SPRING Working Group
Internet Draft
Intended status: Informational
Expires: July 16, 2026

W. Cheng
W. Jiang
China Mobile
C. Lin
New H3C Technologies
R.Chen
ZTE Corporation
Y.Zhang
Huawei Technologies
January 14, 2026

SR Policy Group
draft-ietf-spring-sr-policy-group-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 describes SR Policy Group in MPLS and IPv6 environments and illustrates some use cases for parent SR Policy and SR Policy Group to provide best practice cases for operators.

Status of this Memo

Copyright Notice

Table of Contents

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 [RFC9256]. In order to distribute SR Policies to the headend, [RFC9830] 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 [RFC9256], 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 convenience, the composite candidate path formed by the combination of SR Policies is called Parent SR Policy.

In a multi-site VPN scenario, there are multiple types of service traffic between each pair of nodes. These traffics need to be forwarded on SR Policy paths with different Service Level Agreements (SLA). Due to the similarity in service forwarding models between different nodes, the configurations of each node are also very similar. However, configuring SR Policy forwarding paths for various services on each ingress node might prove to be a tedious task.

This document describes SR Policy Group in MPLS and IPv6 environments and illustrates some use cases for parent SR Policy and SR Policy Group to simplify deployment and provide best practice cases for operators.

2. Terminology

The definitions of the basic terms are identical to those found in Segment Routing Architecture [RFC8402], Segment Routing Policy Architecture [RFC9256].

SR Policy As described in [RFC9256], the general concept of SR Policy provides a framework that enables the instantiation of an ordered list of segments on a node for implementing a source routing policy for the steering of traffic for a specific purpose (e.g., for a specific Service Level Agreement (SLA)) from that node. An SR Policy is a forwarding path that meets the specified forwarding requirements.

Parent SR Policy A Parent SR Policy is the composite candidate path that acts as a container for grouping SR Policies which meet different service optimization objectives and constraints and have the same destination endpoint.

SR Policy Group: An SR Policy Group is an instantiation of a group of constituent Parent SR Policies to different destination endpoints with the same service forwarding model. It establishes the mapping relationship between the flow characteristics and the color value of the SR Policy, and guide the flows with different SLA requirements to the SR Policy with different colors.

3. Overview

An SR Policy Group is associated with one or more constituent Parent SR Policies. The hierarchical relationship between SR Policy group, Parent SR Policy and SR Policy is shown in the figure below.

```
                                                  Paths for different
                          Service forwarding              SLAs
                          model to specified        +------------------+
                               endpoint             |  SR Policy POL1 |
                            +------------+    +---->|   (Service-1)   |
                            | Parent SR  |    |     |  (Color=100,E2) |
                        +-->|Policy PP-1 |    |     +------------------+
                        |   |(Color=1,E1)|    |     +------------------+
                        |   +------------+    |     |  SR Policy POL2 |
        Service        |   +------------+    |---->|   (Service-2)  |
   forwarding model |    | Parent SR  |    |     |  (Color=200,E2) |
     +---------+      |-->|Policy PP-2 +---->+     +------------------+
     |SR Policy|      |   |(Color=1,E2)|    |     +------------------+
     |  Group  +--->|   +------------+    |     |  SR Policy POL3 |
     |  PG-1   |      |   +------------+    |     |   (Service-3)  |
     |(Color=1)|      |   | Parent SR  |    |---->|  (Color=300,E2) |
     +---------+      |-->|Policy PP-3 |    |     +------------------+
                        |   |(Color=1,E3)|    |              .
                        |   +------------+    |              .
                        |         .           |     +------------------+
                        |         .           |     |  SR Policy POLm |
                        |   +------------+    +---->|   (Service-m)  |
                        |   | Parent SR  |          |  (Color=XXX,E2) |
                        +-->|Policy PP-n |          +------------------+
                            |(Color=1,En)|
                            +------------+
```

Figure 1 Hierarchical Relationship of SR Policy

The parent SR Policy can be generated through static configuration, or dynamically generated when the destination endpoint accesses based on the service forwarding requirements specified by the SR Policy group.

The following criteria apply for inclusion of constituent Parent SR Policies under a SR Policy Group:

* A SR Policy Group contains one or more Parent SR Policies.

* The colors of SR Policy group and its each constituent Parent SR Policy MUST be identical.

* The colors of SR Policy group and its each constituent SR Policy of echo constituent Parent SR Policies MUST be different.

* There can only be one Parent SR Policy with the same source endpoint and the same destination endpoint in the SR Policy group.

4. Parent SR Policy

An SR Policy is associated with one or more candidate paths. According to section 2.2 of [RFC9256] a parent SR Policy is the composite candidate path that acts as a container for grouping SR Policies. The parent SR Policy is valid when it has at least one valid constituent SR Policy.

As defined in [RFC9256], 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. Parent SR Policy and its constituent SR Policies follow the same criteria:

* The endpoints of the constituent SR Policies and its parent SR Policy MUST be identical.

* The colors of each of the constituent SR Policies and its parent SR Policy MUST be different.

* The constituent SR Policies MUST NOT contain parent SR Policy.

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

If a parent SR Policy 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 the constituent SR Policies of specified color are invalid, a default path (such as a BE path, an SR Policy path, or a composite SR Policy path of another color) can be preconfigured to forward packets according to requirements. The parent SR Policy MAY also enable Drop-Upon-Invalid behavior, and the action is the same as the Drop-Upon-Invalid behavior of the SR Policy described in Section 8.2 of [RFC9256]. This would entail the following:

* A parent SR Policy with an action to drop is kept in the forwarding plane.

* Any steering of a service (PW), destination (BGP-VPN), flow, or packet on the related parent SR Policy is maintained with the action to drop all of this traffic.

The parent SR Policy can be well used for the following scenarios

* Point-to-point leased line customers have multiple services.

* These services need to be forwarded through different SR Policy paths with different SLAs.

5. SR Policy Group

An SR Policy Group is an instantiation of a group of constituent Parent SR Policies to different destination endpoints with the same service forwarding model and represents a composite candidate path defined in [RFC9256]. It implements a source routing policy to steer the service traffic from different source endpoints for a specific purpose (e.g., for a specific SLA). Based on the Parent SR Policy described in Section 3, a SR Policy Group can be built.

According to the service quality requirements, a unified service forwarding model is planned for nodes to determine the forwarding path of service flow. The traffic with the same service forwarding model from different source endpoints to different destination endpoints uses the same SR Policy Group.

An SR Policy Group is identified by <color> on the headend, same with an SR Policy. The color is an unsigned non-zero 32-bit integer value that associates the SR Policy Group with a service forwarding model (e.g., A set of SLA attributes). Different service qualities use different Color values.

The color value identifying the SR Policy Group corresponds to the Color attribute of the BGP route published by the endpoint. The destination endpoint publishes the BGP route and indicates which SR Policy Group path the headend should use to send packets to it through the Color attribute in the route.

In the Policy Group, establish the mapping relationship between the flow characteristics and the color value of the SR Policy path, and guide the service flows with different SLA requirements to the SR Policy path with different colors.

By SR Policy Group, in the multi-site VPN scenario described in Section 1, we can:

* Simply deployment.

* Effectively solve the problem of complex configuration in multi-point scenarios.

6. Steering into SR Policy Group

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

* Per-flow Steering: Specify the mapping relationship between color and flow characteristics (such as DSCP) for SR Policy group, and create a parent SR Policy that binds a specified destination endpoint address on the ingress node according the SR Policy group. Upon receiving a packet with the specified destination address, the ingress node searches for the SR Policy containing the color value mapped to the flow characteristics of the packet in the parent SR Policy. The ingress node will use the matching SR Policy to forward the packet.

  The ingress node obtains a parent SR Policy for traffic steering as follows:

  - The destination endpoint publishes a BGP route with the specified Color extended community attribute.

  - Get the color extended community attribute in the received BGP route.

  - Match the color attribute value of the received BGP route with the SR Policy Group.

  - Searches for a SR Policy Group with color matching the color extended community attribute.

  - Searches for a Parent SR Policy with endpoint address matching the next hop in the BGP route, and recurses the BGP route to the parent SR Policy.

  - If the corresponding Parent SR Policy is not found, it can be handled according to the CO flags, as per section 8.8 of [RFC 9256].

  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 parent SR Policy.

* Policy-based Steering: incoming packets match a routing policy that directs them on a parent SR Policy. 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 parent SR Policy, forward the incoming packets through the matched SR Policy.

Note: Since the SR Policy Group forwards traffic based on flow characteristics to the corresponding SR Policy, the weights of different SR Policies under the same parent SR Policy are no longer effective. However, within the same SR Policy, load balancing can still be achieved based on the weights of different segment lists.

An SR Policy Group can be instantiated with SR Policies which are associated with different set of network resources (i.e., NRPs). Based on SR Policy Group, it is also a network slice deployment scheme for single user and multiple services. When different services are forwarded through different SR Policy paths, different network resources can be used. After associating the SR Policy with the network slice, different network slices can be used for forwarding different traffic of the same user.

When all constituent SR Policies in the parent SR Policy are invalid, or all selected paths are unavailable, service traffic will not be forwarded as specified. In this case, a best-effort forwarding path can be configured for the parent SR Policy, allowing the design of necessary endpoints for traffic traversal. Note that if a constituent or parent SR Policy exhibits the Drop-Upon-Invalid behavior, it remains valid, following the guidelines in Section 8.2 of [RFC9256].

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

7. Information Model of SR Policy Group

In summary, the information model is the following:

```
SR Policy Group PG-1 <Color = 1>

  Parent SR Policy PP-1<Color = 1, Endpoint = E1>

    Service Service-1 mapping-to color 100
```

```
         Service Service-2 mapping-to color 200

         Service Service-3 mapping-to color 300

           SR Policy POL1 <Headend = H1, Color = 100, Endpoint = E1>
              Candidate Path CP1 <Protocol-Origin = 20, Originator =
              64511:192.0.2.1, Discriminator = 1>
              Preference 200
              Priority 10
               Segment List 1 <SID11...SID1i>

           SR Policy POL2 <Headend = H1, Color = 200, Endpoint = E1>
              Candidate Path CP1 <Protocol-Origin = 20, Originator =
              64511:192.0.2.1, Discriminator = 2>
              Preference 200
              Priority 10
                Segment List 1 <SID21...SID2i>

           SR Policy POL3 <Headend = H1, Color = 300, Endpoint = E1>
              Candidate Path CP1 <Protocol-Origin = 20, Originator =
              64511:192.0.2.1, Discriminator = 3>
              Preference 200
              Priority 10
                Segment List 1 <SID31...SID3i>

       Parent SR Policy PP-2<Color = 1, Endpoint = E2>

         Service Service-1 mapping-to color 100

         Service Service-2 mapping-to color 200

         Service Service-3 mapping-to color 300

           SR Policy POL4 <Headend = H1, Color = 100, Endpoint = E2>
              Candidate Path CP1 <Protocol-Origin = 20, Originator =
              64511:192.0.2.1, Discriminator = 4>
              Preference 200
              Priority 10
               Segment List 1 <SID41...SID4i>
```

```
          SR Policy POL5 <Headend = H1, Color = 200, Endpoint = E2>
              Candidate Path CP1 <Protocol-Origin = 20, Originator =
              64511:192.0.2.1, Discriminator = 5>
              Preference 200
              Priority 10
                Segment List 1 <SID51...SID5i>

           SR Policy POL6 <Headend = H1, Color = 300, Endpoint = E1>
              Candidate Path CP1 <Protocol-Origin = 20, Originator =
              64511:192.0.2.1, Discriminator = 6>
              Preference 200
              Priority 10
                Segment List 1 <SID61...SID6i>
```

The SR Policy Group PG-1 is identified by color. It has two constituent Parent SR Policies: PP-1 and PP-2. Each is identified by a tuple <Headend, Color, Endpoint>.

The SR Parent Policy PP-1 is identified by the tuple <Headend = H1, Color = 1, Endpoint = E1>. It has three constituent SR Policies: SR Policy POL1 SR Policy POL2 and SR Policy POL3.

The SR Policy POL1 is identified by the tuple <Headend = H1, Color = 100, Endpoint = E1>. It has one candidate paths: CP1.

The SR Policy POL2 is identified by the tuple <Headend = H1, Color = 200, Endpoint = E1>. It has one candidate paths: CP1.

The SR Policy POL3 is identified by the tuple <Headend = H1, Color = 300, Endpoint = E1>. It has one candidate paths: CP1.

The SR Parent Policy PP-2 is identified by the tuple <Headend = H1, Color = 1, Endpoint = E2>. It has three constituent SR Policies: SR Policy POL4 SR Policy POL5 and SR Policy POL6.

The SR Policy POL4 is identified by the tuple <Headend = H1, Color = 100, Endpoint = E2>. It has one candidate paths: CP1.

The SR Policy POL2 is identified by the tuple <Headend = H1, Color = 200, Endpoint = E2>. It has one candidate paths: CP1.

The SR Policy POL6 is identified by the tuple <Headend = H1, Color = 300, Endpoint = E2>. It has one candidate paths: CP1.

According to the service forwarding quality requirements, three forwarding paths (Color 100, 200, and 300) are planned.

The service forwarding model of PP-1 is adopted for the destination endpoint E1. According to service characteristics services to E1 are divided into three categories: service-1, service-2, and service-3. The service-1 service is forwarded according to the SR Policy POL1 path of Color 100. The service-2 service is forwarded according to the SR Policy POL2 path of Color 200. The services of service-3 are forwarded according to the SR Policy POL3 path of Color 300.

The destination endpoint E2 also uses the same service forwarding model. The traffic to E2 is differentiated in the same way, and the traffic is sent to E2 according to the SR Policy path of Color 100, 200, and 300.

8. Use Cases

8.1 Parent SR Policy in L3VPN over TE Scenarios

In Figure 2, 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 parent SR Policy. 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.

```
                          +----+
                       +--| P3 |--+
                       |  +----+  |
                       |          |
      +-----+   +-----+   +----+    +----+    +-----+   +-----+
      | CE1 |---| PE1 |---| P1 |----| P2 |----| PE2 |---| CE2 |
      +-----+   +-----+   +----+    +----+    +-----+   +-----+
                   |                              |
                   |<============================>|
                          Parent SR Policy
                   Figure 2 L3VPN over TE Scenario
```

It is assumed that in this network, the parent SR Policy 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.

8.2 SR Policy Group in Multi-VPN Tenants Scenarios

In the L3VPN over TE application scenario shown in Figure 3, multi-VPN tenants are connected to the SRv6 network. Controller defines SR Policy Group for each VPN tenant to achieve different forwarding path resource between tenants.

Different VPNs use different SR Policy Groups with different colors. The ingress node generates different parent SRv6 policies as required according to the destination endpoint address dynamically. Since user’s traffic of different services between two endpoints has different requirements for forwarding quality, identify the service type according to the DSCP of the packet, and steer the flow to the corresponding SR Policy path. The path constituting the SR Policy is calculated by the controller and distributed to the ingress node.

```
                             +------------+
                             | Controller |
                             +------------+
                         /                    \
                        /                      \
          ----.        /                        \         .----.
        ( VPN1 )\     /                          \      /( VPN1 )
         '----'  \ +---+     +---+     +---+     +---+ /  '----'
                   + A +-----+ B +-----+ C +-----+ D +
                   /+-+-+     +-+-+     +-+-+     +-+-+
         .----.  /   |         |         |         |
        ( VPN2 )/    |         |         |         |      .----.
         '----'      |         |         |         |    /( VPN1 )
                   +-+-+     +-+-+     +-+-+     +-+-+ /  '----'
                   + E |-----+ F +-----+ G +-----+ H +
         .----.  / +---+     +---+     +-+-+     +---+ \  .----.
        ( VPN2 )/                                       \( VPN2 )
         '----'                                           '----'
```

Figure 3 L3VPN over TE application scenario

VPN1 uses SR Policy group 1 identified by Color 100. Plan the forwarding path for VPN1 traffic, and allocate different sets of network resources for forwarding paths as blow:

* Service-1: Voice service. Low delay forwarding is required, and the DSCP range of the packet is 1~10. The controller calculates the low delay path for the voice traffic, and maps the DSCP 1~10 to Color 500. The voice traffic is forwarded through the constituent SR Policy (Color 500) of the Parent SRv6 Policy (Color 100) corresponding to VPN1.

* Service-2: Video service. The DSCP range of the packet is 11~20, and low delay is not required. However, compared with the traffic of ordinary users, the Video traffic should be forwarded first. The controller calculates the SR Policy path and maps the DSCP 11~20 to Color 501. Video traffic is forwarded along the constituent SR Policy (Color 501) of the Parent SRv6 policy (color 100) corresponding to VPN1.

* Service-3: Non voice and video services. Low latency forwarding and priority forwarding are not required. The controller calculates the SR Policy path and maps all DSCP values outside the range of 1 to 20 to Color 502. Non voice and video traffic is forwarded along the constituent SR Policy (Color 502) of the Parent SRv6 policy (color 100) corresponding to VPN1.

```
                          SRv6 Network
                       +-------------------+
         .-------.     |                   |      .-------.
        /         \ <==|=====Service-1=====|==>  /         \
       (   VPN1    )<==|=====Service-2=====|==> (    VPN1   )
        \         / <==|=====Service-3=====|==>  \         /
         '-------'     |                   |      '-------'
                       | SR Policy Group 1 |
                       |   (Color 100)     |
                       +-------------------+
```

Figure 4 SR Policy Group for VPN1

The traffic of VPN1 from A to D of Service-1 will be forwarded based on the SR Policy (Headend=A, Color=500, Endpoint=D) of Parent SR Policy (Color=100, Endpoint=D) of SR Policy Group1.

Similarly, the traffic of VPN1 from A to H of Service-1 will be forwarded based on the SR Policy (Headend=A, Color=500, Endpoint=H) of Parent SR Policy (Color=100, Endpoint=H) of SR Policy Group1.

VPN2 uses SR Policy Group 2 identified by Color 101. Plan the forwarding path for VPN2 traffic. Different sets of network resources are further allocated for the forwarding paths as blow:

* Service-4: Voice service. Low latency forwarding is required. The DSCP range of the packet is 1 to 10. The controller calculates the low delay path for voice service and maps the DSCP 1~10 to Color 600. The voice traffic is forwarded through the constituent SR Policy (Color 600) of the Parent SRv6 Policy (color 101) corresponding to VPN2.

* Service-5: Non voice services. No special forwarding quality requirements. The controller calculates the SR Policy path and maps all DSCP values outside the range of 1 to 10 to Color 601. Non voice service messages are forwarded along the constituent SR Policy (Color 601) of the Parent SR Policy (color 101) corresponding to VPN2.

```
                          SRv6 Network
                       +-------------------+
         .-------.     |                   |     .-------.
        /         \ <==|=====Service-4=====|==>  /         \
       (   VPN2    )   |                   |    (    VPN2   )
        \         / <==|=====Service-5=====|==>  \         /
         '-------'     |                   |     '-------'
                       | SR Policy Group 2 |
                       |   (Color 101)     |
                       +-------------------+
```

Figure 5 SR Policy Group for VPN2

The traffic of VPN2 from A to H of Service-4 will be forwarded based on the SR Policy (Headend=A, Color=600, Endpoint=H) of Parent SR Policy (Color=101, Endpoint=H) of SR Policy Group2.

Similarly, the traffic of VPN2 from A to E of Service-1 will be forwarded based on the SR Policy (Headend=A, Color=600, Endpoint=E) of Parent SR Policy (Color=101, Endpoint=E) of SR Policy Group1.

Because there are many access endpoints and each endpoint may act as an ingress node, compared with the traditional method of distributing service forwarding policies on each ingress node, the above SR Policy Group can greatly simplify the configuration of VPN access endpoints and effectively improve the efficiency of network deployment and operation and maintenance.

For reliability reasons, a default best-effort forwarding path can also be configured for each VPN tenant. If all the SR Policy forwarding paths of the SR Policy group are invalid, the default path can be used. The endpoints through which traffic forwarding must pass can be designed in the default path.

9. Implementation Status

[Note to the RFC Editor - remove this section before publication, as well as remove the reference to [RFC7942].

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in [RFC7942]. The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations may exist.

According to [RFC7942], "this will allow reviewers and working groups to assign due consideration to documents that have the benefit of running code, which may serve as evidence of valuable experimentation and feedback that have made the implemented protocols more mature. It is up to the individual working groups to use this information as they see fit".

9.1 Huawei Technologies

* Organization: Huawei Technologies.

* Implementation: NE40E series routers implementation of SR Policy Group.

* Description: All sections including all the "MUST" and "SHOULD" clauses have been implemented in above-mentioned Huawei Products(running Version V8R22C00 and above).

* Maturity Level: Product

* Coverage: All sections.

* Version: Draft-04

* Licensing: N/A

* Implementation experience: Nothing specific.

* Contact: zhangyawei@huawei.com

* Last updated: August 13, 2024

9.2 New H3C Technologies

* Organization: New H3C Technologies.

* Implementation: H3C CR16000, CR19000 series routers implementation of SR Policy Group.

* Description: All sections including all the "MUST" and "SHOULD" clauses have been implemented in above-mentioned New H3C Products(running Version 7.1.086 and above).

* Maturity Level: Product

* Coverage: All sections.

* Version: Draft-04

* Licensing: N/A

* Implementation experience: Nothing specific.

* Contact: linchangwang.04414@h3c.com

* Last updated: August 10, 2024

9.3 ZTE Corp

* Organization: ZTE Corporation.

* Implementation: ZTE’s M6000 T8000Series Routers implementation of SR Policy Group.

* Description: All sections including all the "MUST" and "SHOULD" clauses have been implemented in ZTE M6000 and T8000 series routers (running V5.00.10 and above).

* Maturity Level: GA

* Coverage: ALL

* Version: Draft-04

* Licensing: N/A

* Implementation experience: Nothing specific.

* Contact: zhu.xiaolong@zte.com.cn

* Last updated: August 12, 2024

9.4 Ruijie Network

* Organization: Ruijie Networks Co., Ltd.

* Implementation: Ruijie’s N8000Series Routers implementation of SR Policy Group.

* Description: All sections including all the "MUST" and "SHOULD" clauses have been implemented in Ruijie N8000 series routers (running N8000-R_RGOS 12.8(3)B0801 and above).

* Maturity Level: GA
* Coverage: ALL
* Version: Draft-04
* Licensing: N/A
* Implementation experience: Nothing specific.
* Contact: liangyanrong@ruijie.com.cn
* Last updated: August 12, 2024

10. IANA Considerations

This document has no IANA actions.

11. Security Considerations

This document does not introduce any security considerations.

12. References

12.1 Normative References

[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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC9256] Filsfils, C., Talaulikar, K., Voyer, D., Bogdanov, A., and P. Mattes, "Segment Routing Policy Architecture", RFC9256, DOI 10.17487/RFC9256, July 2022, <https://www.rfc-editor.org/info/rfc9256>.

[RFC8402] Filsfils, C., Ed., Previdi, 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>.

[RFC9830] Previdi, S., Filsfils, C., Talaulikar, K., Mattes, P., and Jain, D., "Advertising Segment Routing Policies in BGP", RFC 9830, DOI 10.17487/RFC9830, September 2025, <https://www.rfc-editor.org/info/rfc9830>.

12.2 Informative References

[RFC7942] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", BCP 205, RFC 7942, DOI 10.17487/RFC7942, July 2016, <https://www.rfc-editor.org/info/rfc7942>.

Acknowledgments

The authors would like to thank Nat Kao for his review and comments of this document.

Contributors

Yanrong Liang
Ruijie Networks
China

Email: liangyanrong@ruijie.com.cn

Authors' Addresses

Weiqiang Cheng
China Mobile
china

Email: chengweiqiang@chinamobile.com

Wenying Jiang
China Mobile
China

Email: jiangwenying@chinamobile.com

Changwang Lin
New H3C Technologies
china

Email: linchangwang.04414@h3c.com

Ran Chen
ZTE Corporation
China

Email: chen.ran@zte.com.cn

YaWei Zhang
Huawei Technologies
China

Email: zhangyawei@huawei.com