RTGWG
Internet-Draft
Intended status: Standards Track
Expires: 15 June 2026

F. Yang
China Mobile

12 December 2025

DNS driven traffic steering
draft-yang-rtgwg-dns-driven-traffic-steering-00

Abstract

The Internet provides best-effort service, and for users with quality assurance requirements, selecting an Internet acceleration service provider to gareentee network access quality is a common choice. This document proposes a possible mechanism for leveraging DNS to automatically steer application’ s traffic onto an SRv6 network.

Table of Contents

1. Introduction

The Internet provides best-effort service, and for users with quality assurance requirements, selecting an ISAP (Internet Acceleration Service Provider) to gareentee network access quality is a common choice. This document proposes a possible mechanism for leveraging DNS to automatically steer application' s traffic onto an SRv6 network.

As shown in Figure 1, IASPs typically deploy an Overlay network plane to accelerate user traffic. This network plane consists of PoPs (Points of Presence) and routers, where PoPs are responsible for accessing user traffic and connecting to CSPs (Content Service Provider). Routers and PoPs are usually virtualized devices deployed in the cloud. Typically, when SRv6 is deployed in this network plane for path programming, ACLs are required to classify user traffic and steer it onto SRv6 Policies. Due to the need for extensive ACLs configuration manually, it is quite challenging to apply this approach on a large scale. Thus, how to efficiently steer user traffic becomes an interesting problem.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Terminology

CSP: Content Service Provider, provides content-related services, e.g. gaming, video services.

IASP: Internet Acceleration Service Provider, provides gareenteed internet network access quality for latency, loss sensitive applications, e.g. gaming、video services.

PoP: Points of Presence, network forwarding element in order to accessing user traffic or exchange traffic with internet service provider.

3. DNS driven traffic steering

On IASP perspective, the SRv6 Policy is defined by <source, destination, Color>. To achieve differentiated transport, it is necessary to map applications to the corresponding SRv6 Policy.

On user application perspective, the first interaction with network would be DNS request, which will finally resolve the domain name to destination address. The idea is to get IASP's network snoop the user DNS interaction process in order to steer the user's traffic with that destination to IASP's network. Thereby achieving network quality of service assurance.

Certainly, the IASP needs to configure the mapping between domain names and SRv6 policy colors on the controller in advance. Figure 1 illustrates the necessary network components.

User: DNS server SHOULD be set to IASP's uPoP.

uPoP: For accessing user. It is endpoint of SRv6 policy. DNS relay is needed. It SHOULD check whether the domain name in the DNS request from application is subscribed by the user. Then it SHOULD relay the DNS request to DNS proxy.

cPoP: For connecting to CSP. It is endpoint of SRv6 policy. It will enable NAT for user traffic to ensure that the downstream traffic passes through the cPoP.

DNS Proxy: it will handle the DNS resolution from uPoP. There is one extension for DNS proxy. Once the domain name gets resolved, it SHOULD send domain name, destination address of DNS response packet and application destination address list inside the DNS response packet to controller via DNS-response notification.

The DNS-response notification DNS proxy sent to the controller can be defined by json, xml. Below is json example:

```
{
  "message": {
    "application_destinations": [addr1, addr2],
    "dns_response_destination": "addr3",
    "domain_name": "example.com"
  }
}
```

Controller: once received DNS-response notification, it will resolve <source, destination, color> and then get the corrsponding SRv6 policy programmed to uPoP. The source is destination address of DNS response packet in the notification, because it is the address of the uPoP. The ISAP definitely knows the CSP's domain name and service addresses. So the cPoP connected to the CSP can be resolved by looking up application destination address. The application destinations and the DNS response destination address can be used in ACL in upstream and downstream SRv6 policy steering direction, respectively. Now it is ready to find or create an existing SRv6 policy. And then program the steering rule to cPoP and uPoP. For sure, the ACL on both PoPs SHOULD count the number of packets it has been steered, and that can be used as ACL aging mechanism.

Note, with this proposed mechanism, there will be a short period of time for the steering ACL policies get programmed. In this period, the IASP will only provide best effort service.

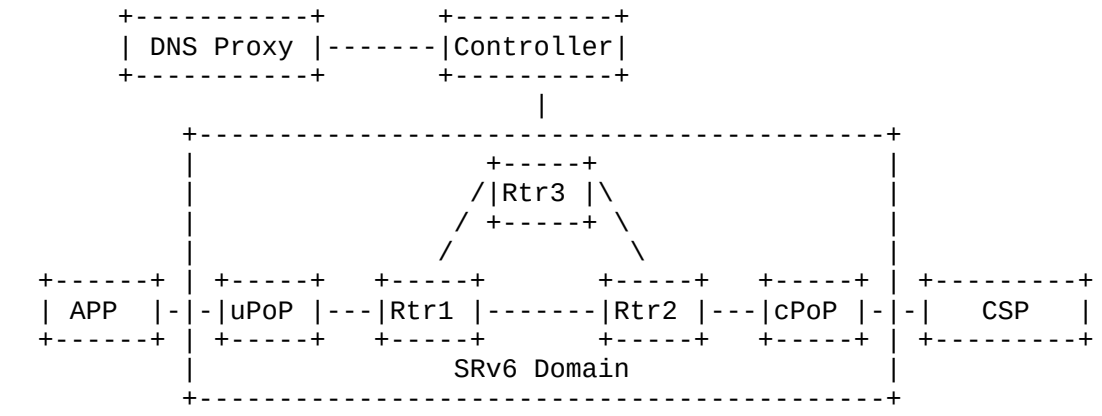

Figure 1: Architecture

4. IANA Considerations

This document has no IANA actions.

5. Security Considerations

The security requirements and mechanisms described in [RFC5625] also apply to this document.

The DNS Proxy and the controller should be deployed within a protected data center.

To minimize the impact of network attacks on the communication channel between the DNS Proxy and the controller, the DNS Proxy and the controller should not be interconnected via the Internet.

The DNS response should be carefully validated in order to avoid DDoS attack. The falsified DNS response can carry long list of application destination. One mechanism is to record all of the active DNS reqeust on DNS proxy, and only send DNS-response notification to controller ony if the DNS request has been received by the DNS proxy.

6. References

6.1. Normative References

[RFC8754] Filsfils, C., Ed., Dukes, D., Ed., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", RFC 8754, DOI 10.17487/RFC8754, March 2020, <https://www.rfc-editor.org/rfc/rfc8754>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

6.2. Informative References

[RFC5625] Bellis, R., "DNS Proxy Implementation Guidelines", BCP 152, RFC 5625, DOI 10.17487/RFC5625, August 2009, <https://www.rfc-editor.org/rfc/rfc5625>.

Author’s Address

Feng Yang
China Mobile
China

Email: yangfeng@chinamobile.com