

SPRING Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 7, 2022

W. Jiang
W. Cheng
China Mobile
C. Lin
Y. Qiu
New H3C Technologies
March 7, 2022

Use Cases for SR Policy Group
draft-jiang-spring-sr-policy-group-use-cases-00

Abstract

Segment Routing is a source routing paradigm that explicitly indicates the forwarding path for packets at the ingress node. An SR Policy is associated with one or more candidate paths, and each candidate path is either dynamic, explicit or composite. This document illustrates some use cases for SR policy group composite candidate path in MPLS and IPv6 environment.

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 September 7, 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

Internet-Draft

SR Policy Group

March 2022

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Terminology	3
3.	SR Policy Group	3
4.	Steering into An SR Policy Group	4
5.	On-demand SR Policy Group	5
6.	SR Policy Group Use Cases	5
6.1.	SR Policy Group in L3VPN over TE Scenarios	5
6.2.	SR Policy Group in Cloud Backbone Acceleration Scenarios	6
6.3.	SR Policy Group in the L2VPN Network Scenarios	7
6.4.	SR Policy Group in the Application-aware Scenarios	8
6.5.	Application of ODN SR Policy Group in Trusted Network Scenarios	9
6.6.	Best-effort Forwarding Scenarios when SR Policy Becomes Unavailable	11
7.	IANA Considerations	11
8.	Security Considerations	11
9.	References	11
	Authors' Addresses	12

[1.](#) Introduction

Segment routing (SR) [[RFC8402](#)] is a source routing paradigm that explicitly indicates the forwarding path for packets at the ingress node. The ingress node steers packets into a specific path according to the Segment Routing policy (SR Policy) as defined in [[I-D.ietf-spring-segment-routing-policy](#)]. In order to distribute SR policies to the headend, [[I-D.ietf-idr-segment-routing-te-policy](#)] specifies a mechanism by using BGP.

An SR policy is associated with one or more candidate paths. A composite candidate path acts as a container for grouping SR policies. As described in section 2.2 in [[I-D.ietf-spring-segment-routing-policy](#)], the composite candidate path construct enables combination of SR policies, each with explicit candidate paths and/or dynamic candidate paths with potentially different optimization objectives and constraints, for load-balanced

steering of packet flows over its constituent SR policies. For service-class based steering, and in the best-effort forwarding scenario when SR policy becomes unavailable, packets are also forwarded over the constituent SR policies of composite candidate path.

This document illustrates some use cases for SR policy group composite candidate path in MPLS and IPv6 environment.

[2.](#) Terminology

The definitions of the basic terms are identical to those found in Alternate Marking [\[RFC8402\]](#).

The important new terms that need to be explained are listed below:

SR policy group: An SR policy which contains a group of constituent SR policies. An SR policy group represents a composite candidate path.

ODN: On-demand Next-Hop.

ODN SR policy: Preconfigure an ODN template specified color. When the device receives a BGP route, if the color extended attribute value of the BGP route is the same as the color value of an ODN template, the device can automatically create an SR policy.

ODN SR policy group: An SR policy group dynamically created through ODN.

[3.](#) SR Policy Group

An SR policy group is specified as a group of its constituent SR policies. It is valid when it has at least one valid constituent SR policy.

As defined in [\[I-D.ietf-spring-segment-routing-policy\]](#), The endpoints of the constituent SR policies and the parent SR policy MUST be identical, and the colors of each of the constituent SR policies and the parent SR policy MUST be different. SR policy group and its constituent SR policies follow the same criteria:

- o The endpoints of the constituent SR policies and its SR policy group MUST be identical.
- o The colors of each of the constituent SR policies and its SR policy group MUST be different.
- o The constituent SR policies MUST NOT contain SR policy groups.

As a special SR policy, SR policy group also has color attribute, which is identified by <color, endpoint> on the headend.

An SR policy can be generated by static configuration or a centralized controller distribution, also can be generated based on the on-demand SR policy optimization template dynamically.

[4.](#) Steering into An SR Policy Group

A headend can steer a packet flow into a valid SR policy group in various ways:

- o Per-flow Steering: Specify the mapping relationship between color and flow characteristics (such as DSCP) for SR policy group, and create a policy group that binds a destination IP address to the SR policy group. Upon receiving a packet with the specified destination address, the device searches for the SR policy containing the color value mapped to the flow characteristics of the packet in the SR policy group. The device will use the matching SR policy to forward the packet.

The device obtains an SR policy group for traffic steering as follows:

- * Matches the destination IP/IPv6 address in a packet with an SR policy group.
- * Searches for an SR policy group with color and endpoint address matching the color extended community attribute and next hop in a BGP route, and recurses the BGP route to the SR policy group.

The Ingress node can match flow characteristics in its ingress

interfaces (upon any field such as Ethernet destination/source/VLAN/TOS or IP destination/source/DSCP or transport ports or application attribute etc.) and color them with an internal per-packet forwarding-class variable. According to the forwarding-class variable the ingress node selects the matching SR policy in the SR policy group.

- o Policy-based Steering: incoming packets match a routing policy that directs them on an SR policy group. Parse the flow characteristics (such as DSCP/802.1p value) from the packet header, find its corresponding color, and then match it to an SR policy in the SR policy group, forward the incoming packets through the matched SR policy.

If an SR policy group has at least one valid constituent SR policy of specified color, flow load-balance steer over its valid constituent SR policies with the same color. When all constituent SR policies of specified color are invalid, packets are forwarded based on a default SR policy preconfigured.

[5.](#) On-demand SR Policy Group

SR policies are generally generated by manual static configuration or distributed by centralized controller. Manual configuration may be troublesome, especially when many SR policies need to be configured. The controller mode may also not be suitable for operators who need to make full use of distributed intelligence.

In scenarios that distinguish service forwarding paths based on DSCP value and 802.1p priority, SR policy groups can be automatically created through ODN to establish the dynamic mapping between service types and SR policy groups, which can greatly reduce the workload of configuration.

Create the ODN template of SR policy group in the headend. When the device receives a BGP route, if the color extended community attribute carried by the BGP route is the same as the color value of the ODN template, the next hop address of the BGP route is used as the destination endpoint address of the SR policy group, and the color value of the ODN template is used as the color attribute of the SR policy group to generate an SR policy group.

After the SR policy group is created by ODN, its constituent SR policy is usually generated by ODN. ODN SR policy dynamically generates candidate paths through affinity attributes, flex algo algorithm or PCE calculation.

6. SR Policy Group 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 SR policy group.

6.1. SR Policy Group in L3VPN over TE Scenarios

In Figure 1, CE1 and CE2 belong to the same L3VPN and access the public network through PE1 and PE2 respectively. There are many kinds of traffic between CE1 and CE2. When the ordinary traffic is too large, the forwarding of important traffic will be affected.

In order to ensure the forwarding quality of important services, the steering based on Forwarding class can be configured using SR policy group. After the steering based on forwarding class is configured, the traffic of different service levels will be carried by the specified SR policy tunnel, which can effectively ensure the forwarding quality of important services with high service levels.

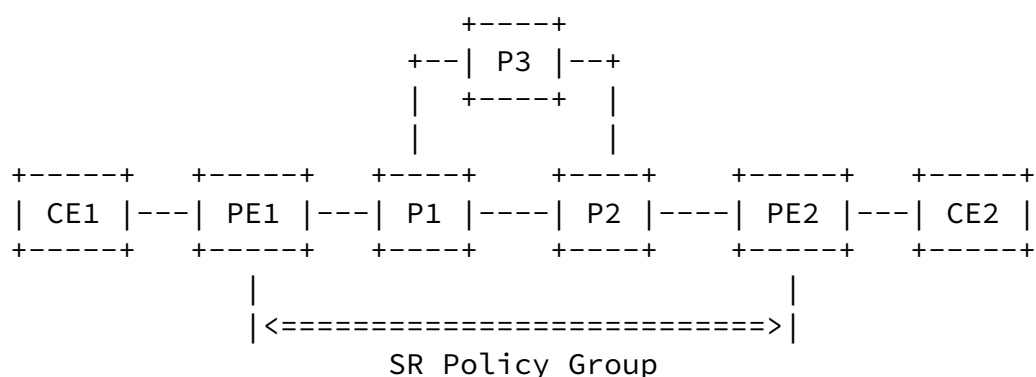


Figure 1

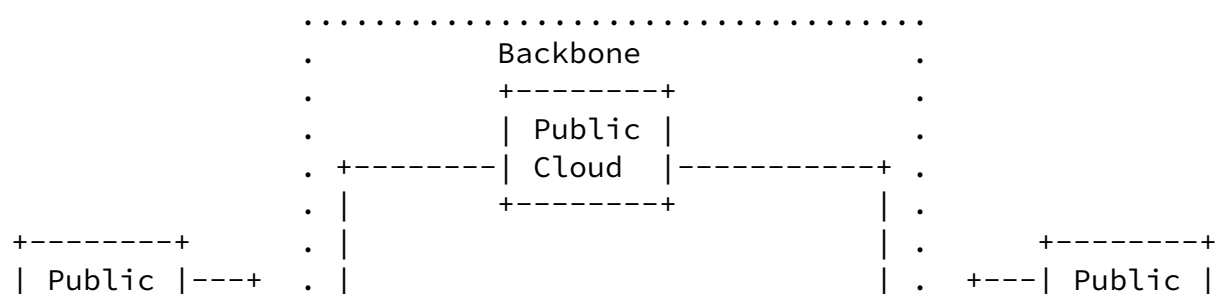
It is assumed that in this network, the policy group contains three constituent policies: Policy-A, Policy-B and Policy-C. Services with

different forwarding class will carry different DSCP values in the packet. Identify the customer's service through DSCP on PE1. The voice traffic of VIP customers is forwarded according to the path of low-delay Policy-A, other traffic of VIP customers is forwarded according to the path of Policy-B, and all businesses of non VIP customers are carried by Policy-C.

6.2. SR Policy Group in Cloud Backbone Acceleration Scenarios

As shown in Figure 2, multiple cloud data centers are interconnected through cloud backbone networks. In the public cloud, there are different SLA requirements for different service types, such as voice service and cloud disk. Deploy a static SR policy group on the core of the cloud backbone network to prevent network congestion. There are multiple SR policies in the SR policy group.

In order to ensure the service quality of different types of services, the service types are distinguished by flow classification, then different services are mapped to different DSCP value, and finally the traffic of different DSCP is imported into different SR policies.



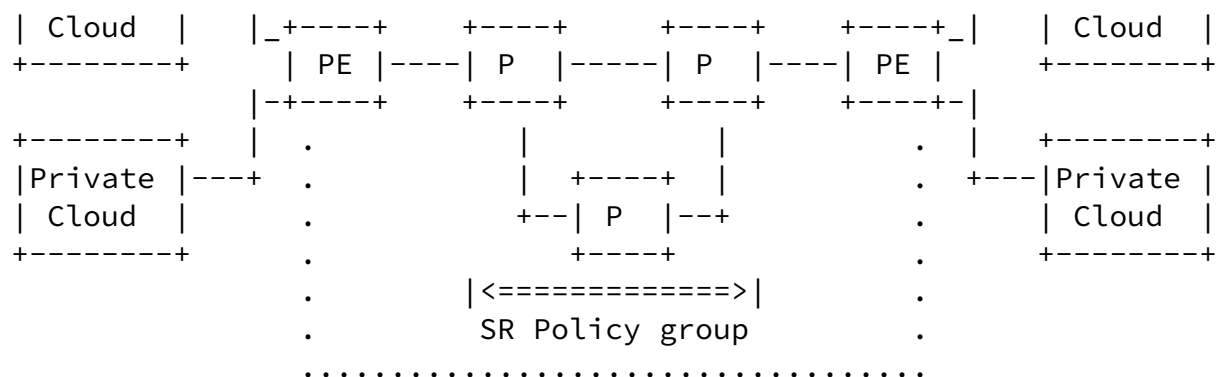


Figure 2

Through the SR policy group, different forwarding paths can be introduced based on the DSCP value in the IP/IPv6 packet header.

First, create an SR policy group and assign color identification to the SR policy group.

Then, configure multiple SR policies into one SR policy group in the headend, specify the mapping relationship between each SR policy and DSCP value in the SR policy group, and then bind the service type to the specified SR policy group.

In this way, when the headend receives traffic, it first matches to the SR policy group according to the next hop and color of the route, and then finds the mapped SR policy in the corresponding group according to the DSCP value carried in the IP/IPv6 packet header.

DSCP based steering is suitable for differentiating services at the source and specifying different DSCP value scenarios.

6.3. SR Policy Group in the L2VPN Network Scenarios

Similar to the DSCP-based steering scenario, in the layer 2 access network and L2VPN network, the service types are distinguished by the 802.1p priority in the packet header, and the 802.1p priority is mapped to color in the SR policy group. Different services can be forwarded into different paths.

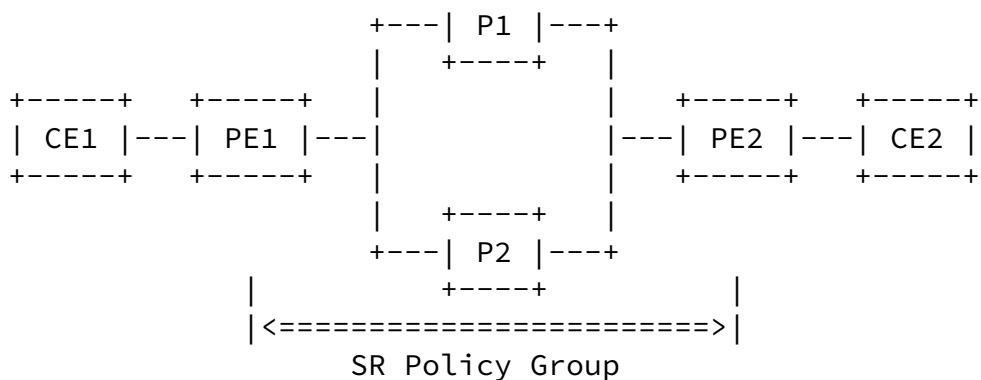


Figure 3

As shown in Figure 3, CE1 and CE2 belong to the same VPLS and are connected to the MPLS backbone network through PE1 and PE2 respectively. Establish two MPLS-SR policy tunnels Policy-A and Policy-B between PE1 and PE2 to carry this VPLS service. Policy-A and Policy-B are the constituent policies of SR policy group. Two SR policy tunnels correspond to two different priorities. The VPLS access end classifies the traffic flow, trusts the priority of 802.1p, and introduces the services of VPLS leased line users and non-leased line users into different SR policy according to different priorities.

6.4. SR Policy Group in the Application-aware Scenarios

By carrying the application attribute (including APP ID and APP parameters) through data packets, i.e., the delivery of application-aware information and ensuring the security and reliability of application-aware information, the network senses the application groups' requirements and provides high-quality differentiated services according to the demand of the applications. And when the network transmits the data packets, it matches the SR policy according to the application attribute in the data packets and selects the corresponding path of constituent SRv6 policy to transmit the data packets (e.g., low latency path) to meet the SLA requirements and service chain in order to improve the service quality.

As shown in Figure 4 below, the policy group contains three constituent SR policies: Policy-A, Policy-B and Policy-C. The data packets of APP1 are forwarded by Policy-A, the data packets of APP2 are forwarded by Policy-B, and the data packets of APP3 are forwarded by Policy-C.

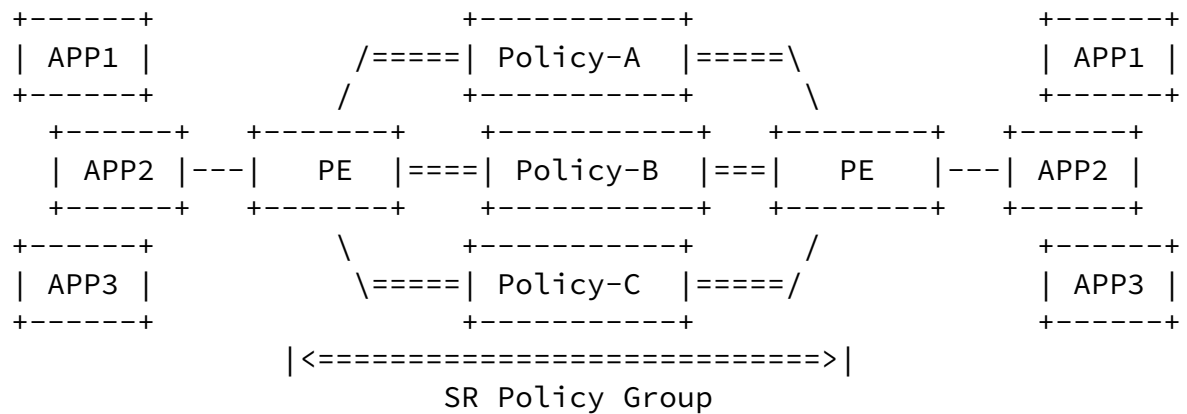


Figure 4

6.5. Application of ODN SR Policy Group in Trusted Network Scenarios

Section 3 of [[I-D.lin-opsec-trustroute-problem-statement](#)] introduces the use case of trusted network. By dynamically creating SR policy through ODN, automatic steering traffic according to security level can be realized.

From the perspective of security and trustworthiness, the security levels for users with different security requirements and the trustworthiness levels of the network transmission devices can be determined according to their performance and reliability. Different forwarding paths are provided for packets with different security levels.

Internet-Draft

SR Policy Group

March 2022

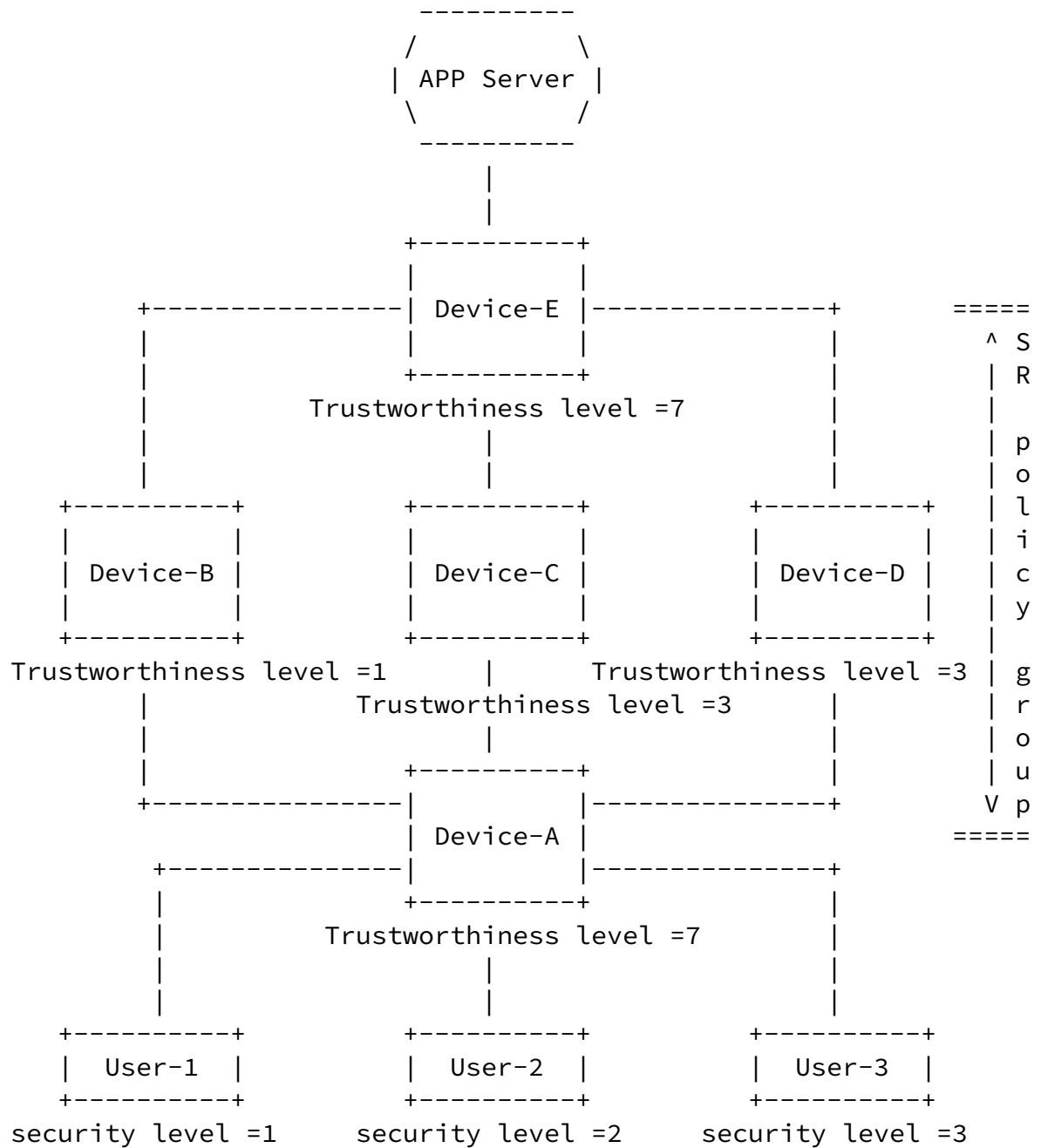


Figure 5

As shown in Figure 5, the trustworthiness level is configured on each

network transmission device.

Device-E colors the advertised BGP routes through the color extended community attribute, and different services correspond to different colors.

When Device-A receives a BGP route with color C1 and endpoint E, device a will automatically generate an SR policy group (C1, E) according to the ODN template of color C1.

The composition SR policy of SR policy group is also generated according to ODN template. DSCP1 is mapped to color C2. After creating an SR policy group (C1, E), Device-A generates an ODN SR policy (C2, E) according to the mapping relationship between DSCP and color (DSCP1->C2).

Services with different security levels use different DSCPs. When the user generates a service packet, it carries the corresponding DSCP value (DSCP1) on the IPv6 packet header, and sends it to the Device-A. After receiving the service packet, the service packet is steered according to SR policy (C2, E).

[6.6.](#) Best-effort Forwarding Scenarios when SR Policy Becomes Unavailable

When all the constituent SR policies in the SR policy group are not valid, or all the selected paths of the SR policy are unavailable, the service traffic will not be forwarded according to the specified path. At this time, the best-effort forwarding path can be configured for the SR policy group, and the endpoints through which traffic forwarding must pass can be designed in the best-effort forwarding path.

During network deployment, The best-effort forwarding path can be a default SR policy or an SR BE forwarding path. Specify an best-effort forwarding path in the SR policy group. When all specified candidate paths are invalid, or the mapping relationship corresponding to their service type is not matched in the SR policy group, select the default best-effort path forwarding.

[7.](#) IANA Considerations

This document has no IANA actions.

8. Security Considerations

This document presents use cases to be considered by the deployment of SR Policy. It does not introduce any security considerations.

9. References

[I-D.ietf-idr-segment-routing-te-policy]

Previdi, S., Filsfils, C., Talaulikar, Ed., K., Mattes, P., Jain, D., and S. Lin, "Advertising Segment Routing Policies in BGP", [draft-ietf-idr-segment-routing-te-policy-14](#) (work in progress), November 2021.

Jiang, et al.

Expires September 7, 2022

[Page 11]

Internet-Draft

SR Policy Group

March 2022

[I-D.ietf-spring-segment-routing-policy]

Filsfils, C., Talaulikar, Ed., K., Voyer, D., Bogdanov, A., and P. Mattes, "Segment Routing Policy Architecture", [draft-ietf-spring-segment-routing-policy-18](#) (work in progress), February 2022.

[I-D.lin-opsec-trustroute-problem-statement]

Lin, T., Li, H., Shi, X., Yin, X., and W. Chen, "Problem Statement and Use Cases of Trustworthiness-based Routing", [draft-lin-opsec-trustroute-problem-statement-01](#) (work in progress), December 2021.

[RFC8402]

Filsfils, C., Ed., Prevdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", [RFC 8402](#), DOI 10.17487/RFC8402, July 2018, <<https://www.rfc-editor.org/info/rfc8402>>.

Authors' Addresses

Wenying Jiang
China Mobile

Email: jiangwenying@chinamobile.com

Weiqiang Cheng
China Mobile

Email: chengweiqiang@chinamobile.com

Changwang Lin
New H3C Technologies

Email: linchangwang.04414@h3c.com

Yuanxiang Qiu
New H3C Technologies

Email: qiuyuanxiang@h3c.com