IP网络系列丛书

SRv6

主编：骆兰军

数据通信数字化信息和内容体验部 出品

HUAWEI

版权声明

主编： 骆兰军

主要参与人员： 彭书萍 卢瑞强

发布日期： 2021-07-09

发布版本： 02

前言

主编简介

骆兰军：2010 年加入华为，长期从事数据通信产品文档开发工作，曾参与《 SRv6 网络编程：开启 IP 网络新时代 》一书的编写。

本书内容

本书重点探索 SRv6 诞生的时代背景，揭示 SRv6 广受瞩目的原因，阐述 SRv6 的技术优势，描绘 SRv6 的广袤发展空间。本书还在第 4 章和第 5 章简要介绍了 SRv6 的工作原理，理解这些内容，会帮助大家更深刻地理解 SRv6 技术的独特价值。

读者对象

本书适合服务提供商和企业的中高层管理人员、网络规划工程师、网络设计工程师，也适合想了解前沿 IP 网络技术的读者阅读。SRv6 涉及许多基础知识，阅读本书需要有一定的 IP 网络技术基础，比如了解 IP 网络的架构，了解 IP 路由和 VPN 技术等。

符号约定

对正文中重点信息的补充说明。“说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

表示如不避免则可能导致轻微或中度伤害的具有低等级风险的危害。

目录

第1章
SRv6 简介

IPv6 经过 20 多年的发展并未得到广泛的部署和应用，SRv6（Segment Routing over IPv6，基于 IPv6 的段路由）的出现顿时使 IPv6 焕发出非比寻常的活力。随着 5G 和云业务的发展，IPv6 扩展报文头蕴藏的创新空间正在快速释放，基于其上的应用不断变为现实，人类正在加速迈入 IPv6 时代。

SRv6 是新一代 IP 承载协议，可以简化并统一传统的复杂网络协议，是 5G 和云时代构建智能 IP 网络的基础。SRv6 结合了 Segment Routing 的源路由优势和 IPv6 的简洁易扩展特质，而且具有多重编程空间，符合 SDN（Software Defined Network，软件定义网络）思想，是实现意图驱动网络的利器。

SRv6 丰富的网络编程能力能够更好地满足新的网络业务的需求，而其兼容 IPv6 的特性也使得网络业务部署更为简便。SRv6 不仅能够打破云和网络的边界，使运营商网络避免被管道化，将网络延伸到用户终端，更多地分享信息时代的红利，还可以帮助运营商快速发展智能云网，实现应用级的 SLA 保障，使千行百业广泛受益。

第2章
SRv6 的产生背景

SRv6从被提出到现在不过几年的时间，已经有多篇文稿成为IETF的RFC标准，截至2020年底，全球已经有上百个商用部署局点，其发展速度之快在IP技术的历史上并不多见，那么SRv6是什么？承载着什么历史使命呢？本章将从IP网络发展的历史展开，分析IP/MPLS网络发展过程中遇到的挑战，揭示SRv6产生的历史背景。

2.1 IP/MPLS 网络面临的挑战

在网络发展初期，为满足不同的业务需求，存在着多种网络形态，其中最主要的是电信网络和计算机网络之间的竞争，它们各自的代表性技术分别是 ATM（Asynchronous Transfer Mode，异步传输模式）和 IP。最终随着网络规模变大、网络业务变多，简洁的 IP 战胜了复杂的 ATM。

但是 IP 网络也确实需要一定的 QoS 保障，而且 IP“最长匹配查表”方式面临着转发性能较差的问题。为此，业界做了很多的探索。1996 年，MPLS 技术的出现解决

了这些问题。MPLS 是一种介于二层和三层之间的“2.5 层”技术，支持 IPv4 和 IPv6 等多种网络层协议，且兼容 ATM 与以太网等多种链路层技术。

IP 与 MPLS 结合，能够在无连接的 IP 网络上提供 QoS 保障，并且 MPLS 标签交换转发方式解决了 IP 转发性能差的问题，所以 IP/MPLS 在一段时期内获得了成功。

随着网络业务的不断发展和网络规模的不断扩大，IP/MPLS 的组合也遇到了如下问题和挑战：

1. **转发优势消失**：随着路由表项查找算法的改进提升，尤其是以 NP 处理器为代表的硬件更新换代，当前 MPLS 的转发性能优势相比于 IP 转发已经不再那么明显。
2. **云网融合困难**：随着互联网和云计算的发展，云数据中心越来越多。为满足多租户组网的需求，多种 Overlay 的技术被提出，典型的就是 VXLAN（Virtual eXtensible Local Area Network，虚拟扩展局域网）。历史上也有不少人尝试过将 MPLS 引入数据中心来提供 VPN 服务，但由于网络管理边界、管理复杂度和可扩展性等多方面的原因，MPLS 进入数据中心的尝试均告失败。
3. **跨域部署困难**：MPLS 被部署到不同的网络域，例如 IP 骨干网、城域网和移动承载网等，形成了独立的 MPLS 域，因此也带来了新的网络边界。但很多业务需要端到端部署，所以在部署业务时需要跨越多个 MPLS 域，就带来了复杂的 MPLS 跨域问题。历史上，MPLS VPN 有 Option A/B/C 等多种形式的跨域方案，业务部署复杂度相对都较高。
4. **业务管理复杂**：在 L2VPN、L3VPN 多种业务并存的情况下，设备中可能同时存在 LDP、RSVP、IGP、BGP 等协议，业务部署和管理复杂，不适合 5G 和云时代大规模业务部署。
5. **协议状态复杂**：在 IGP 速度提升以后，由 IGP 自身来分标签已经不是问题，不再需要 LDP。RSVP-TE 协议实现比较复杂，需要交互大量的协议报文来维持连接的状态，节点和隧道越多，状态数越多，这种指数级状态增长给网络的中间节点带来了很大的性能压力，不利于组建大规模网络。RSVP-TE 实质上在模仿一个 SDH 管道，所以不能有效地进行负载分担，如果人工建立多条隧道来完成负载分担功能，又加剧了复杂度。

2.2 SDN 思想对网络的影响

深究 MPLS 问题的根本原因，是因为传统 MPLS 是分布式架构，每台设备只看到自己的状态，而如果需要知道邻居状态，就必须依靠大量信令去实现。

如果使用集中式架构，增加一个集中控制的节点，统一进行路径计算和标签分发，问题岂不是迎刃而解？而这，也就是 SDN 的重要思路。

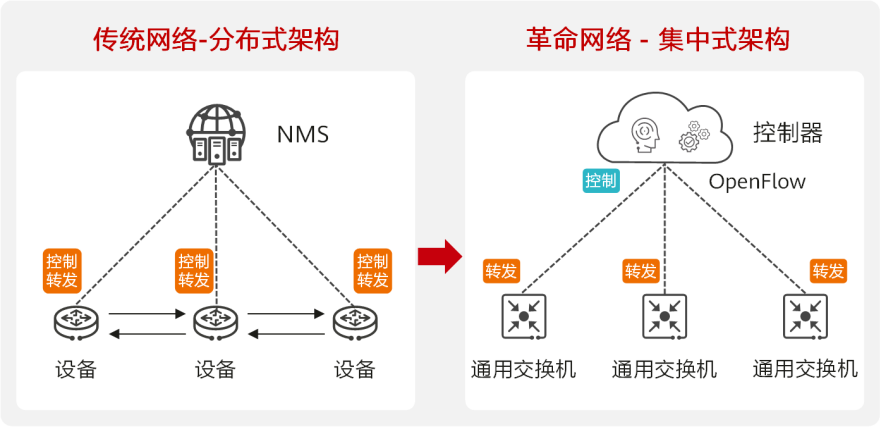
最初的 SDN 实践代表是 OpenFlow，OpenFlow 是一种 SDN 控制平面和数据平面之间交互的通信协议。如图 2-1 所示，基于 OpenFlow 的网络需要对网络硬件设施全部进行升级或者替换，业界称之谓革命型网络。这种网络结构简单，能够支持集中编程，但却难以企及，最主要有几个方面原因：

其一是性能原因，OpenFlow 的转发流表下发速率有瓶颈，而且控制器到转发器的传输速度还依赖于网络本身，对网络要求极高。

其二是业务原因，Openflow 难以适应网络中复杂的业务部署，尤其是骨干网中 L2/L3 VPN、QoS、组播和分片等各种业务需求并存的情况。

其三是经济原因，OpenFlow 需要新硬件的支持，无法保护已有投资。

图2-1 传统网络与革命型网络



因此，Openflow 适用于流表较为简单，转发行为固定的交换机组网，但是承载网需要一种技术，既可以满足 SDN 的管控需求，又可以满足承载网的多业务、高性能和高可靠等需求。

2.3 Segment Routing 的产生

OpenFlow 的初衷是为网络提供一个大脑，通过集中控制实现全局最优，避免传统网络的“局部视角，各自为政，混乱无序”。但要达到集中控制网络这个目的，OpenFlow 不是唯一的解决方案，采用源路由技术一样可以解决问题。

源路由技术由 Carl A. Sunshine 在 1977 年发表的论文"Source routing in computer networks"中提出，源路由技术是指由数据包的源头来决定数据包在网络中的传输路径，这一点和传统网络转发中各个网络节点自行选择最短路由有本质不同。但是源路由技术会对数据包进行处理，导致数据包的格式很复杂，开销也增加了，在早期网络带宽资源紧张的情况下，没有大规模应用。

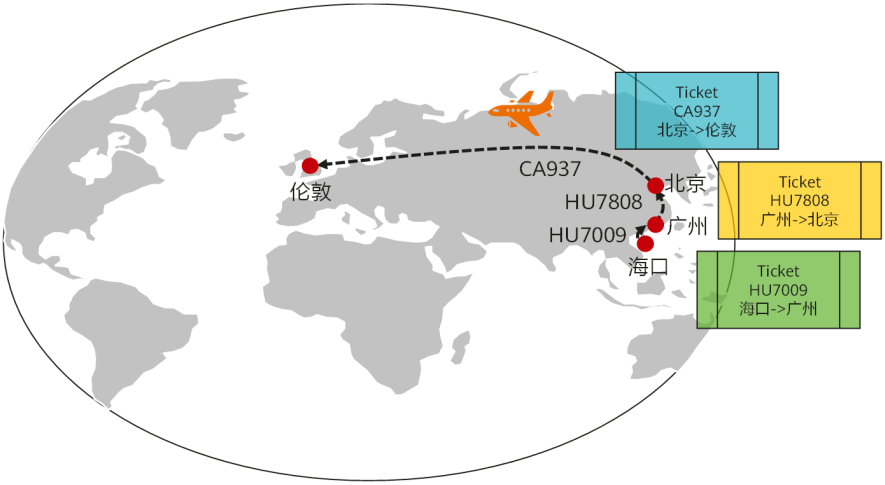
2013 年，出现了 Segment Routing（SR，段路由）协议，Segment Routing 借鉴了源路由思想。Segment Routing 的核心思想是将报文转发路径切割为不同的分段，并在路径头节点往报文中插入分段信息，中间节点只需要按照报文里携带的分段信息转发即可。这样的路径分段，称之为“Segment”，并通过 SID（Segment Identifier，段标识）来标识。

Segment Routing 的设计理念在现实生活中也很容易找到，下面举一个乘坐飞机出行的例子，来进一步解释 Segment Routing，具体如图 2-2 所示。假设从海口到伦敦的飞机需要在广州和北京进行两次中转，所以飞机票就会变为 3 段：海口->广州、广州->北京和北京->伦敦。

如果每到一个换乘机场再去买票，在乘客较多且选择趋同的情况下，可能会买不到票，影响整个行程。相反，如果我们在海口就买好从海口到广州到北京再到伦敦的 1 张联程机票，拿着这张机票，就可以从海口一站一站中转飞到伦敦。在海口，我们知道要乘坐 HU7009 飞往广州；当飞达广州时，根据飞机票，乘坐 HU7808 飞往北京；到了北京再根据机票乘坐 CA937 飞往伦敦。最终我们凭借在海口买到的 1 张联程机票，顺利换乘逐段飞到了伦敦。如果每个人都能按照这种方式提前进行规划，那

么就更容易避免局部的突发竞争，虽然对某个人来说，行程不一定是最优的，但是对于群体而言，却是全局最优。

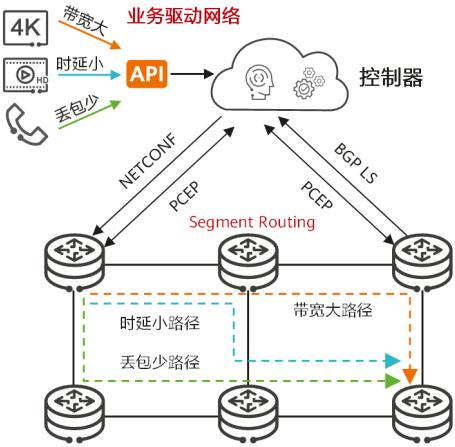
图2-2 从海口到伦敦



在上述过程中存在两个关键点：其一是路径分段（Segment）；其二是在源头位置对 Segment 进行组合，提前确定了整个出行路径（Routing）。Segment Routing 对网络进行分段，并在头节点进行路径组合，中间节点并不感知和维护路径状态，这正是源路由思想。

在网络边界相对明确，业务头尾节点固定的情况下，控制了头节点就可以控制报文的转发路径。仅在头节点进行路径调整，就可以满足不同业务的定制化需求，实现由业务驱动网络，把业务的意图更好地带入网络之中，这也是符合 SDN 思想的。具体如图 2-3 所示。

图2-3 业务驱动网络



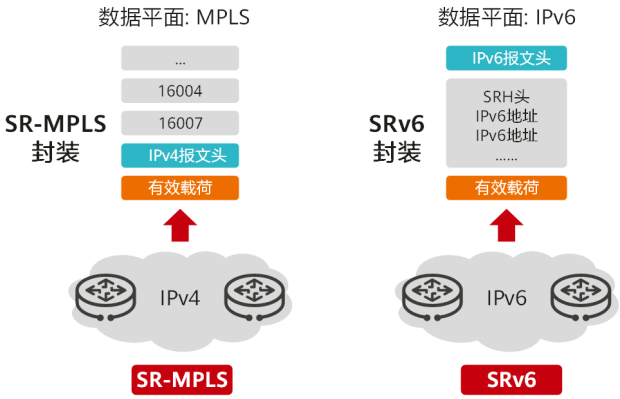
基于 Segment Routing 来优化网络，无须对现网硬件设施进行大量替换，所以对现网有更好的兼容性。运营商可以逐步升级网络，这种增量演进式的创新，更容易落地，业界称之为增量型网络。基于 Segment Routing 的增量型网络具有如下特点:

1. 通过对现有协议进行扩展，能更好地平滑演进。
2. 提供集中控制和分布式转发之间的平衡。
3. 采用源路由技术，提供网络和上层应用快速交互的能力，及时满足业务需求。

2.4 SRv6 是什么

如图 2-4 所示，目前 Segment Routing 支持 MPLS 和 IPv6 两种数据平面，基于 MPLS 数据平面的 Segment Routing 称为 SR-MPLS，其 SID 为 MPLS 标签（Label）；基于 IPv6 数据平面的 Segment Routing 称为 SRv6，其 SID 为 IPv6 地址。

图2-4 Segment Routing 分类



值得注意的是，早在 2013 年 Segment Routing 诞生之初，Segment Routing 的架构文档里面就提及了 SRv6。

“The Segment Routing architecture can be directly applied to the MPLS dataplane with no change on the forwarding plane. It requires minor extension to the existing link-state routing protocols.
Segment Routing can also be applied to IPv6 with a new type of routing extension header.”—RFC 8402

但是当时提出 SRv6 的时候，业界只是希望将节点和链路的 IPv6 地址放在路由扩展头里面引导流量，并没有提及 SRv6 SID 的可编程性，SRv6 相比于 SR-MPLS 是更遥远的目标，所以其关注度不如 SR-MPLS。

2017 年 3 月，SRv6 Network Programming（SRv6 网络编程）草案被提交给了 IETF（Internet Engineering Task Force，因特网工程任务组），原有的 SRv6 升级为 SRv6 Network Programming，从此 SRv6 进入了一个全新的发展阶段。SRv6 Network Programming 通过将长度为 128 比特的 SRv6 SID 划分为 Locator 和 Function 等，实际上 Locator 具有路由能力，而 Function 可以代表处理行为，也能够标识业务。这种巧妙的处理意味着 SRv6 SID 融合了路由和 MPLS（标签代表业务）的能力，使 SRv6 的网络编程能力大大增强，可以更好地满足新业务的需求。

目前，围绕 SRv6 的各项产业活动正在如火如荼地开展。

- 2019 年，MPLS+SDN+NFV 国际会议期间，全球首届 SRv6 产业圆桌论坛在法国巴黎成功举办。与会专家一致认为，SRv6 将是继 MPLS 之后的新一代 IP 承载网核心协议，承载网只有全面具备 SRv6 能力，才能满足 5G 和云时代的智能连接承载需求。
- 2019 年 12 月，中国推进 IPv6 规模部署专家委员会主办了 SRv6 产业沙龙，与会专家共商 SRv6 和 IPv6+的创新工作，探讨 SRv6 技术与产业推动，并联合发布了《SRv6 技术与产业白皮书》和《SRv6 互通测试报告》。
- 截至2020年底，欧洲高级网络测试中心（European Advanced Networking Test Center，EANTC）已经成功地进行了三次 SRv6 多厂商互通测试。测试范围包括基本 SRv6 VPN 业务场景、SRv6 可靠性、SRv6 Ping/Tracert 等，测试结果符合预期且充分证明了 SRv6 的商用部署能力。
- 截至2021年3月，在IETF标准工作领域：SR架构已经通过RFC 8402（Segment Routing Architecture）完成标准化；SRv6 最基本的标准，也通过 RFC 8754（IPv6 Segment Routing Header (SRH)）和 RFC 8986（SRv6 Network Programming）完成标准化，这两个 RFC 为 SRv6 的发展奠定了基石；SRv6 的 IGP/BGP/VPN 协议扩展也正在 IETF 逐步推进，其中，IS-IS 和 VPN 的文稿已经通过 WGLC（Working Group Last Call）阶段。协议的成熟必将有力地推动 SRv6 产业前进的步伐。

随着 2019 年全球 IPv4 公网地址全部耗尽，网络在向 IPv6 迁移，IPv6 的发展在加速，基于 SRv6 的应用越来越广泛，SRv6 的发展势不可挡。

2.5 SRv6 有哪些特点

SR-MPLS可以提供很好的路径编程能力，但是其受限于MPLS封装可扩展性不足等问题，无法很好地满足 SFC（Service Function Chaining，业务功能链）和 IOAM（In-situ Operations，Administration，and Maintenance，随流操作管理和维护）等一些需要携带元数据（Metadata）的业务的需求。另外，MPLS 往 IP 报文头之下插入标签的方式，也使得报文丧失了 IP 技术的普适性，需要网络设备逐跳支持 MPLS 标签转发，这在某种程度上提高了对网络设备的要求，从而将 MPLS 技术限定为运营商骨干网的专属技术，一般只在运营商骨干网或者新建城域网中采用，而在数据中心

中基本没有部署。以上原因使得 SR-MPLS 受限于 MPLS 本身，最终也只能被定义为 MPLS 技术的下一代演进而已。

而基于 IPv6 数据平面的 SRv6 不仅继承了 SR-MPLS 简化网络的所有优点，其 Native IPv6（原生 IPv6）属性使得 SRv6 拥有比 SR-MPLS 更好的兼容性、可扩展性。SRv6 SID 的扩展使得 SRv6 还拥有 SR-MPLS 没有的网络编程能力。SRv6 的技术特点如图 2-5 所示。

图2-5 SRv6 的技术特点

SRv6 和 SR-MPLS 的详细对比如表 2-1 所示。

表2-1 SRv6 和 SR-MPLS 的详细对比

维度	SRv6	SR-MPLS
简化网络协议	控制平面：IPv6 IGP/BGP。 数据平面：IPv6。	控制平面：IPv4/IPv6 IGP/BGP。 数据平面：MPLS。
可编程性	灵活，业务编排器或各种 APP 能够根据 SLA、业务诉求，指定网络、应用（业务链），提供灵活的可编程能力。	困难。
云网协同	容易，数据中心网络容易支持 IPv6。 借助 SRv6 技术，运营商网络可以深入到数据中心内部，甚至用户终端。	困难，数据中心网络，包括虚拟机支持 MPLS 困难。

维度	SRv6	SR-MPLS
终端协同	容易，终端设备已经支持 SRv6。Linux 4.10 版本开始支持 SRv6，4.14 版本支持 SRv6 Function 大部分功能。	困难，终端设备支持 MPLS 困难。
跨域部署	容易，利用 IPv6 可达性，SRv6 跨 AS 域部署容易，不需要跨域扩散主机路由，引入汇聚路由即可，大幅减少了路由数量，降低了路由策略复杂度。	复杂，跨 AS 域只能使用 SR-MPLS TE，需要依赖跨域控制器。本端 PE 需要远端 PE 的 Loopback 主机路由，所有远端 PE 的 Loopback 主机路由都要渗透。
大规模部署	容易，SID 采用 IPv6 地址空间，适合大网规划。	复杂，SID（MPLS 标签）空间有限，设备 SID 统一规划和维护复杂。
业务开通难度	SRv6 可以和普通 IPv6 设备共组网，只需要首尾节点支持 SRv6 即可，业务开通更加敏捷。	SR-MPLS 需要域内所有设备升级支持，业务开通相对复杂一些。
可靠性	TI-LFA。	TI-LFA。
转发效率	以封装 L3VPN 为例，最少需要 40 字节的 IPv6 报文头； SRv6 的 SRH 每增加一个 SID，增加 16 字节。	SR-MPLS 封装头小，以封装 L3VPN 为例，最少需要 8 字节两层 MPLS 标签；SR-MPLS 的标签栈每增加一个 SID，增加 4 字节；转发效率高。

第3章
SRv6 的技术价值

SRv6技术本身可以简化现有网络协议，降低网络管理复杂度，更好地应对未来5G和云网络发展的挑战。除此以外，SRv6更核心的优势是Native IPv6特质与网络编程能力。基于Native IPv6特质，SRv6能更好地促进云网融合、兼容存量网络、提升跨域体验；基于网络编程能力，SRv6可以更好地进行路径编程，满足业务的SLA，同时还能将网络和应用连接起来，构建智能云网。

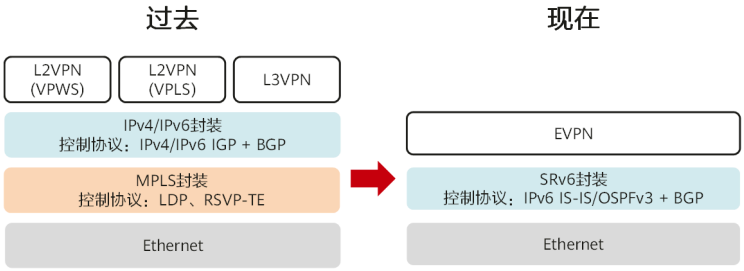
3.1 简化网络协议

面对未来 5G 和云网络发展的挑战，IP 承载网需要简化，降低管理复杂度，提升运维水平。借助 SRv6 和 EVPN（Ethernet Virtual Private Network，以太网虚拟专用网），可以使 IP 承载网的协议简化、归一。

在隧道/Underlay 层面，IPv6 报文的扩展替代了隧道功能，从而取消了原有的 LDP 和 RSVP-TE 等 MPLS 隧道技术。SRv6 只需要通过 IGP 和 BGP 扩展就可以完成 Underlay 功能和隧道功能，简化了信令协议。

在业务/Overlay 层面，通过 EVPN 整合了原来网络中 L2VPN VPWS（基于 LDP 或 MP-BGP）、L2VPN VPLS（基于 LDP 或 MP-BGP）以及 L3VPN（基于 MP-BGP）技术。业务层面可以通过 SRv6 SID 来标识各种各样的业务，也降低了技术复杂度。

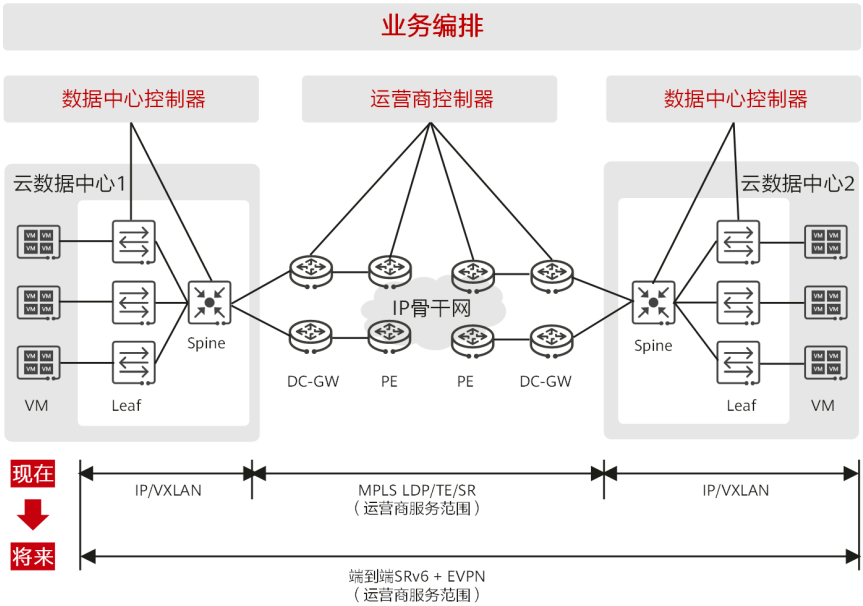
图3-1 SRv6 简化现有网络



3.2 促进云网融合

在图 3-2 所示的云数据中心互联场景中，IP 骨干网采用 MPLS/SR-MPLS 技术，而数据中心网络则通常使用 VXLAN 技术，这就需要引入网关设备，实现 VXLAN 和 MPLS 的相互映射，增加了业务部署的复杂性，却并没有带来相应的收益。

图3-2 云数据中心互联场景 SRv6 应用



SRv6 具备 Native IPv6 属性，SRv6 报文和普通 IPv6 报文具有相同的报文头，使得 SRv6 仅依赖 IPv6 可达性即可实现网络节点的互通，也使得它可以打破运营商网络和数据中心网络之间的界限，进入数据中心网络，甚至服务器终端。

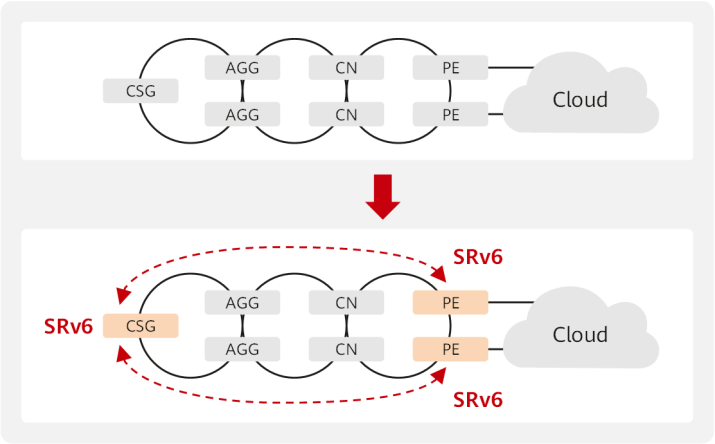
IPv6 的基本报文头确保了任意 IPv6 节点之间的互通，而 IPv6 的多个扩展头能够实现丰富的功能。SRv6 释放了 IPv6 扩展性的价值，基于 SRv6 最终可以实现简化的端到端可编程网络，真正实现网络业务转发大一统，实现“一张网络，万物互联”。

3.3 兼容存量网络

SRv6 与存量 IPv6 网络兼容，因而可以按需快速开通业务。部署业务时，不需要全网升级，能够保护现网已有投资；另外业务开通只需要在头尾节点进行部署，缩短部署时间，提升部署效率。

如图3-3所示，在初始阶段，将一些必要设备（例如头尾节点）升级到支持SRv6的版本，然后基于 SRv6 特性部署新业务，中间设备只要支持 IPv6，按照 IPv6 路由转发即可。后续可以按需升级中间节点，提供基于 SRv6 流量工程的增值服务。

图3-3 SRv6 按需升级

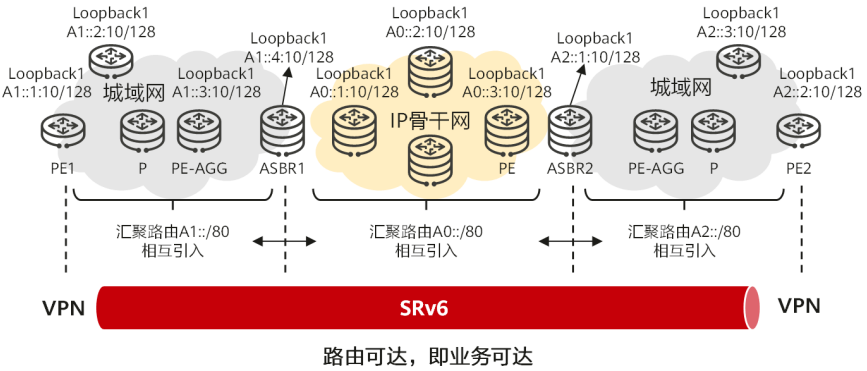


3.4 提升跨域体验

相对于传统的 MPLS 跨域技术来说，SRv6 跨域部署更加简单。SRv6 具有 Native IPv6 的特质，所以在跨域的场景中，只需要将一个域的 IPv6 路由通过 BGP4+引到另外一个域，就可以开展跨域业务部署，由此降低了业务部署的复杂性。

SRv6 跨域在可扩展性方面也具备独特的优势。SRv6 的 Native IPv6 特质，使得它能够基于聚合路由工作。这样即使在大型网络的跨域场景中，只需要在边界节点引入有限的聚合路由表项即可，如图 3-4 所示。这降低了对网络设备能力的要求，提升了网络的可扩展性。

图3-4 SRv6 大规模组网



路由可达，即业务可达

3.5 敏捷开通业务

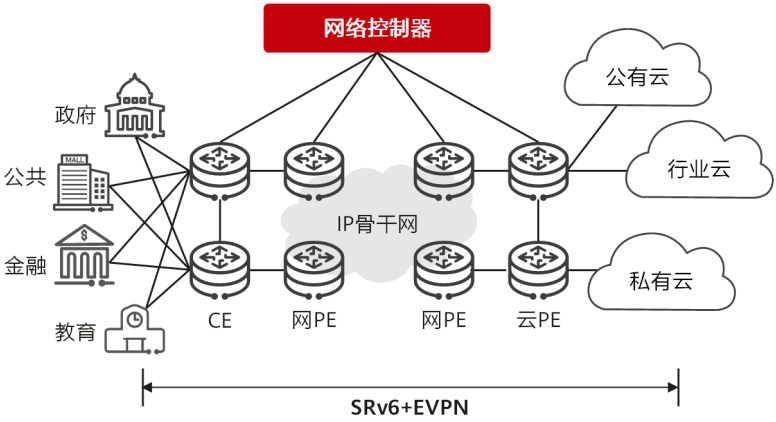
随着多云、混合云成为趋势，企业客户需要灵活访问分布在不同云上的应用，网络需要能够按需提供相应的上云连接。同时，为支撑应用在不同云间的灵活调度，需要承载网络与云进行敏捷打通，为不同云上的资源提供动态、按需的互联互通。

在传统的二层点对点专线模式下，企业需要基于不同云的部署位置租用多条上云专线，并通过手动切换或者企业内部自组网调度实现对不同云应用的访问，影响业务灵活性和多云访问体验，云网协同复杂度高。

同时，由于缺失一张统一互联互通的云骨干网，当有多个不同网络分别访问多个云时，如新建一个云数据中心，意味着所有网络和云的连接都需要新建打通，连接复杂，分段部署难度非常高，业务变现时间长。

智能云网方案通过云骨干网连接多云和多网，云网连接预部署，入网即入云；通过 SRv6+EVPN 技术实现业务一线灵活入多云，业务敏捷开通，具体如图 3-5 所示。

图3-5 基于 SRv6 敏捷开通业务



第4章
SRv6 的基础原理

本章主要介绍SRv6的基础原理，主要包括SRv6扩展报文头、SRv6 SID、SRv6报文转发流程、SRv6协议扩展和SRv6可靠性等内容。SRv6继承了源路由的优点，支持三重编程空间；SRv6具有Native IPv6特质，支持与现有IPv6设备共同组网，有利于现网存量演进；SRv6支持TI-LFA和中间节点保护等新技术，这些技术使用SRv6显式路径作为故障后的修复路径，提升了IP网络故障保护成功率。

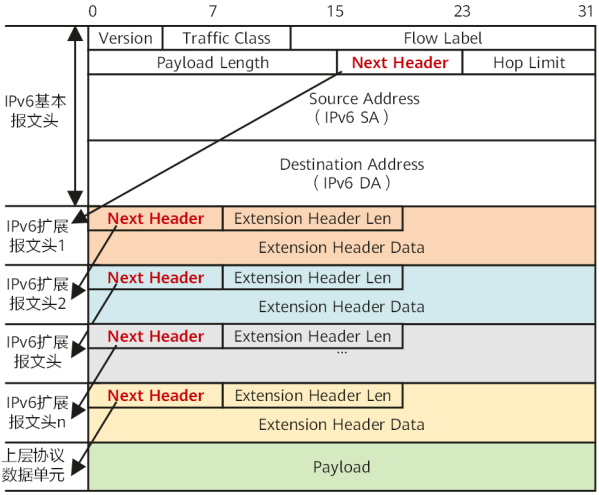
4.1 为什么说 SRv6 是 Native IPv6 技术

提到 SRv6，必然绕不开 IPv6。按照 RFC 8200 描述，IPv6 报文由 IPv6 基本报文头、IPv6 扩展报文头以及上层协议数据单元 3 部分组成，具体结构如图 4-1 所示。

IPv6 基本报文头有 8 个字段，固定大小为 40 字节，每一个 IPv6 数据包都必须包含 IPv6 基本报文头。IPv6 基本报文头提供报文转发的基本信息，会被转发路径上的所有设备解析。

上层协议数据单元一般由上层协议报文头和它的有效载荷构成，上层协议数据单元可以是一个 ICMPv6 报文、一个 TCP 报文或一个 UDP 报文。

图4-1 IPv6 报文格式



IPv6 报文格式的设计思想是让 IPv6 基本报文头尽量简单。大多数情况下，设备只需要处理基本报文头，就可以转发 IP 流量。因此，和 IPv4 相比，IPv6 去除了分片、校验和、选项等相关字段，仅增加了流标签（Flow Label）字段，IPv6 报文头的处理较 IPv4 得到了简化，提高了处理效率。另外，IPv6 为了更好地支持各种选项处理，提出了扩展报文头的概念，新增选项时不必修改现有报文结构，理论上可以无限扩展，在保持报文头简化的前提下，还具备了优异的灵活性。

IPv6 扩展报文头被置于 IPv6 基本报文头和上层协议数据单元之间。一个 IPv6 报文可以包含 0 个、1 个或多个扩展报文头，仅当需要其他节点做某些特殊处理时，才由源节点添加一个或多个扩展报文头。

当使用多个扩展报文头时，前面报文头的 Next Header 字段指明下一个扩展报文头的类型，这样就形成了链状的报文头列表。如图 4-1 所示，IPv6 基本报文头中的 Next Header 字段指明了第一个扩展报文头的类型，而第一个扩展报文头中的 Next

Header 字段指明了下一个扩展报文头的类型（如果不存在，则指明上层协议的类型）。

IPv6 扩展报文头如表 4-1 所示。路由设备根据基本报文头中 Next Header 值指定的协议号来决定是否要处理扩展报文头，并不是所有的扩展报文头都需要被查看和处理。

表4-1 IPv6 扩展报文头

IPv6 扩展报文头名称	协议号
逐跳选项扩展报文头 HBH（Hop-by-Hop Options Header）	0
目的选项扩展报文头 DOH（Destination Options Header）	60
路由扩展报文头 RH（Routing Header）	43
分片扩展报文头 FH（Fragment Header）	44
认证扩展报文头 AH（Authentication Header）	51
封装安全有效载荷扩展报文头 ESP（Encapsulating Security Payload Header）	50
上层协议报文 ULH（Upper-Layer Header）	ICMPv6：58；UDP：17；TCP：6

SRv6 就是通过路由扩展报文头 RH 扩展来实现的，SRv6 报文没有改变原有 IPv6 报文的封装结构，SRv6 报文仍旧是 IPv6 报文，普通的 IPv6 设备也可以识别，所以我们说 SRv6 是 Native IPv6 技术。SRv6 的 Native IPv6 特质使得 SRv6 设备能够和普通 IPv6 设备共同组网，对现有网络具有更好的兼容性。

从 IP/MPLS 回归 Native IPv6，IP 网络去除了 MPLS，协议简化，并且归一到 IPv6 本身，具有重大的意义。利用 SRv6，只要路由可达，就意味着业务可达，路由可以轻易跨越 AS 域，业务自然也可以轻易地跨越 AS 域，这对于简化网络部署，扩大网络的范围非常有利。

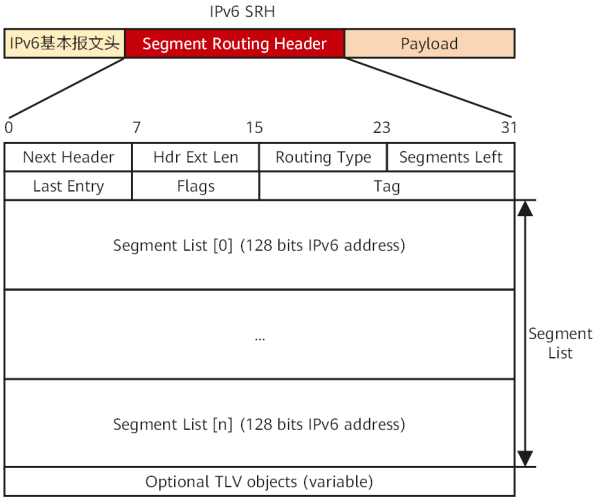
4.2 IPv6 如何扩展支持 SRv6

IPv6 SRH 扩展

为了基于 IPv6 转发平面实现 Segment Routing，IPv6 路由扩展报文头新增加一种类型，称作 SRH（Segment Routing Header，段路由扩展报文头），该扩展报文头指定一个 IPv6 的显式路径，存储的是 IPv6 的路径约束信息（Segment List）。

头节点在 IPv6 报文中增加一个 SRH 扩展头，中间节点就可以按照 SRH 扩展头里包含的路径信息进行转发。SRH 扩展头的格式如图 4-2 所示。

图4-2 SRH 扩展头格式



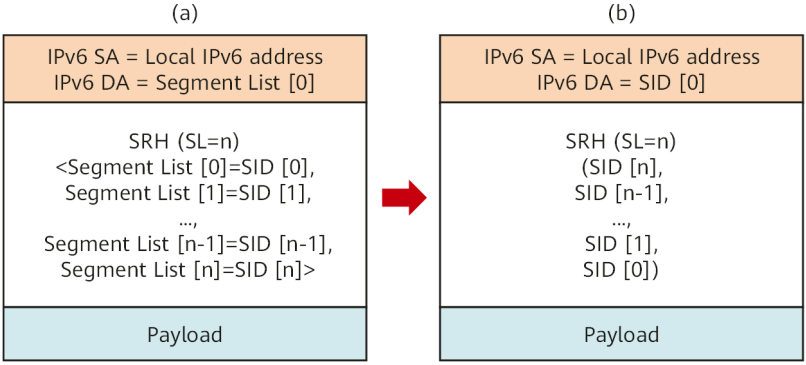
IPv6 SRH 的关键信息有几部分：

1. Routing Type 类型值为 4 时，表明报文头是 Segment Routing Header（SRH）。
2. Segments List（Segment List [0], Segment List [1], Segment List [2], ..., Segment List [n]）是网络路径信息。

3. Segments Left（SL）是一个指针，指示当前活跃的 Segment。

为了便于叙述转发原理，SRH 扩展头可以抽象成为图 4-3，其中图 4-3（a）里 SID 排序是正序，使用<>标识，图 4-3（b）里 SID 排序是逆序，使用（ ）表示，逆序更符合 SRv6 的实际报文封装情况。

图4-3 SRH 扩展头抽象格式



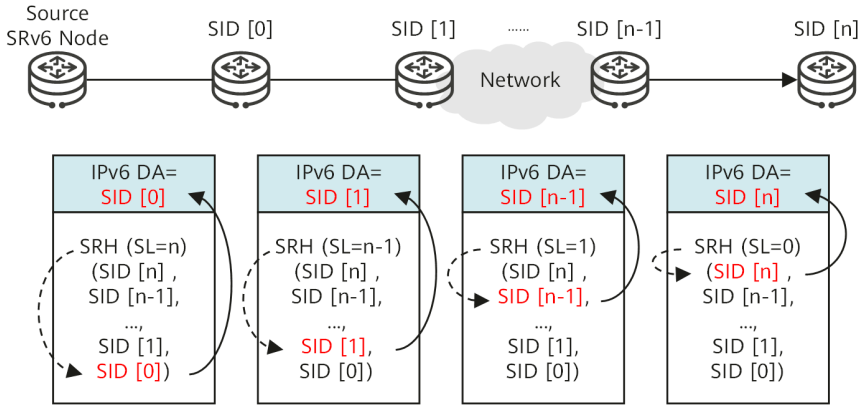
SRv6 SRH 的处理过程

在 SRv6 的 SRH 里，SL 和 Segments List 信息共同决定报文头部的 IPv6 目的地址。指针 SL 最小值是 0，最大值等于 SRH 里的 SID 个数减一。如图 4-4 所示，在 SRv6 中，每经过一个 SRv6 节点，SL 字段减 1，IPv6 DA（Destination Address，目的地址）信息变换一次，其取值是指针当前指向的 SID。SL 和 Segment List 字段共同决定 IPv6 DA 信息。

- 如果 SL 值是 n，则 IPv6 DA 取值就是 SID [0]的值。
- 如果 SL 值是 n-1，则 IPv6 DA 取值就是 SID [1]的值。
- ...
- 如果 SL 值是 1，则 IPv6 DA 取值就是 SID [n-1]的值。
- 如果 SL 值是 0，则 IPv6 DA 取值就是 SID [n]的值。

如果节点不支持 SRv6，则不执行上述动作，仅按照最长匹配查找 IPv6 路由表转发。

图4-4 SRH 的处理过程



从以上描述可见，节点对于 SRv6 SRH 是从下到上进行逆序操作，这一点与 SR-MPLS 有所不同。

SRv6 与 SR-MPLS 的另外一个不同是：SRv6 SRH 中的 Segment 在经过节点处理后也不会弹出。这里主要有 3 个原因：

1. 最早的 IPv6 的路由扩展头（RH）设计跟 MPLS 没有太多关联，当时的设计并没有弹出这个选项。
2. MPLS 每一个标签相对独立，并且位于顶部，可以直接弹出，SRv6 Segment 在 IPv6 包头后面的 SRH 扩展头中，并且与其他扩展头信息存在关联（如安全加密和校验等），不能简单地弹出。
3. 因为没有弹出，SRv6 报文头保留了路径信息，可以做路径回溯。另外有一些创新考虑对 SRH 中保留的 Segment 进行重用，做一些新的功能扩展。

4.3 SRv6 SID 有何特殊之处

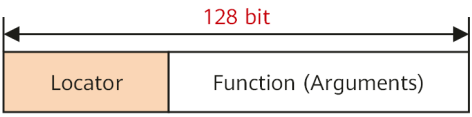
Segment ID（SID）在 SR-MPLS 里是标签形式，在 SRv6 里换成了 IPv6 地址形式。SRv6 也是通过对 SID 栈的操作来完成转发，SRv6 同样是一种源路由技术。那么 SRv6 的 SID 具有哪些特殊之处呢？要回答这个问题，就需要从 SRv6 SID 结构来说起。

SRv6 SID 结构

SRv6 SID 是 IPv6 地址形式，但也不是普通意义上的 IPv6 地址。SRv6 的 SID 具有 128 比特，足够表征任何事物，这样长的一个地址，如果仅仅用于路由转发，显然是很浪费的，所以 SRv6 的设计者对于 SID 进行了更加巧妙的处理。

如图 4-5 所示，SRv6 SID 由 Locator 和 Function 两部分组成，格式是 Locator:Function，其中 Locator 占据 IPv6 地址的高比特位，Function 部分占据 IPv6 地址的剩余部分。

图4-5 SRv6 SID 结构



- Locator 具有定位功能，所以一般要在 SRv6 域内唯一，但是在一些特殊场景，比如 Anycast 保护场景，多个设备可能配置相同的 Locator。节点配置 Locator 之后，系统会生成一条 Locator 网段路由，并且通过 IGP 在 SRv6 域内扩散。网络里其他节点通过 Locator 网段路由就可以定位到本节点，同时本节点发布的所有 SRv6 SID 也都可以通过该条 Locator 网段路由到达。
- Function 代表设备的指令（Instruction），这些指令都由设备预先设定，Function 部分用于指示 SRv6 SID 的生成节点进行相应的功能操作。Function 通过 Operation Code（Opcode）来显性的表征。

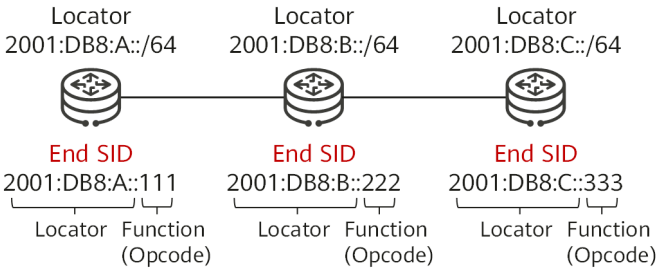
- Function 部分还可以分出一个可选的参数段（Arguments），此时 SRv6 SID 的格式变为 Locator:Function:Arguments，Arguments 占据 IPv6 地址的低比特位，通过 Arguments 字段可以定义一些报文的流和服务等信息。当前一个重要应用是 EVPN VPLS 的 CE 多归场景，转发 BUM 流量时，利用 Arguments 实现水平分割。

Function 和 Arguments 都是可以定义的，这也反映出 SRv6 SID 的结构更有利于对网络进行编程。

下面以 End SID 和 End.X SID 为例来说明 SRv6 SID 的结构。

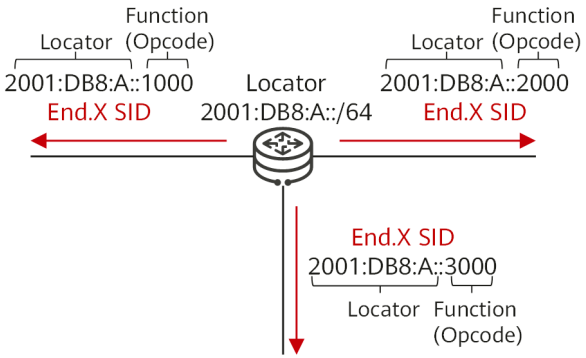
End SID 表示 Endpoint SID，用于标识网络中的某个目的节点（Node）。如图 4-6 所示，在各个节点上配置 Locator，然后为节点配置 Function 的 Opcode，Locator 和 Function 的 Opcode 组合就能得到一个 SID，这个 SID 可以代表本节点，我们称为 End SID。End SID 可以通过 IGP 协议扩散到其他网元，全局可见。

图4-6 End SID



End.X SID 表示三层交叉连接的 Endpoint SID，用于标识网络中的某条链路。如图 4-7 所示，在节点上配置 Locator，然后为各个方向的邻接配置 Function 的 Opcode，Locator 和 Function 的 Opcode 组合就能得到一个 SID，这个 SID 可以代表一个邻接，我们称为 End.X SID。End.X SID 可以通过 IGP 协议扩散到其他网元，全局可见。

图4-7 End.X SID



End SID 和 End.X SID 分别代表节点和邻接，都是路径 SID，使用二者组合编排 SID 栈已经足够表征任何一条网络路径。SID 栈代表了路径的约束，携带在 IPv6 SRH 中，SRv6 就是通过这种方式实现了流量工程（Traffic Engineering，TE）。

此外，也可以为 VPN/EVPN/EVPL（Ethernet Virtual Private Line，以太网虚拟专线）实例等分配 SID，这种 SID 就代表业务。由于 IPv6 地址空间足够大，所以 SRv6 SID 能够支持足够多的业务。

SRv6 常用 SID

当前 SRv6 SID 主要包括路径 SID 和业务 SID 两种类型。例如 End SID 和 End.X SID 分别代表节点和链路，而 End.DT4 SID 和 End.DT6 SID 分别代表 IPv4 VPN 和 IPv6 VPN 等。

实际由于业务的发展，业务 SID 在不断增多，具体如表 4-2 所示。

表4-2 SRv6 常用 SID

SID	含义	发布协议	类型
End SID	表示 Endpoint SID，用于标识网络中的某个目的节点（Node）。对应的转发动作（Function）是：更新 IPv6 DA，查找 IPv6 FIB 进行报文转发。	IGP	路径 SID
End.X SID	表示三层交叉连接的 Endpoint SID，用于标识网络中的某条链路。对应的转发动作是：更新 IPv6 DA，从 End.X SID 绑定的出接口转发报文。	IGP	路径 SID
End.DT4 SID	表示 PE 类型的 Endpoint SID，用于标识网络中的某个 IPv4 VPN 实例。对应的转发动作是：解封装报文，并且查找 IPv4 VPN 实例路由表转发。End.DT4 SID 在 L3VPNv4 场景使用，等价于 IPv4 VPN 的标签。	BGP	业务 SID
End.DT6 SID	表示 PE 类型的 Endpoint SID，用于标识网络中的某个 IPv6 VPN 实例。对应的转发动作是：解封装报文，并且查找 IPv6 VPN 实例路由表转发。End.DT6 SID 在 L3VPNv6 场景使用，等价于 IPv6 VPN 的标签。	BGP	业务 SID
End.DX4 SID	表示 PE 类型的三层交叉连接的 Endpoint SID，用于标识网络中的某个 IPv4 CE。对应的转发动作是：解封装报文，并且将解封后的 IPv4 报文在该 SID 绑定的三层接口上转发。End.DX4 SID 在 L3VPNv4 场景使用，等价于连接到 CE 的邻接标签。	BGP	业务 SID
End.DX6 SID	表示 PE 类型的三层交叉连接的 Endpoint SID，用于标识网络中的某个 IPv6 CE。对应的转发动作是：解封装报文，并且将解封后的 IPv6 报文在该 SID 绑定的三层接口上转发。End.DX6 SID 在 L3VPNv6 场景使用，等价于连接到 CE 的邻接标签。	BGP	业务 SID
End.DX2 SID	表示二层交叉连接的 Endpoint SID，用于标识一个端点。如果网络中存在 Bypass 隧道，则会自动生成 End.DX2L SID。对应的转发动作是：解封装报文，去掉 IPv6 报文头及其扩展头，然后将剩余报文转发到 SID 对应的出接口。End.DX2 SID 可以用于 EVPN VPWS 场景。	BGP	业务 SID

SID	含义	发布协议	类型
End.DT2U	表示二层交叉连接且进行单播 MAC 表查找功能的 Endpoint SID，用于标识一个端点。如果网络中存在 Bypass 隧道，则会自动生成 End.DT2UL SID。End.DT2UL SID 可以用于本地双归 PE 发送 Bypass 单播流量。对应的转发动作是：去掉 IPv6 报文头及其扩展头，然后使用剩余报文的目的 MAC 地址查找 MAC 表，根据 MAC 表项将报文转发到对应的出接口。End.DT2U SID 可以用于 EVPN VPLS 单播场景。	BGP	业务 SID
End.DT2M SID	表示二层交叉连接且进行广播泛洪的 Endpoint SID，用于标识一个端点。对应的转发动作是：End.DT2M SID 对应的转发动作是去掉 IPv6 报文头及其扩展头，然后将剩余报文在 BD 内广播泛洪。End.DT2M SID 可以用于 EVPN VPLS BUM 流量转发场景。	BGP	业务 SID
End.OP SID	End.OP SID（OAM Endpoint with Punt）是一个 OAM 类型的 SID。对应的转发动作是：对 OAM 报文实现上送操作。End.OP SID 主要用于 Ping/Tracert 场景。	IGP	业务 SID

本地 SID 表

使能 SRv6 的节点维护一个本地 SID（Local SID）表，该表包含所有在本节点生成的 SRv6 SID 信息，根据该表可以生成一个 SRv6 转发表（Forwarding Information Base，FIB）。本地 SID 表有以下用途：

- 定义本地生成的 SID，例如 End.X SID 等。
- 指定绑定到这些 SID 的指令。
- 存储和这些指令相关的转发信息，例如出接口和下一跳等。

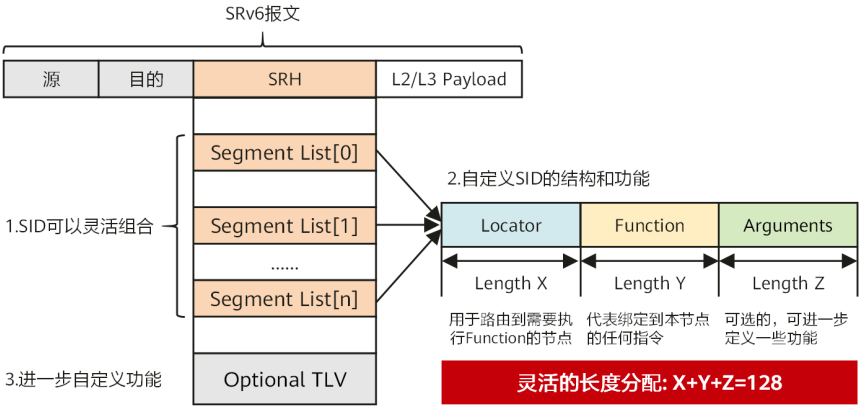
4.4 SRv6 的三重编程空间

由于 SRv6 赋予了 SID 更多的内涵，SRv6 SID 不仅可以代表路径，还可以代表不同类型的业务，也可以代表用户自己定义的任何功能，所以我们说 SRv6 具有更强的网络可编程能力。

如图 4-8 所示，SRv6 支持三重编程空间：

1. SRv6 SID 可以自由组合进行路径编程，由业务提出需求，控制器响应业务需求，定义转发路径，这一点完美地契合了 SDN 思想。比如某公司承接省外另一家公司的业务，在一个月内需要和对方大量交换数据，因此立即需要一定的带宽保障，那么该公司就需要向运营商购买一个月的服务，如果按照传统的业务开通方式，多个部门协调运作，业务开通时间很长，常以月计，时间上难以满足该公司需求。但是借助 SRv6 路径编程，运营商控制器可以快速响应该公司需求，计算符合用户 SLA 的业务路径，快速开通业务，在一个月的合约到期后运营商也可以快速拆除连接，释放网络资源。
2. Function 和 Arguments 字段可以自定义功能。Function 可以由设备商定义，比如数据包到达 SRv6 尾节点后，利用 Function 指示节点将数据包转发给某个 VPN 实例；Function 在未来也可以由用户来定义，比如数据包到达 SRv6 节点后，指示节点将数据包转发给某个 APP。由于 Linux 系统支持 SRv6，所以未来基于 Linux 系统进行创新，定义不同的 Function，可以支持很多新型的业务。
3. SRH 里还有可选 TLV，可以用于进一步自定义功能，比如有一种思路就是用来携带 iFIT 的指令头。

图4-8 SRv6 的三重编程空间



4.5 SRv6 如何通过协议扩展实现

为了支持 SRv6，网络节点需要发布两类 SRv6 信息：

1. Locator 信息：Locator 信息用于帮助网络中的其他节点定位到发布 SID 的节点，然后由该节点执行 SID 的指令。域内 Locator 信息一般需要通过 IGP 扩展来泛洪。
2. SID 信息：SID 信息用于完整描述 SID 的功能，比如 SID 绑定的 Function 信息。SID 信息包括路径类 SID 和业务类 SID，都是全局可见，本地有效的。路径类 SID 主要描述节点或者链路，需要通过 IGP 扩展来进行泛洪；而业务类 SID 和路由信息强相关，一般通过 BGP 扩展来发布，携带在 BGP 的 Update 报文里。

综合以上，实现 SRv6 的基础功能至少需要 IGP 扩展和 BGP 扩展。

IGP 扩展

链路状态路由协议基于 Dijkstra 最短路径优先（Shortest Path First，SPF）算法计算到达指定地址的最短路径。链路状态路由协议的工作原理是相邻节点通过发送

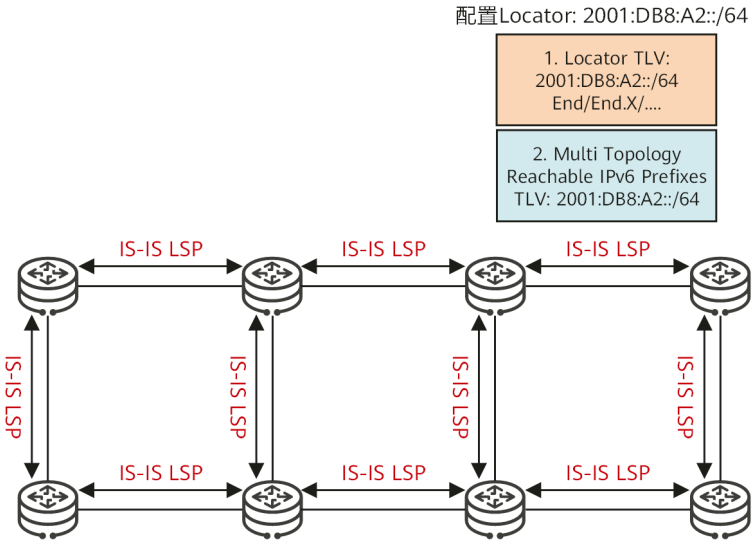
Hello报文建立邻居关系，并将本地链路状态信息（LSP）在全网扩散，形成全网一致的链路状态数据库（Link-State Database，LSDB），每个节点基于LSDB运行SPF算法计算出路由。

如图 4-9 所示，IS-IS 通过两个 TLV 来发布 Locator 的路由信息，这两个 TLV 具有不同的作用：

1. SRv6 Locator TLV：该TLV包含Locator的前缀和掩码，用于发布Locator前缀。通过该 TLV，网络中其他 SRv6 节点能学习到 Locator 路由；Locator TLV 除了携带用于指导路由的信息外，还会携带不需要关联 IS-IS 邻居节点的 SRv6 SID，例如 End SID。
2. Multi Topology Reachable IPv6 Prefixes TLV：该 TLV 携带的 IPv6 Prefix 与 SRv6 Locator TLV 里携带的 Locator 信息拥有相同的前缀和掩码。Multi Topology Reachable IPv6 Prefixes TLV 是 IS-IS 协议已有的 TLV，普通 IPv6 节点（不支持 SRv6 的节点）也能处理该 TLV。因此普通 IPv6 节点也能够通过此 TLV 生成 Locator 路由，指导报文转发到发布该 Locator 的节点，进而支持与 SRv6 节点共同组网。

   如果设备同时收到 Multi Topology Reachable IPv6 Prefixes TLV 和 SRv6 Locator TLV，则 Multi Topology Reachable IPv6 Prefixes TLV 优先使用。

图4-9 IS-IS SRv6 TLV 发布



IS-IS 针对 SRv6 的扩展具体如表 4-3 所示。

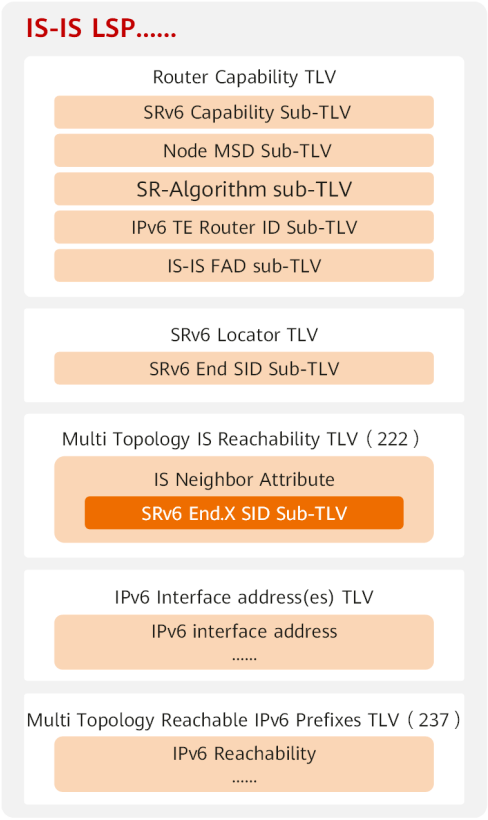
表4-3 IS-IS 针对SRv6 的 TLV 扩展

名称	作用	携带位置
SRv6 Locator TLV	用于通告 SRv6 的 Locator 以及该 Locator 相关的 End SID。	IS-IS LSP
SRv6 Capabilities sub-TLV	用于通告 SRv6 能力。	IS-IS Router Capability TLV-242
SRv6 End SID sub-TLV	用于通告 SRv6 的 SID。	SRv6 Locator TLV

名称	作用	携带位置
SRv6 End.X SID sub-TLV	用于在 P2P 网络中通告 SRv6 的 SID。	IS-IS Extended IS reachability TLV-22 IS-IS IS Neighbor Attribute TLV-23 IS-IS inter-AS reachability information TLV-141 IS-IS Multitopology IS TLV-222 IS-IS Multitopology IS Neighbor Attribute TLV-223
SRv6 LAN End.X SID sub-TLV	用于在 LAN 网络中通告 SRv6 的 SID。	IS-IS Extended IS reachability TLV-22 IS-IS IS Neighbor Attribute TLV-23 IS-IS inter-AS reachability information TLV-141 IS-IS Multitopology IS TLV-222 IS-IS Multitopology IS Neighbor Attribute TLV-223
Node MSD sub-TLV	用于通告设备能够接受的最大 SID 栈深度 MSD（Maximum SID Depth）。	IS-IS Router Capability TLV-242
IS-IS FAD sub-TLV	发布自己的算法定义。	IS-IS Router Capability TLV-242
SR-Algorithm sub-TLV	用于对外通告自己使用的算法。	IS-IS Router Capability TLV-242

一个常见的携带 SRv6 信息的 IS-IS LSP 结构如图 4-10 所示。

图4-10 携带SRv6信息的IS-IS LSP

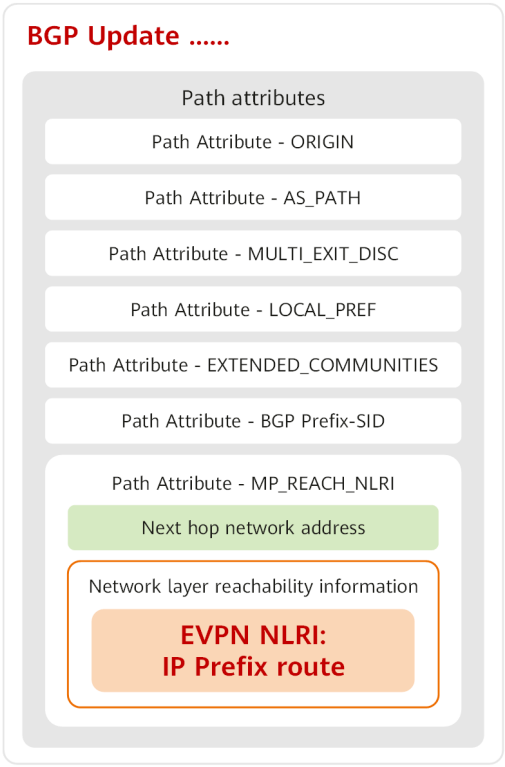


BGP 扩展

BGP 扩展包括 MP-BGP 和 BGP EVPN。L2VPN 和 L3VPN 的业务 SID 都需要通过 BGP Update 来发布。

一个常见的携带 SRv6 信息的 BGP EVPN Update 结构如图 4-11 所示。

图4-11 携带 SRv6 信息的 BGP EVPN Update



4.6 SRv6 如何确保高可靠性

高价值业务要求IP承载网提供高可用性，例如高品质企业专线，如政府，金融，医疗行业对可用性的要求往往是比较高的 99.99%。而 5G 业务，尤其是对于 uRLLC（Ultra-Reliable Low-Latency Communication，超高可靠超低时延通信）业务而言，其可用性要求是 99.999%。部分业务如远程控制，高压供电等，其可靠性关系着社会与生命安全，可用性则是极高的 99.9999%。

50ms 故障恢复已经成为 IP 承载网的基础要求，例如传统的语音和 IPTV 业务都要求故障恢复时间控制在毫秒级，如果达到秒级，则对业务的影响会比较严重。而 5G 的 eMBB（Enhanced Mobile Broadband，增强型移动宽带）和 uRLLC 业务，则对端到端时延的要求更加苛刻，比如智慧家庭、虚拟现实/增强现实等 eMBB 业务，要求时延在 10ms 以内，而自动驾驶、远程医疗、智慧能源、智能制造等 uRLLC 业务要求时延在 1ms 以内。

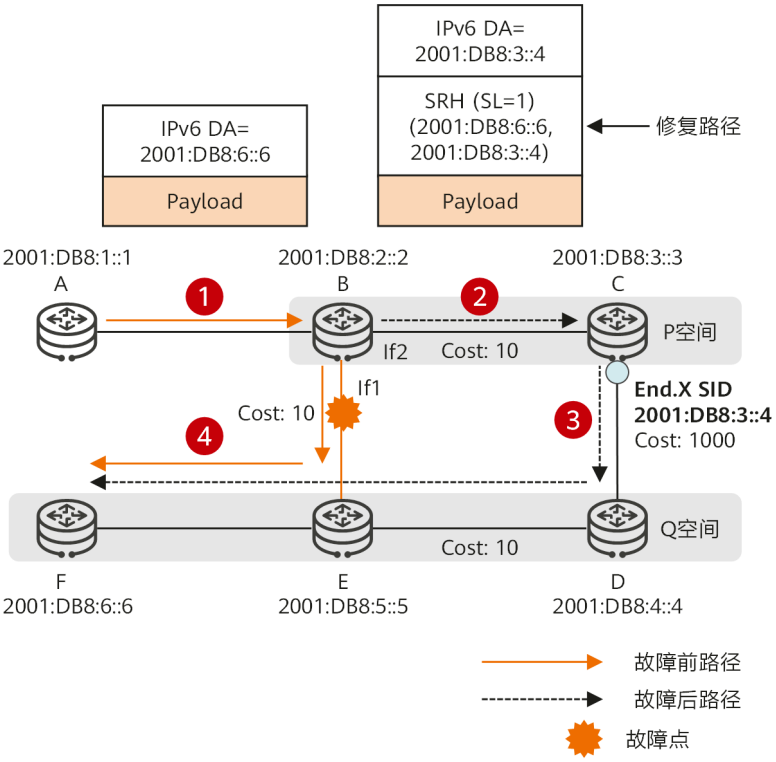
SRv6 提供针对 IP 网络端到端故障点的本地保护技术，从而实现任意拓扑的 50ms 本地保护。在网络发生故障时，SRv6 先由邻近故障点的设备切换到次优路径，然后通过逐级路由收敛，收敛到最优路径。SRv6 独有的本地保护技术主要有 TI-LFA（Topology-Independent Loop-free Alternate，拓扑无关的无环路备份路径）和中间节点保护等，利用这些技术可以极大地提高保护成功率，增强 IP 承载网的可靠性。

TI-LFA

下面通过图 4-12 介绍 SRv6 TI-LFA 的工作原理。在图 4-12 中，节点 A 到节点 F 的最短路径为 A->B->E->F，节点 B 需要计算到节点 F 的备份路径，步骤如下：

1. 排除主下一跳（链路 B-E）计算收敛后的最短路径：A->B->C->D->E->F。
2. 计算扩展 P 空间：以保护链路源端的所有邻居为根节点分别建立 SPF 树，所有从根节点不经过保护链路可达的节点集合称为扩展 P 空间。扩展 P 空间中的节点都是 P 节点，包括{节点 B，节点 C}。
3. 计算 Q 空间：以保护链路末端为根节点建立反向 SPF 树，所有从根节点不经过保护链路可达的节点集合称为 Q 空间。Q 空间中的节点都为 Q 节点，包括{节点 D，节点 E，节点 F}。
4. 计算修复路径（Repair Segment List）：我们可以把任意路径表示为：源节点->P 节点->Q 节点->目的节点。其中源节点到 P 节点是无环路径，Q 节点到目的节点也是无环路径。如果存在 PQ 节点（PQ 节点是指既在扩展 P 空间又在 Q 空间的节点），则从源可以到该节点，从该节点可以到目的节点，且均不经过故障路径，此时直接将流量转发到 PQ 节点即可，整条路径均为无环路径，此时 Repair Segment List 可以是 PQ 节点的 End SID。如果不存在 PQ 节点，则需要指定 P 节点到 Q 节点的无环转发路径，此时 P 节点到 Q 节点的 Repair Segment List 可能是 End SID 和 End.X SID 的组合。本例中最远的 P 节点 C 到最近的 Q 节点 D 之间的 Repair Segment List 可以为 End.X SID 2001:DB8:3::4。

图4-12 SRv6 TI-LFA 保护原理



如表 4-4 所示，PLR 节点 B 根据 TI-LFA 计算结果预先安装备份转发表，用于主下一跳故障的时候激活备份下一跳，确保到目的节点 F 的可达性。

表4-4 节点 B 的 TI-LFA 备份转发表

路由前缀	出接口	Segment List	角色
2001:DB8:6::6	If1	-	主用
	If2	2001:DB8:3::4	备份

当链路 B-E 故障时，数据转发过程描述如下：

1. 节点 B 收到目的地址为 2001:DB8:6::6 的报文，根据 2001:DB8:6::6 查找转发表，主出接口为 If1。
2. 节点 B 查询到 If1 接口状态为 Down，使用备份表项转发，备份出接口为 If2，并使用“H.Insert”的方式封装 Segment List 2001:DB8:3::4，新增 1 个 SRH 扩展报文头，将用于修复故障的 Segment List 和目的地址 2001:DB8:6::6 封装在 SRH 扩展报文头，SL 初始化为 1。
3. 节点 C 收到报文以后，识别目的地址 2001:DB8:3::4 是 End.X SID，所以需要执行 End.X SID 对应的指令：将 SL 减 1，外层 IPv6 地址更新为 2001:DB8:6::6，并按 2001:DB8:3::4 绑定的出接口和下一跳沿着链路 C-D 转发到节点 D。由于 SL = 0，所以节点 C 可以按照 PSP 操作去掉 SRH 扩展报文头。
4. 节点 D 收到报文以后，根据报文的目的地址 2001:DB8:6::6 查找 IPv6 路由表沿着最短路径转发到目的地址 F。

根据上面的描述可以看出，TI-LFA 可以满足 100%拓扑的故障保护，而且还具有如下优势：

1. TI-LFA 备份路径和网络故障收敛后的最短路径在大多数情况下都是一致的，这减少了转发路径的切换次数。TI-LFA 算法是基于收敛后最短路径计算的，只有在少数链路故障和节点故障收敛后路径不一致的情况下才会出现备份路径和收敛后路径不一致的情况。
2. TI-LFA 备份路径依赖 IGP SRv6 实现，这样减少了为部署可靠性技术而额外引入的协议。
3. TI-LFA 利用已有的 End.X SID 或 End SID 建立备份路径，不需要维护额外的转发状态。

SRv6 中间节点的故障保护

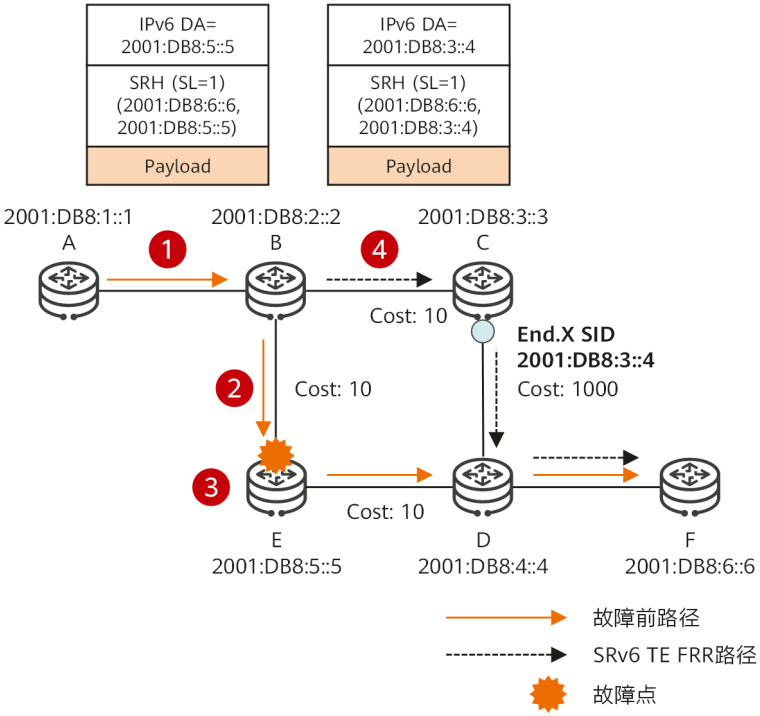
SRv6 中间节点（Midpoint）在处理 SRv6 报文时，需要执行的转发行为是 SL 减 1，并将下层 SID 复制到 IPv6 报文头的目的地址字段。但是当某一个中间节点故障时，它就无法完成对应 SID 的处理动作，造成转发失败。

为了解决上述问题，需要由中间节点的上游节点代替它完成这个转发处理，这个上游节点我们称之为代理转发（Proxy Forwarding）节点。代理转发节点感知到报文的下一跳接口故障，并且下一跳是报文目的地址，且 SL > 0 时，代理转发节点代替故障的中间节点执行 End 行为，将 SL 减 1，并将下层要处理的 SID 更新到外层 IPv6 报文头，然后按照下层 SID 的指令进行转发，从而绕过故障节点，实现 SRv6 中间节点故障的保护。

以图 4-13 为例，SRv6 中间节点故障的保护过程介绍如下：

1. 节点 A 向目的节点 F 转发报文，并在 SRv6 SRH 中指定经过中间节点 E。
2. 节点 E 故障的时候，节点 B 感知到报文下一跳接口故障，而下一跳正好是报文当前的目的地址 2001:DB8:5::5，且 SL > 0，所以节点 B 执行代理转发行为，将 SL 减 1，并将下层 SID 2001:DB8:6::6 复制到外层 IPv6 报文头的目的地址字段。此时由于 SL = 0，节点 B 可以去掉 SRH 扩展报文头，然后根据目的地址 2001:DB8:6::6 查表转发。
3. 由于目的地址 2001:DB8:6::6 的主下一跳依然是节点 E，但是节点 B 不是该目的地址的倒数第二跳，且 SL = 0，所以节点 B 不再符合代理转发条件，而是按照正常 TI-LFA 转发流程切换到备份路径转发，备份路径的 Repair Segment List 为 <2001:DB8:3::4>，所以节点 B 使用“H.Insert”的方式封装 Segment List 2001:DB8:3::4，新增 1 个 SRH 扩展报文头，经过备份路径转发到节点 F。
4. 在节点 A 感知到节点 E 故障，且 IGP 完成收敛以后，节点 A 删除到节点 E 的路由转发表项，所以节点 A 根据 2001:DB8:5::5 查表转发的时候，无法命中路由，此时节点 A 就要作为代理转发节点执行代理转发行为，SL 减 1，并将下层 SID 2001:DB8:6::6 更新到外层 IPv6 报文头，然后根据目的地址 2001:DB8:6::6 查表转发到节点 B。节点 B 如果完成收敛，则按照收敛后的最短路径将报文转发到节点 F；节点 B 如果未完成收敛，则按照 TI-LFA 流程经过备份路径转发到节点 F。通过上述方式，就绕过了故障节点 E。

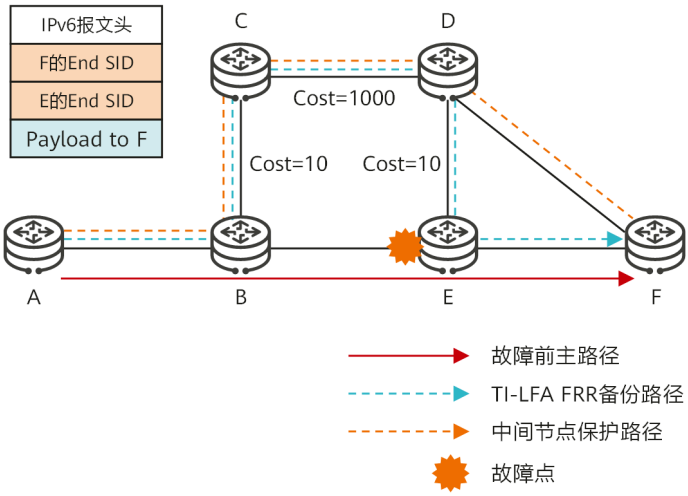
图4-13 SRv6 Midpoint 节点故障保护



读者可能不太容易理解普通 TI-LFA 和 SRv6 中间节点保护的区别，本质上二者的区别在于下一跳节点是中转节点还是目的地址中的 SRv6 中间节点。

如图 4-14 所示，节点 A 发送报文携带 Segment List <E，F>。由于 TI-LFA 是根据报文目的地址计算一条备份路径，所以 TI-LFA 计算的备份路径也经过节点 E。如果节点 E 故障，普通 TI-LFA 无法实现保护。而 SRv6 中间节点保护是根据下层 SID 计算的备份转发路径，所以它能绕过故障的中间节点，从而实现了 SRv6 TE Policy 的中间节点故障保护功能。

图4-14 TI-LFA 和 Midpoint 保护的区别



第5章
SRv6 的工作模式

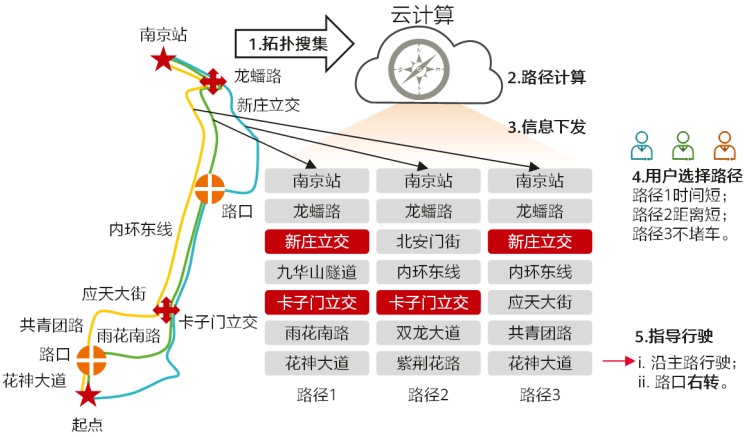
本章主要介绍SRv6的两种工作模式：SRv6 TE Policy和SRv6 BE。这两种模式都可以承载常见的传统业务，比如：BGP L3VPN、EVPN L3VPN、EVPN VPLS/VPWS、IPv4/IPv6公网等。SRv6 TE Policy可以实现流量工程，配合控制器可以更好地响应业务的差异化需求，做到业务驱动网络。SRv6 BE是一种简化的SRv6实现，正常情况下不含有SRH扩展头，只能提供尽力而为的转发。在SRv6发展早期，基于IPv6路由可达性，利用SRv6 BE快速开通业务，具有无与伦比的优势；在后续演进中，可以按需升级网络的中间节点，部署SRv6 TE Policy，满足高价值业务的需求。

5.1 SRv6 TE Policy

什么是 SRv6 TE Policy

SRv6 TE Policy 利用 Segment Routing 的源路由机制，通过在头节点封装一个有序的指令列表来指导报文穿越网络。SRv6 TE Policy 的思想在现实生活中也容易找到，图 5-1 就是一个导航地图的工作过程。

图5-1 导航地图工作过程

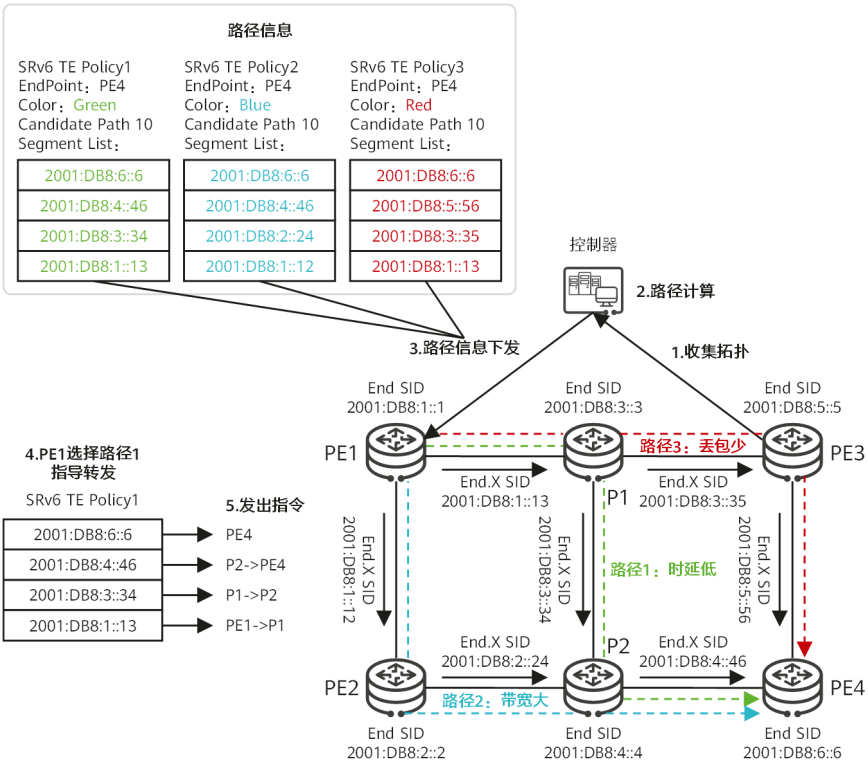


在图 5-1 中，整个工作过程可以概括为 5 个步骤：

1. 拓扑收集：主要是收集交叉路口信息、车道信息、流速信息和信号灯信息等。
2. 路径计算：基于多种约束来计算路径，符合多个维度的 SLA，比如收费少、时间少、距离短、高速优先等等。
3. 信息下发：计算的路径信息发送到用户终端设备。
4. 路径选择：由用户根据目的地址以及自己的喜好来选择路径。每一个路径都是多个道路和关键交叉路口的组合。
5. 指导行驶：按照一个个分段路径信息指导行驶。每个分段信息可以引导用户行驶。在接近路口时提前向用户发出指令（例如：直行、左转、右转、掉头等等）。

自然规律都是相通的。如果我们把一个地图换成网络，就可以发现 SRv6 TE Policy 的工作原理与导航地图非常相似。SRv6 TE Policy 的工作流程具体如图 5-2 所示。

图5-2 SRv6 TE Policy 的工作流程



SRv6 TE Policy 的工作流程主要也可以概括为 5 个步骤：

1. 转发器将网络拓扑信息通过 BGP LS 上报给网络控制器。拓扑信息包括节点（类比交叉路口）、链路信息（类比道路），以及链路的开销（类比流速）、带宽（类比车道）和时延（类比信号灯）等 TE 属性。
2. 控制器基于收集到的拓扑信息，按照业务需求计算路径，符合业务的 SLA。
3. 控制器通过 BGP SR-Policy 扩展将路径信息下发给网络的头节点，头节点生成 SRv6 TE Policy。生成的 SRv6 TE Policy 包括头端地址、目的地址和 Color 等关键信息。

4. 网络的头节点为业务选择合适的 SRv6 TE Policy 指导转发。
5. 数据转发时，转发器需要执行自己发布的 SID 的指令。

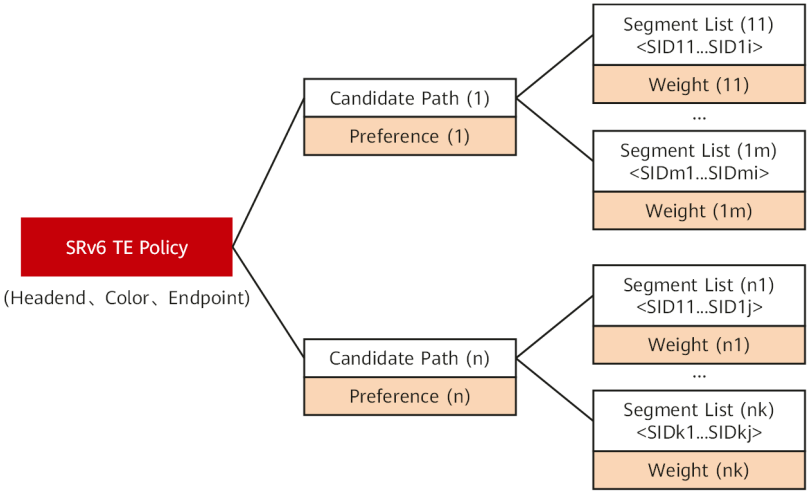
从图 5-2 可以看出，通过在 SRH 中封装一系列的 SRv6 SID，可以显式指导报文按照规划的路径转发，实现对转发路径端到端的细粒度控制，满足业务的低时延、大带宽、高可靠等 SLA 需求。如果业务的目的地址与 SRv6 TE Policy 的 EndPoint 匹配，业务的偏好（通过路由的 Color 扩展团体属性标识）与 SRv6 TE Policy 的一致，那么业务的流量就可以导入指定的 SRv6 TE Policy 进行转发。

SRv6 利用 IPv6 地址 128 比特的可编程能力，丰富了 SRv6 指令表达的网络功能范畴，除了用于标示转发路径的指令外，还能标示 VAS，例如防火墙、应用加速，或者用户网关等。除此之外，SRv6 还有着非常强大的扩展能力，如果要支持一个新的网络功能，只需要定义一个新的指令即可，不需要改变协议的机制或部署，这大大缩短了网络创新业务的交付周期。所以说，SRv6 TE Policy 可以实现业务的端到端需求，是实现 SRv6 网络编程的主要机制。

SRv6 TE Policy 的结构与优势

为了提升可靠性，提升带宽利用率，SRv6 TE Policy 的结构做了精心的设计，具体如图 5-3 所示。

图5-3 SRv6 TE Policy 结构



SRv6 TE Policy 包括以下三个要素：

1. 头端（Headend）：SRv6 TE Policy 生成的节点。
2. 颜色（Color）：SRv6 TE Policy 携带的扩展团体属性，携带相同 Color 属性的 BGP 路由可以使用该 SRv6 TE Policy。
3. 尾端（Endpoint）：SRv6 TE Policy 的目的地址。

SRv6 TE Policy 的结构具有如下优势：

1. 灵活引流：Color 和 Endpoint 信息通过配置添加到 SRv6 TE Policy，业务网络头端通过路由携带的 Color 属性和下一跳信息来匹配对应的 SRv6 TE Policy 实现业务流量转发。Color 属性定义了应用级的网络 SLA 策略，可基于特定业务 SLA 规划网络路径，实现业务价值细分，构建新的商业模式。
2. 可靠性高：一个 SRv6 TE Policy 可以包含多个候选路径（Candidate Path）。候选路径携带优先级属性（Preference）。优先级最高的有效候选路径作为 SRv6 TE Policy 的主路径，优先级次高的有效候选路径作为 SRv6 TE Policy 的备路径。
3. 负载分担：一个候选路径可以包含多个 Segment List，每个 Segment List 携带 Weight 属性。每个 Segment List 都是一个显式 SID 栈，Segment List 可以指

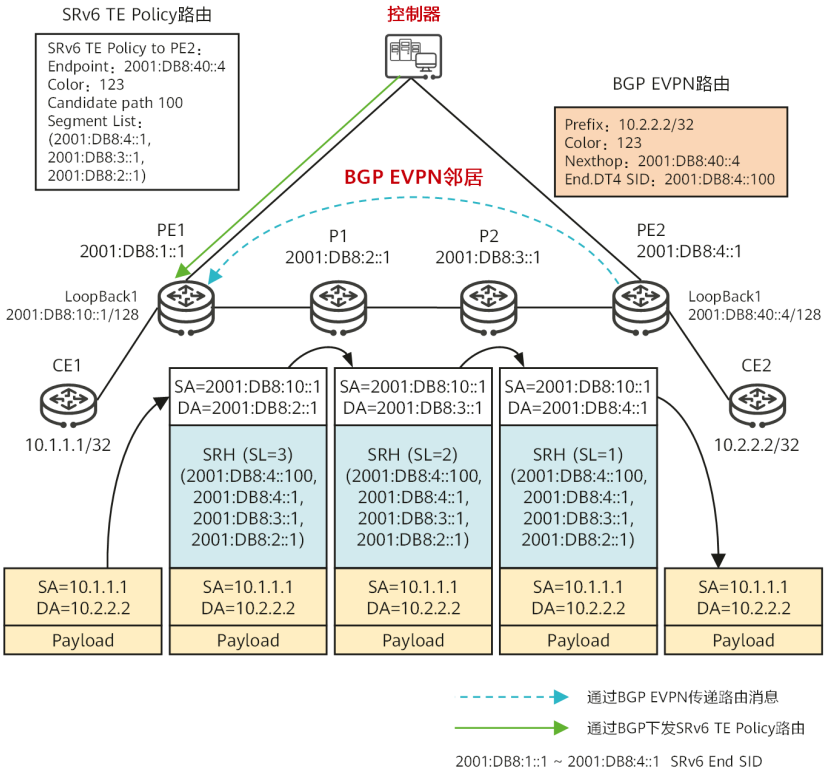
示网络设备转发报文。多个 Segment List 之间可以形成等价或非等价负载分担（ECMP/UCMP）。

SRv6 TE Policy 的业务实现

SRv6 TE Policy 可以承载常见的传统业务，它们的转发过程都比较类似。下面以 EVPN L3VPNv4 over SRv6 TE Policy 为例介绍 SRv6 TE Policy 的业务实现。

EVPN L3VPNv4 over SRv6 TE Policy 的数据转发过程具体如图 5-4 所示。

图5-4 SRv6 TE Policy 数据转发



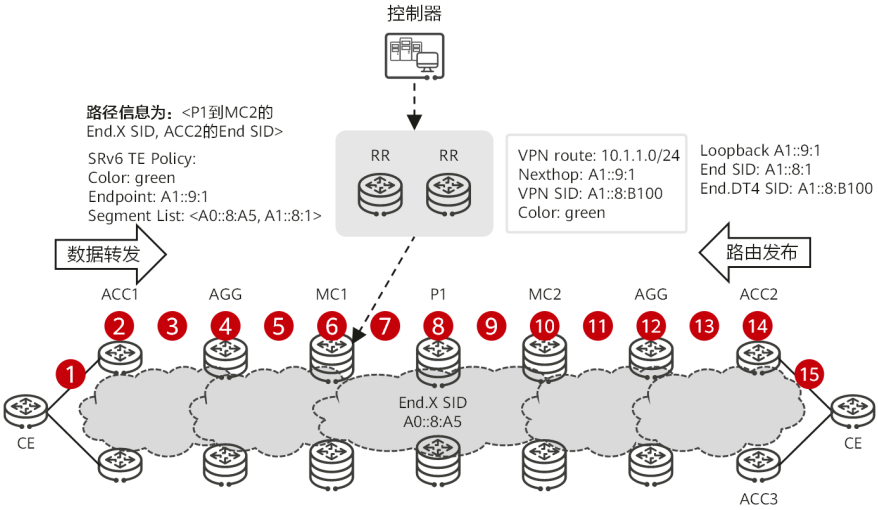
总体过程简述如下：

1. 控制器向头节点 PE1 下发 SRv6 TE Policy，Color 为 123，Endpoint 为 PE2 的地址 2001:DB8:40::4，只有一个 Candidate Path，且 Candidate Path 也只包含一个 Segment List <2001:DB8:2::1，2001:DB8:3::1，2001:DB8:4::1>。
2. 尾节点 PE2 向 PE1 发布 BGP EVPN 路由 10.2.2.2/32，BGP 路由的下一跳是 PE2 的地址 2001:DB8:40::4/128，Color 为 123。
3. PE1 在接收到 BGP 路由以后，利用路由的 Color 和下一跳迭代到 SRv6 TE Policy。
4. PE1 接收到 CE1 发送的普通单播报文后，查找 VPN 实例路由表，该路由迭代到了一个 SRv6 TE Policy。PE1 为报文插入 SRH 信息，封装 SRv6 TE Policy 的 Segment List，Segment List 里最后一个 SID 是 VPN 路由对应的 End.DT4 SID，同时封装 IPv6 报文头信息，并查表转发。
5. 中间 P1 和 P2 节点根据 SRH 信息逐跳转发。
6. 报文到达 PE2 之后，PE2 使用报文的 IPv6 目的地址 2001:DB8:4::1 查找本地 SID 表，命中了 End SID，所以 PE2 将报文的 SL 减 1，IPv6 DA 更新为 VPN SID 2001:DB8:4::100。
7. PE2 使用 VPN SID 2001:DB8:4::100 查找本地 SID 表，命中了 End.DT4 SID，PE2 执行 End.DT4 SID 的指令，解封装报文，去掉 SRH 信息和 IPv6 报文头，使用内层报文的目的地址查找 End.DT4 SID 2001:DB8:4::100 对应的 VPN 实例路由表，然后将报文转发给 CE2。

SRv6 TE Policy 场景可靠性方案

SRv6 TE Policy 场景的可靠性方案如图 5-5 所示，控制器计算的 SRv6 TE Policy 的 Segment List 可以通过 TI-LFA 进行路径保护；同时为了确保极端场景下的可靠性，建议将 SRv6 BE 作为 SRv6 TE Policy 的逃生路径，也就是说 SRv6 TE Policy 产生故障，业务切换到 SRv6 BE 路径上尽力转发。关于 SRv6 BE，可以参考 5.2 的描述。

图5-5 SRv6 TE Policy 可靠性设计



在图 5-5 中，不同位置故障都有相应的保护技术。简述如下：

- 对于故障点 1 和 2，可以通过链路检测技术进行感知，通过 ECMP/IP FRR 进行保护。
- 对于故障点 3 & 4 & 5 & 6 & 7 & 10 & 11 & 12，其 SID 不在 SRv6 TE Policy 的 Segment List 中，可以通过 TI-LFA FRR 进行保护，使用链路检测技术或者 BFD for IGP 进行故障感知，触发 FRR 切换。
- 对于故障点 8 和 9，由于故障点 9 的 SID 在 SRv6 TE Policy 的 Segment List 中，可以通过中间节点保护技术进行保护，通过链路检测技术或者 BFD for IGP 进行感知，触发 FRR 切换。
- 对于故障点 13 和 14，可以通过 IP FRR/VPN FRR 进行保护，通过链路检测技术或者 BFD for IGP 进行感知，触发 FRR 切换。
- 对于故障点 15，可以通过链路检测技术进行感知，对于 L3VPN，通过 ECMP 或 VPN 下的 IP FRR（也称为混合 FRR，当 ACC2 去往 CE 的路由下一跳不可达时，流量可以通过隧道转发到达其他 ACC3，然后查私网路由转发到达目的地）进行保护。对于 EVPN，通过 ECMP 或 Local-remote-FRR（当 ACC2 与 CE 之间的链

路故障后，流量发到 ACC2 后，可以绕行到其他 ACC3，再发送到 CE，减少丢包）进行保护。

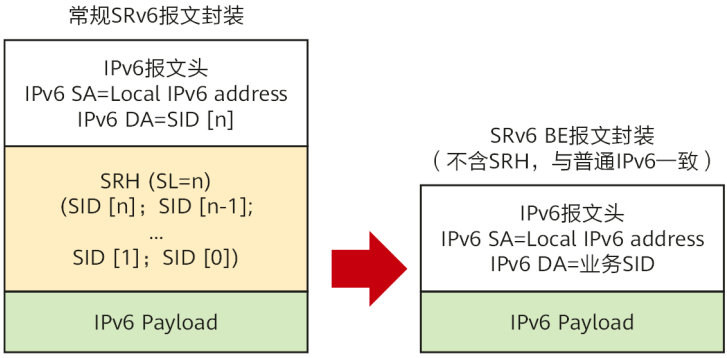
5.2 SRv6 BE

什么是 SRv6 BE

传统 MPLS 有 LDP 和 RSVP-TE 两种控制协议，其中 LDP 方式不支持流量工程能力，LDP 利用 IGP 算路结果，建立 LDP LSP 指导转发。在 SRv6 里，也有类似的方式，只不过 SRv6 仅使用一个业务 SID 来指引报文在 IP 网络里进行尽力而为（Best Effort，BE）的转发，这种方式就是 SRv6 BE。

如图 5-6 所示，SRv6 BE 的报文封装没有代表路径约束的 SRH，其格式与普通 IPv6 报文格式一致，转发行为也与普通 IPv6 报文转发一致。这就意味着普通的 IPv6 节点也可以处理 SRv6 BE 报文，这也是 SRv6 兼容普通 IPv6 设备的秘密。

图5-6 SRv6 BE 的结构

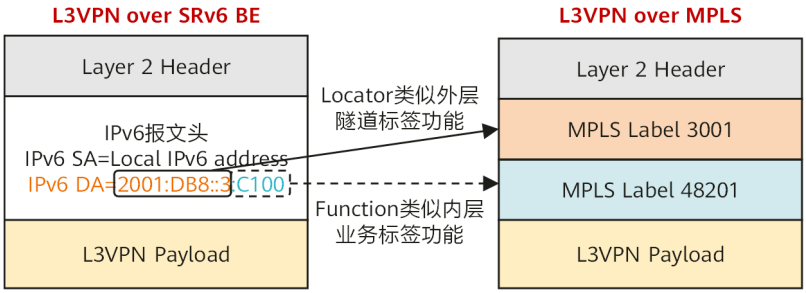


SRv6 BE 的报文封装与普通 IPv6 报文封装的不同点在于：普通 IPv6 报文的目的地址是一个主机或者网段，但是 SRv6 BE 报文的目的地址是一个业务 SID。业务 SID

可以指引报文按照最短路径转发到生成该 SID 的父节点，并由该节点执行业务 SID 的指令。

L3VPN over MPLS 时一般使用两层 MPLS 标签，外层 MPLS 标签用来引导报文到指定的 PE，内层 MPLS 标签属于业务标签，一般标识 PE 上的某个 VPN 实例。在 L3VPN over SRv6 场景，一个 SRv6 的业务 SID 即可做到两层 MPLS 标签的功能。如图 5-7 所示，业务 SID 2001:DB8:3::C100 的 Locator 部分是 2001:DB8:3::/64，Function Opcode 是::C100。Locator 2001:DB8:3::/64 具有路由功能，可以将报文引导到对应的 PE；Function Opcode ::C100 是在 PE 上配置的本地功能，可以标识 PE 上的业务，比如某个 VPN 实例，这也是 SRv6 SID 融合了路由和 MPLS（标签代表业务）能力的具体体现。

图5-7 业务 SID 的两个作用

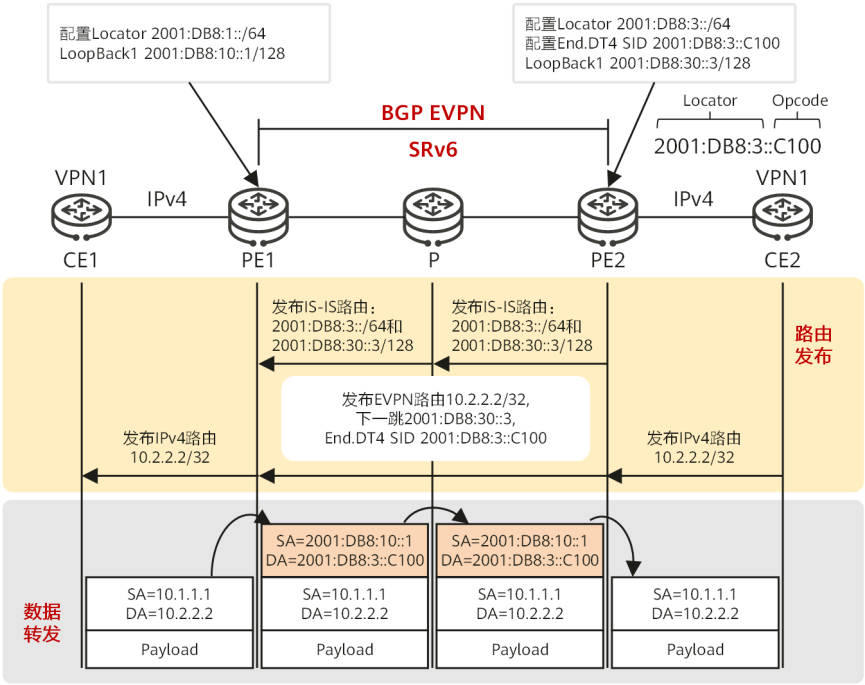


SRv6 BE 的业务实现

SRv6 BE 可以承载常见的传统业务，它们的转发过程都比较类似。下面以 EVPN L3VPNv4 over SRv6 BE 为例介绍 SRv6 BE 的业务实现。

EVPN L3VPNv4 over SRv6 BE 的路由发布和数据转发过程如图 5-8 所示。

图5-8 EVPN L3VPNv4 over SRv6 BE 路由发布和数据转发过程



在路由发布阶段：

1. PE2 上配置 Locator，然后 PE2 通过 IGP 协议将 SRv6 SID 对应的 Locator 网段路由 2001:DB8:3::/64 发布给 PE1。PE1 安装路由到自己的 IPv6 路由表。
2. PE2 在 Locator 范围内配置 VPN 实例的 End.DT4 SID 2001:DB8:3::C100，生成本地 SID 表。
3. PE2 收到 CE2 发布的私网 IPv4 路由后，PE2 将私网 IPv4 路由转换成 IP Prefix Route 形式的 EVPN 路由，通过 BGP EVPN 邻居关系发布给 PE1。此路由携带 SRv6 VPN SID 属性，也就是 VPN 实例的 End.DT4 SID 2001:DB8:3::C100。
4. PE1 接收到 EVPN 路由后，将其交叉到对应的 VPN 实例 IPv4 路由表，然后转换成普通 IPv4 路由，对 CE1 发布。

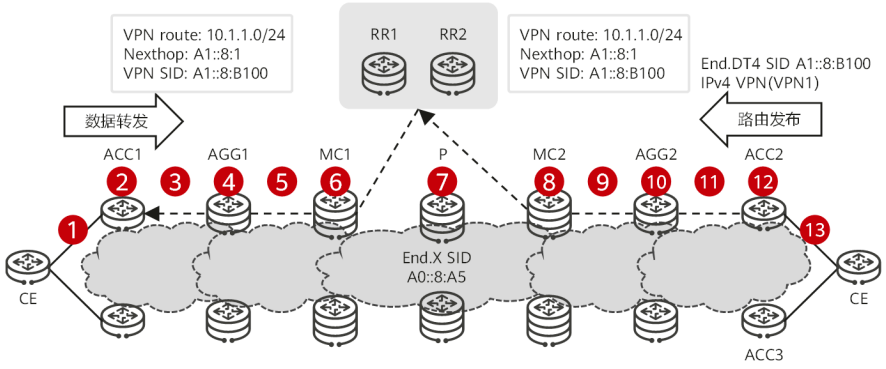
在数据转发阶段：

1. CE1 向 PE1 发送一个普通 IPv4 报文。
2. PE1 从绑定了 VPN 实例的接口上收到私网报文以后，查找对应 VPN 实例的 IPv4 路由转发表，匹配目的 IPv4 前缀，查找到关联的 SRv6 VPN SID 以及下一跳信息。然后直接使用 SRv6 VPN SID 2001:DB8:3::C100 作为目的地址封装成 IPv6 报文。
3. PE1 然后按照最长匹配原则，匹配到路由 2001:DB8:3::/64，按最短路径转发到 P 设备。
4. P 设备按照最长匹配原则，匹配到路由 2001:DB8:3::/64，按最短路径转发到 PE2。
5. PE2 使用 2001:DB8:3::C100 查找本地 SID 表，匹配到 End.DT4 SID 对应的转发动作，将 IPv6 报文头去除，然后根据 End.DT4 SID 匹配 VPN 实例，查找 VPN 实例 IPv4 路由表进行转发。

SRv6 BE 场景可靠性方案

SRv6 BE 路径的中间节点在 IGP 域内可以通过 TI-LFA FRR 实现拓扑无关的保护。在进行网络设计时，不需要对 TI-LFA 进行特殊的设计，只需要在 IGP 下使能即可。端到端的可靠性保护场景和技术如图 5-9 所示。

图5-9 SRv6 BE 的可靠性设计



在图 5-9 中，不同位置故障都有相应的保护技术。简述如下：

- 对于故障点 1 和 2，可以通过链路检测技术感知，通过 ECMP/IP FRR 进行保护。
- 对于故障点 3-10，可以通过 TI-LFA FRR 进行保护，使用链路检测技术或者 BFD for IGP 进行故障感知，触发 FRR 切换。
- 对于故障点 11 和 12，可以通过 IP FRR/VPN FRR 进行保护，通过链路检测技术或者 BFD for IGP 进行感知，触发 FRR 切换。
- 对于故障点 13，可以通过链路检测技术进行感知，对于 L3VPN，通过 ECMP 或者 VPN 下的 IP FRR 进行保护。对于 EVPN，通过 ECMP 或者 Local-remote-FRR（当 ACC2 与 CE 之间的链路故障后，流量发到 ACC2 后，可以绕行到其他 ACC3，再发送到 CE，减少丢包）进行保护。

SRv6 BE 与 SRv6 TE Policy 对比

结合前面的描述我们知道，SRv6 BE 与 SRv6 TE Policy 的主要差异在于 SRv6 BE 报文封装不含有 SRH 信息，所以自然也不具备流量工程能力。SRv6 BE 仅使用一个业务 SID 来指引报文转发到生成该 SID 的父节点，并由该节点执行业务 SID 的指令。

SRv6 BE 只需要在网络的头尾节点部署，中间节点仅支持 IPv6 转发即可，这种方式对于部署普通 VPN 具有独特的优势。比如视频业务在省中心和市中心之间传递，需要跨越数据中心网络、城域网络、国家 IP 骨干网络，在传统方式部署 MPLS VPN 时，不可避免地需要跟省干、国干的主管单位进行协调，各方配合执行部分操作才能成功，开通时间比较慢，错失很多商业机会；但是采用 SRv6 BE 承载 VPN，只需要在省中心和市中心部署两台支持 SRv6 VPN 的 PE 设备，很快就开通了业务，这种方式显然更容易抓住商业机会。

我们汇总了 SRv6 BE 与 SRv6 TE Policy 的详细对比，如表 5-1 所示。

表5-1 SRv6 BE 与 SRv6 TE Policy 的对比

维度	SRv6 BE	SRv6 TE Policy
配置	很简单。	复杂。
路径计算	基于 IGP 开销。	基于 TE 约束。
SRH	正常转发不携带 SRH，仅在 TI-LFA FRR 保护场景，按照修复路径转发时才携带 SRH。	携带 SRH。
路径编程	否，没有 SRH，无法携带路径信息。	是。
需要控制器	否，IGP 算路即可。	是。SRv6 TE Policy 可以静态配置，但是配置复杂，一般推荐使用控制器动态下发 SRv6 TE Policy，这样可以更快速地响应业务的需求，做到业务驱动网络。
保护技术	TI-LFA FRR（50ms）。	TI-LFA FRR（50ms）。
场景	适合服务 SLA 要求低、流量不需要指定路径的场景。	适合服务对 SLA 要求严格的场景。例如网络拥塞时，流量需要切换到其他路径，或者需要重定向到指定目的地的流量，如反 DOS 清洗等。

第6章
SRv6 支持 5G 与云业务

本章主要介绍SRv6如何支持5G与云业务。5G改变了连接的属性，云改变了连接的范围，它们为SRv6技术的发展带来了最好的机会。IP承载网的本质就是连接。5G业务的发展对于网络连接提出了更多的要求，例如更强的SLA保证、确定性时延等，这些通过SRv6扩展都可以很好地满足。云业务的发展，使得业务处理所在位置更加灵活多变，而一些云业务（如电信云）进一步打破了物理网络设备和虚拟网络设备的边界，使得业务与承载融合在一起，这些都改变了网络连接的范围。SRv6的业务与承载统一编程能力，以及Native IPv6属性，都使得它能够快速地建立连接，满足连接范围灵活调整的需求。

6.1 SRv6 支持网络切片

网络切片介绍

网络发展的历史表明，IP 骨干网、城域网、移动承载网等存在网络边界，给业务的端到端部署带来很多困难，管理和维护的复杂度也比较高。随着社会的进步，网络的复杂性越来越阻碍了业务的发展，建立一张超宽、简单、智能、可靠、安全的统一 IP 承载网已是业界共识，“IP 承载一切（Everything over IP）”正在逐步变为现实。

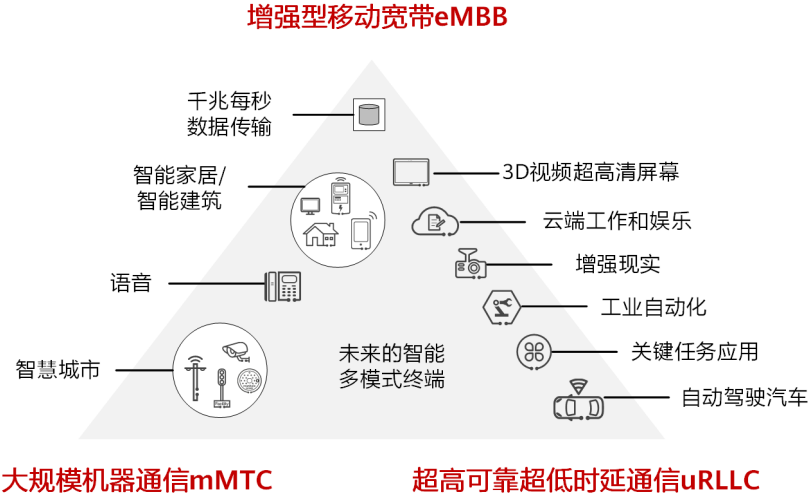
那么统一的一张IP承载网如何满足众多业务的多样化、差异化、复杂化需求呢？这是一个新的挑战。运营商如何避免被管道化，获得新的商业价值呢？这是另外一个挑战。

以 5G（5th Generation，第五代移动通信技术）业务来说，5G 中各种垂直行业的业务特征差异巨大。对于智能家居、环境监测、智能农业和智能抄表等业务，需要网络支持海量设备连接和大量小报文频发；视频回传和移动医疗等业务对传输速率提出了很高的要求；车联网、智能电网和工业控制等业务则要求毫秒级的时延和接近100%的可靠性。因此，为了渗透到更多的垂直行业业务中，5G 应具备更强的灵活性和可扩展性，以适应海量的设备连接和多样化的用户需求，在满足移动宽带的基础上，以垂直行业需求为导向，构建灵活、动态的网络，满足不同行业需求。

如图 6-1 所示，5G 时代的主要业务需求划分为 3 类：

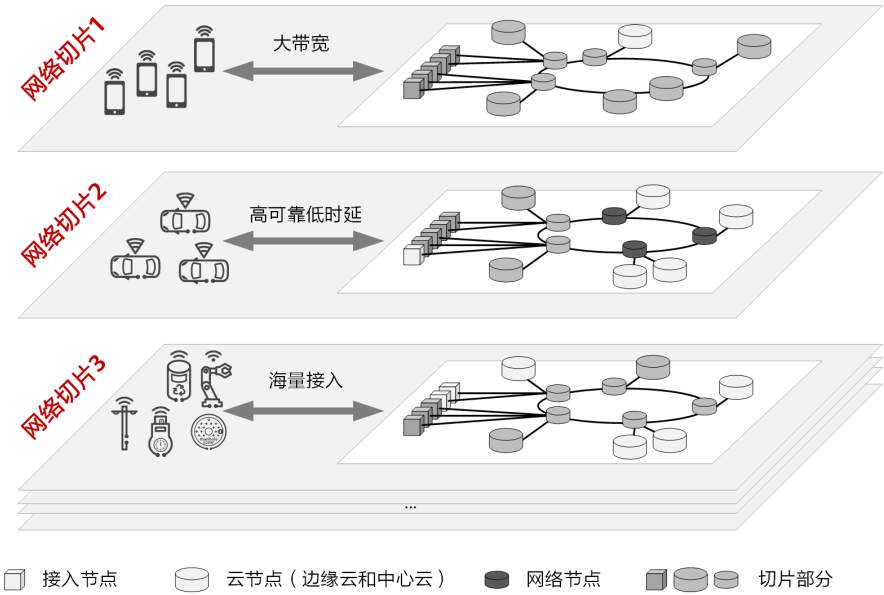
- eMBB（Enhanced Mobile Broadband，增强型移动宽带）聚焦对带宽有高要求的业务，如高清视频、虚拟现实/增强现实；
- uRLLC（Ultra-Reliable Low-Latency Communication，超高可靠超低时延通信）聚焦对时延和可靠性极其敏感的业务，如自动驾驶、工业控制、远程医疗、无人机控制；
- mMTC（Massive Machine Type Communication，大规模机器通信）则覆盖具有高连接密度的场景，如智慧城市、智慧农业。它们需要完全不同类型的网络特性和性能要求，这些多样的需求难以用一套网络解决。

图6-1 5G 时代的主要业务需求



为了在一张物理网络中同时满足不同业务的差异化需求，网络切片的理念应运而生。网络切片是在一张物理网络上切分出多张包含特定网络功能、由定制网络拓扑和网络资源组成的虚拟网络，用于满足不同网络切片租户的业务功能需求和提供服务质量 SLA 保证。5G 网络切片的示例如图 6-2 所示。

图6-2 5G 网络切片示例



5G 网络将基于一套共享的网络基础设施来为多租户提供不同的网络切片服务，各垂直行业客户将会以切片租户的形式来使用 5G 网络。对垂直行业来说，为租户提供服务的网络切片之间需要实现隔离，这点对于确保安全性和可靠性至关重要。

- 安全性：租户之间的数据/信息能有效隔离。
- 可靠性：有效避免某一租户的网络异常或故障影响同一网络中的其他租户。

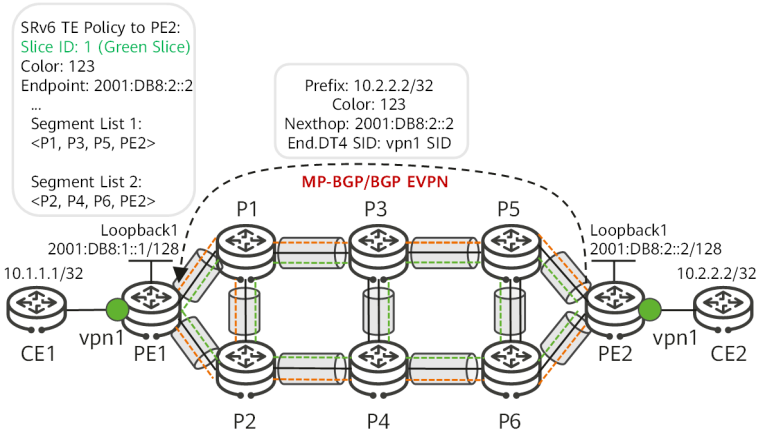
在提供网络切片服务的同时，运营商也从流量创收模式转变为服务创收模式。按需、定制、差异化的服务将是未来运营商业务提供的主要模式，也是运营商新的价值增长点。

基于 SRv6 的网络切片

在 SRv6 场景中，只有物理网络的节点分配 End SID，物理链路分配 End.X SID，切片网络内的逻辑节点或者逻辑链路当前不分配 SID，直接使用物理网络的 SID。

如图 6-3 所示，以 L3VPNv4 over SRv6 TE Policy 为例说明路由传递过程。

图6-3 网络切片控制层面路由传递过程

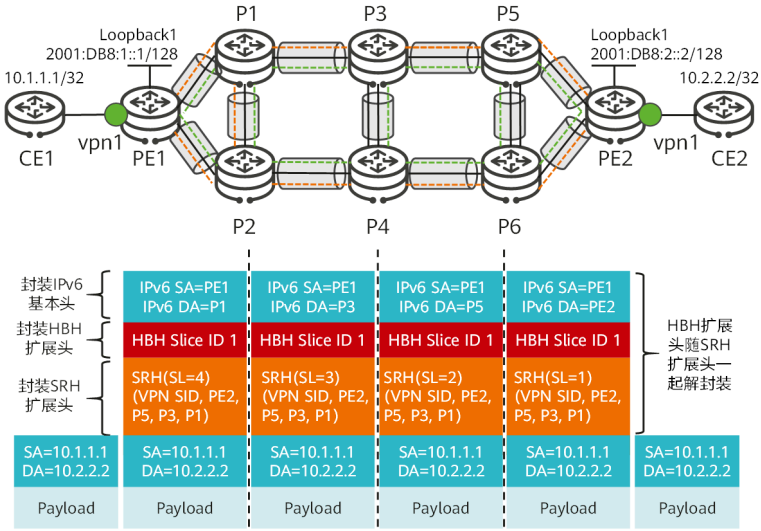


在路由传递阶段，PE2 可以通过 MP-BGP/BGP EVPN 邻居向 PE1 传递 VPN 路由，路由信息携带 Color、下一跳和 VPN SID 等信息。

PE1 上预先创建 SRv6 TE Policy，在 SRv6 TE Policy 下面配置 Slice ID，将 SRv6 TE Policy 和 Slice ID 关联。VPN 路由 10.2.2.2/32 在 PE1 上根据 Color 属性和下一跳信息进行路由迭代，迭代到 SRv6 TE Policy，进而通过该 SRv6 TE Policy 下的 Slice ID 关联到指定的切片网络，享有该切片网络的转发资源。

图 6-4 展示了 L3VPNv4 over SRv6 TE Policy 的数据转发过程。

图6-4 网络切片数据转发过程



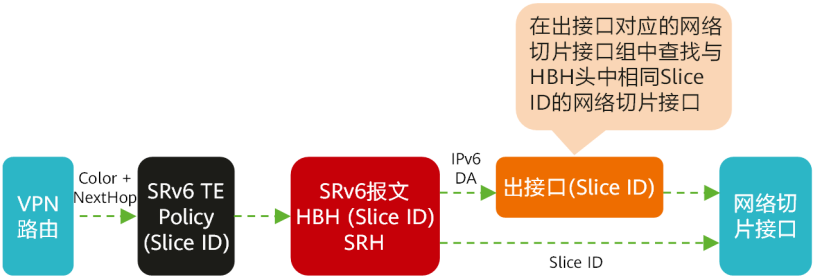
在数据转发阶段：

1. CE1 向 PE1 发送一个普通 IPv4 单播报文。
2. PE1 接收到 CE1 发送的报文之后，查找 VPN 实例路由表，该路由的出接口是 SRv6 TE Policy。PE1 为报文插入 SRH 信息，封装 SRv6 TE Policy 的 SID List，然后封装 HBH 扩展头，扩展头里携带 SRv6 TE Policy 的 Slice ID 信息，最后封装 IPv6 基本报文头。完成之后，PE1 将报文对 P1 转发，转发时通过 Slice ID 信息关联到指定的网络切片接口。
3. 中间 P1 设备根据 SRH 信息转发，转发时使用 HBH 扩展头里的 Slice ID 信息关联到指定的网络切片接口。P3 和 P5 的转发过程与 P1 类似。
4. 报文到达尾节点 PE2 之后，PE2 使用报文的 IPv6 目的地址查找本地 SID 表，命中到 End SID，所以 PE2 将报文 SL 减 1，IPv6 DA 更新为 VPN SID。

   PE2 使用 VPN SID 查找本地 SID 表，命中到 End.DT4 SID，PE2 解封装报文，去掉 SRH 扩展头、HBH 扩展头和 IPv6 报文头，使用内层 IPv4 报文的目的地址 10.2.2.2 查找 VPN SID 对应的 VPN 实例路由表，然后将报文转发给 CE2。

从以上过程可以看出，Slice ID 是控制层面和转发层面的纽带，所以这种网络切片方案也称为基于 Slice ID 的网络切片，具体如图 6-5 所示。

图6-5 Slice ID 连接控制层面和转发层面



6.2 SRv6 支持 iFIT

5G 业务由移动宽带服务拓展到了海量的机器互联和高可靠低时延通信，三大业务场景对承载网提出了更高要求，从网络运维及性能监控方面看，5G 网络需要在以下几个方面进一步提升：

- 网络性能劣化故障定位手段缺乏，需要引入有效的排障手段，提升运维效率。
- 目前的性能检测 OAM 粒度较粗（如端口/隧道/伪线），需要提供基于业务流级的、实时、高精度且准确反馈客户实际流量的性能检测机制。
- 为 5G 时延敏感类业务提供全网时延可视化、时延异常监控、时延选路等功能，提升 5G 用户体验。

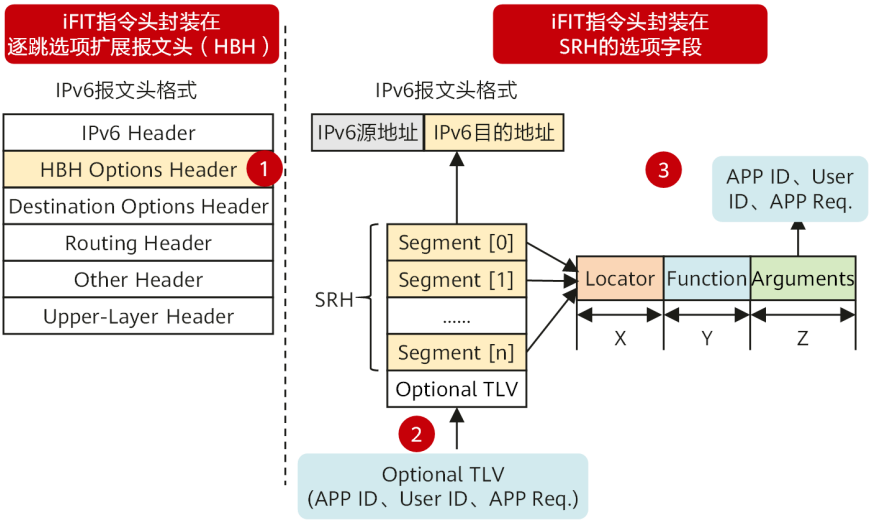
为应对 5G 承载网对性能监控的需求，针对目前 OAM 检测技术存在的不足，产生了 iFIT 随流性能检测方案。

- 扩展功能：iFIT 检测精度高，部署简单，具有未来的扩展能力。
- 故障快速定位功能：iFIT 提供了随流检测功能，可以真正实时地检测用户流的时延和丢包情况。

- 可视化功能：iFIT 通过可视化界面展示性能数据，并具备快速发现故障点的能力。

SRv6 技术在数据平面为应用提供了丰富的可编程空间。iFIT 的指令头可以封装在 IPv6 的逐跳选项扩展报文头（HBH Options Header）中，也可以封装在 SRH 的 Optional TLV 中。不同的封装形式具有不同的处理语义，也为 SRv6 的 OAM 带来了丰富的特性。

图6-6 SRv6 iFIT 封装



封装在逐跳选项扩展报文头中的 iFIT 指令会被所有的 IPv6 转发节点处理，如果封装在 SRH 扩展头之中，则只能由 SRv6 节点处理。在 SRv6 BE 或者是在 SRv6 TE Policy 松散路径的场景下，报文的转发路径并不固定，此时将 iFIT 指令封装在逐跳选项扩展报文头中可以让运维人员知道报文是怎么逐跳转发的，在网络出现故障时也方便进行问题定界。

6.3 SRv6 支持电信云

传统电信网络建设一直秉承软硬件一体化的思路，使用由设备厂商提供的专用硬件设备（如移动数据业务的 MME/SGW/PGW，固定业务的 BNG 等）组网为用户提供电信服务。随着电信业务的高速发展（如 5G 等新兴业务的兴起），网络的快速响应，业务场景多样性，高频率的新业务上线都成为电信网络不得不面对的挑战。传统专用硬件的电信设备，强依赖于设备供应商，网络扩容和新版本上线周期一般至少需要数月，极大地增加了新业务上线时间和经济成本。

随着网络功能虚拟化（Network Functions Virtualization，NFV）技术以及 IT 领域 Cloud Native 设计的成功应用与发展，虚拟化以及云化逐步成熟，并演变成为一种新的生产力，为电信网络提供了新的建设思路。电信运营商也想能像 IT 一样，实现电信设备软件和硬件的分离。通过采购通用或简化的硬件，实现能力/转发通量的提升及成本的降低；通过开发与硬件解耦的软件，能够快速开通新功能、上线新业务，提高响应速度。因此，云化电信网络及电信云成为电信网络的建设新架构。电信云的建设即原有电信业务网元节点的 NFV/云化。

当前边缘电信云承载的总体思路是将 DCN 与 WAN 网络融合，形成一个为 Spine - Leaf 的 Fabric 架构。我们将该网络架构称为 NAAF（Network as a Fabric）。

如图 6-7 所示，NAAF 的角色可以分为定义如下 Leaf（叶子节点）和 Spine（骨干节点）两类。

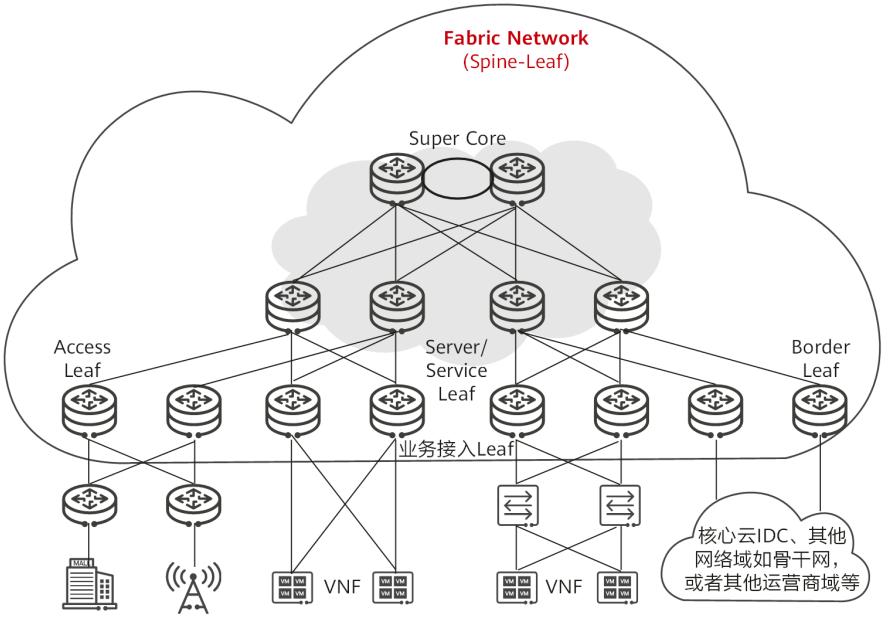
Leaf 是 Fabric 网络功能接入节点，提供各种网络设备接入 Fabric 网络的能力（通常为 WAN 网络中的 PE 设备）。按照接入的设备不同，Leaf 可以分为 Access Leaf、Server/Service Leaf 和 Border Leaf。

- Access Leaf：用于用户接入的节点，如移动接入的基站，固定接入的 OLT 等。
- Server/Service Leaf：提供 VNF 服务接入的节点，包括 VAS、vCPE、vUPF 和 BNG-UP 等的接入。
- Border Leaf：整体网络外联的节点，如用于连接背靠背的核心 DC、其他运营商和/或其他部门的网络。

Spine 不作为业务接入的设备，主要做高速流量转发，通常为 WAN 网络中的 P 设备。Spine 具有如下特点。

- 通过高速接口连接各个功能 Leaf 节点，避免各接入节点自行进行逐对全连接，同时使业务/Leaf 扩展更为容易，对已有业务无影响，可以做到平滑的向外扩展（Scale Out）。
- 为了覆盖较大的网络，Spine 节点可能会产生分级互联。

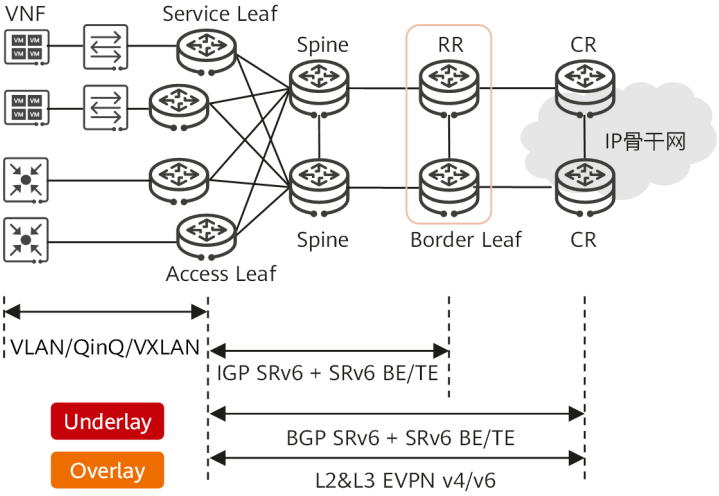
图6-7 Spine-Leaf 的 Fabric 架构



NAAF 边缘电信云网络架构由于拉通的 DCN 及传统的 WAN，因此整体的传输承载协议也需要做拉通。由于大规模云化属性的减弱，边缘电信云的电信联通属性要求更明显，因此成熟的电信传输方案（VPN，SRv6）更适合应用在此处。

NAAF 通过 SRv6 + EVPN 的技术支撑 IPv4/IPv6 双栈业务能力，同时为 5G、企业和 MEC 等提供业务能力支撑。NAAF 的关键技术如图 6-8 所示。

图6-8 NAAF 的关键技术



NAAF 传输层设计的关键优势表现在如下几个方面：

- 协议简化：统一 DCN 和 WAN 承载方案，简化了承载协议。
- 端到端业务能力：通过 E2E 统一的 SRv6 BE/TE，基于 SRv6 强大的可编程能力为 NAAF 提供端到端的路径调优、网络切片能力。
- 简化运维：承载在 E2E 的 SRv6 BE/TE 上的 VPN 技术消除了背靠背的 DC-GW 和 PE 间的跨域 VPN Option A 的业务配置点，并且能够提供端到端的 OAM 能力。
- 简化网络层级：统一了 DCN 和 WAN 承载网络，不需要再独立设置 PE、DC-GW、Leaf 等多层角色，将原来多层设备归并在一起由一层设备复用兼职完成，减少了建网成本。

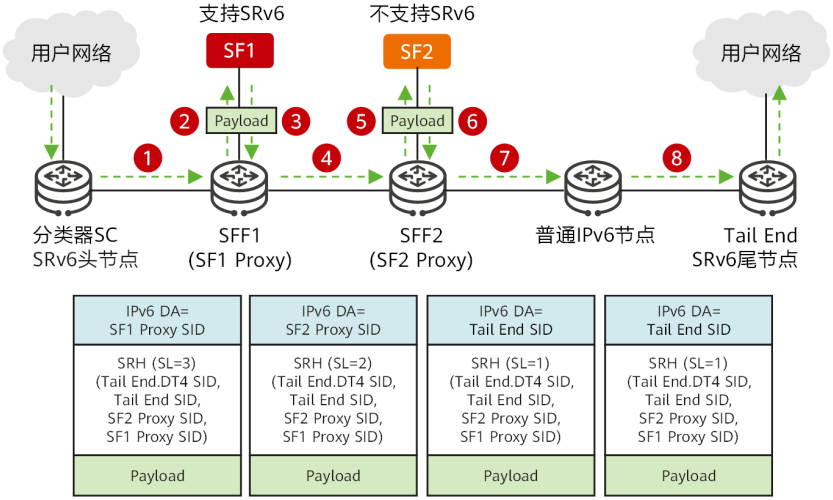
6.4 SRv6 支持业务链

业务功能链 SFC（Service Function Chain）是一种给应用层提供有序服务的技术。SFC 用来将网络设备上的服务在逻辑层面上联接起来，从而形成一个有序的服务组合。SFC 通过在原始报文中添加业务链路径信息来实现报文按照指定的路径依次经过服务设备。

数据报文在网络中传递时，往往需要经过各种各样的服务节点，从而保证网络能够按照预先的规划为用户提供安全、快速、稳定的服务。这些服务节点包括熟知的防火墙 FW（Firewall）、入侵防御系统 IPS（Intrusion Prevention System）、应用加速器和 NAT 等，网络流量需要按照业务逻辑所要求的既定顺序经过这些服务节点，才能实现所需要的业务。

如图 6-9 所示，SF1 和 SF2 是 SRv6-unaware SF（不支持 SRv6 的 SF）。为了实现业务链，需要分别在 SFF1 和 SFF2 配置 SF Proxy 功能，并且为 SF1 Proxy 和 SF2 Proxy 分配 SRv6 SID。分类器 SC 上基于 SF1 Proxy SID，SF2 Proxy SID 和 Tail End SID 组成一个 SRv6 TE Policy 的 Segment List，SRv6 TE Policy 作为业务链路径。

图6-9 SRv6 支持业务链



详细的数据转发原理描述如下：

1. 分类器 SC 从用户网络接收到原始 IPv4 报文，通过匹配五元组等分类信息进行分类，分类后的流量被重定向到 SRv6 TE Policy 中。分类器根据 SRv6 TE Policy 进行 SRv6 报文封装，SRv6 报文目的地址是 SF1 Proxy SID。在图 6-9 中，SRH 信息里除了 SRv6 TE Policy 路径信息以外，还有代表 VPN 业务或公网业务的 Tail End.DT4 SID。
2. SFF1 收到报文以后，执行 SF1 Proxy SID 对应指令，解封装报文，然后将原始报文发送到 SF1 进行处理。
3. SF1 处理完报文以后，将报文发回给 SFF1。
4. SFF1 根据报文的入接口（SFF 上与 SF 相连的接收 IPv4 报文的接口）信息，查找配置信息，然后依据配置重新添加 SRH 信息，进行 SRv6 封装，此时 SRv6 报文目的地址是 SF2 Proxy SID。
5. SFF2 收到报文以后，执行 SF2 Proxy SID 对应指令，解封装报文，然后将原始报文发送到 SF2 进行处理。
6. SF2 处理完报文以后，将报文发回给 SFF2。
7. SFF2 根据报文的入接口（SFF 上与 SF 相连的接收 IPv4 报文的接口）信息，查找配置信息，然后依据配置重新添加 SRH 信息，进行 SRv6 封装，此时 SRv6 报文目的地址是 Tail End SID。报文沿着 IGP 最短路径转发给 Tail End 节点。
8. Tail End 节点收到 SRv6 报文后，发现报文目的地址是自己的 End SID，所以执行该 End SID 相关的指令，解封装报文，SL 减 1，变为 0，同时更新 IPv6 目的地址字段。当前报文 IPv6 目的地址字段是 Tail End.DT4 SID，Tail End 节点使用 Tail End.DT4 SID 查找本地 SID 表，执行 Tail End.DT4 SID 相关的指令，将原始 IPv4 报文转发到对应的 IPv4 VPN 或者公网。

6.5 SRv6 支持 SD-WAN

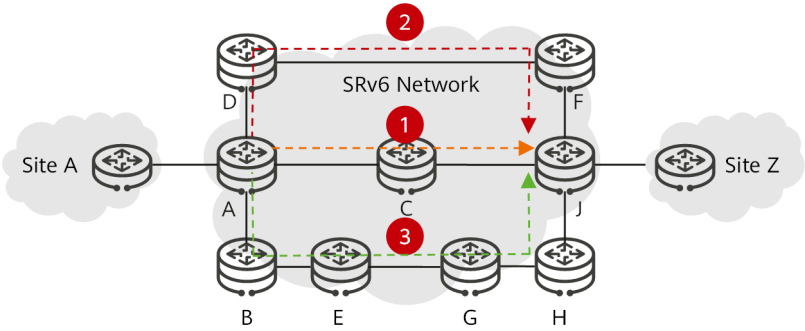
SD-WAN（Software-Defined Wide Area Network） EVPN 是一种通过扩展现有 EVPN 技术来实现 Overlay 业务网络和 Underlay 传输网络分离的 VPN 解决方案，用于解决企业分支互联的问题。

SD-WAN EVPN 在 BGP 协议基础上扩展了新的网络层可达信息（Network Layer Reachability Information，NLRI），即：定义了新的 BGP SD-WAN 路由，站点之间通过 BGP SD-WAN 路由来互相传递 TNP（Transport Network Port）信息，其中包含了站点之间建立 SD-WAN 隧道所需的关键信息。然后，站点之间利用 EVPN 的 IP 前缀路由（Type5 路由）来互相通告各自的业务路由，当本端站点收到对端站点发来的 EVPN 路由后，触发创建到达对端站点的 SD-WAN 隧道，打通 Underlay 网络的数据通道；同时，使 EVPN 路由最终迭代到 SD-WAN 隧道，打通 Overlay 网络的业务路径。

如图 6-10 所示，服务提供商网络支持应用触发创建多条不同 SLA 的路径。我们列举了 3 种满足不同 SLA 需求的路径：

1. 缺省路径（SRv6 BE）。
2. 按应用需求触发创建的低时延路径。
3. 按应用需求触发创建且保证 100 Mbit/s 带宽的路径。

图6-10 服务提供商网络创建多条满足不同 SLA 需求的路径



1.缺省路径（SRv6 BE）：<2001:DB8:C9::1>
2.低时延路径：<2001:DB8:C4::1，2001:DB8:C6::1，2001:DB8:C9::1>
3.保证宽带100 Mbit/s的路径：<2001:DB8:C2::1，2001:DB8:C5::1，2001:DB8:C8::1，2001:DB8:C9::1>

总结起来，SRv6 SD-WAN 方案的优势主要包括如下几个方面：

1. 整网统一调度：支持 4G 和 5G 的 Native IPv6 的 SD-WAN，替代原有的 VXLAN 和 GRE。
2. 可以大规模扩展：服务提供商网络不知道 SD-WAN 实例的任何策略变化，无论是分类流，何时引导它以及在哪条路径上。服务提供商的作用主要是在网络边缘维护 SRv6 TE Policy 状态，并在其网络中维护几百个 SID。这充分地利用了 SRv6 无状态属性的优势。
3. 高度保护隐私：服务提供商网络不共享其基础设施、拓扑、容量、内部 SID 的任何信息，确保网络隐私安全。

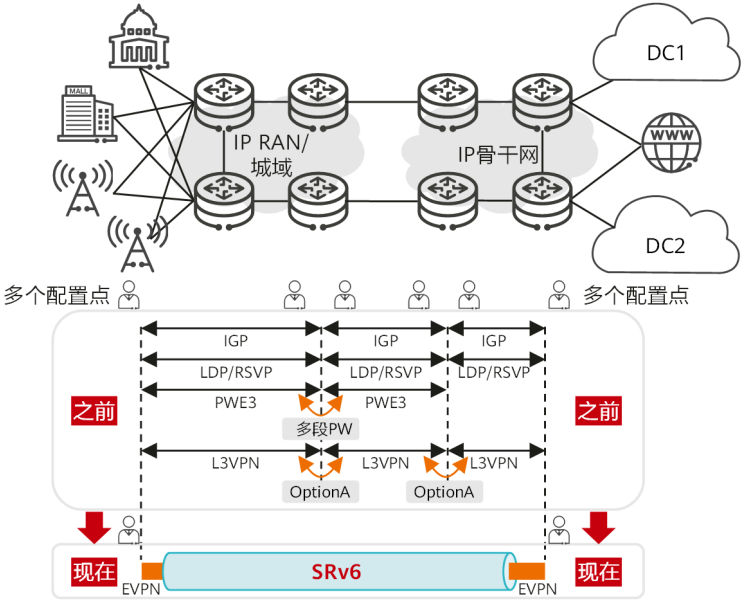
第7章
SRv6 的成功应用

本章主要介绍SRv6的成功应用案例。随着云计算的逐渐发展，业务上云已成为大多数客户首要考虑的服务部署方式，而多云/ 混合云则是大多数上云需求的首选策略。云网融合产品通过云专线满足客户快速、安全、可靠访问云资源池；通过云骨干，跟多云商云池互联，实现企业一线接入多云的需求；同时，通过云网智能化运营平台，打造云网差异化服务品牌，实现云网业务自动发放、带宽动态调整等功能。

7.1 简化统一 IP 承载网

如图 7-1 所示，IP 承载网存在诸多跨域业务，包括移动 3G/4G、VoIP 与专线业务等。现网采用分段式业务部署方案，不仅端到端部署复杂，而且做分段跨域配置操作时，需要多个部门对接协调操作，业务开通速度很慢，时间按月计，很大程度影响了业务运营。此外，当前网络里多种协议并存，运营商希望能够简化网络架构，实现业务自动化部署，并提升业务部署速度。

图7-1 简化统一 IP 承载网



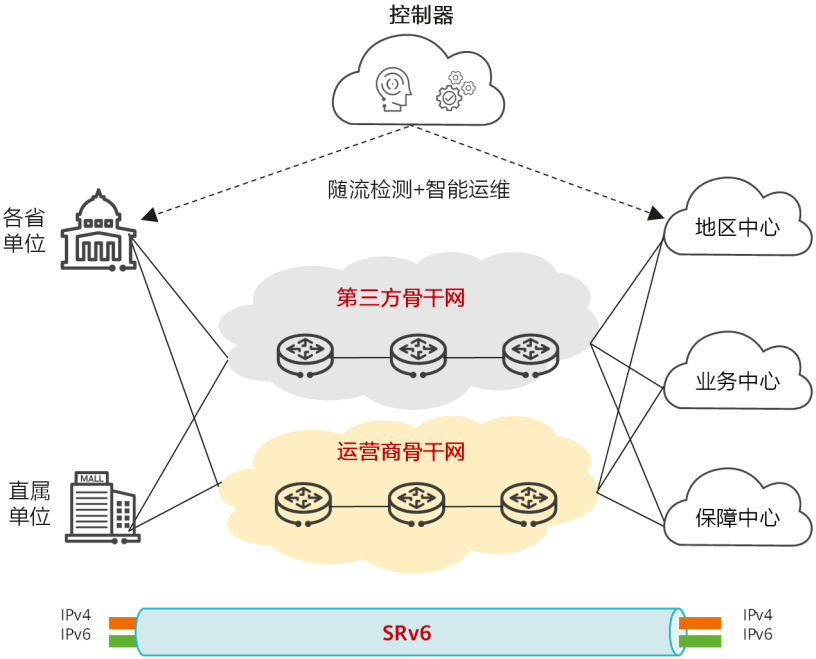
为了解决上述问题，在网络里引入了 SRv6。该方案具有如下特点：

1. 网络协议极简：SRv6 是对网络架构的一次革命性简化，面对传统架构中复杂的 MPLS 协议，SRv6 实现了网络协议的去 MPLS 化，所有现网业务无须进行 MPLS 配置，仅保留了 IGP 与 BGP 两种基础网络协议。
2. 业务开通快速：基于 IPv6 路由的可达性，SRv6 简化了跨域的难度。一方面，对于非关键业务保持 SRv6 BE 承载，业务仅两端部署，中间节点仅需支持 IPv6，从而最大程度地提升网络运维效率。另一方面，通过 SRv6 TE Policy 承载 B2B 专线业务，实现了专线业务自动发放，将开通时间缩短到 1 天。
3. 可持续演进：基于 SRH 的可编程性，SRv6 实现了网络与业务的解耦，在未来演进中也无须新增其他协议，而且支持网络可持续演进。

7.2 构建智能专业广域网

如图 7-2 所示，某业务骨干网需要基于第三方的骨干网络和运营商的 MPLS VPN 网络构建全国业务单位的联接，但是由于无法管控第三方网络，因此穿越第三方骨干网和运营商骨干网网络时，依靠传统的 SDN 技术无法实现网络的智能调整和优化。

图7-2 智能专业广域网



该网络选择 SRv6 技术部署，采用 SRv6 TE Policy 开通 L3VPN 专网承载方案，穿越了第三方网络实现了 SDN 网络调优。

该方案具有如下特点：

1. 跨域体验好：多种业务都通过 SRv6 进行统一承载，关键业务通过 SRv6 TE Policy 承载，提供差异化 SLA 能力保障，确保无损。

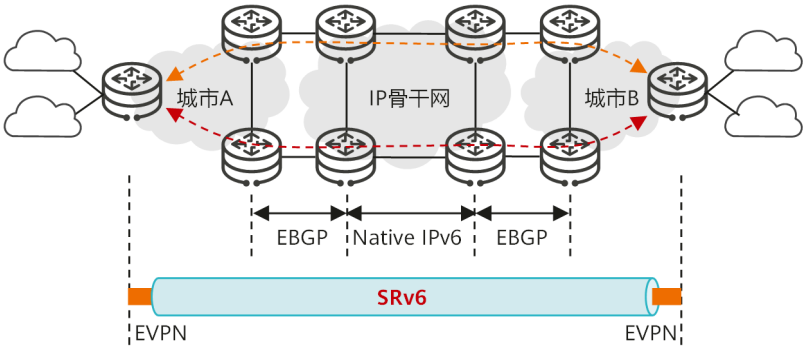
2. 端到端高可靠：基于 SRv6 实现端到端 50ms 故障倒换，加上随流检测、智能运维等技术，网络更加可靠安全。

7.3 跨域云骨干专线

在云时代，企业的业务可能会同时接入多种不同类型的云，而各个地域的云也有互联的需求。按照传统方案，跨越多个地域进行云互联时，只能选择 OptionA/B/C 或 Seamless MPLS 等方案，不仅需要多个地域的相关部门配合来开通业务，而且由于协议众多，网络状态复杂，业务运维十分不便，网络的可靠性不足。

如图 7-3 所示，某运营商单独建设了多云汇聚新型城域网，通过 SRv6 Overlay 方案实现了跨域云骨干专线。

图7-3 跨域云骨干专线方案



该方案具有如下特点：

1. 业务开通快速：仅对城市 A 的城域设备和城市 B 的数据中心出口设备升级，就可以部署 SRv6 功能。通过 SRv6 VPN 跨越互联骨干网，从而快速构建了城市 A 和城市 B 两大核心城市之间的跨省云骨干专线。
2. 按需升级演进：如果在部分中间节点上引入 SRv6，还可以实现按需的路径选择，根据业务服务需求，引导流量通过骨干网络，轻松实现网络路径优化。

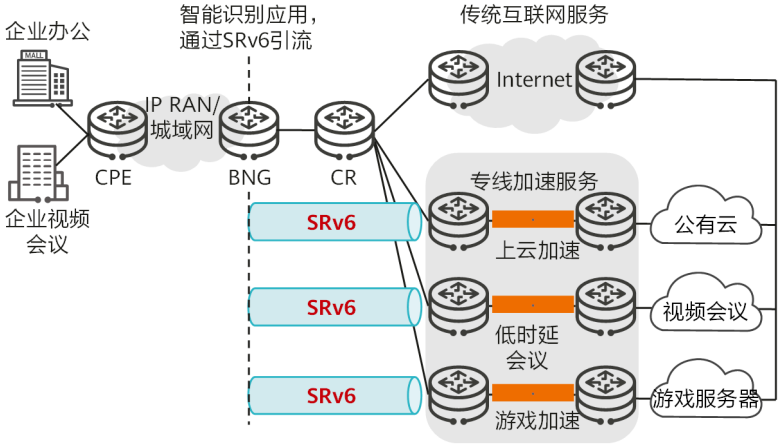
3. 跨域体验好：SRv6 改变了传统专线跨域场景下的多段拼接方式，方便不同网络之间的跨域，实现一跳入云。通过 L3VPN/EVPN L3VPN 等 L3 技术承载云专线及云间互联，利用 L3 网络路由能力实现企业站点一点接入、灵活访问任意云资源池，同时借助 SRv6 TE Policy 对不同的云上应用提供差异化的 SLA 保障。

7.4 国际互联网云专线

数据网络成为我们每个人工作、生活的必备品，与水、电、燃气一样。越来越多的企业加速适应了在线办公的场景，开始在线上召开视频会议、在线上协同开发软件产品，在线上实时交互生产数据。对跨国公司来说，线上办公需求更是广泛且迫切。

通过引入 SRv6 技术，轻松解决了上述需求，具体如图 7-4 所示。

图7-4 国际互联网云专线



该方案具有如下特点：

1. 智能引流加速：通过在 BNG 设备智能识别应用，灵活导入不同的 SRv6 路径，按照不同的策略进行加速，提升终端用户体验。整个过程对用户来说不需要任何操作。
2. 轻松业务变现：对运营商来说只需要预部署 SRv6，后续不需要过多操作，即可通过提升业务体验实现商业变现。

7.5 智能云网政府行业

人类社会正在进入万物互联的智能时代，传统网络也在向智能云网迈进。未来网络至少有如下显著的特点与需求：

1. 企业业务多云应用兴起，云计算将进入多云时代，云数据中心互联需求，云与网络的融合需求都更加迫切。
2. 各种不同类型的业务对于网络的要求不尽相同，网络必须从尽力而为到能够提供确定性 SLA 保障，实现一网承载千行百业。
3. 云网一站式服务、快速开通、灵活调整成为关键需求。未来的智能云网将不再是独立的云和承载网，而是一张云网融合的业务网，面向最终的客户提供云网一体化的产品与服务。客户可以像在电商平台采购一样任意选择产品组合，从签约到履约实现在线自助，快速开通，流程可视。

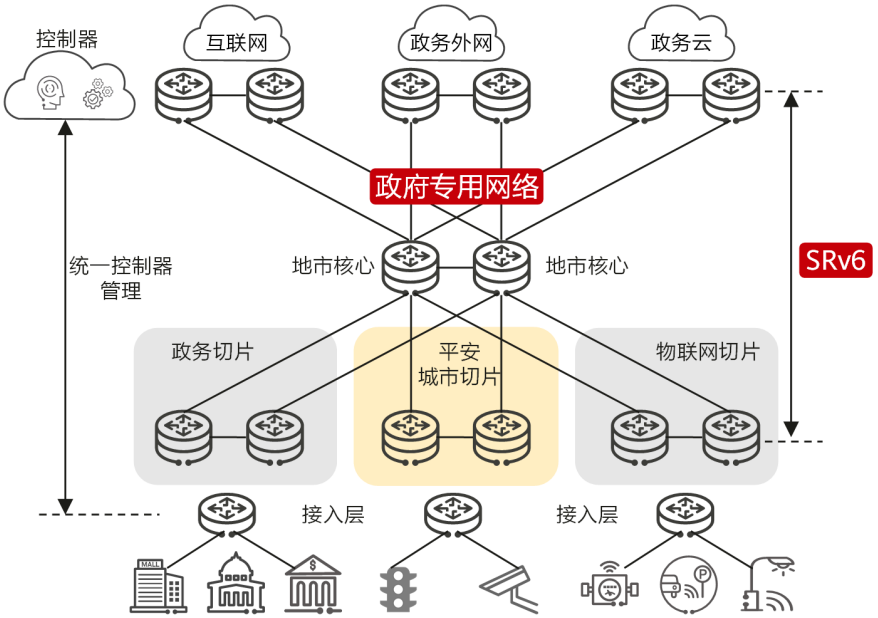
智能云网方案是以智能 IP 网络为基础，而智能 IP 网络的基础正是 SRv6。智能云网方案能够助力运营商打造面向千行百业的解决方案，支撑行业数字化转型，这些行业包括政府、医疗、教育、金融和能源等。以下以政府行业为例介绍智能云网方案，并且介绍 SRv6 如何实现智能云网。

智慧政务深化改革过程中，面临着诸多问题，比如各委办局之前没有联通，成为信息孤岛，信息共享难；政务外网接入点少等。智慧政务的核心诉求主要是两点：

1. 一网统管：进行网络集约化建设，各专网并入政务外网。实现关键点是必须保证业务安全隔离。
2. 一网通办：数据集中统一管理和共享，城市的海量物联感知数据和监控视频上传至多级政务云，供多个委办局调用。实现关键点是网络广覆盖，业务快速上多云，以及云间灵活互通。

如图 7-5 所示，通过 SRv6 简单快速地打通云和各地接入设备之间的基础网络连接，确保业务高效开通，后续通过网络切片技术，政企专网划分不同业务平面，保障政府办公、物联、视频等业务严格隔离，同时为不同业务提供差异化确定性 SLA 保障。

图7-5 智能云网政府行业 SRv6 的应用



该方案具有如下特点：

1. 快速开通业务：业务全面上云，云下一张网络，各个部门利用 SRv6 一跳入云，极速开通业务。
2. 业务体验好：一张网络，划分多个网络切片，实现资源硬隔离，满足不同部门的业务需求，SLA 可承诺。
3. 端到端高可靠：基于 iFIT 技术进行可视化运维，实现分钟级故障定位。

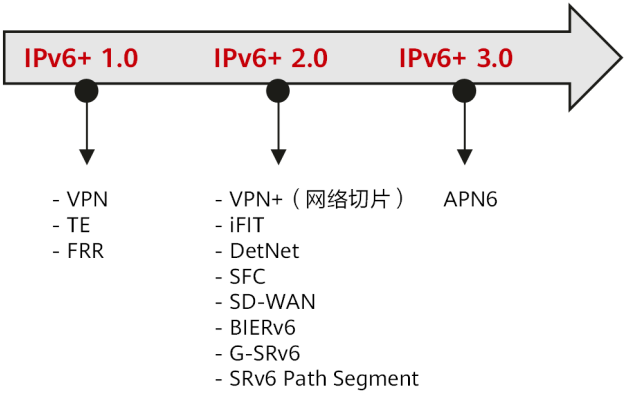
第8章
从 SRv6 到 IPv6+

SRv6 的出现为 IPv6 的规模部署提供了新的机遇，SRH 扩展头的使用给了人们很大的启发。随着新业务的发展，技术层面上也已经不再局限于 SRv6，也就是说数据平面不仅是基于 SRv6 SRH 封装，而且扩展到基于其他 IPv6 扩展头封装，比如：

- 基于目的选项扩展报文头 DOH 来实现 BIERv6；
- 基于逐跳选项扩展报文头 HBH 来实现网络切片；
- 基于逐跳选项扩展报文头或 SRH 的 Optional TLV 也可以使 SRv6 支持 iFIT。

可以说，自从 SRv6 打开了基于 IPv6 扩展报文头的创新之门以后，基于 IPv6 的新应用方案开始层出不穷。业界将这些统一定义为 IPv6+，同时定义了 IPv6+发展的 3 个阶段，如图 8-1 所示。

图8-1 IPv6+发展的3个阶段



这三个阶段具体包括：

1. IPv6+ 1.0：主要包括 SRv6 基础特性，包括 TE、VPN 和 FRR 等。这 3 个特性在现网应用广泛，SRv6 需要继承下来，并利用自身的优势来简化网络的业务部署。
2. IPv6+ 2.0：重点在面向 5G 和云的新特性。这些新特性需要 SRv6 SRH 引入新的扩展，也可能是基于其他 IPv6 扩展头进行扩展。这些可能的新特性包括但不局限于 VPN+（网络切片）、iFIT（in-situ Flow Information Telemetry，随流检测）、DetNet（Deterministic Networking，确定性网络）、SFC（Service Function Chaining，业务功能链）、SD-WAN（Software Defined Wide Area Network，软件定义广域网）、BIERv6（BIER IPv6 Encapsulation，位索引显示复制 IPv6 封装）、G-SRv6（Generalized SRv6）和 SRv6 Path Segment 等。
3. IPv6+ 3.0：重点是 APN6（Application-aware IPv6 Networking，应用感知的 IPv6 网络）。随着云和网络的进一步融合，需要在云和网络之间交互更多的信息，IPv6 无疑是最具优势的媒介。

IPv6 不是下一代互联网的全部，而是下一代互联网创新的起点和平台，IPv6+的路线图有利于引导网络有序演进。随着 IPv6 的规模部署，以 SRv6 为代表的 IPv6+技术将在网络中广泛应用，构建出智能化、简单化、自动化、SLA 可承诺的下一代网络。

IP网络
系 列 丛 书

联系我们

networkinfo@huawei.com

获取更多 IP 网络系列丛书

https://e.huawei.com/cn/solutions/enterprise-networks/ip-ebook