Workgroup: Network Working Group
Internet-Draft: draft-liu-msr6-use-cases-01
Published: 11 July 2022
Intended Status: Informational
Expires: 12 January 2023
Authors: Y. Liu (China Mobile)
F. Yang (China Mobile)
A. Wang (China Telecom)
X. Zhang (China Unicom)
X. Geng (Huawei)
Z. Li (Huawei)

MSR6(Multicast Source Routing over IPv6) Use Cases

Abstract

MSR6 (Multicast Source Routing over IPv6) defines multicast replication as a Layer 3 function. It reuses existing IPv6 headers, functions, and capabilities to forward packets through non-multicast nodes, and adds no flow state at intermediate network nodes.

This document introduces the use cases for MSR6.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

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 12 January 2023.

Copyright Notice

Table of Contents

1. Introduction

MSR6 (Multicast Source Routing over IPv6) defines multicast replication as a Layer 3 function. It reuses existing IPv6 headers, functions, and capabilities to forward packets through non-multicast nodes, and adds no flow state at intermediate network nodes ([[I-D.cheng-spring-ipv6-msr-design-consideration]]).

MSR6 encodes a set of destination nodes or a multicast tree in an IPv6 header, which supports both BE(Best Effort) forwarding based on SPF(Shortest Path First) and TE(Traffic Engineering) forwarding based on explicit path.

MSR6 focuses on use cases with 1 or several following characteristics:

*Large network scale with Numerous multicast service;

*IPsec to guarantee security when multicast transmitting through Internet;

*Host Initiated or overlay Multicast Transport.

These characteristics also corresponds to MSR6 deployment modes introduced in [I-D.cheng-spring-ipv6-msr-design-consideration], including P2MP Multicast Tunnel, Multicast Overlay Network and Host-Initiated Multicast.

This document describes diverse use cases the MSR6 technology may be Used in different deployment modes.

2. MSR6 in DCN

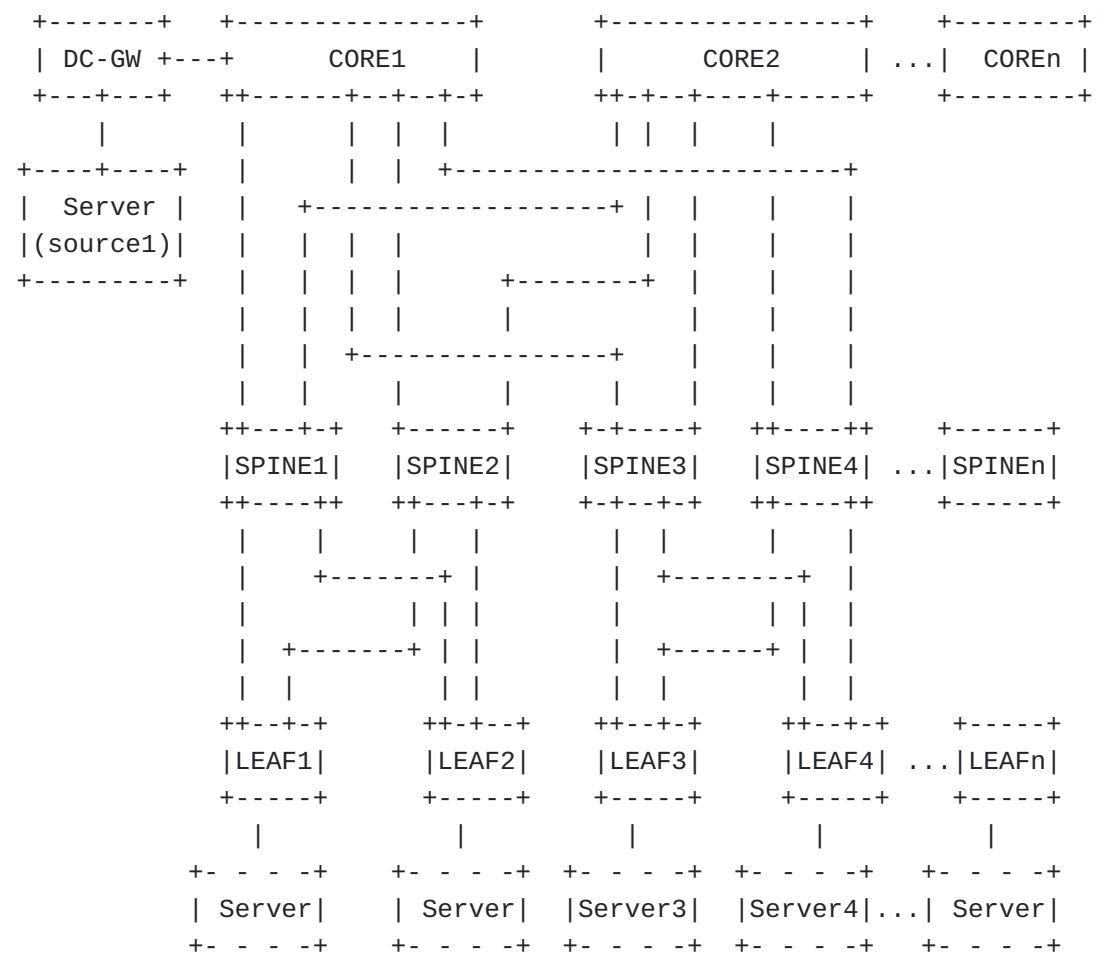
There are applications in data center with point-to-multipoint communication patterns that would benefit from network multicast service, without which, these applications, when migrating to public clouds, will use server based packet replication techniques. This leads to CPU load inflation and prevents tenants from sustaining high throughputs and low latencies for multicast workloads.

At the same time, An increasing number of organizations are adopting IPv6 in their clouds, driven by the public IPv4 space exhaustion, private IPv4 scarcity, especially within large-scale networks, and the need to provide connectivity to IPv6-only clients.

Similar as the case in DCN, MSR6 could also be used in other large scale network, like nationwide inter-AS network or large metro network. For example OTT live streaming could be conveyed in a nationwide network with multiple multicast source distributed in different areas.

2.1. Use of MSR6 TE

The following figure shows an example of a data center network with dual-homes hosts for reliability. There are about 10k swtiches, 9k of which are leaves, and 100k adjacencies.



For multicast application in DCN, multicast source could be inside DCN or outside DCN.

For example, a multicast stream could be from source1 to service 3 and server 4. The multicast tree is from DC-Gateway to LEAF3 and LEAF4, which could be presented as:

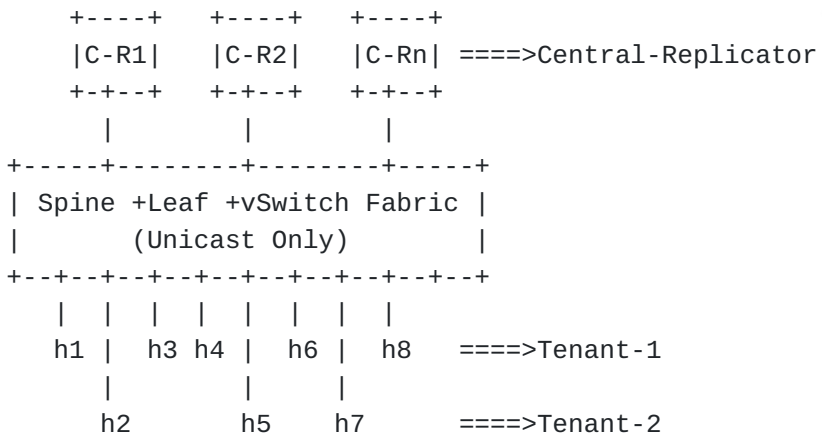
DC-GW(ingress node)-->CORE1---->SPINE3--[replicate]--->LEAF3(leaf) +LEAF4(leaf)

MSR6 could be used in Data Center Network(DCN) to provide scalable multicast solution. Only the nodes/adjacencies in the multicast tree are encoded in the packet with segment/bitstring, which decouples from network size and number of services.

2.2. Use of MSR6 BE

As illustrated in the following figure, a data-center may contain: a network fabric configured in unicast-only mode, hosts running as virtual machines (VMs) managed by tenants, central replicators (C-R)

for providing MSR6 packet delivery service among the hosts of a tenant.



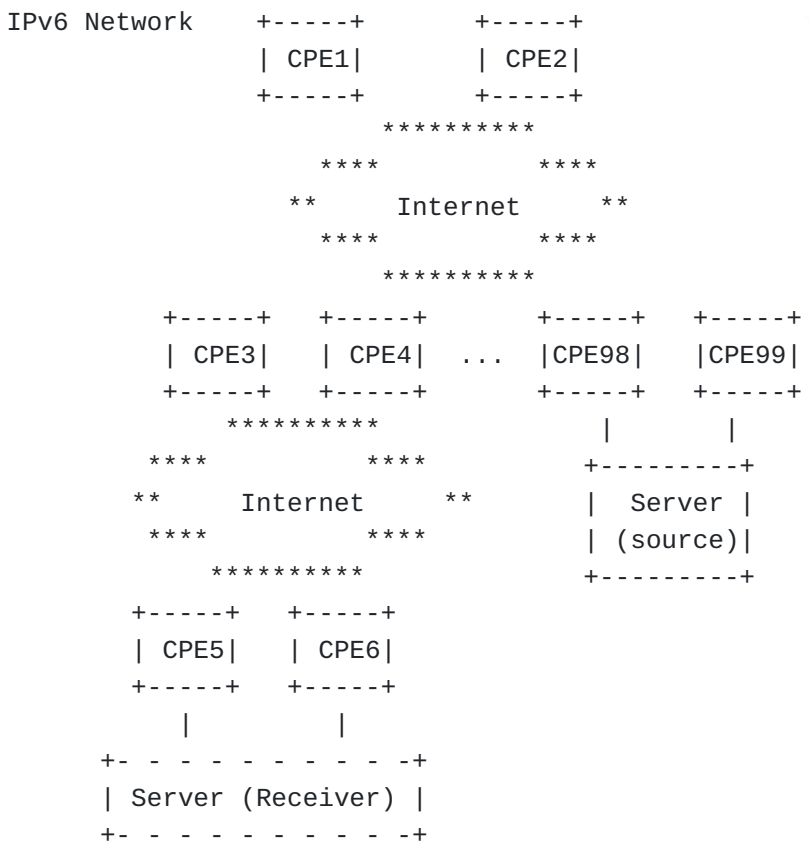
Take tenant-1 for example. The host h1 can send multicast flow using MSR6 packets to C-R1, the MSR6 packets include one or more of the destination hosts h3/h4/h6/h8 encoding in the MSR6 header. An MSR6 packet may be sent to C-R1 where it is replicated and sends to the desired destination hosts. An MSR6 packet may be sent to C-R1 where it is replicated and sends to the part of the destination hosts, and another copy to C-R2 for replication and delivery to the left destination hosts.

A Tenant may have a dedicated set of C-Rs for its own use, or a Tenant may use a shared C-Rs for its replication requirement among VMs.

3. MSR6 in SD-WAN

3.1. SD-WAN over Public Internet

SD-WAN can be deployed based on public Internet, where the underlay network is providing nothing else but a simple service normally called "Best Effort" unicast. In this case, security is one of the fundamental requiremnt in SD-WAN network. Multicast services for SD-WAN also request encryption. The following figure shows an example of SD-WAN multicast.

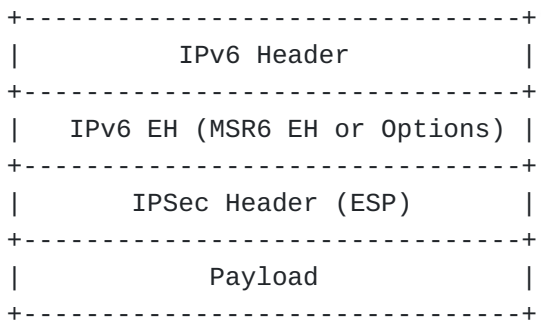


A multicast case in SD-WAN is from CE99 to CE3, CE5 and CE6. The multicast tree could presented as:

CE99(ingress node)-->CPE2--[replicate]-->CE3(leaf)+CE4--[replicate]--->CE5(leaf)+CE6(leaf)

For MSR6, which is designed based on native IPv6, it is allowed to reuse IPv6 Authentication header and Encapsulating Security Payload header.

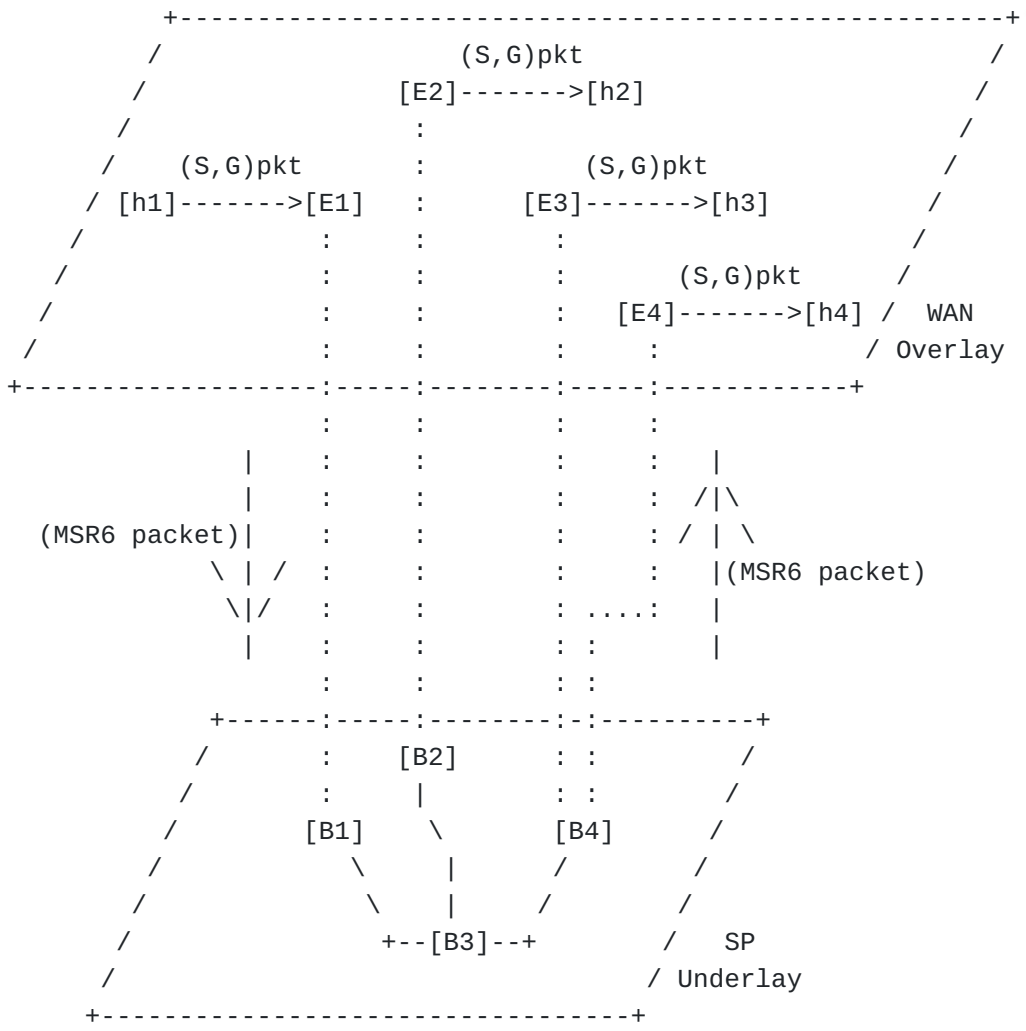
As shown in the following figure, MSR6 header, as an IPv6 extension header, will not be encrypted during the P2MP transmission. So there is no encryption and decryption between each replication nodes and its downstream nodes. Encryption and decryption only happens respectively on the MSR6 Ingress Node and MSR6 Egress node, which could increase packet processing efficiency in the intermediate nodes.



3.2. SD-WAN over Service-Provider Network

Another typical deployment mode of SD-WAN is based on a Service provider(SP) network, where the underlay network is a managed network.

As illustrated in the following figure, the MSR6 packet delivery service can enable the underlay network to provide a new service to SD-WAN.



SD-WAN Edge E1 encapsulate the received (S,G) packet into an MSR6 header, transforming the packet an MSR6 packet, and send to Service provider backbone router B1. According to the MSR6 routing and forwarding table that has pre-built for the SD-WAN, the underlay network delivery the received MSR6 packet to E2/E3/E4. E2/E3/E4 then decapsulates the outer MSR6 header, obtains the original (S,G) packet, and forward to h2/h3/h4.

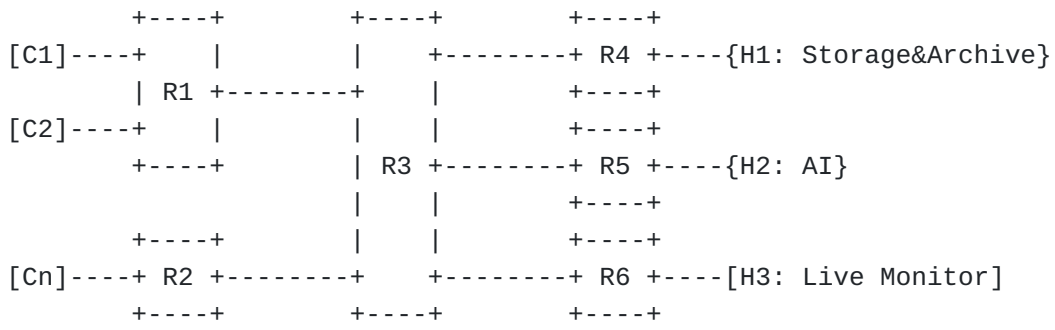
4. Host-initiated Multicast

There are some enterprise cases where the hosts and network device are managed and maintained in the same domain. MSR6 could be used to simplify multicast deployment without control plane protocol for multicast joining and leaving. The host could send/receive MSR6 packet and the network could replicate the packet based on MSR6 header.

4.1. Multicast for Surveillance Camera Data Transmission

In automated factory, surveillance cameras are usually deployed to ensure security. Data from these surveillance cameras is transmitted to different sites for analysis, processing and storage.

As illustrated in the following figure, the MSR6 packet delivery service can be used in an Industry Environment.



C1/C2/Cn: Camera
R1/R2/R3/R4/R5/R6: Router
H1/H2/H3: Host of Applications to process the camera video.

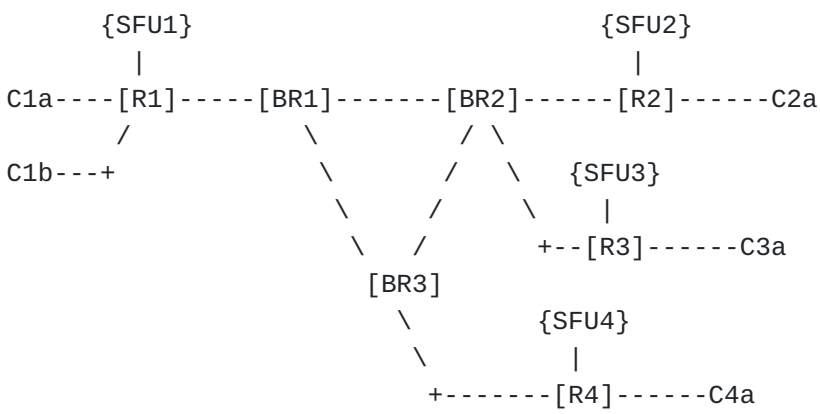
With the MSR6 packet delivery service supported by the network, the cameras can send the packet to a few applications directly by using MSR6 packets to encode the desired destination hosts of applications.

4.2. Multicast for Audio and Video Conferencing

Multicast can save bandwidth for audio and video conferencing in large enterprises. Selective Forwarding Units (SFU) [I-D.ietf-

avtcore-rtp-topologies-update], is associated centralized unit for scalable video coding and simulcasting, which could be used in audio and video conferences.

MSR6 could provide multicast among SFUs as illustrated in the following figure. In practice, these SFUs may be open Real-Time-Communication(RTC) gateways, either private RTC implementation or open RTC like WebRTC, to support WAN scope meeting.



C1x/C2a/C3a/C4a: WebRTC Client;
R1/R2/R3/R4: Router;
BR1/BR2/BR3: Backbone Router;
SFU1/SFU2/SFU3/SFU4: Selective Forwarding Unit (WebRTC Gateway);

When SFU1 receives a RTC flow packet from C1a, the next step is to forward it to one or more of SFU2, SFU3 and SFU4, depending on the RTC session established by them. The SFU1 can send the packet using MSR6 packets with the destination hosts SFU2/SFU3/SFU4 encoding in the MSR6 header. The enterprise WAN, including the edge routers R1/R2/R3 and backbone routers BR1/BR2/BR3 get the MSR6 packet multicast to its final destinations.

Using the socket API as defined in [RFC3493] and [RFC3542], it has been testd that this could work on a host operation system. Following is an illustration of code that can enable a socket to send and receive an IPv6 packet with a Destination Options Header.

```
//Code for the Sending Procedure (SFU1).
sock_fd = socket(AF_INET6, SOCK_DGRAM, IPPROTO_UDP);
setsockopt(sock_fd, IPPROTO_IPV6, IPV6_DSTOPTS, (void *)extbuf, len);

//Code for the Receiving Procedure (SFU2)
sock_fd = socket(AF_INET6, SOCK_DGRAM, IPPROTO_UDP);
setsockopt(sock_fd, IPPROTO_IPV6, IPV6_RECVDSTOPTS, &on, sizeof(on));
```

5. IANA Considerations

This document makes no request of IANA.

6. Security Considerations

TBD

7. Acknowledgements

TBD

8. Normative References

[I-D.cheng-spring-ipv6-msr-design-consideration] Cheng, W., Mishra, G., Li, Z., Wang, A., Qin, Z., and C. Fan, "Design Consideration of IPv6 Multicast Source Routing (MSR6)", Work in Progress, Internet-Draft, draft-cheng-spring-ipv6-msr-design-consideration-01, 25 October 2021, <https://www.ietf.org/archive/id/draft-cheng-spring-ipv6-msr-design-consideration-01.txt>.

[I-D.ietf-avtcore-rtp-topologies-update] Westerlund, M. and S. Wenger, "RTP Topologies", Work in Progress, Internet-Draft, draft-ietf-avtcore-rtp-topologies-update-10, 2 July 2015, <https://www.ietf.org/archive/id/draft-ietf-avtcore-rtp-topologies-update-10.txt>.

[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/info/rfc2119>.

[RFC3493] Gilligan, R., Thomson, S., Bound, J., McCann, J., and W. Stevens, "Basic Socket Interface Extensions for IPv6", RFC 3493, DOI 10.17487/RFC3493, February 2003, <https://www.rfc-editor.org/info/rfc3493>.

[RFC3542] Stevens, W., Thomas, M., Nordmark, E., and T. Jinmei, "Advanced Sockets Application Program Interface (API) for IPv6", RFC 3542, DOI 10.17487/RFC3542, May 2003, <https://www.rfc-editor.org/info/rfc3542>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

Authors' Addresses

Yisong Liu
China Mobile

Email: liuyisong@chinamobile.com

Feng Yang
China Mobile

Email: yangfeng@chinamobile.com

Aijun Wang
China Telecom

Email: wangaj3@chinatelecom.cn

Xueru Zhang
China Unicom

Email: zhangxr49@chinaunicom.cn

Xuesong Geng
Huawei

Email: gengxuesong@huawei.com

Zhenbin Li
Huawei

Email: lizhenbin@huawei.com