IPv6におけるネットワーク構成隠蔽に関する検討

久保敷　透[†1]　鈴木秀和[†2]　渡邊　晃[†2]

グローバル IPv4 アドレスの枯渇に伴い，IPv6 への移行が必須とされている．これまで IPv4 では，NAT によりネットワークが隠蔽されるという利点があった．IPv6 へ移行した場合においても同様にしてネットワークを隠蔽したいという要求がある．これを実現するための方式として，Mobile IPv6 を用いた方式や，ルータにホストルートを設定する方式が提案されている．しかし，Mobile IPv6 を用いた方式では，経路冗長やカプセル化によるオーバヘッド，ホストルートでは，ルーティングテーブルの増大が課題となる．本稿では，これらの課題を解決できる方式を提案し評価する．

Researches on a concealing method of network topology in IPv6

Toru Kuboshiki,[†1] Hidekazu Suzukki[†2]
and Akira Watanabe[†2]

With a global IPv4 address depletion, it is said that the transition to IPv6 is essential. Until now, there was an advantage that the network was concealed by NAT in IPv4. There is a demand that it wants to conceal network in the same way even if it transition to IPv6. The method to use Mobile IPv6 and the method to set the host routes to the router are proposed as a method to achieve this. However, the overhead by encapsulation and redundant route become problems in the method to use Mobile IPv6, and the increase of the routing table becomes a problem in the method to host routes. In this paper, We propose the method that can solve these problems, and evaluate it.

†1 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University
†2 名城大学理工学部
Faculty of Science and Technology, Meijo University

1. はじめに

インターネットを利用する機器の増加によりグローバル IPv4 アドレスの不足が問題となっている[1)]．アドレス枯渇問題に対する短期的な解決策として，プライベートアドレスを定義し，組織内でこのアドレスを使いまわす方法がとられてきた．プライベートアドレスネットワークからインターネットへ接続する場合には NAT（Network Address Translation）が必要となる．NAT はプライベートアドレスをグローバルアドレスへ変換する機能を持ち，一つのグローバルアドレスを複数の端末で共有することによりアドレスを節約できる．この結果，インターネット側から組織内へ向けて通信を開始することができない，いわゆる NAT 越え問題が生じている．また，アドレスを書き換えるため，IP アドレスを直接扱うアプリケーションが利用できないという制約がある．しかし NAT を用いることにより，インターネット側から組織内の端末やネットワーク構成などが隠蔽されるという副次的な利点があった．企業が IPv4 を使用し続ける要因として，IPv6 への移行が面倒であるだけでなく，NAT によるアドレスの隠蔽が企業にとってセキュリティ上有益であると考えられていることも挙げられる．しかし，現在のグローバル IPv4 アドレスの枯渇は深刻であり、根本的な解決策となる IPv6 への移行が必須とされている．

IPv6 へ移行した場合には，NAT が不要になるため，NAT 越え問題やアプリケーションの制限がなくなり、エンド端末同士が自由に通信することができる．しかし，NAT を使用することによって生まれてきたネットワーク内部が隠蔽される利点がなくなり，端末を特定されたりネットワーク内部の構成を予測される可能性がある．

そこで，IPv6 へ移行した場合においても端末やネットワーク構成が隠蔽される方法が考えられている．[2)–3)]．端末のプライバシー保護の問題を解決するアドレスとして，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一時アドレス（Temporary Address）[4)] がある．しかし，一時アドレスは，サブネット ID が隠蔽できないため，ネットワーク構成が予測されてしまうという懸念がある．ネットワーク構成まで隠蔽する技術として，NAT66（IPv6-to-IPv6 Network Address Translation）[5)]，Mobile IPv6[6)]，およびホストルート[6)] を用いた方式が考えられている．NAT66 は，ゲートウェイでアドレスを変換する方式である．IPv4 のような NAT 越え問題は存在しないが，IP アドレスを直接扱うアプリケーションが利用できないという問題は解決できない．Mobile IPv6 を用いた方式は，移動透過性の技術をアドレスの隠蔽に利用する方式である．しかしこの方式では，内部端末同士の通信においても経路冗長が発生し，カプセル化によるオーバヘッドが発生するという

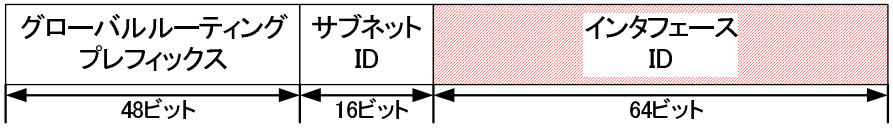


図 1 一時アドレスの構成
Fig. 1 Temporary Address

課題がある．ホストルートを用いた方式は，ルータに全端末のホストルートを設定する方式である．この方式では，ルーティンテーブルのエントリー数が膨大になるという課題がある．Mobile IPv6 とホストルートを用いた方式に関しては，アドレスの重複検出が行えないという課題がある．

本稿では，ネットワーク構成を隠蔽する方式として，内部端末に 2 つのアドレスを持たせ，通信相手端末の位置によりアドレスを使い分ける方式を提案する．外部端末との通信に用いるアドレスのルーティング方法としてトンネリング方式とホストルート方式のそれぞれを提案し比較する．

以下，2 章で既存技術の詳細を説明し，3 章で提案方式について述べる．4 章で評価，5 章でまとめを行う．

2. 既 存 技 術

2.1 一時アドレス

図 1 に一時アドレスの構成を示す．IPv6 アドレスのステートレスアドレス自動生成では，下位 64 ビットのインタフェース ID を MAC アドレスを基に生成する．そのため，インタフェース ID から端末を特定する事ができる．一時アドレスは，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により，端末の特定を防ぐものである．しかし，組織内のネットワークをルーティングするために使われるサブネット ID の値はそのままであるため，この値を解析することにより内部のネットワーク構成が予測されてしまう可能性がある．

2.2 NAT66（IPv6-to-IPv6 Network Address Translation）

IPv6 では NAT を使用する必要がないため，エンドエンド通信が行えることが最大の利点である．しかし，IPv4 運用者の間では NAT を利用することによりネットワーク内のアドレスの管理が容易になり，セキュリティが容易に確保できるという考えが根強い．そこで，IPv6 の移行をスムーズに行うためにも NAT が必要であるとして，NAT66 が提案された．NAT66 では，IPv4 のプライベートアドレスと同様に，ネットワーク内部でのみ有効なアドレスを用い，インターネットへ接続する際にグローバルアドレスへ変換する．NAT66 では外部から見た場合，グローバルアドレスは内部端末の数だけ存在するため，IPv4 のような NAT 越え問題は起こらない．NAT66 機器の内側のプレフィックスには ULA（Unique Local Unicast IPv6 ）[7]，外側にはグローバルルーティングプレフィックスが割り当てられる．NAT66 は IPv6 アドレスの後半 64 ビットのインタフェース ID は変換せずに前半の 64 ビットのみを変換する．このとき，アドレス全体のチェックサムが変わらないような工夫が取り入れられている．NAT66 ではネットワーク内部を完全に隠蔽することが可能であるが，アドレス変換を行っているため，ペイロード内に IP アドレス情報を含む SIP（Session Initiation Protocol）や FTP（File Transfer Protocol）などのプロトコルではアプリケーションごとに対応が必要になってくる．

2.3 Mobile IPv6 によるネットワークの隠蔽方式

図 2 に Mobile IPv6 を用いたネットワーク構成の隠蔽方式を示す．この方式ではゲートウェイが Mobile IPv6 における HA（Home Agent），内部端末 IN（Internal Node）が移動ノード MN（Mobile Node），外部端末 EN（External Node）が通信相手ノード CN（Correspondent Node）の役割を果たす．内部端末 IN にはホームアドレス（HoA : Home Address）としてサブネット ID が任意のアドレスを割り当てる．任意のサブネット ID が割り当てられている領域を論理サブネット（Logical Subnet）と呼ぶ．論理サブネットは実際のトポロジーに関係なく存在する．IN には HoA とは別に実際のネットワーク構成に応じた気付けアドレス（CoA : Care-of Address）が割り当てられる．IN はゲートウェイに HoA と CoA の関係を登録しておく．EN が IN と通信を行う場合，EN は IN のアドレスを HoA と認識し，HoA へ宛ててパケットを送信する．ゲートウェイまで届けられたパケットは，CoA でカプセル化し IN へパケットを送信する．これにより，EN は常に論理サブネットに存在するアドレス HoA を通信相手と認識する．HoA と CoA の関係はゲートウェイしか知らないため，EN は実際のサブネット ID を知ることができない．しかしこの方式には，以下のような課題がある．Mobile IPv6 では経路最適化が定義されている．経路最適化とは，HA を経由した冗長経路にならないように，実際に端末に割り当てられているアドレスを通信相手に通知する機能である．経路最適化を行うと，IN が EN に対して CoA を通知することになり，EN に実際のサブネット ID を知られてしまう．そのため，経路最適化を行うことができない． すなわち，内部端末同士の通信においても，ゲートウェイを経由した通信を行わなければならない．また，HoA のサブネット ID の値は任意であるため，ア

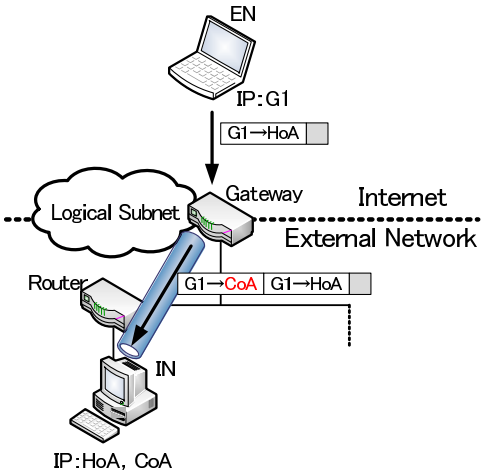


図 2 Mobile IPv6 によるネットワーク構成の隠蔽方式
Fig. 2 network topology concealment by Mobile IPv6

ドレス重複検出が行えないという課題がある．

2.4 ホストルートを用いた方式

ホストルートを用いた方式では，サブネット ID を任意の値にしたアドレスをそのまま端末に割り当て，全ルータに全端末のホストルートを設定する．ホストルートとはルーティングテーブルに端末までのルートを一意に設定するものである．これにより，サブネット ID が任意な値であってもパケットをルーティングすることが可能となる．この方式は，すべての端末のホストルートを各ルータに設定する必要があるため，ルーティングテーブルが膨大になる課題がある．また，Mobile IPv6 を用いた方式と同様にアドレス重複検出が行えない．

3. 提 案 方 式

本稿では，端末に 2 つのアドレスを保持させ，アドレスを使い分けることによってネットワーク内部を隠蔽する方式を提案する．外部端末と通信を行う場合には，ランダムに生成したアドレスを用いて通信を行い，内部端末同士の通信では，内部でのみ有効なアドレスを用いて通信を行う．以下では，外部のアドレスのルーティング方法を 2 つ提案し評価を行う．

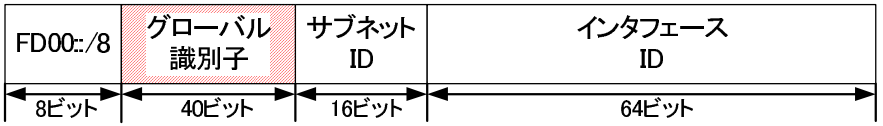


図 3 ユニークローカル IPv6 ユニキャストアドレスの構成
Fig. 3 Unique Local IPv6 Unicast Address

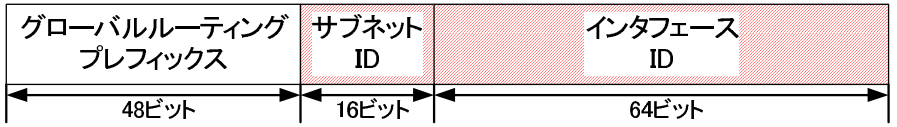


図 4 隠蔽アドレスの構成
Fig. 4 Concealed Address

3.1 アドレス定義

提案方式では以下の 2 つのアドレスを使用する．通信相手がネットワーク内部に存在する場合には，ULA（Unique Local IPv6 Unicast Address）を使用する．ULA の構成を**図 3** に示す．IPv6 では，以前にサイトローカルアドレスと呼ぶ組織内でのみ有効なアドレスが定義されていた[8]．しかし，サイトローカルアドレスはアドレスが重複する可能性があるなどの理由で廃止され，その代わりに ULA が新たに定義された．ULA は組織内のネットワークでのみ使用することを目的としているが，グローバル識別子の 40 ビットをランダムに生成することにより，万が一アドレスがインターネットへ漏洩した場合でも，アドレス重複の可能性を極めて低くしているのが特徴である．ULA はインターネット上での使用は推奨されておらず，提案方式においても組織内部での通信に使用する．

一方，外部端末と通信を行う場合は，新たに隠蔽アドレス（CA:Concealed Address）を導入する．**図 4** に CA の構成を示す．CA はサブネット ID を含めた下位 80 ビットをランダムに生成する．サブネット ID の部分もランダムに生成するため，ネットワーク内部を隠蔽することができる．しかし，このままではネットワーク内をルーティングすることができないため，3.3 に述べる方法によりルーティングを行う．

3.2 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）は，外部通信用に使用する CA の管理に用いられる．CAM サーバの基本的な機能として，端末からの要求により外部通信用アドレス CA を生成し端末に割り当てる．すべての CA は

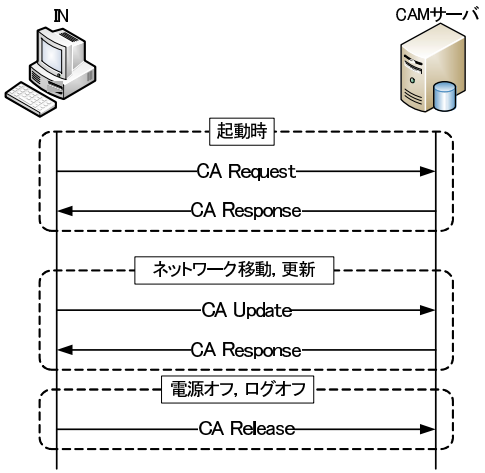


図 5 CA の取得と解放
Fig. 5 Acquisition and Release of CA

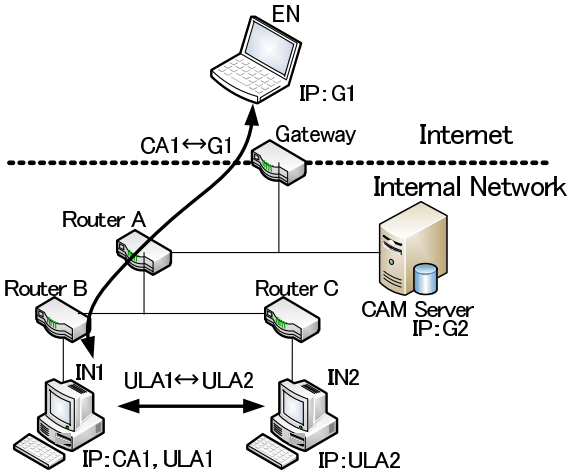


図 6 通信方式
Fig. 6 Communication method

CAM サーバで管理されており，各端末に割り当てている CA を把握しているため，アドレスの重複を防ぐことができる．CA には有効期限を設け，有効期限が過ぎた CA を使用できないようにする．**図 5** に CA の取得と開放について示す．端末の起動時に CA Request, CA Response により CA を取得する．ネットワークを移動したときや，CA の使用期限が近づいてきたときは，端末が CAM サーバに向かって新たな CA を要求する CA Update を送信する．電源オフ時やログオフ時ではアドレスを開放するため，CA Release を CAM サーバへ通知する．

3.3 通 信 方 式

図 6 に通信方式を示す．内部端末の IN1 は外部との通信を行う端末で，ULA1 と CA1 の 2 つのアドレスが割り当てられている．IN2 は内部との通信のみを行う端末で，ULA2 だけが割り当てられている．外部端末 EN には，グローバルアドレス G1 が割り当てられている．IN1 が IN2 と通信を行う場合は，通信相手が内部端末であることを判断し，ULA1 を用いて通信を行う．ULA1 は通常のサブネット ID によるルーティングにより通信が行える．IN1 が EN と通信を行う場合は CA1 を用いて通信を行う．ネットワーク外部から届けられる CA1 宛てのパケットをルーティングするために，以下に示すトンネリング方式とホストルート方式が考えられる．

3.3.1 トンネリング方式

宛先 CA のパケットをルーティングするためにトンネリング技術を用いる．CA 宛のパケットを ULA 宛ての IP ヘッダによりカプセル化する．カプセル化する点では Mobile IPv6 を用いた方式でも同様であるが，内部端末同士で通信を行う時にも HA を経由するため，冗長経路になる．そこで，提案方式では通信相手端末が自ネットワークに存在しているとを判断すると，ULA を送信元アドレスとして通信を行う．**図 7** にトンネリング方式のルーティング方式を示す．ネットワーク構成については図 6 と同様とし，IN はルータ B の配下に存在する．IN1 はプレフィックス情報を，ルータ広告により取得し ULA1 を生成済みであるとする．また，CAM サーバのアドレスを登録しておく．外部との通信が必要であると，IN1 は CA を要求する CA Request を CAM サーバへ送信する．CA Request の送信元アドレスは ULA1 である．これを受け取った CAM サーバは重複しないアドレス CA1 を生成し，CA1 を CA Response により通知する．このとき CAM サーバは ULA1 と CA1 の関係を登録しておく．EN と通信を行う場合，送信元 ULA1，宛先 G1 のパケットを送信元 ULA1，宛先 G2 でカプセル化し CAM サーバへ送信する．CAM サーバは受け取ったパケットのカプセル化を外し EN へ転送する．EN からパケットが到達した場合は，宛先アドレス CA1 から対応する内部端末の ULA1 を検索し，送信元 G2，宛先 ULA1 でカプセル化して IN1

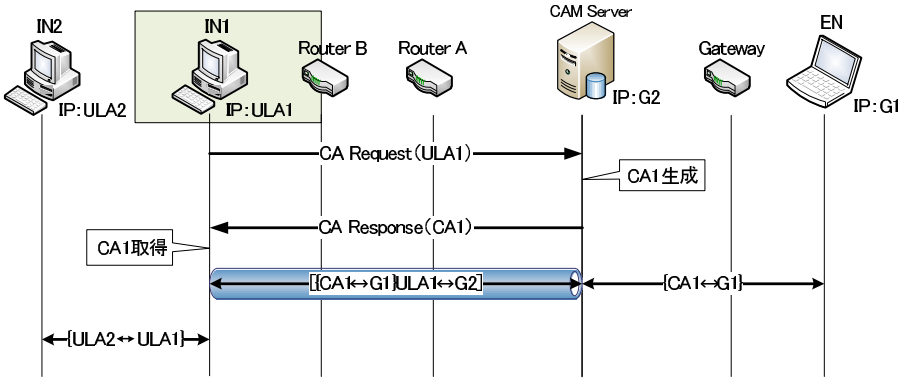


図 7 トンネリング方式のルーティング
Fig. 7 A routing method by a tunnel technology

まで送信する．ルータは通常のルーティングによりパケットを中継するだけでよい．

3.3.2 ホストルート方式

宛先 CA のパケットをルーティングするために，通信経路上のルータに対してホストルートを設定する．ルーティングテーブルが増大することを避けるため，必要なルータにのみホストルートを設定する．**図 8** にホストルート方式のルーティングを示す．外部端末との通信が必要な場合には，トンネリング方式と同様に CAM サーバへ CA Request を送信する．CAM サーバは CA Request を受け取ると，CA1 を生成する．このとき CAM サーバは，要求のあった ULA1 が割り当てられている端末の所属するサブネットから外部ネットワークまでの通信経路上に存在するルータ A とルータ B，ゲートウェイにホストルートを設定する．この方式では，CAM サーバがあらかじめネットワーク構成を把握しておく必要がある．CAM サーバは SNMP（Simple Network Management Protocol）を用い，ルータが所持する MIB（Management Information Base）を参照することにより，ネットワーク構成を把握することができる．ホストルートの設定においては SNMP の Set Request によりルータのルーティングテーブルの変更を指示する．ルータが所持しているルータ情報を Set Request により変更する．これに対しルータは Get Response を返信する．すべてのルータから Get Response が返ってきたら，IN1 へ CA Response として CA1 を通知する．ルータは，宛先が ULA であれば通常のルーティング，宛先が CA であればホストルートによるルーティングを行う．

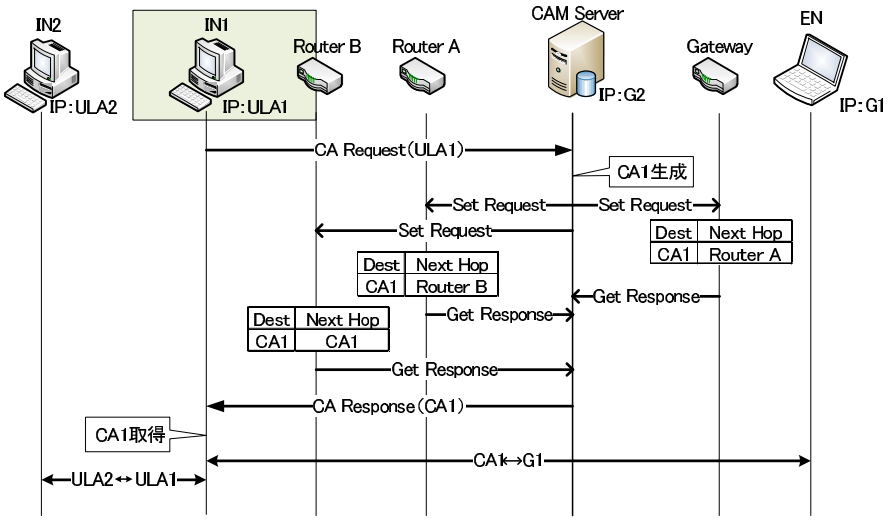


図 8 ホストルート方式のルーティング
Fig. 8 A routing method by a host routes technology

表 1 評価
Table 1 Evaluation

	トンネリング	ホストルート	NAT66	MIPv6
ルータ負荷	○	△	○	○
経路冗長	△	○	○	×
ヘッダオーバヘッド	△	○	○	△
アプリケーション	○	○	×	○
導入コスト（端末）	△	△	○	×
導入コスト（GW）	○	○	△	△
第三装置	△	△	○	○

4. 評　　価

表 1 にネットワーク構成を隠蔽する方式として，提案するトンネリング方式，ホストルート方式および既存方式について比較する．ホストルート方式では，ホストルートを必要なルータのみに設定することによりルータ負荷を回避するが，他の方式に比べると負荷が高い．ルーティングテーブルの増大を更に抑える方法として，CAM サーバを複数設置し，そ

れぞれの CAM サーバで範囲指定された中で CA の生成をすることが考えられる．しかし，ゲートウェイに近いルータほどルーティングテーブルのエントリー数は増加していくのは避けられない．経路冗長およびヘッダオーバヘッドについては，トンネリング技術を用いる方式に発生する．Mobile IPv6 を用いた方式では内部端末同士の通信においても経路冗長が発生する．NAT66 はアドレス変換を行うため，ペイロード内にアドレス情報が含まれているアプリケーションでは個別に対応が必要である．それぞれの導入コストは，トンネリング方式，ホストルート方式，Mobile IPv6 を用いた方式では端末に新たなソフトウェアが必要となり，特に Mobile IPv6 ではカーネルに実装を施す必要があり，導入コストが高い．NAT66 と Mobile IPv6 ではゲートウェイを交換する必要があり，提案方式では 2 方式とも CAM サーバを設置する必要がある．相対的に提案方式は，既存方式の課題を解決しており，有用であると考えられる．今後はトンネリング方式とホストルート方式について実装の検討を行い，実現可能性について評価する必要がある．

5. ま と め

本稿では，IPv6 へ移行したときのネットワーク構成の隠蔽方式として，通信相手により内部通信用アドレス ULA と隠蔽アドレス CA の 2 つのアドレスを使い分ける方式を提案した．CA のルーティング方法として，トンネリング方式とホストルート方式を提案した．今後は実装の検討を進める予定である．

参 考 文 献

1) IPv4 アドレス枯渇対応タスクフォース：. http://www.kokatsu.jp/blog/ipv4/
2) 北村　浩，阿多信吾，村田正幸：IP 通信のセッション多重化を刷新する Unified Multiplex 通信アーキテクチャ，信学技報，IN2006-134, Vol. 106, No. 420, pp. 121–126 (2006).
3) 榊間慧一，阿多信吾，北村　浩：匿名性を有しつつ識別管理可能な IP アドレスを用いた通信システムの構築，信学技報，IN2008-185, Vol.108, No.458, pp.315–320 (2009).
4) Narten, T., Draves, R. and Krishnan, S.: Privacy Extensions for Stateless Address Autoconfiguration in IPv6, RFC 4941, IETF (2007).
5) Wasserman, M. and Baker, F.: IPv6-to-IPv6 Network Address Translation (NAT66), Internet-draft, IETF (2008). draft-mrw-behave-nat66-02.txt
6) de Velde, G.V., Hain, T., Droms, R., Carpenter, B. and Klein, E.: Local Network Protection for IPv6, RFC 4864, IETF (2007).
7) Hinden, R. and Haberman, B.: Unique Local IPv6 Unicast Addresses, RFC 4913, IETF (2005).
8) Huitema, C. and Carpenter, B.: Deprecating Site Local Addresses, RFC 3879, IETF (2004).

IPv6におけるネットワーク構成隠蔽に関する検討

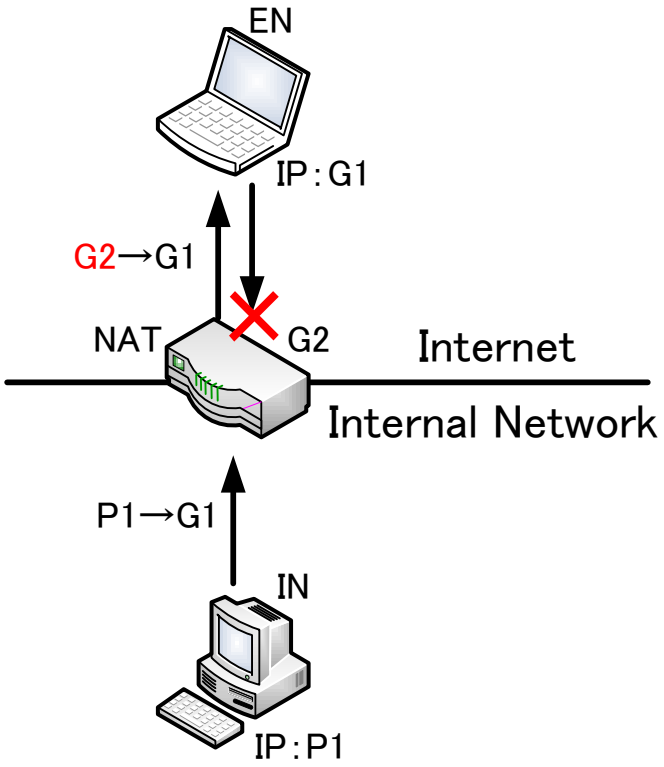
名城大学大学院理工学研究科
久保敷透　鈴木秀和　渡邊晃

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使用
- NATによる影響
  - NAT越え問題
  - アプリケーションの制限
  - 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の内部が隠蔽される

IPv6アドレスへの移行



NAT: Network Address Translation
IN：Internal Node
EN：External Node

研究目的

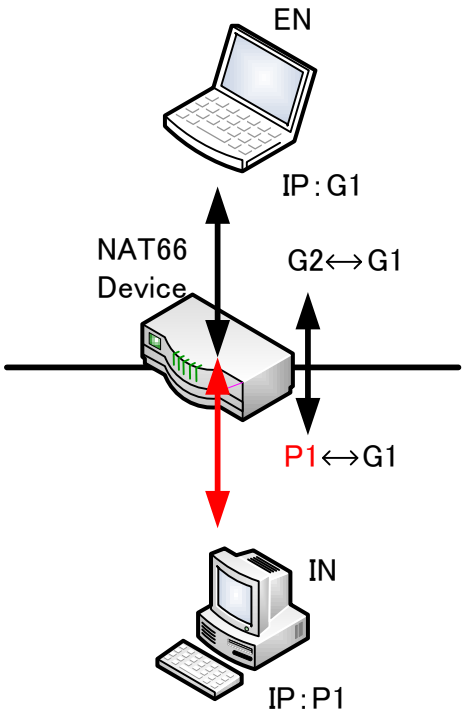
- IPv6アドレスへ移行すると
  - 一意なアドレスが割り当てられる
  - エンドツーエンド通信が可能
  - アドレスが十分確保されるためNATが必要ない
    - **ネットワーク内部が隠蔽される利点がなくなる**

端末の特定やネットワーク構成が予測される可能性がある

ネットワーク構成の隠蔽

既存技術(1)

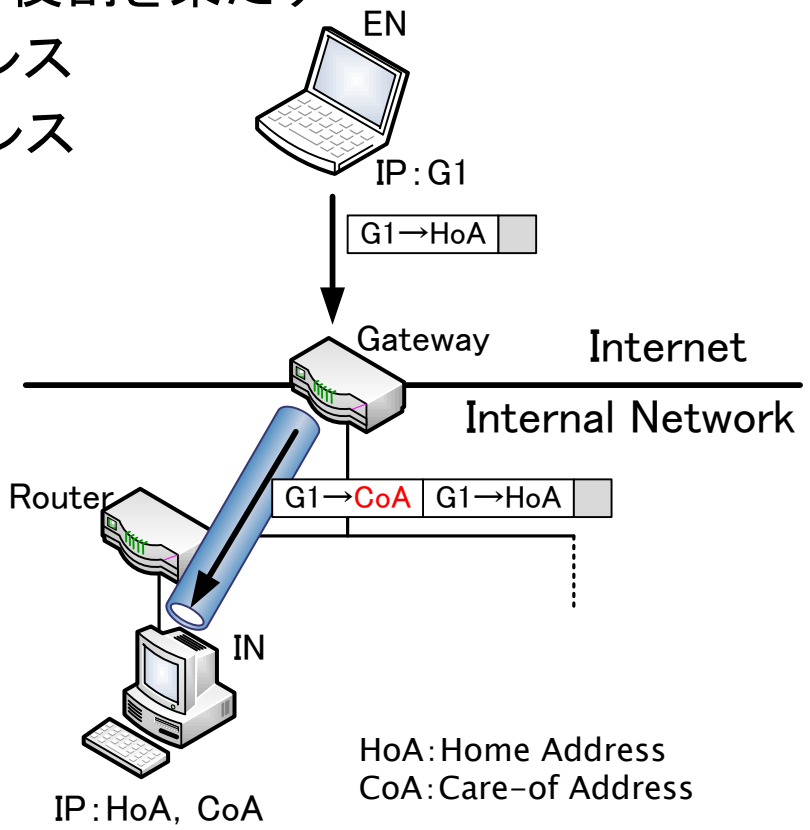
- NAT66(draft-mrw-behave-nat66-02)
  - IPv4におけるNATと同様にアドレス変換する
  - 一対一でアドレスを対応させて変換
  - 双方向で通信を開始できる
  - ペイロード内にアドレスが含まれるアプリケーションは通信ができない



既存技術(2)

- Mobile IPv6を用いたネットワーク構成隠蔽(RFC4864)
  - 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):任意のアドレス
  - 気付けアドレス(CoA):実際のアドレス

- 問題点
  - 内部端末同士の通信に経路の冗長
  - カプセル化によるオーバヘッド



de Velde, G.V., Hain, T., Droms, R., Carpenter, B. and Klein, E.: Local Network Protection for IPv6, RFC 4864, IETF (2007)

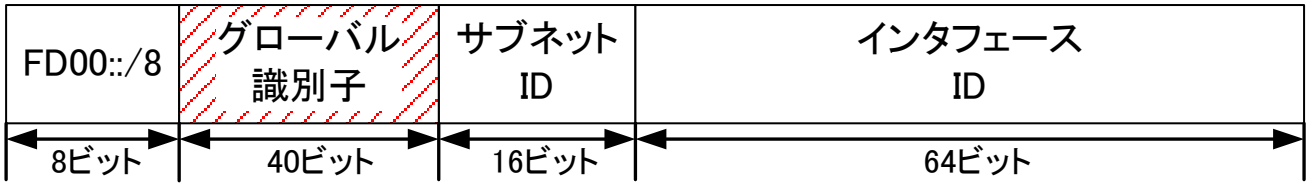
既存技術(3)

- ホストルートを用いたネットワーク構成隠蔽（RFC4864）
  - 任意に設定したアドレスを使用
  - 端末までのルートをルータに一意に設定する

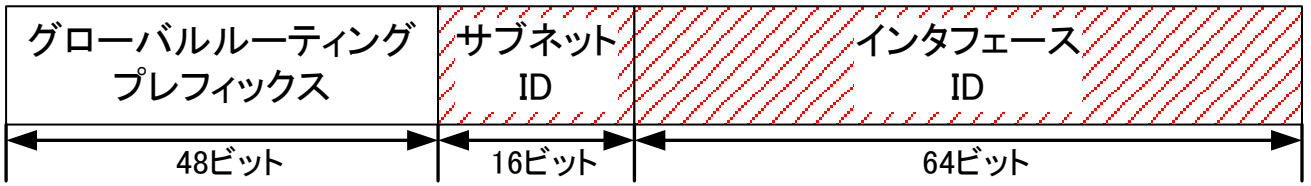
- 問題点
  - 端末ごとに各ルータへホストルートを設定するためルーティングテーブルが膨大になる
  - アドレス重複検出が行えない

提案方式のアドレス定義

- 提案方式では2種類のアドレスを使用する
  - 内部通信用アドレス
    - Unique Local IPv6 Unicast Address（RFC4913）



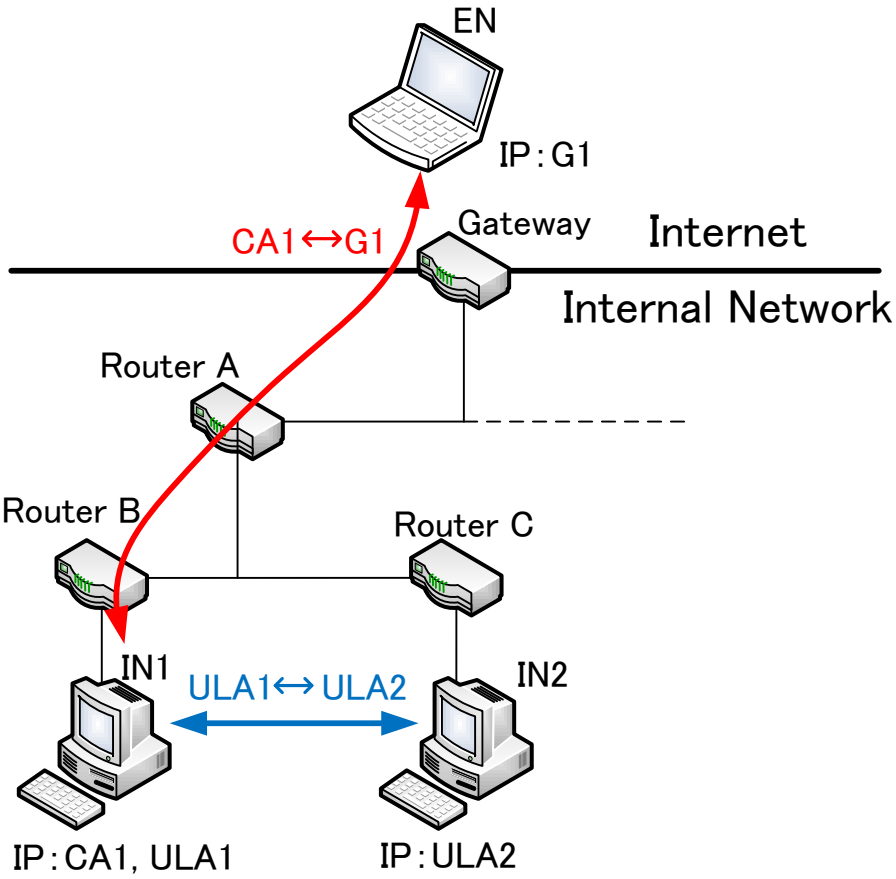
  - 外部通信用アドレス
    - 隠蔽アドレス（Concealed Address）



Hinden, R. and Haberman, B.: Unique Local IPv6 Unicast Addresses, RFC 4913, IETF (2005)

提案方式の概要

- 端末に2つのアドレスを割り当てる
- 2つのアドレスが割り当てられている端末は相手端末の位置により，アドレスを使い分ける



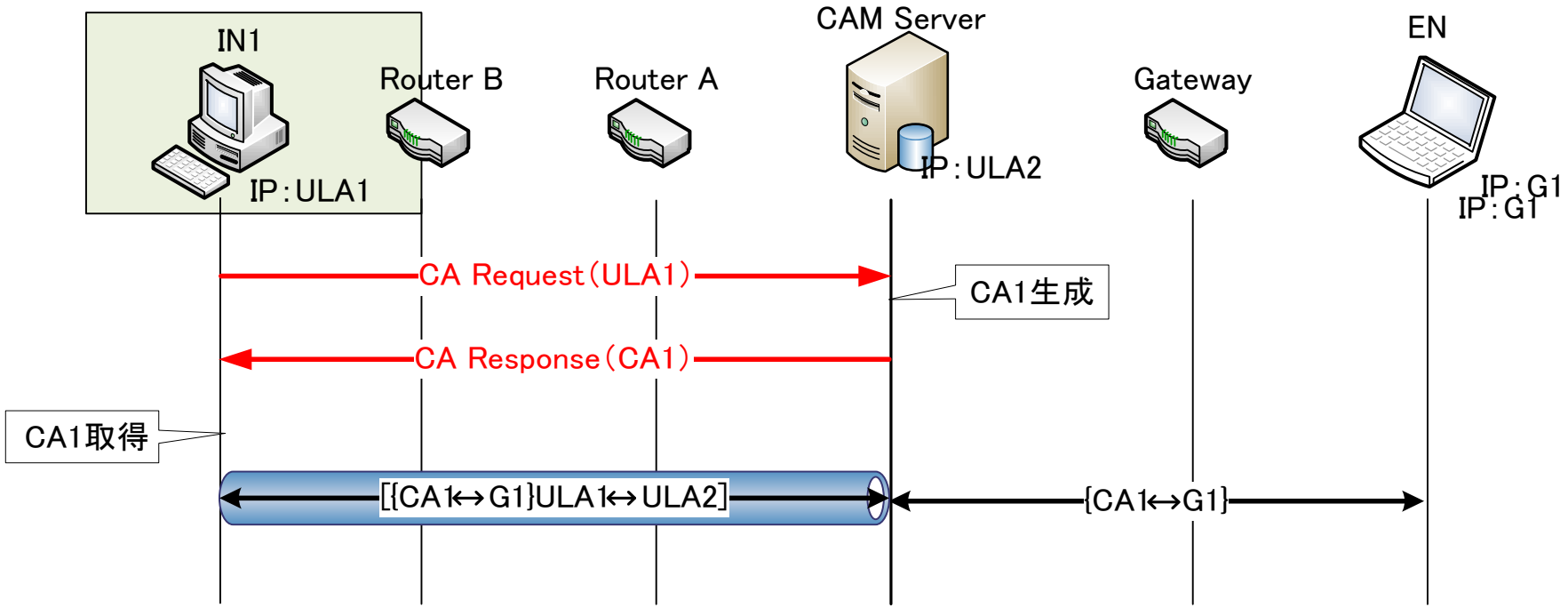
CA：Concealed Address
ULA：Unique Local IPv6 Unicast Address

CAを使用するために

- CAはサブネットIDの値がランダム
  - ネットワーク内でのルーティングができない
    - トンネリング方式
    - ホストルート方式
  - CAのアドレス重複検出
    - サブネットに関係なくアドレスを割り当てるためアドレスの重複検出が行えない
      - 隠蔽アドレス管理サーバ(Concealed Address Management Server)の設置
        - CAの生成，割り当て

トンネリング方式

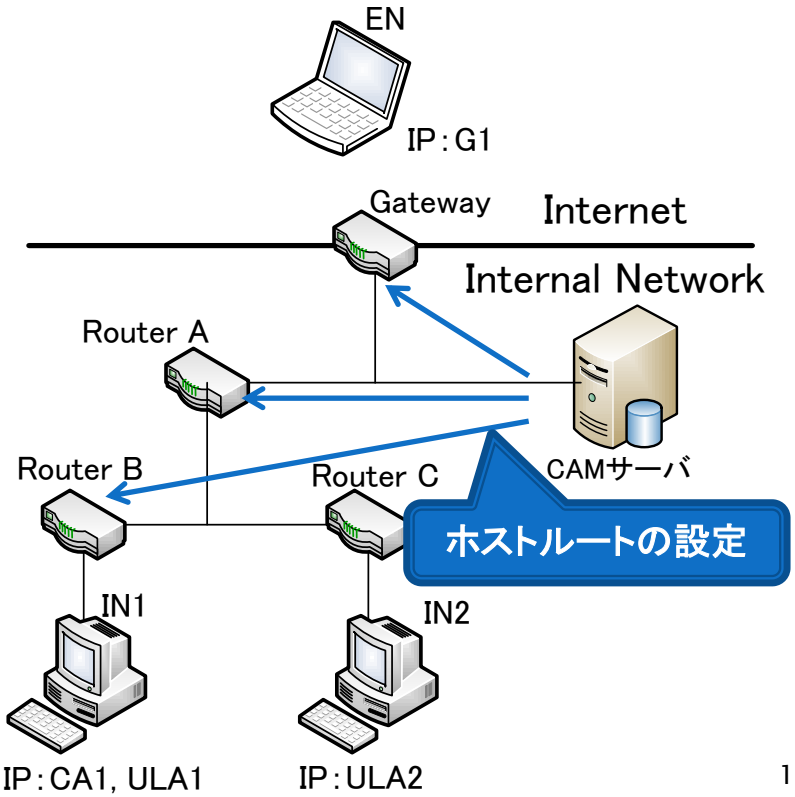
- CAMサーバと端末間でトンネリング



ホストルート方式

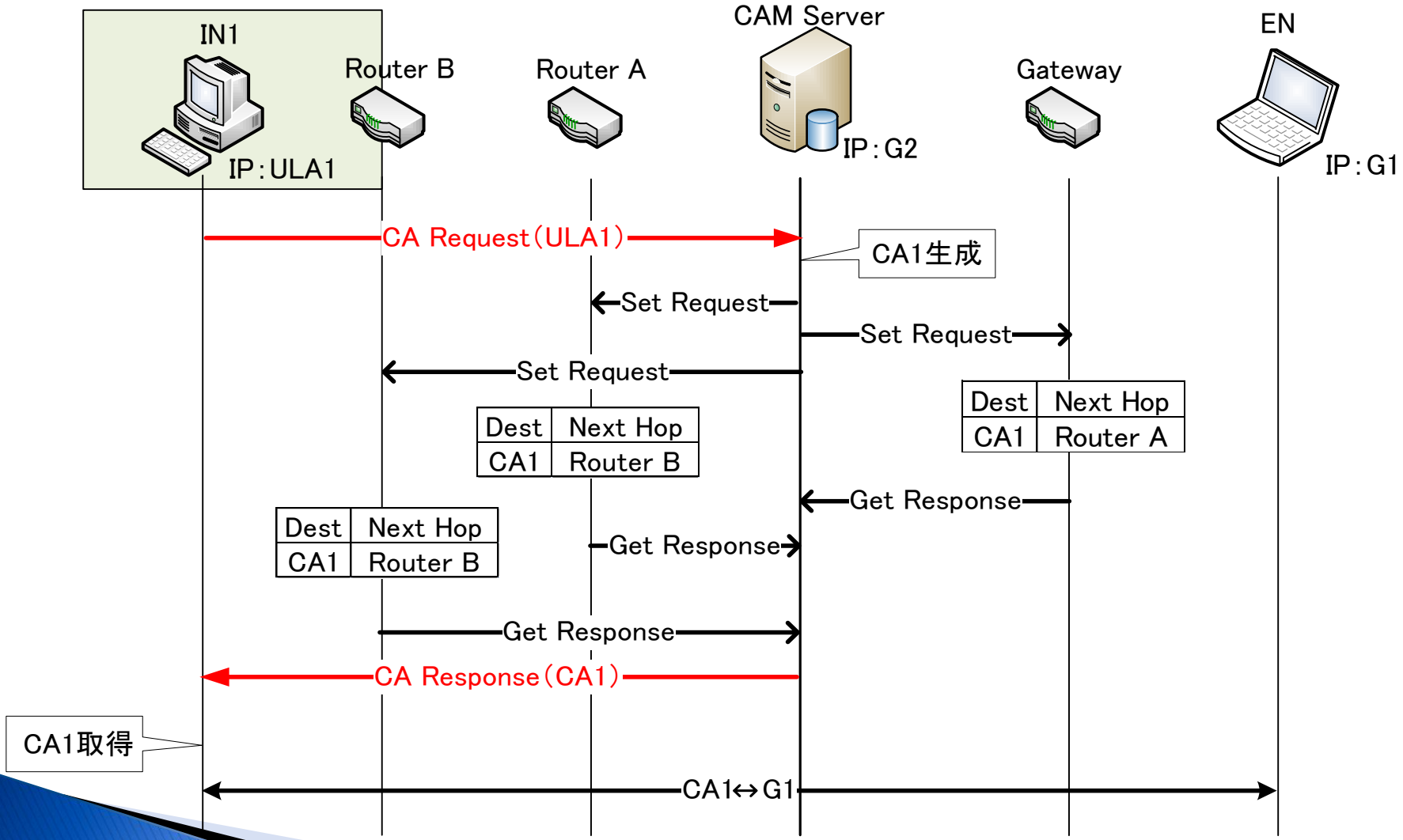
- ホストルート方式
  - ホストルートを必要なルータにのみ設定を行う
    - ゲートウェイ，ルータA，ルータB
  - CAMサーバはあらかじめネットワーク構成を把握しておく必要がある

- ホストルートの設定方法
  - SNMPを用いてルータのMIBを参照し，ネットワーク構成を把握する
  - MIBを変更することでホストルートを設定する



SNMP：Simple Network Management Protocol
MIB：Management Information Base

ホストルート方式


IN1
IP：ULA1
Router B
Router A
CAM Server
IP：G2
Gateway
EN
IP：G1
CA Request（ULA1）
CA1生成
Set Request
Set Request
Set Request
Dest | Next Hop
CA1 | Router A
Dest | Next Hop
CA1 | Router B
Get Response
Dest | Next Hop
CA1 | Router B
Get Response
Get Response
CA Response（CA1）
CA1取得
CA1↔G1

比較評価

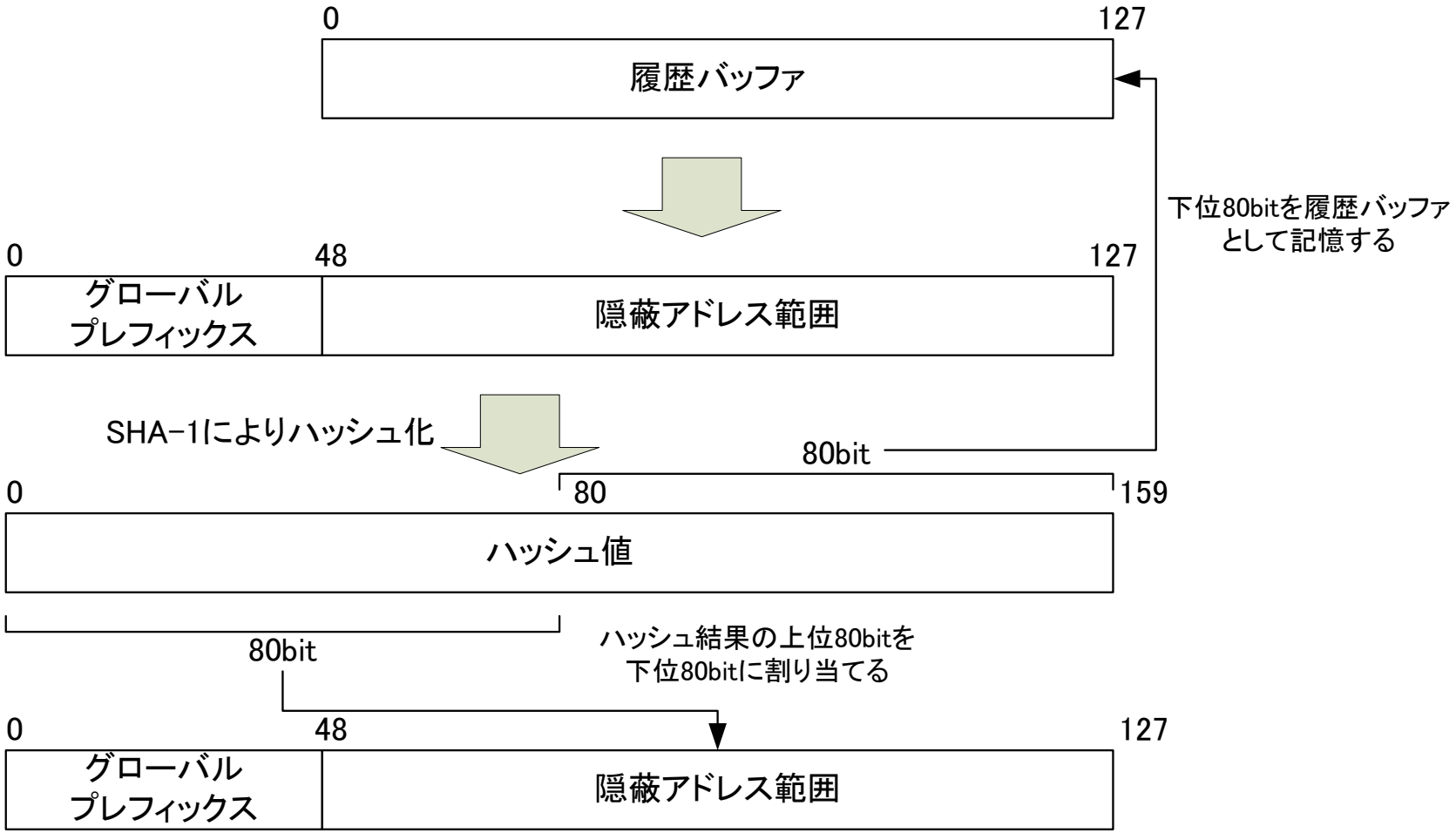
	提案方式		既存技術	
	トンネリング方式	ホストルート方式	NAT66	MIPv6
ルータ負荷	○	△	○	○
経路冗長	△	○	○	×
ヘッダオーバヘッド	△	○	○	△
アプリケーション	○	○	×	○
導入コスト	△	△	△	×

まとめ

- IPv6におけるネットワーク構成隠蔽の検討
  - 隠蔽アドレスCAの導入
    - 隠蔽アドレス管理サーバ(CAMサーバ)によりCAの管理を行う
  - 隠蔽アドレスのルーティング方法
    - トンネリング方式
    - ホストルート方式

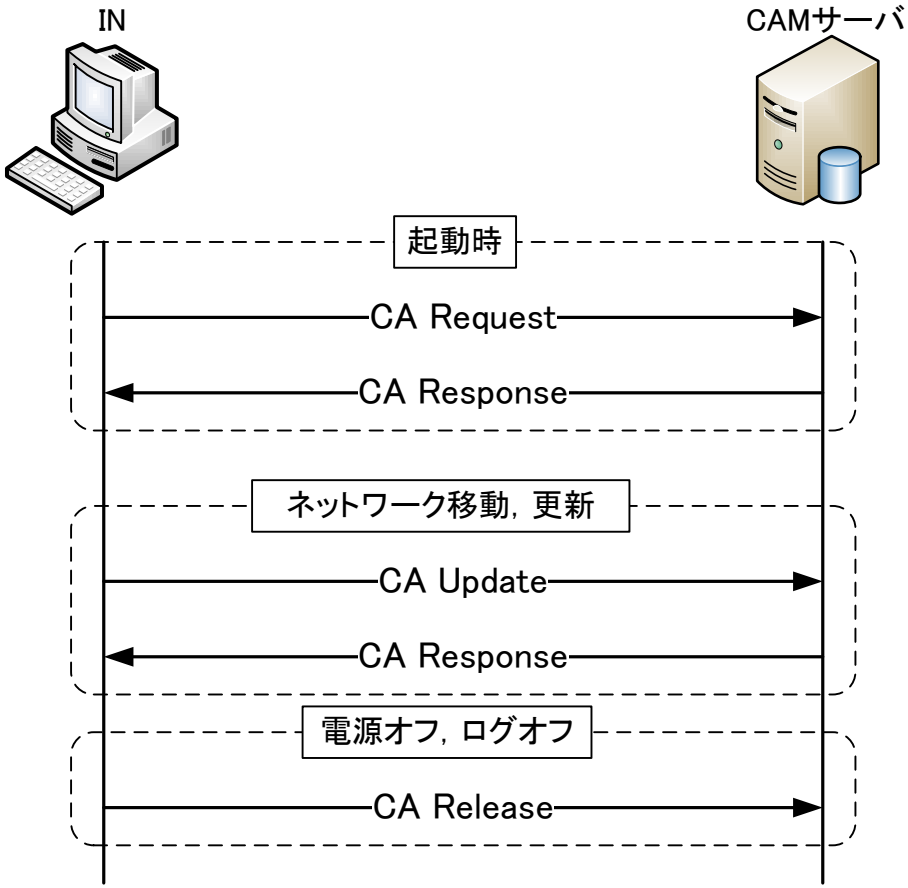
- 今後
  - 両方式の検討
  - 提案方式の実装

CA生成

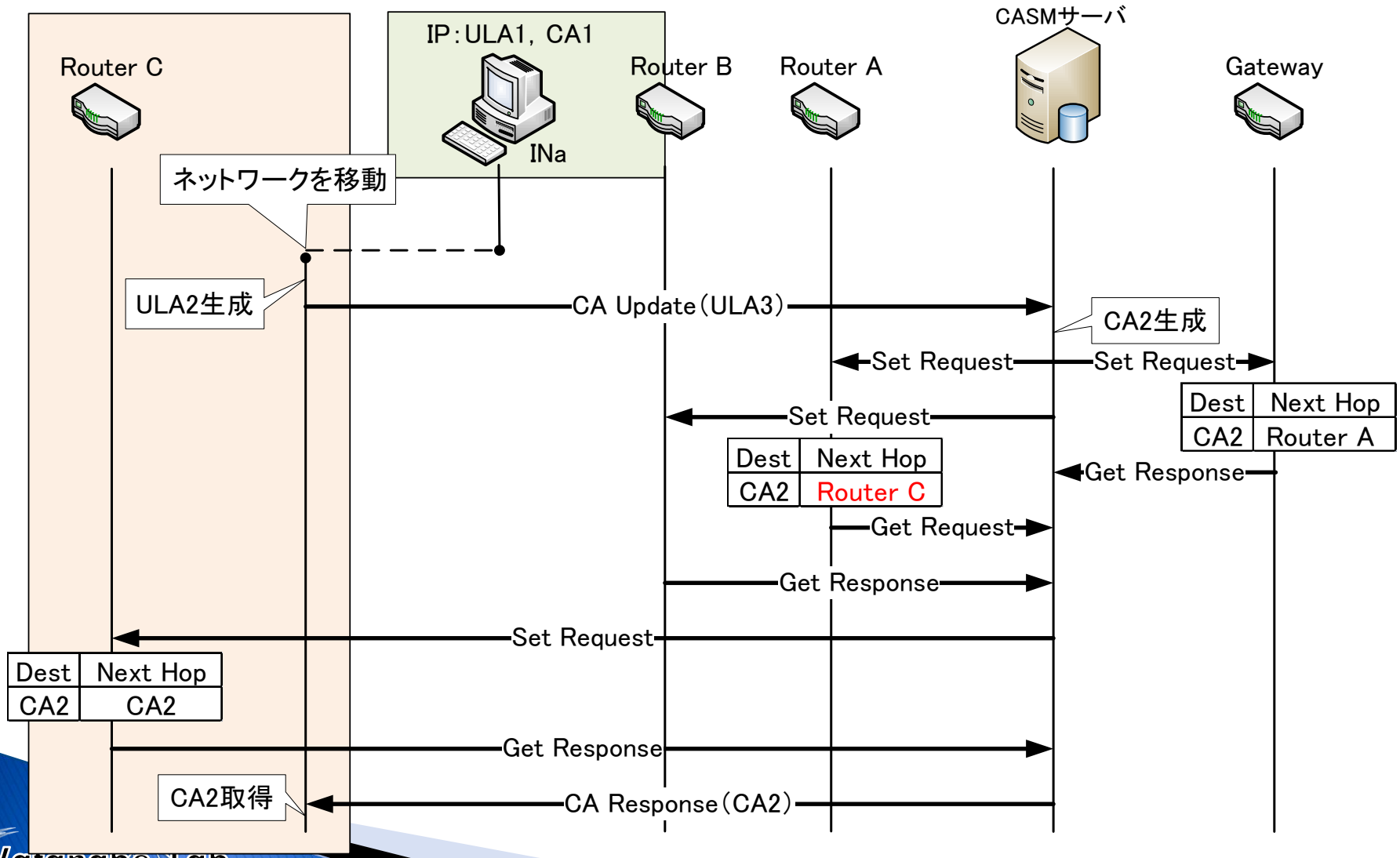

0
127
履歴バッファ
下位80bitを履歴バッファ
として記憶する
0
48
127
グローバル
プレフィックス
隠蔽アドレス範囲
SHA-1によりハッシュ化
80bit
0
80
159
ハッシュ値
80bit
ハッシュ結果の上位80bitを
下位80bitに割り当てる
0
48
127
グローバル
プレフィックス
隠蔽アドレス範囲

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 Management 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(Management Information Base)を参照し、ネットワーク構成を把握する
  - MIBの変更