Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 10, 2021

H. Tian
F. Zhao
CAICT
C. Xie
China Telecom
T. Li
J. Ma
China Unicom
R. Mwehaire
MTN Uganda Ltd.
E. Chingwena
MTN Group Limited
S. Peng, Ed.
Z. Li
Y. Xiao
Huawei Technologies
July 9, 2020

SRv6 Deployment Consideration
draft-tian-spring-srv6-deployment-consideration-03

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 design and 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

Table of Contents

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 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 [RFC8754], 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 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

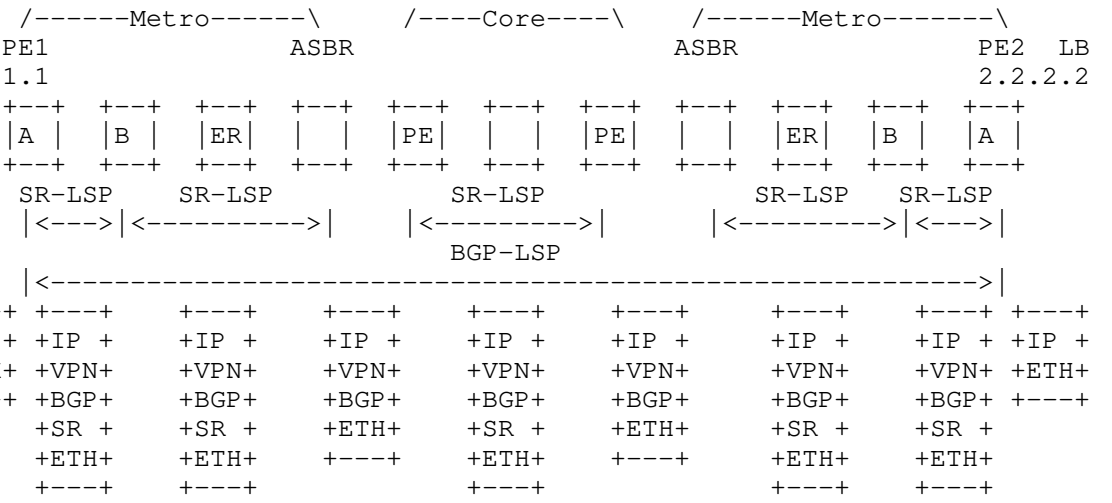
Compared with SR-MPLS, SRv6 has significant advantages especially in large scale networking scenarios.

2.1. IP Route Aggregation

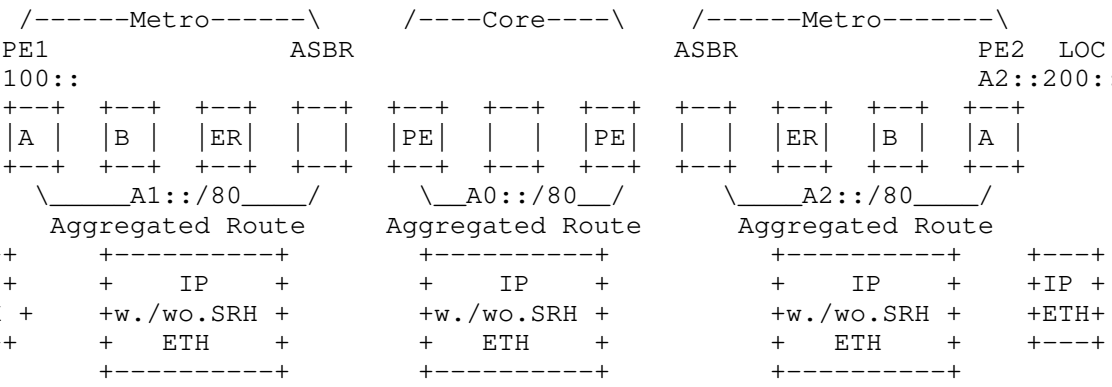
The increasing complexity of service deployment is of concern for network operators, especially in large-scale networking scenarios. With solutions such as multi-segment PW and Option A [RFC4364], the number of service-touch points has increased, and the services, with associated OAM features cannot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



(a) SR-MPLS



(b) SRv6

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.

- 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.

- 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.

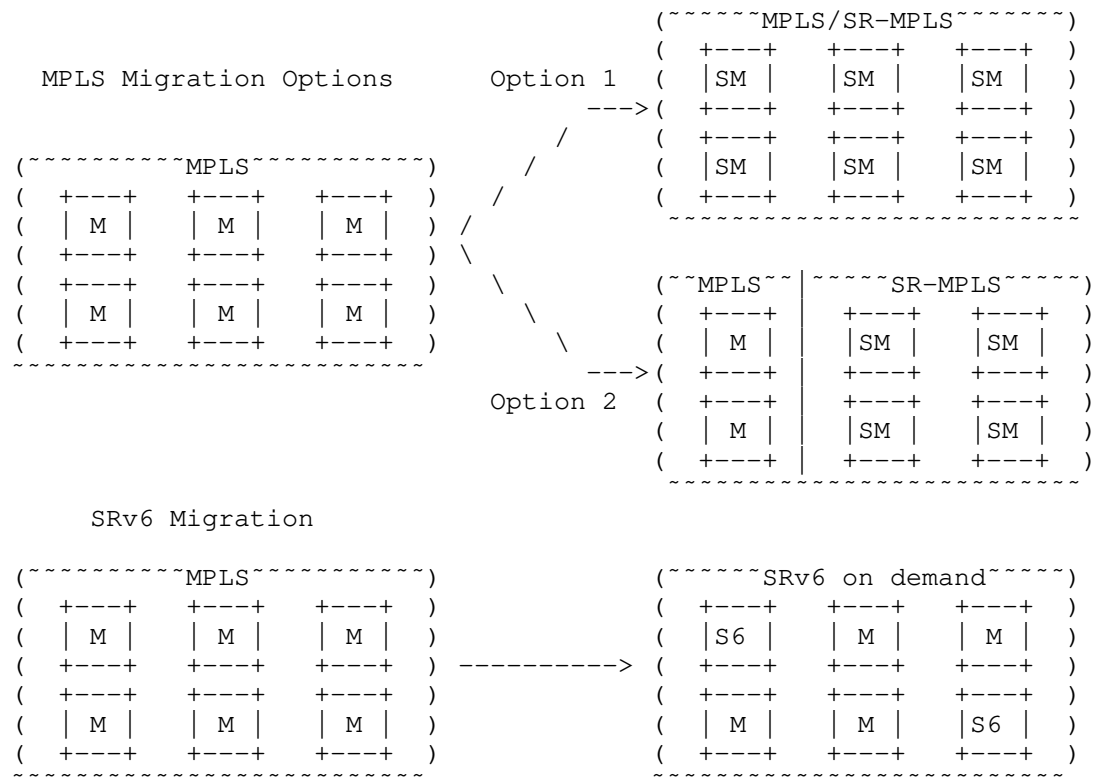


Figure 2. MPLS Domain Migration vs. SRv6 On-Demand Upgrade

2.4. Simplified Service Deployment

With SRv6, the service deployment can be significantly simplified in some scenarios.

2.4.1. Carrier's Carrier

When the customer of the VPN service carrier (Provider Carrier) is itself a VPN service carrier (Customer Carrier), it becomes the scenario of Carrier's Carrier. For this scenario, with SRv6, the service deployment can be significantly simplified.

To achieve better scalability, the CEs of the Provider Carrier (i.e. the PEs of the Customer Carriers) only distribute the internal network routes to the PEs of the Provider Carrier. The customers' routes of the Customer Carriers (i.e. from CE3 and CE4) will not be distributed into the network of the Provide Carrier. Therefore, LDP or Labeled BGP will be run between the CEs of the Provider Carrier

(i.e. CE1 and CE2 in the Figure 3) and the PEs of the Provider Carrier (i.e. PE1 and PE2 in the Figure 3), and LDP will be run between the CEs of the Provider Carrier (i.e. the PEs of the Customer Carriers) and the PEs of the Customer Carrier (i.e. PE3 and PE4 in the Figure 3). MP-BGP will be run between the PEs of the Customer Carrier. The overall service deployment is very complex.

If SRv6 is deployed by the Customer Carrier and the Provider Carrier, no LDP will be ever needed. The Locator routes and Loopback routes of the Customer Carriers can be distributed into the network of the Provider Carrier via BGP, and within each carrier's network only IGP is needed. The end-to-end VPN services can be provided just based on the IPv6 interconnections, and the customer carrier is just like a normal CE to the provider carrier, which significantly simplified the VPN service deployment.

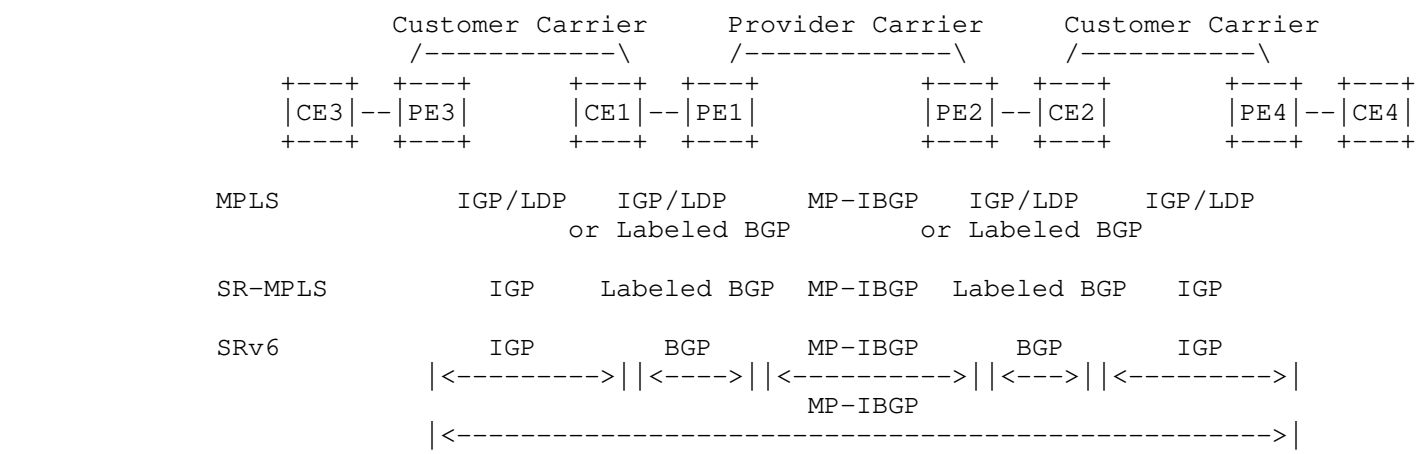


Figure 3. Service deployment with MPLS, SR-MPLS and SRv6

2.4.2. LDP over TE

In a MPLS network, generally RSVP-TE is deployed in the P nodes of the network, and LDP is running between these P nodes and the PE nodes. Customers access to VPN services via the PE nodes. This scenario is called LDP over TE, which is a typical deployment for carriers who want to achieve the TE capability over MPLS network while keep scalability. However, such network configuration and service deployment are very complex.

With SRv6 which can provide both TE capability and IP reachability, the service deployment can be significantly simplified. Only IGP and BGP are needed in the network to launch VPN services.

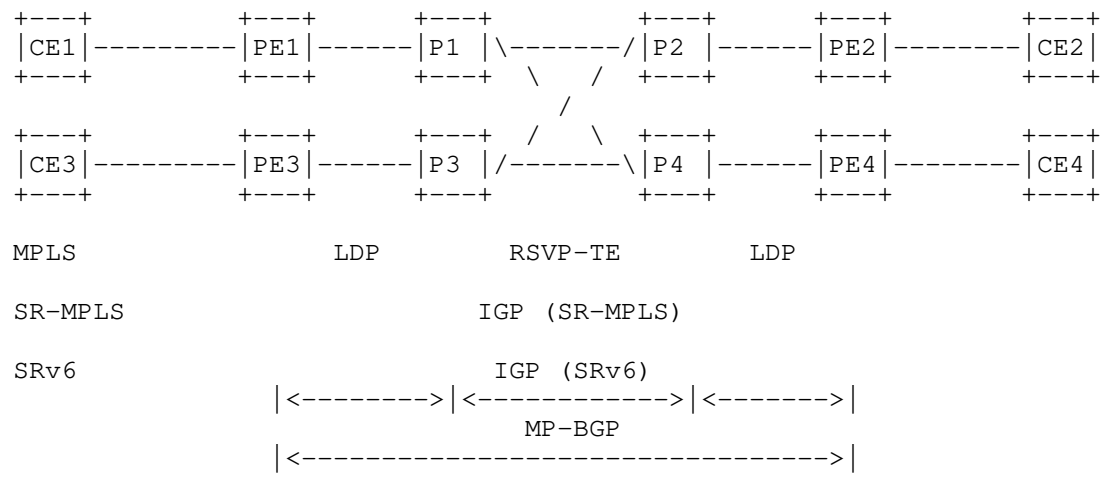


Figure 4. Service deployment with (a) MPLS/SR-MPLS vs. (b) SRv6

3. Compatibility Challenges

By adopting SR Policy, state in the network devices can be greatly reduced, which ultimately evolves the network into a stateless fabric. However, it also brings compatibility challenges on the legacy devices. In particular, the legacy devices need to upgrade software and/or hardware in order to support the processing of SRH.

Furthermore, as the segments in the segment list increase the SR Policy incrementally expands, the encapsulation header overhead increases, which imposes high performance requirements on the performance of hardware forwarding (i.e. the capability of the chipset).

This section identifies the challenges for legacy devices imposed by SRv6 in the following SPRING use cases.

3.1. Fast Reroute (FRR)

FRR is deployed to cope with link or node failures by precomputing backup paths. By relying on SR, Topology Independent Loop-free Alternate Fast Re-route (TI-LFA) [I-D.ietf-rtgwg-segment-routing-ti-lfa] provides a local repair mechanism with the ability to activate the data plane switch-over on to a loop-free backup path irrespective of topologies prior and after the failure.

Using SR, there is no need to create state in the network in order to enforce FRR behavior. Correspondingly, the Point of Local Repair,

i.e. the protecting router, needs to insert a repair list at the head of the segment list in the SRH, encoding the explicit post-convergence path to the destination. This action will increase the length of the segment list in the SRH as shown in Figure 1.

3.2. Traffic Engineering (TE)

TE enables network operators to control specific traffic flows going through configured explicit paths. There are loose and strict options. With the loose option, only a small number of hops along the path is explicitly expressed, while the strict option specifies each individual hop in the explicit path, e.g. to encode a low latency path from one network node to another.

With SRv6, the strict source-routed explicit paths will result in a long segment list in the SRH as shown in Figure 1, which places high requirements on the devices.

3.3. Service Function Chaining (SFC)

The SR segments can also encode instructions, called service segments, for steering packets through services running on physical service appliances or virtual network functions (VNF) running in a virtual environment [I-D.ietf-spring-sr-service-programming]. These service segments can also be integrated in an SR policy along with node and adjacency segments. This feature of SR will further increase the length of the segment list in the SRH as shown in Figure 1.

In terms of SR awareness, there are two types of services, i.e. SR-aware and SR-unaware services, which both impose new requirements on the hardware. The SR-aware service needs to be fully capable of processing SR traffic, while for the SR-unaware services, an SR proxy function needs to be defined.

If the Network Service Header (NSH) based SFC [RFC8300] has already been deployed in the network, the compatibility with existing NSH is required.

3.4. IOAM

IOAM, i.e. "in-situ" Operations, Administration, and Maintenance (OAM), encodes telemetry and operational information within the data packets to complement other "out-of-band" OAM mechanisms, e.g. ICMP and active probing. The IOAM data fields, i.e. a node data list, hold the information collected as the packets traverse the IOAM domain [I-D.ietf-ippm-ioam-data], which is populated iteratively starting with the last entry of the list.

The IOAM data can be embedded into a variety of transports. To support the IOAM on the SRv6 data plane, the O-flag in the SRH is defined [I-D.ietf-6man-spring-srv6-oam], which implements the "punt a timestamped copy and forward" or "forward and punt a timestamped copy" behavior. The IOAM data fields, i.e. the node data list, are encapsulated in the IOAM TLV in SRH, which further increases the length of the SRH as shown in Figure 1.

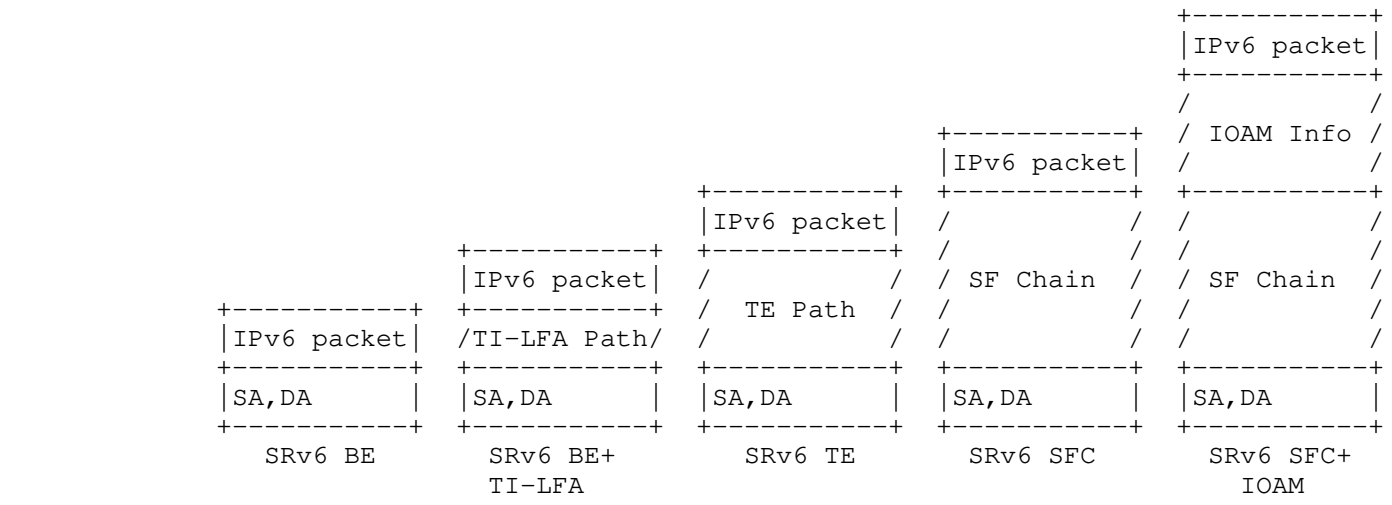


Figure 1. Evolution of SRv6 SRH

Compatibility challenges for legacy devices can be summarized as follows:

- Legacy devices need to upgrade software and/or hardware in order to support the processing of SRH
- As the SRH expands, the encapsulation overhead increases and correspondingly the effective payload decreases
- As the SRH expands, the hardware forwarding performance reduces which requires higher capabilities of the chipset

4. Solutions for mitigating the compatibility challenges

This section provides solutions to mitigate the challenges outlined in section 2.

4.1. Traffic Engineering

With strict traffic engineering, the resultant long SID list in the SRH raises high requirements on the hardware chipset, which can be mitigated by the following solutions.

4.1.1. Binding SID (BSID)

Binding SID [RFC8402] involves a list of SIDs and is bound to an SR Policy. The node(s) that imposes the bound policy needs to store the SID list. When a node receives a packet with its active segment as a BSID, the node will steer the packet in to the bound policy accordingly.

To reduce the long SID list of a strict TE explicit path, BSID can be used at selective nodes, maybe according to the processing capacity of the hardware chipset. BSID can also be used to impose the repair list in the TI-LFA as described in Section 2.1.

4.1.2. PCEP FlowSpec

When the SR architecture adopts a centralized model, the SDN controller (e.g. Path Computation Element (PCE)) only needs to apply the SR policy at the head-end. There is no state maintained at midpoints and tail-ends. Eliminating state in the network (midpoints and tail-points) is a key benefit of utilizing SR. However, it also leads to a long SID list for expressing a strict TE path.

PCEP FlowSpec [I-D.ietf-pce-pcep-flowspec] provides a trade-off solution. PCEP FlowSpec is able to disseminate Flow Specifications (i.e. filters and actions) to indicate how the classified traffic flows will be treated. In an SR-enabled network, PCEP FlowSpec can be applied at the midpoints to enforce traffic engineering policies where it is needed. In that case, state needs to be maintained at the corresponding midpoints of a TE explicit path, but the SID list can be shortened.

4.2. SFC

Currently two approaches are proposed to support SFC over SRv6, i.e. stateless SFC [I-D.ietf-spring-sr-service-programming] and stateful SFC [I-D.ietf-spring-nsh-sr].

4.2.1. Stateless SFC

A service can also be assigned an SRv6 SID which is integrated into an SR policy and used to steer traffic to it. In terms of the capability of processing the SR information in the received packets,

there are two types of services, i.e. SR-aware service and SR-unware service. An SR-aware service can process the SRH in the received packets. An SR-unaware service, i.e. legacy service, is not able to process the SR information in the traffic it receives, and may drop the received packets. In order to support such services in an SRv6 domain, the SR proxy is introduced to handle the processing of SRH on behalf of the SR-unware service. The service SID associated with the SR-unaware service is instantiated on the SR proxy, which is used to steer traffic to the service.

The SR proxy intercepts the SR traffic destined for the service via the locally instantiated service SID, removes the SR information, and sends the non-SR traffic out on a given interface to the service. When receiving the traffic coming back from the service, the SR proxy will restore the SR information and forwards it to the next segment in the segment list.

4.2.2. Stateful SFC

The NSH and SR can be integrated in order to support SFC in an efficient and cost-effective manner while maintaining separation of the service and transport planes.

In this NSH-SR integration solution, NSH and SR work jointly and complement each other. Specifically, SR is responsible for steering packets along a given Service Function Path (SFP) while NSH is for maintaining the SFC instance context, i.e. Service Path Identifier (SPI), Service Index (SI), and any associated metadata.

When a service chain is established, a packet associated with that chain will be first encapsulated with an NSH and then an SRH, and forwarded in the SR domain. When the packet arrives at an SFF and needs to be forwarded to an SF, the SFF performs a lookup based on the service SID associated with the SF to retrieve the next-hop context (a MAC address) between the SFF and SF. Then the SFF strips the SRH and forwards the packet with NSH carrying metadata to the SF where the packet will be processed as specified in [RFC8300]. In this case, the SF is not required to be capable of the SR operation, neither is the SR proxy. Meanwhile, the stripped SRH will be updated and stored in a cache in the SFF, indexed by the NSH SPI for the forwarding of the packet coming back from the SF.

4.3. Light Weight IOAM

In most cases, after the IPv6 Destination Address (DA) is updated according to the active segment in the SRH, the SID in the SRH will not be used again. However, the entire SID list in the SRH will

still be carried in the packet along the path till a PSP/USP is enforced.

The light weight IOAM method [I-D.li-spring-passive-pm-for-srv6-np] makes use of the used segments in the SRH to carry the IOAM information, which saves the extra space in the SRH and mitigate the requirements on the hardware.

4.4. Postcard Telemetry

Existing in-situ OAM techniques incur encapsulation and header overhead issues as described in section 2. Postcard-based Telemetry with Packet Marking for SRv6 on-path OAM[I-D.song-ippm-postcard-based-telemetry], provides a solution that avoids the extra overhead for encapsulating telemetry-related instruction and metadata in SRv6 packets.

5. Design Guidance for SRv6 Network

5.1. Locator and Address Planning

Address Planning is a very important factor for s successful network design, especially an IPv6 network, which will directly affect the design of routing, tunnel, and security. A good address plan can bring big benefit for service deployment and network operation.

If a network has already deployed IPv6 and set up IPv6 subnets, one of the subnets can be selected for the SRv6 Locator planning, and the existing IPv6 address plan will not be impacted.

If a network has not yet deployed IPv6 and there has not been an address plan, it needs to perform the IPv6 address planning first taking the following steps,

1. to decide the IPv6 address planning principles

2. to choose the IPv6 address assignment methods

3. to assign the IPv6 address in a hierarchical manner

For an SRv6 network, in the first step for IPv6 address planning, the following principles are suggested to follow,

1. Unification: all the IPv6 addresses SHOULD be planned altogether, including service addresses for end users, platform addresses (for IPTV, DHCP servers), and network addresses for network devices interconnection.

2. Uniqueness: every single address SHOULD be unique.

3. Separation: service addresses and network addresses SHOULD be planned separately; the SRv6 Locator subnet, the Loopback interface addresses and the link addresses SHOULD be planned separately.

4. Aggregatability: when being distributed across IGP/BGP domains, the addresses in the preassigned subnets (e.g. SRv6 Locator subnet, the Loopback interface subnet) SHOULD be aggregatable, which will make the routing easier.

5. Security: fast tracability of the assigned addresses SHOULD be facilitated, which will make the traffic filtering easier.

6. Evolvablity: enough address space SHOULD be reserved for each subset for future service development.

Considering the above-mentioned IPv6 address planning principles, it has been adopted in some deployment cases to set Locator length 96bits, function length 20bits, and args 12bits.

5.2. PSP

When Locator is imported in ISIS, the system will automatically assign END SID with Flavors such as PSP (Penultimate Segment Pop) and distribute the Locator subnet route through ISIS.

The Flavor PSP, that is, SRH is popped at penultimate segment, provides the following benefits,

1. Reduce the load of ultimate segment endpoint. Ultimate segment endpoint tends to have heavy load since it needs to handle the inner IP/IPv6/Ethernet payload and demultiplex the packet to the right overlay service.

2. Support of incremental deployment on existing network where the ultimate segment endpoint is low-end device that is not fully capable of handling SRH.

6. 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 5.

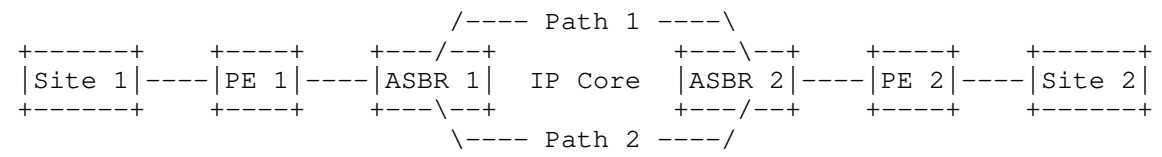


Figure 5. Reference Network Topology

Step1. 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.

7. Migration Guidance for SRv6/SR-MPLS Co-existence Scenario

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 6, 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.

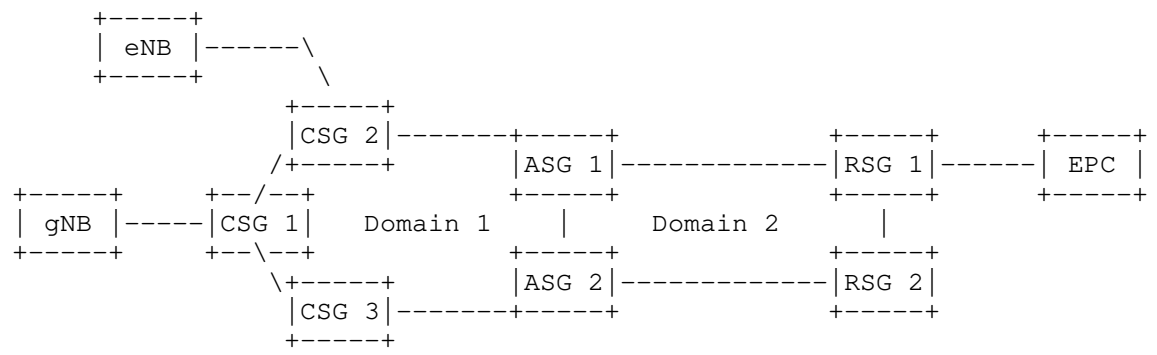


Figure 6. A 3GPP Non-Standalone deployment case

As shown in Figure 6, 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.

8. Deployment cases

With the current network, the launch of leased line service is slow, the network operation and maintainence 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.

8.1. 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 7.

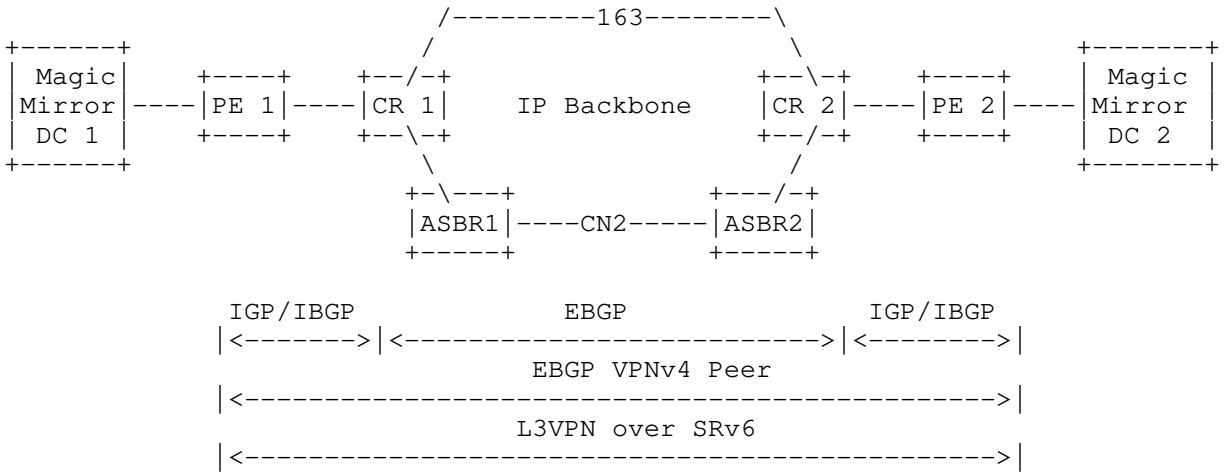


Figure 7. China Telecom Si'chuan deployment case

As shown in Figure 7, 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.

8.2. 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 8.

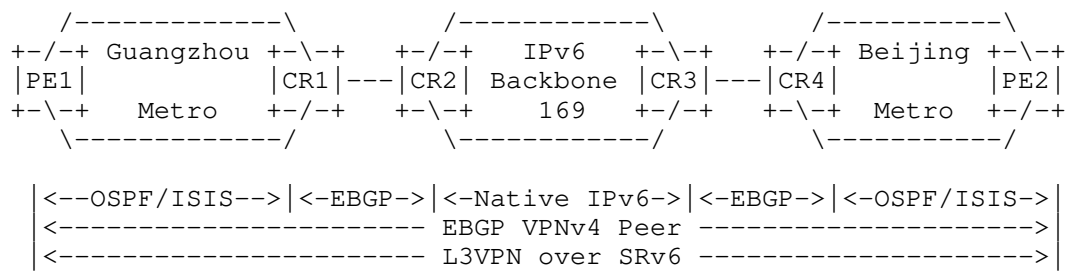


Figure 8. China Unicom SRv6 L3VPN case

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 lauched 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.

8.3. MTN Uganda

MTN Uganda has enabled SRv6 at the MPBN PE/P nodes. The SRv6 BE tunnel has been deployed through the MPBN network which has the IPv6 capability. It enables the fast service provisoning for mobile service, enterprise service and internal IT services, and also improves service SLA such as service monitoring and availability. The deployment case is shown in Figure 9.

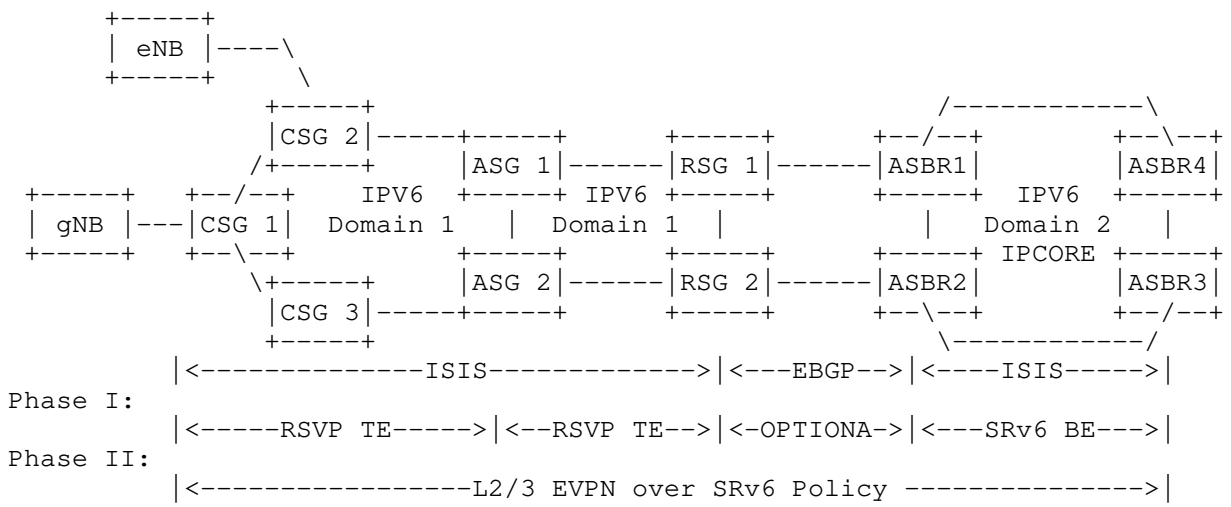


Figure 9. MTN Uganda Deployment Case

As shown in the Figure 9,

In the phase I, SRv6 BE was deployed in MPBN network. All services in the MPBN will be carried through SRv6 BE in the core network. The Option A is deployed between the IPRAN network and Core network.

In the phase II, SRv6 Policy will be deployed E2E from IPRAN to Core. Cross-domain path selection is available for mobile and enterprise services. The service will be carried in SRv6 Policy through the entire MPBN network.

L3VPN and L2VPN services will evolve to EVPN to simplify the network operation and management.

9. IANA Considerations

There are no IANA considerations in this document.

10. Security Considerations

TBD.

11. Acknowledgement

The section on the PSP use cases is inspired from the discussions over the mailing list. The authors would like to acknowledge the constructive discussions from Daniel Voyer, Jingrong Xie, etc..

12. Contributors

Hailong Bai
China Unicom
China

Email:

Jichun Ma
China Unicom
China

Email:

Huizhi Wen
Huawei Technologies
China

Email: wenhuizhi@huawei.com

Ruizhao Hu
Huawei Technologies
China

Email: huruizhao@huawei.com

Jianwei Mao
Huawei
China

Email: maojianwei@huawei.com

13. References

13.1. Normative References

[I-D.ietf-spring-srv6-network-programming]
Filsfils, C., Camarillo, P., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "SRv6 Network Programming", draft-ietf-spring-srv6-network-programming-16 (work in progress), June 2020.

[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>.

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, DOI 10.17487/RFC4364, February 2006, <https://www.rfc-editor.org/info/rfc4364>.

[RFC5659] Bocci, M. and S. Bryant, "An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge", RFC 5659, DOI 10.17487/RFC5659, October 2009, <https://www.rfc-editor.org/info/rfc5659>.

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

[RFC8754] Filsfils, C., Ed., Dukes, D., Ed., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", RFC 8754, DOI 10.17487/RFC8754, March 2020, <https://www.rfc-editor.org/info/rfc8754>.

13.2. Informative References

[I-D.ietf-6man-segment-routing-header]
Filsfils, C., Dukes, D., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", draft-ietf-6man-segment-routing-header-26 (work in progress), October 2019.

[I-D.ietf-6man-spring-srv6-oam]
Ali, Z., Filsfils, C., Matsushima, S., Voyer, D., and M. Chen, "Operations, Administration, and Maintenance (OAM) in Segment Routing Networks with IPv6 Data plane (SRv6)", draft-ietf-6man-spring-srv6-oam-05 (work in progress), June 2020.

[I-D.ietf-ippm-ioam-data]
Brockners, F., Bhandari, S., Pignataro, C., Gredler, H., Leddy, J., Youell, S., Mizrahi, T., Mozes, D., Lapukhov, P., remy@barefootnetworks.com, r., daniel.bernier@bell.ca, d., and J. Lemon, "Data Fields for In-situ OAM", draft-ietf-ippm-ioam-data-09 (work in progress), March 2020.

[I-D.ietf-pce-pcep-flowspec]
Dhody, D., Farrel, A., and Z. Li, "PCEP Extension for Flow Specification", draft-ietf-pce-pcep-flowspec-09 (work in progress), June 2020.

[I-D.ietf-rtgwg-segment-routing-ti-lfa]
Litkowski, S., Bashandy, A., Filsfils, C., Decraene, B., Francois, P., Voyer, D., Clad, F., and P. Camarillo, "Topology Independent Fast Reroute using Segment Routing", draft-ietf-rtgwg-segment-routing-ti-lfa-03 (work in progress), March 2020.

[I-D.ietf-spring-nsh-sr]
Guichard, J., Song, H., Tantsura, J., Halpern, J., Henderickx, W., Boucadair, M., and S. Hassan, "Network Service Header (NSH) and Segment Routing Integration for Service Function Chaining (SFC)", draft-ietf-spring-nsh-sr-02 (work in progress), April 2020.

[I-D.ietf-spring-sr-service-programming]
Clad, F., Xu, X., Filsfils, C., daniel.bernier@bell.ca, d., Li, C., Decraene, B., Ma, S., Yadlapalli, C., Henderickx, W., and S. Salsano, "Service Programming with Segment Routing", draft-ietf-spring-sr-service-programming-02 (work in progress), March 2020.

[I-D.li-spring-passive-pm-for-srv6-np]
Li, C. and M. Chen, "Passive Performance Measurement for SRv6 Network Programming", draft-li-spring-passive-pm-for-srv6-np-00 (work in progress), March 2018.

[I-D.matsushima-spring-srv6-deployment-status]
Matsushima, S., Filsfils, C., Ali, Z., Li, Z., and K. Rajaraman, "SRv6 Implementation and Deployment Status", draft-matsushima-spring-srv6-deployment-status-07 (work in progress), April 2020.

[I-D.song-ippm-postcard-based-telemetry]
Song, H., Zhou, T., Li, Z., Shin, J., and K. Lee, "Postcard-based On-Path Flow Data Telemetry", draft-song-ippm-postcard-based-telemetry-07 (work in progress), April 2020.

[RFC8300] Quinn, P., Ed., Elzur, U., Ed., and C. Pignataro, Ed., "Network Service Header (NSH)", RFC 8300, DOI 10.17487/RFC8300, January 2018, <https://www.rfc-editor.org/info/rfc8300>.

[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>.

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

Robbins Mwehaire
MTN Uganda Ltd.
Uganda

Email: Robbins.Mwehair@mtn.com

Edmore Chingwena
MTN Group Limited
South Africa

Email: Edmore.Chingwena@mtn.com

Shuping Peng
Huawei Technologies
China

Email: pengshuping@huawei.com

Zhenbin Li
Huawei Technologies
China

Email: lizhenbin@huawei.com

Yaqun Xiao
Huawei Technologies
China

Email: xiaoyaqun@huawei.com