The Per-Path Service Instruction (PPSI) Option
draft-bonica-6man-vpn-dest-opt-06

Abstract

SRv6+ encodes Per-Path Service Instructions (PPSI) in a new IPv6 option, called the PPSI Option. This document describes the PPSI 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 January 7, 2020.
An SRv6+ [I-D.bonica-spring-srv6-plus] path provides unidirectional connectivity from its ingress node to its egress node. While an SRv6+ path can follow the least cost path from ingress to egress, it can also follow any other path.

SRv6+ paths are encoded as IPv6 [RFC8200] header chains. When an SRv6+ ingress node receives a packet, it encapsulates the packet in an IPv6 header chain. It then forwards the encapsulated packet to the path’s egress node. When the egress node receives the packet, it processes the SRv6+ payload (i.e., the original packet).

SRv6+ paths are programmable. They support several instruction types, including Per-Path Service Instructions (PPSI). PPISIs determine how path egress nodes process SRv6+ payloads. In the
absence of a PPSI, the egress node processes SRv6+ payloads as described in [RFC8200].

The following are examples of PPSIs:

- Remove any SRv6+ encapsulation and forward the SRv6+ payload through a specified interface.
- Remove any SRv6+ encapsulation and forward the SRv6+ payload using a specified routing table.

SRv6+ encodes PPSIs in a new IPv6 option, called the PPSI Option. This document describes the PPSI Option.

PPSIs can be used to support Virtual Private Networks (VPN). Therefore, Appendix A of this document describes VPN technology and how PPSIs can be used to support a VPN.

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. PPSI Identifiers

PPSI Identifiers identify PPSIs. When a path egress node instantiates a PPSI, it also allocates a PPSI Identifier and associates the PPSI with the identifier.

PPSI Identifiers have node-local significance. This means that a path egress node must assign a unique PPSI Identifier to each PPSI that it instantiates. However, one path egress node can assign a PPSI Identifier to an instruction that it instantiates, while another path egress node can assign the same PPSI Identifier to a different PPSI that it instantiates.

4. The PPSI Option

The PPSI Option contains the following fields:

- Option Type: 8-bit selector. PPSI option. Value TBD by IANA. (Suggested value: 144). See Note below.
o 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.

o PPSI identifier - (32-bit selector). Identifies a PPSI.

The SRv6+ PPSI option MAY appear in a Destination Options header that precedes an upper-layer header. It MUST NOT appear in a Hop-by-hop Options header or in a Destination Options header that precedes a Routing header.

When the SRv6+ PPSI option appears in a Destination Options header, it MUST be the only option listed in the header. This is because the PPSI defines all path egress node behaviors.

NOTE : The highest-order two bits of the Option Type (i.e., the "act" bits) are 10. These bits specify the action taken by a destination node that does not recognize the option. The required action is to discard the packet and, regardless of whether or not the packet’s Destination Address was a multicast address, send an ICMPv6 [RFC4443] Parameter Problem, Code 2, message to the packet’s Source Address, pointing to the unrecognized Option Type.

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. Destination Option Header Considerations

As per [RFC8200], the Destination Options header includes a Next Header field. The Next Header field identifies the header following the Destination Options header.

SRv6+ can carry Ethernet payload after a Destination option header. Therefore, this document requests IANA to assign a protocol number for Ethernet. (The suggested value is 143.)

6. Security Considerations

SRv6+ domains MUST NOT span security domains. In order to enforce this requirement, security domain edge routers MUST do one of the following:

o Discard all inbound SRv6+ packets

o Authenticate [RFC4302] [RFC4303] all inbound SRv6+ packets
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 "Per-Path Service Instruction Option". The "act" bits are 10 and the "chg" bit is 0. The suggested value is 144.

IANA is also requested to allocate a code point for Ethernet from the Assigned Internet Protocol Numbers registry (https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml). The suggested value is 143.

8. Acknowledgements

Thanks to Brian Carpenter, Adrian Farrel, Tom Herbert, John Leddy and Tony Li for their comments.

9. References

9.1. Normative References

[I-D.bonica-spring-srv6-plus]


9.2. Informative References


Appendix A. Virtual Private Networks (VPN)

Virtual Private Network (VPN) technologies allow network providers to emulate private networks with shared infrastructure. For example, assume that red sites and blue sites connect to a provider network. The provider network facilitates communication among red sites and facilitates communication among blue sites. However, it prevents communication between red sites and blue sites.

The IETF has standardized many VPN technologies, including:

- Layer 2 VPN (L2VPN) [RFC6624].
- Layer 3 VPN (L3VPN) [RFC4364].
- Virtual Private LAN Service (VPLS) [RFC4761][RFC4762].
- Ethernet VPN (EVPN) [RFC7432].
- Pseudowires [RFC8077].

The above-mentioned technologies include the following components:

- Customer Edge (CE) devices.
- Provider Edge (PE) devices.
- Routing Instances.
- Service Instructions.
- Service Instruction Identifiers.
- Transport tunnels.

CE devices participate in closed communities called VPNs. CEs that participate in one VPN can communicate with one another but cannot communicate with CEs that participate in another VPN.
CE devices connect to provider networks through PE devices. Each PE maintains one Routing Instance for each VPN that it supports. A Routing Instance is a VPN specific Forwarding Information Base (FIB). In EVPN, Routing Instances are called Ethernet Virtual Instances (EVI).

Assume that one CE sends a packet through a provider network to another CE. The packet enters the provider network through an ingress PE and leaves the provider network through an egress PE. The packet may traverse one or more intermediate nodes on route from PE to PE.

When the ingress PE receives the packet, it:

- Identifies the Routing Instance that supports the originating CE’s VPN.
- Searches that Routing Instance for the packet’s destination.

If the search fails, the ingress PE discards the packet. If the search succeeds, it yields the following:

- A Service Instruction Identifier.
- The egress PE’s IP address.

The ingress PE prepends the Service Instruction Identifier and a transport header to the packet, in that order. It then forwards the packet through a transport tunnel to the egress PE.

The egress PE removes the transport header, if it has not already been removed by an upstream device. It then examines and removes the Service Instruction Identifier. Finally, it executes a service instruction that is associated with the Service Instruction Identifier. The service instruction causes the egress PE to forward the packet to its destination (i.e., a directly connected CE).

In the above-mentioned VPN technologies, the ingress PE encodes Service Instruction Identifiers in Multiprotocol Label Switching (MPLS) [RFC3031] labels. Depending upon the transport tunnel type, the transport header can be:

- A MPLS label or label stack.

Some PE devices cannot process MPLS headers. While these devices have several alternatives to MPLS-based transport tunnels, they require an alternative to MPLS-based encoding of Service Instruction Identifiers. The PPSI Option can be used to encode Service Instruction Identifiers. It is applicable when VPN payload is transported over IPv6.

Authors’ Addresses

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

Email: rbonica@juniper.net

Yuji Kamite
NTT Communications Corporation
3-4-1 Shibaura, Minato-ku
Tokyo  108-8118
Japan

Email: y.kamite@ntt.com

Chris Lenart
Verizon
22001 Loudoun County Parkway
Ashburn, Virginia  20147
USA

Email: chris.lenart@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

Greg Presbury
Hughes Network Systems
11717 Exploration Lane
Germantown, Maryland  20876
USA

Email: greg.presbury@hughes.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

Guangming Yang
China Telecom
109 West Zhongshan Ave, Tianhe District
Guangzhou
P.R. China

Email: yanggm.gd@chinatelecom.cn