Abstract

SRm6 encodes Per-Segment Service Instructions (PSSI) in a new IPv6 option, called the PSSI Option. This document describes the PSSI Option.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 23, 2020.
1. Introduction

An SRm6 [I-D.bonica-spring-srv6-plus] path provides unidirectional connectivity from its ingress node to its egress node. While an SRm6 path can follow the least cost path from ingress to egress, it can also follow any other path.

An SRm6 path contains one or more segments. A segment provides unidirectional connectivity from its ingress node to its egress node.

SRm6 paths are programmable. They support several instruction types, including Per-Segment Service Instructions (PSSI). The following are examples of PSSIs:

- Expose a packet to a firewall policy.
- Expose a packet to a sampling policy.
PSSIs are executed at segment egress nodes and can be used to implement limited service chains. However, they do not provide an alternative to the Network Service Header (NSH) [RFC8300].

SRv6 encodes PSSIs in a new IPv6 option, called the PSSI Option. This document describes the PSSI Option.

2. 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.

3. PSSI Identifiers

PSSI Identifiers identify PSSIs. They have domain-wide significance. When a controller creates a limited service chain, also allocates a PSSI Identifier. It then distributes the following information to each node that contributes to the limited service chain:

- The PSSI Identifier.
- The PSSI that the node should execute when it receives a packet that has the PSSI Identifier encoded within it.

4. Option Format

The PSSI Option contains the following fields:

- Option Type: 8-bit selector. PSSI option. Value TBD by IANA. (Suggested value: 0x10). See Note below.
- Opt Data Len - 8-bit unsigned integer. Length of the option, in octets, excluding the Option Type and Option Length fields. This field MUST be set to 4.
- PSSI identifier - (32-bit selector). Identifies a PSSI.

The PSSI option MAY appear in any Destination Options header, regardless of whether that Destination Options header precedes a Routing header or an upper-layer header. The PSSI option MUST NOT appear in a Hop-by-hop Options header.

NOTE: The highest-order two bits of the Option Type (i.e., the "act" bits) are 00. These bits specify the action taken by a destination
node that does not recognize the option. The required action is to skip over this option and continue processing the header.

The third highest-order bit of the Option Type (i.e., the "chg" bit) is 0. This indicates that Option Data cannot be modified along the path between the packet’s source and its destination.

5. Security Considerations

The PSSI option shares many security concerns with IPv6 routing headers. In particular, any boundary filtering protecting a domain from external routing headers should also protect against external PSSI options being processed inside a domain. This occurs naturally if encapsulation is used to add routing headers to a packet. If external routing headers are allowed, then protections must also include ensuring that any provided PSSI option is properly protected, e.g. with an IPSEC AH header or other suitable means.

As with Routing headers, the security assumption within a domain is that the domain is trusted to provide, and to avoid improperly modifying, the PSSI Option.

6. ICMPv6 Considerations

SRm6 implementations MUST comply with the ICMPv6 processing rules specified in Section 2.4 of [RFC4443]. For example:

- An SRm6 implementation MUST NOT originate an ICMPv6 error message in response to another ICMPv6 error message.
- An SRm6 implementation MUST rate limit the ICMPv6 messages that it originates.

7. IANA Considerations

IANA is requested to allocate a code point from the Destination Options and Hop-by-hop Options registry (https://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml#ipv6-parameters-2). This option is called "PSSI". The "act" bits are 00 and the "chg" bit is 0. (Suggested value: 0x10).

8. Acknowledgements

Thanks to Fred Baker, Shizhang Bi and Reji Thomas for their careful review of this document.
9. Normative References

[I-D.bonica-spring-srv6-plus]
Bonica, R., Hegde, S., Kamite, Y., Alston, A., Henriques, D., Jalil, L., Halpern, J., Linkova, J., and G. Chen,
"Segment Routing Mapped To IPv6 (SRm6)", draft-bonica-
spring-srv6-plus-06 (work in progress), October 2019.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
Requirement Levels", BCP 14, RFC 2119,
DOI 10.17487/RFC2119, March 1997,

Control Message Protocol (ICMPv6) for the Internet
Protocol Version 6 (IPv6)Specification", STD 89,
RFC 4443, DOI 10.17487/RFC4443, March 2006,
<https://www.rfc-editor.org/info/rfc4443>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,

(IPv6) Specification", STD 86, RFC 8200,
DOI 10.17487/RFC8200, July 2017,

"Network Service Header (NSH)", RFC 8300,
DOI 10.17487/RFC8300, January 2018,

Authors’ Addresses

Ron Bonica
Juniper Networks
2251 Corporate Park Drive
Herndon, Virginia  20171
USA

Email: rbonica@juniper.net
Joel Halpern
Ericsson
P. O. Box 6049
Leesburg, Virginia  20178
USA
Email: joel.halpern@ericsson.com

Yuji Kamite
NTT Communications Corporation
3-4-1 Shibaura, Minato-ku
Tokyo  108-8118
Japan
Email: y.kamite@ntt.com

Tomonobu Niwa
KDDI
3-22-7, Yoyogi, Shibuya-ku
Tokyo  151-0053
JP
Email: to-niwa@kddi.com

Luay Jalil
Verizon
Richardson, Texas
USA
Email: luay.jalil@one.verizon.com

Ning So
Reliance Jio
3010 Gaylord PKWY, Suite 150
Frisco, Texas  75034
USA
Email: Ning.So@ril.com
Fengman Xu
Reliance Jio
3010 Gaylord PKWY, Suite 150
Frisco, Texas 75034
USA

Email: Fengman.Xu@ril.com

Gang Chen
Baidu
No.10 Xibeiwang East Road Haidian District
Beijing 100193
P.R. China

Email: phdgang@gmail.com

Yongqing Zhu
China Telecom
109 West Zhongshan Ave, Tianhe District
Guangzhou
P.R. China

Email: zhuyq.gd@chinatelecom.cn

Yifeng Zhou
ByteDance
Building 1, AVIC Plaza, 43 N 3rd Ring W Rd Haidian District
Beijing 100000
P.R. China

Email: yifeng.zhou@bytedance.com