション	×	○	○
ルータ負荷	○	△	△

- NAT66
  - アプリケーションが制限されるのは大きな問題
- Mobile IPv6
  - 経路冗長、オーベーヘッドによりゲートウェイに負荷がかかる
  - Mobile IPv6をすべての端末に実装
- 提案方式
  - ホストルートによるルータ負荷