

M-058

Anycast Address を用いたマルチホーミング multihoming using anycast address

山田 貴久[†]
Takahisa Yamada

小林 孝史[‡]
Takashi Kobayashi

1. はじめに

インターネットによって多くのサービスが運用されるようになり、インターネット無しには、社会が成り立たないほどにインターネットが普及している。このように重要なインフラになったインターネットもインターネットの利用者の増加に伴い通信量が增大している。インターネットに繋がる多くのサービスは、常時サービスを提供し続けることがのぞまれるようになり、サービスの停止が大きな損害を生むことになる。そのために我々はサービスが停止しないように障害を回避し、障害が発生した時には、迅速に障害からの復旧を行うことが必要になる。そこで、ネットワークの耐障害性のために IPv6 で採用されている Anycast アドレスを用いてネットワークを冗長化することを提案する。現在、Anycast Address は DNS の冗長化や Mobile IP におけるホームエージェント (HA) の検索に使用されるだけで多く使われていない。しかし Anycast Address を使えば、多くの重要リソースまでの経路を簡単に冗長化出来る。本稿では冗長化を行うための手法についての提案を行う。

2. Anycast Address

Anycast Address は同じアドレスを持つインターフェイスが複数存在し、そのうちのいずれかに届けられるが、どのインターフェイスに届けられるかはその時点で設定されている経路に依存する [?]。同一のアドレスを複数のマシンに付与できるため、耐障害性にすぐれたアドレスである。Anycast Address を用いるメリットは、冗長化だけではなく Address が同じ Anycast Address を用いるのでアドレスの設定を間違いにくい。同じ Address を重要なサービスが起動しているマシンに割り当てることで、アドレスを共有することができるため同じサービスを提供しているマシンの追加や取り外しを容易に行うことができる。

3. 実装

Fedora Core5 上の VMware Server1.0.2 上で仮想のルータとホストを作成して実験を行う。Anycast Address を付与したルータの実装には、FreeBSD5.4RELEASE を用いた。

4. 実験の概要

図 1 のようなネットワークを用いて実験を行う。図 1 にあるルータはノード側のインターフェイスに Anycast Address を付与した 2 台である。ルータの障害を起こすために片方のルータのインターフェイスのステータスを down にする。ルータが繋がっているノードから通信相手

のノードへの通信を監視する。この実験では ssh と ping6 を用いて通信を行う。通信ノードでは sshd のサービスが起動しているサーバとして用い、ノードはクライアントとして用いて通信を行う。図 1 では、右の gateway の方がネットワーク的に近いため、右の gateway を経由してパケットが届く。ノードは通信相手にパケットを送信し、gateway を経由して通信ノードに到達する。通信の応答確認ができた時点で通信に使用されている方のルータのインターフェイスを down にする。それをルータ 2 台で交互に行い、障害時のネットワークの切替えを検証する。

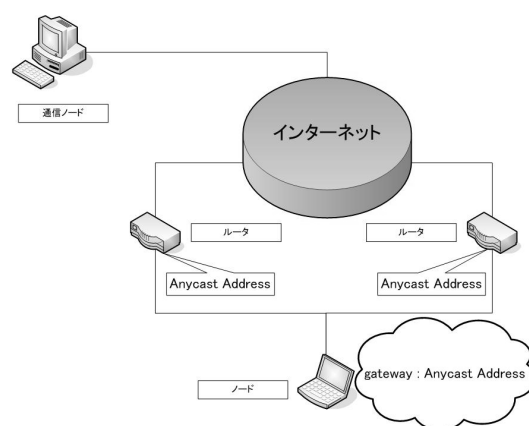


図 1: 実験用ネットワーク

5. 結果

Router Advertisement (RA) を使用するマルチホーミングとは違い RA を使用していないノードも通信を継続することができた。ネットワークに障害が起こった時に、全てのノードが別の gateway を自動的に選択し、通信を継続することに成功した。

5.1 gateway の切替え

IPv6 では Address をステートレスアドレスで自動的に割り当てる方法と固定アドレスを割り振る方法の 2 種類がある。本稿では、ステートレスアドレスを割り当てるために Router Solicitation (RS) を有効にした場合と、固定アドレスを割り振るために RS を無効にした場合を一つのホストで検証した。固定アドレスを割り当てているノードの場合、アドレスと gateway を手動で設定する。この実験ではネットワークが変化しても、gateway のアドレスを変化させることなく通信を行うことができたが、gateway の切替えによって少しの間パケットが届かない時間が存在した。しかし、Anycast Address の付与されているルータが一台でも残っている限り、通信を継続す

[†]関西大学, Kansai University

[‡]関西大学, Kansai University

ることが可能であった。また、Anycast Address を付与したルータが故障した場合、Anycast Address を付与したルータをもう一台設置するだけで復旧を行うことができた。ステートレスアドレス自動生成でルータ広告からアドレスを作成した場合、gateway が内部のリンクローカルアドレスとなる。自動生成を行うためルータに障害が起こり故障しても、ルータ広告によって動的に gateway を作り直すことができるため、Anycast Address をルータに割り当てなくてもノードは通信を行うことができる。障害から復旧した後、以前使用していた gateway が復旧しても gateway の変更は起こることは無かった。

5.2 復旧時間の検証

インターフェイスを down から up で回復させて、ネットワークへの復旧を行った。ネットワークの復旧時間が変動するため、障害が発生してネットワークが回復するまでを1復旧として、10復旧を1回の試行として計測し1復旧の平均時間を求めた。ステートレスアドレスを用いた場合、rtadvdのインターバルタイムとルータライフタイムの値を変化することで、復旧の時間が大幅に変動した。ルータライフタイム値とインターバルタイムの値の減少に比例して復旧の時間が早くなり、インターバルタイムの最大値と最小値の差が小さいほど復旧の時間のばらつきが少ない。Anycast Address ではRAが関係しないため、rtadvdのパラメータに関係無くランダムな値を示した。これはAnycast Address Resolving Protocol(AARP)でAnycast AddressをUnicast Addressに変換するオーバーヘッド時間と考えられる。図2では試行回数を増やしていくと復旧時間が長くなる傾向を示した。もっとも大きな平均値となった5回目の試行では、一回の試行での最大値と最小値の差が大きくなった。大きな値が表れる直前には、小さな値が表れることが本実験の結果で示された。それは、ネットワークにアドレスがキャッシュされるためと考えられる。そのため、キャッシュされていないアドレスへのgatewayの切替えが遅くなり、キャッシュされたアドレスへのgatewayの切替えが早くなると推測できる。

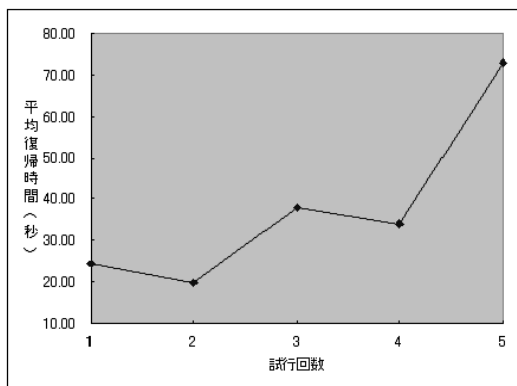


図 2: Anycast Address の復旧時間

5.3 セキュリティ

ルータの gateway に Anycast Address を設定する方法は、ネットワーク内に悪意のあるユーザがいる場合には大変危険である。Anycast Address を gateway に使用しているとわかれば、悪意のあるユーザによって Anycast Address を付与したルータを設置することが考えられる。必ずしも悪意のあるユーザの設置したルータを経由するとは限らないため、そのルータに気付くのが遅れたり、そのルータが発見されそうになればインターフェイスを down にすることで発見を防ぐことが可能である。また、ルータへのなりすましが容易なため man-in-the-middle attack を行うことができる。ルータへの信頼性を検証する仕組みが導入されない限り、この問題を防ぐのは難しい。また、Anycast Address を推測するのはネットワークプレフィックス部分が判明すれば簡単である。そのため、悪意のあるユーザが Anycast Address を推測して攻撃を行うことも容易であると考えられる。外部からの攻撃の場合はファイヤーウォールで防ぐことができるが、内部のネットワークから攻撃された場合は防ぐことができない。

6. 終わりに

IPv6 化されたネットワークの重要なリソースに Anycast Address を付与するメリットは大きい。また、経路を冗長化するための単純なマルチホーミング機構として活用ができる。しかし、IPv6 から採用されたプロトコルのため、現ネットワークの主流である IPv4 では使うことができない。IPv6 のネットワークでしか使うことが出来ず、このメリットを享受するためには IPv6 へのネットワークへの移行を推進する必要がある。単純なマルチホーミングを行うために複雑な仕組みを利用せず Anycast Address を用いて行ったので、shim6[?] や BGP[?] を利用した高度なマルチホーミングのようにネットワークの選択的な切替えや、ネットワークによつての gateway の選択などを行うことができない。Anycast Address を用いるため、回線速度が遅くてもネットワーク的に近ければ、選択されるのは遅い方の gateway になってしまう。優先度をネットワークに付与してネットワーク的な距離以外での切替えや、既存の技術と Anycast Address を併用、あるいは状況に応じて現行のマルチホーミングを選択的に使用することで欠点を補うことができる [?]

参考文献

- [1] IRI・ユビキタス研究所, “マスタリング TCP/IP IPv6 編”, オーム社, 2005.
- [2] 松本 存史, 藤川 賢治, 岡部 寿男, 太田 昌孝, 寺岡 文男, 國司 光宣, 石山 政浩, “モバイルネットワークアーキテクチャ LIN6 のマルチホーミング対応,” DICO2002, pp.321-324, 3 July 2002.
- [3] 尾家 祐二, 鬼丸 敬輔, “マルチホーム環境実現のための IPv6 プレフィックス変換機構の開発”, 2002
- [4] IETF <http://www.ietf.org> draft-ietf-shim6-applicability-02(RFC3582)