Compressed SRv6 Deployment and Operations White Paper

Foreword

SRv6 supports simplified network protocols, capability openness, and programmability based on IPv6 basic technologies. It meets the requirements of emerging services such as 5G, cloud-network synergy and provides high scalability and flexibility. SRv6 uses 128-bit IPv6 addresses as segment IDs (SIDs), inheriting the advantages of flexible connection, global routing, and programmability of IPv6 addresses, as well as the advantages of SR source routing, network simplification, and path reversion. It represents an important development direction of IPv6-based networks and will become the core technology of the next generation IP networks.

However, SRv6 deployment still needs to solve various problems, such as bearer efficiency, hardware compatibility, and smooth network upgrade and migration. Many experts around the world worked together and proposed the C-SID header compression optimization solution and promoted standardization at the IETF.

This white paper aims to describe the global networking deployment of the C-SID solution since it was proposed. Chapter 1 introduces SRv6 and the rationale for SRv6 compression, serving as a reference for readers unfamiliar with SRv6. Those already versed in SRv6 may proceed directly to Chapter 2 (History of SRv6 Compression) and Chapter 3 (Deployment Scenarios and Practices of SRv6 Compression). The white paper goes over some design and deployment cases to provide reference and guidance for the industry when deploying SRv6 C-SIDs. We hope that the preceding work will accelerate SRv6 deployment, and also accelerate IP network innovation in the cloud-network era.

Contents

Foreword ii

1 Background and Requirements of SRv6 Compression 4

1.1 SRv6 Development 4

1.2 Why Does SRv6 Require Header Compression 5

1.3 Benefits of SRv6 Compression 7

2 History of SRv6 Compression 9

2.1 Development Process of SRv6 Compression Standard 9

2.2 Trial and Interop-Test of SRv6 Compression 9

3 Deployment Scenarios and Practices of SRv6 Compression 12

3.1 SRv6 Compression SID Assignment 12

3.2 SRv6 Compression Inter-AS Deployment 14

3.3 SRv6 Compression Visualization 18

3.4 SRv6 Compression Traffic Steering 19

3.5 SRv6 Compression Traffic Protection 20

4 Deployment Cases of SRv6 Compression 23

4.1 Cloud Private Network of China Mobile 23

4.2 IPRAN and Backbone Network of Carrier-M in Africa 25

5 Prospects for SRv6 Compression Deployment 28

A References 29

B Acronyms and Abbreviations 30

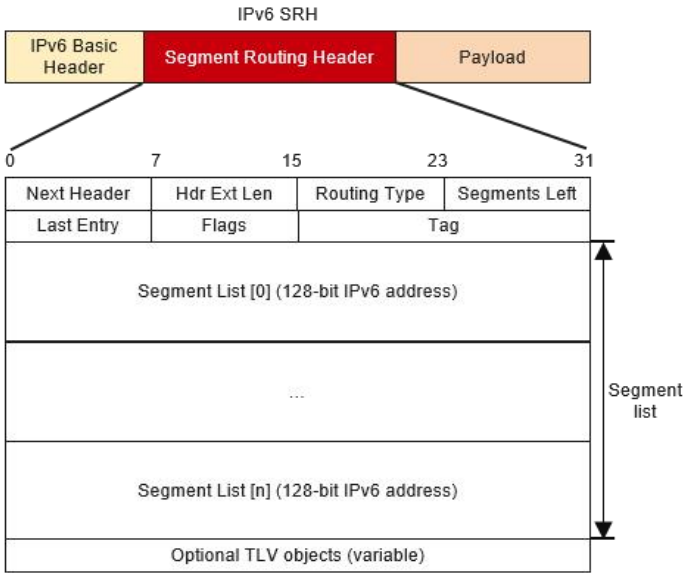
1 Background and Requirements of SRv6 Compression

1.1 SRv6 Development

SRv6 is a next-generation IP transport protocol that simplifies networks by eliminating the need to run some complex, traditional protocols. In the 5G and cloud era, it serves as the foundation for building intelligent IP networks. SRv6 combines the advantages of the source routing mechanism used in Segment Routing (SR) with the simplicity and extensibility that IPv6 offers. It also provides a multi-dimensional programming space and complies with the Software Defined Networking (SDN) paradigm, making it a powerful tool for implementing intent-based networks[1].

To implement SR based on the IPv6 data plane, a new type of IPv6 Routing Header (RH) called SRH (Segment Routing Header) is defined. The SRH format is shown in Figure 1-1.

Figure 1-1 SRH format



The SRH stores SRv6 path information (segment list, also called SID list) to specify an SRv6 explicit path. The ingress adds an SRH to each IPv6 packet, allowing transit nodes to forward

the packets based on path information contained in the SRH. SRv6 is transparent for all nodes with IPv6 support (no additional/specific information) necessary if only forwarding without specific SR functionality is required.

SRv6 programming standardization and packet encapsulation format standardization are carried out by the Internet Engineering Task Force (IETF) Source Packet Routing in Networking (SPRING) and IPv6 Maintenance (6MAN) Working Groups (WGs), respectively. The standardization of relevant control protocol extensions, for example, Interior Gateway Protocol (IGP), Border Gateway Protocol (BGP), Path Computation Element Communication Protocol (PCEP), and Virtual Private Network (VPN) extensions, are carried out by the Link State Routing (LSR), Inter-Domain Routing (IDR), Path Computation Element (PCE), and BGP Enabled ServiceS (BESS) WGs, respectively.

By the end of 2023, many SR standardization achievements had been made in IETF. Specifically, the SR architecture had been standardized through RFC 8402 "Segment Routing Architecture"[2]. Basic SRv6 standards had been standardized through RFC 8754 "IPv6 Segment Routing Header (SRH)"[3] and RFC 8986 "SRv6 Network Programming"[4] laying the foundation for SRv6 development. At present, SRv6-based IGP, BGP, and VPN extensions are being promoted by the IETF, and drafts related to VPN, Intermediate System to Intermediate System (IS-IS), Open Shortest Path First version 3 (OSPFv3), and Border Gateway Protocol-Link State (BGP-LS) have been released as RFCs. In addition, Yet Another Next Generation (YANG) model drafts regarding basic SRv6 features have been adopted by the SPRING WG and will facilitate the interconnection between third-party controllers and network devices. The maturity of protocols will promote the development of the SRv6 industry considerably.

On April 5, 2022, the 23rd MPLS SD & AI Net World Congress was held in Paris, France, under the theme "SRv6 Momentum". Senior experts and analysts from the SRv6 industry — covering device vendors, carriers, third-party independent test organizations, and standards organizations — delivered keynote speeches on SRv6 technical standards, industry cooperation, commercial deployment progress, and more. They also shared insights into the status quo, commercial deployment, and future development trends of SRv6.

By the end of 2022, European Advanced Networking Test Center (EANTC) had successfully conducted multiple SRv6 multi-vendor interoperability tests, covering basic SRv6 VPN service scenarios, SRv6 reliability, SRv6 ping/traceroute, and SRv6 Policy inter-vendor interoperability. The test results met expectations and proved the commercial deployment capability of SRv6. Furthermore, SRv6 had been commercially deployed at more than 100 sites around the world, covering Europe, East Asia, Southeast Asia, South Asia, the Middle East, North Africa, South Africa, and Latin America. It has received wide acclaim by many carriers and its global development is accelerating. In addition to carriers' sites, SRv6 is widely deployed in sectors and verticals such as government, finance, education, energy, and transportation.

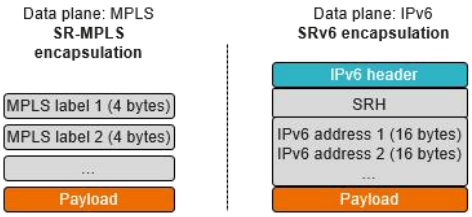
1.2 Why Does SRv6 Require Header Compression

SRv6 has been deployed in hundreds of commercial networks and is developing rapidly due to its compatibility with IPv6. However, when multiple Segment Identifiers (SIDs) are used in real-world SRv6 deployments, the ingress encapsulates an outer IPv6 basic header and a Segment Routing Header (SRH) into a packet before forwarding[3,4]. Such encapsulation increases the packet header overhead. If there are a large number of SRv6 SIDs, the SRH size increases even more, further reducing payload efficiency.

As shown in Figure 1-2, the 40-byte IPv6 basic header is equivalent to 10 Multiprotocol Label Switching (MPLS) labels in Encaps mode. In addition, SRv6 uses 16-byte IPv6 addresses as

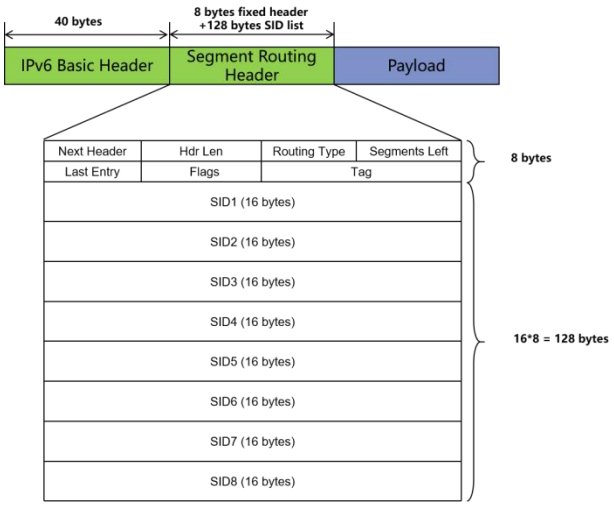
SIDs, whereas Segment Routing over MPLS (SR-MPLS) uses 4-byte MPLS labels as SIDs. This means that an SRv6 SID is four times the length of an SR-MPLS SID.

Figure 1-2 SR-MPLS and SRv6



On a large-scale network, if a forwarding path needs to be specified hop by hop, many SRv6 SIDs need to be encapsulated, which significantly increases the SRv6 header length. For example, in scenarios where packets are forwarded over an End-to-End (E2E) strict explicit path, the number of required SRv6 SIDs may be more than 5 and even as much as 10. If 8 SRv6 SIDs are used, the total length of the IPv6 header reaches 176 bytes, composed of 40 bytes for the IPv6 basic header, 8 bytes for the fixed header, and 128 bytes (16 bytes × 8) for the segment list. Figure 1-3 shows the SRv6 header overhead in this case.

Figure 1-3 SRv6 header overhead when 8 SRv6 SIDs are used

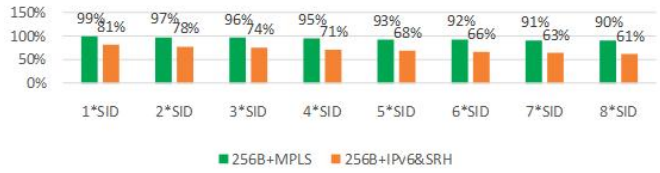


On a network with video services, packets are typically large. This means that the packet header overhead has only relatively limited impact on the payload efficiency. Figure 1-4 shows the transmission efficiency comparison between MPLS and SRv6 when the payload is 424 bytes. If there are 8 SIDs, the SRv6 bandwidth usage is only about 72%.

Figure 1-4 Transmission efficiency comparison between MPLS and SRv6 when the payload is 424 bytes

On a network without video services, most of the packets are small. In this case, if the packet header is too long, the proportion of the payload in packets decreases significantly, reducing the payload efficiency. Figure 1-5 shows the transmission efficiency comparison between MPLS and SRv6 when the payload is 256 bytes. However, if there are 8 SIDs, the SRv6 bandwidth usage decreases to about 61%.

Figure 1-5 Transmission efficiency comparison between MPLS and SRv6 when the payload is 256 bytes



Another problem caused by excessively long SRv6 packet headers is that the SRv6 packet headers are incompatible with old devices with insufficient label stack depth on the existing network. However, compatibility is really key to whether the new protocol can be widely adopted.

To support SRv6, existing devices require software and hardware upgrades. Software upgrades involve adding support for SRv6-related control protocols, such as extending IGPs and BGP to support SRv6, and have a controllable impact on live networks. In contrast, hardware upgrades are extremely challenging and usually require huge investments.

SRv6 requires a network processor to read the complete SRH (including all SIDs). A larger number of SIDs indicates a higher bandwidth requirement for the internal processing bus of a network processor, which is a key factor that affects the chip cost and power consumption. As the number of SIDs increases, the depth of the SID stack in SRv6 packets may exceed the depth that hardware can read each time, meaning that the hardware must perform a second read. This impacts the forwarding performance. Furthermore, due to SRv6 imposing high requirements on hardware for packet processing, some legacy devices on existing networks cannot support in-depth packet header replication. As a result, these devices require hardware upgrades, preventing existing networks from being smoothly upgraded to SRv6.

1.3 Benefits of SRv6 Compression

SRv6 faces practical deployment challenges, including low payload efficiency, high hardware requirements, and difficulties in existing network upgrades. So SRv6 compression is essential and it can bring the following benefits:

1. Efficient Carriage: Saving space occupied by packet encapsulation, significantly improving transmission efficiency, and reducing the cost of underlying transmission investment.

2. High Scalability: The SR Policy supports more SIDs and has better compatibility with devices on the existing network. Using compressed SIDs supports the formation of larger-scale networks.

3. Smooth Evolution: Compatible with native SRv6, inheriting all existing features. Compressed SID proposals can support a combination of compressed and non-compressed segments in a single path, which is beneficial when not all SRv6 nodes deploy the compression proposal or when 128-bit SIDs are required.

2 History of SRv6 Compression

2.1 Development Process of SRv6 Compression Standard

To improve SRv6 payload efficiency, multiple SRv6 compression solutions emerged in the industry around 2019 and the industry entered into heated discussions. For solution convergence and standardization purposes, the IETF SPRING WG temporarily set up a dedicated design team to discuss SRv6 compression requirements and analyze existing solutions. After more than one year discussions, the design team finally reached a consensus and output IETF WG drafts *draft-ietf-spring-compression-requirement*[5] and *draft-ietf-spring-compression-analysis*[6].

The IETF draft *draft-ietf-spring-compression-requirement* details the requirements to be met by specific SRv6 compression solutions. These requirements are solution-independent, ensuring that all solutions are fairly treated during requirement satisfaction assessment. Based on these requirements, the IETF draft *draft-ietf-spring-compression-analysis* analyzes in detail whether each solution meets the requirements.

G-SRv6 and uSID are two of the SRv6 compression solutions with quite similar technical implementations and can be used in the same SRH, so they are integrated into the Compressed-SID (C-SID) solution. After nearly two years of in-depth discussions, the preferred solution gradually emerged. The IETF SPRING WG finally reached a consensus on adopting the C-SID draft *draft-ietf-spring-srv6-srh-compression*[7] as a WG draft. The draft entered the Working Group Last Call (WGLC) phase in January 2024. After long discussion in SPRING WG and 6MAN WG, the consensus was finally reached, and then the draft published as an IETF standard in Request for Comments (RFC) 9800[8] in June 2025.

The IETF RFC 9800 describes the basic principles of the C-SID solution and also defines new behaviors and flavors for SRv6 compression[7][8]. Generally speaking, the C-SID solution is fully compatible with the SRv6 architecture. It mainly defines two flavors now — REPLACE-C-SID and NEXT-C-SID, where the REPLACE-C-SID and NEXT-C-SID flavors are known in the industry as G-SRv6 and uSID, respectively. Except for their differences in C-SID programming and update modes, the two flavors are implemented in a similar way, both helping to reduce the overhead by deleting redundant information from SIDs.

2.2 Trial and Interop-Test of SRv6 Compression

In the WGLC for the C-SID solution draft, more than 50 enterprises, operators and universities showed the support of moving the standard forward, which showed the great support from the whole industry.

In fact, since 2020, the industry has successfully completed multiple rounds of C-SID interoperability tests based on the C-SID draft, fully proving the feasibility of the C-SID solution.

In December 2020, Huawei worked with Cisco to conduct a complete C-SID interoperability test in a China Mobile lab, covering various items including the REPLACE-C-SID and NEXT-C-SID flavors[7][8]. In addition, China Mobile organized a total of 12 vendors to conduct large-scale REPLACE-C-SID interoperability tests. The vendors include router vendors such as Huawei, ZTE, H3C, and Ruijie Networks, network processor vendors such as Broadcom, Intel, Centec, and Marvell, test vendors such as Spirent and IXIA, and controller vendors such as China Unitects.

In 2021, Huawei completed a REPLACE-C-SID interoperability test between Huawei routers and Linux open-source software and demonstrated the test results at IETF 110 Hackathon. Moreover, China Mobile, Intel, Beijing University of Posts and Telecommunications, and other organizations initiated G-SRv6 open-source projects in the Open Networking Foundation (ONF), completed G-SRv6 development based on Open Network Operating System (ONOS) and Programming Protocol-independent Packet Processors (P4), and performed verification on China Environment for Network Innovations (CENI) networks.

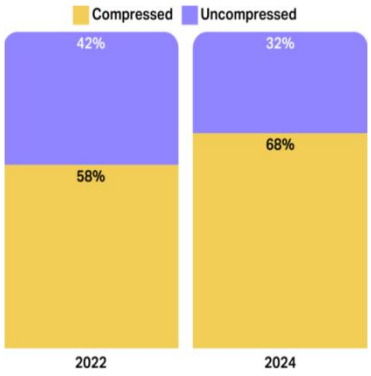
In 2022, Huawei and Cisco completed a NEXT-C-SID interoperability test in Indonesia, led by the carrier Indosat Ooredoo Hutchison (IOH). The interoperability test covered IGP, Layer 3 Virtual Private Network (L3VPN), Ethernet Virtual Private Network (EVPN) and Layer 2 Virtual Private Network (L2VPN).

In April 2023, mainstream vendors in the industry participated in the SRv6 and NEXT-C-SID interoperability tests organized by the EANTC at the MPLS, SD & AI Net World Congress, covering basic SRv6 and NEXT-C-SID functions as well as NEXT-C-SID-based L3VPN, EVPN, Traffic Engineering (TE), and Topology-Independent Loop-Free Alternate (TI-LFA) features. Another interop-test with wider scope and more vendors also happened in EANTC 2024, which showed the maturity of SRv6 compression implementations.

In terms of live-network deployment, the C-SID solution has been quickly applied to multiple networks around the world and become a basic feature of SRv6. For example, even back in November 2020, China Mobile had completed pilot deployment of REPLACE-C-SID on existing networks in China's Guangdong, Zhejiang, and Henan provinces. In the pilot deployment, devices of three vendors worked with controllers to provision REPLACE-C-SID-based L3VPN services.

According to the survey of Ciena, Compressed Segment Identifier (SID) remains the favored design choice for SRv6, with respondent preference rising to 68% from 58%, as shown in Figure 2-1.

Figure 2-1 Which Type of SRv6 forwarding is your organization planning to deploy



While compressed SID is clearly gaining supporters, this too, is a gradual evolution. What stood out in the in-depth interviews is that a fair share of respondents are concerned about the C-SIDs. But despite the perceived complexity, progress is steady.

Since 2022, the C-SID solution has been widely deployed in the networks of a number of carriers in different continents. For example, Asiacell in the Middle East, MTN in Africa, and China Mobile have widely deployed REPLACE-C-SID for commercial use since 2022, and Softbank and OSP completed NEXT-C-SID deployment. In addition, China Mobile continued to deploy REPLACE-C-SID on thousands of routers on China Mobile Network (CMNet) in 2023. Considering the maturity of SRv6 Compression solution, it has nearly become a mandatory feature in all the SRv6 deployments. Increasing numbers of networks around the world are deploying SRv6 compression in their live networks. The following section will showcase some typical SRv6 compression deployment from different regions in our planet.

3 Deployment Scenarios and Practices of SRv6 Compression

The SRv6 compression solution can be applied to all IP networks such as IP backbone, metro, mobile transport, and data center networks. It can be applied both in intra-AS and in E2E inter-AS VPN scenarios. This chapter provides suggestions for planning addresses in SRv6 compression solution deployments, describes how to deploy such a solution on typical networks scenarios, introduces traffic steering approaches, protection implement, and visualization when deploying the SRv6 compression solution.

3.1 SRv6 Compression SID Assignment

SRv6 SID consists of three parts: locator, function and arguments, as shown in Figure 3-1. SID allocation basic principle and practice can be referenced in RFC 8986[4], but operators need to provide deployment guidance for SRv6 SID planning, especially compressed SID planning for existing or future SRv6 networks.

Figure 3-1 SRv6 SID Structure

It is necessary to ensure efficient address utilization of SRv6 SID space and simplifies network management. However, existing work primarily focuses on basic SRv6 deployments without considering the complexities introduced by SRv6 compression requirements.

Prior to SRv6, operators typically allocate IPv6 addresses based on "administrative divisions" (e.g., province, city) and "network types" (e.g., IP network, wireless network, transport network). This approach assigns distinct unicast addresses (e.g., interface and loopback addresses) for network device. However, introducing SRv6 with independent allocations within each administrative division or network type creates challenges:

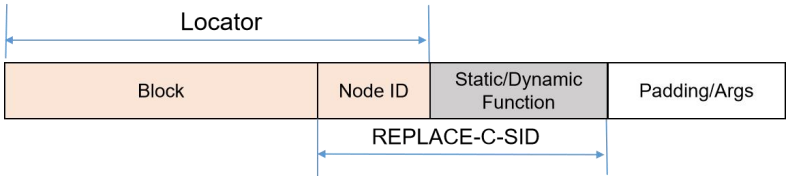
1. Fragmented SRv6 SID Space: Independent allocations result in scattered SRv6 address blocks across the provider's network, hindering SRv6 SID aggregation. Aggregation can simplify network design and allow efficient use of address space.
2. Edge Filtering Complexity: With fragmented SRv6 SID space, filtering SRv6 traffic at network edges becomes significantly more complex due to the dispersed nature of the addresses. This complicates network security and policy enforcement.

To address these two challenges, it's recommended to allocate a "dedicated IPv6 address block" (one solution is described in draft *draft-eknb-srv6ops-interdomain-sidspace*[9]) for SRv6 across the entire service provider network. It can also structure the address space by Autonomous System Number (ASN) in support of Inter-Domain SRv6 networks.

Integrated SRv6 SIDs planning can simplify edge configuration by requiring only a single policy for the dedicated SRv6 prefix. This approach of block assignment improves network management efficiency and reduces configuration complexity.

Figure 3-2 shows the SRv6 REPLACE-C-SID Structure. An SRv6 REPLACE-C-SID consists of a node identifier (Node ID) and a static or dynamic function.

Figure 3-2 SRv6 REPLACE-C-SID Structure



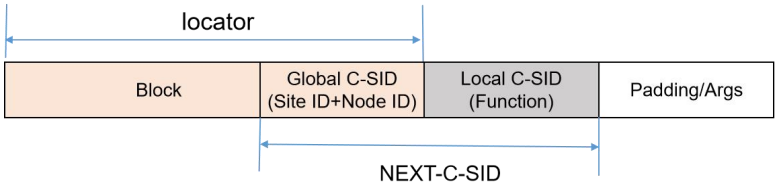
Node ID allocation can be flat or structured, with flat requiring less resources but complex management due to geographical administrative divisions. Structured allocation allows for refined administrative divisions in SRv6 SIDs. Consistency of Node IDs between compressed and uncompressed SIDs is very important, which can save SRv6 SID space, but may reduce available length for uncompressed SIDs. Sharing Node IDs for compressed and uncompressed SIDs means that functions will share the same space, which can limit the flexibility of function allocation. Additionally, this will restrict the Node ID length of non-compressed SIDs due to the length limitation for compressed SIDs.

Function ID should have enough space for different functionalities and services. It should also be considered about balancing the length of node ID and function ID for compressed SIDs. It means that due to the inherent length limitations of compressed SIDs, a trade-off must be made between the scope of manageable nodes and the range of network functions that each node can provide.

For function ID allocation, there could be dynamic or static. Dynamic assignment can be used for functions with large number of SIDs like End.X and VPN service SIDs. Static assignment with manual configuration for easy management, is suitable for functions with small number of SIDs like End SIDs.

Figure 3-3 shows the SRv6 NEXT-C-SID Structure. An SRv6 NEXT-C-SID consists of a Global C-SID and/or a Local C-SID.

Figure 3-3 SRv6 NEXT-C-SID Structure



The allocation strategy of NEXT-C-SID is designed to efficiently distribute SRv6 locator prefixes from a /32 C-SID block to different ISIS Areas, taking into account the network's structure and the need for unique identification of each node.

The NEXT-C-SID network is identified by a C-SID block, such as fccc:cc00::/32, and each node within this network is assigned a unique 16-bit Global C-SID, which is configured as an SRv6 locator in the form of fccc:cc00:XXXX::/48.

Area Classification categorizes network areas into Small, Medium, or Large, which influences how C-SIDs are allocated. C-SID Sets are groups of C-SID addresses used to encode the SRv6 Site ID and Node ID within the 16-bit Global C-SID.

The SRv6 NEXT-C-SID locator encodes several variables, including the SRv6 Flexible Algorithm (Algo), SRv6 Site ID (equivalent to ISIS Area ID), Node ID, and ISIS Level. The Flex Algo is encoded in the last two nibbles (8bits) of the C-SID block, allowing for the use of user-defined link metrics and topology constraints for IGP shortest path computations. The SRv6 Site ID & Node ID are encoded in the 16-bit Global C-SID, with the Site ID represented by Sets in the first two nibbles and the Node ID in the last two nibbles.

For NEXT-C-SID,the encoding of the Global ID Block (GIB) and the Local ID Block (LIB) share the same C-SID Sets, with the last 32 sets(E0-FF) reserved for the LIB and the remaining 224 sets(00-DF) for the GIB. This encoding allows for the distinction between Global and Local C-SIDs.

3.2 SRv6 Compression Inter-AS Deployment

The inter-Autonomous System (AS) deployment of C-SID entails configuring three distinct levels -IGP, BGP, and SRv6-which generally follows a similar process as that of SRv6 deployment.

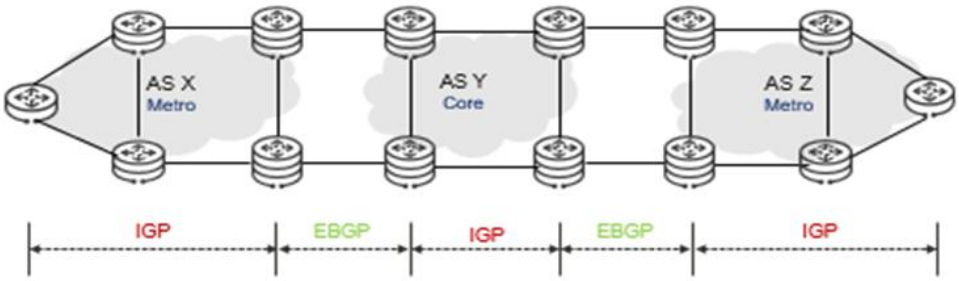
In the realm of carriers' network, end-to-end inter-AS SRv6 (spanning IPRAN/Metro and Backbone) has been implemented as an underlay solution for Mobile and 2B lease line services. Likewise, this same inter-AS SRv6 deployment scenario is also deployed within carriers' private cloud services. Especially for user services with specific SLA (Service Level Agreement) guarantees, the network provides differentiated experiences. Typical examples are outlined in chapters 4.

IGP Design

The IGP design in an inter-AS SRv6 scenario is similar to that in a 128-bit SRv6 scenario. To achieve basic network connectivity, information (such as interface addresses, whether nodes support SRv6 compression, 128-bit SRv6 SIDs, and C-SIDs) in each AS needs to be advertised on the network through an IGP. In the SRv6 compression solution, the recommended IGP is IS-IS IPv6, which cloud accommodates more nodes in a single IGP process, particularly in scenarios where SRv6 extends to the edge.

Figure 3-4 shows the IGP design in an inter-AS scenario.

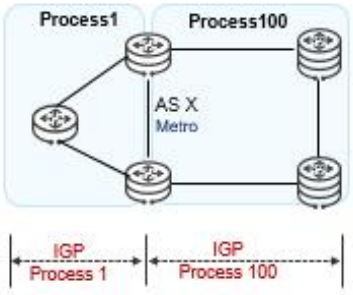
Figure 3-4 IGP design in an inter-AS scenario



In a single AS of current networks, there may exist multiple-layers networks, which correspondingly require the deployment of multiple IGP processes. For instance, the access layer and aggregation layer are planned with different IGP processes, or they may belong to different levels or areas of the same IGP process.

Figure 3-5 shows typical IGP planning inner AS scenario. Different IGP domains are deployed at different network layers. Here we take the different domain deploy different IGP instance as an example.

Figure 3-5 Multiple IGP processes inner AS



In an intra-AS scenario, only an IGP needs to be used to advertise locator routes. In an inter-AS scenario, however, both an IGP and BGP need to be used for this purpose, with BGP being mainly used to transmit locator routes between ASs.

The route advertisement and cost planning for each IGP domain are similar to the IGP design for a single AS. In an inter-AS scenario, only aggregated routes (not specific ones) are advertised between ASs. Cost values need to be designed according to the expected traffic direction, by considering factors such as traffic diversion avoidance, easy load balancing, interface bandwidth, and the transmission distance.

BGP Design

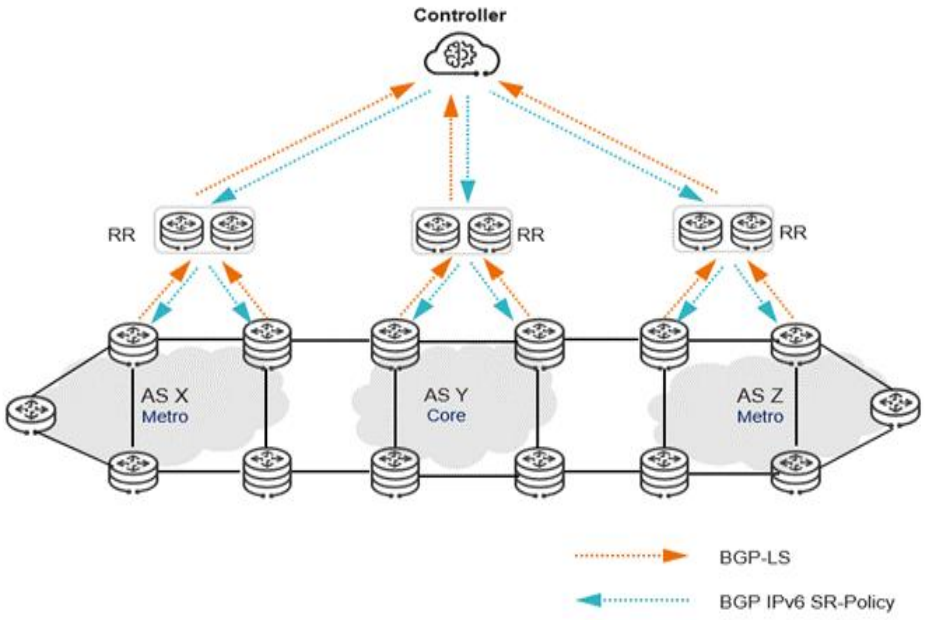
In an inter-AS SRv6 scenario, inter-AS locator and loopback routes need to be advertised through BGP. Specifically, an External Border Gateway Protocol (EBGP) peer relationship needs to be established between the Autonomous System Boundary Routers (ASBRs) in two neighboring ASs in order to advertise SRv6 loopback and locator routes. After the IGP routes

in one AS are imported to EBGP for aggregation and advertisement, EBGP imports the aggregated route to the other AS, which then imports this route as an IGP route.

Advertising public network BGP routes requires BGP peer relationships. In addition to this, path computation and delivery require BGP-LS and BGP IPv6 SR-Policy peer relationships to be established between forwarders and a controller for them to exchange information.

Figure 3-6 shows the BGP-LS and BGP IPv6 SR-Policy peer relationship design in an inter-AS scenario.

Figure 3-6 BGP-LS and BGP IPv6 SR-Policy peer relationship design in an inter-AS scenario



Forwarders use BGP-LS to report information to the controller for topology display and path computation. Such information includes the network topology, latency, SRv6 compression capability of nodes, C-SIDs, and 128-bit SRv6 SIDs. After computing an SR path, the controller delivers the path information to the ingress through the BGP IPv6 SR-Policy peer relationship to guide traffic forwarding.

The method of establishing a BGP peer relationship between each device and Route Reflector (RR) in the local AS on an inter-AS SRv6 network is similar to that on an intra-AS SRv6 network and therefore is not described here.

In an inter-AS scenario, the controller must establish BGP-LS and BGP IPv6 SR-Policy peer relationships with the RRs in different ASs so that it can obtain network topology information from the RRs and deliver SRv6 Policy routes to them. The RRs then reflect the SRv6 Policy routes to the specified ingress.

SRv6 BE for Service Transport

Because SRHs are not encapsulated in an SRv6 Best Effort (BE) scenario, the SRv6 compression solution is not involved.

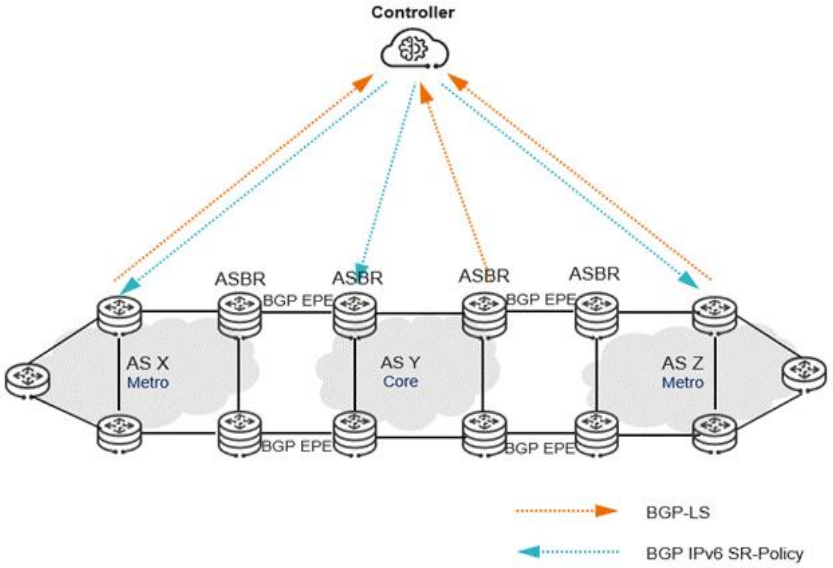
For service transport in inter-AS scenarios, the design of SRv6 BE is similar to that of native SRv6 BE. SRv6 BE only requires SRv6 locator routes in different ASs to be advertised across the ASs and VPN routes to be advertised across the ASs to the peer node through RRs.

SRv6 Policy for Service Transport

In inter-AS scenarios, E2E SRv6 Policy needs to be deployed for services that have high Service Level Agreement (SLA) requirements. The E2E paths in this case are orchestrated using intra-AS and inter-AS SIDs. As such, BGP Egress Peer Engineering (EPE) needs to be deployed between ASBRs, and EPE SIDs need to be allocated to the corresponding BGP peers. The controller can compute an E2E path consisting of intra-AS SIDs and an inter-AS BGP EPE SID and then deliver the path to the ingress. Both the intra-AS path SIDs and inter-AS EPE SIDs support C-SID-oriented reconstruction, thereby reducing the SRv6 header overhead and network resource consumption.

Figure 3-7 shows the inter-AS SRv6 Policy.

Figure 3-7 Inter-AS SRv6 Policy



In single-layer controller mode, a single controller is responsible for unified path computation and control of multiple ASs. The routing devices in each AS establish BGP-LS peer relationships with the controller and send intra-AS information (topology, SRv6 SIDs of nodes, and SRv6 SIDs of links) and inter-AS information (EPE links and their SRv6 SIDs) to the controller, which then uses this information to construct a complete network topology and compute E2E paths.

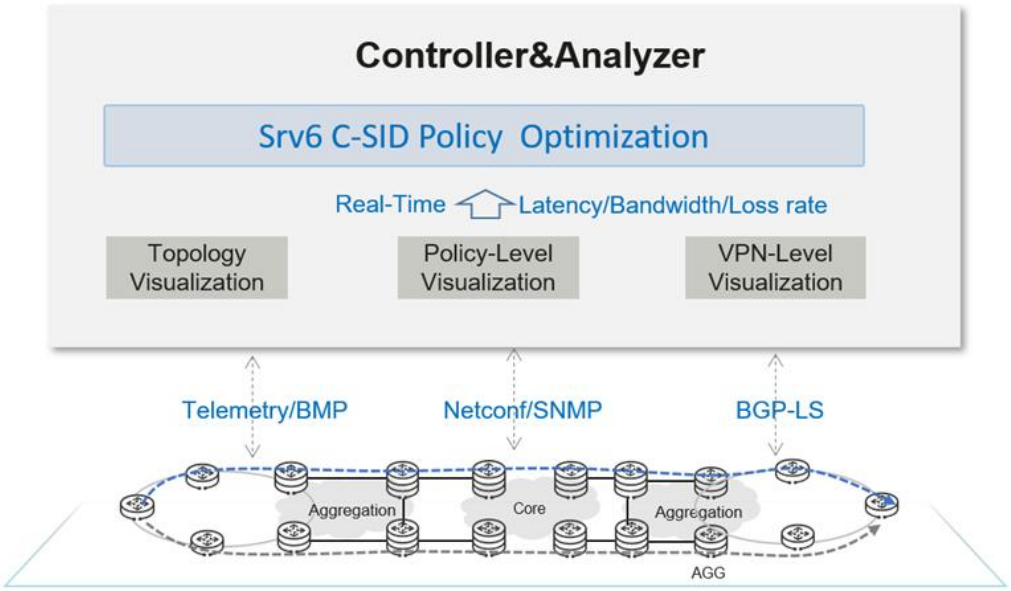
In addition, to deliver path computation results, the controller can establish BGP IPv6 SR-Policy connections with all routing devices in each AS. Based on the path computation results, the controller generates an inter-AS E2E segment list with the highest compression efficiency and delivers it to the ingress to establish an inter-AS E2E path.

3.3 SRv6 Compression Visualization

The visualization technology of SRv6 C-SID stems from two primary demands: firstly, for the fundamental operation and maintenance of numerous SRv6 tunnels; secondly, as a technological cornerstone for delivering high-quality service tunnels, the SLA monitoring and path optimization capabilities of SRv6 Policy are key methods for corresponding quality assurance. By leveraging SRv6 C-SID quality visualization, it could further enable functions such as SRv6 C-SID Policy path re-calculation and optimization.

Figure 3-8 shows the architecture of SRv6 C-SID quality visualization.

Figure 3-8 SRv6 C-SID Visualization



Current technologies have established capabilities on visualization on the following three layers:

1. **Physical Topology Visualization**: Utilizing the reporting of topology information (e.g., links, nodes) from Link Layer Discovery Protocol (LLDP) and YANG-Push, visualization of the physical topology cloud is achieved. Through integrating the per-link latency information based on Two-Way Active Measurement Protocol (STAMP) detection and BGP-LS reporting, the latency of physical links can be further visualized on the controller.
2. **SRv6 C-SID Policy Visualization:** The existing In-situ Operations, Administration and Maintenance (IOAM)/In-situ Flow Information Telemetry (IFIT) technology for SRv6 C-SID Policy enables the detection of latency, bandwidth, and packet loss rates at the SRv6 C-SID Policy level. When pushing it via the efficient reporting of Telemetry, real-time SRv6 C-SID Policy quality visualization can be presented at the controller (or analyzer). Based on these measurements, when it cannot meet the original SLA requirements (e.g., latency, bandwidth) of the SRv6 Policy, the path recalculation and optimization could been triggered.
3. **Service Visualization**: For VPN/EVPN services carried over SRv6 C-SID Policy as the underlay tunnel, service-level quality indicators can be probed using IOAM/IFIT/STAMP detection technologies. By reporting via YANG-Push and IPFIX,

real-time quality visualization at the service layer can be achieved at controller (or analyzer). Furthermore, this enables the optimization and switching of the underlay policy.

Additionally, aside from the aforementioned SRv6-based visualization technologies, BGP Monitoring Protocol (BMP) technology also offers complementary capabilities of routes' statistical analysis at the service layer.

For services adopting SRv6 C-SID Policy as the underlay tunnel, these three-level visualizations are not merely a construction of a visualization system across multiple network layers; rather, it serves as a fundamental basis to monitor and optimize the allocation of network resources, ensure a load-balanced distribution of traffic, guarantee performance and reduce congestion to provide users with a better network experience.

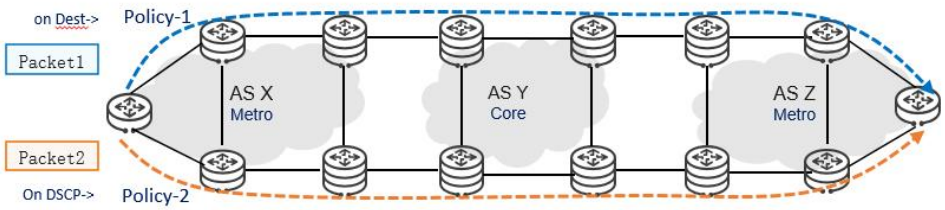
3.4 SRv6 Compression Traffic Steering

From the scenario perspective, SRv6 C-SID cloud carry traffic that in almost all of the generic use cases on the network, including the public, VPN, and EVPN traffic scenarios. SRv6 C-SID facilitates the basic traffic steering method in these scenarios, while also offering traffic steering methods to meet service requirements of SLA, resources optimization, and load balancing further.

In terms of traffic steering and provisioning mechanisms, SRv6 C-SID Policies can be statically configured on forwarders (via CLI/NETCONF) or dynamically generated by controllers and subsequently download to forwarding plane, and the dynamic approach is more conducive to automatic operation for network deployment.

For the diverse traffic steering requirements of different services, SRv6 C-SID Policies can be generally classified into two categories: steering based on destination IP address and steering based on traffic characteristics, as shown in Figure 3-9.

Figure 3-9 SRv6 C-SID Policy Steering



Each category can be further fall into several sub steering methods:

(1) Traffic Steering Based on Destination Address:

- Binding SID (BSID)-based Traffic Steering: A straightforward method that can directly specify a corresponding SRv6 C-SID Policy, or also facilitate the nesting and expansion of multiple SRv6 C-SID Policy one-by-one.
- Color-based Traffic Steering: A policy selection approach that refers to the "Color" attribute of the route of a destination IP address.

- IGP-Shortcut Traffic Steering: An SRv6 C-SID Policy forwarding method serves as an alternative to the IGP-Shortcut iteration approach used in traditional MPLS-TE tunnel scenarios.

(2) Traffic Steering Based on Traffic Characteristics:

Packets also could be distinguished and steered into SRv6 C-SID Policy based on the characteristic factors they carry inside the packets themselves, primarily including packet steering based on Differentiated Services Code Point (DSCP) (encapsulated in the IP header), 802.1Q (encapsulated in the L2 header), and Service-Class (a local defined identifier on the device).

Apart from these predefined steering methods above, SRv6 C-SID Policies also support dynamic traffic distinguishing and steering based on more packet characteristics, during the service packets already in the transmitting process:

- Traffic Steering via BGP-FlowSpec: Enables dynamic traffic steering based on matched packet field information (e.g., via ACLs) through the BGP-FlowSpec protocol.
- Traffic Steering via Policy-Based Routing (PBR): Facilitates traffic distinguishing and steering into Policy for specific packets based on matched packet information (e.g., via ACLs) through PBR.

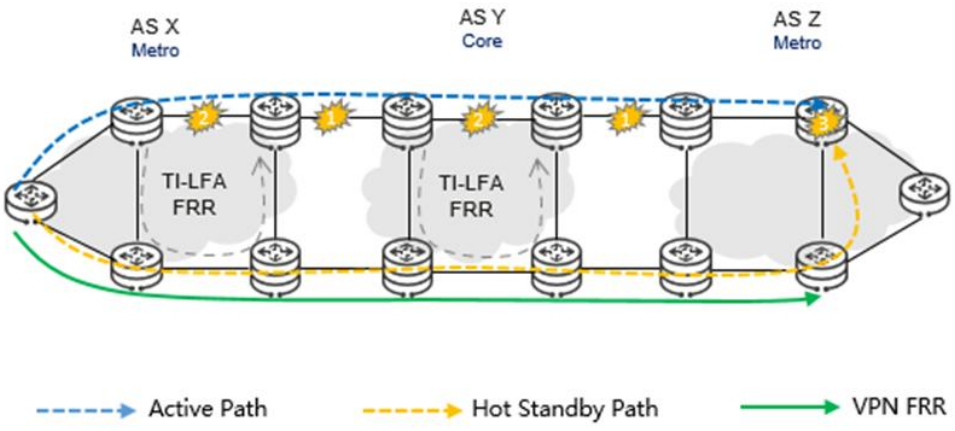
These two methods dynamically offer more fine-grained SRv6 C-SID Policy steering capabilities by leveraging a wider range of packet field information beyond just destination addresses and traffic Quality of Service (QoS) details according to the demand of network service.

3.5 SRv6 Compression Traffic Protection

In network operations, technical requirements for protection schemes arise frequently due to both anticipated upgrades and unforeseen link/device-level failures, aiming to ensure seamless service continuity. The existing SRv6-C-SID-defined protection feature framework and standard drafts encompass various levels of protection capabilities, spanning from local protection to end-to-end protection within SRv6 C-SID.

Figure 3-10 shows the SRv6 C-SID Policy protection schematic

Figure 3-10 SRv6 C-SID Policy Protection



Policy-Level Protection, Hot-Standby, operates as an end-to-end protection mechanism. When a link or node failure occurs among the SRv6 Policy path, traffic can be switched over through the pre-deployed Hot-Standby path. This process involves a switching of the Policy's Segment List at the ingress node. Upon the recovery from the failure, traffic will seamlessly switch back to the primary path：

- Establish the primary and backup paths (both use C-SID)
- Detect failure in the primary path and the head node finishes a quick switch

For practical deployments, it is advisable to integrate these switching technologies with failure detection mechanisms, such as Bidirectional Forwarding Detection (BFD) to assistant to achieve fast failure switchover.

- Echo BFD or path segment to ensure BFD detection bidirectional paths consistency
- Adjust the detection time according to the actual situation of the network to prevent network instability
- Deploy the SRv6 BE escape mechanism, used for both primary and backup paths to fail

Hot-Standby could protect the failure happening on point 1 and 2 in Figure 3-10.

Local Protection, named TI-LFA, in addition to End-to-End policy-level protection and path switching, also incorporates protection mechanisms at intermediate nodes within the Policy path, notably TI-LFA. In the event of a local failure detected at a link on the path, an immediate local protect switching is initiated.

- A fast-rerouting protection mechanism based on IGP
- Establish a backup path in advance, switch quickly from adjacent upstream nodes to the backup path when detecting a failure
- Repair list should use C-SID list

BFD detection deployment in TI-LFA scenarios is recommended to:

- BFD detection time is related to transmission distance delay, adjust the detection time according to the actual situation of the network to prevent network instability
- If deploying Hot-Standby at the same time, trigger local protection first, set the detection time path BFD to be greater than local BFD

TI-LFA could protect the failure happening on point 1 and 2 in Figure3-8.

VPN-level Protection, named VPN FRR, a method aiming to address the issue of E2E service convergence caused by PE node failures in a CE dual-homed VPN network, by pre-configuring primary and standby PEs respectively to the remote PEs.

- Ingress PE establishes C-SID path to both primary and backup egress PEs in advance
- Detect failure in the primary egress PE, ingress PE finishes a quick switch to backup egress PE by VPN FRR

VPN FRR adopts the same BFD (Bidirectional Forwarding Detection) deployment recommendations as those employed in the C-SID Policy Hot-Standby scenario. VPN FRR could protect the failure happens on point 1 and 2 in Figure 3-9.

It's important to note that Policy-level and local protection can be deployed both or independently, if both are implemented, the standard procedure involves the intermediate node first detecting the failure and promptly initiating a local path switch, followed by the Policy ingress node switching to the Hot-Standby path or recalculating the entire path upon detecting the intermediate failure.

In the absence of these protection technologies above for an SRv6 C-SID Policy, upon detecting a failure, the SRv6 Policy will initiate a re-computation of the tunnel path, load the new C-SID list to the forwarding plane, and thereby restore traffic forwarding. However, this method tends to be slower compared to scenarios where fast protection mechanisms are implemented.

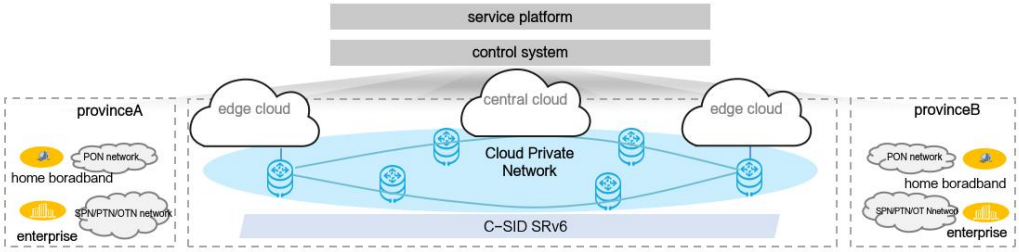
Moreover, for VPN service resilience and protection, existing CE-side switching technologies (e.g., IP Fast Reroute (FRR)) and VPN-level protection technologies (e.g., VPN FRR) continue to be viable under the SRv6 C-SID underlay carrying scenario, maintaining their inherent principles and deployment methodologies unchanged.

4 Deployment Cases of SRv6 Compression

4.1 Cloud Private Network of China Mobile

China Mobile's Cloud Private Network (CPN) has deployed SRv6 C-SID policy, covering more than 700 devices in 31 provinces across the country, with a planned bandwidth of 47 Tbps. Based on this network, China Mobile computing network base is built. China Mobile's CPN is facing the new service application scenarios of CHBN (customer/consumer, home, service/B2B, and new) and computing network. Based on the IPv6 innovation technology system of SRv6 C-SID, CPN will build a new IPv6 network with wide connection, ultra-wide, automation, certainty, low delay and ubiquitous security. Figure 4-1 shows the architecture of China Mobile CPN.

Figure 4-1 China Mobile CPN Architecture



China Mobile's CPN management and control system integrates the multi-system capabilities of Operation and Maintenance Center (OMC), network management and controller, and the unified SDN management and control architecture achieves the centralized management and control of large-scale networks. The SDN controller can provide a complete set of functions for service distribution management, network calculation, and network analysis. The northbound RESTful interface is used to receive L3VPN/EVPN, tunnel, and services configurations. In the southbound interface, NETCONF is used for collecting device configuration information and issuing service configurations. BGP-LS is used for topology collection, tunnel path issuance, and status collection. SNMP, Telemetry, etc., are used for interface and tunnel traffic collection, performance data collection, etc. Single layer SDN controller architecture, centralized IP network management control and operation and maintenance platform achieve day-level service opening and second-level bandwidth adjustment.

With the deployment of SRv6 C-SID and combined with the refined detection of the services with the flow detection technology, the path planning and optimization capabilities of the services are achieved. The full path SID arrangement makes the end-to-end service deployment and operation and maintenance simple. The Hot-Standby of SRv6 C-SID policy and BFD echo for SRv6 C-SID policy are deployed, and the TI-LFA and micro-loop prevention are deployed on demand for local protection, so as to achieve high reliable quality assurance network.

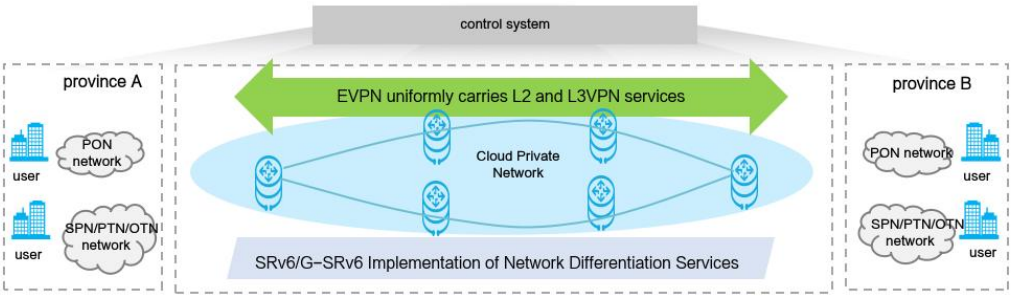
The CPN deploys SRv6 C-SID policy technology to support the creation of new and intelligent VPN dedicated line services and cloud computing network integration services.

(1) New VPN Dedicated Line

Traditional MPLS VPN can provide undifferentiated services for headquarters and branches connections, except for bandwidth. Based on IGP shortest path forwarding, traditional MPLS VPN dedicated line have problems such as long and short path latency imbalance and bandwidth limitations, etc.

As shown in Figure 4-2, CPN deploys new technologies such as L2/L3 EVPN and SRv6/SRv6 C-SID in the network to provide new VPN dedicated line services. The control plane of the new VPN dedicated line is unified, and L2/L3 services are uniformly carried. Combined with network slicing, flow detection and other technologies, differentiated carrying is provided for the requirements of different users and services , supporting new service capabilities such as low latency dedicated lines, ultra-high bandwidth dedicated lines, and high reliability dedicated lines.

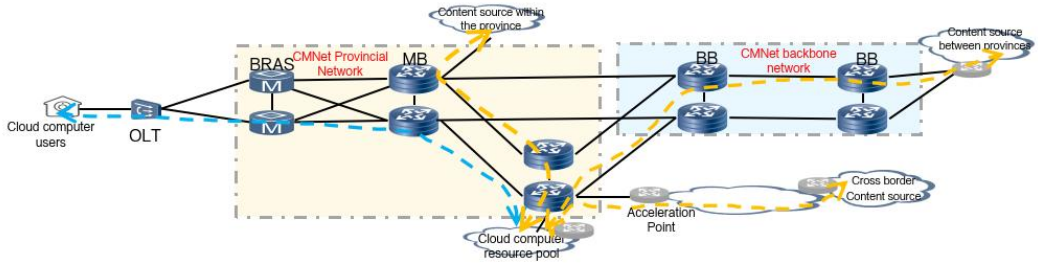
Figure 4-2 New VPN Dedicated Line Network Diagram



(2) Cloud Computer Service

Figure 4-3 shows the network diagram of Cloud Computer Service. To meet the requirements of home users to run large games and software programs through low-cost terminals, cloud computers can provide virtual hosts, and users can install applications by themselves. When accessing domestic and cross-border internet, services can be accelerated on demand. Home broadband users access the cloud computer resource pool through Broadband Remote Access Server (BRAS), which can identify their service based on their service IP, and steer the traffic to the SRv6 C-SID acceleration channel on demand. For provincial content source, based on the source IP and destination IP, the traffic is steered into the SRv6 C-SID low latency channel of the CMNet provincial network; for cross provincial content source, the traffic is steered into SRv6 C-SID low latency paths through BGP-FlowSpec on CMNet backbone (BB) devices; for cross-border content source, the traffic is identified as requiring accelerated service and sent to international exports through network acceleration points. The network accelerates cloud computer access to intra provincial, inter provincial, and cross-border content source services on demand.

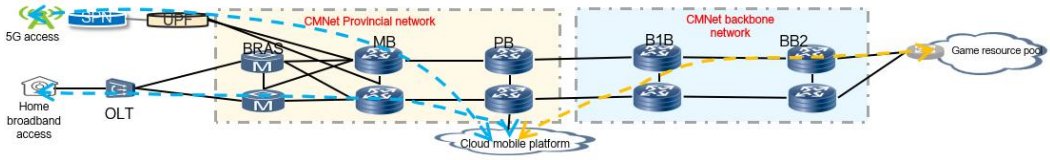
Figure 4-3 Cloud Computer Service Network Diagram



(3) Cloud Mobile Phone

Figure 4-4 shows the network diagram of Cloud Mobile Phone Service. To meet the security and privacy requirements of customers running large scale games through cloud mobile phones, internet acceleration services can be opened on demand during domestic internet access. The acceleration segment is divided into user to cloud mobile phone platform and cloud mobile phone platform to third-party content sources. Users can use home broadband Passive Optical Network (PON) to access CMNet metropolitan/provincial networks on BRAS, or use wireless 5G via Slicing Packet Network (SPN)/PON to access CMNet metropolitan/provincial networks. For the traffic of users accessing cloud mobile platforms, by identifying service through cloud mobile IP addresses, CMNet provincial network can use SRv6 C-SID to ensure the service traffic steered into low latency paths, achieving smooth access for cloud mobile phones. Users can access third-party content sources through cloud mobile phones, and use BGP-FlowSpec based on IP addresses to steer service traffic for bidirectional acceleration, achieving cross provincial content source access.

Figure 4-4 Cloud Mobile Phone Service Network Diagram

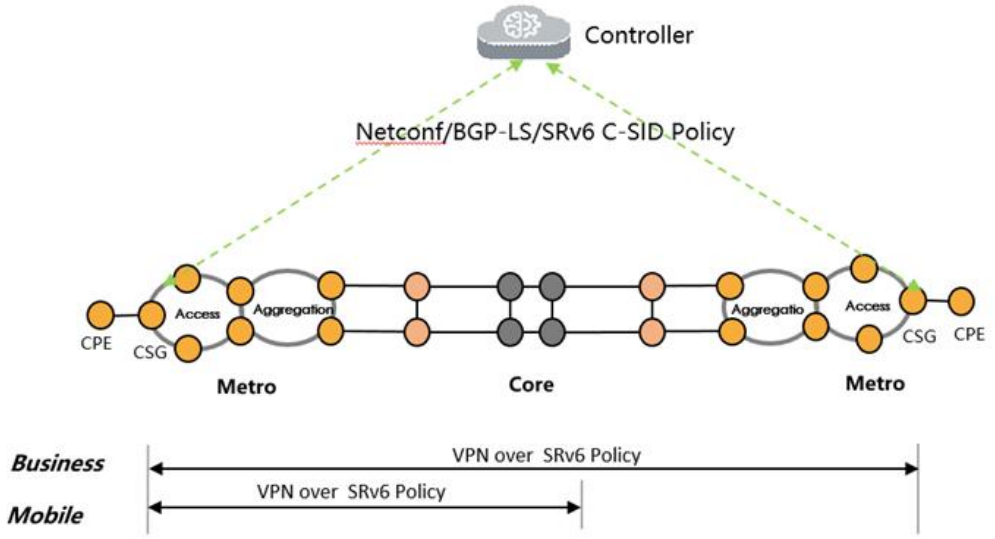


China Mobile's large-scale deployment of SRv6 C-SID policy in the cloud private network can provide low latency guarantee for key services and deterministic network services. China Mobile's scale deployment of SRv6 C-SID low latency plane based on the internet services in the CPN has accelerated the evolution of IP network.

4.2 IPRAN and Backbone Network of Carrier-M in Africa

Africa Carrier-M, taking a typical operator's IP Radio Access Network (IPRAN) and backbone network topology, has embraced VPNs over the end-to-end SRv6 Policy as its targeted deployment strategy for both the Mobile and Enterprise services that across multiple domains, encompassing both IPRAN and backbone networks, as shown in Figure 4-5. These end-to-end services can potentially traverse over 20 nodes with 20 SIDs in the SRv6 list.

Figure 4-5 SRv6 C-SID technology deployment for Carrier-M in Africa



On the network above:

- SRv6 C-SID policy is deployed on the IPRAN to carry mobile services such as voice,data and signal of 2G, 3G, 4G LTE scenarios; SRv6 BE to carry X2/Xn.
- SRv6 C-SID Policy is deployed between CSG in IPRAN and remote CSG in other IPRAN to carry E2E enterprise services.
- L3 EVPN and L2VPN implemented for Mobile and enterprise services.
- TI-LFA + VPN FRR deployed to protect link or node faulty.

Upon deploying the SRv6 C-SID technology, comparing with the original uncompressed SRv6 deployment, the statistical findings reveal:

In extreme 20-hop scenarios:

The SRv6 packet header consists of the IPv6 basic header and the SRH (Segment Routing Header) extension header. The length of the IPv6 basic header is fixed at 40 bytes. In the SRH extension header, the fixed header is 8 bytes, and each SRv6 SID is 128 bits, i.e., 16 bytes. In a 20-hop scenario, the Segment List contains 20 SRv6 path SIDs and one VPN SID, with a length of 336 bytes. Therefore, the length of the SRv6 packet header in a 20-hop scenario is 384 bytes.

The SRv6 C-SID technology reduces the overhead of the Segment List by carrying compressed generalized SIDs (G-SIDs). Typically, a G-SID uses a 32-bit length, every four 32-bit G-SIDs are combined into a 128-bit (16-byte) G-SID container. 20-hop G-SIDs can form five G-SID containers. In a 20-hop scenario that includes an uncompressible VPN SID (16 bytes). So the length of the Segment List is 96 bytes. The IPv6 basic header and the SRH are the same. Therefore G-SRv6 packet header in a 20-hop scenario is 144 bytes.

In this context, when carrying 3G services with an average packet length of 300 bytes, the SRv6 C-SID technology can improve the carrying efficiency from 43.9% to 67.6%. When carrying 4G services with an average packet length of 700 bytes, the carrying efficiency can be improved from 64.6% to 82.9%.

In average 10-hop scenarios:

Similarly, in a 10-hop scenario, it can be calculated that the length of the SRv6 packet header is 208 bytes, and the length of the G-SRv6 packet header is 68 bytes. When carrying 3G services, G-SRv6 can improve the carrying efficiency from 57.2% to 78.1%; when carrying 4G services, the carrying efficiency can be improved from 75.8% to 89.3%.

In multi-hop cross-domain networks of this type, the implementation of SRv6 C-SID technology not only satisfies operational simplification and service requirements but also achieves cost-effectiveness and efficient overhead reduction for SRv6 Policy deployments.

5 Prospects for SRv6 Compression Deployment

This white paper started with the background and history of SRv6 compression, and then introduced the deployment practice of SRv6 compression, including the SID assignment, inter-AS, visualization, traffic steering and protection, etc. This white paper also briefly introduces a series of commercial deployment cases from the industry leading operators such as China Mobile, Swisscom, Deutsche Telekom, MTN and Alibaba Cloud etc., around the world. The successful deployment cases show that the significant benefits of using SRv6 compression in networks.

Because of the standardization maturity of SRv6 and SRv6 compression in IETF, and the maturity of vendors' implementation readiness, SRv6 compression has been a required feature in SRv6 commercial deployments, and has been deploying on more than 350 networks around the world.

In IETF, the standardization work also is starting to transit from SRv6 protocol extension to operation. A dedicated SRv6OPS WG has been formed to discuss the operational aspects of deploying and managing SRv6 networks.

We would like to encourage more discussion and collaboration with partners on SRv6 compression deployment globally to speed up the deployment of SRv6 compression, and drive the technology evolvement to enable an intelligent network, increasing the revenue of networks, bring better internet services for the world.

A References

[1] CLEMM A, CIAVAGLIA L, GRAVILLE L Z, et al. Intent-Based Networking - Concepts and Definitions [EB/OL]. (2022-10)[2024-09-10]. RFC 9315.

[2] FILSFILS C, PREVIDI S, GINSBERG L, et al. Segment Routing Architecture [EB/OL]. (2018-12-19)[2024-09-10]. RFC 8402.

[3] FILSFILS C, DUKES D, PREVIDI S, et al. IPv6 Segment Routing Header (SRH) [EB/OL]. (2020-03-14)[2024-09-10]. RFC 8754.

[4] FILSFILS C, CAMARILLO P, LEDDY J, et al. SRv6 Network Programming [EB/OL]. (2021-02-01)[2024-09-10]. RFC 8986.

[5] CHENG W, XIE C, BONICA R, et al. Compressed SRv6 SID List Requirements [EB/OL]. (2023-04-03)[2024-09-10]. draft-ietf-spring-compression-requirement.

[6] BONICA R, CHENG W, DUKES D, et al. Compressed SRv6 SID List Analysis [EB/OL]. (2023-04-03)[2024-09-10]. draft-ietf-spring-compression-analysis.

[7] CHENG W, FILSFILS C, LI Z, et al. Compressed SRv6 Segment List Encoding [EB/OL]. (2023-10-23)[2024-09-10]. draft-ietf-spring-srv6-srh-compression-09.

[8] CHENG W, FILSFILS C, LI Z, et al. Compressed SRv6 Segment List Encoding [EB/OL]. (2025-06-30)[2025-07-09]. RFC 9800.

[9] KLINE E, BURAGLIO N. SID Space (5f00::/16) Inter-domain Addressing Recommendations [EB/OL]. (2024-11-05)[2025-07-04]. draft-eknb-srv6ops-interdomain-sidspace.

B Acronyms and Abbreviations

Acronym and Abbreviation	Full Name
5G	Fifth Generation/5th Generation
6MAN	IPv6 Maintenance
ACL	Access Control List
AS	Autonomous System
ASBR	Autonomous System Boundary Router
BE	Best Effort
BFD	Bidirectional Forwarding Detection
BESS	BGP Enabled ServiceS
BGP	Border Gateway Protocol
BGP-LS	Border Gateway Protocol-Link State
BMP	BGP Monitoring Protocol
BRAS	Broadband Remote Access Server
CENI	China Environment for Network Innovations
CMNet	China Mobile Network
CPN	Cloud Private Network
CRH	Compact Routing Header
C-SID	Compressed SID
DSCP	Differentiated Services Code Point
E2E	End-to-End
EANTC	European Advanced Networking Test Center
EBGP	External Border Gateway Protocol

Acronym and Abbreviation	Full Name
EPE	Egress Peer Engineering
EVPN	Ethernet Virtual Private Network
FRR	Fast Reroute
G-SRv6	Generalized SRv6
HSB	Hot-Standby
ID	Identifier
IDR	Inter-Domain Routing
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IFIT	In-situ Flow Information Telemetry
IGP	Interior Gateway Protocol
IOAM	In-situ Operations, Administration and Maintenance
IP	Internet Protocol
IPRAN	IP Radio Access Network
IPv6	Internet Protocol version 6
IS-IS	Intermediate System to Intermediate System
IOH	Indosat Ooredoo Hutchison
L2VPN	Layer 2 Virtual Private Network
L3VPN	Layer 3 Virtual Private Network
LSR	Link State Routing
MPLS	Multi-protocol Label Switching
OMC	Operation and Maintenance Center
ONF	Open Networking Foundation
ONOS	Open Network Operating System
OSPFv3	Open Shortest Path First version 3
P4	Programming Protocol-independent Packet Processors
PCEP	Path Computation Element Communication Protocol
PBR	Policy-Based Routing
PON	Passive Optical Network
PSP	Penultimate Segment Pop of the SRH

Acronym and Abbreviation	Full Name
QoS	Quality of Service
RFC	Request For Comment
RH	Routing Header
SDN	Software Defined Networking
SID	Segment Identifier
SLA	Service Level Agreement
SPN	Slicing Packet Network
SPRING	Source Packet Routing in Networking
SR	Segment Routing
SRH	Segment Routing Header
SR-MPLS	Segment Routing over MPLS
SRv6	Segment Routing over IPv6
STAMP	Simple Two-Way Active Measurement Protocol
TE	Traffic Engineering
TI-LFA	Topology-Independent Loop-Free Alternate
USD	Ultimate Segment Decapsulation
uSID	Micro SID
USP	Ultimate Segment Pop of the SRH
VPN	Virtual Private Network
vSID	variable length SID
VXLAN	Virtual Extensible Local Area Network
WG	Working Group
WGLC	Working Group Last Call
YANG	Yet Another Next Generation

Contributors

China Mobile: Xiaodong Duan, Weiqiang Cheng, Yisong Liu

Bell Canada: Daniel Voyer, Daniel Bernier, Clayton Hassan,

Swisscom: Thomas Graf

Deutsche Telekom： Nicolai Leymann

Alibaba： Linjian Song

MTN: Zoltan Miklos

Telefonica: Luis Contreras