

Automatic Service Routing System(ASRS) の提案と設計

上野 幸杜[†]
eden@sfc.wide.ad.jp

堀場 勝広[‡]
qoo@sfc.wide.ad.jp

概要

インターネット上でサーバ/クライアントモデルを用いてサービスを提供する場合、サービス提供者には自身の設備のメンテナンスまたは障害に関係なくサービスを継続することに対する要求がある。現在のインターネットアーキテクチャはサービスの移設を考慮して設計されていないため、この要求を満たすには新たな技術が必要となる。近年ではこの要求を満たすため、レイヤ2/レイヤ3拡張技術やホスト仮想化技術が使用される場合が多い。また Content Centric Networking(CCN) という概念は、この問題に対して全く異なるアプローチで解決方法を示している。しかし、いずれの方法もサービス提供者にとってのデメリットをはらんでおり、それらのデメリットを持たない新しい技術が必要である。そこで、DNS やレイヤ3ネットワーク、ポート番号に依存せずサービスへのルーティングを行えるシステムとして、本論文では Automatic Service Routing System(ASRS) を提案、設計した。

1. 背景

現在のインターネット上では、様々なサービスがサーバ/クライアントモデルによってユーザに提供されている。サービス提供者は、ユーザに対して継続的にサービスを提供したいという要求を持っている。そのため、サービス提供者の設備のメンテナンスまたは障害があった場合、サービスをメンテナンスまたは障害の影響を受けない別の設備に移設して継続する手段が必要となる。

しかし、サービスとホストのマッピングを解決する DNS はキャッシュを用いるシステムであるため、サービスの移動があった場合、キャッシュの TTL が失効するまでは新たなサービスとホストのマッピングを解決することはできない。また、DNS は FQDN と IP アドレスのマッピングをクライアントサイドで解決するため、サービスの識別はサービス提供者の保有するグローバルな IP アドレスの個数や、その運用の制約を受ける。さらに、IANA によって定義されるレイヤ4のポート番号は任意に変更することができず、例えば http であれば 80 番以外を使用する場合プロキシやロードバランサなど別の技術を併用するか、クライアントサイドで対応しなければならない。

一方で、近年レイヤ2拡張技術 [1][2]、ホスト仮想化技術等の普及により、サービスを提供するホストを様々なネットワーク間で移動させつつも、離れた拠点間で同一セグメントに所属させることが可能になっている。また、レイヤ3における Locator/ID separation [3] 技術により、インターネットの経路情報に依存しないレイヤ3ネットワークを構築する運用形態も増えつつある。しかし、これらの技術はレイヤ2/レイヤ3ネットワークの用途を本来想定されていた使い方とは別に拡張するものであり、サービス提供者のネットワークを複雑化し、運用コストを増大させるというデメリットがある。

これに対して、コンテンツなどに独立した識別子を与え、DNS やレイヤ3のネットワーク、ポート番号に依存せずユーザの要求するデータを提供する技術も研究され

ている。Content Centric Networking(CCN) [4] やその発展としての Named Data Networking(NDN) [5] がこれに該当する。NDN はユーザが要求するデータをコンテンツという単位で定義し、個々のコンテンツに識別子を与えることで、コンテンツ単位でのデータの取得を可能にする。NDN は必ずしも既存の IP ネットワーク上で動作することを前提としておらず、現在のインターネットアーキテクチャ全体を作り直すことを指向している。しかし、現在ではインターネットアーキテクチャとして IP ネットワークが普及しており、インターネット全体のアーキテクチャを作り直すことは困難である。

したがって、現在のインターネットアーキテクチャである IP ネットワーク上でのクライアント/サーバモデルによるサービスを、DNS のキャッシュ TTL や IP アドレス、ポート番号に依存せずに識別することに対する要求があるといえる。

2. Automatic Service Routing System (ASRS) の提案

本論文では、以上の要求を満たすシステムとして、自動サービスルーティングシステム Automatic Service Routing System(ASRS) を提案する。図1に既存の DNS を使用したサービス提供モデルと、ASRS を使用した場合のサービス提供モデルの違いを示す。既存のモデルでは、クライアントはサービスの識別子である IP アドレスとポート番号の組み合わせを DNS によって取得し、サービスにアクセスする。このモデルでは、サービスの追加や移動は IP アドレスやポート番号による制約を受ける。一方で ASRS では、クライアントは目的のサービスをサービス専用の識別子によって識別し、実際のサービス提供ホストがどのような IP アドレスとポート番号の組み合わせによってサービスを提供しているかを関知しない。従って、ASRS ではサービスの追加や移動をする際に IP アドレスやポート番号による制約を受けない。つまり、ASRS はサービスの識別を IP アドレス及びポート番号から切り離す技術と言える。ASRS では、サービスを提供するホストが自発的にサービス提供先を登録し、サービス提供者のネットワークに設置されたゲートウェイが登録された情報に基づいてサービス提供ホストを制御する。このとき ASRS 上のサービス提供ホストの制御はサービス提供者のネットワーク内に閉じているため、DNS が持つキャッシュ TTL による運用上の制約を受けない。

3. ASRS の設計

図2に ASRS の構成と動作を示す。ASRS は、クライアントからのパケットをサービス登録情報に基づいて書き換える「サービスルータ」、サービスを提供するホストからのサービス登録を管理し、サービスルータにサービス情報を通知する「サービスマップサーバ」、サービスを提供するホスト上で動作する「サービス登録デーモン」の3つの要素で構成される。ASRS では、サービスを一意に識別するために URI で表現されるサービス識別子を使用する。サービス識別子に対応する IP アドレス、ポート番号は、サービスを提供するホスト上で動作するサービス登録

[†]慶應義塾大学 環境情報学部

[‡]慶應義塾大学 政策・メディア研究科

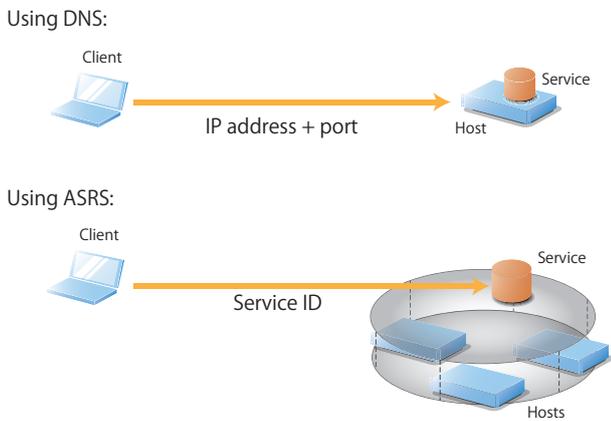


図 1: 既存のサービス提供モデルと ASRS の違い

デーモンがサービスマップサーバに定期的に登録し、サービスマップサーバは登録されたサービス識別子ごとの IP アドレス、ポート番号などの宛先情報の中で、最も優先度の高い宛先情報に変化があった場合にサービスルータにその変更を通知する。サービスマップサーバとサービスルータは TCP を用いたコネクションを用いてシグナリングを行い、サービスマップサーバはサービス識別子と宛先情報のマッピングの変更についてプッシュ型の通知をおこなう。

ASRS では、クライアントが URI で表現されるサービス識別子を入力しなければならない。現在のインターネットではサービスを提供するホストを検索するために DNS が使用されるため、ASRS では DNS を利用してサービス識別子を入力することを前提とした設計とする。ある FQDN で ASRS を使用してサービスを提供する場合、あらかじめ FQDN にサービスルータの A または AAAA レコードとサービス識別子を示す TXT レコードを設定しておき、クライアントはそれらの情報を利用してサービスにアクセスする。

サービス識別子の解釈に対応したクライアントの場合、ASRS に対応した FQDN の A または AAAA レコードを宛先アドレスとし、ASRS 用に固定的に設定されたポート番号を宛先ポートとして、サービス識別子を示す TXT レコードの内容を含んだパケットを送出する。ASRS のサービスルータは、パケットに含まれるサービス識別子に対応する IP アドレス、ポート番号をパケットの宛先とし、サービスルータ自身の IP アドレス、任意のポート番号を送信元としてサービス提供ホストにパケットを転送する。このとき、サービスルータはクライアントのソース IP アドレス、ポート番号と書き換え後のソース IP アドレス、ポート番号を紐付けるセッションテーブルを保持し、返信されてきたパケットを先ほどと逆に書き換えてクライアントに転送する。

サービス識別子の解釈に対応しないクライアントの場合、制約はあるものの、ASRS を使用すること自体は可能である。クライアントは ASRS でサービスを提供する FQDN に設定された TXT レコードを解釈しないため、例えば http であれば宛先アドレスを A または AAAA レコードとし、宛先ポートを 80 番ポートとしてパケットを送出する。サービスルータには、宛先ポート 80 番に対してあらかじめ静的にサービス識別子を設定しておき、そのサービス識別子に対応する IP アドレス、ポート番号をパケットの宛先とし、サービスルータ自身の IP アドレス、任意のポート番号を送信元としてサービス提供ホストにパケットを転送する。この場合も同様に、サービスルータはクライアントのソース IP アドレス、ポート番号と書き換え後のソース IP アドレス、ポート番号を紐付けるセッション

テーブルを保持し、返信されてきたパケットを先ほどと逆に書き換えてクライアントに転送する。

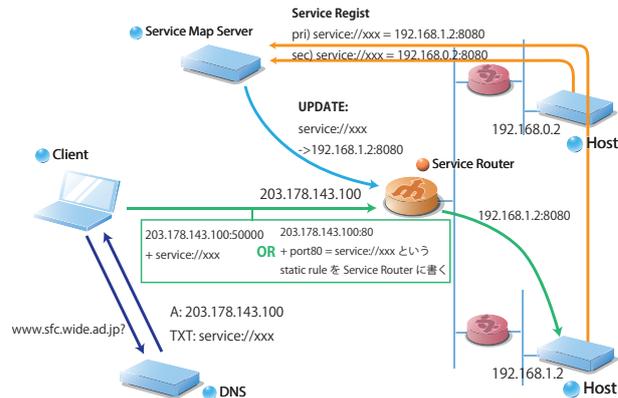


図 2: ASRS の構成と動作

4. 予想される問題

ASRS を導入後に予想される問題として、スケーラビリティの確保が比較的難しい点が考えられる。サービスルータはクライアントからのコネクションとサービス提供ホストのマッピングをセッションテーブルに保持するため、NAT やロードバランサと同じくコネクションあたりに必要なリソースが比較的大きい技術と言える。また、サービスマップサーバはサービス登録情報の更新をプッシュ方式でサービスルータに通知するため、サービスルータとは常に TCP コネクションを張っていないといけない。サービスルータの台数が増えた場合、サービスマップサーバの負荷が増大し、処理しきれなくなる可能性があると考えられる。サービスルータのスケーラビリティを確保する方法として、エニーキャストを用いて複数のサービスルータを同一 IP アドレスで設置し、負荷を分散する方法が考えられる。また、サービス登録デーモン及びサービスルータは複数のサービスマップサーバを使用できる実装とすることで、サービスマップサーバのスケーラビリティもある程度確保できる。

5. 結論

本研究では、サービス識別子の変更が DNS のキャッシュ TTL に依存せず、またその識別子としてサービス専用の URI で表現される識別子が使用可能であり、サービス提供ホストには任意の IP アドレス、ポート番号が使用可能であるシステム、ASRS を提案、設計した。また、ASRS を使用した場合に予想される問題点について検討し、その上で考えられる解決策を示した。

参考文献

- [1] M. Mahalingam, D. Dutt, K. Duda, P. Agarwal, L. Kreeger, T. Sridhar, M. Bursell, and C. Wright, "VXLAN: A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks", August 2012. IETF Internet-Draft.
- [2] H. Grover, D. Rao, D. Farinacci, and V. Moreno, "Overlay Transport Virtualization", July 2011. IETF Internet-Draft.
- [3] D. Farinacci, V. Fuller, D. Meyer, and D. Lewis, "Locator/ID Separation Protocol (LISP)", May 2012. IETF Internet-Draft.
- [4] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, R. L. Braynard "Networking Named Content", CoNEXT 2009, December 2009.
- [5] Named Data Networking(NDN), <http://www.named-data.net/>, October 2012.