IPv6 におけるネットワーク構成隠蔽の提案

103430010　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より，グローバル IPv4 アドレスの枯渇が問題になっている．これまで，IPv4 アドレスの延命措置として，プライベートアドレスを定義し，インターネットへの接続時には NAT（Network Address Translation）を使用してきた．このとき，インターネット側からネットワーク内の端末へ通信を開始できない NAT 越え問題も起きている．また，組織内の端末やネットワーク構成が隠蔽されるという副次的な利点が生まれ，これは，ネットワーク管理者にとって，セキュリティ上有用であるという考えがある．しかし，すでに ICANN や JPNIC ではアドレスの在庫が無くなったと報告されており，IPv6 への移行が必須となっている．しかし，IPv6 へ移行することにより，利点であったネットワーク構成を隠蔽することができなくなる．そのため，IPv6 においてネットワーク構成を隠蔽する方式が検討されている．アドレスを NAT のように変換する NPTv6（IPv6-to-IPv6 Network Prefix Translation）[1] や Mobile IPv6 を用いた方式 [2] などが提案されている．しかし，NPTv6 ではアプリケーションが制限される課題や，Mobile IPv6 を用いた方式では，ネットワーク内の端末同士での通信開始時に経路冗長が生じる課題がある．

そこで本論文では，ネットワーク内部を隠蔽する方式として，内部端末に内部通信用と外部通信用の 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．

2. 既存技術

2.1 一時アドレス

一時アドレス（TA:Temporary Address）は，端末の特定を防ぐ目的で定義されたアドレスである．IPv6 アドレスの構成として，長さが 128 ビットあるうちの下位 64 ビットのインタフェース ID を，固有の値である MAC アドレスから生成する，しかし，これではアドレスが一意に生成され，端末が特定されやすくなる．そこで端末のプライバシーの観点から TA が定義された．TA 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，端末を特定されにくくする．しかし，サブネット ID はそのままの値であるため，アドレスからネットワーク構成が予測される可能性がある．

2.2 NPTv6

NPTv6 は，IPv4 の NAT のように，インターネットとネットワークの境界でアドレスを変換する方式である．IPv6 環境では元々NAT は必要ないが，組織内のアドレス空間をインターネットから切り離すことにより，アドレス管理が容易になるとして考えられた．このとき，この方式の第一の目的ではないが，IPv4 における NAT のように，副次的な利点としてネットワーク構成を隠蔽することができる．NPTv6 は，IPv4 の NAT と異なり，アドレスを一対一に対応させ変換するため，NAT 越え問題は生じない．しかしこの方式では，ペイロード内にアドレス情報を含む FTP や SIP などのアプリケーションでは通信をすることが出来ず，IPv6 へ移行したときの利点が損なわれてしまう．

2.3 Mobile IPv6 を用いた方式

この方式では，移動透過性の技術である Mobile IPv6 を利用し，ネットワーク構成を隠蔽する．Mobile IPv6 は，通信中に移動したときに，通信相手に対して移動後のアドレスを隠蔽して，移動後でも通信を継続させる方式である．移動後の通信には，中継サーバであるホームエージェント（HA:Home Agent）を介して通信を行う．これにより，通信相手には移動前のアドレスで通信をしていると思わせ，通信を継続させている．この方式を応用し，ネットワーク内の端末は移動前のアドレスとして，サブネット ID を任意に設定したアドレスを用いることによって，ネットワーク構成を隠蔽する．

しかし，この方式では以下のような課題がある．Mobile IPv6 には経路最適化という機能があり，この機能が有効であると移動後のアドレスを通信相手に通知することになり，実際のネットワーク構成が知られてしまう．そのため，経路最適化機能は無効にしなければならない．この機能を無効にしているときは，常に HA を経由した通信になるため，内部端末同士でも HA と経由してしまうため，経路冗長となる．内部端末と直接通信を行いたいときに，経路最適化パケットをゲートウェイでフィルタリングしたとしても，通信開始時に HA を経由してしまうことは避けられない．

3. 提案方式

3.1 システム構成

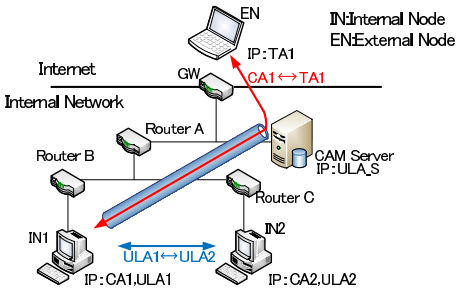


図 1: 提案方式のシステム構成

提案方式では，内部端末に 2 つのアドレスを保持させ，通信相手端末の位置に応じてアドレスを使い分けることにより，ネットワーク構成を隠蔽する．提案方式のシステム構成を図 1 に示す．ネットワーク内には IN1 と IN2 が存在し，インターネット上には EN があるものとする．内部端末には新たに定義する外部通信用アドレス CA（Concealed Address）と内部通信用アドレス ULA（Unique Local IPv6 Unicast Address）の 2 つのアドレスが割り当てられる．外部端末 EN との通信時には，ランダムに生成したアドレスを用いて通信し，内部端末との通信には，ローカルでのみ有効なアドレスを用いて通信する．

また，アドレスの管理に隠蔽アドレス管理サーバ（Concealed Address Management Server）をゲートウェイ直下に設置する．

3.2 アドレスの定義

提案方式で使用するアドレスについて以下に述べる．通信相手がネットワーク内部に存在する場合は，ネットワーク内のみで使用するために定義された ULA（Unique Local IPv6 Unicast Address）を使用する．

通信相手がインターネット上の端末の場合は，新たに定義した CA（Concealed Address）を用いる．CA のアドレス構成を図 2 に示す．CA はサブネット ID を含めた下位 80 ビットを独自に生成し，グローバルルーティングプレフィックスと組み合わせて構成されている．80 ビットのうち上位 4 ビットを CA 判定ビットとして，CA であると判断する領域とする．それ以下の 76 ビットはランダム生成した値を用いる．これにより，ネットワーク構成を隠蔽することができる．

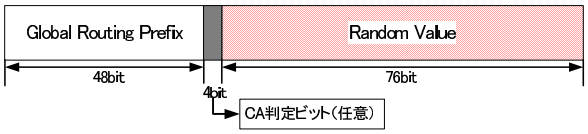


図 2: 隠蔽アドレスの構成

3.3 隠蔽アドレス管理サーバ

隠蔽アドレス管理サーバ（以下 CAM Server）の主な機能として，CA の生成，再配布，および内部端末が外部端末との通信に必要となるトンネルを構築する役割を担う．図 3 に CA の取得動作を示す．IN は起動時に，ルータ広告により ULA を生成し，この ULA を用いて CAM Server に CA を要求する．これに対し，CAM Server は CA を生成し，IN へ通知する．このとき CAM Server は CA と ULA の関係を登録する．そして，CA を用いた通信を可能とするために，IN と CAM Server 間で ULA によるトンネル経路を構築する．

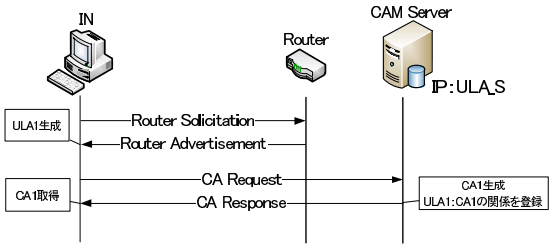


図 3: CA の取得動作

3.4 通信動作

図 4 に提案方式の通信動作を示す．すでに IN1 は CAM Server から CA1 を取得しているものとする．IN1 は EN と通信する場合，通信相手がインターネット上に存在すると判断すると，送信元アドレスを CA1 としたパケットを生成する．上記パケットのネットワーク内でのルーティングを可能とするため，送信元アドレス ULA1，宛先アドレス ULA_S でカプセル化し，CAM Server との間でトンネリング通信を行う．CAM Server には，CA 生成時に CA1 と ULA1 の関係が登録されているため，これを用いてパケットをカプセル化，デカプセル化する．IN1 の通信相手が IN2 であった場合，送信元アドレスを ULA1 に設定し，カプセル化を行ず通常の通信を行う．

以上により，提案方式では CA を用いることによりインターネット上の端末からネットワーク構成を隠蔽することができる．また，エンドエンドのアドレスを使用しているため，アプリケーションの制限も生じない．

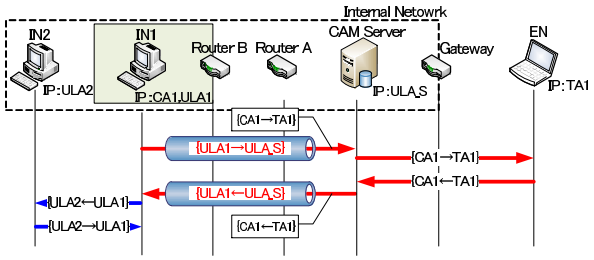


図 4: 通信動作

4. 実装設計

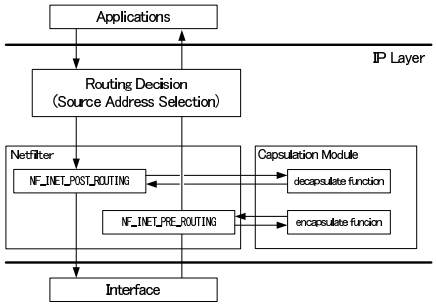


図 5: Linux における実装設計

Linux における提案方式の実装設計を図 5 に示す．提案方式のパケットのカプセル化はカーネルモジュールにより実現する．パケットのカプセル化をカーネル内で実現することにより，カプセル化のオーバヘッドを抑える．送信時，ルーティング処理が行われた送信パケットは Netfilter の NF_INET_POST_ROUTING でフックされ，カプセル化処理を行う Capsulation Module へ渡される．その後，カプセル化パケットは通常のルーティング処理へ戻される．送信元アドレスが CA でない場合は，カプセル化処理は行わない．受信時は，Netfilter の NF_INET_PRE_ROUTING で受信パケットデータをフックし，カプセル化されている受信パケットであるかどうかを判断する．カプセル化されているパケットであった場合，デカプセル化処理を行い Netfilter へ差し戻す．以上により，パケット毎に Capsulation Module で送信元アドレスをチェックしカプセル化，デカプセル化の処理をカーネルモジュールで行う．

5. まとめ

本論文では，IPv6 におけるネットワーク構成隠蔽について，既存技術の問題を取り上げ，これらの課題を解決するために，通信相手に応じて CA と ULA を使い分ける方式を提案した．今後は Linux への実装を完了させ，評価を行う予定である．

参考文献

[1] Wasserman, M. and Baker, F.: IPv6-to-IPv6 Network Prefix Translation, RFC 6296, IETF (2011).

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

IPv6における
ネットワーク構成隠蔽の提案

名城大学大学院
理工学研究科　情報工学専攻
渡邊研究室
103430010　久保敷　透

Watanabe Lab.

研究背景

- グローバルIPv4アドレスの枯渇問題
  - これまでの解決策
    - プライベートアドレスの導入
      - 一つのグローバルアドレスを複数のプライベートアドレスで共有する
      - グローバルアドレスとプライベートアドレスの変換にNATを使用

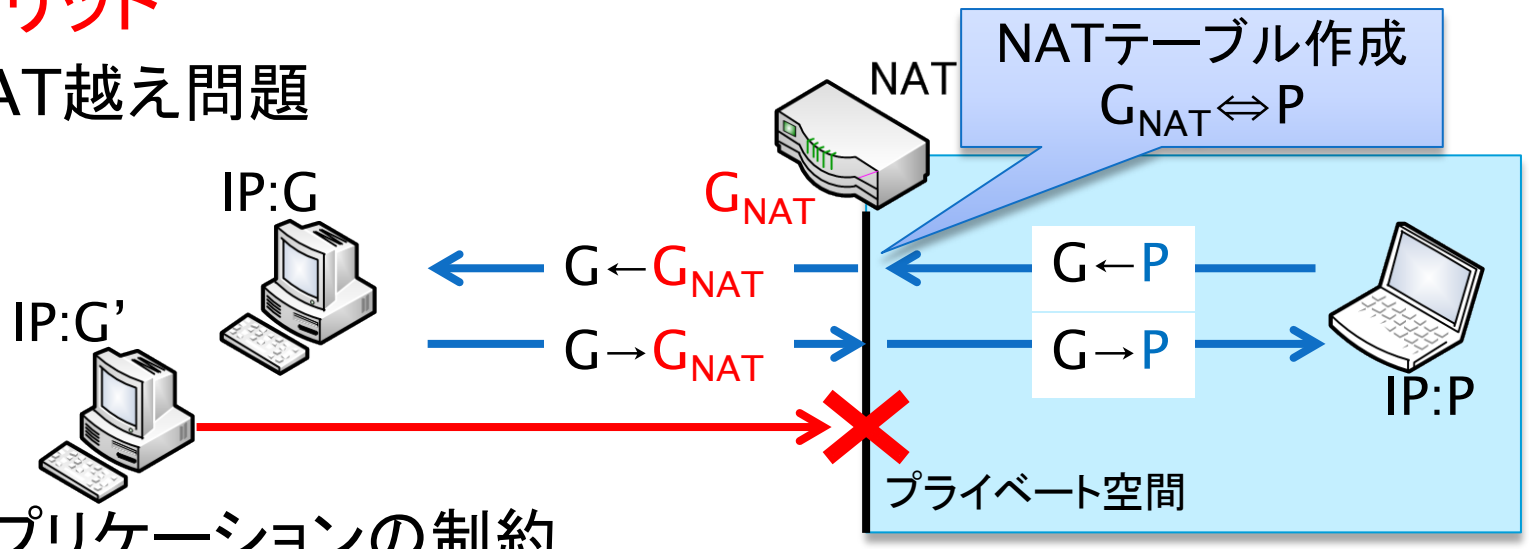
- アドレスの枯渇問題は深刻
- 根本的な解決策として

IPv6アドレスへの移行が必須

NAT:Network Address Translation

プライベートアドレス導入による影響

- デメリット
  - NAT越え問題

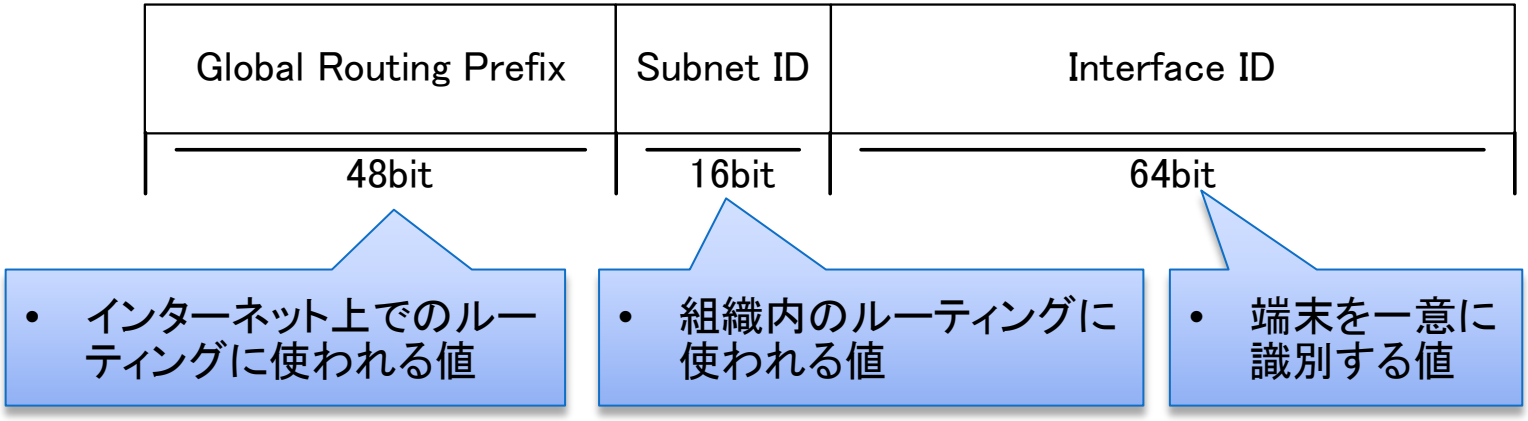


  - アプリケーションの制約
    - メッセージ内にアドレス情報が含まれるアプリケーションが制約される
- メリット
  - 副次的にNAT配下のネットワークが隠蔽される

このメリットに着目

IPv6アドレスの構造

- ステートレスアドレス自動生成
  - IPv6アドレスの特徴の一つ



- IPv6アドレスは端末毎に一意に決まるため，端末やネットワーク構成が特定されやすい

目的

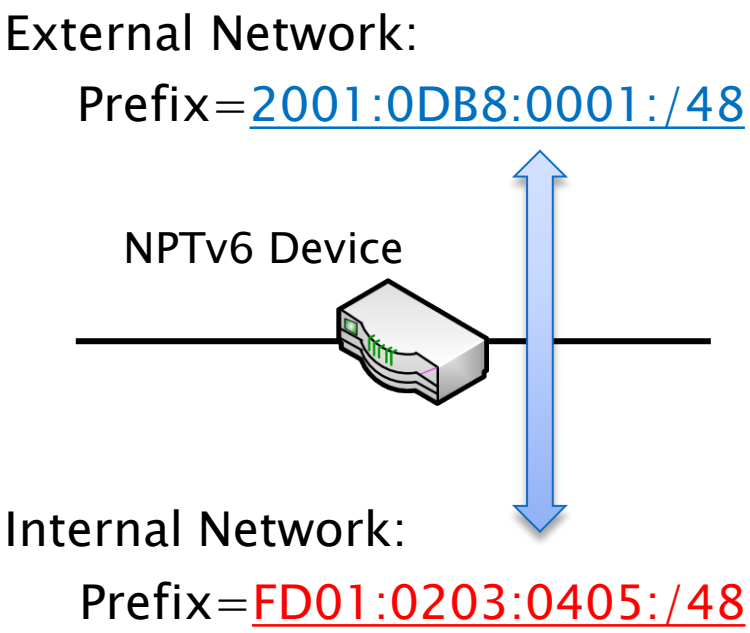
- IPv6移行への問題点
  - IPv4アドレスとの互換性がない
  - ネットワーク構成までは隠蔽できない
    - ネットワーク管理者はできるだけ情報を公開したくない．これがIPv6へ移行する際の不安要素の一つ

目的

IPv6においてネットワーク構成を隠蔽する検討

NPTv6 (IPv6-to-IPv6 Network Prefix Translation)

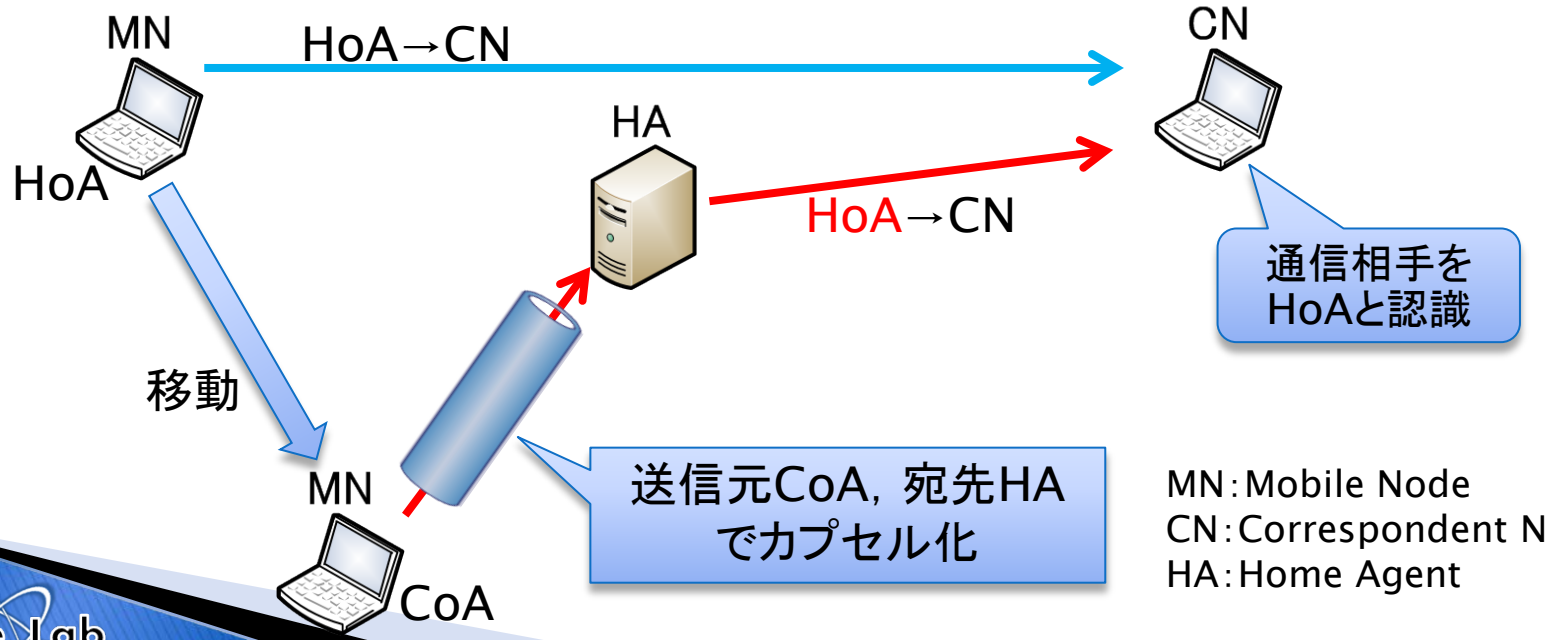
- IPv6アドレス変換機能
- アドレスを一対一に対応させて変換するため，NAT越え問題は生じない
- 問題点
  - アプリケーションの制約
  - エンドエンド通信の弊害



Wasserman, M. and Baker, F.: IPv6-to-IPv6 Network Prefix Translation, RFC 6296, IETF (2011).

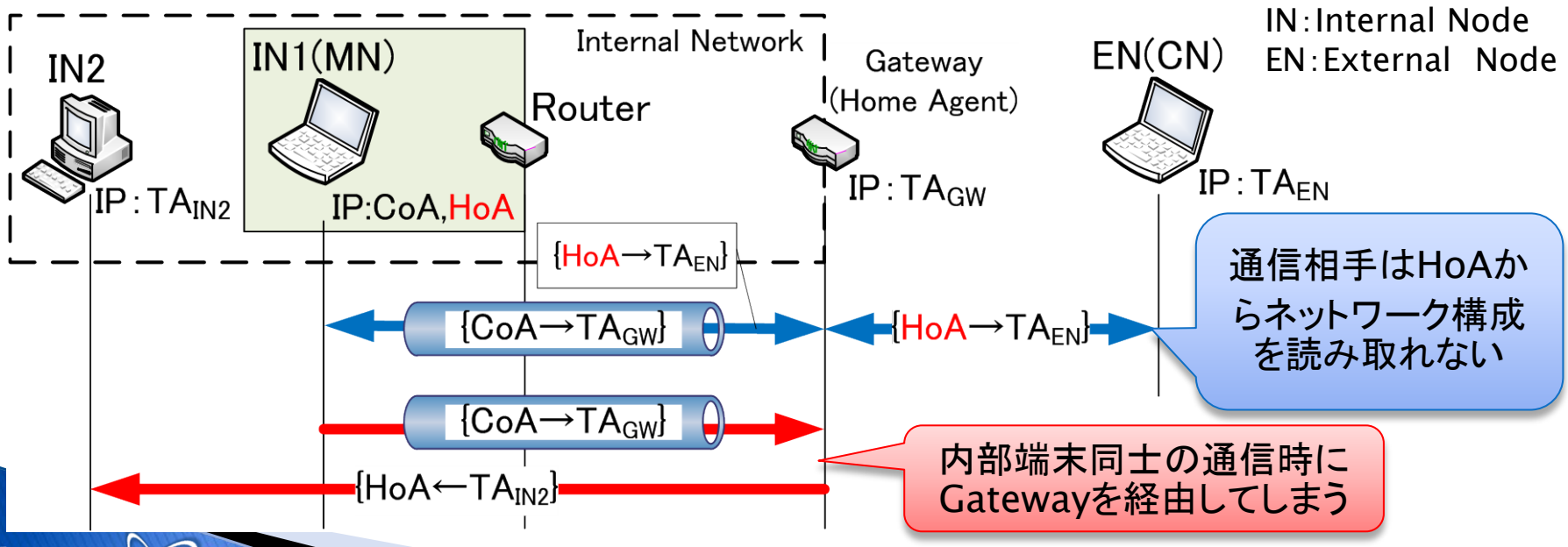
Mobile IPv6を用いた方式(1/2)

- Mobile IPv6は移動通信の技術
  - 通信相手には移動前のアドレスで通信し続ける
    - 移動前アドレス:ホームアドレス(HoA:Home Address)
    - 移動後アドレス:気付けアドレス(CoA:Care of Address)
- 移動後はHome Agentを経由



Mobile IPv6を用いた方式(2/2)

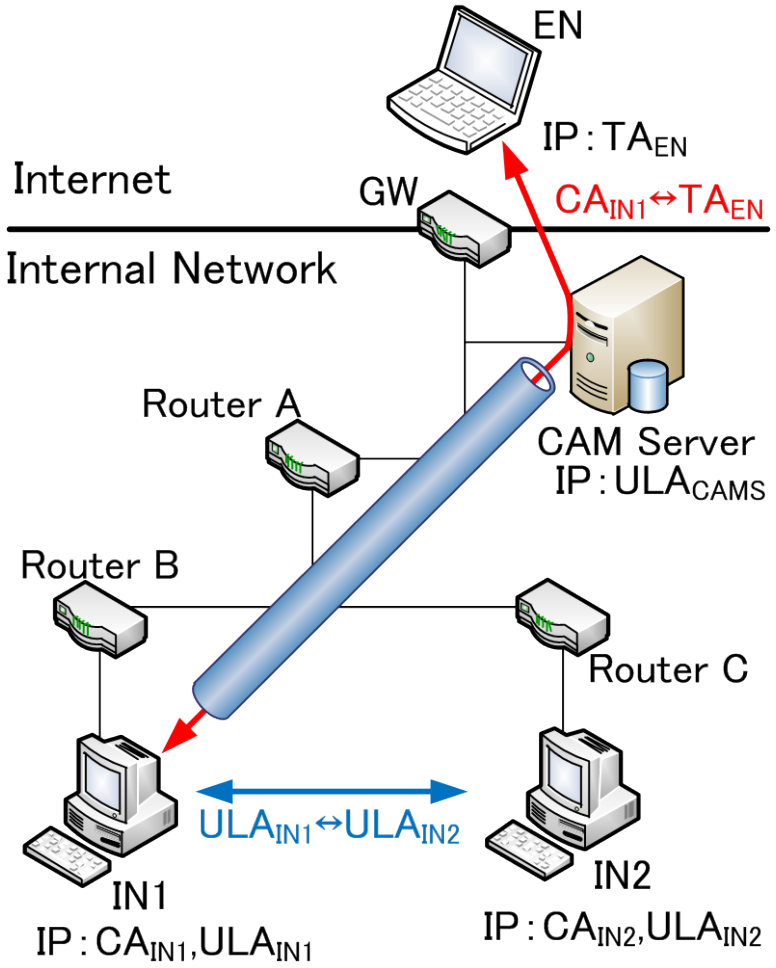
- ネットワーク構成を隠蔽するために
  - HoAに任意に設定したアドレスを割り当てる
- 問題点
  - 内部端末同士で経路冗長が生じる
  - 不要な機能が多い



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

提案方式

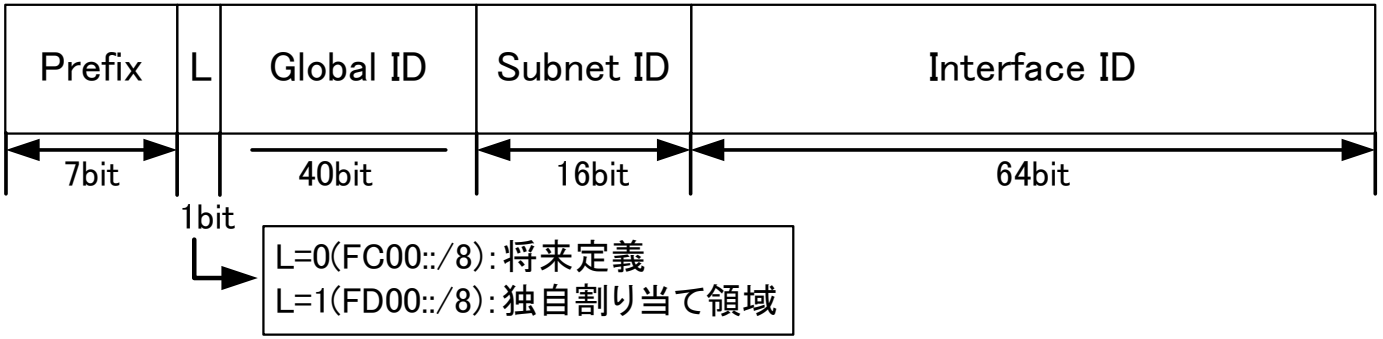
- 2つのアドレスを持たせ，通信相手によりアドレスを使い分ける
  - 内部端末：ULA
  - 外部端末：隠蔽アドレス
    （CA：Concealed Address）
- アドレスの管理
  - 隠蔽アドレス管理サーバ（Concealed Address Management Server：以下CAM　Server）の設置



IN:Internal Node
EN:External Node

Unique Local Unicast IPv6 Address（INとの通信に使用）

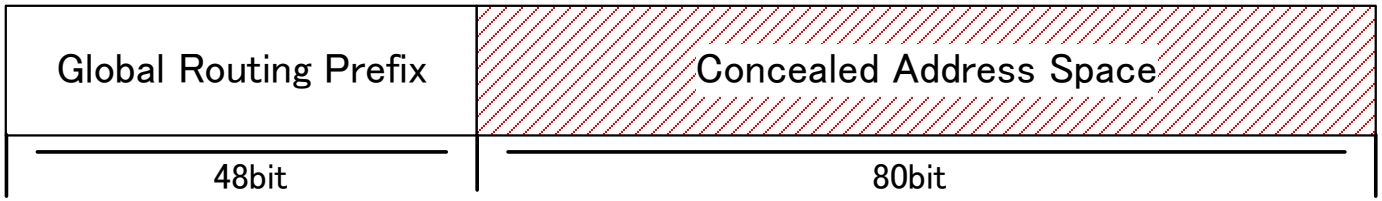
- Unique Local Unicast IPv6 Address（RFC4913）
  - IPv6におけるプライベートアドレスのようなもの
    - ネットワーク内での通信に使用



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

Concealed Address （ENとの通信に使用）

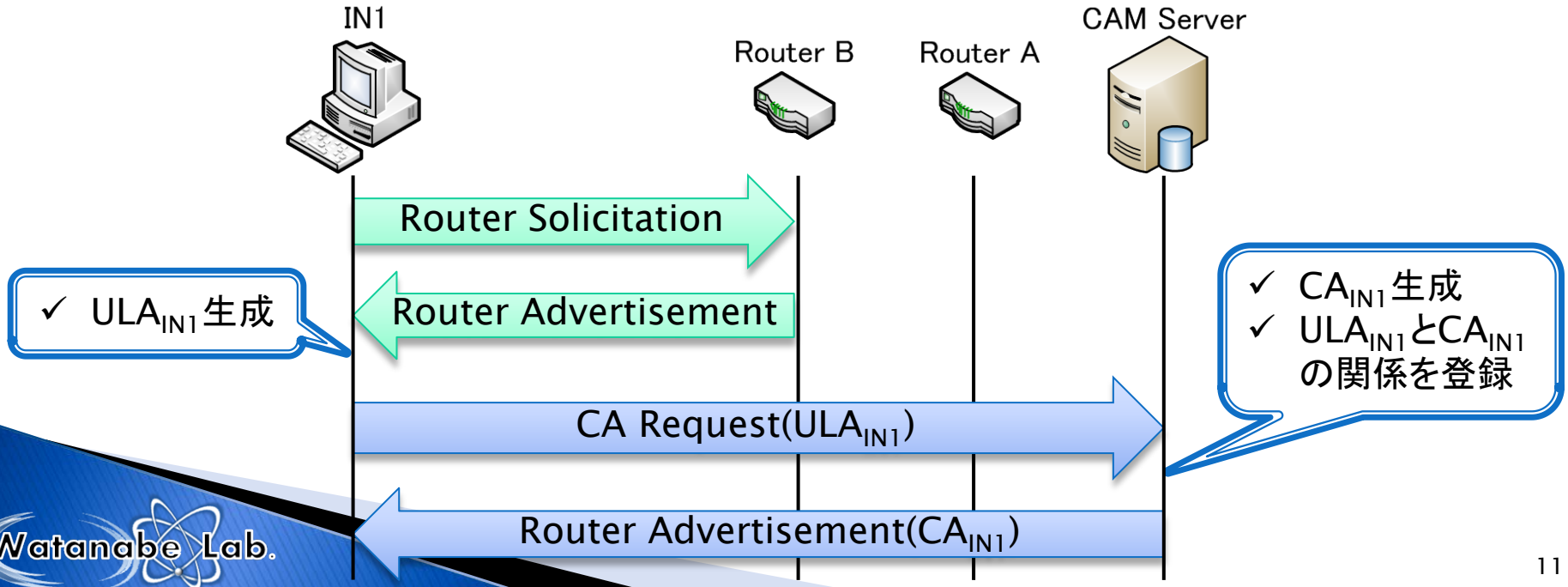
- 隠蔽アドレス（CA:Concealed Address）
  - 下位80ビットをCA用に設定することによりサブネットまでを隠蔽する



- サブネットIDの値を変更しているため、ネットワーク内でルーティングできない
  - ULAでカプセル化することでルーティングを可能にする

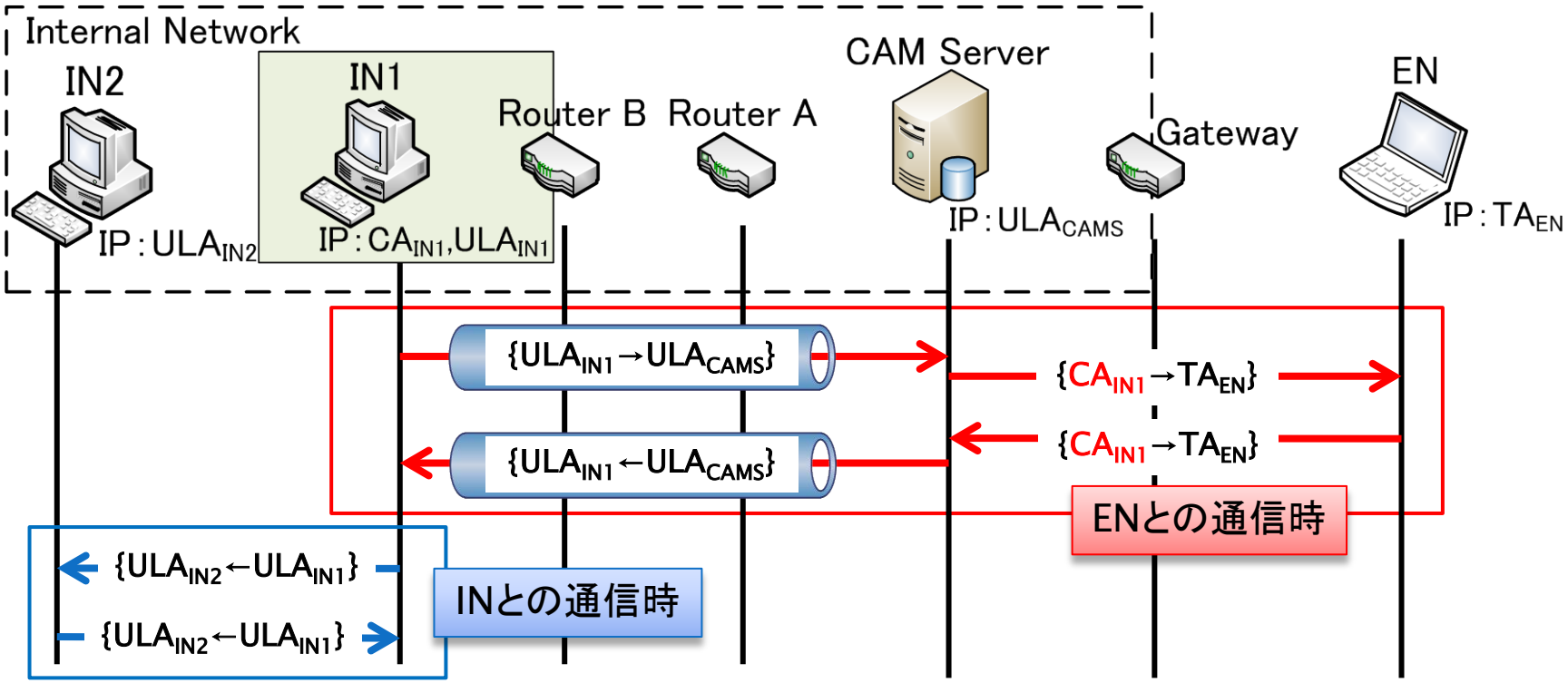
CAM Sever

- CAの生成、管理機能
  - 端末からの要求に対するCAの生成、配布
- ULAとCAの関係を登録
  - CAのルーティングを可能とするための端末とサーバ間でトンネル経路を構築する



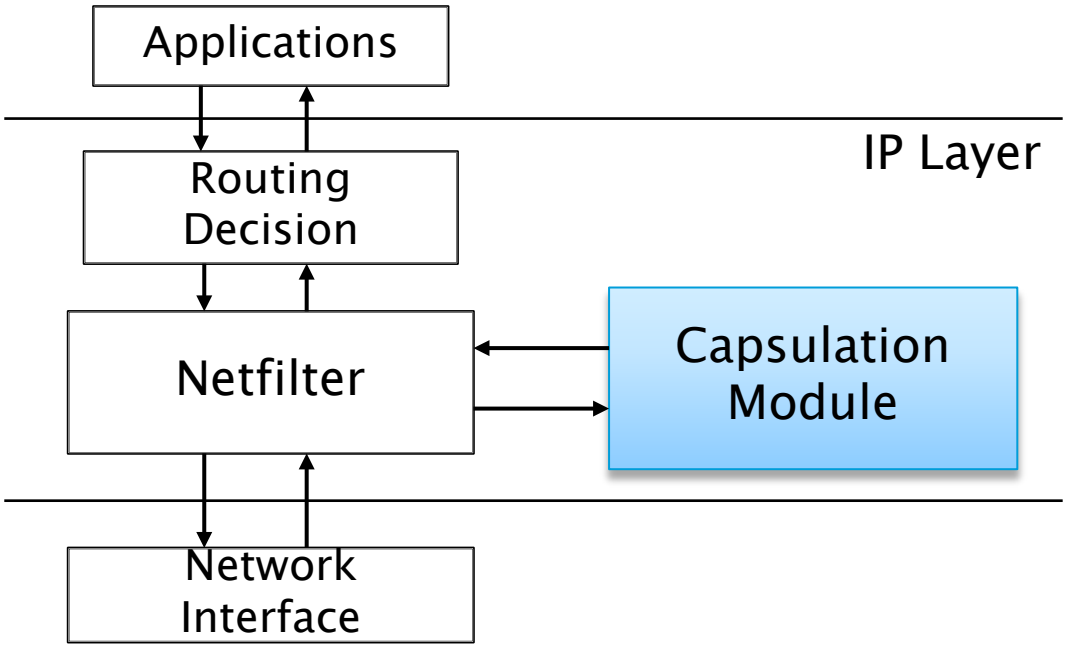
通信方法

- ENとの通信時
  - 通信パケットの送信元アドレスにCA1を設定し，IN1とCAM Serverとの間でULAによるトンネル通信を行う
- INとの通信時
  - ULAで通常の通信を行う



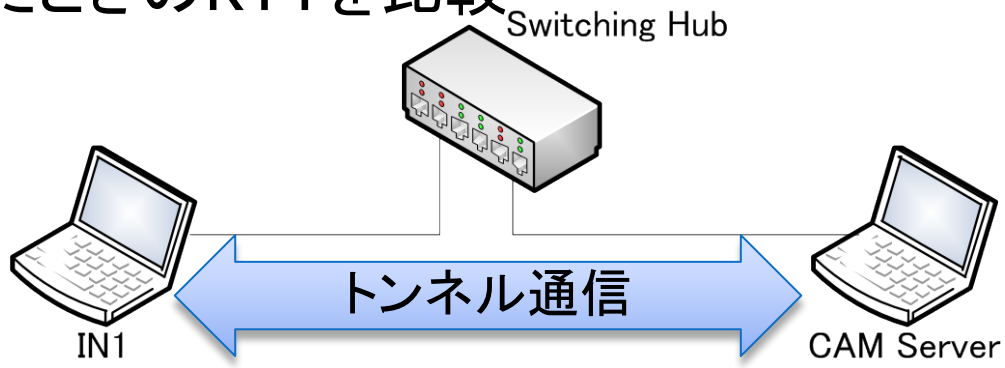
実装

- 提案方式をLinuxに実装
  - パケットのカプセル化処理するカーネルモジュールを実装
  - LinuxのNetfilter機能によりパケットをフックしカプセル化する



性能評価

- カプセル化処理にかかるオーバヘッドの測定
  - IN1とCAM Server間でトンネル通信をさせる
  - IN1とCAM Serverとの間でping6を送信し，モジュールを導入したときのRTTを比較



	IN1	CAM Server
OS	Linux(Ubuntu10.04)	
Kernel version	linux-2.6.32-21-generic	linux-2.6.32-28-generic
CPU	Intel Core 2 Duo 2.40Ghz	
Memory	2.00GB	

結果

- 100回送信したRTTの平均値を測定

	ping6（RTT）
通常時	0.570ms
提案方式	0.569ms

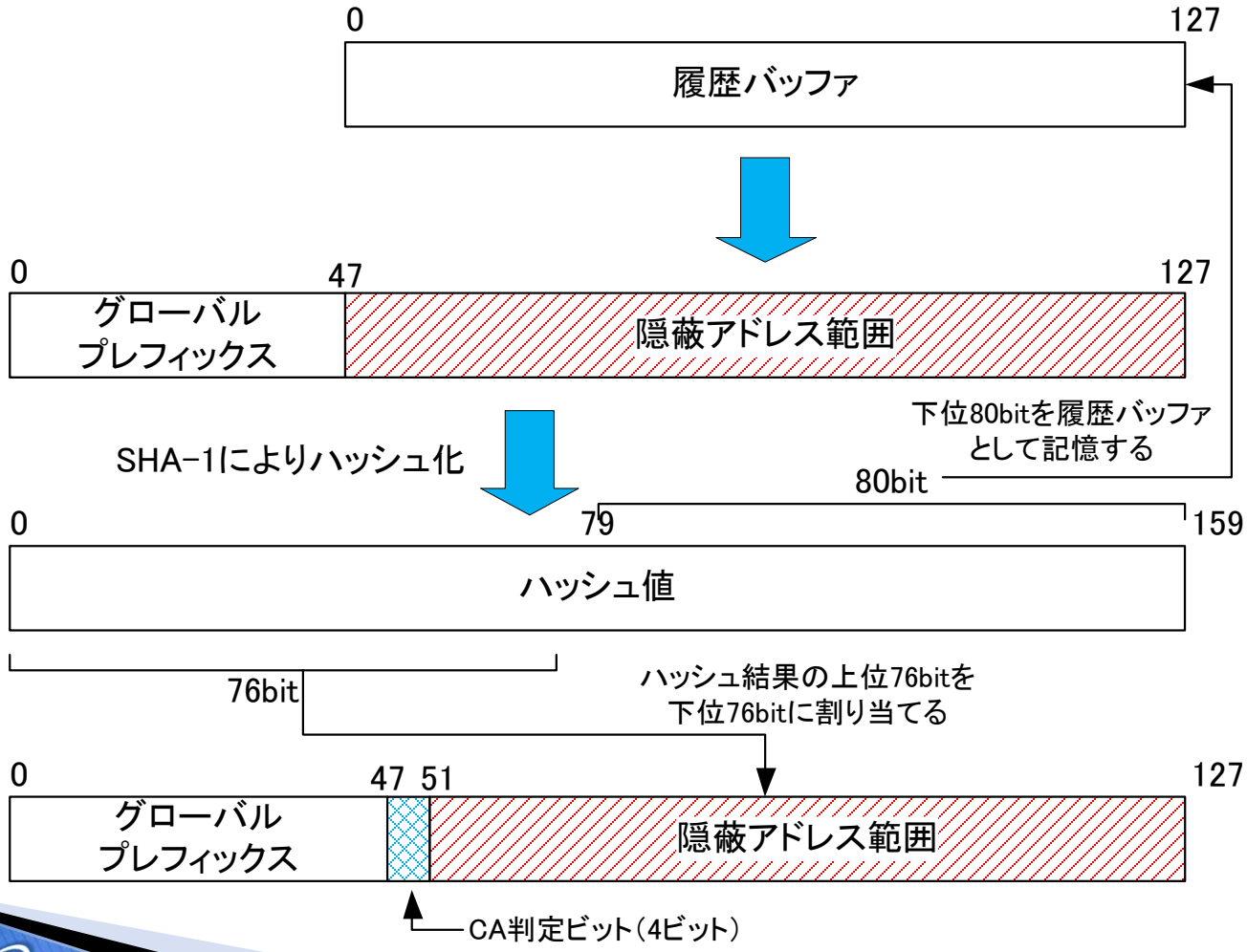
- 提案方式のモジュールを追加しても，劣化が見られないことを確認

まとめ

- IPv6ネットワーク構成を隠蔽する方式の提案
  - 外部端末用のアドレスCAの定義
  - CAMサーバの設置
  - CAのルーティングにはULAによるカプセル化通信
  - 評価によりカプセル化処理のオーバヘッドによる劣化が見られないことを確認

- 今後
  - 実装を完了させる
  - 端末数が増加したときのCAM Serverの負荷の検討

CA生成方法


0
127
履歴バッファ
0
47
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
下位80bitを履歴バッファ
として記憶する
80bit
0
79
159
ハッシュ値
76bit
ハッシュ結果の上位76bitを
下位76bitに割り当てる
0
47
51
127
グローバル
プレフィックス
隠蔽アドレス範囲
CA判定ビット（4ビット）