



# 中国移动弹性 SD-WAN 技术 白皮书 (2020 年)

中国移动研究院

## 前 言

在新业务、新需求层出不穷的云时代，企业上云是数字化转型的必经之路。为提供灵活的网络连接和高质量上云同时降低广域网的开支，在 SDN 技术的推动下 SD-WAN 应运而生。

SD-WAN 是将 SDN 技术应用到广域网场景中所形成的一种服务，本质是一种 OTT 业务，基于无线、传输和承载等物理网络（也称为 Underlay 网络）之上利用隧道技术创建一个 Overlay 虚拟网络，并利用 SDN 在广域范围对该虚拟 Overlay 网络进行管控的技术。

当前中国移动企业上云主要产品为基于 Underlay 网络的专线，价值高、性能高但开通流程长。现有 SDWAN 为基于纯 overlay 的虚拟网络，开通快但性能难以得到保障。通过弹性 SD-WAN，一方面可以实现 Underlay 和 Overlay 的协同实现服务质量保障；另一方面可以融合云内虚拟化网元提供业务链服务。弹性 SD-WAN 整合云、网资源为企业用户提供全新云网服务体验，将会成为未来弹性 SD-WAN 的重要发展方向。

本白皮书旨在提出中国移动弹性 SD-WAN 技术方案，充分发挥运营商 Underlay 网络资源优势，为应用提供差异化服务能力，希望能够为产业在研究、部署弹性 SD-WAN 相关技术、产品和解决方案时提供参考和指引。

本白皮书的版权归中国移动所有，未经授权，任何单位或个人不得复制或拷贝本建议之部分或全部内容。

## 目 录

1	概述.....	2
2	技术背景.....	4
2.1	Overlay 技术概述.....	4
2.2	SRv6 技术概述.....	5
3	弹性 SD-WAN 的技术架构.....	7
3.1	总体架构.....	7
3.2	应用场景分析.....	8
3.2.1	大型企业场景.....	8
3.2.2	中小微型企业场景.....	9
3.2.3	企业混合场景.....	11
3.3	控制和转发原理.....	11
3.3.1	大企业场景.....	11
3.3.2	中小微企业场景.....	14
3.3.3	采用 G-SRv6.....	15
4	弹性 SD-WAN 的方案亮点.....	16
4.1	Underlay 协同能力.....	16
4.2	IPv6 原生业务链.....	17
4.3	Telemetry.....	17
4.4	应用感知能力.....	18
5	测试验证.....	18
6	总结.....	19
	缩略语列表.....	21
	参考文献.....	23

## 1 概述

传统企业广域网是企业通过租用运营商链路或自建链路，解决地域大跨度范围的总部、数据中心、分部、办事处以及移动办公等各级节点间互联互通的企业私有网络。近年来，企业数字化变革和经济全球化趋势不断演进，同时，云计算和网络虚拟化等新技术逐渐成熟，这一切都对传统企业广域网的网络架构和业务模型都产生了深远的影响，新形势下的企业广域网在组网、应用体验保证、安全等方面正面临一系列新的挑战。SD-WAN 正是在这种背景下应运而生，它是一种把 SDN 运用到广域网实现企业上云、组网的技术。

企业应用的基础设施部署方式发生了变化，可以选择自建的数据中心承载应用，也可以选择公有云提供的 IaaS 或 SaaS 服务来承载。对于企业自建数据中心及其他知道企业总部、办事处等节点的广域互联，可以通过私有专线网络连接其他广域节点，也可以基于 Internet/4G/5G 的加密安全隧道连接，还可以同时部署两种以上混合的方式互连。企业公有云的应用基础设施部署，有的是通过服务提供商提供的专线云连接实现用户站点和公有云的互通；也有的是通过 Internet 的加密安全隧道连接。

企业大量的企业关键应用中，常见的企业应用包括：企业经营管理类应用，如 SAP/ERP 类应用，企业办公类应用，如语音、视频会议、远程桌面、文件传输、Mail 等。这些不同的应用对广域网链路质量的要求不同。

这些大量的应用和基础设施云化使得整体广域网带宽及组网复杂度都大幅度增加，原有的企业广域网的分散的管理每个单独的节点设备方式，很难解决基于不同应用所需的各种复杂策略配置。此外，企业公有云的使用，也打破了企业 IT 传统的封闭架构，使得安全性管理愈发复杂。

企业寻求从传统的管理每个单独的广域网设备，到集中式系统，支持进行全网协调，端到端地保证应用的 SLA 体验和安全。

针对企业传统广域网的问题，SD-WAN 解决方案主要通过以下方式来满足新一代广域网管理的需求：

- 1) 支持物理广域网节点和云节点（私有云、公有云）融合组网，并支持多种 WAN 接入方式，包括支持 MPLS 与 Internet 等多种类型 WAN 链路，并

进行负载分担，支持安全可靠的 WAN 连接，如果链路质量劣化，链路动态进行负载分担，并保证业务收敛性能；

- 2) 支持根据应用不同的 SLA 要求不同的 WAN 接入进行选路，将重要的应用流量分配到传输质量更优的线路上，最大化地利用网络投资；
- 3) 广域网连接与应用统一部署和管理，并基于企业站点、应用以及 VPN 的流量和性能报告和可视化；
- 4) 零配置开局与自动业务发放，实现海量广域节点集中快速管理和控制；

大多数 SD-WAN 解决方案，都是通过 SD-WAN 控制器和编排器对企业的广域节点进行集中管理和控制，从而根据全网的资源状态集中调度基于应用的转发及 QOS 策略，然而由于在这种实现下割裂的方式看待 Overlay 和 Underlay，以及割裂的看待云和网，只能以相对固定的方式基于云、网提供服务，难以发挥 SD-WAN 最大价值。例如为保障服务质量。当前主流的方式是可以透过专线接入企业广域节点并在其上运行 SD-WAN 来保障 SLA。这种方式本质是资源售卖，难以在新业务、新需求层出不穷的云时代，应对业务快速创新、敏捷开通、差异化服务等各种挑战。

SRv6 同时具备隧道和 VPN 业务能力，可以推动云服务、物理网络技术归一化到 SRv6。而运营商经过多年的投资建设，形成了规模庞大的全面覆盖所有省份、地市以及区县的物理网络及覆盖大区、省份、地市的云资源池。

弹性 SD-WAN 旨在利用 SRv6 技术，基于物理网络能力和云服务能力的对外开放，在 Overlay 层实现云、网能力的整合提供网加云的产品服务。将会为广域服务注入新能力，提供应用粒度的服务，为每应用提供不同 SLA 保障，为每应用提供不同增值业务服务，从而最大化发挥云网资源能力。网络可实现按需进行定制，既可以提供有 SLA 保障的低时延专线产品，也可以提供时延不敏感的大带宽业务的产品，还可以针对细分的需求进行精确定制。基于云部署的增值业务可按需提供服务，例如互联网流量经防火墙、入侵检测，而视频会议流量需经广域网加速等等。

## 2 技术背景

SD-WAN 的技术核心是利用 SDN 在广域范围对虚拟 Overlay 网络进行管控。Overlay 技术可以屏蔽各种运营商 WAN 网络 Underlay 的差异，用好 Underlay 网络的能力对于 SD-WAN 的品质至关重要。SD-WAN 常见的 Overlay 网络技术常使用 IETF 定义的 VxLAN/GRE/IPSec 等隧道技术，一方面多段隧道技术导致端到端连接开通需要对多个设备进行配置使得系统性协同高度复杂，另一方面隧道的反复的封装和解封装操作降低转发效率。

SRv6 不仅可以提供所有上述隧道的能力，而且还可以融合 Overlay、Underlay，并且具备网络可编程能力。可以预见到，SD-WAN 未来利用 SRv6 融合云、网能力在盘活基础云、网资源的同时为市场提供极具竞争力的全新政企产品。

### 2.1 Overlay 技术概述

Overlay 在网络技术领域，是一种网络虚拟化技术，基于底层物理网络抽象出一个利用 IP 隧道互联的叠加虚拟网络，使得网络摆脱物理网络的多专业、多供应商、多管理域的复杂性，对外呈现为一个单一 IP 技术的虚拟网络，通过结合 SDN 技术实现集中管理、跨广域管理的一个 VPN。

当前 Overlay 隧道技术存在多种，源自数据中心的 VxLAN，源自网络的 IPSec、GRE 等。对于现有的隧道来说，流量在指定源、目的端点之间进行转发，不具备指定或变更任何转发路径的能力。换一句话说，如果流量需要被差异化对待，则不同流量需要被引入到不同隧道中，而往往一条完整的路径需要多条隧道拼接而成，并且隧道的配置涉及到源、目的两个不同的设备。综上，如果要为海量客户的不同业务提供精细化服务，基于现有技术的实现将会非常复杂。

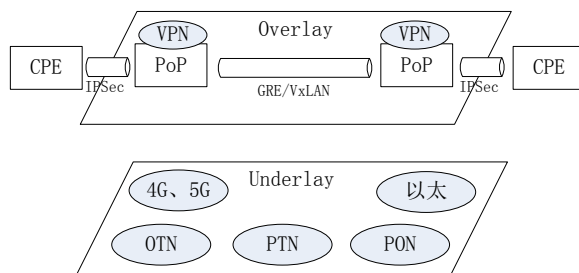


图 2.1 SRv6 在 SD-WAN 中的应用

## 2.2 SRv6 技术概述

Segment Routing (SR) 是一种源路由技术，通过为网络中的节点、链路或业务功能分配 Segment，并在头节点将这些 Segment 进行按需组合，形成封装在报文头中的 Segment 序列。当报文到达 SR 域的入口时，可以根据需求压入 Segment 序列，按照 Segment 序列中 Segment 的指示依次引导报文到对应的节点、链路或业务功能。

SR 的优点可以总结为四个方面：

(1) 控制协议简化：SR 通过 IGP 和 BGP 协议分发段标识 (Segment Identifier, SID)，无需部署和维护传统的 LDP, RSVP-TE 等信令协议。

(2) 高可扩展性：SR 通过对有限的链路和节点 Segment 的组合生成海量的 SR 路径，且路径信息只需在头节点保存，网络中间节点无需维护每路径状态信息。

(3) 可编程能力：在 SR 技术体系中，可以把 Segment 看成是一种指令，通过 Segment 的组合形成满足特定需求的 SR 路径可以看成是对网络的编程。这种编程可以灵活建立满足不同需求的路径，释放网络的价值。

(4) 高可靠保护：SR 能提供 100%网络覆盖的快速重路由 (Fast Re-Route) 保护，解决了 IP 网络长期面临的技术难题，能够在高可扩展性同时达到完全的可靠性保护。

SRv6 是一种基于 IPv6 数据平面实现的 SR 源路由技术。SRv6 的 Segment ID (SID) 的长度为 128 比特，与 IPv6 地址保持一致，其格式通常由 3 部分组成，包括 Locator (定位标识)，Function (功能) 和可选的 Argument (参数) 字段，如下图所示：

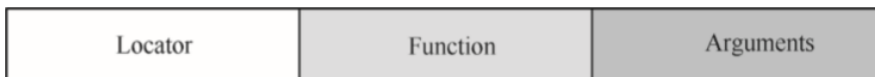


图 2.2 SRv6 SID 格式

其中：

- Locator 是分配给一个网络节点的标识，用于路由和转发数据包。在 SRv6 SID 中 Locator 是一个可变长的部分，用于适配不同规模的网络。Locator 标识的有两个重要的属性：可路由和可聚合。
- Function 是用来表达该指令要执行的转发动作，相当于计算机指令的操作码。在 SRv6 网络编程中，不同的转发行为由不同的 Function 来表达。
- Argument 是一个可选字段，用于携带在执行指令时所需要的参数。这些参数可能包含流，服务或任何其他相关的信息。

通过对 SRv6 SID 格式的如上定义，使 SRv6 SID 可以被用于灵活指示网络中的各种操作和参数。

另一方面，SRv6 在 IPv6 的路由扩展报文头中引入了新的分段路由头（Segment Routing Header, SRH），用于携带 SRv6 SID 的序列，实现对 SRv6 网络路径和各种功能的灵活编程。SRH 还可以包括可选的 TLV 字段，用于携带长度可变的数据，为 SRv6 提供了更好的扩展性。SRH 的格式如下图所示。

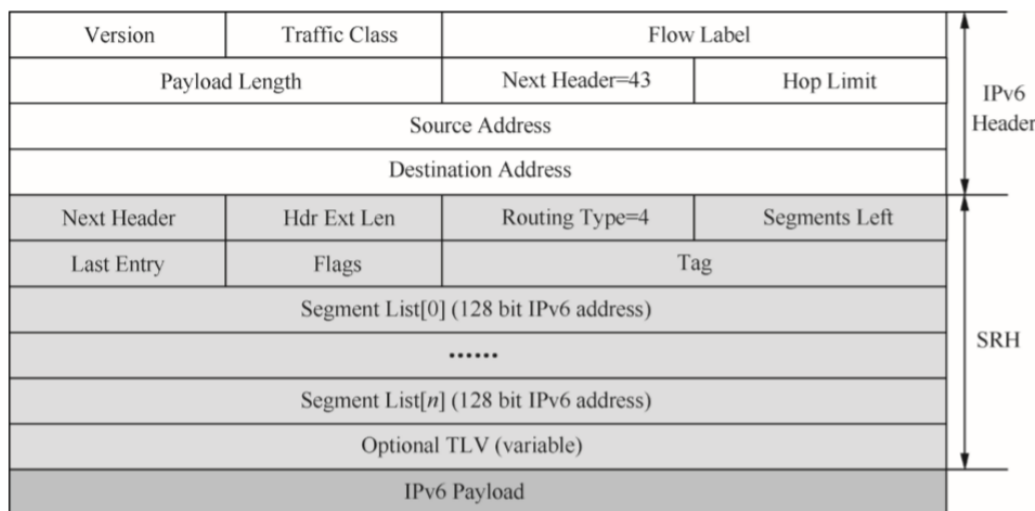


图 2.3 SRH 头封装原理

SRv6 在继承 SR 全部优点的同时，通过与 IPv6 的结合获得了更强的扩展性和可编程能力，在网络简化和满足新业务需求方面有独特的优势，使其成为下一代





弹性 SD-WAN 业务主要提供两大类 SD-WAN 业务：

1. 应用定义的组网、上云专线：为企业客户同时提供上网、上云和组网服务，提供一线多业务能力。对企业客户主要是提供灵活的带宽和时延连接业务，可通过 SD-WAN CPE 为应用定义相应 Underlay 网络的切片，动态为不同应用选择不同带宽和时延的路径，直接实现为应用粒度的业务开放网络能力。
2. 基于 NFV 的增值业务：为企业客户提供网络服务的同时结合云资源和 NFV 技术提供不同类型的 VNF 服务。SD-WAN CPE 基于应用粒度定义其增值服务，通过 CPE 实现网络和云内增值服务能力的组合。例如为客户上网业务提供尽力而为的网络和防火墙增值服务；为客户视频会议业务提供专用的网络路径及 FEC 增值服务实现品质优化。

## 3.2 应用场景分析

按照客户类型分类，弹性 SD-WAN 解决方案分为了面向大型企业、中小微企业两种应用场景，每种应用场景均包含上网，入云和分支互联三种业务类型。

### 3.2.1 大型企业场景

对于大型企业，企业的自主管理能力较强，业务透明传输的需求明显，这种解决方案的优点是为企业应用提供自主可控的网络路径选择。该场景下三种业务类型描述如下。

#### 1. 分支互联业务

SRv6 隧道从企业分支的一端 CPE1 开始，结束在远端分支的 CPE2，即借助运营商网络实现端到端 SRv6 隧道连接。PoP GW 仅充当运营商提供的可选增值业务锚点，不需要感知客户的 VPN 路由。

#### 2. 入云业务

企业租用运营商或者第三方公有云业务，在云端部署 VPC GW，SRv6 隧道从企业端 CPE1 开始，结束在云端的 VPC GW，实现企业便捷上云。

随着运营商云网一体的逐步推进，后期 VPC GW 可逐渐与云 PE 融合，通过 SD-WAN 控制器与骨干网控制器、云管控平台联动，实现端到端入云业务的拉通。

### 3. 企业上网

CPE 作为企业出口网关,可直接与城域网基于 IPv6 互通,满足本地上网需求,如需对上网业务进行精细化控制,也可将上网流量统一引导至城域网 PoP GW。

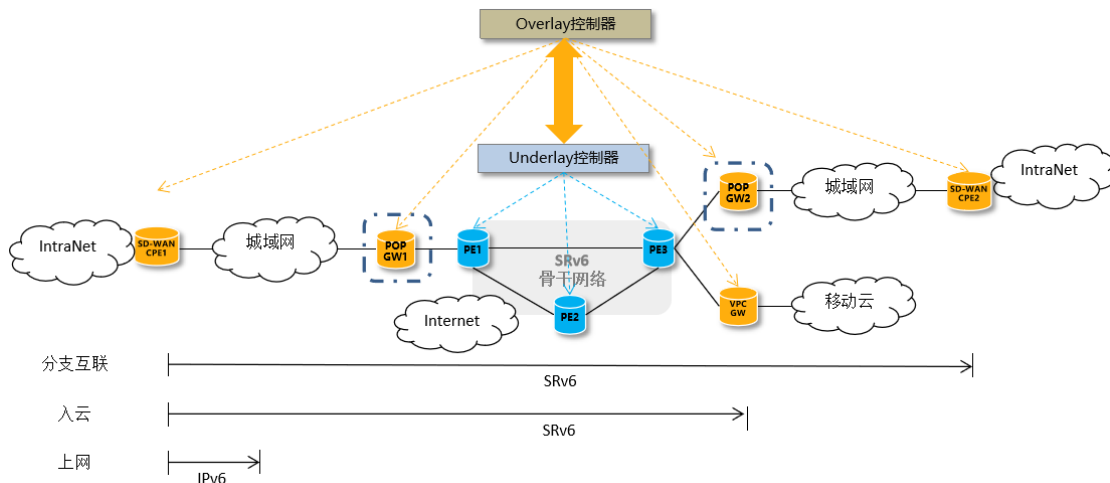


图 3.2 大型企业业务承载方案

#### 3.2.2 中小微型企业场景

在中小微型企业的解决方案中,企业内部不需要多租户隔离, PoP GW 作为共享的业务控制点, SD-WAN 控制器需要控制 CPE 和 PoP GW, 并基于 SRv6 控制器提供的 BSID 实现 CPE 之间的动态路径选择等功能。这种解决方案的优点是运营商可对用户的流量进行更加精细化的管控,从而匹配最佳的差异化服务和无缝的增值业务。该组网模型下三种业务类型承载方案如下:

##### 1. 分支互联业务

SRv6 隧道从企业分支的一端 CPE1 开始, 结束在近端的 PoP GW1, 业务在 PoP GW1 落地, 并进行不同用户的 VPN 隔离, 然后封装第二段 SRv6 隧道到 PoP GW2 并落地, 最后由 PoP GW2 转发到 CPE2。

##### 2. 入云业务

企业租用运营商或者第三方公有云业务, 在云端部署 VPC GW, SRv6 隧道从企业端 CPE1 开始, 结束在近端 PoP GW1, 然后继续第二段 SRv6 隧道, 结束在云端的 VPC GW, 实现企业上云业务的承载。

和大型企业一样, 随着运营商云网一体的逐步推进, 后期 VPC GW 可逐渐与云 PE 融合, 通过 SD-WAN 控制器与骨干网控制器、云管控平台联动, 实现端到端

入云业务的拉通。

### 3. 企业上网

CPE 作为企业出口网关,可直接与城域网基于 IPv6 互通,满足本地上网需求,如需对上网业务进行精细化控制,也可将上网流量统一引导至城域网 PoP GW。

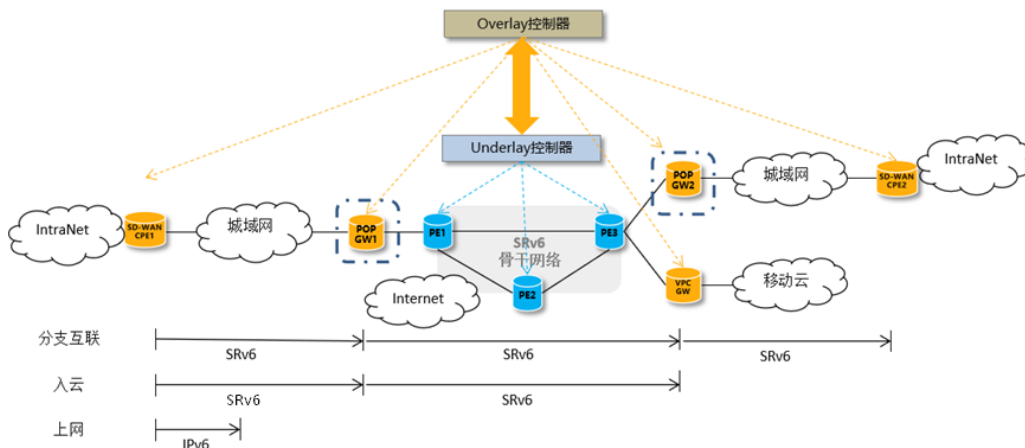


图 3.3 中小微型企业业务承载方案

下面以分支互联业务为例,对具体承载方案进行详述。对于第一段 CPE1 到 PoP GW1 的 SRv6 路径, SRv6 隧道封装的源地址为 CPE1,目的地址为 PoP GW1 的声明为 SID 的公网 IPv6 地址。由于 CPE1 收到的是用户的私网地址,因此 CPE1 上部署了 VPN 业务。在此解决方案中,第一段 SRv6 隧道终止于 PoP GW1,并从 PoP GW1 从新入第二段 SRv6 隧道,因此 PoP GW1 也需要部署 VPN,学习对应的私网路由。

在 SD-WAN 场景中,从 CPE 到 PoP GW1 的方式可以有多种,比如基于 Internet、4G 或者 5G 上联。因此此处只需要保证从 CPE 到 PoP GW1 IPv6 可达即可。一般情况下, PoP GW1 部署在云化的数据中心的,如边缘云数据中心的。因此需要通过 SD-WAN 控制器在 CPE 上配置到 PoP GW1 的 SRv6 BE 隧道。

第二段 SRv6 路径的起点为 PoP GW1,终点为对端的 PoP GW2,其穿越了一个或者多个 SRv6 域。为了实现 SD-WAN 选路和跨域, PE 节点,也即 SRv6 骨干网的边缘节点,需要骨干网的路径以 SID 列表或 BSID 的形式对外提供差异化服务。因此在 PoP GW1 上, PoP GW1 可以基于私网路由查询数据包的下一跳,也即对应的 PoP GW2 的 VPN SID,并匹配到不同的骨干网 TE 路径。PoP GW1 将私网数据包封装上 SRv6 外层封装,并携带对应的骨干网路径 SID 和 PoP GW2 的 VPN SID,将数据包发送给 SRv6 域的入口 PE。在 PE 处,如果是 BSID 则根据 SRv6 Policy

使用指定路径将数据包转发到对应 PoP GW2, 并进行解封装操作。至此第二段 SRv6 路径结束。

第三段 SRv6 路径的起点在 PoP GW2, 终点在 CPE2。PoP GW2 节点在解封装得到私网数据包之后, 根据私网数据包的目的地址查询 VPN 路由, 得到对应的路由下一跳为 CPE2 的 SID, 并将私网数据包封装一层外层的 SRv6 BE 封装, 其目的地址为 CPE2 SID, 发送给 CPE2。与第一段 SRv6 路径类似, 这段 SRv6 BE 路径可以通过多种方式到达 CPE, 只需要保证 IPv6 可达即可。

综上所述, 在这个解决方案中, 主要由三段 SRv6 路径组成。每一段路径之间通过 Option A, 也即 VRF-TO-VRF 的方式来连接。因此 PoP GW 和 CPE 都需要学习到私网路由。

### 3.2.3 企业混合场景

针对不同企业的组网需求, 可灵活选择以上描述的上网、入云和分支互联的承载方案, 不同承载方案可混用, 以满足企业多变的网络需求。

## 3.3 控制和转发原理

SD-WAN 控制器计算端到端路径, 可以分为本端接入段 (CPE 到 PoP GW1), 本端汇聚段 (PoP GW1 到 PE1), 骨干段 (PE1 到 PE3), 远端汇聚段 (PE3 到 PoP GW2), 远端接入段 (PoP GW2 到 CPE2) 等多段路径。接入段采用 Overlay 方式的连接, 骨干段为提升网络质量需要和 Underlay 协同。根据应用场景不同, 以下分别对大企业场景中流量经过 POP GW、不经过 POP GW 两种方案以及中小微企业流量过 POP GW 方案进行介绍。

### 3.3.1 大企业场景

在大企业场景中, VPN 功能在 CPE 实现以对不同部门机构进行隔离。以流量是否经过 POP GW 区分, 可以分为两种方案。两种方案的控制面和转发面机制基本相同, 差别在于 SID List 是否包含 POP GW 的 SID。

### 3.3.1.1 流量经过 POP GW 方案

这种方案适合 Underlay 转发路径可变更，以及需要隐藏 Underlay 路径信息的场景。端到端隧道中骨干段（PE 到 PE）的路径计算中，不同应用对网络质量有不同的要求，因此流量需不同质量的路径承载。SD-WAN 控制器向骨干段的 Underlay 控制器发起路径请求，Underlay 控制器计算骨干段的网络连接，并用 SRv6 BSID 封装后返回 SD-WAN 控制器。SD-WAN 控制器然后向 CPE 下发对应的 SRv6 Policy，其中包括 CPE、PoP GW 的 SID，PE 间的路径 BSID，远端 PoP GW 的 SID 以及 VPN SID 等。这种模式中流量在经过 Underlay PE 路由器时，BSID 会以隧道方式展开，封装到报文头中，骨干网节点 SID 不对外暴露。

该模式下控制面建立转发路径的过程如下：

- ① Overlay 控制器算路：根据应用需求确定 Overlay 源、目的、SLA 需求，同时通过路径计算得到端到端路径，分为 CPE1 到 PoP GW1，PoP GW1 到 PoP GW2，以及 PoP GW2 到 CPE2 等几段；
- ② Overlay 控制器根据 PoP GW 确定 Underlay 入、出口 PE 后向 Underlay 控制器发出路径请求，参数有 Underlay {入口、出口、SLA 需求}；
- ③ Underlay 控制器计算出一条路径 SR Policy，以 BSID 直接返回 Overlay 控制器；
- ④ Overlay 控制器把 Overlay 和 Underlay 路径拼接为 SR Policy {PoP GW1, BSID, PoP GW2, CPE2}，下发 CPE1。至此，转发面端到端路径建立完成。

该模式下转发面的报文转发流程如下图所示，需特别指出的是，PE 采用 END.B6.ENCAP 操作将 BSID 展开为骨干网 SR Policy，封装在新的 SRH 中，同时添加新 IPv6 头部。

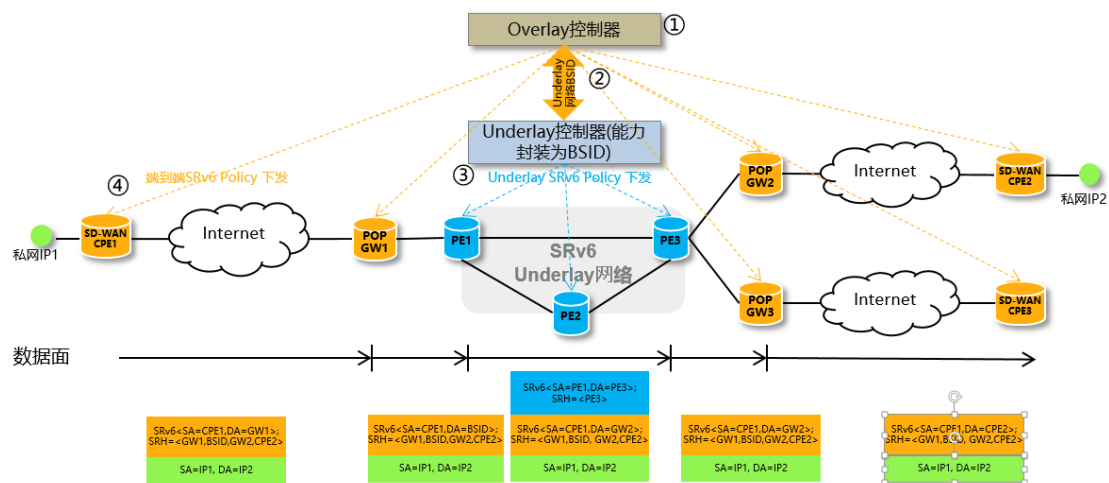


图 3.4 大企业场景流量经过 POP GW 示意图

在这种方案里，流量会经过 POP GW，因此运营商可以在 POP GW 为 SD-WAN 流量提供增值服务；另外有 PoP GW 可以缩短 CPE 和网络接入点的距离，对服务质量有要求的业务可以选择此方案。

### 3.3.1.2 流量不经过 POP GW 方案

此方案整体和流量经过 POP GW 的方案流程一致，区别在于下发的 SID list 中不包含 POP GW 的 SID。该模式下控制面建立转发路径的过程如下：

- ① Overlay 控制器算路：根据应用需求确定 Overlay 源、目的、SLA 需求。
- ② Overlay 控制器确定 CPE 到 Underlay 入、出口 PE 后向 Underlay 控制器发出路径请求，参数有 Underlay {入口、出口、SLA 需求}；
- ③ Underlay 控制器计算出一条路径 SR Policy，以 BSID 直接返回 Overlay 控制器；
- ④ Overlay 控制器把 Overlay 和 Underlay 路径拼接为 SR Policy {BSID, CPE2}，下发 CPE1。至此，转发面端到端路径建立完成。

该模式下转发面的报文转发流程如上图所示，需特别指出的是，PE 采用 END.B6.ENCAP 操作将 BSID 展开为骨干网 SR Policy，封装在新的 SRH 中，同时添加新 IPv6 头部。

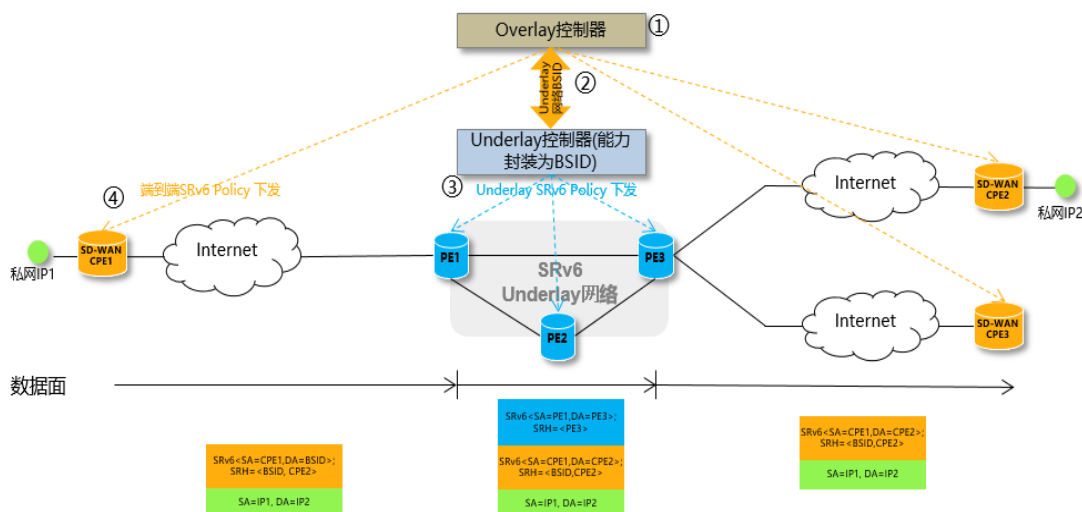


图 3.5 大企业场景流量不经过 POP GW 示意图

这种方案无需 POP GW, 并且可以具备 Underlay 协同的能力, 网络架构简单、部署便捷。

### 3.3.2 中小微企业场景

在中小微企业场景中, POP GW 需要感知 VPN 私网路由, 因此流量必须要经过 POP GW。因此在这个场景中, 只有一种方案选项。

与大企业场景一样, Underlay 路径通过 BSID 来描述, 从而支持 Underlay 转发灵活变更以及隐藏 Underlay 路径信息。而从 CPE 到 POP GW 的这段网络只需 IP 可达即可 (以下以 IPv6 可达为例)。CPE 只需将 POP GW 发布的 VPN SID 写入到外层隧道封装的 IPv6 目的地址即可支持将 VPN 流量按照最短路径转发到 POP GW。具体端到端算路步骤如下:

- ① Overlay 控制器算路: 根据应用需求确定 Overlay 源、目的、SLA 需求, 同时通过路径计算得到端到端路径, 分为 CPE1 到 PoP GW1, PoP GW1 到 PoP GW2, 以及 PoP GW2 到 CPE2 等几段;
- ② Overlay 控制器根据 PoP GW 确定 Underlay 入、出口 PE 后向 Underlay 控制器发出路径请求, 参数有 Underlay {入口、出口、SLA 需求};
- ③ Underlay 控制器计算出一条路径 SR Policy, 以 BSID 直接返回 Overlay 控制器;
- ④ Overlay 控制器把 Overlay 和 Underlay 路径拼接为 SR Policy {BSID, PoP GW2}, 下发到 POP GW1。



⑤ CPE1 到 POP GW1、POP GW2 到 CPE2 的隧道按照 VPN 关系创建。至此，转发面端到端路径建立完成。

该模式下转发面的报文转发流程如上图所示，需特别指出的是，PE 采用 END.B6.ENCAP 操作将 BSID 展开为骨干网 SR Policy，封装在新的 SRH 中，同时添加新 IPv6 头部。

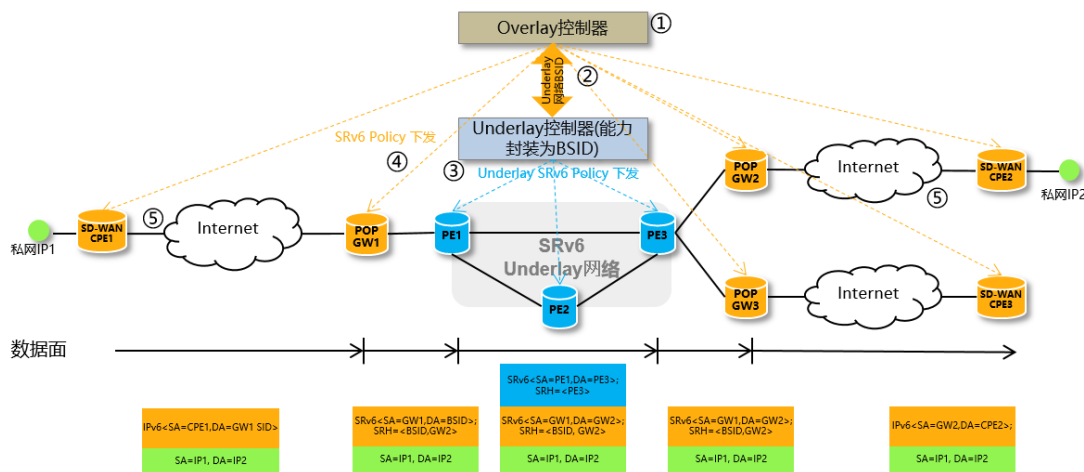


图 3.6 中小微企业场景流量经过 POP GW 示意图

在这种方案里，流量会经过 POP GW，因此运营商可以在 POP GW 为 SD-WAN 流量提供增值服务。

### 3.3.3 采用 G-SRv6

特别值得一提的是，由于 SD-WAN 业务经过的 Overlay 和 Underlay 路径通常较长，从而导致 SR Policy 的 SID List 过长。然而当前的 SRv6 在 SID 数目过多时可能会带来报文头过长的问题，影响了报文的转发效率，也限制了 SRv6 的大规模商用。因此在部署 SD-WAN 时，可以考虑基于开销更小，支持多种 SID 混合编程的 G-SRv6 进行 SRH 头压缩。G-SRv6 完全兼容 SRv6，在不改变 SRH 的情况下，通过定义一类新的压缩 SID 来支持更高效的传输，从而降低了 SRv6 对网络硬件的需求。当前中国移动正在推动 G-SRv6 的多厂商互通和 SRv6 的试点部署项目，后续将基于 G-SRv6 部署 SD-WAN。

G-SRv6 利用一个 SRv6 网络中很多 SID 都具有共同前缀（Common Prefix），SID list 中去掉 SRv6 SID 中的 Common Prefix 部分和其他冗余部分，保留 Node ID 和 Function ID 作为压缩 SID，可以很好的减少报文头开销。下图描述了 G-SRv6 数据面部分的数据封装方式，G-SRH 与 SRH[RFC8754] 格式保持一致，没有对其格式和字段语义进行改动，兼容但支持将 128bit SRv6 SID 和 32bit G-SID 混合编程在 G-SRH 中。为方便实现 G-SID 和完整 SID 混编并确保 128bit 对齐，引入 G-SID Container 概念。为标识当前 G-SID 在 Container 中的位置，定义 SI(SID Index)。最后定义了 CoC flavor 标识 G-SID，当收到 SID 有 CoC flavor 时，需把 SID 更新到 IPv6 DA 地址的 G-SID 部分。

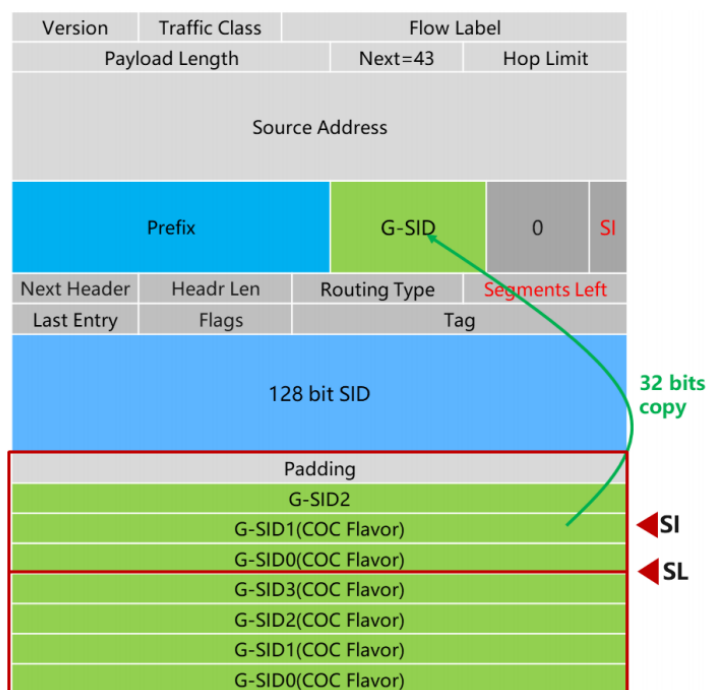


图 3.6 G-SRv6 原理示意图

## 4 弹性 SD-WAN 的方案亮点

### 4.1 Underlay 协同能力

接入段是 CPE 和 PoP GW 之间的网络，CPE 是 Underlay 资源调度的端点。CPE 上感知业务，因此可以实现精细的流量调度。在大企业场景中，CPE 具有 SRv6 能力，还可以根据业务需求压入端到端的 SRv6 Policy。

骨干段是 PoP GW 之间的网络，在这段网络中，Underlay 网络协同是重点。PoP GW 之间的路径连同业务链以及 Underlay 网络 SR Policy 一起可以组成一个包含增值业务以及指定网络路径的服务，实现 Overlay 和 Underlay 的协同。

## 4.2 IPv6 原生业务链

增值业务涉及到流量的清洗、加速、加密等处理。弹性 SD-WAN 的业务链需要各个增值业务的功能支持 SRv6，这带来几个好处：1) 增值业务可以按需组合，流量可以按照 SRv6 指定的路径顺序流过各个虚拟化功能；2) 按需启用增值业务，不需要增值业务的报文不会在 SR Policy 中压入虚拟化功能地址；3) 虚拟化的增值业务便于功能的快速迭代和演进，使运营商管道增值，向服务化演进。

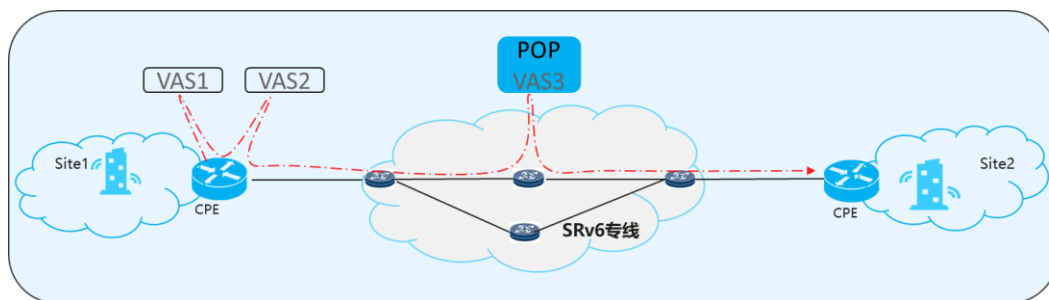


图 4.1 基于应用信息的 SFC 策略

特定类型的应用流量有增值服务的需求，例如应用加速、流量清洗等。提供增值服务的 VAS 具有不同的设备形态，并部署在 SD-WAN 网络中的不同位置。如图 3 所示，VAS1 与 VAS2 以 VM 形态部署在 uCPE 中，VAS3 以物理设备形态部署在 SRv6 专线网络的 PoP GW。CPE 可以基于应用信息选择对应的 SFC 策略，将形态不同、部署位置不同的 VAS 灵活组织，为应用提供特性化服务。

## 4.3 Telemetry

Telemetry 是一项远程的从物理设备或虚拟设备上高速采集数据的技术。设备通过推模式（Push Mode）周期性的主动向采集器上送设备的接口流量统计、CPU 或内存数据等信息，相对传统拉模式（Pull Mode）的一问一答式交互，提供了更实时更高速的数据采集功能，使得控制器可以接近实时的感知网络状态，针对网络突发时间随时做出响应。

## 4.4 应用感知能力

传统 SD-WAN 实现应用感知路由的方式依赖于网络节点（如 CPE 等）实现 DPI 功能，而弹性 SD-WAN 提供了潜在的原生应用感知路由能力。在弹性 SD-WAN 中，可以根据报文中 IPv6 可扩展头的可编程空间携带应用信息，可以根据 DNS 域名、DPI 等识别应用信息，网络设备根据这些应用信息将数据报文映射到相应的 SRv6 路径实现 SLA 保障。存在如下场景：

### 1. 基于应用信息选择 WAN 网络平面

当 CPE 接收到带有应用信息的数据报文时，根据应用类型将流量转发至不同的 WAN 网络平面，如对时延敏感的视频会议应用流量转发至 SRv6 专线网络。在 CPE 将视频会议流量转发满足低时延要求的 SRv6 路径。在 SRv6 路径中，中间节点根据策略将视频会议应用报文分配至高优先级队列。

### 2. 基于应用信息企业上云

当企业有应用上云的需求时，CPE 可以基于应用信息与云位置信息选择对应的网络平面，并在网络平面内选择满足上云应用需求的路径。

### 3. 基于应用信息的企业数据处理

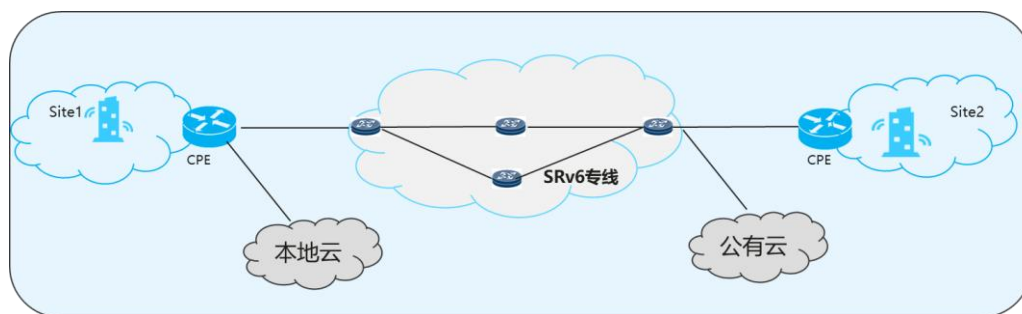


图 4.2 基于应用信息的企业数据处理

企业内的数据有上云处理的需求，SD-WAN 客户希望涉及企业信息安全的数据在本地云处理，其他的数据上公有云处理。CPE 可以基于应用信息中的信息安全标识，将数据处理应用流量转发至不同的云。

## 5 测试验证

测试验证场景包含两个方面。第一，基本功能验证，验证端到端弹性 SD-WAN

转发。如下图所示，CPE 和 PoP GW 虚拟路由器组成一张 Overlay 网络，采用 SRv6 隧道转发。其中，CPE1、PoP GW1 及 CPE2 建立一条 SRv6 隧道，路径为 CPE1、PoP GW1 和 CPE2。第二，服务器性能验证，对服务器基于 FPGA 加速的 SRv6 转发的能力进行验证。测试环境由一台 Intel x86 架构服务器、两台运行 Linux 4.18 内核的白盒 CPE<sup>1</sup>及一台测试仪组成。其中服务器安装一张网卡<sup>2</sup>提供 SRv6 硬件加速功能，运行 DPDK+VPP 协议栈用于 SRv6 软件转发功能。

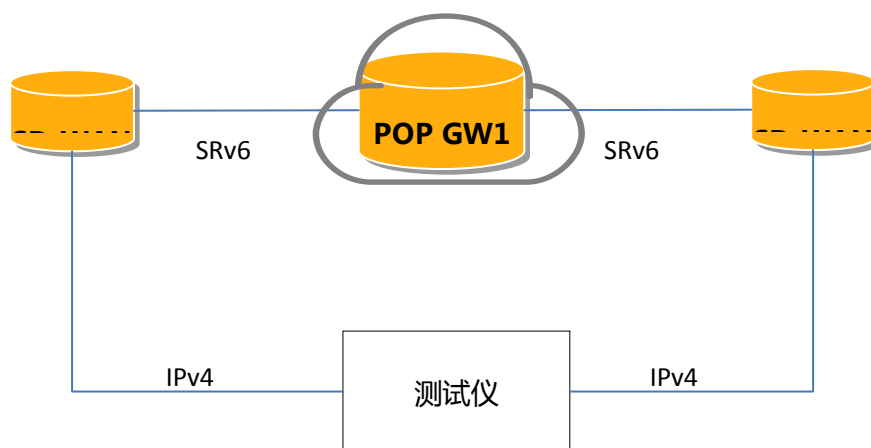


图 4.3 概念验证场景

首先，测试验证了弹性 SD-WAN 的基本功能，流量 SRv6 端到端以及通过 Linux 以及利用 FPGA 硬件加速 SRv6 转发工作正常。其次验证了 FPGA 加速的服务器占用 4 核即可实现 40Gbps 转发的性能，而在 CPU 的转发的情况下需要占用 12 核。

未来将进一步基于 SRv6 能力研究业务链功能，利用统一的 SRv6 技术探索 SD-WAN 融合云、网能力关键技术。

## 6 总结

随着 IPv6 在我国的加速部署，SRv6 的快速部署已成为大势所趋。中国移动充分认识到把 SRv6 的网络供给侧能力和 SD-WAN 的应用侧需求结合带来得巨大价值。通过携手华为、烽火、Intel、ARM、中兴、华辰连科、HCL 等厂商，结合方案制定和测试验证共同推动弹性 SD-WAN 方案的成熟。弹性 SD-WAN 的关键在于 CPE 和服务侧的能力，通过测试初步验证了用 CPE 和服务侧进行 SD-WAN 组网

<sup>1</sup> 白盒 CPE 为山东华辰连科 VN1001B

<sup>2</sup> 智能网卡为 Intel N3000，运行 HCL FPGA 加速程序

的基本功能。未来计划在可靠性、OAM 等方面开展进一步研究。

未来网络将会是一个能力开放的网络，业务创新将基于网络和云基础设施的能力整合。弹性 SD-WAN 一方面将在 Overlay 的视角整合端、边、云、网资源，使得云、网资源得以协同体现除最大价值；另一方面为应用开放能力，通过为应用提供端到端的云网融合产品为广域网络提供新动能。

## 缩略语列表

缩略语	英文全名	中文解释
AS	Autonomous System	自治系统
BGP	Border Gateway Protocol	边界网关协议
BSID	Binding Segment ID	绑定段标识
CPE	Customer Premise Equipment	客户侧设备
CoC	Continue of Compression	继续压缩
DC	Data Center	数据中心
DPDK	Data Plane Development Kit	数据平面开发套件
DPI	Deep Packet Inspection	深度报文检测
FEC	Forward Error Correction	前向纠错
GRE	Generic Routing Encapsulation	通用路由封装协议
GW	Gateway	网关
IGP	Interior Gateway Protocol	内部网关协议
INT	Inband Network Telemetry	带内网络遥测
LDP	Label Distribution Protocol	标签分发协议
MPLS	Multi-Protocol Label Switching	多协议标签交换
NFV	Network Functions Virtualization	网络功能虚拟化
OAM	Operation Administration and Maintenance	操作维护管理
PE	Provider Edge	运营商边缘路由器
PoP	Point of Presence	入网点
QoS	Quality of Service	服务质量
RSVP	Resource ReSerVation Protocol	资源预留协议
SDN	Software Defined Network	软件定义网络
SID	Segment ID	段标识
SLA	Service-Level Agreement	服务等级协定
SR	Source Packet Routing in Networking	基于分组报文的源路由
SRH	Segment Routing Header	段路由头
TE	Traffic Engineering	流量工程
TLV	Type Length Value	类型长度值
TWAMP	Two-Way Active Measurement Protocol	双向主动测量协议
VNF	Virtual Network Function	虚拟网络功能
VPN	Virtual Private Network	虚拟私有网

VPP	Vector Packet Processor	向量报文处理
WAN	Wide Area Network	广域网



## 参考文献

- [1] 中国移动 G-SRv6 技术白皮书, 中国移动, 2020
- [2] 中国移动 SRv6 头压缩优化方案, 中国移动, 2020
- [3] draft-cl-spring-generalized-srv6-for-cmpr-01, IETF, 2020
- [4] RFC8754, IETF, 2020
- [5] draft-ietf-spring-srv6-network-programming-16, IETF, 2020