Segment routing in SR OS

Tools and applications for IP network architects

Application note
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction and overview</td>
<td>3</td>
</tr>
<tr>
<td>Segment routing - traffic engineering (SR-TE)</td>
<td>3</td>
</tr>
<tr>
<td>SR policies and SR-TE tunnels</td>
<td>4</td>
</tr>
<tr>
<td>Local and end-to-end path protection and restoration</td>
<td>5</td>
</tr>
<tr>
<td>Segment routing in Nokia SR OS</td>
<td>6</td>
</tr>
<tr>
<td>Getting started with segment routing</td>
<td>7</td>
</tr>
<tr>
<td>Advanced segment routing applications</td>
<td>8</td>
</tr>
<tr>
<td>Network Function Interconnect Architecture</td>
<td>9</td>
</tr>
<tr>
<td>Segment routing in data centers</td>
<td>10</td>
</tr>
<tr>
<td>Legacy migration to segment routing</td>
<td>11</td>
</tr>
<tr>
<td>SR-MPLS introduction and LDP/RSVP-TE migration</td>
<td>11</td>
</tr>
<tr>
<td>SRv6 introduction and SR-MPLS interworking</td>
<td>12</td>
</tr>
<tr>
<td>Nokia differentiators</td>
<td>13</td>
</tr>
<tr>
<td>Abbreviations</td>
<td>13</td>
</tr>
<tr>
<td>Standards and recommendations</td>
<td>15</td>
</tr>
<tr>
<td>Further reading</td>
<td>16</td>
</tr>
</tbody>
</table>
Introduction and overview

Segment routing (SR) is a powerful technology to protect and engineer network traffic. This application note gives a practical overview of the SR tools and applications supported by the Nokia Service Router Operating System (SR OS) to help take full advantage of these capabilities.

SR (RFC 8402) offers a scalable approach for establishing predefined forwarding paths in the IP network that override the default shortest path, while meeting specific constraints like available bandwidth, latency, or physical diversity. SR removes the need for resource-intensive, per-path control plane signaling and keeps a minimum of forwarding state information on routing nodes. As a result, it scales better than RSVP-TE or LDP and can engineer more granular traffic flows.

Segment routing - traffic engineering (SR-TE)

SR is an ideal technology to engineer forwarding paths with granular policy constraints—for example, nodes and links to include or exclude in the path, physical diversity, administrative state, and path metrics such as available bandwidth, accumulative latency and maximum number of hops. SR takes a source-based routing approach, which only requires the ingress or headend router to maintain policy and state information about the path. In its simplest form, a segment route is a sequence of segments that must be traversed when forwarding packets along a constrained path that meets a given policy (Figure 1).

Figure 1. SR basic principles
Traffic-engineered paths for segment routes can be conveyed to a headend router in various ways, such as model-driven CLI, NETCONF/YANG, BGP updates or the Path Computation Element Protocol (PCEP – RFC 5440). Segments can refer to different types of network objects:

- Adjacency segments refer to numbered router interfaces and are locally unique to a router.
- IGP prefix segments refer to a subnet or routing node and are globally unique.
- BGP prefix segments refer to border nodes such as data center gateways.
- BGP peer segments refer to an outgoing peering interface or node, which allows traffic to be steered to a particular egress point.
- Anycast segment is a node prefix that is advertised by more than one node. The set of nodes advertising the same anycast-SID form a group called an anycast set.

SR supports multiple data plane options to facilitate network portability and evolution:

- SR for MPLS (SR-MPLS) represents segments as MPLS labels that are encoded in an MPLS label stack (RFC 8663). SR-MPLS can be deployed on existing MPLS routers and silicon.
- SR-MPLS over User Datagram Protocol (UDP). MPLS traffic is encapsulated over UDP (RFC 7510). This option is useful for IP-only data center fabrics that do not natively support MPLS.
- SR for IPv6 (SRv6) represents each segment as an IPv6 address construct encoded in an IPv6 segment routing header (SRH) extension (RFC 8754) and typically requires new hardware.

When deployed over an MPLS data plane, the segment identifiers (SIDs) are allocated from a reserved block in the MPLS label space. To advertise segment reachability information within IPv4 or IPv6 routing domains, SR-MPLS and SRv6 can use interior link-state gateway protocol (IGP) extensions for OSPF (RFC 8665) and IS-IS (RFC 8667). This enables a straight-forward migration that preserves all transport capabilities of LDP and RSVP-TE, while improving failure recovery. BGP is used to advertise BGP prefix and peer segments, and to advertise segment reachability information in IP fabrics without an IGP such as data center fabrics.

**SR policies and SR-TE tunnels**

Segment routing supports traffic engineering through the use of SR-TE LSPs or SR Policies. Both provide a logical traffic tunnel that adheres to specific forwarding constraints. From a user perspective, SR-TE LSPs are similar to traditional traffic engineered LSPs such as RSVP-TE and offer a natural migration path. They support primary and secondary paths with strict or loose hops that can be initiated by a router or by an external Path Computation Element (PCE) controller. SR-TE LSP paths can be computed locally or controlled by PCE.

SR Policies consist of multiple candidate paths, of which one is selected as active at a given time. Each candidate path has multiple traffic-engineered segment lists, which are all programmed for the active candidate path and across which packets are sprayed using equal cost multi-path (ECMP) load-balancing. Sub-address family extensions to BGP allow dynamic instantiations and advertisement of SR policies in an intra-domain or inter-domain context. These extensions allow unique identification of an SR policy by means of an abstract color (a 4-byte number), end points and a route distinguisher. Each SR Policy can be assigned a unique binding SID (BSID) for the purpose of steering traffic into the policy. This SR Policy binding concept allows to dynamically alter or optimize the policy path and segment list, without impacting the SR-TE tunnel itself.
SR-TE with SDN, whether using SR-TE LSPs or SR Policies, allows to dynamically provision traffic paths on behalf of service requests and track these paths in a centralized Traffic Engineering Database. Centralized path computation does not face the resource constraints of distributed routing algorithms and can potentially optimize resource use from a global network perspective. It also avoids collisions, re-tries, and packing problems that has been observed in networks using distributed TE path calculation, where head-ends make autonomous decisions.

However, where distributed path computation meets a service provider’s operational objectives, IGP Flexible Algorithms (Flex-Algo) complement SR-TE by adding new prefix segments with specific optimization objectives and constraints that can be advertised by supporting router nodes. Pre-defined algorithms and metrics are referred to by an agreed upon 7-bit identifier, where algorithm 0-127 are standard algorithms such as the shortest path algorithm, and 128-255 are operator defined. Applicable Flex-Algo link metrics include the default IGP metrics, a minimum unicast link delay or the TE metric, and links to be excluded or included based on their administrative group link affinity/color or SRLG membership.

**Local and end-to-end path protection and restoration**

Besides engineering a working traffic path, segment routing can also be applied to pre-calculate backup paths that protect against failure of the primary path. Since intermediate routers do not have state information about the path, autonomous recovery mechanisms such as MPLS fast reroute will not work properly because a point of local repair (PLR) that is doing a local detour will not be able to identify the downstream nodes of the SR-TE path.

Therefore, where fast reroute is used in an SR context, an alternate next-hop path must be pre-computed so that when a failure is detected with the primary next hop, the alternate can rapidly be used until an SPF algorithm is run and a new primary next hop is installed. When a PLR attempts to pre-compute an alternate backup next hop, the backup next hop is generically called a loop-free alternate or LFA (RFC 5286). The existence of a suitable LFA—and therefore the percentage of fast reroute coverage that a given network can obtain, depends on the topology. Basic LFA calculations have good coverage for meshed topologies, but generally perform poorly in ring topologies, in which case they may create micro loops (see RFC 6571).

Remote LFA (RLFA – RFC 7490) and directed (DLFA) extend the basic LFA repair mechanism by extending the topology coverage to nearly 100 percent. If a link cannot be protected for a given destination with local, adjacent LFA neighbors, RLFA attempts to create a virtual LFA by using a tunnel to carry packets to a point in the network where they will not be looped back. However, when an RLFA repair tunnel uses RSVP or LDP, targeted LDP sessions must be tunneled to repair tunnel endpoints so that inner labels can be exchanged. Since the repair points can dynamically change along with the topology, the targeted LDP sessions must also be dynamically set up and torn down, but many operators do not favor such dynamic behavior.
Another remaining issue is that the backup path established through RLFA and DLFA repair mechanisms may be altered when IGP re-convergence occurs and reachability information is updated, which means a second transition that impacts the service. Topology independent LFA (TI-LFA) addresses this issue by using the so-called P/Q algorithm to engineer repair paths that reduce these two transitions to a single pre-convergence to post-convergence transition, to minimize the impact of failures on services (see Figure 2).

Seamless Bidirectional Forwarding Detection (SBFD – RFC 7880) is complementary to LFA and used for rapid and deterministic path failure detection in as little as 30 ms. SBFD sessions are established on every path of an SR-TE label switched path (LSP) or segment list of an SR Policy. If an SBFD session on the active path goes down, SR switches to a pre-programmed standby path or SR Policy. If there are multiple active segment lists in an SR Policy (ECMP), then SBFD can trigger the failed segment list to go out of service to prevent blackholing of traffic. SBFD can also detect “silent faults” that are not visible to the control plane. Since SBFD works on the end-to-end paths, it does not trigger an LFA.

**Segment routing in Nokia SR OS**

Support for segment routing in the Nokia Service Router Operating System (SR OS) started in 2015 and has since evolved into a robust, comprehensive and versatile toolkit that has been validated and deployed by network operators for a variety of applications (Table 1).

Table 1. SR OS segment routing toolkit

<table>
<thead>
<tr>
<th></th>
<th>Programmatic control</th>
<th>Protection/assurance</th>
<th>Traffic engineering</th>
<th>Control plane</th>
<th>Data plane</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PCEP</td>
<td>BGP, BGP Link-State</td>
<td>SR-TE</td>
<td>IS-IS, OSPF, BGP or static, IPv4 or IPv6</td>
<td>SR-MPLS (IPv4, IPv6)</td>
</tr>
<tr>
<td><strong>Programmatic control</strong></td>
<td>PCEP</td>
<td>BGP, BGP Link-State</td>
<td>SR Policy</td>
<td>Flex-Algo</td>
<td></td>
</tr>
<tr>
<td><strong>Protection/assurance</strong></td>
<td>LFA, TI-LFA, RLFA</td>
<td>Primary-secondary</td>
<td>LSP ping/trace, BFD</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Traffic engineering</strong></td>
<td>SR-TE</td>
<td>SR Policy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Control plane</strong></td>
<td>IS-IS, OSPF, BGP or static, IPv4 or IPv6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data plane</strong></td>
<td>SR-MPLS (IPv4, IPv6)</td>
<td>SRv6 (IPv4)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SR OS currently implements a full SR-MPLS feature set for IPv4 and IPv6 networks and segment routing for IPv6 (SRv6) is added over the course of 2021.

**Getting started with segment routing**

Using the SR OS segment routing toolkit, operators can enhance traffic visibility, control and resiliency in their existing MPLS networks.

The scope and depth of the SR toolkit can be intimidating, but operators can incrementally add the SR features they need to an existing LDP/RSVP network with the options they’re comfortable with. This eases the migration and enables operational experience to be gained before introducing more powerful features. (see Figure 3)

![Figure 3. Advanced SR applications](image)

**Shortest path routing** is a good starting point for introducing SR as a replacement for LDP and only requires control plane extensions for IS-IS or OSPF. Global SR label blocks, node and link adjacencies can be configured for each router, after which SR-IS-IS or SR-OSPF tunnels can be used by IP services.

**Constraint-based shortest path routing** could be a logical next step, for example to engineer low-latency paths for delay-sensitive applications, or to ensure traffic flows are kept within a controlled set of links (data sovereignty). By augmenting the SR shortest path with an IGP flexible algorithm (Flex-Algo) it becomes possible to add topology constraints and alternative link-metrics to the shortest path calculation. This application invokes SR traffic engineering capabilities (SR Policy and Flex-Algo), and programmatic control (BGP and BGP-LS). SR-TE capabilities can be further extended with BGP and BGP-LS to include BGP prefix and peer segments, and steer traffic to a particular egress point (i.e., egress peer engineering).
Path diversity and end-to-end protection enable highly available, premium transport services as a more scalable alternative for MPLS fast reroute based on RSVP-TE. SR-TE LSPs with diverse primary and secondary paths are enabled by including SRLG constraints for the candidate paths. Seamless BFD is used for fast detection of failures, including silent failures that are not visible to the control plane, and to trigger a failover to the secondary path if the primary path fails.

Advanced segment routing applications

More advanced intra-domain and inter-domain SR-TE applications are enabled by additional programmatic capabilities that are provided through BGP extensions, PCEP or NETCONF/YANG, and orchestrated by a centralized Segment Routing Interconnect Controller (SRIC). The SRIC is a cross-domain SDN controller that can perform network-wide SR path computation and optimization functions. The Nokia Network Services Platform (NSP) supports the SRIC function in multivendor networks.

Many operators are building digitalized, cloud-native infrastructures that are capable of hosting numerous virtualized network/service functions that can be dynamically instantiated and scaled on-demand. Service function chaining (RFC 7665) addresses the need to compose programmable and flexible end-to-end services by concatenating Service Functions (SFs) in a specific order and subsequently steering user flows along the resulting Service Function Path or SFP (Figure 4). This enables, for example, support for cloud or centralized radio access network models where 5G radio units must interconnect with virtualized base band signal processing and mobility control functions in distributed and centralized units that are attached to the mobile backhaul network.

Figure 4. Service function chaining

An SFC can perform various end-to-end services by including or excluding specific SFs in the SFC transport path, and can be quite complex, with various branches, loops or jumps. The SFs in an SFP may reside on different servers, data centers or network devices. The SFC service plane is separated from the transport plane to enable various data path implementations, such as SR-MPLS, SR-MPLS over UDP and SRv6. Network layer reachability information (NLRI) is exchanged through BGP control plane updates using address family extensions for Network Service Header (NSH) and SR-based service chaining. These BGP extensions enable the SRIC to learn the SFC topology and construct the various SFPs by including and concatenating service segments in the order of their advertised Service Index.
A Classifier function at the headend of an SFC matches incoming user flows against an SFC policy to select the applicable SFP that renders the desired end-to-end service. The Classifier then encodes the SFP forwarding instructions in an NSH and composes the corresponding SFC transport path as an ordered list of service segments that must be traversed along the service chain. SFCs can be implemented in two ways:

- **A decoupled model** where SR provides the individual transport tunnels between Service Function Forwarders (SFFs), and NSH is used for service chaining and associated metadata
- **A coupled or integrated model** for SFs that supports segment routing. Each service hop in the SFP is represented as a segment and SR steers traffic through all necessary SFFs, while NSH is used for maintaining the service plane and holding SFC instance context and metadata.

**Network Function Interconnect Architecture**

The Network Function Interconnect Architecture or NFIX is a Nokia standardization initiative that combines service function chaining with seamless MPLS to support inter-domain use cases in multi-cloud infrastructures. NFIX does not define any new protocols but rather outlines how existing standards-based protocols can be applied in a unified and scalable manner to interwork physical and virtual network functions in and across wide area network and data center domains, while maintaining the ability to deliver against SLAs (Figure 5).

Figure 5. Network Function Interconnect Architecture (NFIX)

The SRIC learns wide area network topology information and allocation of segment routing SIDs within that domain using BGP link-state (RFC 7752) with appropriate SR extensions. Equally it learns data center topology information and Prefix-SID allocation using BGP labeled unicast (RFC 8277) with appropriate SR extensions, or BGP link-state if a link-state IGP is used within the data center. If route reflection (RR) is used for exchange of BGP link-state or labeled unicast NLRI within one or more domains, then the SRIC can peer as an RR client to learn the topology.

The SRIC also acquires real-time network state through protocols such as IP Flow Information Export (IPFIX) (RFC 7011), streaming telemetry, NETCONF/YANG, BGP link-state, and the BGP monitoring protocol (RFC 7854) to make informed decisions and take preventive or corrective actions as necessary. Based on this data, the SRIC can auto-provision SR-TE policies and route-color aware inter-domain transport tunnels.
seamlessly across the wide area network and assure that SLA policies are adhered to. Binding SIDs are assigned to the inter-domain transport tunnels that interconnect the edge cloud and core data centers across the wide area network to facilitate provider edge (PE) routers and data center interconnect (DCI) gateways to steer user traffic into them.

**Segment routing in data centers**

Segment routing is also being adopted for data center networks and DCI applications. The use case example shown in Figure 6 applies to SR-enabled data center fabrics and uses SR-TE to establish a reliable, low-latency transport service to interconnect two Ethernet VPN (EVPN) service instances in geographically separated data centers over a physically diverse, dual-plane core network. The EVPN endpoints are instantiated on leaf nodes with multiple uplinks to a cluster of spine routers. As the state of the uplink between the spine and core is not visible to the leaf nodes, protection from uplink failures is required to avoid blackholing traffic.

Figure 6. Interconnecting leaf-spine DC fabrics over a low-latency dual-core network

To accomplish this, all spine nodes of the connecting IP fabric are included in an anycast set with anycast SID 13005, which allows load balancing across the spine cluster nodes. The low-latency transport tunnel through the dual-plane core network segment is established using Flex-Algo and assigned with binding SID 15000. The destination leaf node hosting the remote EVPN instance is assigned SID 1000.

The primary SR path is implemented as a multi-path policy defined by the spine-anycast-SID (13005), the low-latency-core-SR-policy-BSID (15000) and the destination-node-SID (1000). The primary SR policy is backed up with an ECMP set of single path SR policies that identify the next alternative spine node to take over in case the uplink of the primary spine node fails. For example, if the core uplink of primary spine with node-SID 12005 fails, secondary spine-node 12006 will steer the EVPN leaf traffic into the low-latency SR core policy.
Legacy migration to segment routing

Many operators have already deployed traffic engineering and protection capabilities based on LDP or RSVP-TE. SR-MPLS offers a smooth and straight-forward migration path for these legacy networks and eases the evolution to next-generation networks using IPv6.

SR-MPLS introduction and LDP/RSVP-TE migration

Because SR-MPLS supports native IPv4 and IPv6 data planes without adding new hardware requirements, it can normally be deployed on existing hardware through a software upgrade. The capabilities of the SR toolkit can be gradually introduced and yield immediate service benefits, without sacrificing any transport capabilities offered by LDR and RSVP-TE:

- BGP base router and virtual routing and forwarding (VRF) routes can be migrated service-by-service using auto-bind-tunnels
- Alternatively, the migration can be done PE-by-PE. Ingress PE can bind the same VRF to LDP/RSVP-TE or SR-IS-IS/SR-OSPF/SR-TE tunnel based on the capability of each remote PE.
- For new networks we recommend skipping RSVP-TE and deploy SR-IS-IS/SR-OSPF and SR-TE. Table 2 compares some of the important differences between RSVP-TE and SR to highlight the key benefits of legacy migration.

Table 2. Comparing segment routing with RSVP-TE

<table>
<thead>
<tr>
<th>Aspect</th>
<th>RSVP-TE</th>
<th>Segment Routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data plane state</td>
<td>Locally significant LSP context</td>
<td>Global or local LSP context</td>
</tr>
<tr>
<td>Control protocols</td>
<td>Two: IS-IS or OSPF, RSVP</td>
<td>One: IS-IS or OSPF</td>
</tr>
<tr>
<td>Traffic engineering</td>
<td>Network-based: IGP-TE/RSVP-TE</td>
<td>Network and controller-based:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SR-TE, SR policy, Flex-Algo</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IGP-TE with CSPF, SDN Controller</td>
</tr>
<tr>
<td>Inter-area/AS</td>
<td>Inter-AS TE (needs IGP across BGP boundaries)</td>
<td>Binding SID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Egress Peer Engineering</td>
</tr>
<tr>
<td>Network programmability</td>
<td>PCEP, NETCONF, PCC-init</td>
<td>PCEP, BGP, NETCONF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PCC-init or PCE-init</td>
</tr>
<tr>
<td>Granularity and steering</td>
<td>Single level: Next hop or end-to-end paths</td>
<td>Multi-level: Steer traffic across any kind of crafted</td>
</tr>
<tr>
<td></td>
<td>ECM into parallel end-to-end LSPs</td>
<td>path (node, adjacency, anycast, etc.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Can combine loose/ECMP hops within strict TE path</td>
</tr>
<tr>
<td>Protection/OAM</td>
<td>MPLS FRR, Active/standby LSP ping/trace/self-</td>
<td>LFA/RLFA/TILFA, Active/standby</td>
</tr>
<tr>
<td></td>
<td>ping/LSP BFD</td>
<td>LSP ping/trace/seamless BFD</td>
</tr>
<tr>
<td></td>
<td>Control plane-based re-optimization</td>
<td>IGP + SBFD-based re-optimization</td>
</tr>
<tr>
<td>Multicast support</td>
<td>Point-to-multipoint (P2MP) LSPs</td>
<td>Tree-SID (SR P2MP)</td>
</tr>
</tbody>
</table>

In summary, segment routing offers several operational benefits compared to LDP/RSVP-TE:

- Better scalability by only requiring ingress routers to keep state information
- Operationally simpler by avoiding the need for an additional signaling protocol (RSVP-TE)
- Greater control flexibility and scope by also supporting centralized TE controllers to facilitate inter-domain/inter-area traffic engineering applications (egress peering engineering, etc.)
- Granular multi-level traffic steering across any crafted path with strict and loose constraints and built-in ECMP load-balancing capabilities
- Better protection with full coverage for all topologies through LFA, RLFA and TI-LFA
- Multicast-capable without additional control protocols such as P2MP RSVP, Multicast Label Distribution Protocol, and Protocol-Independent Multicast.

**SRv6 introduction and SR-MPLS interworking**

The SRv6 standardization effort is far more recent than SR-MPLS and still evolving. The goal is to provide a programmable framework for IPv6 networks that tightly integrates overlay service functions and underlay transport functions ([RFC 8986](https://tools.ietf.org/html/rfc8986)). SRv6 takes advantage of the larger address space to encode 128-bit SIDs as an IPv6 address:

- SRv6 shortest path routing encodes the destination SID in the Destination Address (DA) field of the outer IPv6 header.
- SRv6 source routing encodes the top SID in the DA field and the rest of the SIDs of nodes the packet must visit as SID list in the SRH.

Because the SRv6 service extensions impose additional data path requirements on IPv6 packet header processing, feature support is contingent on routing silicon and typically demands new hardware. For example, FP4 silicon is required to support the full SRv6 PE feature set on Nokia 7750 SR and 7950 XRS routers, and Jericho 2 silicon for 7250 IXR platforms.

**Figure 7. SRv6 support and SR-MPLS interworking**

With next generation hardware factoring into the business case, the adoption of SRv6 is expected to be slower than IPv6 and more gradual than SR-MPLS. Pockets of SRv6 deployments will emerge in IPv6 network domains that do not typically require MPLS, such as metro aggregation and data center networks, while wide area networks with strong IPv4 and MPLS support considerations will prefer SR-MPLS. Where SR-MPLS and SRv6 must coexist, the interworking of SR-MPLS and SRv6 is essential to seamlessly deploy services across domain boundaries (Figure 7).

SRv6 deployments are few and in early stages, and much work is left to be done. For example, the use of 128-bit SIDs would add a significant packet overhead without some form of header compressing. Another issue is the use of SRv6 to encode programming instructions for SFs in the forwarding path in a coupled/
integrated SFC model, which constitutes a mindset shift for network operations and troubleshooting. Nokia is an active member of the IETF SRv6 compressed SID design team to help resolve open points such as these and enable stable, interoperable implementations.

It is beyond the scope of this application note to discuss or comment on the SRv6 proceedings in the IETF. SRv6 and SR-MPLS achieve similar goals with different implementations. SR-MPLS is more mature, widely deployed, highly interoperable to enable network evolution with a low cost, risk, and time-to-market. SR-MPLS also maintains a decoupled overlay/underlay network model that more network operators are familiar with, and despite the misconceptions, it supports IPv6 as well.

### Nokia differentiators

Segment routing is a powerful and proven technology for deploying highly programmable IP services that meet deterministic service level objectives on cost, performance and reliability. Segment routing addresses all operational scalability issues of legacy traffic engineering and protection approaches using LDP or RSVP-TE and enables a wide range of new applications, especially when used in combination with the Nokia NSP.

The Nokia SR OS offers a comprehensive segment routing toolkit for IP/MPLS networks, next-generation IPv6 networks, and the transition between them. Segment routing capabilities that differentiate Nokia service routers include:

- Standards compliance and proven multivendor interoperability through Orange labs/EANTC
- Full SR support for IP and Ethernet VPNs, Virtual Private LAN, and virtual leased line services
- Complete SR policy management support through PCEP, SR-TE LSP and BGP SR policy
- Extensive protection and restoration through basic and remote LFA, topology independent LFA, link and node protection and advanced LFA policy for control of backup path
- The industry’s largest label stack (LER push up to 12 labels, LSR hash up to 16 labels)
- The industry’s most flexible SR gateway solution with capabilities to interwork and translate among different data and control planes: MPLS, SR-MPLS, SRv6, Virtual Extensible LAN, MPLS-over-UDP
- Programmability and flexibility of FP4 routing silicon to support variable SID lengths (32-bit, 16-bit or 128-bit) and new data path optimizations to compress segments in SRv6.

Please consult our product documentation and user guides for detailed information on supported features and platforms or contact Nokia sales to learn more.

### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFD</td>
<td>bi-directional failure detection</td>
</tr>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
</tr>
<tr>
<td>BGP-LS</td>
<td>Border Gateway Protocol Link-State</td>
</tr>
<tr>
<td>BSID</td>
<td>binding segment identifier</td>
</tr>
<tr>
<td>CLI</td>
<td>command line interface</td>
</tr>
<tr>
<td>DCI</td>
<td>data center interconnect</td>
</tr>
<tr>
<td>DLFA</td>
<td>directed LFA</td>
</tr>
</tbody>
</table>
Standards and recommendations

RFC 3209  RSVP-TE: Extensions to RSVP for LSP Tunnels
RFC 4655  A Path Computation Element (PCE)-Based Architecture
RFC 5286  Basic Specification for IP Fast Reroute: Loop-Free Alternates
RFC 5440  Path Computation Element (PCE) Communication Protocol (PCEP)
RFC 6020  A Data Modeling Language for the Network Configuration Protocol (NETCONF)
RFC 6241  Network Configuration Protocol (NETCONF)
RFC 6571  LFA applicability in service provider networks
RFC 7011  IPFIX Protocol Specification
RFC 7432  BGP MPLS-based Ethernet VPN
RFC 7490  Remote Loop-Free Alternate Fast Reroute (RLFA)
RFC 7510  Encapsulating MPLS in UDP
RFC 7665  Service Function Chaining Architecture
RFC 7752  Link-State Information Distribution Using BGP
RFC 7854  BGP Monitoring Protocol
RFC 8277  BGP and Labeled Address Prefixes
RFC 8402  Segment routing architecture
RFC 8426  Recommendations for RSVP-TE and segment routing LSP coexistence
RFC 8661  Segment routing interworking with LDP
RFC 8663  MPLS Segment Routing over IP
RFC 8665  OSPF Extensions for Segment Routing
About Nokia

At Nokia, we create technology that helps the world act together. As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs. Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Nokia operates a policy of ongoing development and has made all reasonable efforts to ensure that the content of this document is adequate and free of material errors and omissions. Nokia assumes no responsibility for any inaccuracies in this document and reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Nokia is a registered trademark of Nokia Corporation.

Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2023 Nokia
Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: 534804 (April) CID210750

Further reading


RFC 8667  IS-IS Extensions for Segment Routing
RFC 8754  IPv6 Segment Routing Header (SRH)
RFC 8986  Segment Routing over IPv6 (SRv6) Network Programming
RFC 9085  Border Gateway Protocol - Link State (BGP-LS) Extensions for Segment Routing
Flex-Algo IGP Flexible Algorithm
NFIX An architecture for Network Function Interconnect