Internet Engineering Task Force (IETF)
Request for Comments: 8354
Category: Informational
ISSN: 2070-1721
March 2018

J. Brzozowski
J. Leddy
Comcast
C. Filsfils
R. Maglione, Ed.
M. Townsley
Cisco Systems

Use Cases for IPv6 Source Packet Routing in Networking (SPRING)

Abstract

The Source Packet Routing in Networking (SPRING) architecture describes how Segment Routing can be used to steer packets through an IPv6 or MPLS network using the source routing paradigm. This document illustrates some use cases for Segment Routing in an IPv6-only environment.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Source Packet Routing in Networking (SPRING) architecture leverages the source routing paradigm. An ingress node steers a packet by including a controlled set of instructions, called segments, in the SPRING header. The SPRING architecture is described in [SEGMENT-ROUTING]. This document illustrates some use cases for SPRING / Segment Routing in an IPv6-only environment.

2. IPv6 SPRING Use Cases

The use cases described in this section do not constitute an exhaustive list of all the possible scenarios: this section only includes some of the most common envisioned deployment models for Segment Routing over IPv6 (SRv6).

In addition to the use cases described in this document, all the SPRING use cases [RFC7855] are also applicable to the SRv6 data plane.

2.1. SPRING in the Small Office

An IPv6-enabled Small Office, Home Office (SOHO) provides ample globally routed IP addresses for all devices in the SOHO. An IPv6 small office with multiple egress points and associated provider-assigned prefixes will, in turn, provide multiple IPv6 addresses to hosts. A small office performing source and destination routing [PA-MULTIHOMING] will ensure that packets exit the SOHO at the appropriate egress based on the associated delegated prefix for that link.

A SPRING-enabled SOHO provides the ability to steer traffic into a specific path from end hosts in the SOHO or from a customer edge router in the SOHO. If the selection of the source-routed path is enabled at the customer edge router, that router is responsible for classifying traffic and steering it into the correct path. If hosts in the SOHO have explicit source selection rules, classification can be based on the source address or associated network egress point, thus avoiding the need for implicit classification techniques based on Deep Packet Inspection (DPI). If the traffic is steered into a specific path by the host itself, it is important to know which networks can interpret the SPRING header. This information can be provided as part of the host configuration as a property of the configured IP address.

The ability to steer traffic to an appropriate egress or utilize a specific type of media (e.g., low power, Wi-Fi, wired, femtocell, Bluetooth, Multimedia over Coax Alliance (MoCA), HomePlug, etc.) within the home itself are obvious cases that may be of interest to an application running within a SOHO.

Steering to a specific egress point may be useful for a number of scenarios, including:

- regulatory compliance;
- performance of a particular service associated with a particular link;
- cost imposed due to data caps or per-byte charges;
- distinguishing between personal vs. work traffic in homes with one or more teleworkers; and
- provision of specific services by one ISP vs. another.

Information included in the SPRING header, whether imposed by the end host itself, a customer edge router, or within the access network of the ISP, may be of use at the far ends of the data communication as well. For example, an application running on an end host with application support in a data center can utilize the SPRING header as a channel to include information that affects its treatment within the data center itself, which allows for application-level steering and load balancing without relying upon implicit application-classification techniques at the edge of the data center. Further, as more and more application traffic is encrypted, the ability to extract (and include in the SPRING header) just enough information to enable the network and data center to load balance and steer traffic appropriately becomes more and more important.

2.2. SPRING in the Access Network

Access networks deliver a variety of types of traffic from the service provider’s network to the home environment and from the home towards the service provider’s network.

For bandwidth management or related purposes, the service provider may want to associate certain types of traffic to specific physical or logical downstream capacity pipes.

This mapping is not the same thing as classification and scheduling. In the cable access network, these pipes are represented at the Data-Over-Cable Service Interface Specification [DOCSIS] layer as different service flows, which are better identified as distinct data links. As such, creating this separation allows an operator to differentiate between different types of content and perform a variety of differing functions on these pipes, such as byte capping, regulatory compliance functions, and billing.

In a cable operator’s environment, these downstream pipes could be a DOCSIS [DOCSIS] service flow, a service group, or a specific Quadrature Amplitude Modulation (QAM) as in Annex B of [ITU.J83].

Similarly, the operator may want to map traffic from the home sent towards the service provider’s network to specific upstream capacity pipes. Information carried in a packet’s SPRING header could provide the target pipe for this specific packet. The access device would not need to know specific details about the packet to perform this mapping; instead, the access device would only need to know the interpretation of the SPRING header and how to map it to the target pipe.

2.3. SPRING in Data Center

Some data center operators are transitioning their data center infrastructure from IPv4 to native IPv6 only, in order to cope with IPv4 address depletion and to achieve larger scale. In such an environment, source routing (as enabled by SRv6) can be used to steer traffic across specific paths through the network. The specific path may also include a given function that one or more nodes in the path are requested to perform.

Additionally, one of the fundamental requirements for data center architecture is to provide scalable, isolated tenant networks. In such scenarios, Segment Routing can be used to build a construct to steer the traffic across that specific path and to identify specific nodes, tenants, and functions.

2.4. SPRING in Content Delivery Networks

The rise of online video applications and new, video-capable IP devices has led to an explosion of video traffic traversing network operator infrastructures. In the drive to reduce the capital and operational impact of the massive influx of online video traffic, as well as to extend traditional TV services to new devices and screens, network operators are increasingly turning to Content Delivery Networks (CDNs).

Several studies showed the benefits of connecting caches in a hierarchical structure following the hierarchical nature of the Internet. In a cache hierarchy, one cache establishes peering relationships with its neighbor caches. There are two types of relationships: parent and sibling. A parent cache is essentially one level up in a cache hierarchy. A sibling cache is on the same level. Multiple levels of hierarchy are commonly used in order to build an efficient cache architecture.

In an environment where each single cache system can be uniquely identified by its own IPv6 address, a list containing a sequence of the caches in a hierarchy can be built. At each node (cache) in the list, the presence of the requested content is checked. If the requested content is found at the cache (a cache hits scenario), the sequence ends even if there are more nodes in the list; otherwise, the next element in the list (the next node/cache) is examined.

2.5. SPRING in Core Networks

While the overall amount of traffic offered to the network continues to grow, and considering that multiple types of traffic with different characteristics and requirements are quickly converging over a single network architecture, the network operators are starting to face new challenges.

Some operators are currently building, or plan to build in the near future, an IPv6-only native infrastructure for their core network. These operators are also looking at the possibility to set up an explicit path based on the IPv6 source address for specific types of traffic in order to efficiently use their network infrastructure. In the case of IPv6, some operators are currently assigning or plan to assign IPv6 prefix(es) to their IPv6 customers based on regions/geography, thus the subscriber’s IPv6 prefix could be used to identify the region where the customer is located. In such an environment, the IPv6 source address could be used by the edge nodes of the network to steer traffic and forward it through a specific path other than the optimal path.

The need to set up a source-based path that goes through some specific middle/intermediate points in the network may be related to different requirements:

- The operator may want to be able to use some high-bandwidth links for a specific type of traffic (like video) and thus avoid the need for overdimensioning all the links of the network;

- The operator may want to be able to set up a specific path for delay-sensitive applications;

- o The operator may have the need to be able to select one (or multiple) specific exit point(s) at peering points when different peering points are available;

- o The operator may have the need to be able to set up a source-based path for specific services in order to be able to reach some servers hosted in some facilities that are not always reachable through the optimal path; or

- o The operator may need to be able to provision guaranteed disjoint paths (a so-called "dual-plane network") for diversity purposes.

All these scenarios would require a form of traffic engineering capabilities in an IPv6-only network environment.

3. IANA Considerations

This document has no IANA actions.

4. Security Considerations

This document presents use cases to be considered by the SPRING architecture and potential IPv6 extensions. As such, it does not introduce any security considerations. However, there are a number of security concerns with source routing at the IP layer [RFC5095]. It is expected that any solution that addresses these use cases also addresses any security concerns.

5. References

5.1. Normative References

[RFC7855] Previdi, S., Ed., Filsfils, C., Ed., Decraene, B., Litkowski, S., Horneffer, M., and R. Shakir, "Source Packet Routing in Networking (SPRING) Problem Statement and Requirements", RFC 7855, DOI 10.17487/RFC7855, May 2016, <https://www.rfc-editor.org/info/rfc7855>.

5.2. Informative References

[DOCSIS] CableLabs, "New Generation of DOCSIS Technology", October 2013, <http://www.cablelabs.com/news/new-generation-of-docsis-technology/>.

[ITU.J83] ITU-T, "Digital multi-programme systems for television, sound and data services or cable distribution", ITU-T Recommendation J.83, December 2007, <https://www.itu.int/rec/T-REC-J.83/en>.

[PA-MULTIHOMING]
Baker, F., Bowers, C., and J. Linkova, "Enterprise Multihoming using Provider-Assigned Addresses without Network Prefix Translation: Requirements and Solution", Work in Progress, draft-ietf-rtgwg-enterprise-pa-multihoming-03, February 2018.

[RFC5095] Abley, J., Savola, P., and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6", RFC 5095, DOI 10.17487/RFC5095, December 2007, <https://www.rfc-editor.org/info/rfc5095>.

[SEGMENT-ROUTING]
Filsfils, C., Previdi, S., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", Work in Progress, draft-ietf-spring-segment-routing-15, January 2018.

Acknowledgements

The authors would like to thank Brian Field, Robert Raszuk, Wes George, Eric Vyncke, Fred Baker, John G. Scudder, Adrian Farrel, Alvaro Retana, Bruno Decraene, and Yakov Rekhter for their valuable comments and inputs to this document.

Contributors

Many people contributed to this document. The authors of this document would like to thank and recognize them and their contributions. These contributors provided invaluable concepts and content for this document's creation.

Ida Leung
Independent
Email: ida@brumund.ca

Stefano Previdi
Cisco Systems
Via Del Serafico, 200
Rome 00142
Italy
Email: stefano@previdi.net

Christian Martin
Arista Networks
Email: cmartin@arista.com

Authors' Addresses

John Brzozowski
Comcast

Email: john_brzozowski@cable.comcast.com

John Leddy
Comcast

Email: John_Leddy@cable.comcast.com

Clarence Filsfils
Cisco Systems
Brussels
Belgium

Email: cfilsfil@cisco.com

Roberta Maglione (editor)
Cisco Systems
Via Torri Bianche 8
Vimercate 20871
Italy

Email: robmgl@cisco.com

Mark Townsley
Cisco Systems

Email: townsley@cisco.com