IPv6 におけるネットワーク構成隠蔽の提案

久保敷　透[†1]　鈴木秀和[†1]　渡邊　晃[†1]

グローバル IPv4 アドレスの枯渇に伴い，IPv6 への移行が必須である．しかし，IPv6 へ移行した場合，組織内の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．これを防止する方法として，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，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，ネットワーク構成を隠蔽するため，新たに隠蔽アドレスを定義し，このアドレスを使った通信方法について提案し，実装検討を行った．

Proposal of Network Topology Concealment in IPv6

Toru Kuboshiki,[†1] Hidekazu Suzuki[†1]
and Akira Watanabe[†1]

With a global IPv4 address depletion, it is said that the transition to IPv6 is indispensableness. Although, .network topology may be predicted by an address within an organization when I 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 hiding network topology. However, the redundant route become problem 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, to hide the network topology to define a new address hiding, and propose how to communicate using this address, we examined the implementation.

1. はじめに

インターネットが急激に普及したことにより，グローバル IPv4 アドレスの枯渇が問題となっている．アドレス枯渇の短期的な解決策として，プライベートアドレスを定義することにより，IPv4 の延命をしてきた．プライベートアドレス空間とインターネットを接続させるには，NAT（Network Address Translation）を必要とする．そのため，インターネット側からプライベートアドレス空間の端末へ接続を開始しようとしたときに，ネットワーク内部の構成がわからないため，通信を開始できない弊害が生じている．これを NAT 越え問題と呼び，IPv4 の汎用性を阻害する要因となっている．また，NAT ではパケットのアドレスを書き換えるため，アドレス情報を扱うアプリケーションは利用できないという課題もある．

その反面，NAT を用いることによって，組織内のネットワーク構造や端末に割り当てられているアドレスを隠蔽できるという利点が副次的に生まれた．企業のネットワーク管理者はできるだけ外部に情報を漏らしたくないという考えがあり，ネットワーク内部の情報を隠蔽できることは，セキュリティ上有用であるという考えが根強い．また，PCI（Payment Card Industry）のデータセキュリティ基準（PCI Data Security Standard）[1] では，支払いカードの情報を扱う組織はインターネット側に組織内のアドレスを開示してはならないことが規定されている．

一方，グローバル IPv4 アドレスの枯渇問題は深刻であり，すでに ICANN（Internet Corporation for Assigned Names and Numbers）から各地域レジストリへの配布が終了した．また，JPNIC（Japan Network Information Center）においても IPv4 アドレスの在庫が枯渇したとの報告がある[2]．そのため，アドレス枯渇の根本的な解決策である IPv6 への移行が必須である．

IPv6 では，NAT が不要であるため NAT 越え問題やアプリケーションの制限が解消され，インターネット本来のエンドエンド通信が可能となる．しかし，NAT によるネットワーク内部を隠蔽できるという副次的な利点がなくなり，アドレスから端末やネットワーク構成が特定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を隠蔽できる方法が考えられている．端末に対するプライバシー問題を解決するアドレスとして，下位 64 ビットのインターネット ID をランダムに生成する一時アドレス（Temporary Address）[3] が定義されている．しかし，一時アドレスは端末の特定を防ぐことはできるが，実際のサブネット ID が公開されるため，ネットワーク構成が予測される懸念がある．ネットワーク構成を隠蔽できる技術として，以下のような方式がある．NPTv6（IPv6-to-IPv6 Network Prefix Translation）[4] はアドレス変換を行う方式であり，IPv4 の NAT に類似した技術である．

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

NPTv6 は，ネットワーク内部を隠蔽できるが，アドレス変換を行っているため，SIP などのようにメッセージにアドレス情報が含まれるようなアプリケーションが，制限されるという IPv4 の NAT と同様の課題がある．Mobile IPv6 を用いた方式[5] は，移動透過性の技術をネットワークの隠蔽に応用する方式である．この方式では，ホームエージェントを経由する経路の冗長が生じるという課題がある．また，ネットワークを隠蔽するために，アドレスをランダムにしたものを用い，そのときのルーティングのために，ホストルートを用いた方式[5] がある，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，ルーティングテーブルのエントリー数が膨大になってしまいルータへの負荷が大きいという課題がある．

そこで本稿では，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．ネットワーク外部に存在する端末との通信には，サブネット ID とインタフェース ID をランダムに生成したアドレスを用いる．このアドレス宛のパケットをネットワーク内部でルーティングさせるためにトンネル技術を用いる．

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 章で実装検討，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（TA：Temporary Address）の構成を示す．IPv6 はステートレスアドレス自動生成が特徴である．ルータからのプレフィックス広告から上位 64 ビットのグローバルルーティングプレフィックスとサブネット ID を取得し，MAC アドレスからインタフェース ID を生成する．しかし，MAC アドレス情報が含まれるため端末が特定されやすい課題がある．一時アドレスは，この課題を解決し下位 64 ビットをランダムに生成することにより，端末の特定を防ぐことができる．しかし，サブネット ID はインターネット上にもそのまま流れるため，内部ネットワーク構成を推測されるおそれがある．

2.2 NPTv6

NPTv6 は，IPv6 においてもアドレス変換を行う方式である．IPv6 においてはアドレスが豊富であるため本来はアドレス変換をする必要がない．しかし，ネットワーク管理者は NAT を使用することにより，ネットワーク内部のアドレス管理が容易になると考えている．アドレスの隠蔽が第一の目的ではないが，副次的な利点としてインターネット側からネットワークの内部を隠蔽できる．NPTv6 では，IPv4 の NAT とは異なり内部の端末数だけグローバルアドレスを保持する．NPTv6 によりアドレス変換をする際には，インターネット側のアドレスと内側のアドレスを一対一に対応させて変換させるため，NAT 越え問題は生じない．NPTv6 の外側にはグローバルプレフィックスのアドレスが割り当てられ，内側にはローカルネットワークでのみ有効な ULA（Unique Local Unicast IPv6 Address）[6] が割り当てられる．アドレス変換するときには，下位 64 ビットのインタフェース ID は変換せずに上位 64 ビットのみを変換する．このときチェックサムが変わらないようにサブネット ID の値を工夫したアドレス変換を行う．この方式では，メッセージ内にアドレス情報が含まれるようなアプリケーションは通信を行うことが出来ず，IPv6 の利点が活かされない．

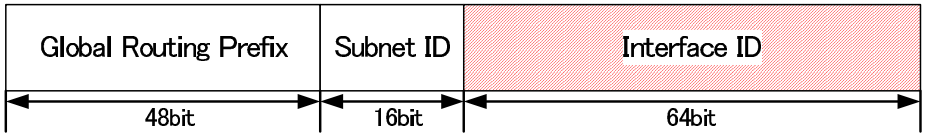


図 1 一時アドレス
Fig. 1 Temporary Address

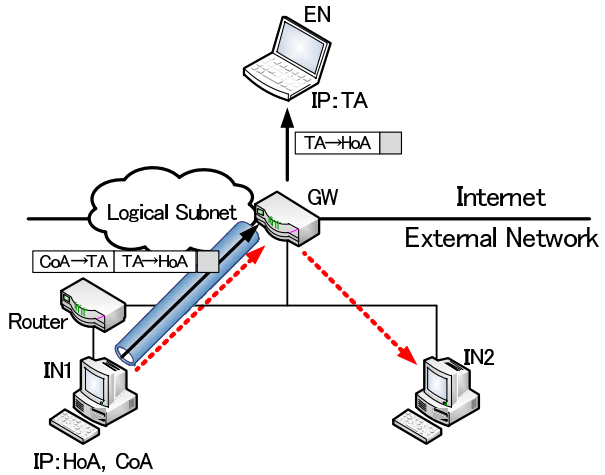


図 2 Mobile IPv6 によるネットワーク構成隠蔽
Fig. 2 Network topology hiding by Mobile IPv6

2.3 Mobile IPv6 を用いた方式

図 2 に Mobile IPv6 によるネットワーク構成隠蔽の例を示す．Mobile IPv6 は移動透過性を実現する技術である．ゲートウェイが Mobile IPv6 における HA（Home Agent），内部端末 IN（Internal Node）1,2 が MN（Mobile Node），外部端末 EN（External Node）が CN（Correspondent Node）の役割を果たす．IN1 にはホームアドレス（HoA：Home Address）としてネットワーク内部を隠蔽できるサブネット ID を任意に設定したアドレスを割り当てる．この任意に割り当てたサブネット ID のアドレス領域を論理サブネットと呼ぶ．この論理サブネットは実際のネットワーク構成に関係なく存在する．また，実際のネットワーク構成に応じたアドレスを気付けアドレス（CoA：Care-of Address）として割り当てる．EN と IN1 が通信をする場合，IN1 は送信元アドレスを HoA に設定する．そして，このパケットを CoA によりカプセル化して送信する．ゲートウェイまで届いたパケットはデカプセル化され，EN まで届けられる．EN からは送信元アドレスが HoA に見えるため，実際のネットワーク構成を知ることが出来ない．

しかし，この方式には以下のような問題がある．Mobile IPv6 には経路最適化という機能があり，この機能を有効にすると IN1 は移動後のアドレスを通信相手に通知し，HA を経由せずに直接通信を行おうとする．この場合，ネットワーク構成に対応したアドレス，すなわち CoA を CN に通知することになり，ネットワークを隠蔽したことにはならない．したがって，経路最適化の機能は無効にする必要がある．この結果，内部端末同士の通信においても必ずゲートウェイを経由した通信となってしまう．内部端末に対してのみ経路最適化を行いたい場合は，ゲートウェイに経路最適化パケットをフィルタリングする機能を組み込む必要があり，通信開始時にのみゲートウェイを経由することになる．

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 を任意の値に設定したアドレスを端末に割り当て，このアドレスのルーティングのために，ホストルートを設定するものである．ホストルートとは，全ルータのルーティングテーブルに端末ごとのルートを全てに設定するものである．ホストルートでは，サブネット ID がどのような値であってもルーティングが可能である．しかし，端末数だけルータにホストルートを設定しなければならないため，ルーティングテーブルのエントリ数が膨大になり，ルータに負荷がかかる可能性がある．

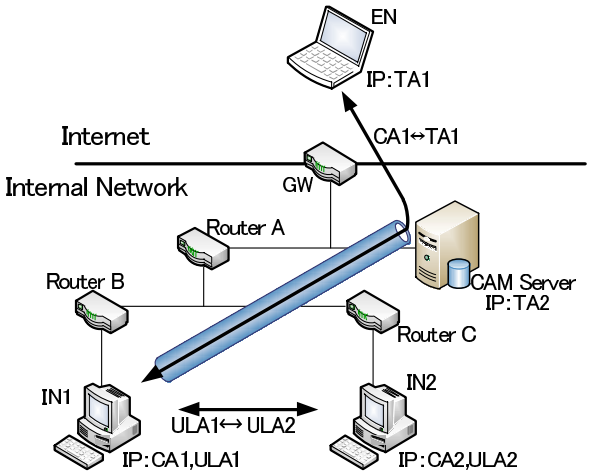


図 3 提案方式のシステム構成
Fig. 3 System configuration of proposal method

3. 提 案 方 式

3.1 システム構成

提案方式では，端末に 2 つのアドレスを持たせ，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ってネットワーク内部を隠蔽する．外部端末との通信時には，ランダムに生成したアドレスを用い，内部端末との通信には，内部でのみ有効なアドレスを用いて通信を行う．提案方式のシステム構成を**図 3** に示す．ネットワーク内部には IN1 と IN2 が存在し，インターネット上に EN があるものとする．内部端末 IN1，IN2 はアドレスとして外部通信用と内部通信用の 2 つのアドレスが割り当てられる．CA（Concealed Address）は本提案で新たに定義する隠蔽アドレスであり，ULA（Unique Local IPv6 Unicast Address）はネットワーク内部の通信に用いる．また，アドレスの管理に使用する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．内部端末 IN1 が EN と通信を行う場合，IN1 は相手の位置がネットワークの外側に存在すると判断したときに，CA1 を送信元アドレスとして通信を行う．相手端末が IN2 である場合は，ULA により通信を行う．

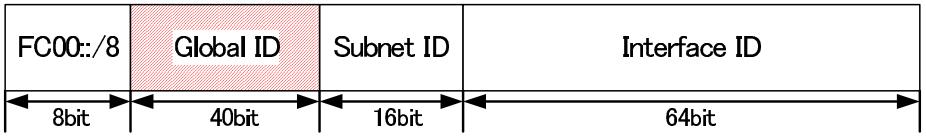


図 4 ユニークローカル IPv6 ユニキャストアドレス
Fig. 4 Unique Local IPv6 Unicast Address

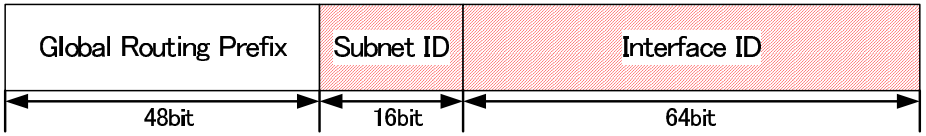


図 5 隠蔽アドレス
Fig. 5 Concealed Address

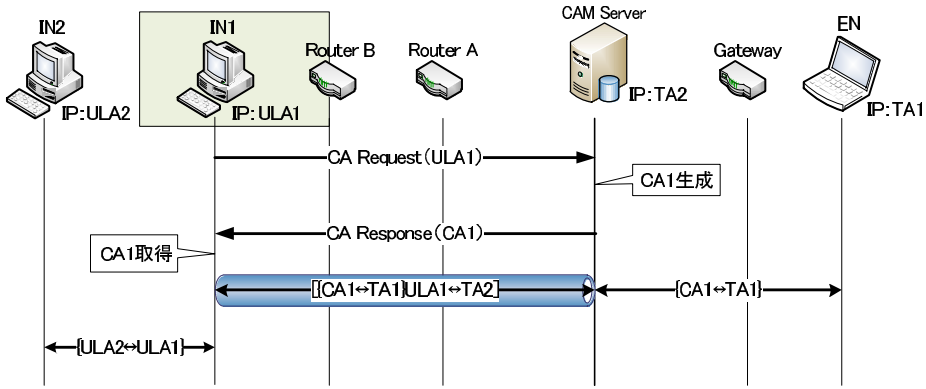


図 6 外部端末との通信動作
Fig. 6 Communication behavior with external Node

3.2 アドレスの定義

相手端末がネットワーク内部に存在する場合は，ULA を使用する．ULA のアドレス構成を**図 4** に示す．以前，IPv6 では内部でのみ有効なアドレスとしてサイトローカルアドレスが定義されていたことがある．しかし，スコープの定義が曖昧などの理由により廃止[7] され，その代わりとして新たに ULA が定義された．ULA はグローバル識別子の 40 ビットがランダムに生成されているアドレスである．そのため，万が一アドレスが漏れた場合でもアドレスが重複する可能性が極めて低い．ULA も同一ネットワーク内での通信を目的に定義されたものであり，インターネット上での利用は推奨されていない．

外部端末との通信には，新たに定義した隠蔽アドレス（CA：Concealed Address）を用いる．CA のアドレス構成を**図 5** に示す．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した値を用いる．これにより，端末やネットワーク構成の特定を防ぐことができる．サブネット ID をランダムに生成しているため，ネットワーク内部をルーティングするために，CAM サーバとの間にトンネルを生成し，新たに付加した IPv6 ヘッダには ULA を設定する．また，通常の重複アドレス検出の有効範囲は同一リンクのみである．そのため，実際のサブネットに関係無く割り当てられる CA は，CAM サーバで生成することによりアドレスの重複を防ぐ．

3.3 隠蔽アドレス管理サーバ

隠蔽アドレス管理サーバは，CA の管理および外部端末と内部端末との通信時に必要なトンネル経路を生成する役割を担う．CA 管理の主な機能として，CA の生成，重複アドレスチェックや再配布がある．端末は起動時に CAM サーバに対して CA を要求する．これに対して CAM サーバは重複しない CA を生成し端末へ配布する．この時 CAM サーバは CA と ULA の関係を登録しておく．CA には期限を設け，期限が近づくと，端末側から新たな CA を要求する．また，ネットワークを移動したときには，端末が CA の更新を要求する．これに対して CAM サーバは，新たな CA を生成し端末へ通知する．予め登録してあった CA と ULA の関係を，新 CA とネットワーク移動後に取得した新 ULA に更新する．そして，CAM サーバは CA を用いた通信を可能とするために，内部端末と CAM サーバの間で ULA によるトンネルを生成し，ネットワーク内でのルーティングを可能とする．

3.4 通 信 方 法

図 6 に内部端末 IN1 が外部端末 EN と通信する動作を示す．ネットワーク構成は図 3 と同様である．まず，内部端末 IN1 は起動後に，ステートレスアドレス自動生成により ULA1 を生成する．その後，外部端末との通信を必要とする場合は，CA を取得するために CAM サーバへ CA 要求パケット (CA Request) を送信する．このパケット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 CA1 を生成し，すでに生成されている他の CA と重複していないかどうかを確認する．重複していなければ，ULA1 と CA1 の関係を登録し，内部端末 IN1 へ CA1 の通知パケット（CA Response）を送信する．以上により内部端末 IN1 は外部端末との通信が可能となる．IN1 は EN との通信開始時に，相手が内部端末か外部端末かをアドレスから判断し，外部端末であれば，CA1 を送信元アドレス

として決定する．さらに，ネットワーク内部でのルーティングを可能とするため，カプセル化を行う．カプセル化ヘッダの送信元アドレスを ULA1，宛先アドレスを CAM サーバのアドレス TA2 とする．パケットが CAM サーバに到達したら，CAM サーバはデカプセル化して，送信元アドレス CA1，宛先アドレス TA1 のパケットを取り出し，EN へ送信する．EN から IN1 宛にパケットが送信されてきた場合，インターネット側から来たパケットはまず，ゲートウェイまで届き，宛先アドレスが CA の場合，CAM サーバへ転送される．CAM サーバでは CA1 と ULA1 の関係が登録されているため，送信元アドレス TA2，宛先アドレス ULA1 の IP ヘッダでカプセル化し IN1 まで送信する．

相手端末が IN2 であった場合，相手端末の位置がネットワーク内部であるので，送信元アドレスを ULA1 に設定し，カプセル化を行わずに直接通信を行う．

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，エンドエンド通信を実現し，アプリケーションの制限も生じない．

4. 実装検討

本提案を Linux へ実装する場合について検討する．提案方式は相手端末の位置によりアドレスを使い分ける．そのとき送信元アドレスの決定にはソースアドレス選択[8] という機能を用いる．IPv6 には，複数のアドレスを割り当てることができるようになっている．そのため，宛先アドレスに応じて，適切なアドレスを選択する必要があり，様々なパターンを考慮しなければならない[9]．この選択の規則についてはポリシーテーブルによって決めることができる．**図 7** に Linux で初期に設定されているポリシーテーブルを示す．それぞれのプレフィックスが登録されており，宛先アドレスに近いプレフィックスの送信元アドレスが選択される．本提案の内部端末同士での通信に用いる ULA のプレフィックスは，すでにポリシーテーブルに追加されており，`fc00::/7` がこれに該当する．宛先が ULA の場合はプレフィックスの値が近いアドレス，すなわち自身 ULA が送信元アドレスに設定される．このポリシーテーブルは変更が可能であり，今後，様々なアドレスに対応して送信元アドレスを決定させたい場合は，適宜変更が必要である．

Linux における提案方式の実装設計を**図 8** に示す．送信元アドレスが CA である場合，ネットワーク内部でのルーティングを可能とするために，カプセル化を行う．パケットのカプセル化はカーネル内の Capsulation Module により実現し，処理中のパケットをフックするために Netfilter を用いる．まず，受信パケットがアプリケーションから IP Layer へ

```
prefix ::1/128 label 0
prefix ::/96 label 3
prefix ::ffff:0.0.0.0/96 label 4
prefix 2001::/32 label 6
prefix 2001:10::/28 label 7
prefix 2002::/16 label 2
prefix fc00::/7 label 5
prefix ::/0 label 1
```

図 7 ルーティングポリシー
Fig. 7 Routing Policy

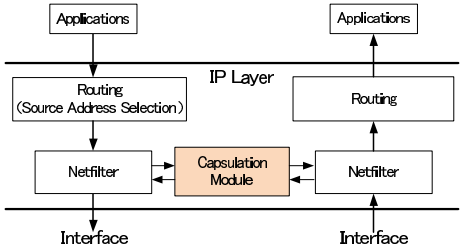


図 8 Linux における実装
Fig. 8 Implementation to Linux

渡されルーティング処理に入る．この時に，先に述べたソースアドレス選択の機能により送信元アドレスが決定され，宛先アドレスに応じた送信元アドレスが設定される．その後，Netfilter で送信パケットをフックし，カプセル化処理を行う Capsulation Module へ渡す．Capsulation Module ではソースアドレス選択により決定された送信元アドレスをチェックし，CA であった場合，カプセル化処理を行った後，送信パケットを通常のルーティング処理へ戻す．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ず，そのまま送信パケットを Netfilter へ戻す．受信パケットの場合，受信パケットが Interface から IP Layer へ渡されたときに，Netfilter で受信パケットをフックし，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し，カプセル化されている受信パケットである場合，デカプセル化処理を行い Netfilter へ差し戻し，ルーティング処理を行う．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で行う．

5. まとめ

本稿では，RFC4864 で示された IPv6 へ移行したときのネットワーク構成の隠蔽方式について，運用上の問題を取り上げた．Mobile IPv6 を用いた方式では，経路冗長の問題や Mobile IPv6 の導入コストの敷居が高いと考えられる．NPTv6 についてもインターネット本来のエンドエンド原則が満たされないと考えられる．これらの課題が生じない方式として，通信相手に応じて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通信を行う方式を提案した．

今後は検討した Linux への実装を完了させ，動作検証と評価を行う予定である．

参 考 文 献

1) PCI Security Standards Council, LLC: PCI Security Standards Council. https://www.pcisecuritystandards.org/.
2) Task Force on IPv4 Address Exhustion: IPv4 アドレス枯渇対応タスクフォース. http://www.kokatsu.jp/blog/ipv4/.
3) Narten, T., Draves, R. and Krishnan, S.: Privacy Extensions for Stateless Address Autoconfiguration in IPv6, RFC 4941, IETF (2007).
4) Wasserman, M. and Baker, F.: IPv6-to-IPv6 Network Prefix Translation, Internet-draft, IETF (2011). draft-mrw-nat66-16.txt.
5) de Velde, G.V., Hain, T., Droms, R., Carpenter, B. and Klein, E.: Local Network Protection for IPv6, RFC 4864, IETF (2007).
6) Hinden, R. and Haberman, B.: Unique Local IPv6 Unicast Addresses, RFC 4913, IETF (2005).
7) Huitema, C. and Carpenter, B.: Deprecating Site Local Addresses, RFC 3879, IETF (2004).
8) Draves, R.: Default Address Selection for Internet Protocol version 6 (IPv6), RFC 3484, IETF (2003).
9) Matsumoto, A., Fujisaki, T., Hiromi, R. and Kanayama, K.: Problem Statement for Default Address Selection in Multi-Prefix Environments: Operational Issues of RFC 3484 Default Rules, RFC 5220, IETF (2008).

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
久保敷 透, 鈴木 秀和, 渡邊 晃

Watanabe Lab.

背景

- IPv4アドレスの枯渇
  - 短期解決策
    - プライベートアドレスの導入
    - NATの導入
  - 根本的解決策
    - IPv6アドレスの導入 ← **必須**

- NATによる影響
  - NAT越え問題
  - アプリケーションの制約
  - 副次的にネットワーク内部が隠蔽される

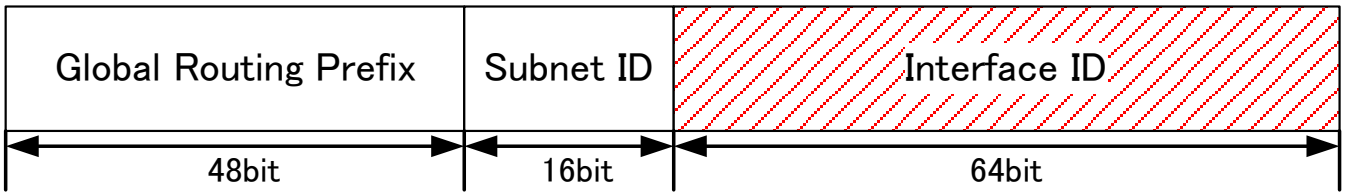
目的

- IPv6ネットワーク環境において
  - 各端末にグローバルアドレスが割り当てられる
  - NAT超え問題が解消されエンドエンド通信が可能
  - ネットワーク構成や端末が特定されやすい
    - ネットワーク管理者にとってはできるだけ情報を公開したくない
    - IPv6へ移行する際の不安要素の一つ

ネットワーク構成を隠蔽する方法の検討

一時アドレス

- 一時アドレス（TA:Temporary Address）
  - 端末のプライバシーを考慮したアドレス
  - 下位64ビットのインタフェースIDをランダム生成



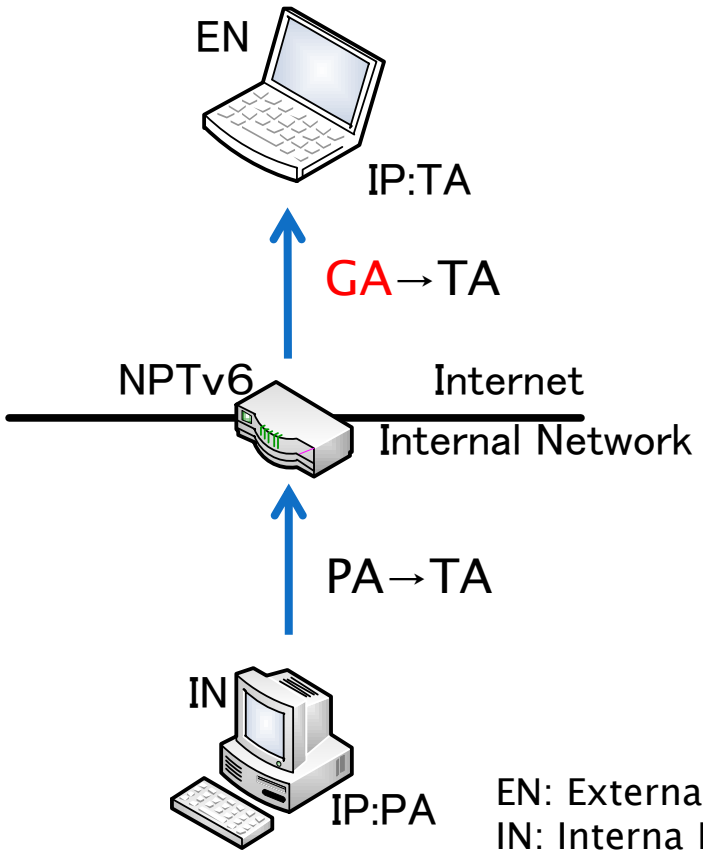
- ネットワーク構成までは隠蔽出来ない

Narten, T., Draves, R. and Krishnan, S.: Privacy Extensions for Stateless Address Autoconguration in IPv6, RFC 4941, IETF (2007).

NPTv6

- NPTv6(IPv6-to-IPv6 Network Prefix Translation)
  - IPv6アドレスを変換する機能
  - ステートレスなアドレス変換
  - NAT越え問題は生じない

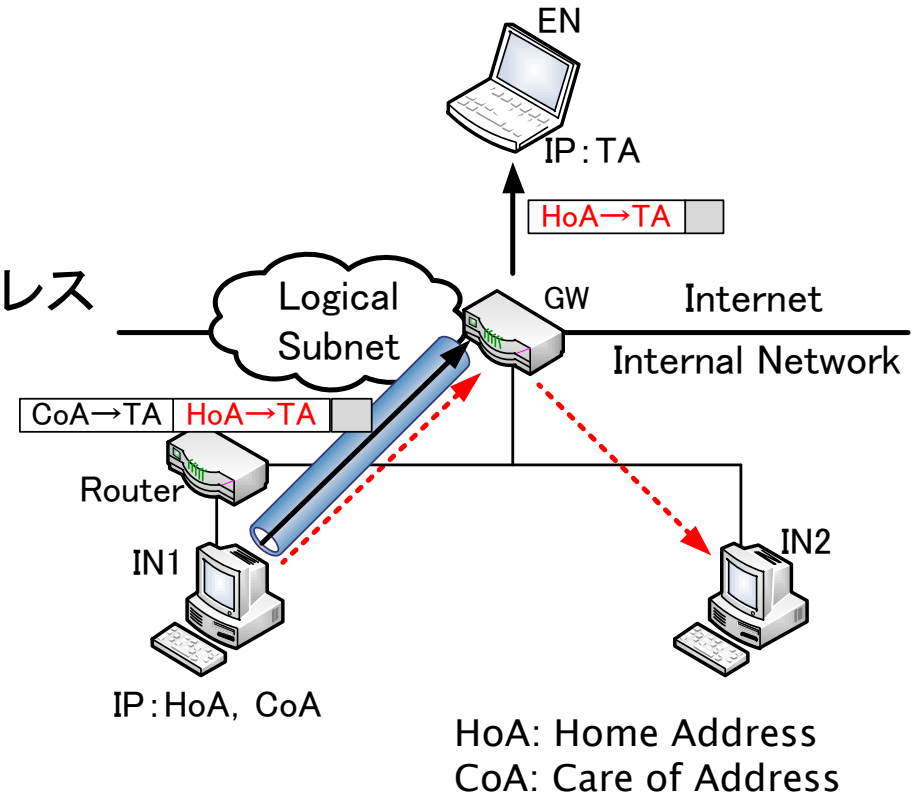
- 問題点
  - アプリケーションの制約
  - エンドエンド通信の弊害



Wasserman, M. and Baker, F.: IPv6-to-IPv6 Network Prex Translation, Internet-draft, IETF (2011). draft-mrw-nat66-16.txt.

Mobile IPv6を用いた方式

- 移動透過性技術をネットワーク構成隠蔽に適用（RFC4864）
  - ホームアドレス（HoA）
    - アドレスの値が任意
  - 気付けアドレス（CoA）
    - ネットワーク構成に応じたアドレス



- 問題点
  - 通信開始時の経路冗長
  - 不要な機能，導入の手間

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

既存技術の課題と解決方法

- NPTv6
  - エンドエンド通信の弊害となる
  - アプリケーションの制約

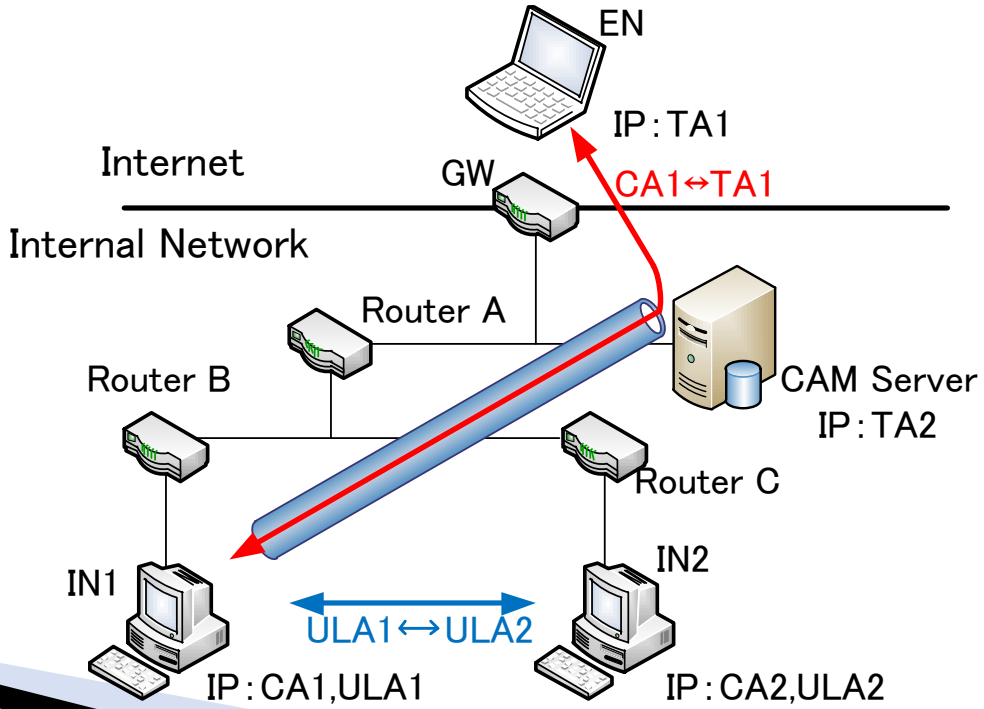
端末自身に隠蔽できる
アドレスを割り当てる

- Mobile IPv6
  - 内部端末との通信において
    経路冗長が起こる
  - 設定が煩雑になる

シンプルな
システムの提案

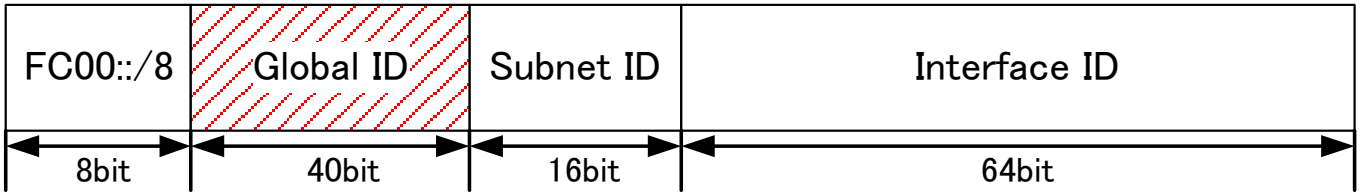
提案方式

- ネットワーク構成を隠蔽するために
  - 2つのアドレスを通信相手により使い分ける
  - 隠蔽アドレス(CA:Concealed Address)の導入
  - CAM(Concealed Address Management)サーバの導入

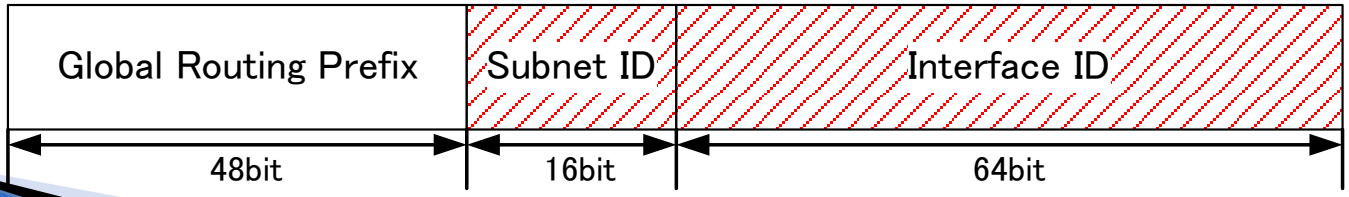


アドレス定義

- Unique Local IPv6 Unicast Address（RFC4913）
  - 内部端末同士の通信に使用



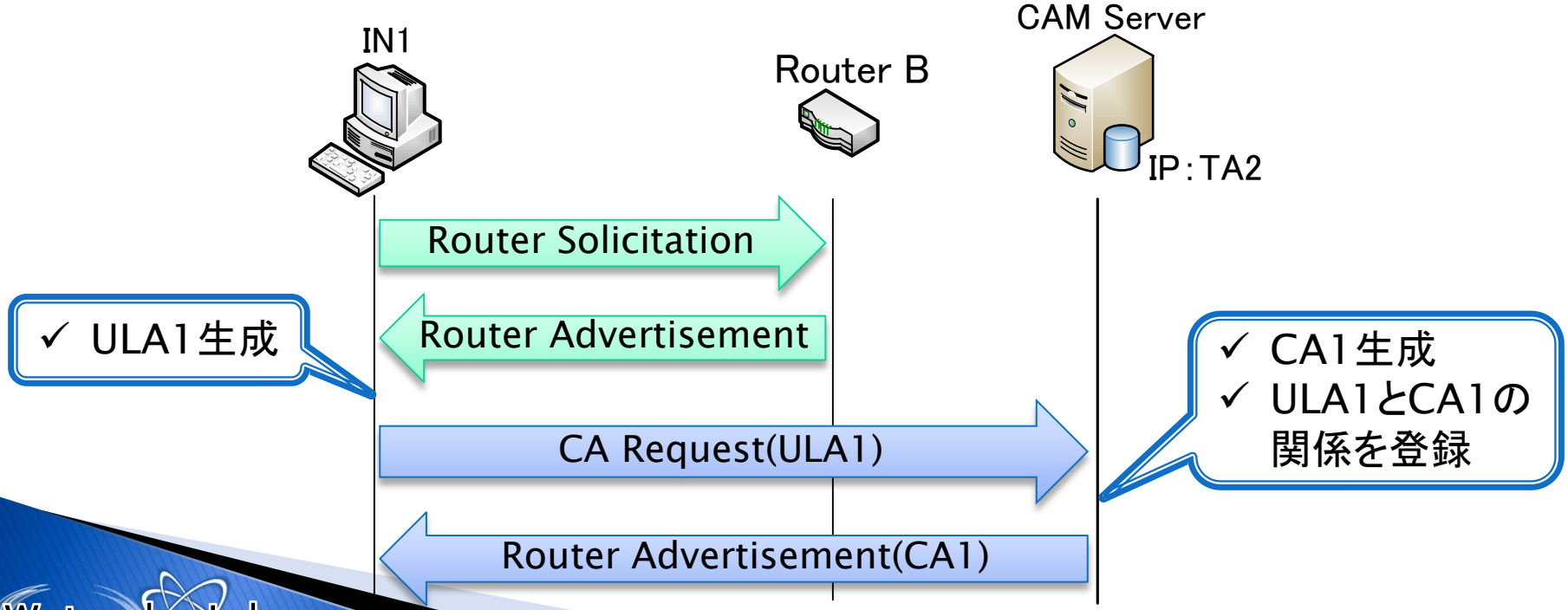
- Concealed Address
  - 外部端末との通信に使用
  - 下位80ビットをランダム生成



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

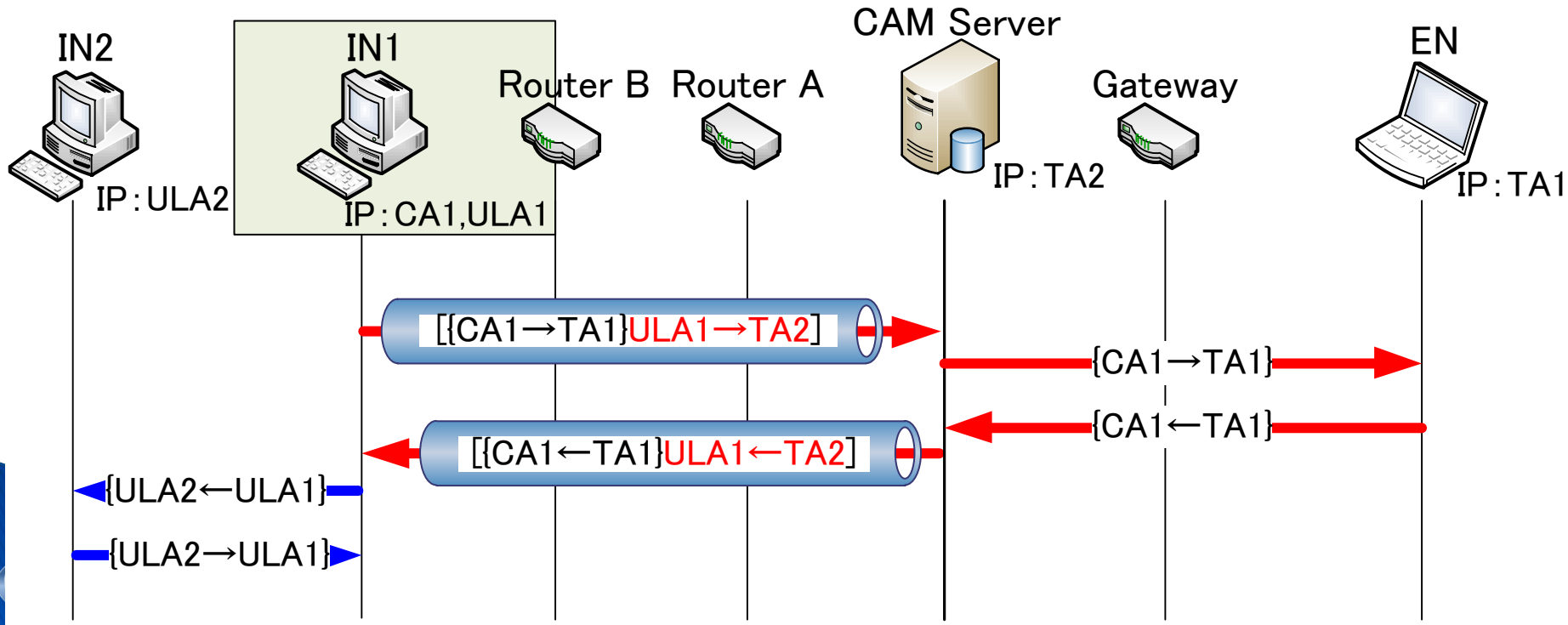
CAMサーバ

- 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
- トンネル経路生成
  - CAのルーティングを可能とするためのトンネル経路生成



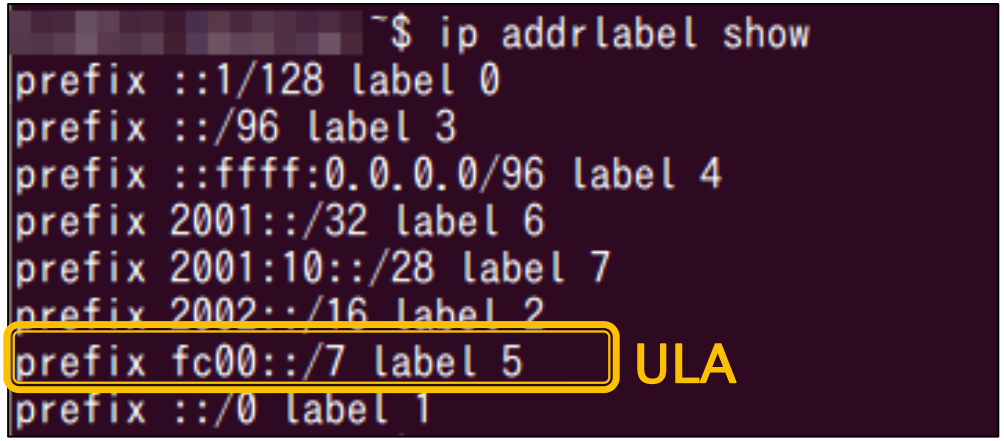
通信概要

- 外部通信時
  - 端末とCAM Server間でトンネルを生成する
- 内部通信時
  - ULA同士で通信を行う



実装検討(アドレス選択)

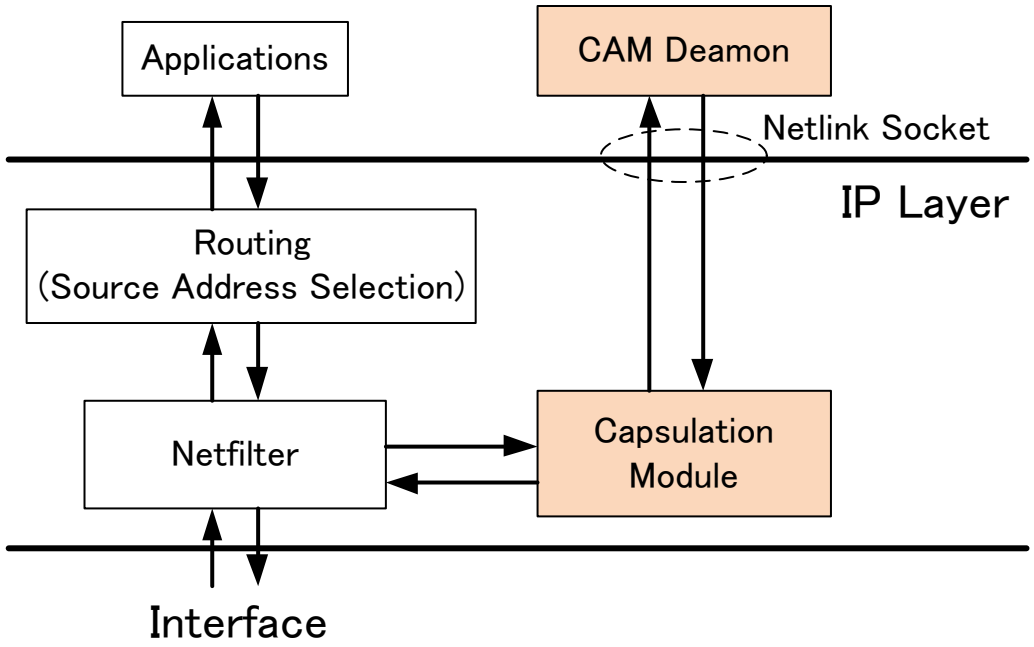
- デフォルトアドレス選択(RFC3484)
  - IPv6における使用するアドレスを選択する機能
  - 通信相手により送信元アドレスを設定するようにポリシーを設定する
- ip addrlabel showで確認できる



Draves, R.: Default Address Selection for Internet Protocol version 6 (IPv6), RFC3484, IETF (2003).

実装検討(クライアント)

- Linuxへの実装を検討
  - パケットのカプセル化をカーネルで実現する
  - LinuxのNetfilterによりパケットをフックしカプセル化する



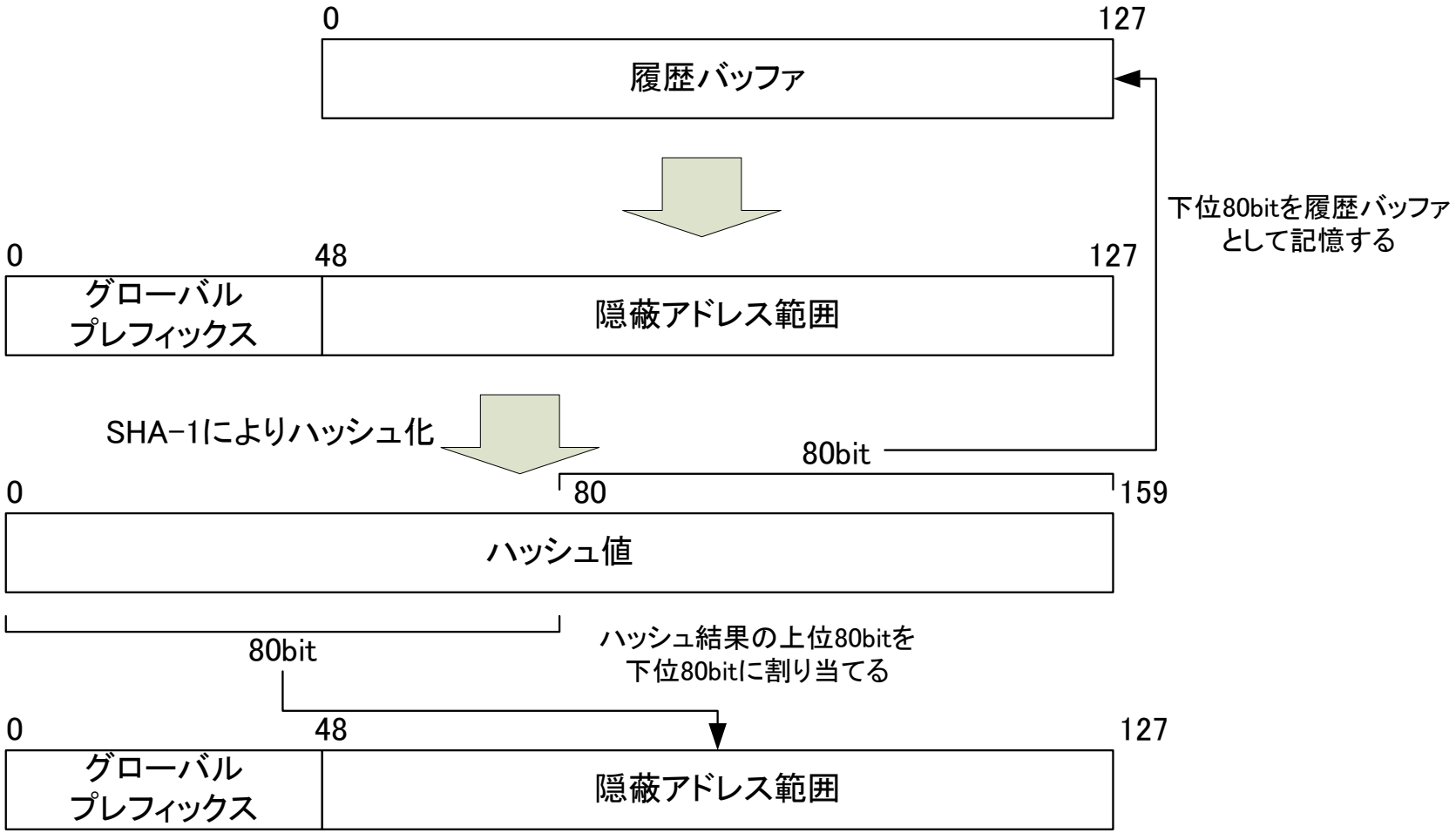
まとめ

- IPv6ネットワーク内部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サーバの導入

- 今後
  - 実装を完了させ動作の確認、評価を行う

付録

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