SRv6 Deployment Consideration
draft-tian-spring-srv6-deployment-consideration-00

Abstract

SRv6 has significant advantages over SR-MPLS and has attracted more and more attention and interest from network operators and verticals. Smooth network migration towards SRv6 is a key focal point and this document provides network migration guidance and recommendations on solutions in various scenarios. Deployment cases with SRv6 are also introduced.

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."

Tian, et al. Expires May 7, 2020
1. Introduction

SRv6 is the instantiation of Segment Routing deployed on the IPv6 data plane[RFC8200]. Therefore, in order to support SRv6, the network must first be enabled for IPv6. Over the past several years, IPv6 has been actively promoted all over the world, and the deployments of IPv6 have been ever-increasing which provides the basis for the deployments of SRv6.

With IPv6 as its data plane, for network migration towards SRv6, both software and hardware need to be upgraded. Compared with other new
Internet-Draft                      SRv6 Deployment Consideration                   November 2019

protocols, only IGP and BGP need to be extended to support SRv6, which significantly simplifies the software upgrade required. While the hardware needs to support the new SRv6 header SRH[I-D.ietf-6man-segment-routing-header], the design of SRv6 assures compatibility with the existing IPv6 network as an SRv6 SID is designed as a 128-bit IPv6 address and the encapsulation of an SRv6 packet is the same as an IPv6 packet. When only L3VPN over SRv6 BE (Best-Effort) is deployed, there will be no SRH. Therefore, no additional hardware capabilities are required but only software upgrade for protocol extensions.

As the number of services supported by SRv6 increase, e.g. SFC, network slicing, iOAM etc., more SIDs in the SRH may impose new requirements on the hardware. Besides upgrading the hardware, various solutions [I-D.peng-spring-srv6-compatibility] have already been proposed to relieve the imposed pressure on the hardware, such as Binding SID (BSID) etc. to guarantee the compatibility with the existing network. On the other hand SRv6 has many more advantages over SR-MPLS for the network migration to support new services.

This document summarizes the advantages of SRv6 and provides network migration guidance and recommendations on solutions in various scenarios.

2. Advantages of SRv6

Compared with SR-MPLS, SRv6 has significant advantages especially in large scale networking scenarios.

2.1. IP Route Aggregation

The increasing complexity of service deployment is of concern for network operators, especially in large-scale networking scenarios. With solutions such as multi-segment PW and Option A [RFC4364], the number of service-touch points has increased, and the services, with associated OAM features cannot be deployed end-to-end.

- With Seamless MPLS or SR-MPLS, since the MPLS label itself does not have reachability information, it must be attached to a routable address. The 32-bit host route needs to leak across domains. For an extreme case, as shown in Figure 1a, in a large scale networking scenario, millions of host route LSPs might need to be imported, which places big challenges on the capabilities of the edge nodes.

- With SRv6, owing to its native IP feature of route aggregation as shown in Figure 1b, the aggregated routes can be imported across network domains. For large scale networking, only very few
aggregated routes are needed in order to start end-to-end services, which also reduces the scalability requirements on the edge nodes.

Figure 1. Large-scale Networking with (a) SR-MPLS vs. (b) SRv6

2.2. End-to-end Service Auto-start

In the SR cross-domain scenario, in order to set up end-to-end SR tunnels, the SIDs in each domain need to be imported to other domains.
o With SR-MPLS, SRGB and Node SID need overall network-wide planning, and in the cross-domain scenario, it is difficult or sometimes even impossible to perform as the node SIDs in different domains may collide. BGP Prefix SID can be used for the cross-domain SID import, but the network operator must be careful when converting the SID to avoid SID collision. Moreover, the pre-allocated SRGB within each domain needs to consider the total number of devices in all other domains, which raises difficulties for the network-wide planning.

o With SRv6, owing to its native IP feature of route reachability, if the IPv6 address space is carefully planned, and the aggregated routes are imported by using BGP4+ (BGP IPv6), the services will auto-start in the cross-domain scenario.

2.3. On-Demand Upgrade

The MPLS label itself does not hold any reachability information, so it must be attached to a routable address, which means that the matching relationship between the label and FEC needs to be maintained along the path.

SR-MPLS uses the MPLS data plane. When the network migrates to SR-MPLS, there are two ways, as shown in Figure 2:

1. MPLS/SR-MPLS Dual stack: the entire network is upgraded first and then deploy SR-MPLS.

2. MPLS and SR-MPLS interworking: mapping servers are deployed at some of the intermediate nodes and then removed once the entire network is upgraded

Regardless of which migration option is chosen, big changes in a wide area is required at the initial stage therefore causing a long time-to-market.

In contrast, the network can be migrated to SRv6 on demand. Wherever the services need to be turned on, only the relevant devices need to be upgraded to enable SRv6, and all other devices only need to support IPv6 forwarding and need not be aware of SRv6. When Traffic Engineering (TE) services are needed, only the key nodes along the path need to be upgraded to support SRv6.
### 3. Incremental Deployment Guidance for SRv6 Migration

Incremental deployment is the key for a smooth network migration to SRv6. In order to quickly launch SRv6 network services and enjoy the benefits brought by SRv6, the recommended incremental SRv6 deployment steps are given as follows. These are based on practical deployment experience earned from the use cases described in [I-D.matsushima-spring-srv6-deployment-status].

The referenced network topology is shown in Figure 3.
Step 1. All the network devices are upgraded to support IPv6.

Step 2. According to service demands, only a set of selected PE devices are upgraded to support SRv6 in order to immediately deploy SRv6 overlay VPN services. For instance, in Figure 3, PE1 and PE2 are SRv6-enabled.

Step 3. Besides the PE devices, some P devices are upgraded to support SRv6 in order to deploy loose TE which enables network path adjustment and optimization. SFC is also a possible service provided by upgrading some of the network devices.

Step 4. All the network devices are upgraded to support SRv6. In this case, it is now possible to deploy strict TE, which enables the deterministic networking and other strict security inspection.


As the network migration to SRv6 is progressing, in most cases SRv6-based services and SR-MPLS-based services will coexist.

As shown in Figure 4, in the Non-Standalone (NSA) case specified by 3GPP Release 15, 5G networks will be supported by existing 4G infrastructure. 4G eNB connects to CSG 2, 5G gNB connects to CSG 1, and EPC connects to RSG 1.

To support the 4G services, network services need to be provided between CSG 2 and RSG 1 for interconnecting 4G eNB and EPC, while for the 5G services, network services need to be deployed between CSG 1 and RSG 1 for interconnecting 5G gNB and EPC. Meanwhile, to support X2 interface between the eNB and gNB, network services also need to be deployed between the CSG 1 and CSG 2.
As shown in Figure 4, in most of the current network deployments, MPLS-based network services may have already existed between CSG 2 and RSG 1 for interconnecting 4G eNB and EPC for 4G services.

When 5G services are to be supported, more stringent network services are required, e.g. low latency and high bandwidth. SRv6-based network services could be deployed between CSG 1 and RSG 1 for interconnecting 5G gNB and EPC.

In order to perform smooth network migration, a dual-stack solution can be adopted which deploys both SRv6 and MPLS stack in one node.

With the dual-stack solution, only CSG 1 and RSG 1 need to be upgraded with SRv6/MPLS dual stack. In this case, CSG 1 can immediately start SRv6-based network services to RSG 1 for support of 5G services, but continue to use MPLS-based services to CSG 2 for X2 interface communications. The upgrade at CSG 1 will not affect the existing 4G services supported by the MPLS-based network services between CSG 2 and RSG 1. RSG1 can provide MPLS services to CSG2 for 4G services as well as SRv6 services to CSG 1 for 5G services.

5. Deployment cases

With the current network, the launch of leased line service is slow, the network operation and maintenance is complex, and the configuration points are many. SRv6 can solve the issues above. There have already been several successful SRv6 deployments following the incremental deployment guidance shown in Section 3.
5.1. China Telecom Si’chuan

China Telecom Si’chuan (Si’chuan Telecom) has enabled SRv6 at the PE node of the Magic-Mirror DC in Mei’shan, Cheng’du, Pan’zhihua and other cities. The SRv6 BE tunnel has been deployed through the 163 backbone network which has the IPv6 capability. It enables the fast launch of the Magic-Mirror video service, the interconnection of the DCs in various cities, and the isolation of video services. The deployment case is shown in Figure 6.

As shown in Figure 6, IGP (some cities such as Chengdu deploy ISIS, while other cities such as Panzhihua deploy OSPF) and IBGP are deployed between PE and CR, and EBGP is deployed between CRs of cities in order to advertise the aggregation route. EBGP VPNv4 peers are set up between PEs in different cities to deliver VPN private network routes.

The packet enters the SRv6 BE tunnel from the egress PE of DC, and the packet is forwarded according to the Native IP of the 163 backbone network. When the packet reaches the peer PE, the SRH is decapsulated, and then the IP packet is forwarded in the VRF according to the service SID (for example, End.DT4).

In order to further implement the path selection, ASBRs can be upgraded to support SRv6. Different SRv6 policies are configured on the DC egress PE so that different VPN traffic reaches the peer PE.
through the 163 backbone network and the CN2 backbone network respectively.

5.2. China Unicom

China Unicom has deployed SRv6 L3VPN over 169 IPv6 backbone network from Guangzhou to Beijing to provide inter-domain Cloud VPN service. The deployment case is shown in Figure 7.

```
+--/+ Guangzhou +--/+ IPv6 +--/+ Beijing +--/+  
|PE1| CR1|---|CR2| Backbone |CR3|---|CR4| PE2|  
+--/+ Metro +--/+ 169 +--/+ Metro +--/+  
          \----------------------- EBGP VPNv4 Peer \-----------------------/  
          |<--------------- EBGP VPNv4 Peer ---------------|  
          |<---------------- L3VPN over SRv6 ----------------->  
          |<---------------- OSPF/ISIS------------------------->  
```

Figure 7. China Unicom SRv6 L3VPN case

In Guangzhou and Beijing metro networks, routers exchange basic routing information using IGP(OSPF/ISIS). The prefixes of IPv6 loopback address and SRv6 locator of routers are different, and both of them need to be imported into the IGP. The 169 backbone is a native IPv6 network. Between metro and backbone, the border routers establish EBGP peer with each other, e.g. CR1 with CR2, CR3 with CR4, to form basic connectivity. All of these constitute the foundation of overlay services, and have not been changed.

PE1 and PE2 establish EBGP peer and advertise VPNv4 routes with each other. If one site connects to two PEs, metro network will use multi RD, community and local preference rules to choose one best route and one backup.

After basic routing among networks and VPN routes between the two PEs are all ready, two PEs encapsulate and forward VPN traffic within SRv6 tunnel. The tunnel is SRv6 best effort (BE) tunnel. It introduces only outer IPv6 header but not SRH header into traffic packets. After encapsulation, the packet is treated as common IPv6 packet and forwarded to the egress PE, which performs decapsulation and forwards the VPN traffic according to specific VRF.

Guangdong Unicom has also launched the SRv6 L3VPN among Guangzhou, Shenzhen, and Dongguan, which has passed the interop test between different vendors.
With SRv6 enabled at the PE devices, the VPN service can be launched very quickly without impact on the existing traffic. With SRv6 TE further deployed, more benefits of using SRv6 can be exploited.

6. IANA Considerations

There are no IANA considerations in this document.

7. Security Considerations

TBD.

8. Contributors

Hailong Bai
China Unicom
China

Email:

Jichun Ma
China Unicom
China

Email:

Ruizhao Hu
Huawei
China

Email: huruizhao@huawei.com

Jianwei Mao
Huawei
China

Email: maojianwei@huawei.com

9. References

9.1. Normative References

[I-D.ietf-6man-segment-routing-header]
9.2.  Informative References

[I-D.matsushima-spring-srv6-deployment-status]

[I-D.peng-spring-srv6-compatibility]

Authors' Addresses

Hui Tian
CAICT
China

Email: tianhui@caict.ac.cn
Feng Zhao
CAICT
China
Email: zhaofeng@caict.ac.cn

Chongfeng Xie
China Telecom
China
Email: xiechf.bri@chinatelecom.cn

Tong Li
China Unicom
China
Email: litong@chinaunicom.cn

Jichun Ma
China Unicom
China
Email: majc16@chinaunicom.cn

Shuping Peng
Huawei Technologies
China
Email: pengshuping@huawei.com

Zhenbin Li
Huawei Technologies
China
Email: lizhenbin@huawei.com

Yaqun Xiao
Huawei Technologies
China
Email: xiaoyaun@huawei.com