SRv6技术与产业白皮书

（2019版）

推进IPv6规模部署专家委员会

2019年12月

目录

前 言

2017年11月，中共中央办公厅、国务院办公厅印发了《推进互联网协议第六版(IPv6) 规模部署行动计划》(以下简称《行动计划》)。《行动计划》发布以来，政府部门、基础电信企业、互联网企业、通信设备与服务提供商、相关中央企业、事业单位、科研机构等积极响应，纷纷制定具体的落地实施方案和工作计划，加快IPv6升级改造。

我们必须认识到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。在互联网发展的历程上，数据通信产业经历了Native IP、MPLS两代协议。当前，为了满足5G和云服务的灵活组网、按需服务、差异化保障等需求，SRv6成为下一代互联网演进的主流技术路线。因此，依托我国IPv6规模部署进展成果，整合IPv6相关产业链力量，加强基于IPv6下一代互联网技术体系创新，从网络路由协议、管理自动化、智能化及安全等方向积极开展IPv6+网络新技术（包括SRv6、VPN+、 Detnet、BIER6、SFC和OAM等）创新研究、试验验证、应用示范，不断完善IPv6技术标准体系，将有力提升我国在下一代互联网领域的国际竞争力。

为此，“推进IPv6规模部署专家委员会”IPv6+技术创新工作组组织编写了《SRv6技术与产业白皮书》-2019版。本白皮书力求从需求、技术、产业和应用等多维度呈现SRv6技术和产业发展状况，为持续推进IPv6+技术创新和产业实践提供支撑。本次白皮书编制得到了中国信息通信研究院、中国电信、中国移动、中国联通、华为、天融信等诸多工作组成员单位的大力支持和协作，在此一并表示感谢！

1.为什么需要SRv6

1.1.当前网络面临的挑战

随着企业信息化建设的深入、移动互联网和云数据中心的发展，社会走向全面数字化和智能化。传统只能提供有限电信级连接的网络已经无法满足以云为中心的业务对网络海量的、随时随地可能发起的数据连接的要求。未来网络应当满足以下要求：

1、海量连接扩展能力

信息自动化、IoT等业务发展，要求网络的连接数量可以无限扩展。除了带宽，网络中应尽量减少其他与业务相关的限制。未来网络应当在带宽能够满足的情况下，可以任意发展业务，减少业务对网络能力的感知。

2、业务任意接入、任意连接能力

传统的电信网络严格限制了业务接入点，在全面数字化的时代，业务接入点不可控。网络需要满足业务任意点接入，跨越任意区域连接的能力。

3、差异化服务能力

传统的电信网络为用户提供了无差异的连接服务，导致对网络质量要求不高的业务获得了过高的服务，造成资源浪费，而一些有特别质量要求的业务却难以保证。未来的网络应当由业务根据需求选择网络质量，既节省资源，又保障业务。

4、端到端的可靠性需求

为了保证可靠性，网络中往往部署了快速检测和倒换技术。但这些技术在网络规模较大，节点间距离较远的情况下不能很好的工作——比如受光纤中光信号200KM/ms传输速度影响，端端检测无法及时发现故障（比如北京到广州需要100ms以上才能发现故障）保护无法满足质量要求，局部检测配合局部保护部署方案又非常复杂。因此提供距离无关的端到端可靠性方案也是未来网络应当具备的能力。

1.2.什么是SRv6

Segment Routing（SR）是一种源路由技术。它为每个节点或链路分配Segment，头节点把这些Segment组合起来形成Segment序列（Segment路径），指引报文按照Segment序列进行转发，从而实现网络的编程能力。

Segment Routing有如下四个优点：

1.简化了控制协议。它只采用IGP，统一了控制协议，不再像MPLS那样在IGP的基础还要LDP、RSVP-TE等协议，降低了运维的复杂度。

2.良好的扩展性。以前实现路径编程（流量工程，TE）时一般采用RSVP-TE，网络中的每个节点都要感知到每条路径的状态，协议的消耗很大，限制了TE隧道的规格，难以部署和维护。Segment Routing路径编程则是在头结点进行，海量的路径都是依赖于有限的表示链路和节点的Segment的组合，网络中间节点几乎不感知路径状态，具备很高的扩展性。

3.可编程性好。Segment Routing中的Segment非常类似于计算机的指令，通过对Segment的编排可以实现类似于计算机指令的功能。具备非常好的灵活性，可以非常灵活地建立满足不同需求的路径，释放网络的价值。

4.更可靠的保护。Segment Routing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，能够在高可扩展性的前提下，又可以达到完全的可靠性保护。

Segment Routing转发层有两种封装格式，一种是MPLS即SR MPLS，另一种是IPv6即SRv6。SRv6不仅继承了SR的优点，还具备标签空间数量无限、全网唯一、任意点可达的优点（IPv6地址特点）。进而可以实现只要地址可达，可以任意点接入，任意点之间互联。SRv6具有的独特优势，使其成为下一代IP网络的核心技术，成为业界研究的热点。

2.SRv6技术/Usecase

2.1.SRv6基本原理

SRv6采用长度为128bit的Segment定义网络功能，然后通过对Segment进行排列就可以实现网络设备的一系列转发、处理行为，从而完成业务编排。

2.1.1.网络指令：SRv6 Segment

在设计SRv6网络编程的时候，需要定义网络指令——SRv6 Segment。SRv6 Segment的标识称为SRv6 SID 。SRv6 SID是一个128 bit的值，每个SRv6 SID就是一条网络指令，它通常由三部分组成：

1.SRv6 SID 格式

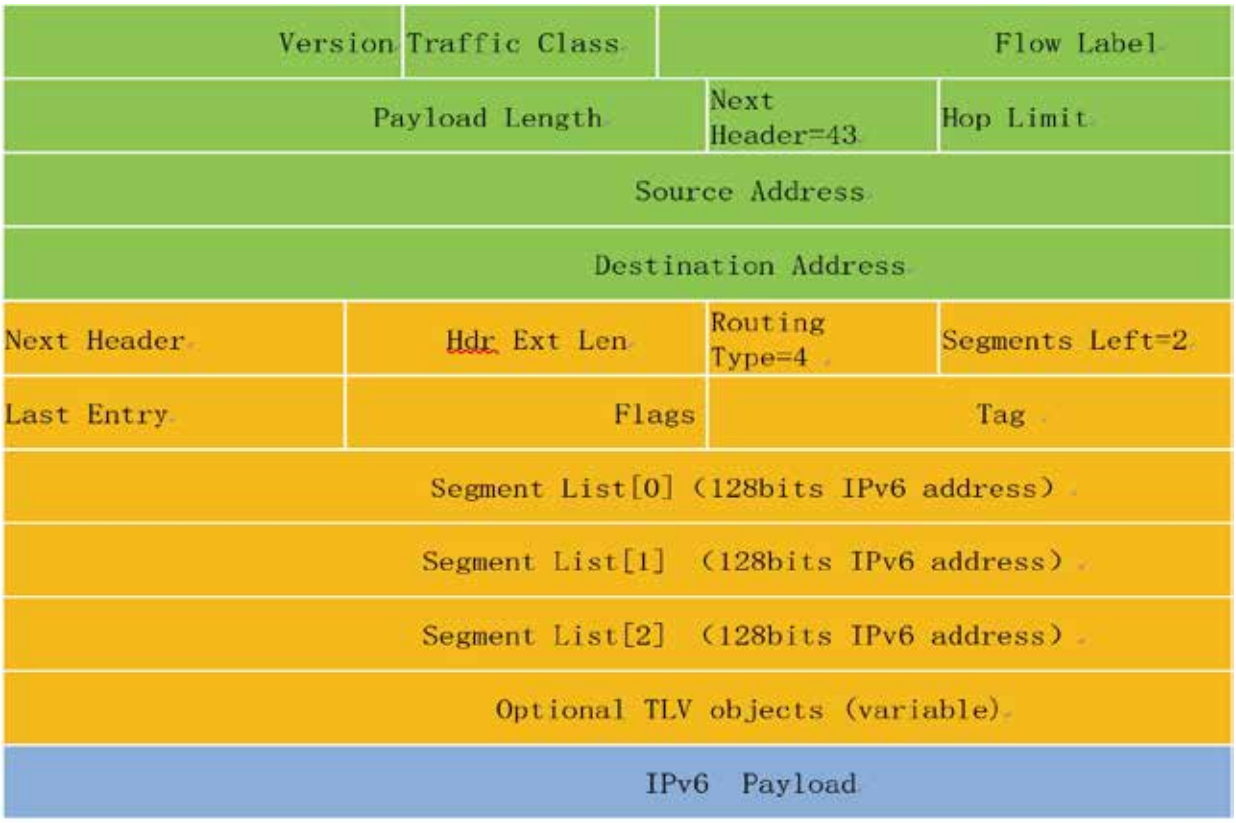
1. Locator:是分配给一个网络节点的标识，用于路由和转发数据包。在SRv6 SID中Locator是一个可变长的部分，用于适配不同规模的网络。

2. 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。

3. Argu是指令在执行的时候所需要的参数。这些参数可能包含流，服务或任何其他相关的信息。例如：定义一个对网络报文进行报文分片的指令，就可以在Argu携带报文的分片长度。

2.1.2.SRv6扩展头设计

下面是基于IPv6的SRv6报文封装。棕色部分是为SRv6引入的扩展头Segment Routing Header（SRH），用于进行Segment的编程组合形成SRv6路径。



2.SRv6 SRH格式

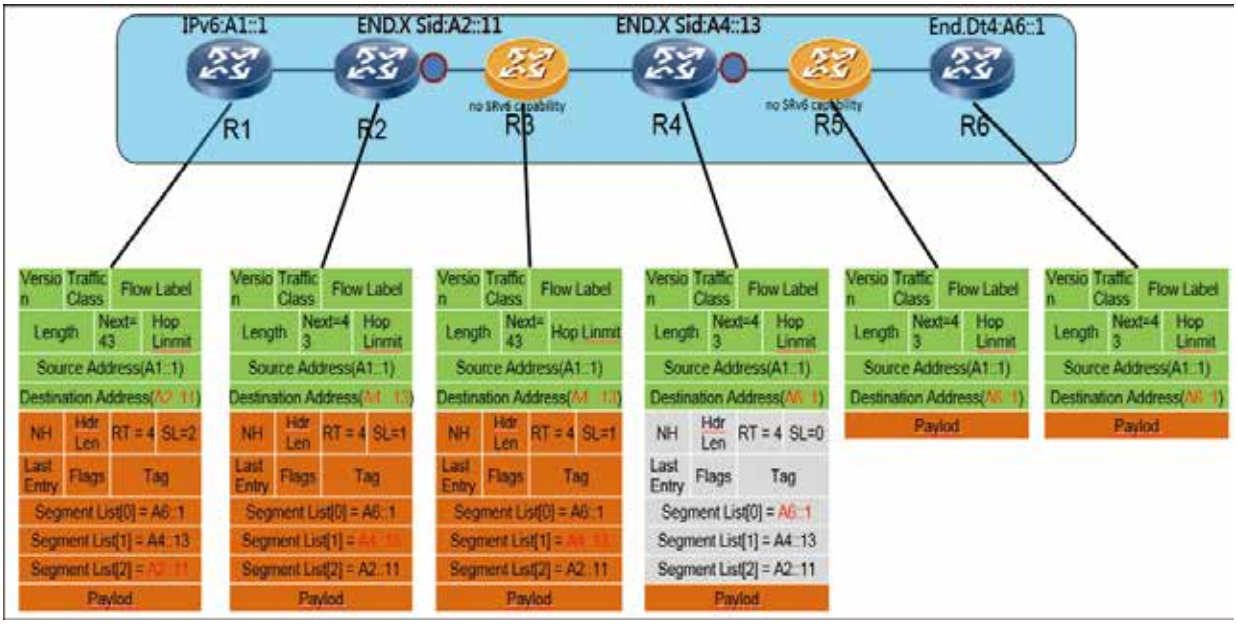
SRH的Routing Type为4。各字段解释如下：

字段名	长度	含义
Next Header	8比特	标识紧跟在SRH之后的报文头的类型。
Hdr Ext Len	8比特	SRH头的长度。主要是指从Segment List [0]到Segment List [n]所占用长度。
Routing Type	8比特	标识路由头部类型，SRH Type是4。
Segments Left	8比特	标识路由头部类型，SRH Type是4。
Last Entry	8比特	在段列表中包含段列表的最后一个元素的索引。
Flags	8比特	数据包的一些标识。
Tag	16比特	标识同组数据包。
Segment List[n]	128*n比特	段列表，段列表从路径的最后一段开始编码。Segment List是IPv6地址形式。
Optional TLV	variable	可变长TLV部分

表 21 SRH 报文头字段

SRH扩展头存储的内容相当于计算机的程序，这个程序就是解决业务在网络的端到端连接问题，Segment List[0]~ Segment List[N]相当于计算机程序。第一个要执行的指令是Segment List[N]，Segment　Left相当于计算机程序的PC指针，永远指向当前正在执行的指令，初始化为N，每执行完一个执行，SL--，指向下一条要执行的指令。通过这种模拟，SRv6转发过程可以用计算机程序执行过程来进行简单的模拟。

2.1.3.报文转发流程

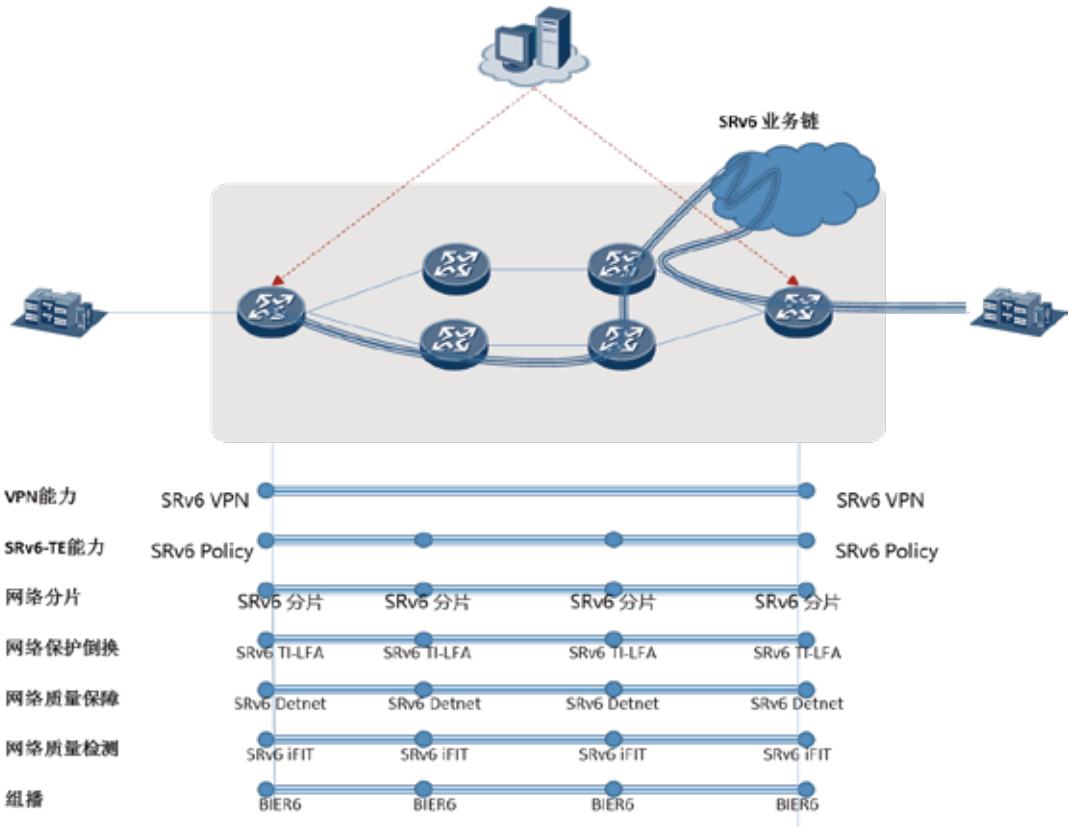


3.SRv6 报文转发流程示意图

如上图所示，结点R1要指定路径转发到R6，其中R1,R2,R4,R6为有SRv6能力的的设备，R3,R5为不支持SRv6的设备。

2.2.SRv6Usecase

SRv6的整体架构如下，总共包含9个方面的内容，分别是SRv6 Policy（SRv6 TE能力）、SRv6可靠性方案、SRv6　VPN能力、SRv6网络分片、SRv6业务链、SRv6质量保障（Detnet）、SRv6质量检测、SRv6组播、SRv6业务链，以及逐条应用感知能力APP-Aware IPv6。



4.SRv6 Usecase全景图

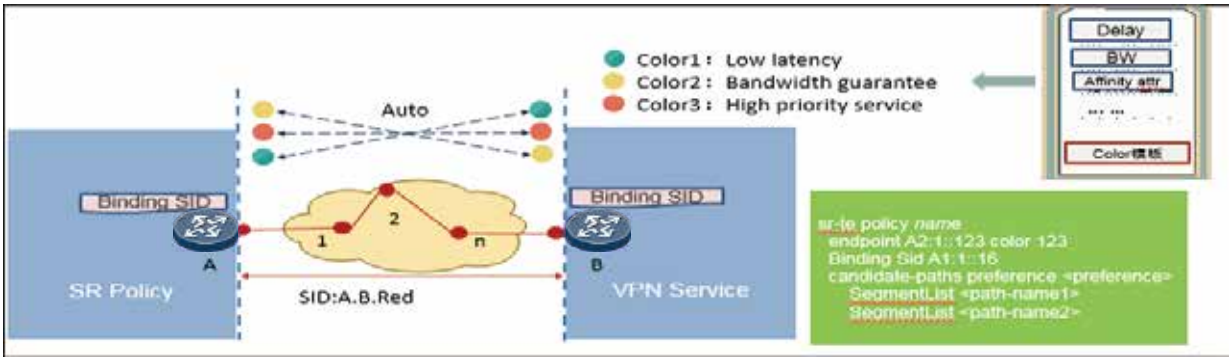
2.2.1.SRv6 Policy

SRv6在Native IPv6的基础上，融合了Segment Routing的网络编程能力。Native IPv6保证了网络任意结点的可达性，SRv6的网络编程能力可以对路径编程以满足业务的SLA需求。SRv6 Policy就是SRv6流量工程技术。SRv6 Policy由下列三元组标示：

1.The head-end of the policy （SR Policy源节点）

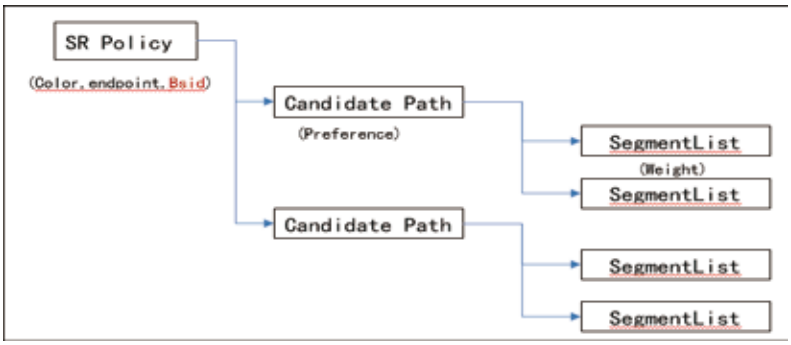
2.The endpoint (SR Policy的目的节点).

3.The color (颜色，用于标示该SRv6 Policy的意图).



5.SRv6 Policy 原理

颜色（Color）是SRv6 Policy非常重要的属性，它描述的是应用对网络的需求的模板。它可以使得业务在不关心网络配置细节的情况下，就可以和SRv6 Policy进行关联。例如：有个多点连接的低时延业务，使用传统隧道接口网络运维人员需要查询任意连接的满足低时延需求的隧道接口，并把业务和隧道进行关联。而采用SRv6 Policy模型，只需要将业务路由标示出对应低时延的Color。业务就能自动关联相应的SRv6 Policy。查询复杂度由O（n2）降到O（n）。SRv6 Policy模型如下：



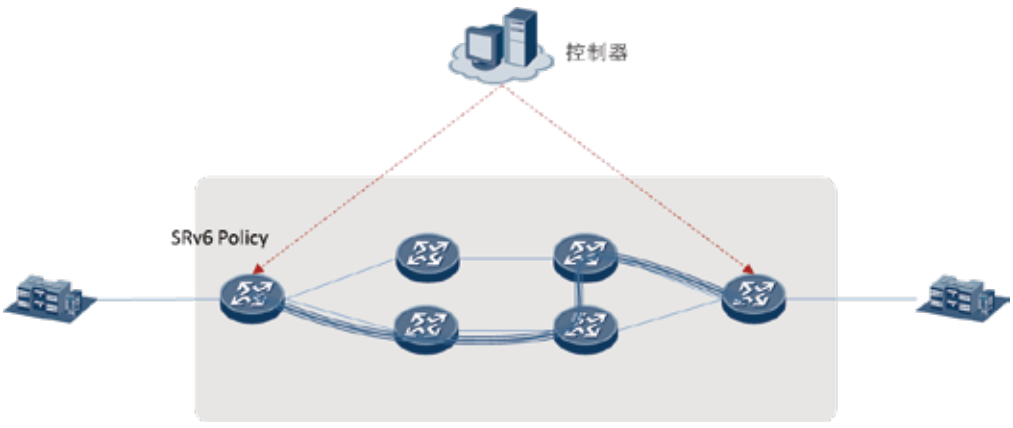
6.SRv6 policy模型

1.BSID: BSID是SRv6 Policy对外提供网络服务的接口。对应的转发行为是封装该SRv6 Policy对应的Segment List。也意味着只要报文封装该SID，就能将流量引导到该SRv6 Policy。

2.Candidate path：SRv6 Policy可以通过多种方式生成路径，静态配置，设备动态算路，控制器集中算路。不同的算路方式可以形成不同优先级的Candidate Path，这些Candidate Path可以形成冗余保护。Candidate Path封装在SRv6 Policy内部使得业务可以不用关心算路的来源，屏蔽了SRv6 Policy内部实现细节。

3.Segment List：标示发送流量到目的地址的源路由路径，每个Candidate path的不同的Segment List可以形成等值/非等值负载分担。调整Weight可以达到网络流量全局优化的效果。多路径还提供了网络路径资源scale-out能力。

SRv6 Policy结合性能检测，可以实时监控业务连接质量，配合控制器的路径闭环优化，提供实时满足业务需求的网络连接服务。



7.SRv6 Policy

2.2.2.SRv6 网络可靠性

一. 网络可靠性保护技术的挑战

传统网络依赖层次化的BFD部署保证端到端网络可靠性，这会导致如下问题：

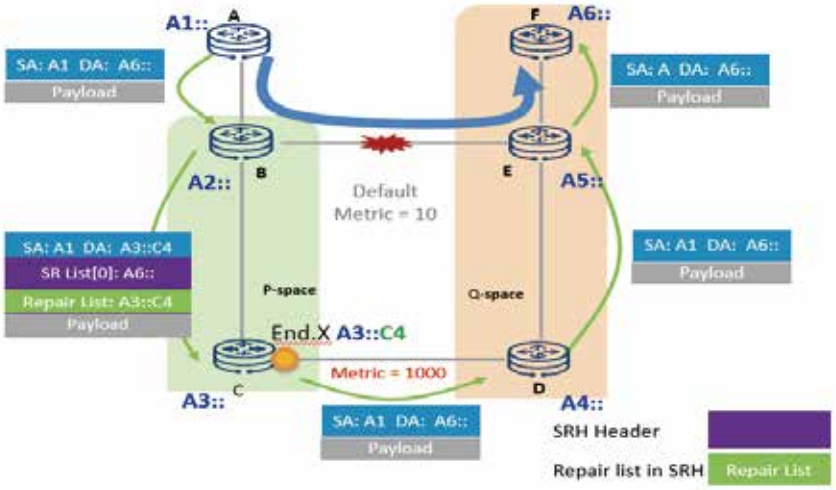
1.层次化BFD依赖不同的BFD发包间隔分层切换，无法满足50ms切换性能。

2.BFD容量限制会限制网络和业务部署。

3.部署复杂。

SRv6采用本地切换方案，不依赖多跳BFD，任意结点故障都采用本地FRR保护的方式。主要包含SRv6 Ti-LFA，SRv6 Midpoint保护，SRv6 防微环，从而实现端到端50ms保护。

二. SRv6 Ti-LFA



8.TI-LFA原理

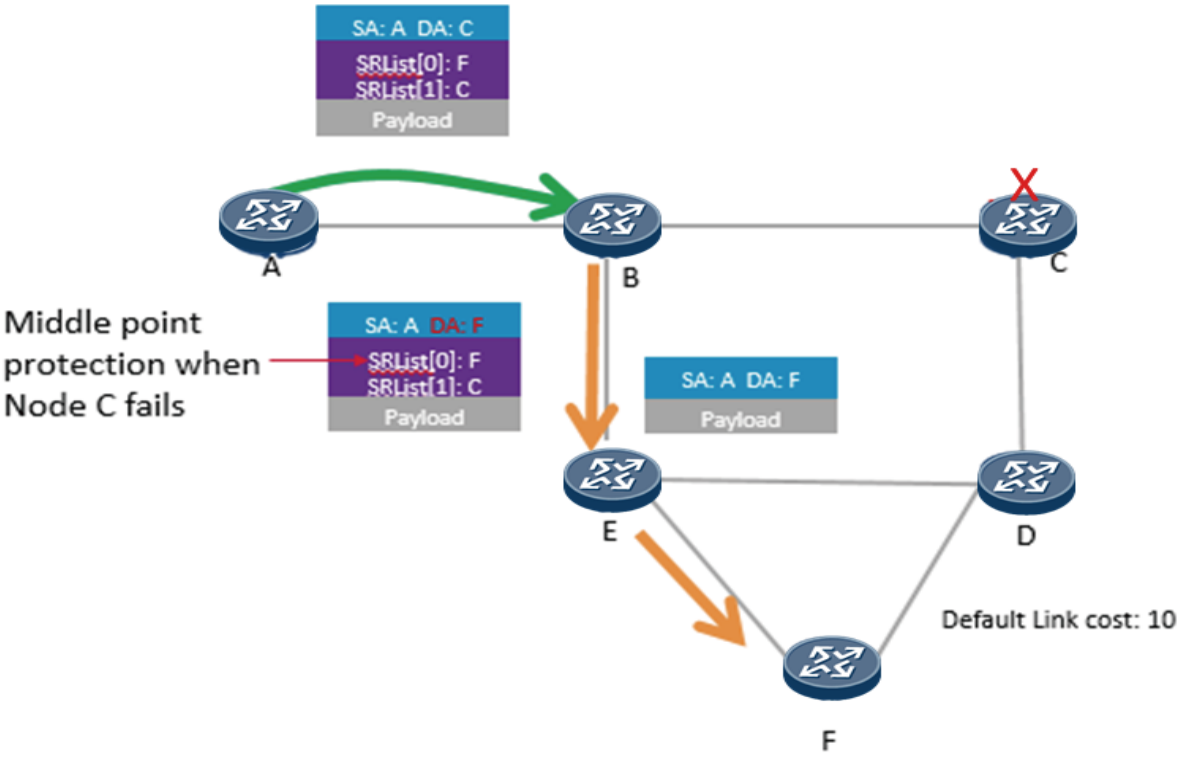
对于网络中每个目的地址，TI-LFA都会预先计算一个备份转发下一跳，当主一跳故障时，激活备份转发下一跳，从而修复节点的可达性。

三 . SRv6 Ti-LFA midpoint保护

SRv6 Ti-LFA midpoint保护用于SRv6 Policy指定结点故障的保护，Proxy Forwarding节点，感知到IPv6目的地址对应的下一跳接口故障的时候，且SRH的SL > 0，则执行Proxy Forwarding行为，代替Endpoint节点执行End行为，SRH的SL--，将Next SID拷贝到IPv6目的地址中，然后按照Next SID进行转发，从而实现了SRv6 Endpoint节点故障的保护。

下面我们举个例子来描述SRv6 Endpoint TI-LFA的保护过程。如下图所示，A->F的业务指定经过节点C。

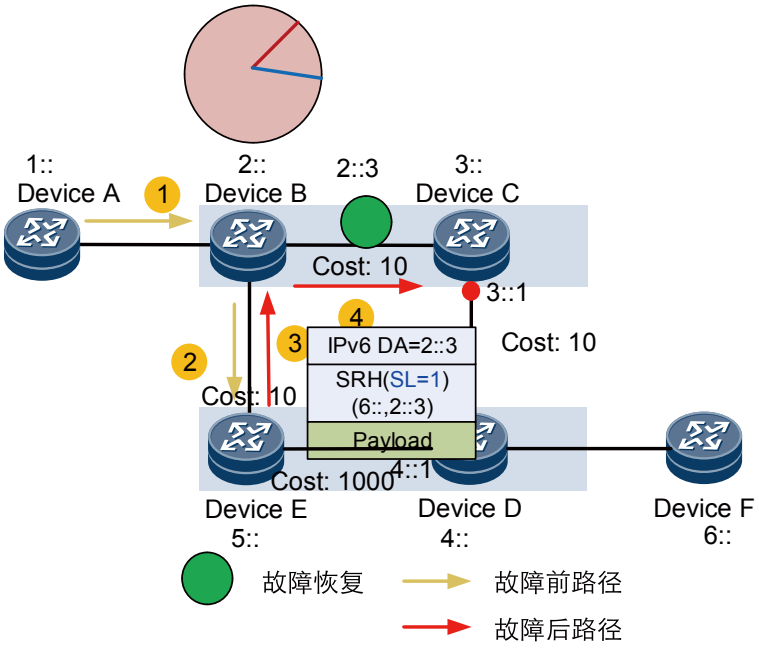
·节点C发生故障时，B感知到C的出接口故障，报文的目的地址C为B的直连邻居，且SRH的SL>0，节点B执行Proxy Forwarding操作。SL--，将Next SID F拷贝到IPv6目的地址中，由于SL已经减为0，则POP SRH，根据目的地址F转发。此场景中根据SPF计算，B到F的最短路径不经过C节点，因此流量可以经过B->E顺利到达F。



9.Middle Point 保护原理

以上，我们可以看到，使用SRv6 Endpoint TI-LFA技术，可以在SRv6 Policy中指定的节点/链路发生故障时，依然做到100%拓扑50ms保护。正是因为SRv6使用IPv6地址作为SID，且所有SID都可以全局寻址到达，使得Proxy Forwarding可以通过获取Next SID作为新的目的地址进行寻址，转发流量到备份路径上。

四. SRv6 防微环



10.SRv6防微环原理

Fast-Rerouting解决的问题是在控制面还没有完成收敛期间转发面有一条无环的备份路径可以指导转发，当网络中某些结点完成收敛，另外一些结点未完成收敛的时候，可能产生微环。所以，防微环解决的是网络收敛期间的环路问题，不管是正切还是回切，从网络中第一个结点开始收敛，到最后一个结点收敛结束，期间都可能产生微环。

SRv6防微环的收敛过程：

1.结点B和结点C的链路故障后恢复，结点E率先完成收敛。

2.结点E启动定时器T1，在收敛后路径插入结点B到C的邻接SID 2::3。

3.结点A将报文转发给结点B，由于结点B未完成收敛，依然按照图中路径2转发，转发给结点E。

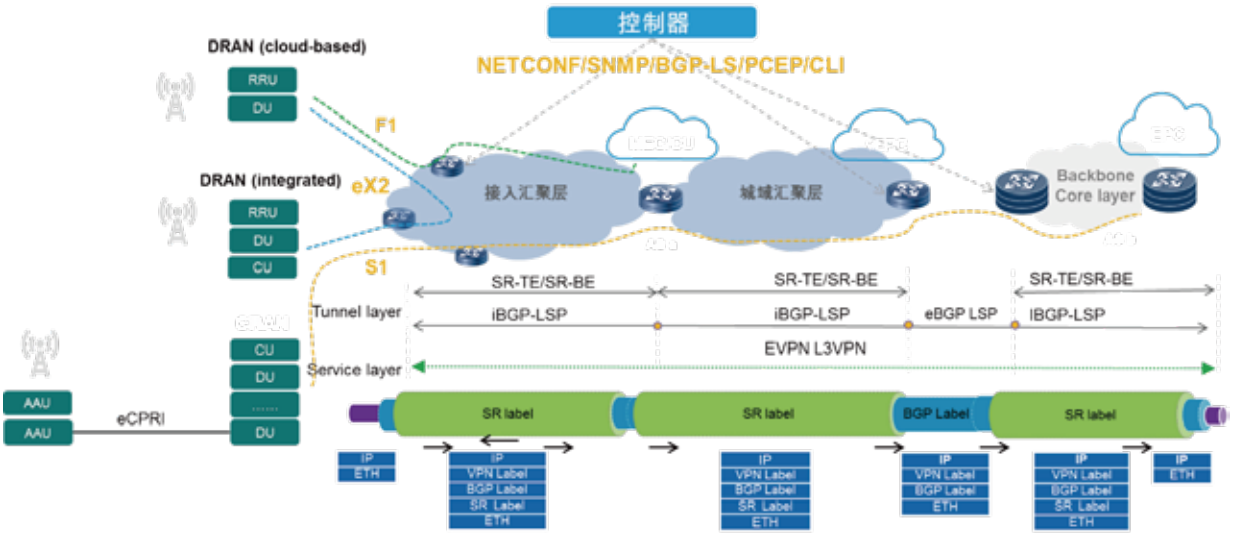
4.结点E根据计算的无环路径在报文插入结点B到C的邻接SID 2::3，并转发到结点B。(我们注意到报文在结点B和E来回了一次，但是由于在结点E修改了报文目的地址，所以不会成环)

5.结点B根据SID 2::3指令执行转发动作，沿着SID 2::3指定的出接口转发到结点C，并执行SL--，将外层IPv6头变更为6::。

6.结点C按最短路径转发到目的地址F

2.2.3.SRv6 VPN

VPN（虚拟专用网络)指的是在公用网络上建立专用网络的技术。VPN的基本原理是利用隧道技术，把VPN报文封装在隧道中，建立专用数据传输通道，实现报文的透明传输。



11.传统VPN和SRv6 VPN对比

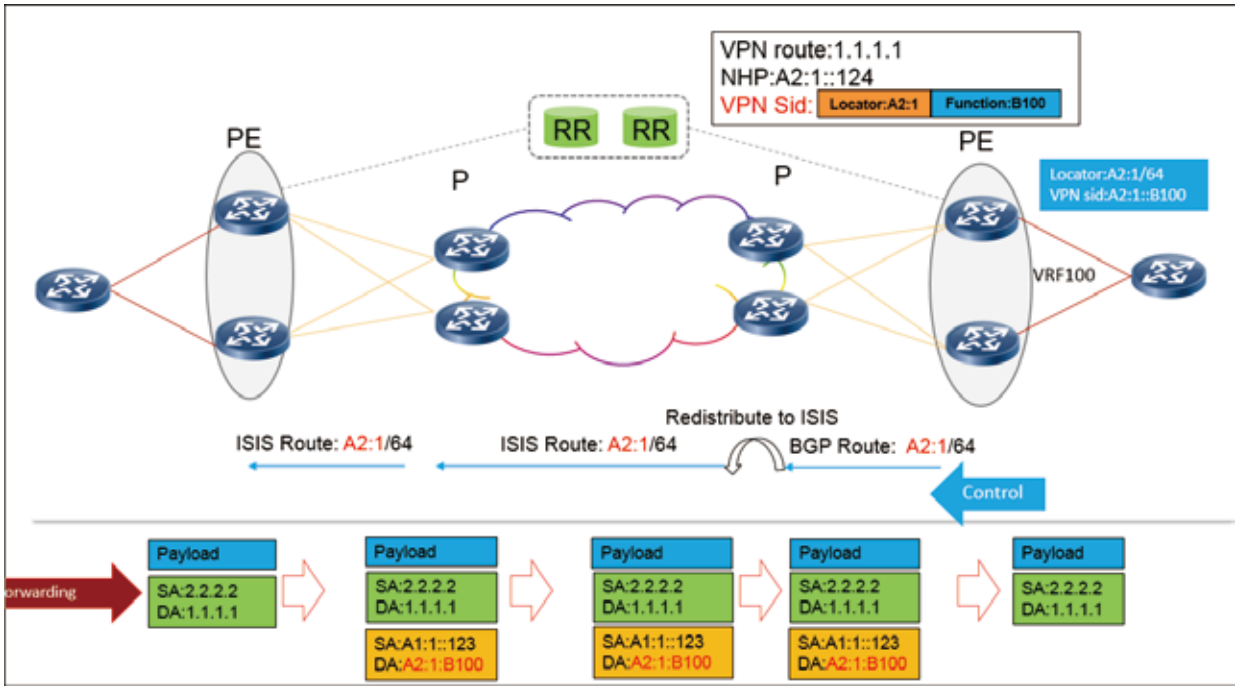
传统Seamless MPLS VPN要打通一个端到端跨域VPN，MPLS VPN需要Over到端到端BGP Lsp和域内公网隧道上，而且，由于边缘结点需要学习对端的明细路由，扩展性也会带来一定的压力。得益于SRv6 VPN SID本身就有路由能力，SRv6 VPN可以直接overlay在Native IPv6上。这使得SRv6 VPN具备如下优势：

1.网络简化：Best Effort（BE）类型的VPN业务不需要建立隧道，BE VPN可以直接承载在Native IPv6上。

2.网络扩展性：IPv6路由的聚合能力使得网络边缘结点只需要维护聚合或默认路由，这降低了大规模网络边缘结点的压力。

3.简化部署：只需要构造一个处处可达的IPv6网络，我们可以在任意点直接创建VPN，而不需要任何Underlay相关的配置。

另外，由于VPN可以直接承载在Native IPv6上，使得网络收敛性能，网络可靠性也会得到大幅的提升。

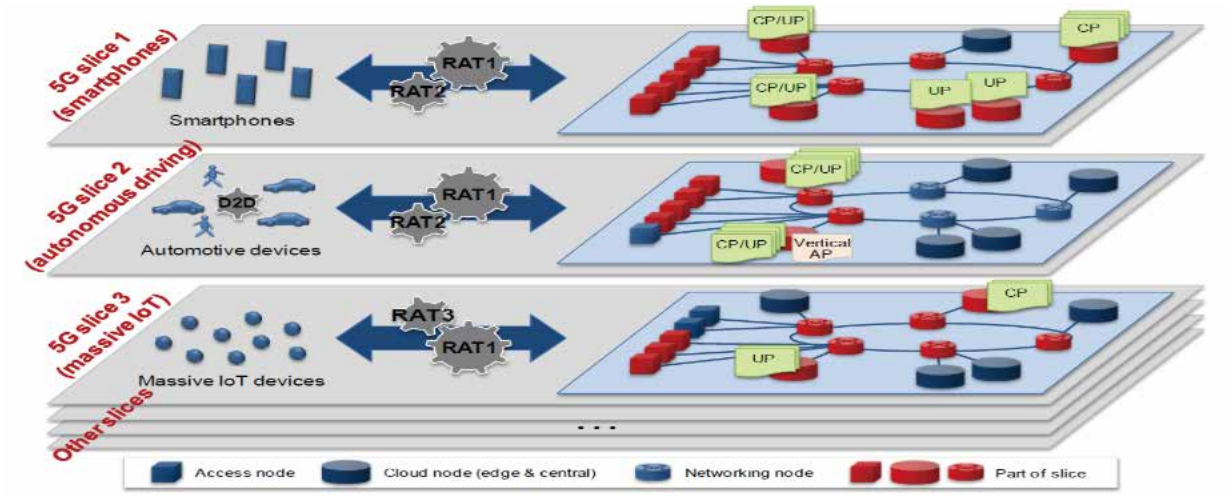


12.SRv6 VPN转发示意图

2.2.4.SRv6网络切片

一. 背景介绍

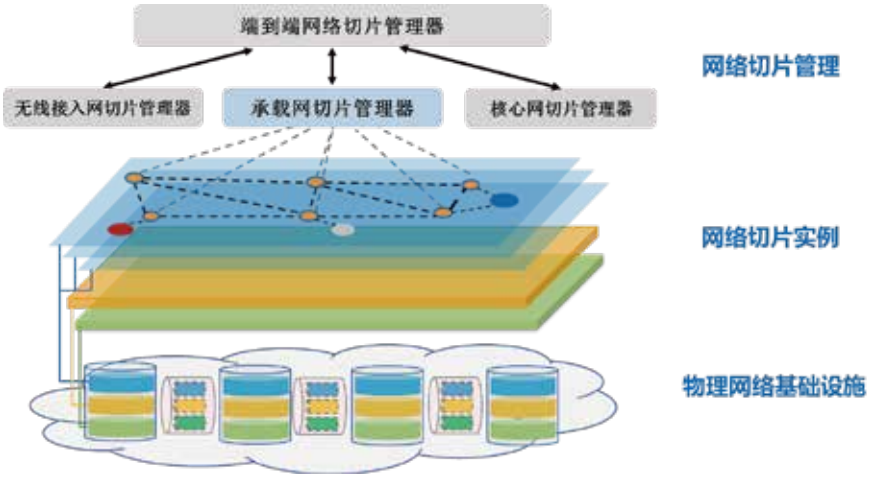
为了实现在同一张网络中同时满足各种各样类型业务的差异化需求，网络切片成为5G的关键技术之一。网络切片是指在一张物理网络上划分出多张由特定网络功能，网络拓扑和网络资源组成的虚拟网络，用于满足不同网络切片租户的业务功能，连接，和服务质量要求。例如，运营商可以在网络中为5G不同的业务类型EMBB，URLLC和MMTC划分不同的网络切片，分别满足业务的大带宽，低时延高可靠和海量连接需求。



13.分片示意图

二. 工作原理

承载网切片为5G的端到端切片提供定制化的网络拓扑和连接，以及为不同网络切片的业务提供差异化且可保证的服务质量(SLA, Service Level Agreement)。承载网切片的整体架构包含三个层次，网络基础设施层，网络切片实例层和网络切片管理层，如下图所示：



14.网络分片系统架构图

物理网络基础设施层通过各种底层技术提供网络资源切分和隔离能力，为不同的网络切片提供资源隔离，避免或减少不同网络切片之间的影响。

网络切片实例层负责在物理网络中生成不同的虚拟网络切片实例，提供按需定制的虚拟网络拓扑等属性，并实现切片虚拟网络与为切片分配的底层网络资源有机整合。SRv6的数据面和控制面技术是网络切片实例层的重要组成技术。

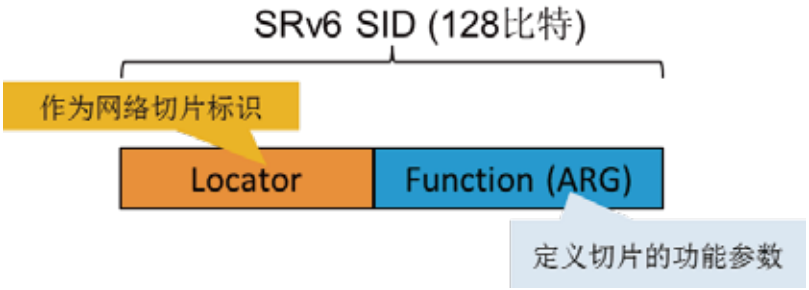
网络切片管理层提供网络切片的生命周期管理功能，包括切片的规划，创建，监控，调整和删除。网络切片管理层还提供开放接口与5G的端到端切片管理器交互切片的需求和能力信息。

三. SRv6网络切片

SRv6的可编程能力和对协议的简化使其可以提供网络切片实例层的数据平面和控制平面功能。

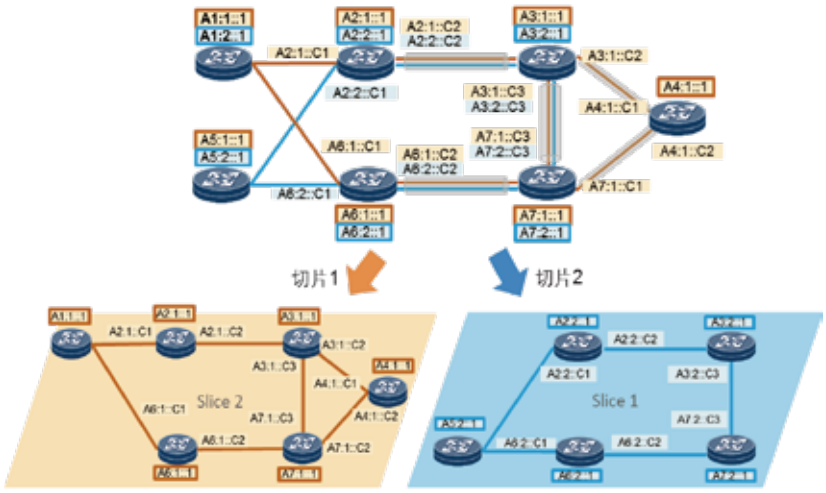
在数据平面，利用SRv6的可编程能力，网络设备为每个所参与的网络切片分配专用或共享的网络资源，同时为每个切片分配专用的SRv6 Locator作为切片标识，并使用该Locator为前缀的SRv6 SID标识为该切片分配的网络资源。不同网络设备对应同一网络切片的SRv6 Locator和SID集合组成一张SRv6虚拟网络。对于每个切片内的业务报文，使用对应切片的SRv6 SID生成Segment List封装在SRv6报文头中。沿途的网络设备根据SRv6 Locator或SID识别报文所属的网络切片，使用该切片定义的拓扑和资源执行转发处理，从而为不同网络切片中的业务提供差异化的转发路径和相互隔离的资源，保证切片间业务互不影响。

在控制平面，得益于SRv6对协议的简化以及对SDN的内生支持，网络切片控制器与网络设备的分布式控制平面相互配合，提供网络切片信息的分发，收集以及基于网络切片的集中式或分布式路径计算和转发表生成。



15.SRv6 SID 格式

下图给出一个基于SRv6的网络切片示例。网络切片管理平面根据不同业务的需求，规划出两张不同的切片网络拓扑，棕色标识网络切片1的拓扑，蓝色标识网络切片2的拓扑，并根据业务需求为每个网络切片规划需要分配的资源。每个网络节点为所参与的每个切片分配专用的SRv6 Locator作为切片标识，并使用该Locator为前缀的SRv6 SID标识为切片分配的资源。属于网络切片1的SRv6 Locator和SID集合组成切片1对应的SRv6虚拟网络。同理，属于网络切片2的SRv6 Locator和SID集合组成切片2对应的SRv6虚拟网络。



16.SRv6 for 分片原理图

四.小结

网络切片是使能差异化业务承载和保证的关键技术。将SRv6的可编程能力和网络简化能力应用在网络切片场景，可以实现灵活可定制的网络切片。通过使用SRv6　SID标识各种网络资源，可以进一步提供资源隔离的网络切片，满足不同业务的隔离和差异化服务需求。

2.2.5.SRv6业务链

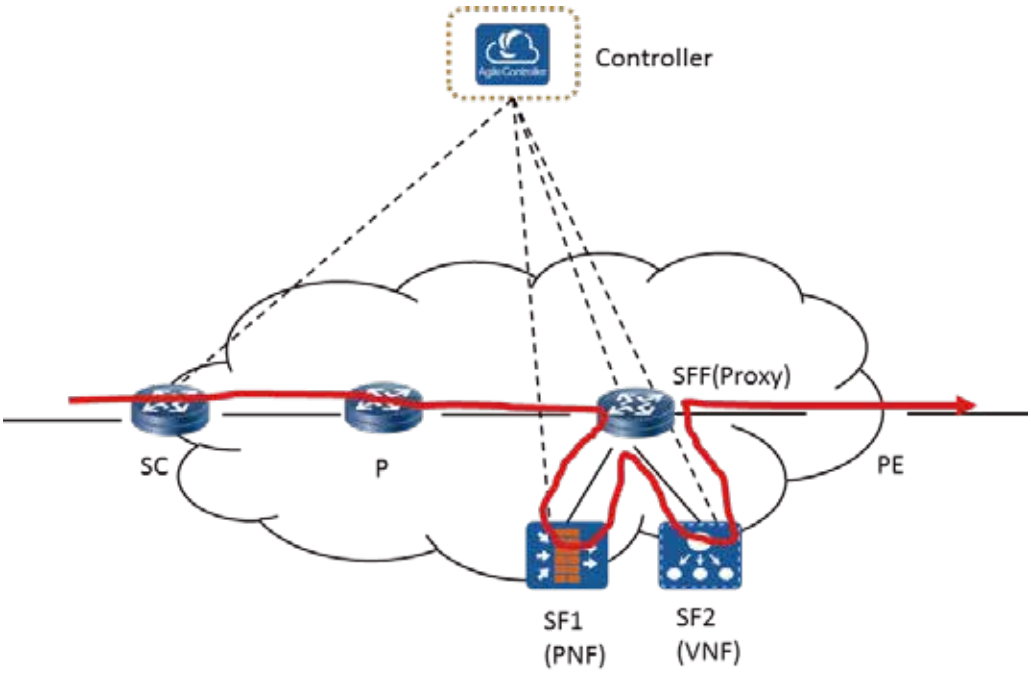
一.背景介绍

对于IP业务而言，除了要求网络将IP报文准确地传输到目的地之外，通常还要求在转发过程中，使IP报文按指定的顺序经过一系列的业务功能设备处理，例如：防火墙、NAT、DPI等。

由于业务功能设备提供的是增值业务处理，因此，通常部署在"旁路"网络中（例如，DCN）。如果使用路由协议来将业务流量引导至这些业务功能设备，不仅配置复杂、灵活性和扩展性都很差，在某些情况下甚至无法实现。为了提供通用的业务功能设备引流解决方案，IETF定义了业务链（SFC, Service Function Chain）技术和标准。

二.SFC技术原理

IETF定义的业务链的实现架构如下图所示，主要由两大部分构成：



17.业务链架构图

1.控制面：分为静态控制面和动态控制面这两种形式。二者分别使用命令行/MIB/Netconf等管理接接口、SDN控制器对业务链相关参数进行配置和维护。

2.数据面：根据所实现功能的不同，可以将业务链报文的转发设备分为如下几种类型：

（1） SC（Service Classifier，业务分类器）：负责将指定的业务报文引流到业务链中，并添加业务链相关的封装。

（2） SFF（Service Function Forwarder，业务功能转发设备）：负责将业务链相关报文转发给SF处理。

（3） SF（Service Function，业务功能设备）：实现了指定业务功能（防火墙、NAT、DPI等）的设备。根据实现和部署形态的差异，可以分为PNF和VNF两种形态。

（4）SFC Proxy（业务链代理设备）：如果SF不支持业务链相关的报文封装格式，还需要实现和部署代理设备，负责去除/恢复业务链相关的报文封装格式。

目前较为常见的业务链技术主要有PBR（Policy-based Routing，策略路由）和NSH（Network Service Header）。

使用PBR实现业务链时，存在如下一些问题：

1.PBR需要基于每条业务流进行配置，配置复杂，可扩展性差。

2.PBR不能支持携带元数据（metadata），难以满足将来业务的需求。

3.PBR缺乏故障检测与保护倒换机制。在发生故障时，容易产生流量黑洞。

4.NSH是一种标准化的业务链实现技术。NSH的意图是为各种网络承载技术提供通用的业务链解决方案，但也存在一些问题，特别是在SRv6网络中，NSH显得有些冗余：

1.NSH的转发路径需要基于每条业务流配置，配置复杂，可扩展性差。

2.NSH不具备故障保护能力和灵活编程能力。

3.SRv6本身具有业务链所需要的业务和路径编排能力。

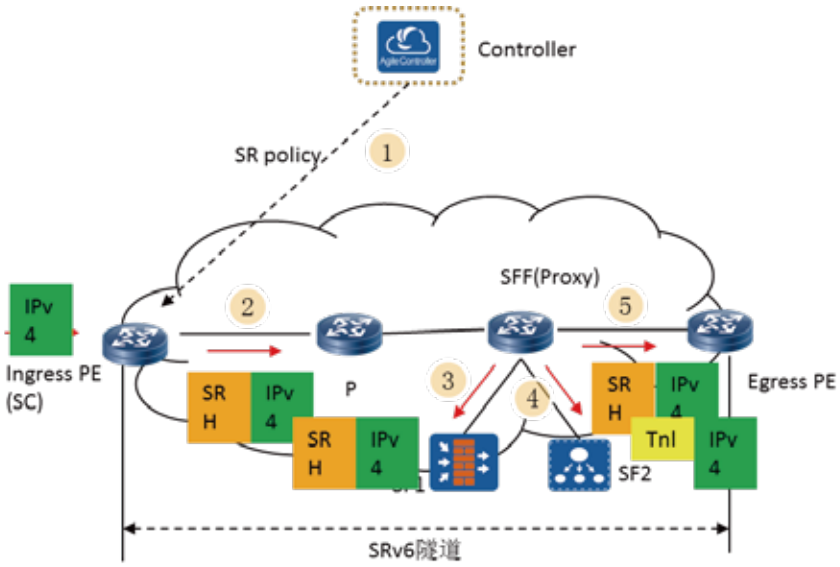
4.在SRv6网络中同时部署NSH，会增加网络层次、增加报文封装长度，为网络设备带来更大的挑战。

三. SRv6业务链

SRv6 SID作为指导SRv6报文转发的指令，可以具有拓扑语义和业务语义。SID的拓扑语义通常用于指示SRv6报文在网络中的转发路径，而SID的业务语义则用于指示SRv6报文在指定的设备上实现特定的业务功能（防火墙过滤、VPN业务等）。在SRv6网络中，利用SID的业务语义实现业务链功能无疑是最佳的选择。

SRv6业务链基于SRv6 SID的业务语义（称为service SID）实现业务链的相关功能，即使用SID list表示需要按顺序执行的一系列业务功能（FW、WAF、LB等）。

下图显示了SRv6业务链的处理过程：



18.SRv6业务链处理流程

（1）SDN控制器将service SID与其他SID，进行统一编排，以SRv6 policy的形式下发给入口PE（Ingress PE）。在部署SRv6业务链时，入口PE通常也会作为业务链的流分类器（SC）。

（2）当入口PE接收到IPv4业务报文（也可以是IPv6或Ethernet报文）时，迭代到SRv6 policy，完成SRH封装后，转发给下游设备。对于中间设备（P节点）而言，按照SRv6的常规转发流程处理。

（3）对于业务链的转发设备（SFF）而言，需要区分两种情况：

a.如果所接入的业务功能设备自身支持SRv6（例如，SF1），即，service SID是安装在SF上的，SFF行为与其他P设备类似，SF1支持处理SRv6报文，以匹配业务链相关功能。

b.如果所接入的业务功能设备（SF）自身不支持SRv6（例如，SF2），那么，SFF需要实现代理功能。即，SFF在将IPv4业务报文转发给SF2之前，需要将SRv6头部封装替换为指定形式的隧道头部，并在接收到SF2返回的报文时恢复SRv6头部封装。

四. 小结

使用SRv6实现业务链，与其他方式（PBR/NSH等）相比可以带来如下优势：

（1）管理面无状态：SDN控制器只需要基于SF粒度为SFF/SF节点配置SID，这个SID可以被所有相关业务流所使用，而无需为每条业务流配置转发表项。

（2）网络层次简化：拓扑SID与业务SID可以统一编排，简化了实现与维护。无需像NSH那样，需要分别编排隧道转发路径和NSH SFP。

（3）支持SF无缝扩容/缩容：在网络中动态添加或缩减SF时，控制器只需要向头节点下发更新后的SRv6 policy即可，而无需修改网络中其他设备的配置信息。

（4）故障收敛性能高：PBR/NSH等业务链技术本身没有故障保护能力，而SRv6业务链可以充分利用SRv6动态可编程能力，实现各种故障场景下的流量保护与倒换。

2.2.6.SRv6 Detnet

背景介绍

承载网作为5G端到端URLLC服务的重要组成部分，需要新的技术提供可保证的SLA。传统的承载网的服务技术主要有两种：时分复用和统计复用。分组交换网（IP/Ethernet）提供了基于统计复用的转发，具有带宽利用高，部署简单的特点，但是无法提供网络服务质量（SLA Service Level Agreement）的严格保证；时分复用（TDM Time Division Multiplexing)是一种基于时间的多路复用技术，时间域被分成周期循环的等长区间，两个以上的数据流轮流使用等长区间，对外表现为同一通信信道的子信道。TDM可以提供严格的SLA保证，但是部署成本较高，灵活性较弱，且信道的最小粒度；

确定性网络技术（DetNet Deterministic Networking）是一种提供可承诺SLA保证的网络技术，它能够综合统计复用网络和时分复用网络的优势，在IP、Ethernet分组网络中提供类似TDM转发的服务质量，保证高价值流量在传输过程中低抖动，零丢包，具有可预期的端到端时延上限。

二. 工作原理

DetNet代表的是一个技术合集，包括了很多相对独立的单点技术，主要包括：

1.资源分配（Resource Allocation）：在当前统计复用网络中，拥塞是造成分组网络时延不确定以及丢包的重要原因。TSN/DetNet依靠资源预留和队列管理算法来避免高优先级报文之间的冲突，避免网络中出现拥塞，同时提供可保证的端到端时延上限。

2.显式路径（Explicit Route）：为了保证业务的网络质量稳定，不受网络拓扑变化的影响，确定性网络需要提供显式路径，对报文的路由进行约束，以防止路由震动或其他因素对业务产生影响；

3.业务保护（Service Protection）：业务保护是指同一份业务在网络中选取两条或多条不重合的路径同时传输，并在汇合节点保留先到达的报文，即在网络中实现“多发选收”；这种机制能够在某一条路径发生断路丢包时无损切换到另一条路径，保证业务的高可靠传输。

这些单点技术互相结合，可以形成完成的解决方案，其中涉及转发面的队列管理算法，数据面的报文封装设计，以及控制面的资源预留和路径管理等。

三. SRv6 for Detnet

SRv6提供了丰富的TE和可编程能力，切合了DetNet多维度的技术的需求，其中：

1.SRH中的Segment List可以指定流量在网络中的传输路径，满足DetNet显式路径的需求；

2.SRH中的Optional TLV可用于携带业务保护、冗余传输所需要的Flow Identification和Sequence Number，同时可以扩展相应的Function，指示报文在特定节点进行流量的复制，以及冗余报文的删除；

3.SID中的Arguments可用于携带DetNet流量在设备内预留的资源信息，以保证DetNet流

量不会因为资源不足而发送拥塞，影响DetNet流量的服务质量；

2.2.7.SRv6 iFIT

一. 背景介绍

iFIT（In-situ Flow Information Telemetry）是一类随路流检测技术的总称。区别于主动的OAM方法（e.g. TWAMP、OWAMP），随路网络测量并不会发送主动探测报文，而是将OAM的指令携带在用户报文中。处理节点根据报文中的OAM指令信息，收集数据并处理。相较与主动测量，随路网络测量可以获得诸多的好处，包括：

1.测量真实的用户流量；

2.可实现逐报文的监控；

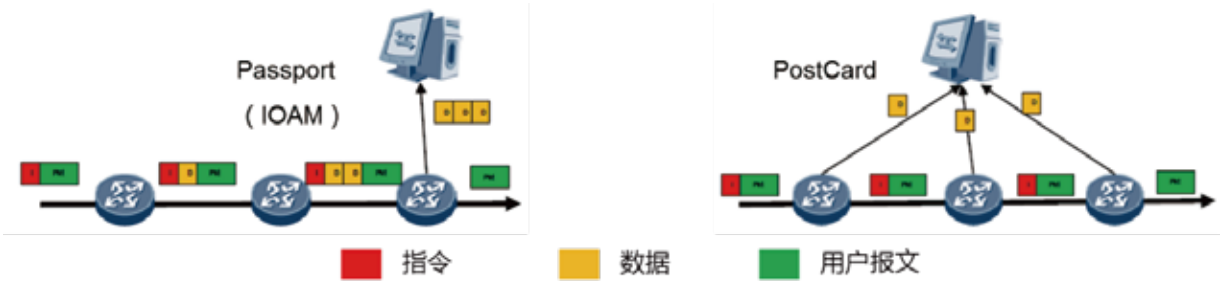
3.可以获得更多的数据面信息。

iFIT提供了一种随路网络测量的架构和方案，通过智能选流、上送数据压缩、动态网络探针等技术，并融合隧道封装的考虑，使得iFIT可以在实际网络中部署。

二. 工作原理

随路网络测量根据对收集数据的处理方式不同，存在两种基本模式：Passport和Postcard。对于Passport模式，在测量域的入口节点处为指定的报文添加一个指令头（Telemetry Information Header, TIH），包含有数据收集指令。中间节点根据数据收集指令，逐跳的收集沿途数据，并将数据记录在报文里。在测量域的出口节点处，上送所有收集的沿途数据，并剥离指令头和数据，还原数据报文。这就好像一个周游世界的游客，每到一个国家就在护照上盖上一个出入境的戳。

Postcard模式和Passport模式的区别在于，测量域中的每个节点在收到包含指令头的数据报文时，不会将采集的数据记录在报文里，而是生成一个上送报文将采集的数据发送给收集器。Postcard模式就好比游客到了一个景点，就寄一张明信片回家。



19.Passport模式和Postcard模式对比

IETF为iFIT定义了一个可以在各种封装中携带的数据收集指令。设备节点不论是支持Passport还是Postcard，都可以根据该指令中描述的数据收集需求，抓取数据。当前定6义的数据收集能力如下表所示：

比特位	数据域	比特位	数据域
0	短格式的当前跳+节点ID	7	增量校验和
1	短格式的入接口ID+出接口ID	8	长格式的当前跳+节点ID
2	报文到达的秒以上部分时戳	9	长格式的入接口ID+出接口ID
3	报文到达的秒以下部分时戳	10	长格式的名字空间特定数据
4	转发时延	11	缓存占用
5	短格式的名字空间特定数据	22	变长的不透明数据
6	队列深度	其他	未定义

表 22 iFIT当前支持收集的数据

三.SRv6 for iFIT

得益于SRv6灵活的扩展性和强大的网络可编程能力，iFIT的指令和数据可以根据功能需求使用不同的封装形式。IPv6的逐跳扩展头包含转发设备逐跳处理的语义。将iFIT的指令封装在逐跳扩展头内，可以让沿途的每一个节点都处理iFIT指令，并且按照指令收集数据。IPv6的目的扩展头只有在报文封装的目的地址对应的节点才处理。将iFIT指令封装在目的扩展头内，可以完成端到端数据收集。SRH会被SID List中指定的节点处理。因此，可以将iFIT指令封装在SRH的扩展TLV中，实现对指定节点的数据收集。

iFIT的Passport模式需要将逐跳收集的Metadata插入到数据报文中。随着跳数的增加，会导致报文头的不断增长，并对数据的转发造成负担。特别是在做逐跳数据收集时，Metadata被封装在逐跳头中，如果后面还有SRH需要处理，会增加将SRH挤出报文处理的缓存窗口的风险。一种解决的方案是将指令和数据分离，将Metadata单独封装在SRH之后，从而避免转发时移动包窗引入性能的下降。

四. 小结

iFIT相对于主动测量技术，提供了流级的SLA可视。结合SRv6灵活的可编程能力，iFIT可以为网络提供更好的OAM能力。iFIT不论是对SR-BE还是指定路径的SR-TE都能够有效的简化运维。

2.2.8.SRv6组播BIER6

一.背景介绍

IP组播技术实现了IP网络中点到多点的高效、实时数据传送，在运营商网络IPTV等业务中有着广泛的应用。

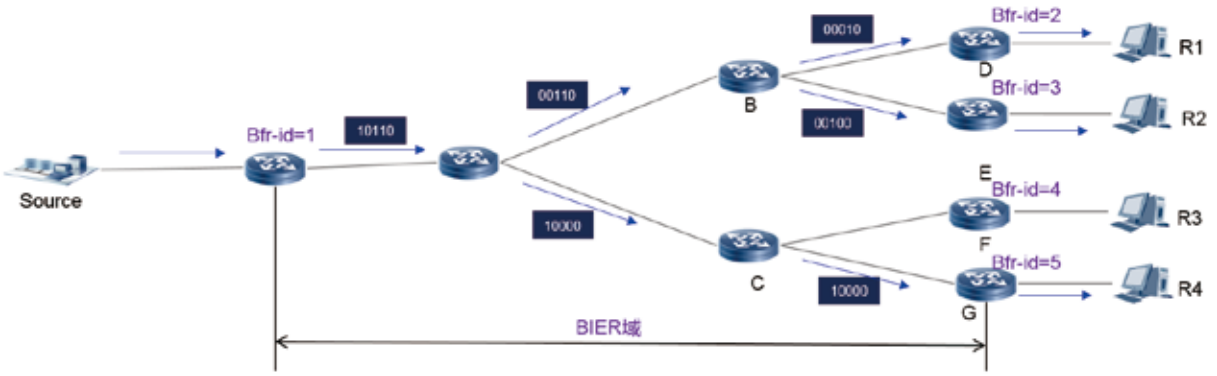
IP组播路由协议主要包括PIM和mLDP。其中PIM是负责逐跳的向组播源或者RP发送组播加入、建立组播报文转发路径，mLDP是负责逐跳的向组播源侧的PE路由器发送组播加入、建立MPLS P2MP报文转发路径。

无论是PIM还是mLDP，都需要针对每个组播节目，在网络中各个节点建立组播转发树。随着组播节目的增加，网络中各节点需要建立的组播转发树状态也越来越多，设备的压力增大。当网络中发生链路故障时，设备需要针对每个组播表项对应的组播树，重新向新的链路上发送组播加入以修复组播树，业务收敛恢复的时间较长。这是现有组播技术针对每个组播节目逐跳建立组播树的固有特点。针对传统组播的缺点，BIER技术应运而生。

二.BIER技术原理

BIER(Bit Indexed Explicit Replication)是一种新的组播数据报文转发架构，它提供了一种在组播域中转发组播报文的理想方案，而不需要针对每个组播节目逐跳显式、逐跳建树，也不需要为每个组播节目在各路由器上保存转发状态。当一个组播报文进入到由BIER转发路由器组成的BIER域时，由BIER域的头端节点确定报文要到达BIER域的哪些尾端节点，将需要到达的尾端节点封装在报文的BIER头中。BIER头中使用一个BitString来表示要到达的尾端节点的集合，其中每个Bit位置代表一个尾端节点。各路由器根据BIER头中的BitString复制和转发报文，而无需感知每一个组播节目有哪些下一跳出接口。

下图是一个BIER域及报文转发示例：



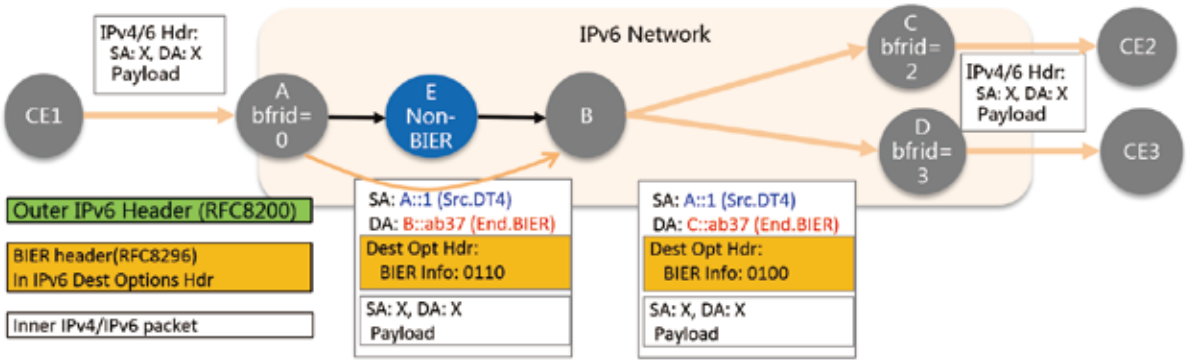
20.BIER转发示意图

BIER域中的基本配置管理、信令消息的单位是子域Sub-domain。在一个Sub-domain中为各边缘节点配置一个唯一的编号，即Bit Forwarding Router(BFR) ID，或BFR-id，比如从1到256的BFR-id。当需要从一个节点复制到多个目的节点时，将多个目的节点用一个Bit串(BitString)来表示，BitString中的每个Bit位(BitPosition)标识一个边缘节点，例如一个256bit的BitString，从右往左第1个Bit位表示BFR-id=1的节点，第2个Bit位表示BFR-id=2的节点，第256个Bit位表示BFR-id=256的节点。当Bit位置1时表示需要往该Bit位所代表的节点复制报文，反之当Bit位置0时表示不需要往该Bit位所代表的节点复制报文。例如一个<1100……0110>的BitString，表示要往BFR-id=2/3/255/256共4个节点复制发送报文。

其中BitString长度根据业务诉求和硬件能力，可以是64bit、128bit、256bit、512bit、1024bit、2048bit、4096bit，默认值是256bit。在默认值下，如果一个域中有多于256台边缘PE节点，可以将这些设备划分成多个集合（Set），并使用集合ID（Set ID，SI）标识。例如，有512台边缘PE设备，其BFR-id配置为1至512之间，其中BFR-id 1到256属于第一个集合，其SI为0，而BFR-id 257到512属于第二个集合，其SI为1。在转发时，除了有一个256bit的BitString外，还有一个标识报文属于哪个SI的信息。在BIER-MPLS封装中，使用一个MPLS标签来标识报文使用的BitString长度（Bit String Length，BSL）、报文属于哪个SI。在非MPLS的BIER封装中，使用一个BIFT-id字段来标识报文使用的BSL以及SI。

三. SRv6 for BIER（BIER6）

SRv6网络使用IPv6为基础的IP转发而不依赖于MPLS信令和封装转发，BIER同样也可以应用在SRv6/IPv6网络中，基本原理如下图所示：



21.SRv6 BIER原理

BIER6域头结点A收到用户侧组播报文，封装外层IPv6头和扩展头，扩展头里携带BIER头，BIER头有表示目的节点集合的BitString。A还根据BIER头及其BitString信息，将报文发送给B，发送时使用B的单播地址B::AB37。

B根据BIER头及其BitString信息，将报文发送给C和D，发送时使用C的单播地址C::AB37以及D的单播地址D::AB37。

C和D根据BIER头及其BitString信息，确定其BitString包含有本机的BFR-id，将报文解封装，根据外层报文IPv6源地址确定报文属于哪个VPN实例或公网实例，再根据内层报文查找组播表项出接口，将解封装以后的报文发送给CE2或者CE3。

整个报文转发过程，均使用单播IP地址，如果A和B之间有一个节点不支持BIER6转发但支持IPv6，可以转发A发送给B的BIER6报文，无需任何额外的配置或处理。

为了支持组播VPN和公网组播，还需要一个区分不同VPN的标识。和SRv6采用IPv6目的地址标识VPN实例相似，BIER6采用IPv6源地址标识一个MVPN实例。这是因为组播是从一个源节点PE发送给多个目的节点PE，无法采用目的地址标识。用报文的IPv6源地址标识VPN以后，BIER6就不再需要在报文中额外封装一个VPN标签了，减少了不必要的封装开销，也从承载层面(underlay)和业务层面(overlay)都消除了MPLS，简化了信令。另外，作为组播源侧的Ingress PE节点，也不必要为Sub-domain分配BFR-ID值，在跨域的组播部署中，这可以简化BFR-ID的分配和管理。

四. 小结

BIER6是基于SRv6和BIER的架构思想及IPv6大地址空间、可扩展、可编程的特点而设计的组播方案。它使用IPv6的扩展头机制封装标准的BIER头、使用SRv6 SID作为目的地址指导数据面进行BIER头的处理、使用IPv6源地址标识MVPN，不再需要MPLS、VXLAN等任何额外的封装，单个封装即可支持逐跳的BIER组播复制、跨Non-BIER节点的多跳组播复制、跨AS域的报文发送或复制等场景，是IPv6/SRv6网络下的新一代组播方案。

2.2.9.APP-Aware IPv6 Networking

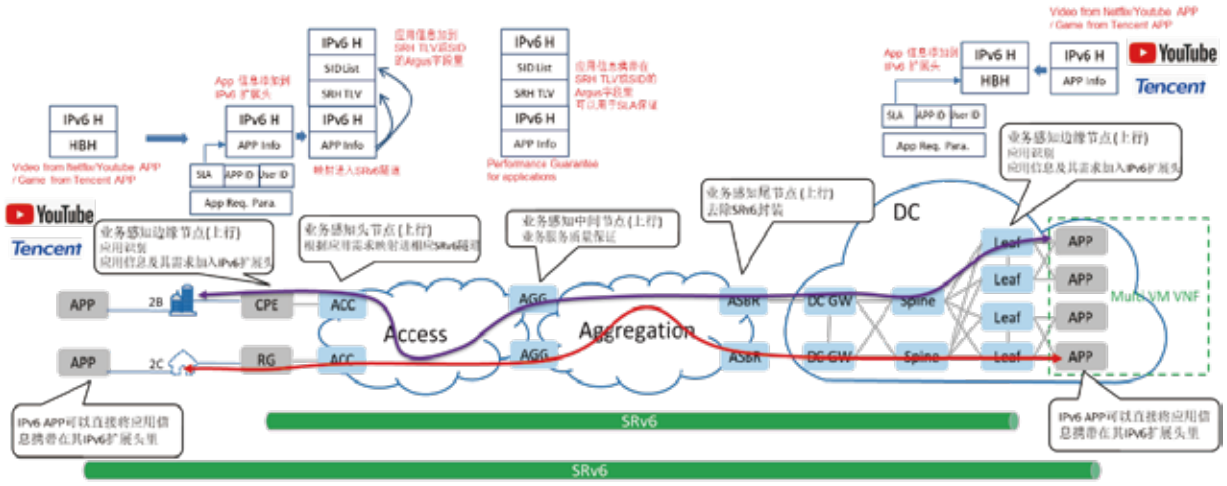
一.背景介绍

App-aware IPv6 Networking（APN6）是面向未来的一种新型IPv6网络架构，其架构全景如图一所示。APN6新型网络架构，针对网络无法感知应用而导致的运营商现网运营痛点，如网络利用率低、无法提供精细化差异化的运营服务等，意在改变网络与应用割裂现状，充分利用新兴的SRv6网络可编程能力，有效衔接网络与应用。

二.工作原理

App-aware IPv6 Networking利用IPv6扩展头（如Hop-by-hop Options Header (HBH)、SRv6 Segment Routing Header (SRH)）将应用信息由报文携带进入网络，使网络感知用户应用及其对网络的需求，从而为高优先级应用（视频、游戏等）提供精细化运营服务。所携带

的应用信息包括用户信息、应用标识、SLA需求等级信息和网络需求信息（如带宽、时延、丢包、抖动等）。终端设备的OS（如Linux kernel）需要扩展支持对应用信息的获取，并将其封装进IPv6扩展头内，由报文携带进入网络，或在网络侧识别应用并在扩展头中记录应用信息。当报文到达网络边界时，网络会根据报文携带的应用信息，为报文选择一条满足其SLA要求的SRv6传输路径，以此保证业务的体验质量。



22.App-aware IPv6 Networking (APN6) 架构全景

三.总结

APN6架构使能网络为应用（游戏/Cloud VR、交互式直播、支付和抢红包等）提供定制化服务，提升用户网络体验，提高网络价值，实现网络变现，提升运营商营收。APN6具有以下优点：

1.能够利用IPv6扩展头和SRv6的可编程能力，传递应用需求到网络层，使能网络对用户应用进行精细化运营

2.能够基于SDN进行快速业务部署，满足应用需求的快速动态响应

3.突破应用与网络边界，实现应用级的业务导流以及差异化SLA保证

4.应用侧云化资源与承载网络可以进行信息交互，能够统一调度云网资源以匹配新业务需求，实现真正的云网协同

5.仅需在网络边缘部署业务，无需改动网络中间节点，即可支持新业务的部署，简化网络

利用IPv6端到端可达性，实现从应用到应用真正的端到端网络，能够提供更优的服务质量。

3.产业进展

3.1.标准进展

SRv6的标准化工作主要集中在IETF SPRING（Source Packet Routing in Networking）工作组，其报文封装格式SRH（Segment Routing Header）等标准化工作在6MAN（IPv6 Maintenance）工作组，其相关的控制协议扩展的标准化，包括IGP、BGP、PCEP、VPN等，分别在LSR、IDR、PCE、BESS等工作组进行。

截止目前，SRv6的标准化基本上分为三大部分：

第一部分是SRv6基础特性，包括SRv6网络编程框架、报文封装格式SRH以及IGP、BGP/VPN、BGP-LS、PCEP等基础协议扩展支持SRv6，主要提供VPN、TE、FRR等应用。所有SRv6基本特性文稿均由华为和思科共同引领，并有Bell Canada、SoftBank、Orange等运营商参与。目前所有文稿（除OSPFv3）均被接收为工作组文稿，标准的成熟度进入了一个新的阶段，特别是最关键的SRH封装草案已经经过IETF IESG批准，很快就会成为RFC。

Area	Topic	Draft
Architecture/ Use case	SRv6 Network Programming	draft-ietf-spring-srv6-network-programming
SRH	IPv6 Segment Routing Header(SRH)	draft-ietf-6man-segment-routing-header
IGP	ISIS Extensions for SRv6	draft-ietf-lsr-isis-srv6-extensions
	OSPFv3 Extensions for SRv6	draft-li-ospf-ospfv3-srv6-extensions
VPN	SRv6 VPN	draft-ietf-bess-srv6-services
SDN Interface	BGP-LS for SRv6	draft-ietf-idr-bgpls-srv6-ext
	PCEP for SRv6	draft-ietf-pce-segment-routing-ipv6

表 31 SRv6标准

第二部分是SRv6面向5G和云的新应用，这些应用包括网络切片、确定性时延 （DetNet）、OAM、IOAM（In-situ OAM）、SFC、SD-WAN、组播/BIER等。这些应用都对网络编程提出了新的需求，需要在转发面封装新的信息。SRV6可以很好地满足这些需求，充分体现了其在网络编程能力方面具备的独特优势。当前客户对于这些应用需求的紧迫性并不一致，反映到标准化和研究的进展也不尽相同。总体而言SRV6用于OAM、IOAM、SFC的标准化进展较快，已经有多篇工作组草案，网络切片也是当前标准化的一个重点，VPN+切片框架草案已经被接纳为工作组，SRV6 SID用于指示转发面的资源保证服务需求逐渐获得了广泛的认同。

第三部分是SRv6面向应用感知的网络，即APN6（Application-aware IPv6 Networking）。

借助IPv6和SRv6的多重可编程空间，华为积极创新，在业界率先提出APN6概念，并携手Bell Canada、中国电信、中国移动、中国联通、丰田等运营商和垂直行业伙伴，共同提出Problem statement & use cases文稿，澄清目前运营商当前网络痛点以及APN6将如何支持运营商增加收益的use cases等。同时提出APN6架构草案，介绍APN6的整体框架、应用信息携带、关键功能网元等。在IETF105，华为进行了APN6的HotRFC宣讲，并成功举办APN6的SIDe Meeting，获得了包括运营商、OTT、学术界、厂商等业界多方的广泛参与和认可，参会人数达50余人。华为将联合业界继续探索APN6的商业价值及技术特性设计，积极助力客户商业成功。

3.2.SRv6 产业进展

3.2.1.产品实现

目前主流设备厂商、测试仪和商用芯片均已明确支持SRv6。

主流设备厂商：

·华为全系列路由器产品均支持SRv6。

·思科ASR9000、ASR1000、NCS5500、NCS540等产品已经支持SRv6。

测试仪厂商：思博伦和IXIA支持SRv6。

芯片厂商：海思、博通等也已发布可以规模部署的商用芯片，并在主流设备上完成验证。

除此以外，大部分主流开源平台也支持SRv6，如Linux Kernel，Linux Srext module，FD.io VPP等，提供对SRH的一些功能处理；一些开源工具应用，如Wireshark、Tcpdump、Iptables、Nftables，Snort等，也已经支持对包含SRH的IPv6报文的处理。

3.2.2.互通测试

一. 2019 IPv6专委会SRv6互通测试

2019年11月由中国推进IPv6规模部署专家委员会成功的组织了SRv6互通测试。华为、天融信、参与了互通测试。通过SRv6技术实现VPN、灵活路径编排和业务链等功能。场景涵盖：

1. 基于SRv6 BE的业务应用场景

（1）基于SRv6 BE的L3VPN

·基于SRv6 BE的L3VPN基本功能

·基于SRv6的拓扑独立(TI-LFA)快速重路由机制，进行链路保护

·基于SRv6 BE的L3VPN的OAM（ping和traceroute）

（2）基于SRv6 BE的L2VPN（点到点）

（3）基于SRv6 BE的L2VPN（点到多点）

2. 基于SRv6 POLICY的业务应用场景

（1）基于SRv6 Policy的L3VPN业务布放

（2）基于SRv6 Policy的业务路径调优

（3）基于SRv6 POLICY的业务链

·业务链1——TCP SYN报文攻击防御

·业务链2——IP流访问控制和流量监控

·业务链3——web用户访问控制和内容审计

二. 2019 EANTC

2019年3月 EANTC成功的开展了SRv6互通测试。并在2019年4月MPLS + SDN + NFV世界大会上展示了互通测试结果。该测试验证了SRv6草案在五种不同设备上的实现，包括华为NE9000-8、NE40E-F1A路由器，思科NCS 5500路由器，思博伦和Keysight IXIA测试仪。对SRv6互操作（包括SRH处理）进行了验证。 场景涵盖：

1. 基于SRv6的IPv4流量的L3VPN 行为。

2. 基于SRv6的IPv6流量的L3VPN 行为。

3. 基于SRH的拓扑独立(TI-LFA)快速重路由机制，进行链路保护。

4. OAM流程（ping和traceroute）

在入口PE和出口PE之间发送双向流量，即同时实现封装(T.Encaps)和解封装（END.DT4、END.DT6）功能，流量经过P节点（非-SRv6能力）的多种实现，证明中间转发节点只需支持IPv6即可实现转发。

3.2.3.产业活动

随着SRv6技术和标准不断成熟，业界对SRv6的认可和接受度也越来越高。为了进一步凝聚产业共识、推动SRv6创新应用，经过业界共同努力，目前已举办多次SRv6产业活动。

2019年4月，法国巴黎，MPLS+SDN+NFV大会期间举办了首届SRv6产业圆桌会议：与会业界专家围绕SRv6的价值场景以及如何促进SRv6创新和部署等话题进行了热烈讨论。

2019年6月，中国北京，推进IPv6规模部署专家委员会主办了第一期SRv6产业沙龙：与会专家分享了SRv6标准创新的最新进展、整体解决方案以及现网部署应用等。

这些产业活动对于SRv6创新应用均起到了积极的推动作用。

3.3.中国IPv6政策

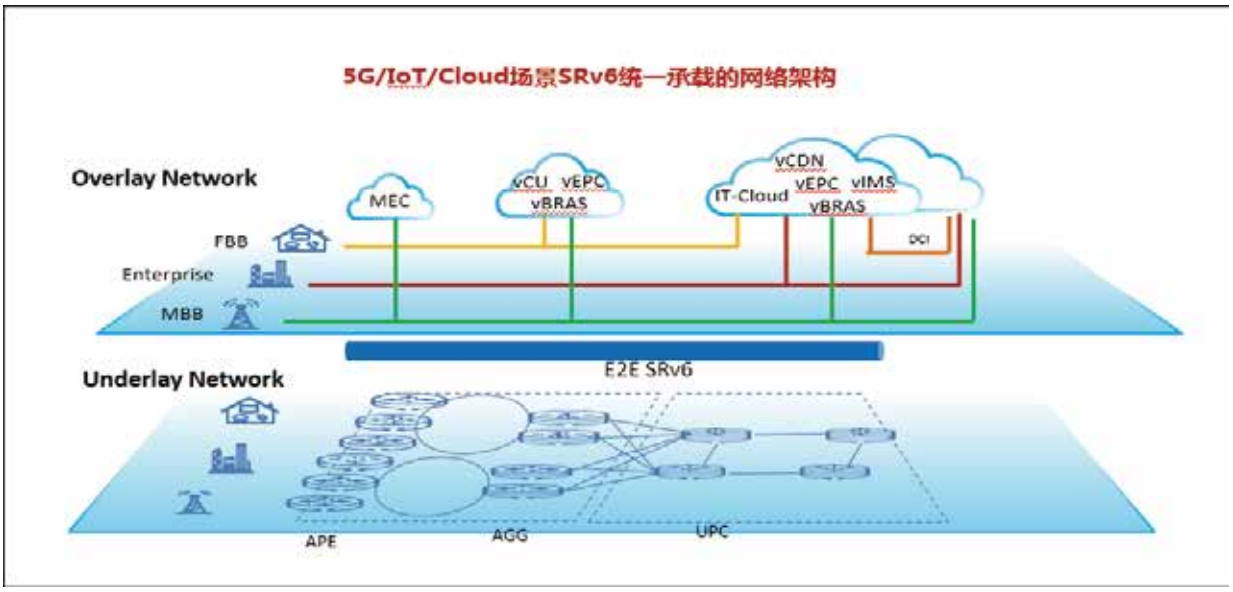
2017年11月26日，中共中央办公厅、国务院办公厅印发了《推进互联网协议第六版（IPv6）规模部署行动计划》（以下简称《行动计划》），明确提出用5-10年的时间，形成下一代互联网自主技术体系和产业生态，建成全球规模的IPv6商业应用网络，实现下一代互联网在经济社会各领域深度整合应用，并成为全球下一代互联网发展的主导力量。

在国家推进IPv6规模部署专家委员会下，已立项IPv6+技术创新工作组，整合IPv6相关技术产业链（产、学、研、用等）力量，积极开展IPv6+网络新技术（包括SRv6、VPN+、 Detnet、BIER6、SFC和OAM等）、新应用的试验验证与应用示范，加强基于IPv6下一代互联网技术的体系创新。

4.应用场景

4.1.应用场景介绍

SRv6是未来众多场景的关键使能技术。未来5G/IoT/Cloud是主要的新型场景，这些业务对网络的可扩展性、高质量、可运维性、可靠性、稳定性和安全性提出了很高的诉求，而SRv6的多种关键技术可以很好地匹配这些需求。



23.SRv6 网络架构示意图

如上图，5G核心网各功能模块按需放在EDC/RDC/CDC内，固网业务BRAS云化后放在RDC/CDC内，企业IT资源也放置在云端。5G业务访问核心网，5G终端之间互访通过E2E SRv6承载。固网用户访问互联网，到BRAS拨号上线，上线报文和数据报文通过E2E SRv6承载。企业用户访问IT资源，企业站点之间互访，通过E2E SRv6承载。骨干网或DCI通过SRv6承载。通过SRv6统一承载各种业务，达到协议简化，运维简化，高可靠性，智能化，扩展性强，SLA可承诺。

4.2.5G业务场景

4.2.1.业务场。景需求介绍

5G带来的几个关键问题：

1 .5G基站数量庞大，组网规模的变大对网络简化如即插即用，协议简化，极简布放，智能运维等提出了更高的要求；

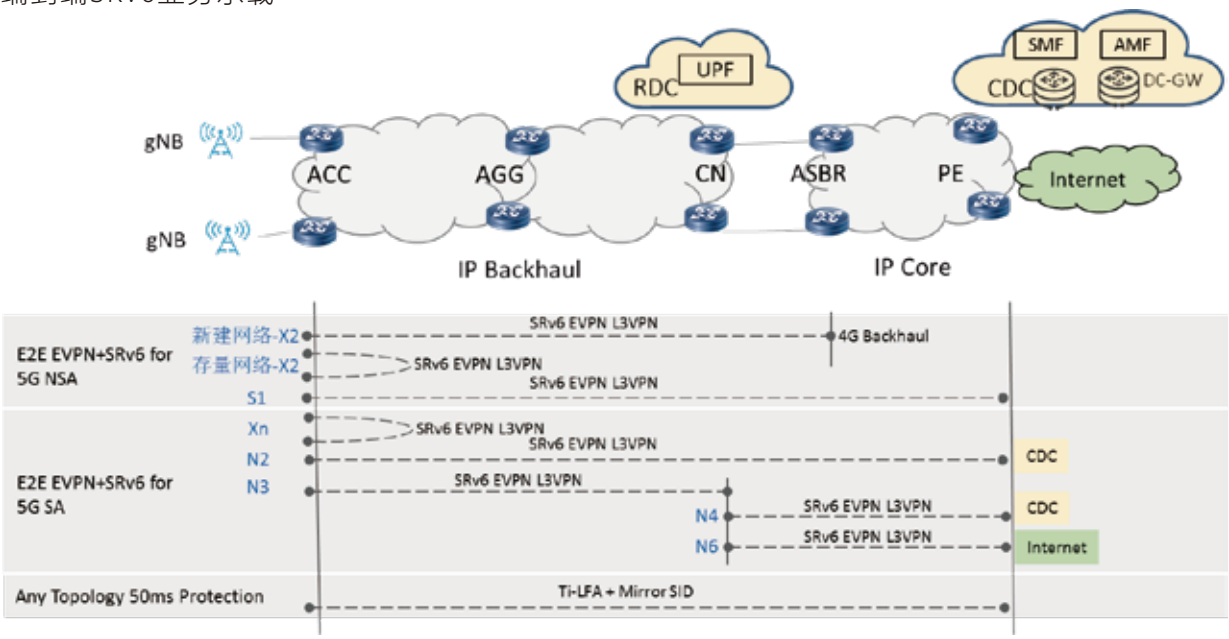
2. 5G的URLLC业务面向车联网、工业控制、智能制造、智能交通物流及垂直行业的特殊应

用需求，要求为用户提供毫秒级的端到端时延和接近100%的业务可靠性保证；

3.5G核心网架构演进要求5G核心网的网元全部都云化，并放置在数据中心中，5G承载网络必须要能够提供Site2Site，Site2DC，DC2DC的多样化管道承载能力，以及云网端到端协同运维，业务快速开通的能力。

4.2.2SRv6实现方案

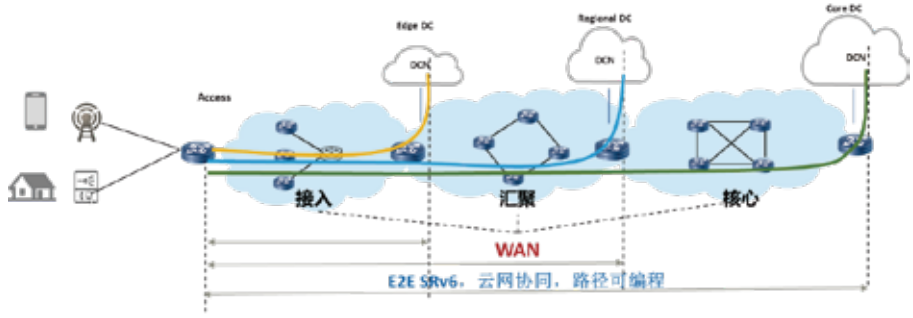
端到端SRv6业务承载



24.SRv6的业务承载方案

如图所示，5G基站到核心网的N2/N3业务，5G基站和基站之间的Xn业务，核心网和核心网之间的N4/N9业务，核心网和Internet之间的N6业务，所有业务均采用SRv6+EVPN L3VPN方案承载。一般情况下，业务采用SRv6 BE承载，对于有特殊要求的业务，采用SRv6 Policy方案，实现路径选择，提供SLA保障。

同时SRv6入云，可实现网络和DC的统一管理，实现云网端到端拉通及协同，业务自动化部署，运维检测无断裂点，提高部署和运维效率。



25.SRv6 for 云网协同

综上，通过SRv6承载，简化部署，为5G应用提供SLA保障和高可靠性，同时端到端协同部署，保证业务快速开通，提升运维效率。

4.3.家宽业务场景

4.3.1.业务场景需求介绍

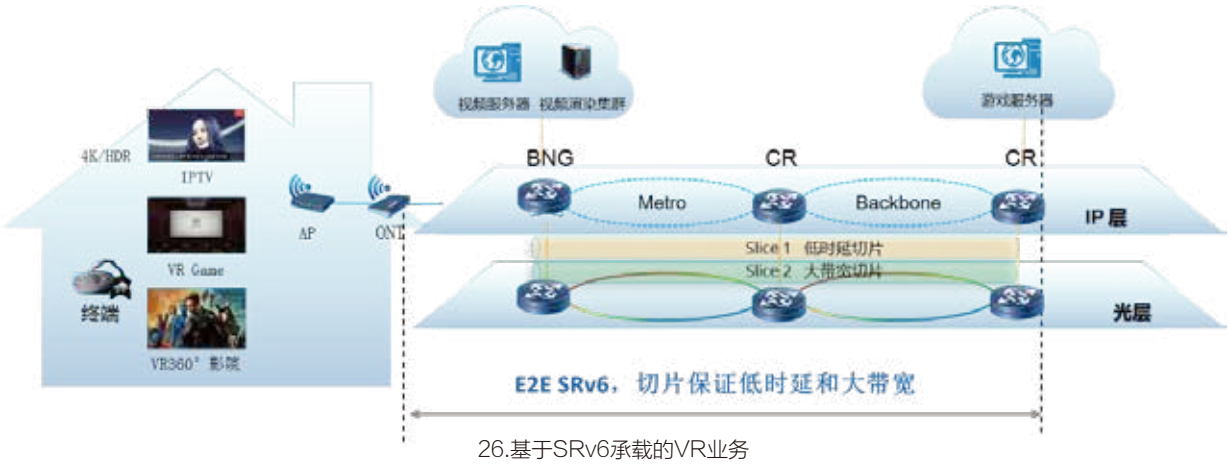
Cloud VR是5G的一个最典型应用，同时也是千兆家宽的主力应用场景。它将云计算、云渲染的理念及技术引入到VR业务应用中，VR业务内容和渲染部署在云端，借助高速稳定的网络，将云端的显示输出和声音输出等经过编码压缩后传输到用户的终端设备。Cloud VR业务对网络的要求如下，要求大带宽，丢包少，时延低。

业务场景	指标项	参考值
强交互VR业务	带宽	≥80Mbps
	RTT	≤20ms
	丢包率	1.00E-5
多种业务并发场景	含上网、VR强交互业务、投屏等	260Mbps
VR视频业务	带宽	≥60Mbps
	RTT	≤20ms
	丢包率	9E-5

表41 VR业务对网络的需求

4.3.2.SRv6实现方案

通过CDN边缘/边缘渲染节点下沉，采用边缘计算、SRv6切片等技术，可更好地承载VR社交、VR游戏、6DoF VR（6自由度VR，6 Degree-of-Free VR）等VR业务要求。

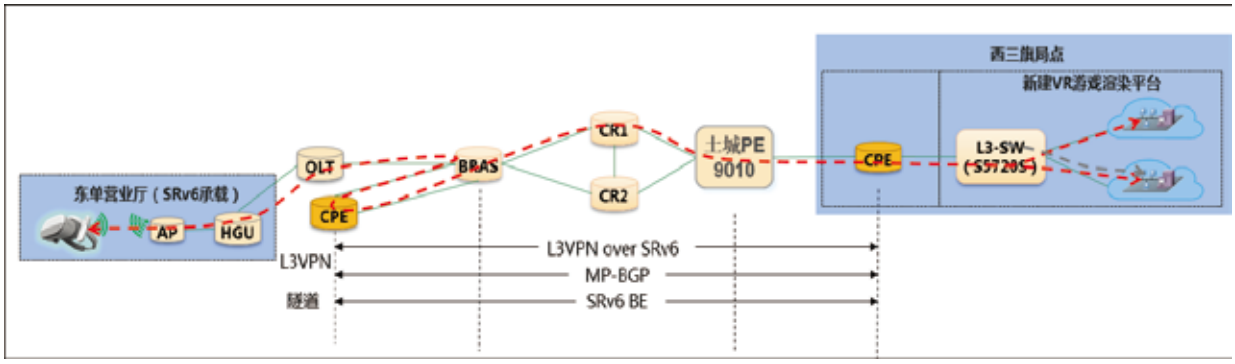


26.基于SRv6承载的VR业务

承载网络根据VR业务的需求建立从接入网络到CDN的 E2E SRv6隧道，满足时延、带宽要求。

4.3.3.实际案例及亮点介绍

千兆时代的到来对Cloud VR产业的发展起到了非常大的促进作用，北京联通顺应产业趋势在东单营业厅建立了CloudVR 云游戏体验中心。作为体验中心的业务需要快速开通并保证高品质体验效果。 针对以上业务诉求，北京联通联合华为推出了CloudVR云游戏承载方案：使用SRv6快速打通营业厅上联BRAS 设备的旁挂CPE设备与同城VR游戏渲染平台CPE 之间的隧道，CloudVR云游戏业务使用L3vpn专线承载与该隧道之上，进而实现业务的快速开通。随着项目后续持续推进，在业务质量监控等方面会进一步增强，充分保障cloud VR业务极致体验。



27.北京联通基于SRv6的云游戏承载方案

4.4.企业专线业务场景

4.4.1.业务场景需求介绍

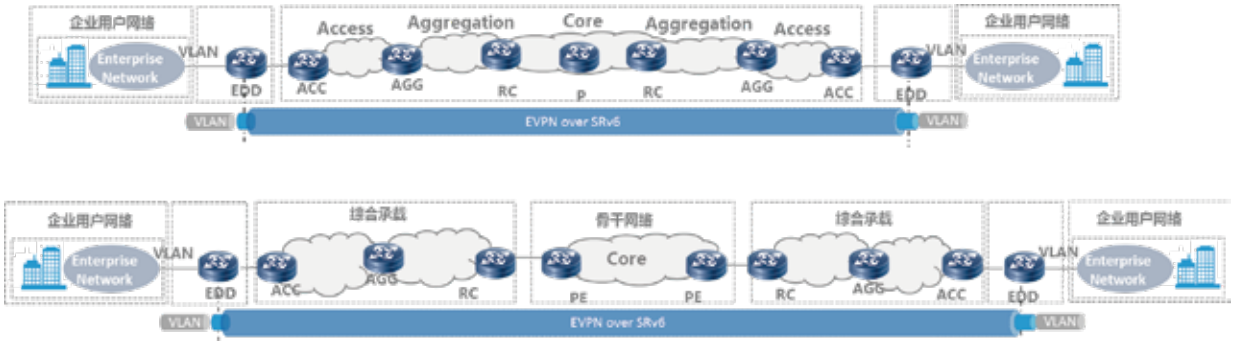
随着工业互联网和行业/企业数字化转型的发展，行业/企业用户的网络互联需求逐步增加。大量企业分支，中小企业office，商业门店需要接入专线，覆盖范围广，接入位置任意，同时

要求网络服务提供商灵活提供差异化的服务，比如带宽/时延SLA，增值业务等。

由于安全和可管理性问题，中国区大网不允许主机路由在全网传递，不管是传统MPLS，还是SR-MPLS，都无法支撑CPE到CPE的端到端业务部署，只能分段建，然后再拼接，造成了多段PW组网、跨域，业务发放复杂。另外多厂商插花组网，协同难，导致业务长期开不通。

采用SRv6，支持SID地址聚合，不用发布每台设备的明细路由，可以部署Seamless方案；业务部署相关节点数减少为2个节点；业务发放支持两端敏捷发放，很好地解决了多厂商插花组网；业务跨域简化为路由跨域；业务E2E部署，无逐段复杂的状态联动，OAM和可靠性方案得到极大简化。

4.4.2.SRv6实现方案



28.EDD到EDD的企业专线端到端业务承载方案

1.网络部署EDD，用户通过EDD接入承载网，接入方式采用VLAN

2.EDD作为业务接入点，根据接入VLAN进入EVPN

3.EDD支持SRv6，EVPN采用SRv6承载，实现端到端EVPN

4.承载网不支持SRv6支持IPv6时，EDD到EDD采用BE方式承载业务

5.承载网支持SRv6时，EDD到EDD可以采用Policy方式承载业务

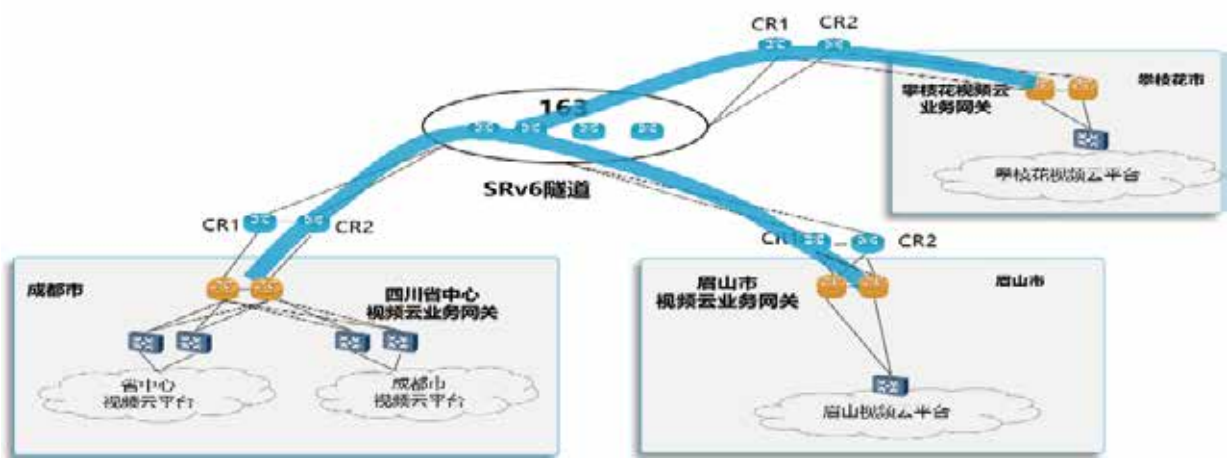
通过E2E SRv6能实现端到端SRv6，承载网不感知业务，简化网络部署；利用SRv6 Policy可以提供SLA保障；有利于承载网从传统网络逐步演进到SRv6。

4.4.3.实际案例及亮点介绍

中国电信四川公司视频云平台是一个高性能综合视频平台，省中心和地市视频平台间通过视频专线实现业务互访。该业务要求网络提供跨骨干的业务通道，需满足快速开通、大宽带、弹性扩容、业务可视、业务安全等多种诉求。

中国电信四川公司联合华为推出SRv6 视频云专网承载方案：首先对成都和眉山的视频平台出口路由器设备进行升级来使能SRv6功能，穿越电信163骨干网打通SRv6隧道；视频云平台出口路由器间部署L3VPN专线承载于该隧道上，业务路径中间节点设备只做IPv6转发，从而实现

两地间视频云业务的快速开通。当前该方案在四川省内已向攀枝花等地推广，在国内江苏电信视频专网、广东联通跨域组网专线和上云专线等也以此方案为基础适配业务场景进行了现网试点部署。

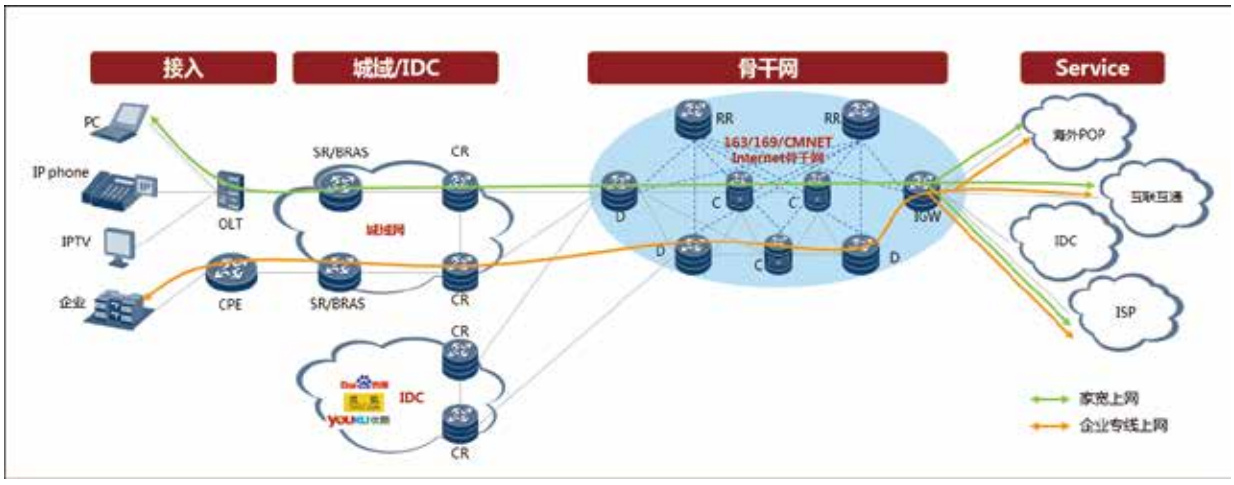


29.中国导电性四川公司视频云专线

4.5.骨干网业务场景

4.5.1业务场景需求介绍

当前三大T骨干网主要承载家宽、手机上网、以及政企专线、大客户互联网专线接入，DCI等业务。当前网络中全部为Native　IP流量，骨干设备数量少，流量大，无QoS，提供的主要是“尽力而为”服务，可靠性主要依赖负载分担以及协议硬收敛。



30.骨干网业务承载示意图

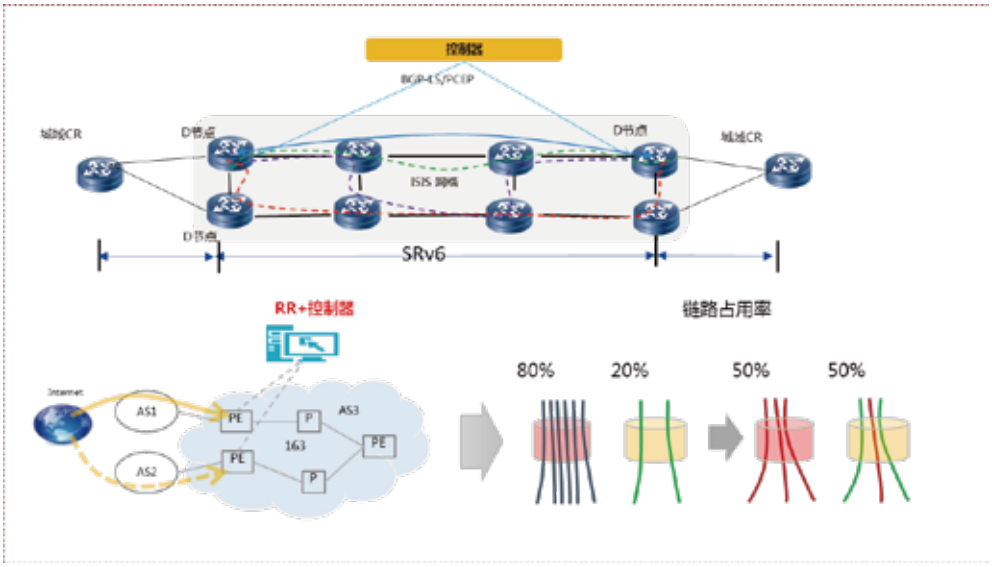
如何为不同价值的用户提供差异化的服务，比如为高价值用户提供无拥塞、大带宽、低时延的流量转发路径，实现增收；另外骨干网内IP转发，如何充分利用带宽资源、负载均衡、降低费用成本是很多运营商面临的问题。

4.5.2.SRv6实现方案

一. 提高骨干网链路利用率的方案

控制器收集骨干网络拓扑和带宽，时延等信息，规划出不同的隧道。控制器向骨干网域设备下发SRv6-TE隧道信息。IP报文迭代入隧道。

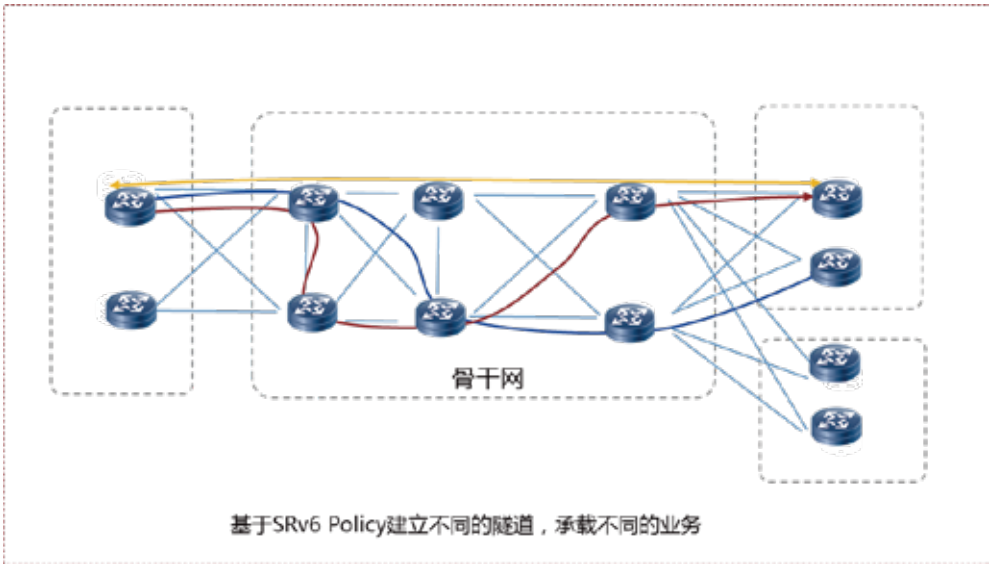
这种方式能避免根据cost选路造成的业务流量集中在某些链路上，其他链路空闲，负载不均衡的问题，提高骨干网络链路利用率。



31.SRv6 TE 在流量调优上的应用

二. 骨干网提供差异化服务能力方案

在骨干网域内部署端到端的SRv6-TE隧道，不同业务报文迭代入不同SLA属性的隧道，满足不同用户的带宽、时延诉求。



32.基于SRv6 Policy的业务承载

5.总结

在过去的十多年里，IP技术取得了巨大成功，统一了网络承载，可以将其称之为All IP 1.0时代。这其中MPLS扮演了非常重要的角色。基于MPLS的承载技术用于IP 骨干承载，再到城域承载、移动承载，替代了帧中继、ATM、TDM等多种网络技术，实现了网络承载技术的统一。MPLS成功依赖于三个重要的特性：VPN、TE和FRR，因此SRv6技术发展首先要把这三个特性优势继承下来，经过两年多的发展，这个目标已经基本达成。

All IP 1.0成功的同时也带来了一些问题和挑战，总结起来主要有三个方面，IP承载网络的孤岛问题、IPv4与MPLS封装的可编程空间有限、应用与网络承载解耦的现状。这些问题导致网络自身的优化困难，而且难以提升价值。

33.IP技术发展代际

SRv6技术的出现，实际承担了解决这些关键问题的使命：

第一个是SRv6兼容IPv6路由转发，基于IP可达性实现不同网络域间的连接更加容易，无需像MPLS那样必须引入额外信令、需要全网升级。

第二个是基于SRH能够支持更多种类的封装，可以很好地满足新业务的多样化需求。

第三个是SRv6对于IPv6的亲和性使得它能够将IP承载网络与支持IPv6的应用无缝融合在一起，通过网络感知应用，给运营商带来更多可能的增值。

IPv6发展的二十年的历程证明，仅仅依靠地址空间的需求不足以支撑其规模部署，SRv6技术快速发展的实践说明通过新的业务应用可以更好地促进IPv6发展应用。随着5G、物联网、云等业务的发展，更多网络设备的接入对于地址扩展的需求也在增加，SRv6和这方面的需求结合在一起，将会推动网络进入一个新的All IP时代，基于All IPv6实现智简网络。

6.缩略语

A 缩略语

缩略语	英文名称	中文名称
BFD	Bidirectional Forwarding Detection	双向转发检测
BIER	Bit Index Explicit Replication	位索引显式复制
CDN	content delivery network	内容分发网络
DETNET	Deterministic Networking	确定性网络
IDC	Internet Data Center	互联网数据中心
iFIT	in-band Flow Information Telemetry	随路检测
QOS	quality of service	服务质量
SFC	service function chain	业务功能链
SR	Segment routing	段路由
SRH	segment routing header	段路由扩展头
SRv6	IPv6 Segment Routing	IPv6段路由
TI-LFA	Topology-Independent Loop-free Alternate FRR	拓扑无关的无环替换路径快速重路由
VR	virtual reality	虚拟现实