

IPv6 におけるネットワークの隠蔽方式に関する検討

久保敷 透[†] 寺澤 圭史[‡] 鈴木 秀和^{††} 渡邊 晃[‡]名城大学理工学部[†] 名城大学大学院理工学研究科[‡] 日本学術振興会^{††}

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構成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の隠蔽方式を提案する。

2. 既存技術

IPv6 にはプライバシーの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。このアドレスの使用により端末の特定を防止することができる。しかし、組織内のサブネット情報を示すサブネット ID の値はこれまで通りであるため、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も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 をランダムに設定したアドレスを使用する。しかし、サブネット ID がランダムであるため、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。ホストルートとは、ルーティングテーブルにホスト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がランダムに割り当てら

“Researches on the conceal method of the network in the IPv6”

[†]Toru Kuboshiki

Faculty of Science and Technology, Meijo University

[‡]Keiji Terazawa, Akira Watanabe

Graduate School of Science and Technology,

Meijo University

^{††}hidekazu Suzuki

Japan Society for the Promotion of Science

れていたとしてもルーティングが可能となる。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サイト内でのみ有効なアドレスとして、内部端末の通信に用いる。

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 はサイトローカルアドレスが廃止[4]されたのち、新たに考えられたアドレスである。サイトローカルアドレスでのアドレス重複の可能性などの問題を解決し、高い一意性を持っている。ULA はサイト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。CA を外部通信用として使用することによりネットワーク構成を隠蔽することが可能である。

3.2. 動作概要

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 CA を送信元アドレスとして通信を行う。CA を用いた通信を可能とするため、CA のホストルートをルータに設定する。

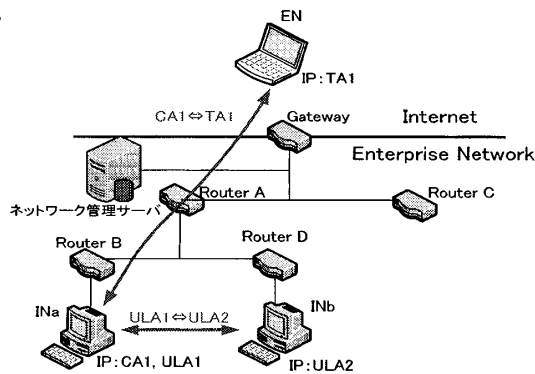


図 1 通信概要

3.3. ネットワーク管理サーバ

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、新たにネットワーク管理サーバを設置し、CA の生成、IPv6 アドレスの重複検出やホストルートの設定などを行う。以下にネットワーク管理サーバが必要とする機能を述べる。

● CA の管理

端末からアドレスの要求があった場合に、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 はネットワーク管理サーバで管理し、どの端末に CA が割り当てられているのかを把握している。また、CA には有効期限を設け、有効期限が過ぎた CA は利用できないようにする。

● ホストルートの自動設定

ホストルートの設定を端末が所属しているサブネットのルータからゲートウェイまでのルータに対して行う。この設定は、外部までの通信ルートだけに設定すればよいため、ルーティングテーブルのエントリー数の増大を抑えることが可能である。

● ネットワーク構成の収集

ネットワーク管理サーバはホストルートの設定のために、端末が所属しているサブネットを把握し、必要なルータにのみホストルートを設定する。そのため、ネットワーク構成を把握しておかなければならない。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。

3.4. CA 取得動作

図 2 に INa の CA の取得動作を示す。ネットワーク構成については図 1 と同様である。まず始めに、INa はルータからの広告により ULA の

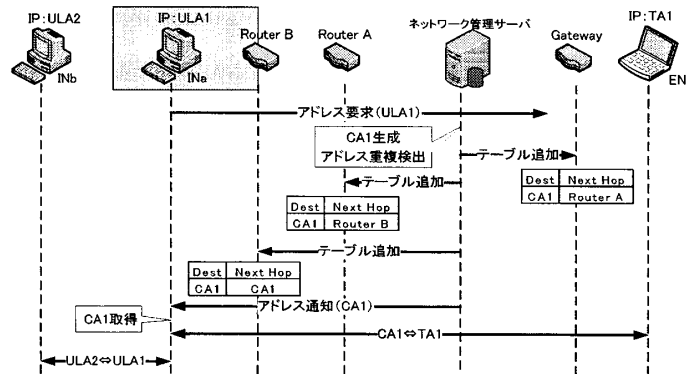


図 2 CA の取得動作

プレフィックスを受け取り、ULA1 を生成する。外部の端末との通信が必要な場合には、CA を取得するためにネットワーク管理サーバへ CA を要求するパケットを送信する。CA の要求パケットの送信元は ULA1 である。それを受け取ったネットワーク管理サーバは CA1 を生成する。ネットワーク管理サーバではすべての CA を管理しているため、アドレスの重複を避けることができる。次に取得済みのネットワーク構成と、CA 要求パケットの送信元アドレス ULA1 のサブネット ID を比較する。そして、INa の所属しているサブネットからゲートウェイまでのルータにホストルートを設定する。図 2 の場合は Router A と Router B, Gateway にホストルートを設定する。その後、CA を割り当てられた INa は通信相手の位置により、CA1 と ULA1 を使い分け通信を行う。

4. まとめ

IPv6 におけるネットワークの隠蔽方式について、外部と内部の通信に 2 種のアドレスを用いた方式を提案した。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 September 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
- [4] C. Huitema B. Carpenter "Deprecating Site Local Addresses" RFC3879 September 2004