金融行业
SRv6 SD-WAN
技术白皮书

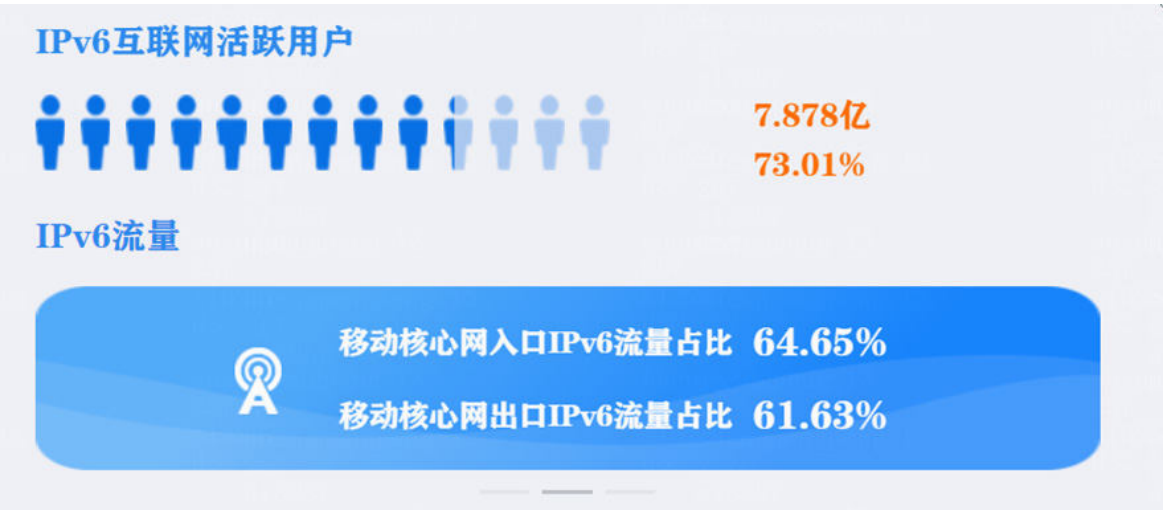
目 录

前言

随着金融行业数字化转型的深入推进，金融服务对高质量网络的需求日益增强，尤其在速度、可靠性和安全性等方面提出了更高要求。然而，传统 IP/MPLS 网络架构在应对快速增长的业务和日益复杂的网络环境方面，逐渐显现出不足。

与此同时，我国在推广 IPv6 方面取得了显著进展。如图 1 所示，根据国家 IPv6 发展监测平台的数据显示，截至 2024 年 5 月，IPv6 活跃用户数量已达 7.878 亿，占比达到 73.01%，这一成果在全球范围内处于领先地位。这一趋势表明 IPv6 技术的广泛接受和应用，为金融行业网络技术的未来演进指明了方向，预示着新一代网络技术的广泛应用将为金融服务带来革命性的变革。

图1 中国 IPv6 综合发展指数



在 IPv6 广泛部署的背景下，SRv6 SD-WAN（Segment Routing over IPv6，基于 IPv6 的段路由和 Software Defined Wide Area Network，软件定义广域网）技术作为一种先进的网络解决方案，充分利用了 IPv6 的扩展能力，不仅具备传统 SD-WAN 的灵活性和成本效益，还提供更加细致的流量管理、卓越的安全性以及更高的网络操作灵活性。

SRv6 SD-WAN 之所以具有显著优势，主要得益于其对 IPv6 的全面支持。这不仅使得 SRv6 SD-WAN 在处理复杂网络流量时更加高效，还增加了网络的安全性和易于管理性，从而满足现代金融服务日益增长的网络需求。

本白皮书旨在深入探讨 SRv6 SD-WAN 在金融行业的关键应用，并在 IPv6 广泛推行的大背景下，探索如何利用此技术优化金融机构的网络架构，以满足当前及未来的业务需求。同时，为金融行业的决策者和技术专家提供有价值的洞察和启示，共同推动金融行业持续向前发展。

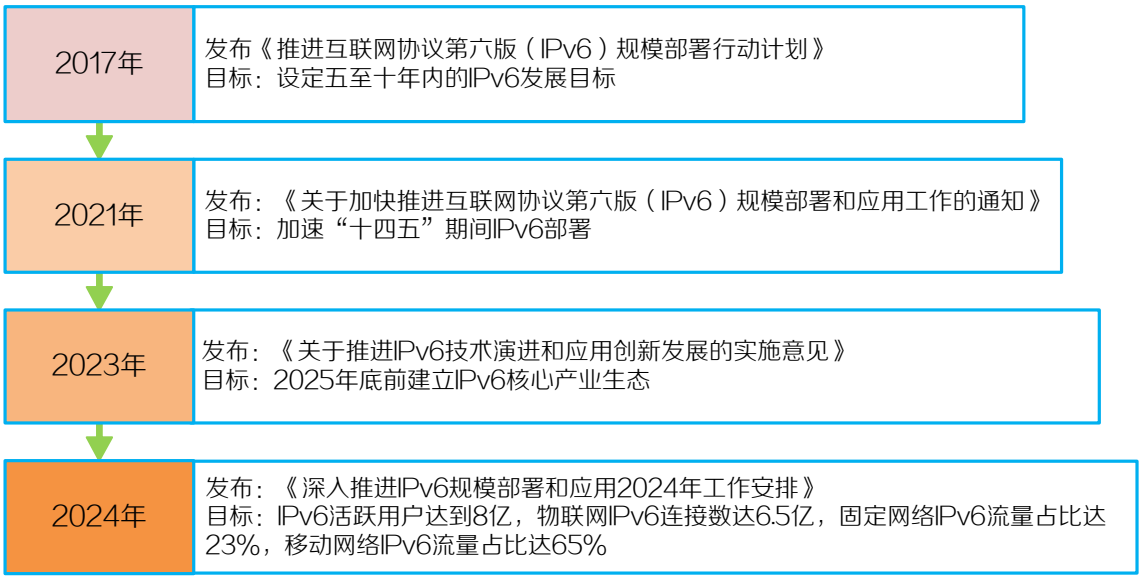
政策背景

1 国家政策

我国的 IPv6 技术发展迅速，用户数和流量占比稳步上升。国家政策大力支持 IPv6 的推广，为金融行业网络的 IPv6+ 转型提供了坚实的政策基础。如图 2 所示，工业和信息化部、中央网络安全和信息化委员会以及国家发展和改革委员会等多部门，已发布了一系列政策和指导意见，旨在推动 IPv6 的全面部署和应用。例如：

- 2017 年，中共中央办公厅和国务院办公厅共同发布《推进互联网协议第六版（IPv6）规模部署行动计划》，设定了我国在未来五至十年内基于 IPv6 的下一代互联网发展的综合目标和实施路径。
- 2021 年，中央网信办联同国家发展改革委和工信部发布《关于加快推进互联网协议第六版（IPv6）规模部署和应用工作的通知》，加快“十四五”期间 IPv6 的部署工作。
- 2023 年，工信部与其他七部门共同发布《关于推进 IPv6 技术演进和应用创新发展的实施意见》，旨在 2025 年底前初步建立以 IPv6 技术为核心的产业生态。
- 2024 年，中央网信办等部门在《深入推进 IPv6 规模部署和应用 2024 年工作安排》中明确了 2024 年的具体目标：力求到年末 IPv6 活跃用户达到 8 亿，物联网 IPv6 连接数达 6.5 亿，固定网络 IPv6 流量占比达 23%，移动网络 IPv6 流量占比达 65%。同时，IPv6 网络性能将显著提升，云服务和数据中心将默认开启 IPv6 功能，主要商业网站和移动应用的 IPv6 支持率预计达到 95%，IPv6 的行业应用将更加广泛深入。

图2 主要 IPv6 相关的国家政策



自党的十八大以来，随着互联网与社会经济的深度融合，网络强国战略逐步得到推进。党的二十大报告中多次提到互联网，强调要建设现代化产业体系，优先发展实体经济，加速推动新型工业化，以及加快建设制造强国和数字中国等战略目标。网络基础设施的建设是实现这些战略目标的关键，当前我国的网络基础设施正在全面向 IPv6 时代迈进，IPv6 不仅提升了互联网的承载能力和安全性，也显著提高了服务质量，成为支撑国家战略成功实施的重要基石。

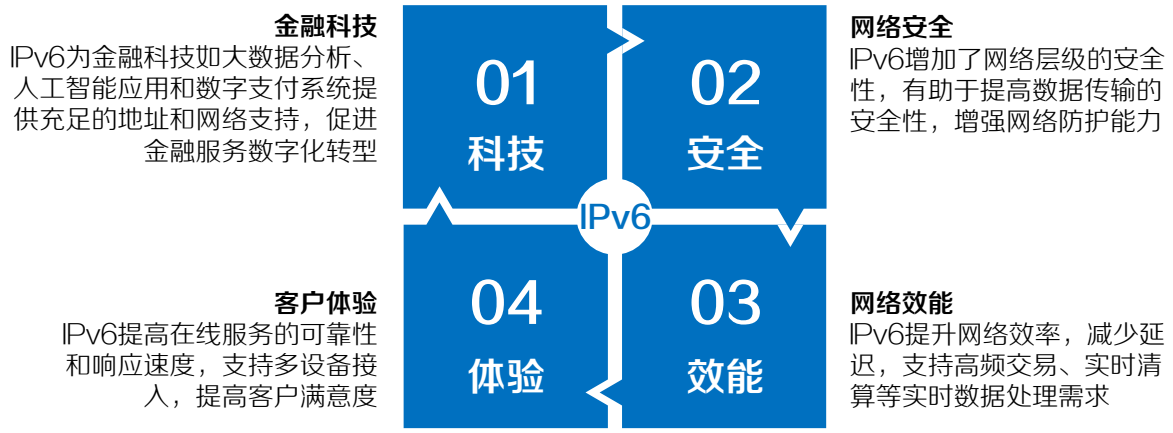
2 行业政策

IPv6 规模部署是互联网演进升级的必然趋势和技术产业创新发展的重要机遇。对于金融行业来说，IPv6 的规模部署不仅构建了实现下一代网络规划的新平台和新路径，同时也在金融科技创新、网络安全加固、数据处理能力增强以及客户体验提升等方面创造了新的可能性，如图 3 所示。在国家政策的大背景下，金融行业的具体指导政策也相继出台。例如：

- 2019 年 1 月，中国人民银行、中国银行保险监督管理委员会、中国证券监督管理委员会联合发布《关于金融行业贯彻〈推进互联网协议第六版（IPv6）规模部署行动计划〉的实施意见》，为金融行业 IPv6 规模部署提供了指导方向和前进路线。
- 2022 年，中国人民银行印发《金融科技发展规划（2022-2025 年）》——金融与科技加快深度融合，全面推进互联网协议第六版（IPv6）技术创新与融合应用，实现从能用向好用转变、从数量到质量转变、从外部推动向内生驱动转变。

一系列政策的实施为金融行业在网络升级方面提供了明确的方向和强有力的支持。这些政策不仅引导金融机构在日常运营中采用 IPv6 技术，还在战略层面强调了在构建现代化金融体系中 IPv6 发挥的关键作用。通过这些政策的支持，金融行业能够更好地规划其技术路线图，提升网络安全性和服务质量，为未来的技术创新奠定基础。

图3 行业政策目标



技术演进与行业现状

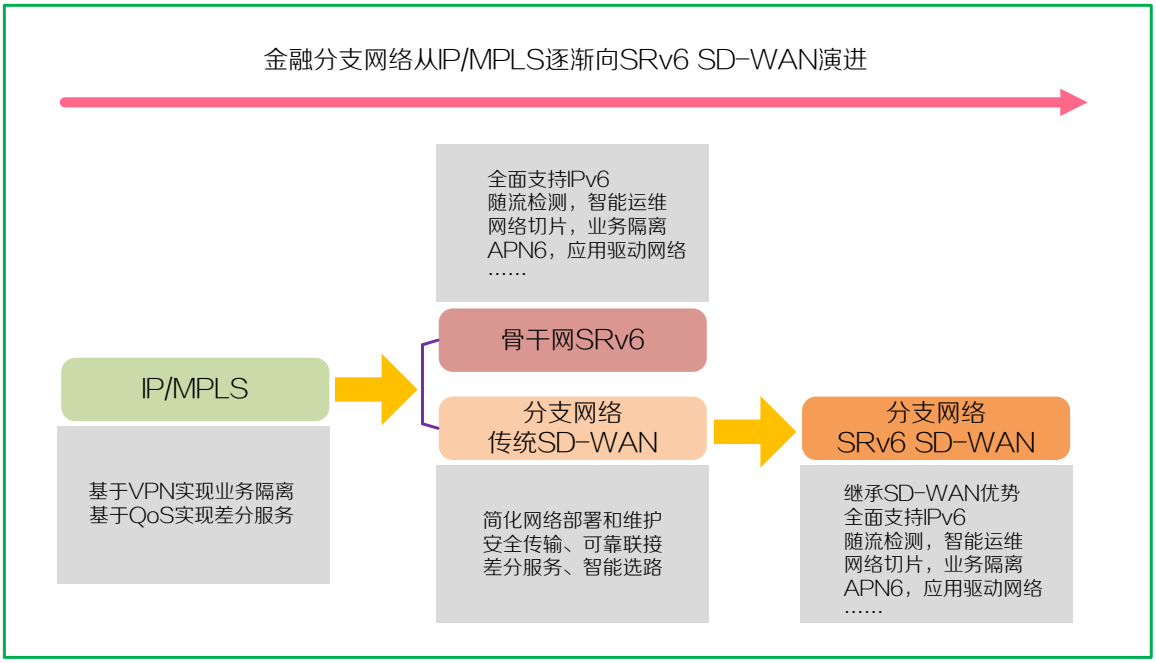
1 从IP/MPLS到SRv6 SD-WAN的技术演进

如图 4 所示，金融行业的网络技术经历了从早期的 IP/MPLS 技术到更先进的 SRv6 SD-WAN 技术的多个创新阶段。每个阶段都标志着金融网络解决方案始终向更灵活、更高效的方向发展。

- **IP/MPLS（起点）**：最初，IP/MPLS 技术为金融网络提供了业务隔离和服务质量的基础支持，构建了金融网络的初步框架。然而，随着业务需求的增加和网络复杂性的提升，IP/MPLS 的局限性逐渐显现，特别是在处理更复杂的业务需求时。
- **分支网络传统 SD-WAN**：随着 SD-WAN 技术的引入，金融行业的分支网络管理方式得到了重大革新。SD-WAN 技术通过优化路由选择和简化网络管理，为分支网络带来了更高的灵活性和效率。这一技术转变不仅提高了服务质量，还加快了业务响应速度，特别是在面对分散的分支网络时。SD-WAN 的应用使金融机构能够更加灵活地处理网络流量，并确保关键业务的稳定运行。
- **骨干网 SRv6**：随着技术的进步，骨干网络逐渐升级到 SRv6，这一变革相比传统 IP/MPLS 网络架构带来了显著的改进和优势。SRv6 通过简化网络架构和无状态操作，减少了对专用协议的依赖，从而简化了网络维护。此外，该技术增强了网络的灵活性、可扩展性、安全性和性能，并支持细粒度服务，如网络切片。SRv6 提供了一种更加高效、灵活且具未来兼容性的网络架构选择，更好地应对了不断增长的数据流量和服务需求。
- **分支网络 SRv6 SD-WAN**：在金融行业的分支网络中，SRv6 SD-WAN 技术的诞生标志着传统 SD-WAN 解决方案的进一步演进。该技术通过结合 IPv6 的先进功能，如 iFIT 随流检测、智能运维和网络切片，显著提升了网络的性能和安全性，并为金融机构提供了更高的灵活性。这些创新技术允许金融机构动态分配网络资源，并更精确地管理和优化高优先级业务流。这确保了关键业务的高效和稳定运行，从而有效应对不断变化的市场需求和技术挑战。

未来，随着技术的不断演进和升级，将推动金融行业网络朝着更加智能化和自动化的方向发展，提升金融服务的安全性、效率和灵活性，帮助金融机构更好地适应市场变化，并在竞争中保持领先。

图4 从 IP/MPLS 向 SRv6 SD-WAN 演进



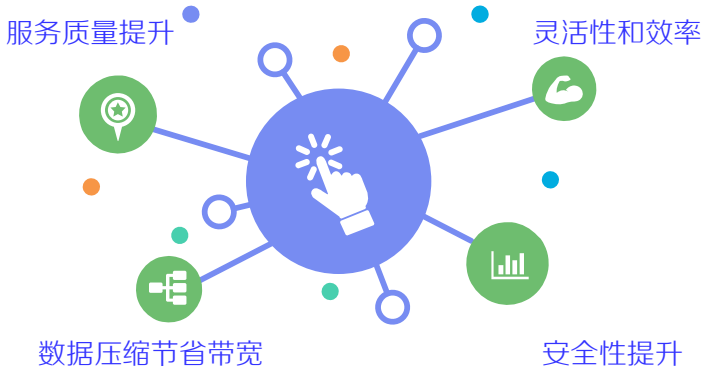
2 当前发展现状及面临的挑战

2.1 发展现状

金融行业正在经历一场由市场需求和技术进步双重推动的深度转型。随着数字化转型的不断推进，网络技术的进步已成为支撑金融服务连续性、数据安全性和业务可靠性的重要保障。现代客户对金融服务的期望不断提高，这促使金融机构在提升网络基础设施的灵活性、效率和安全性方面不断努力。当前，基于 IPv4 的 SD-WAN 技术在金融行业得到了广泛应用，取得了以下显著进展：

- **服务质量提升**：SD-WAN 通过优化路径选择和带宽管理，大幅提升了服务质量和网络性能。
- **灵活性和效率**：SD-WAN 技术提供的动态路由和集中管理功能，使得金融机构能够更灵活、高效地管理其网络资源。
- **数据压缩节省带宽**：SD-WAN 技术的高效数据传输压缩策略显著减少了在传输过程中所需的带宽，从而减轻了对昂贵专线资源的依赖并降低了相关成本。这种优化不仅提高了数据处理速度，还增强了整体网络的传输效率，确保了关键金融操作的连续性和响应速度。
- **安全性提升**：通过虚拟专用网络（VPN）和先进的加密技术，SD-WAN 提升了网络的安全性。

图5 发展现状



2.2 面临的挑战

在推动金融行业数字化转型的过程中，基于 IPv4 的 SD-WAN 技术虽然取得了显著进展，但随着业务的扩展和业务需求的多样化，金融机构面临一系列新的挑战。这些挑战包括但不限于：

- **服务连续性和可靠性要求**：高频交易和实时数据分析需要非常稳定且无中断的网络。任何网络故障都会导致重大的财务损失，因此对网络的连续性和可靠性要求极高。
- **带宽需求的快速增长**：随着业务量的增加以及更多云服务的使用，网络带宽需求迅速增长。这不仅增加了成本，还可能影响网络的性能和服务质量。
- **网络安全与保障**：金融行业必须应对不断增长的网络攻击威胁，并始终确保网络安全。
- **客户体验的持续改进**：在竞争激烈的市场中，金融机构必须不断提升客户体验。任何网络延迟或服务中断都可能直接影响客户满意度和忠诚度。
- **网络管理复杂性**：随着金融服务的数字化和全球化扩展，网络架构变得越来越复杂。管理如此多层次、多技术的网络环境需要专业的技术和知识。传统网络缺乏实时监控工具，难以掌握分支网络状态和管理信息。当网络出现问题时，分支网络的故障响应和维护都很困难，直接影响了客户的服务质量。
- **智能调度与扩展能力不足**：现有基于 IPv4 的 SD-WAN 技术在智能调度和设备响应速度方面存在局限。无法及时开通临时测试业务和实现智能选路策略，使得应对网络故障和劣化的能力不足，影响了业务连续性和可靠性。此外，当前集中式控制方案在处理大规模网络时遇到了挑战，新的分支扩展变得复杂且昂贵，显现出扩展能力的不足。
- **统一协议栈与跨域互联的困难**：目前分支网络的 IPv4 SD-WAN 架构面临着与骨干网络的 SRv6 无法有效协同工作的问题，特别是在利用 IPv6+网络和跨域技术方面。这种不匹配导致分支网络的 IPv4 与骨干网络的 SRv6 之间难以实现无缝连接和统一网络协议栈的构建。由此带来的复合挑战是，尽管 IPv6+网络和跨域技术本身提供了网络管理的简化和增强的灵活性，但由于技术整合的不足，金融机构在快速部署业务和高效运营方面仍面临显著障碍。

图6 面临的挑战

这些挑战虽然凸显了当前 SD-WAN 技术在金融行业中的局限性，但同时也促进了金融网络向简单、安全、可靠和高效等方向的不断发展。这加快了金融机构对创新网络技术的探索步伐。

面对这些复杂挑战，新一代的 SRv6 SD-WAN 技术应运而生。通过整合 IPv6+技术，它不仅提供了更高效和更安全的解决方案，还增强了网络的适应性，满足了金融行业对日益增长的网络性能需求。

SRv6 SD-WAN 创新技术解决方案

1 方案简介

在金融行业，网络的灵活性、安全性和效率是推动数字化转型和满足不断增长的业务需求的关键因素。然而，随着技术的快速发展和业务需求的不断变化，这些领域也面临着新的挑战。为了应对这些新时代的挑战，H3C 提出了一种创新的解决方案——SRv6 SD-WAN。该方案综合了 SD-WAN 的众多优势，并融合了 IPv6+的创新技术，旨在为金融行业构建一个更加安全、高效且灵活的网络环境。

SRv6 SD-WAN 解决方案的核心优势在于其能够提供端到端的网络路径优化、智能流量管理和增强的网络安全保护。该方案通过利用 SRv6 技术的独特能力，为金融机构的网络通信提供了无缝且高度可靠的连接，同时大幅提升了数据传输的效率和安全性。这些能力帮助金融机构更好地适应市场的快速变化，支持包括高频交易和分布式应用在内的各种金融业务。

为帮助读者全面了解 SRv6 SD-WAN 解决方案，接下来，在详细介绍方案内容之前，本文将先简要概述 SRv6 技术和 SD-WAN 技术，以及二者结合所带来的优势。

2 技术概述

2.1 SRv6 技术

什么是 SRv6?

SRv6（Segment Routing over IPv6）是一种基于 IPv6 的先进路由技术，它通过利用 IPv6 的 SRH（Segment Routing Header）扩展头来实现端到端的路径控制和网络编排。SRv6 的核心是“段”（Segment），即预定义的网络路径信息，这些路径可以嵌入到 IPv6 数据包的 SRH 中，从而创建一个灵活且简化的路由环境。SRv6 允许网络操作员通过将多个段组合成一个“Segment List”，来精确控制数据包在网络中的流动路径。每个段对应一个特定的网络操作，比如转发、服务链等。通过这种方式，SRv6 不仅优化了网络资源的利用，提高了服务质量，还简化了网络复杂性。

接下来，采用一个类比的例子来通俗解释其工作原理。如图 7 所示，想象一下，有一位邮局的邮件分拣员，每天需要将大量的信件和包裹准确无误地送达到不同的目的地。在旧系统中，这位分拣员必须依赖复杂的手册和指引来确定每个包裹的路线，这个过程不仅费时，而且容易出错。现在，有了一种新的技术，叫做 SRv6。

假设每个包裹上贴有一个特殊的条码。这个条码不仅指明了目的地，还包含了详细的路线信息——包括哪个邮递员接手、哪辆车负责运送，以及寄件客户和收件客户的 VIP 等级（类似于网络中的用户分组）、包裹类型（对应网络中的应用业务分类）、客户对物流运输时限的特殊要求以及运输过程中的具体需求（类似于网络中的时延和丢包要求），并且还有每个中转站的详细信息。当分拣员扫描这个条码时，所有必要的路线信息立刻清晰展现。这样，分拣员无需查阅任何手册，也不必担心包裹被误送。邮件处理流程因此变得更快、更准确，整个邮局的运作效率也得到显著提高。

图7 SRv6 数据传输示意图

这就像 SRv6 技术在网络世界中的运作方式。在 SRv6 中，每个数据包就相当于带有条码的包裹，而这些条码里面编码了数据包在网络中的精确路径（或称为“段”）。网络设备通过读取这个“条码”（IPv6 地址），就能了解如何处理和转发数据包。这样，数据包就可以沿着预定义的路线安全、高效地到达目的地。

因此，SRv6 就像是网络世界的高效“邮递系统”，让数据包的传输变得更快、更准确、更安全。

为什么需要 SRv6?

传统网络的困局

随着互联网和云计算的飞速发展，网络规模和复杂性不断增加，传统 IP/MPLS 网络在满足多样化业务需求方面遇到了诸多问题：

- **网络孤立问题**：尽管 MPLS 有助于统一骨干网，但 IP 骨干网、城域网和移动骨干网仍然是彼此独立的 MPLS 域。不同域间的连接需要复杂的 VPN 技术，这导致端到端业务的部署变得非常复杂。与此同时，当 L2VPN 和 L3VPN 业务同时存在时，设备上需要运行多种协议（如 LDP、RSVP、IGP、BGP），增加了管理的复杂性，不适合大规模业务的部署。
- **IPv4 与 MPLS 的局限**：许多新业务要求在转发层面添加更多的转发信息，但 IETF 已经停止为 IPv4 制定新标准。此外，MPLS 的 20 比特标签空间有限，且标签字段固定，缺乏灵活性，难以满足未来业务的需求。
- **应用与网络的脱节**：由于应用和骨干网络的分离，导致网络优化变得困难，运营商难以从增值业务中获益。缺少应用层信息，导致只能进行粗放的网络调度，造成资源浪费。尽管 MPLS 曾试图更加靠近主机和应用，但由于复杂的管理和多重边界等问题未能成功。
- **紧耦合的控制面和数据面**：传统网络的控制面和数据面紧密耦合，导致业务上线周期长，难以快速响应新兴业务的需求。

以上问题表明，传统 IP/MPLS 网络面临许多无法忽视的挑战，这些挑战需要新的技术方案来应对。

SRv6 技术价值

作为一种创新的网络技术，SRv6 超越了依赖传统复杂协议的局限，通过简化网络操作和提升整体性能，为各行业带来显著的价值：

- **简化网络操作和架构**：SRv6 通过将路径信息直接嵌入到数据包的 SRH 扩展头中，使得网络设备只需读取这些信息即可完成路由决策。这大大简化了路由表的管理和配置，网络管理员无需手动进行大量复杂的配置。同时，网络设备不再需要存储和维护复杂的路由信息，减少了设备配置和管理的复杂性，从而降低了网络维护的难度。这类似于邮递员只需扫描包裹上的条码即可确定投递路线，而无需查阅复杂的手册。
- **增强数据传输安全性与服务支持**：数据包严格按照设定路径传输，犹如快递只能按照条码上的路线送达，这样可以防止误投和恶意拦截；同时，结合 IPv6 的安全特性，提供更细致的服务保护数据安全。
- **灵活的服务创新**：SRv6 允许网络操作员灵活地设置特定服务或应用的专属传输路径。例如，可以为特定应用的高优先级流量快速创建一条专有路径，提升服务质量，类似于为紧急快递开辟一条高速运输通道。
- **提高网络性能与效率**：通过预定义并优化数据包的传输路径，SRv6 能够显著减少传输延迟，提高数据传输速度，确保数据包更快速、准确地到达目的地。
- **未来兼容性**：随着网络技术的不断发展，SRv6 能够适应新兴技术如 5G 和物联网，就像邮局能够适应新的物流技术一样。

图8 SRv6 的技术优势

综上所述，SRv6 凭借其灵活性、高效性和简洁性，为各种类型的网络环境带来了显著改进。这不仅提升了网络管理的便捷性和数据传输的安全性，同时也为金融机构创造了更多创新的可能性。SRv6 不仅是构建智能、简洁 IP 网络的关键工具，还有助于推动 IPv6 的发展，开启面向未来的 IPv6+时代。

2.2 SD-WAN 技术

什么是 SD-WAN?

软件定义广域网（SD-WAN，Software Defined Wide Area Network）是一种将软件定义网络（SDN）技术应用于广域网络的解决方案。它通过网络控制器来管理和优化跨多个连接方式的数据传输，使企业能够实现高效的分支机构、总部和多云环境的互联。

SD-WAN 技术支持多种链路选项，如 MPLS、Internet、5G 和 LTE，并且能够根据当前网络需求和应用类型选择最佳路径进行数据传输。这不仅改善了上云体验，还大幅提升了网络的可靠性、灵活性以及运维效率，从而确保业务的连续性和稳定性。

为什么需要 SD-WAN?

传统 WAN 架构面临诸多挑战，以下通过一个具体案例来阐述这些挑战及 SD-WAN 的优势。

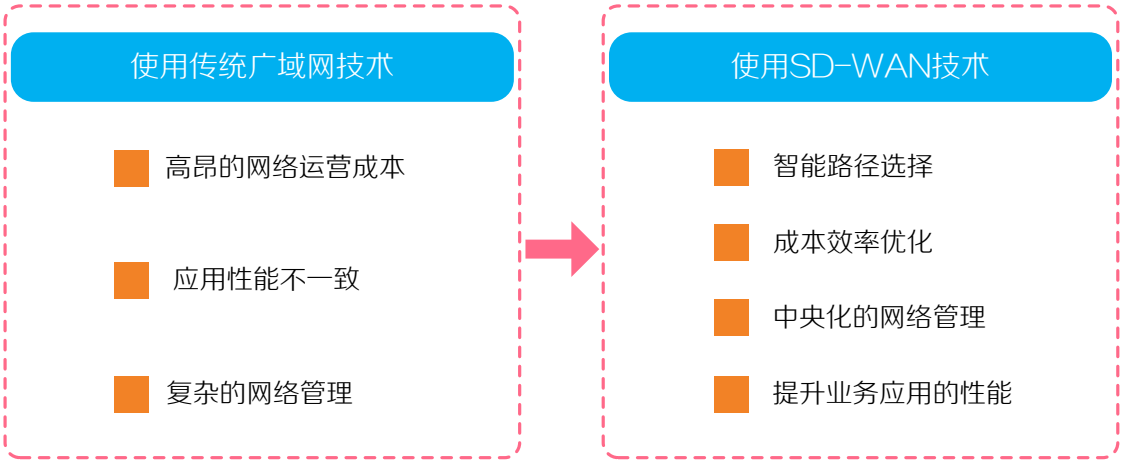
有一家全国性的银行，其分支网络覆盖多个城市和地区。这家银行的业务不仅包括传统的银行服务，还包括在线银行业务，以及与金融科技应用的实时数据交换。如图 9 所示，在使用传统广域网技术的情况下，银行面临以下挑战：

- **高昂的网络运营成本**：所有分支的网络流量都必须经过中心数据中心，主要依赖昂贵的 MSTP 线路，增加了总体网络成本。
- **应用性能不一致**：尤其是金融交易和实时数据处理要求极低的延迟，传统 WAN 在远程分支的应用性能上往往难以满足需求。
- **复杂的网络管理**：由于分支众多，传统网络架构下的配置和维护工作繁重，难以实现快速的策略调整和故障排解。

为了解决这些问题，银行决定采用 SD-WAN 技术。通过部署 SD-WAN，银行实现了以下改进：

- **智能路径选择**：SD-WAN 能够实时监测 MSTP 等各种传输线路的性能，并根据当前网络条件自动选择最佳的数据传输路径。对于需要极低延迟的高优先级金融交易，系统优先选择延迟最低的路径，而对于非关键性应用，则可以利用成本效益更高的线路，确保资源的高效利用。
- **成本效率优化**：SD-WAN 通过实时监控和动态调整各专线的带宽利用情况，有效地为不同业务需求选择最适合的传输线路。这种动态带宽管理不仅平衡了各线路的负载，还大幅提高了网络的带宽利用率，从而优化了成本效益。
- **中央化的网络管理**：SD-WAN 允许银行通过一个中央化的控制平台管理所有分支的网络配置，简化了网络操作，提高了运维效率。
- **提升业务应用的性能**：通过智能的带宽管理和流量优先级设置，SD-WAN 确保了关键业务应用，如实时交易处理和客户数据分析等，始终获得必要的网络资源，从而提升了整体的业务效率和客户满意度。

图9 应用 SD-WAN 的优势



通过应用 SD-WAN，这家银行成功地提升了网络的灵活性和性能，降低了成本，并加强了网络的安全性和可靠性。这种现代化的网络解决方案不仅优化了日常运营，也为银行在数字化和金融科技领域的进一步发展奠定了基础。

2.3 SRv6 SD-WAN 技术

什么是 SRv6 SD-WAN?

SRv6 和 SD-WAN 的结合为金融行业提供了一种强大的网络解决方案，称为 SRv6 SD-WAN。这种整合方案集成了 SRv6 和 SD-WAN 两者的优势，使网络更加智能化和高效。

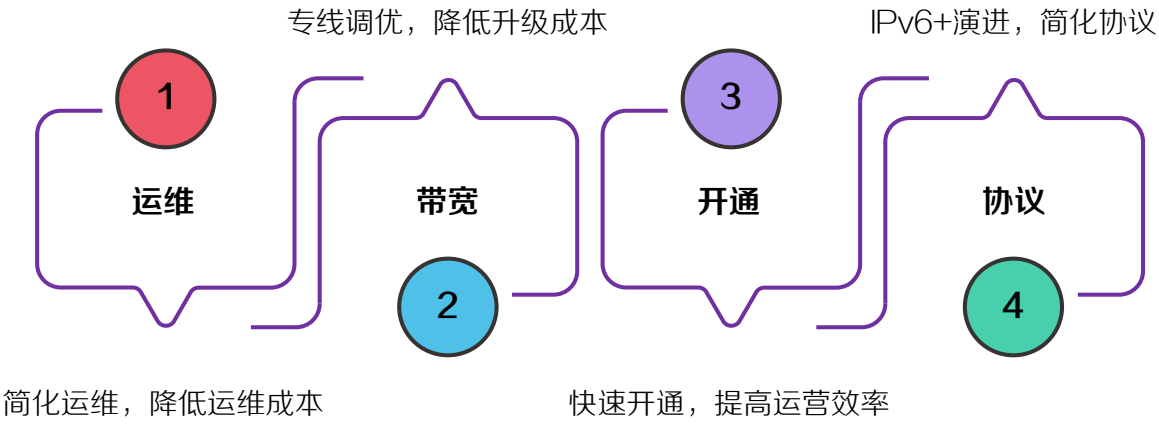
为什么需要 SRv6 SD-WAN?

随着金融行业的迅速发展，网点业务类型逐步向智能化、服务化的新一代金融网点转型。这一转型过程对金融网络提出了新的要求，例如：

- **简化运维，降低运维成本**：金融机构引入大量智能设备增加了业务复杂度，传统的命令行管理方式难以满足需求，运维排障困难。
- **专线调优，降低升级成本**：许多金融业务转移到线上，加上视频和监控业务的增加，对专线带宽产生巨大压力。简单增加专线带宽成本过高，需要更精细化的管理。金融行业也在尝试利用 MV（MPLS VPN）、5G 等技术替代传统专线。
- **快速开通，提高运营效率**：随着智能终端的引入，业务逐步线上化，新业务部署更新频繁，需要降低部署时间，提高业务开通效率。
- **IPv6+演进，简化协议**：金融骨干网基本采用 IPv6+技术路线，未来接入网（即分支网络）需要与骨干网协同发展，利用 IPv6+实现端到端业务管理。

为了满足上述需求，端到端的 SRv6 SD-WAN 方案成为金融行业网络演进的一个重要趋势。

图10 新的网络要求



3 满足金融行业需求的SRv6 SD-WAN解决方案

SRv6 SD-WAN 解决方案通过一张 IPv6 网络统一承载金融业务，采用 SRv6 分段模式和 SD-WAN 控制器端到端开通 VPN，实现业务跨域编排和运维。该解决方案在路径控制与管理、网络性能优化、安全性、成本效益等方面结合了 SRv6 和 SD-WAN 的优势，尤其适合金融行业的需要。

表 1 详细介绍了 SRv6 和 SD-WAN 这两种技术各自的独特优势，并展示了当二者结合使用时，能够带来的综合优势。这种综合优势能够为金融行业提供一个更加强大、灵活、安全且成本效益高的网络解决方案，特别适合需要高度安全、高效率且能够快速适应业务变化的金融服务行业，使得网络运维更加简化，同时保证了业务的连续性和数据的安全性。

表1 SRv6 与 SD-WAN 的技术优势及其结合优势

特性/技术	SRv6	SD-WAN	综合优势（SRv6 + SD-WAN）
安全性	利用IPv6的安全特性，提供路径固定与数据加密	端到端加密和综合安全策略控制	结合SRv6的固定路径和SD-WAN的加密策略，显著提升数据传输安全性；SRv6通过固定路径减少数据泄露风险，SD-WAN则实现端到端加密，共同为金融数据提供多层安全保护，特别是增强对抗网络攻击和数据泄露的能力
服务质量（QoS）	通过精细的路径控制确保服务级别	基于应用的带宽和优先级管理	实现更精细和动态的服务质量管理，通过结合两种技术优化关键业务应用的性能，满足多样化的金融业务需求
路径控制与管理	精确的端到端路径控制，通过预定义的“段”进行编码	路径选择的自动化和优化，中央控制功能	结合SRv6的精确路径控制与SD-WAN的自动化功能，提供高效、灵活的流量管理，实现网络流量的高度控制和实时可视性
网络性能优化	通过优化网络资源利用和减少延迟提高服务质量	智能路径选择，根据实时网络状况动态调整，优化服务质量	动态优化服务质量，根据应用需求和网络条件调整，保证关键应用的性能，同时减少无效或冗余的数据传输
成本效率	通过简化网络架构减少	减少对昂贵专线的	长期成本效益显著，通过智能路径选择和

特性/技术	SRv6	SD-WAN	综合优势（SRv6 + SD-WAN）
	对复杂设备的依赖，降低维护成本	依赖，优化带宽使用	网络资源优化，实现成本节约，同时简化网络操作和管理
自动化与简化管理	网络策略的自动化部署	集中化的管理和策略推送	提高网络可视性与控制，简化管理并减少配置错误
灵活性与扩展性	支持网络编排，快速适应服务变化；兼容未来技术如5G和物联网，适应大规模网络和服务	支持多种连接类型，易于扩展和调整网络配置以适应各种网络条件，快速适应变化的业务需求	通过结合SRv6的固定和预定路径优势与SD-WAN的网络管理灵活性，提供高度的网络自定义能力和扩展性；这使得网络能够有效地适应快速变化的业务需求和技术发展，特别适合于需要高度可定制化和快速扩展的金融行业环境
技术支持与兼容性	适应现代网络需求，支持5G和物联网等新技术	适应多云和混合云环境，支持企业数字化转型	保证长期的技术支持和适应未来技术发展，如AI和大数据分析的集成，为金融机构在数字化和金融科技领域的进一步发展奠定基础

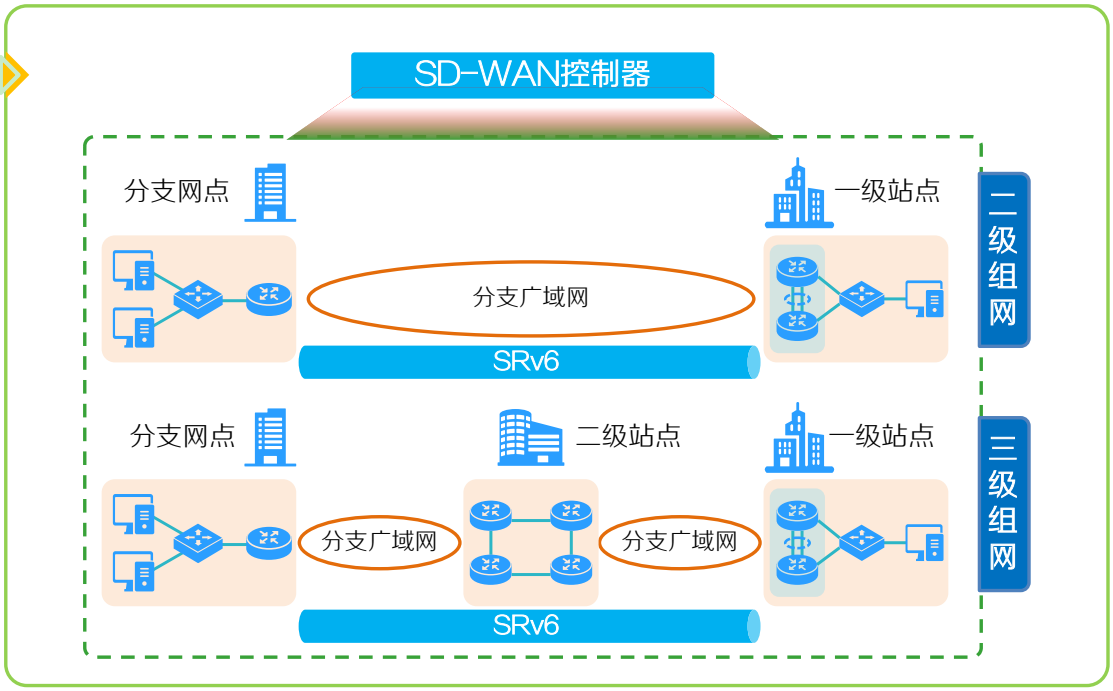
4 适用场景

随着用户的 SRv6 骨干网建设的完成，当前的需求已转向分支 SRv6 网络的构建。SRv6 SD-WAN 技术解决方案特别适用于金融行业，尤其是需要升级网络基础设施以支持数字化转型的金融机构。此技术解决方案在以下典型应用场景中表现出色，能够帮助金融机构构建更安全、高效和可靠的网络环境，从而支持行业的持续创新和业务增长。

4.1 分支网络单独建设 SRv6（适用于中小型金融机构）

适用于需要在分支机构之间建立高效、安全通信的中小型金融机构。如图 11 所示，通过部署 SRv6 隧道，实现网点、各机构和总部之间一跳连通，极大地简化了网络架构并提高了数据传输的效率。

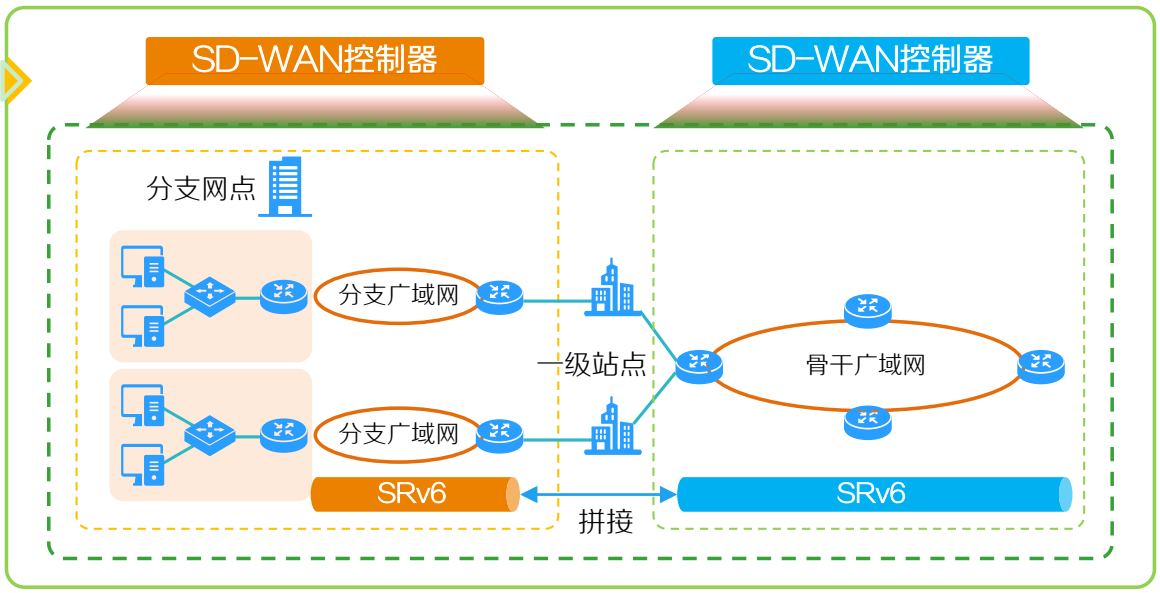
图11 分支网络单独建设 SRv6



4.2 分支网络部署 SRv6 和骨干 SRv6 网络拼接（适用于大型金融机构）

对于拥有广泛地理分布的大型金融机构，SRv6 SD-WAN 提供了一个有效的解决方案来整合分支和骨干网络。如图 12 所示，以省级为例，通过部署 SRv6 隧道实现省内各网点和机构之间一跳连通。同时，分支接入网由分支控制器管理，骨干 SRv6 网络由骨干控制器管理，确保了网络的灵活性和可扩展性。

图12 分支部署 SRv6 和骨干 SRv6 网络拼接



5 方案设计

本章节将介绍如何在不同类型的金融机构中部署 SRv6 SD-WAN 技术，并结合具体的“关键技术”，展示如何通过 SRv6 Policy 实现高效、安全的网络通信。方案设计细分为“分支独立部署 SRv6”和“分支 SRv6 拼接骨干 SRv6”两个核心部分，分别针对不同的网络结构需求。在具体应用过程中，可根据不同的业务需求灵活采用不同的关键技术，以确保整体网络处于最佳运行状态。

5.1 分支独立部署 SRv6

如图 13 所示，对于中小型金融机构，SRv6 SD-WAN 技术的应用包括以下两种组网方案，每种组网方案中均可以结合关键技术，以实现高效、灵活的网络通信。

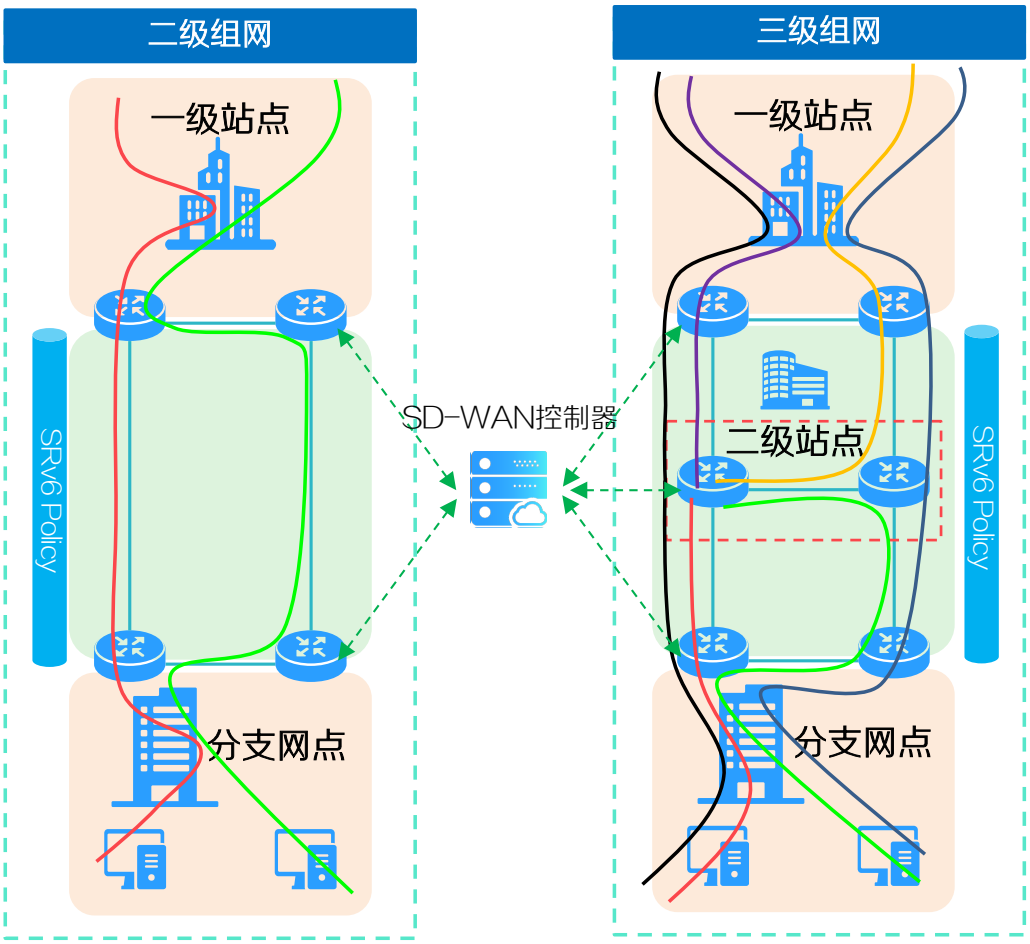
二级组网方案

- 方案概述：该组网场景下，控制器向设备头端下发 2 条 SRv6 Policy，作为 2 条 SD-WAN 隧道。设备头端将基于 iFIT 随流检测结果自主选择 SD-WAN 隧道进行报文转发，实现端到端的高效通信。
- 关键技术：采用智能业务感知与路径调度技术（如 APN6、iFIT 随流检测、分布式智能调度 IPR），实现智能的路径选择和高效的数据传输。

三级组网方案

- 方案概述：三级组网方案在二级组网架构的基础上进行了扩展。控制器向每个分支网点下发 4 条 SRv6 Policy，其中 2 条连接至二级站点，另外 2 条连接至一级站点。同时，向二级站点下发 2 条 SRv6 Policy，从而进一步优化通信路径，提高网络的灵活性和可靠性。
- 关键技术：同样利用智能业务感知与路径调度技术（如 APN6、iFIT 随流检测、分布式智能调度 IPR），实现智能的路径选择和高效的数据传输。

图13 分支独立部署 SRv6



在该分支独立部署 SRv6 方案中，还可以使用带宽优化与效率提升技术（如端到端数据压缩技术、Web Cache 技术）来提高带宽利用率和业务访问速度。此外，零配置开局技术和智能运维可以简化网络部署，提高整体运维效率。

5.2 分支 SRv6 拼接骨干 SRv6

如图 14 所示，在大型金融机构中，分支网络与骨干网络的整合是至关重要的。该方案通过在分支网络和骨干网络各自部署独立控制器，实现网络的分段管理与高效运维。头节点将根据 iFIT 检查结果智能选择 SRv6 Policy 隧道转发报文。

部署策略

在分支网络的一级站点部署下联和上联设备：

- 下联设备：作为分支网络的终结设备，负责 SRv6 业务隧道的终结。
- 上联设备：作为骨干网络的边缘设备，负责分支网络的接入。

拼接方式

分支网络接入骨干网络的拼接方式包括以下几种：

- OptionA 拼接：上下联路由器间采用“背靠背”方式部署，通过 EBGP 引入业务路由，实现跨域互通。
- 两段式拼接：上下联设备间通过 SRv6 Policy 隧道进行直接的数据转发，实现跨域转发。

- 三段式拼接：在下联设备到上联设备间、以及上联设备到骨干网络间分别进行一次路由重生，并在上下联设备间建立 SRv6 BE 隧道，从而实现跨域转发。

图14 分支 SRv6 拼接骨干 SRv6

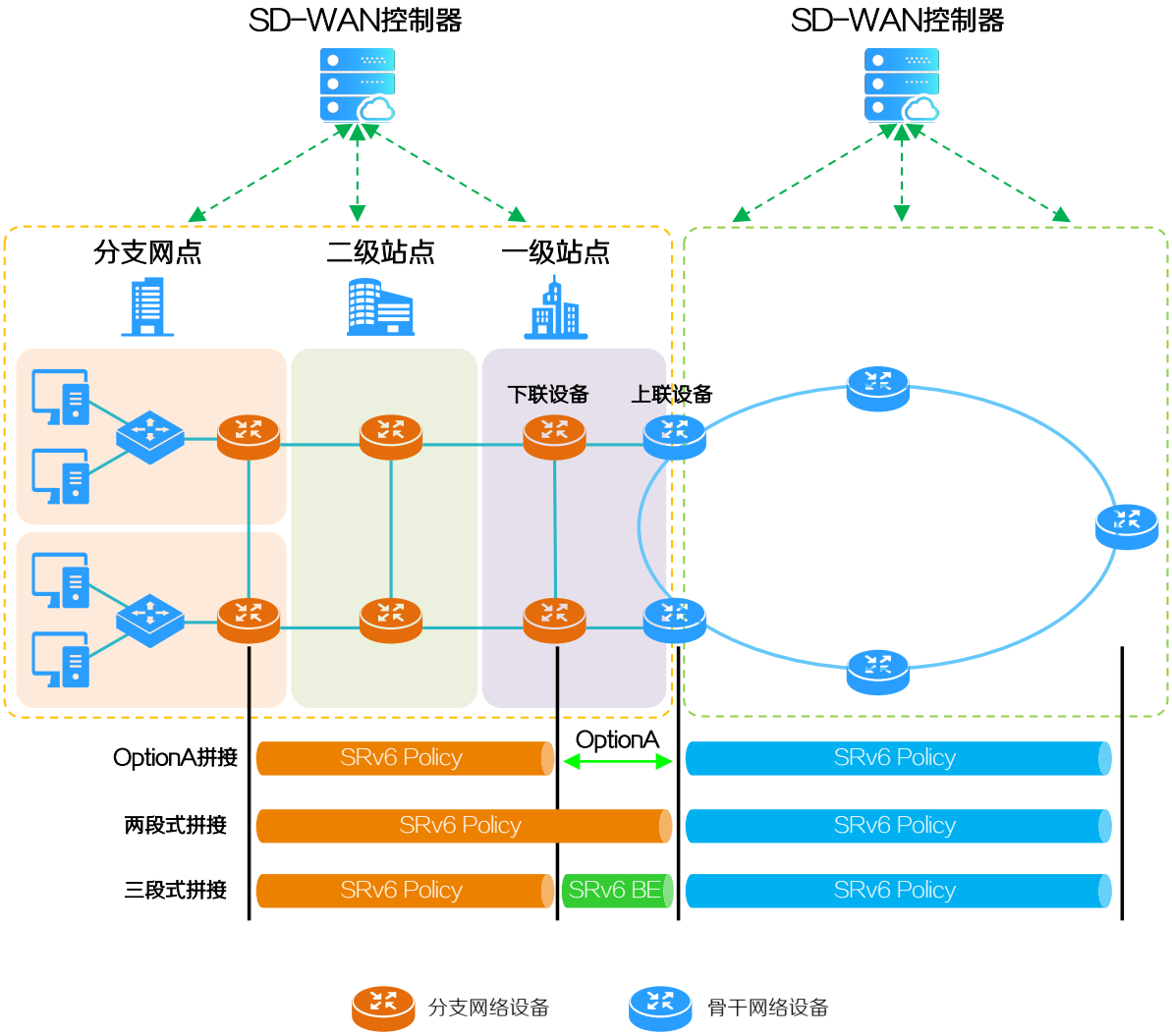


表2 三种拼接方式的特点和适用场景

拼接方式	特点	适用场景
OptionA拼接	• 实现简单，部署便捷 • 通过 EBGP 实现高效的跨域互通 • EBGP 协议广泛支持且稳定可靠	• 快速实现跨域连接 • 对网络稳定性和可靠性有高要求的大型金融机构
两段式拼接	• 直接建立 SRv6 Policy 隧道，数据转发快速高效 • 配置相对简单，易于管理	• SRv6 支持良好的新建网络环境 • 需要高效数据转发的大规模网络
三段式拼接	• 统一 IPv6+网络，实现总部与分支间无缝连接 • 利用 SRv6 BE 跨域技术高效互联	• 利用 IPv6+实现端到端业务管理的环境 • 多层次网络结构的大型金融机构

拼接方式	特点	适用场景
		• 关键业务网络需路径保护和负载均衡

关键技术应用

为了保持方案设计章节的简洁性，在本部分，仅简要概述应用于该方案的主要技术。更多关键技术及详细内容请参见“6 关键技术”。

- 网络性能优化：通过端到端数据压缩技术和 Web Cache 技术提高数据传输效率和业务访问速度。
- 网络可靠性与安全：结合 4G/5G 备份与电子围栏技术以及 IPsec 与 iSec 技术，提供故障备份和增强数据传输的安全性。
- 网络资源管理与业务质量保障：使用 Slice ID 源地址切片与支持细粒度 FlexE 切片网络技术，优化网络资源分配和服务质量。
- 网络部署与运维：采用零配置开局技术和智能运维，简化设备部署和日常维护，提高运维效率。

这种设计通过综合利用智能业务感知与路径调度、带宽优化与效率提升、网络可靠性增强、业务安全保障、业务质量保障和极简部署与智能运维等关键技术，确保了大型金融机构分支网络与骨干网络之间的顺畅、安全和高效运行。

6 关键技术

6.1 智能业务感知与路径调度技术

APN6：智能的业务感知

技术背景

随着不同类型的网络应用对性能需求的日益增加，传统的网络架构已经难以满足对差异化服务的需求。例如，视频会议、实时交易等关键应用都需要高效、稳定的网络传输保障。在这种情况下，网络必须能够识别并优先处理特定应用的数据流，以确保这些关键应用的性能和可靠性。

尽管传统的 IPv6 网络提供了广阔的地址空间和灵活的扩展能力，但它并未直接支持对应用层需求的识别和优化。因此，需要一种新型的网络架构来弥补这一不足，使得网络能够智能地识别并处理不同类型的应用数据流，实现更高效的资源分配和服务质量保障。

技术简介

APN6（Application-aware IPv6 Networking）是一种创新的网络架构，它通过在 IPv6 报文的扩展头中携带应用层信息，使网络设备能够识别应用层需求。这使得网络不仅是传输数据的通道，而且变得“智能”，能够根据应用的具体需求提供定制化的网络服务。

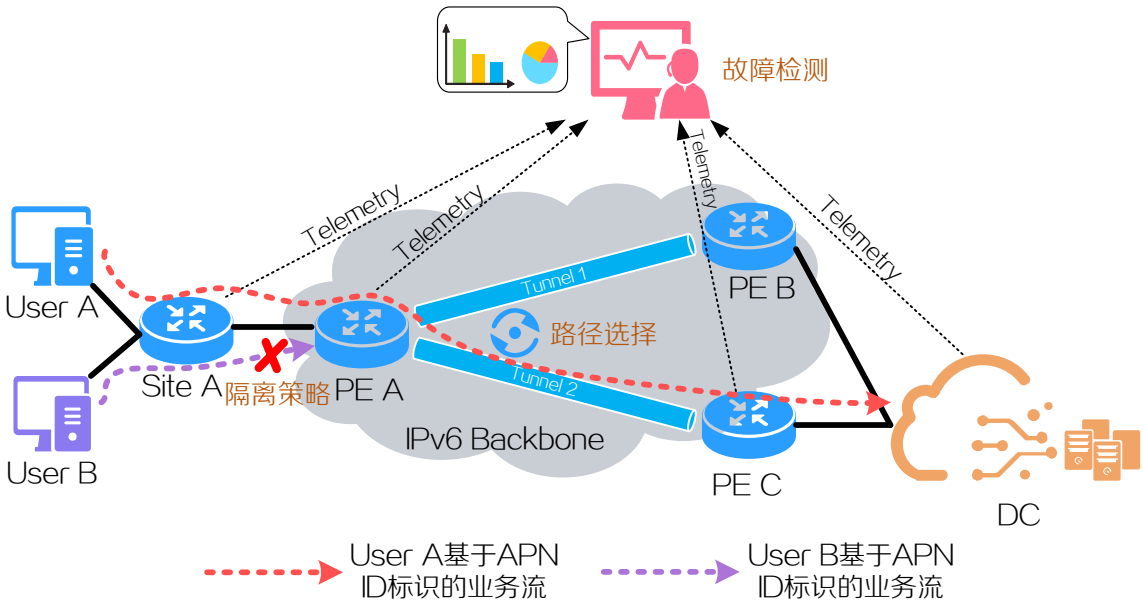
例如，将 IPv6 报文比喻为快递包裹，APN6 允许在这个“快递单”上不仅标注寄件人和收件人信息，还能携带寄件客户的 VIP 等级、包裹类型和对物流运输的特殊要求。这种方法极大地提升了网络的应用敏感性和服务质量。

如图 15 所示，在金融分支网络中，APN6 可以与 SD-WAN 结合应用，分支站点接入数据中心的 SD-WAN 网络中，通过部署 APN6 可以实现多种功能。

- **路径选择**：基于 APN ID，将用户 A 的特定流量引入到对应的 SRv6 TE Policy 隧道中转发，流量从客户端到骨干网再到云数据中心实现端到端的统一路径规划，SRv6 TE Policy 为特定流量提供可靠性保障。

- **隔离策略**：PE A 上可以基于 APN ID 设置隔离策略，不允许 APN ID 标识的某些用户访问数据中心。基于 APN ID 可以实现灵活的访问控制。
- **故障检测**：对于一些重要视频会议业务，可以部署 iFIT 检测，针对特定应用的流量实现逐段的业务质量监控和故障定位，一旦某段网络出现波动可以快速定位故障，并针对性地调优。

图15 APN6 典型应用

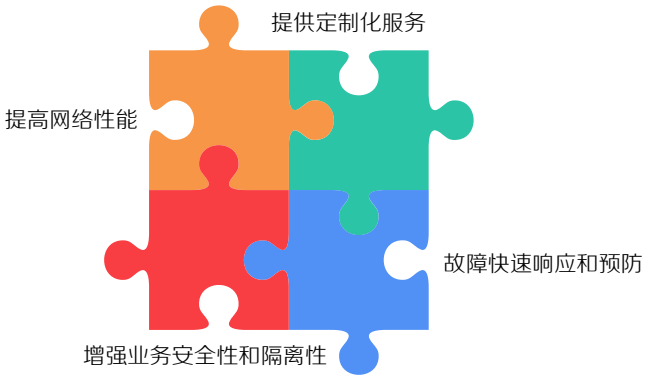


客户价值

APN6 技术为客户提供了显著的价值，包括但不限于：

- **提高网络性能**：通过应用感知的网络服务，能够为不同的业务流量提供优化的传输路径和网络资源，从而显著提高关键应用的性能和可靠性。
- **提供定制化服务**：APN6 使网络服务提供商能够为不同的客户或应用提供定制化的网络解决方案，满足差异化的 SLA 要求。
- **故障快速响应和预防**：结合 iFIT 等技术，APN6 能够进行实时网络监控和故障检测，快速定位和解决网络问题，减少业务中断时间。
- **增强业务安全性和隔离性**：通过 APN ID 部署的访问控制和隔离策略增强了网络的安全性，阻止未授权的访问和数据泄露风险。

图16 客户价值



iFIT 随流检测：应用级网络质量探测

技术背景

网络质量探测技术的进步对于现代网络运维领域至关重要。随着网络环境的不断复杂化，传统的探测技术面临着各种挑战，如结果偏差和效率下降等问题。iFIT 技术的出现，提供了一种更为直接和准确的网络性能探测方法，它通过直接在业务报文中嵌入特定的报文头，能够实现精细的网络性能测量，从端到端测量、逐点测量到多种组网环境的适配，iFIT 技术展现了其独特的价值和广泛的应用潜力。
特别是在 SRv6 网络环境中，iFIT 技术因其能够适应多种组网环境并快速定位网络问题而获得广泛应用。

技术简介

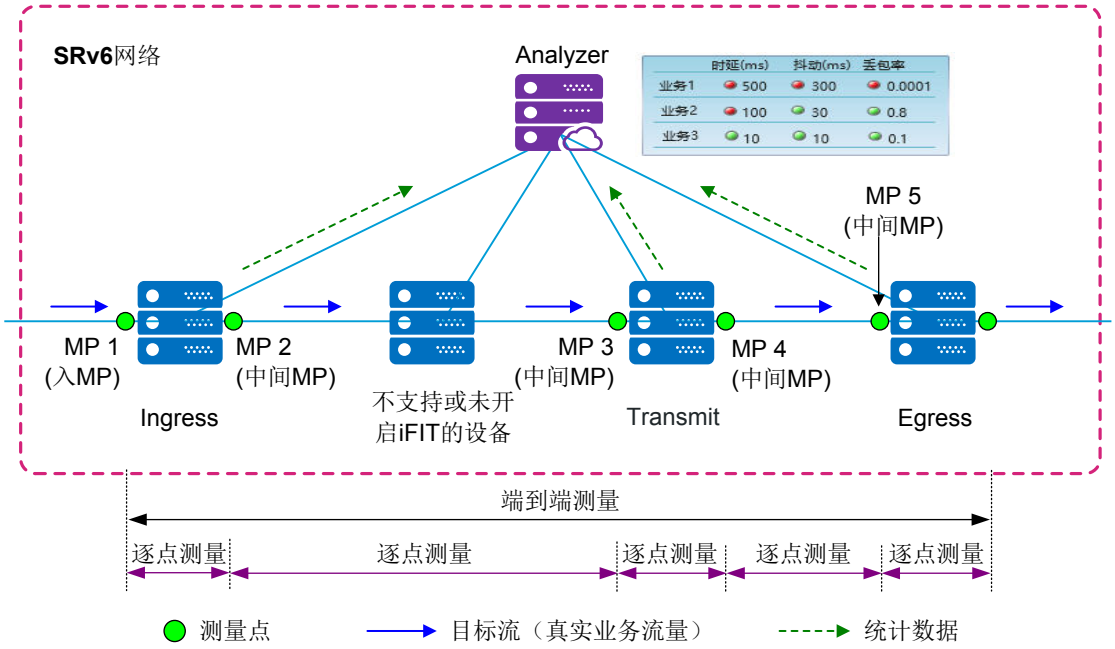
iFIT 技术的核心在于其创新的直接测量方法，它通过将测量功能直接嵌入业务流量中，避免了传统方法中可能出现的数据偏差问题。这种方法不仅提高了测量的准确性，还保持了网络传输的效率。如图 17 所示，iFIT 技术采用多点收集、集中计算的网络模型，包括入节点、中间节点、出节点和分析器等组件。通过这种模型，iFIT 在入节点处为目标流添加报文头，收集统计数据，并在出节点处去除 iFIT 报文头，确保数据的顺利传输。

网络模型组件功能

网络模型中的各个组件具体功能如下：

- **目标流**：iFIT 测量的对象，是符合指定匹配规则的业务流。网络管理员可以根据源 IP、目的 IP、协议类型等参数组合定义一条目标流。
- **入节点（Ingress）**：目标流进入测量网络的设备。负责对目标流进行筛选，添加 iFIT 报文头，收集目标流的统计数据并上报给分析器。
- **中间节点（Transmit）**：根据报文中包含的 iFIT 报文头自动识别 iFIT 目标流，并收集统计数据，然后上报给分析器。
- **出节点（Egress）**：目标流离开测量网络的设备，自动识别、收集统计数据并上报给分析器，然后去除 iFIT 报文头，将目标流转发给下一跳。
- **分析器（Analyzer）**：收集入节点、中间节点、出节点的统计数据，并完成数据的汇总和计算。
- **MP（Measurement Point，测量点）**：MP 通过与接口绑定来执行测量动作并生成统计数据。根据职责的不同，MP 分为入 MP、出 MP 和中间 MP 三种类型。

图17 iFIT 网络模型

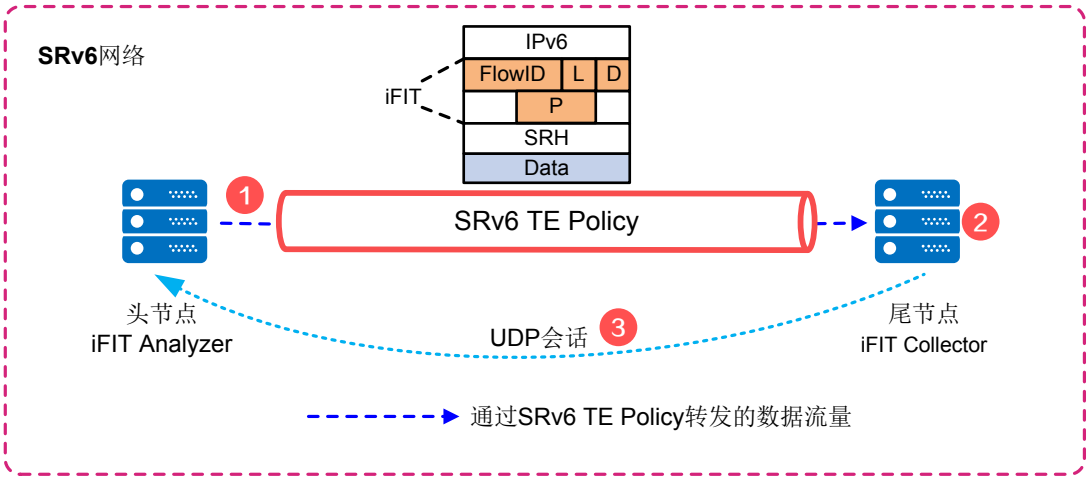


iFIT 在 SRv6 TE Policy 中的应用

如图 18 所示，在 SRv6 TE Policy 场景中，iFIT 测量功能是通过在 SRv6 TE Policy 的头节点和尾节点上部署 iFIT 功能，能够测量各个 SRv6 TE Policy 端到端的丢包率、时延和抖动，并在头节点上分析和计算得到每个 SRv6 TE Policy 的实时数据。SRv6 TE Policy 的 iFIT 测量功能基本工作流程如下：

- **头节点设置为 Analyzer**：SRv6 TE Policy 头节点 iFIT 的工作模式设置为 Analyzer。作为数据发送端，头节点通过 SRv6 TE Policy 转发报文时，为原始报文封装 iFIT 选项字段的 DOH 报文头和 SRH 报文头。这些字段包括标识目标流的 FlowID、丢包测量染色位 L、时延测量染色位 D 及周期标识等信息。
- **尾节点设置为 Collector**：尾节点 iFIT 的工作模式设置为 Collector。作为数据接收端，尾节点需要解析报文中的 iFIT 选项字段并根据报文染色信息统计数据。统计数据通过 UDP 会话按检测周期返回头节点。
- **数据回传与分析**：尾节点与头节点建立 UDP 会话，并通过该 UDP 会话将统计到的报文计数和报文时间戳返回头节点。头节点综合分析这些数据来计算通过 SRv6 TE Policy 转发报文的丢包率、时延和抖动等性能指标。

图18 SRv6 TE Policy 的智能策略路由功能示意图

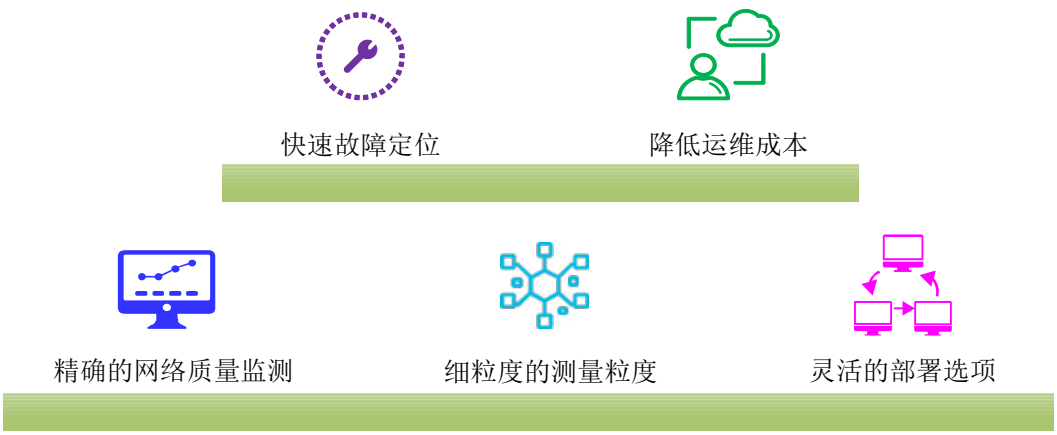


客户价值

iFIT 技术为用户带来了显著的客户价值，主要体现在以下几个方面：

- **快速故障定位**：iFIT 的逐点测量功能使得它在网络出现问题时，可以快速定位到具体的故障节点，大大缩短了故障响应和修复时间。
- **降低运维成本**：通过自动化的网络性能监测和故障处理，iFIT 有助于降低网络运维的复杂性和成本，提高网络服务的可靠性和用户满意度。
- **精确的网络质量监测**：iFIT 通过对业务报文进行直接监测，提供了真实且准确的网络性能指标，例如丢包率和时延，这些数据使网络管理员能够更有效地掌握网络状态并进行管理。
- **细粒度的测量粒度**：iFIT 能够根据二层参数、五元组、PeerLocator 等信息精确匹配业务报文，支持点到点、点到多点、多点到多点等多种测量场景。这种细粒度的测量能力使得 iFIT 能够详尽地分析网络状况，提供更为细致的性能管理。
- **灵活的部署选项**：iFIT 支持多种网络环境和多种测量场景，包括公网、MPLS 和 SRv6 等，为用户提供了极大的部署灵活性。

图19 客户价值



综上所述，iFIT 技术不仅解决了传统质量探测方法中的测量结果偏差等问题，还为现代网络环境中的性能管理和故障诊断提供了一个高效、可靠的工具。

分布式智能调度 IPR：自适应 SLA 的路径调度

技术背景

在广域网中，传统的流量工程（TE，Traffic Engineering）技术通常仅在当前路径出现故障时，才会将流量切换到其他路径。对于 SRv6 TE Policy，若当前最优候选路径中存在多条转发路径，只有全部转发路径都发生故障后才会进行路径切换。这种故障切换策略难以满足金融业务对服务级别协议（SLA，Service Level Agreement）的需求，可能存在以下问题：

- **单条路径承载不足**：在金融业务中，若多条转发路径发生故障，仅剩单条路径可用，将无法触发候选路径切换。这会导致单条路径无法承载巨大的业务流量，造成网络拥塞和数据包大量丢失。
- **路径质量劣化不触发切换**：出现拥塞导致转发路径的质量劣化时，比如时延升高、丢包率增大、总体带宽能力下降等情况，并不会触发候选路径的切换和优化。即使所有路径故障后，依赖控制器进行的被动路径重计算和调优也耗时长，调整过程中用户业务可能已经出现丢包等问题。

技术简介

为解决上述问题，提出了 SRv6 TE Policy 智能策略路由（IPR，Intelligent Policy Route）技术。IPR 通过设备自主决策，实时监控网络状态，根据实时数据及预设策略自动调整路径，以保证网络性能和业务连续性。SRv6 TE Policy 通过智能策略路由技术实现了灵活的路径调度，主要包括以下两种方式：

- **基于网络质量选路**：通过实时检测路径的时延、抖动、丢包率等参数，确保选择的路径满足业务的 SLA 需求。
- **基于带宽选路**：根据各条路径的可用带宽情况，选择能够承载当前业务流量的最佳路径，避免因带宽不足而导致的网络拥塞。

这两种技术确保了 SRv6 TE Policy 能够在网络状态变化时快速响应，优化数据流的传输路径，避免拥塞和性能瓶颈，从而满足金融业务持续高效运行的要求。

基于网络质量选路

如图 20 所示，采用 SRv6 TE Policy 智能策略路由 IPR 技术，实现根据网络质量对流量进行灵活路径调度的简要流程如下：

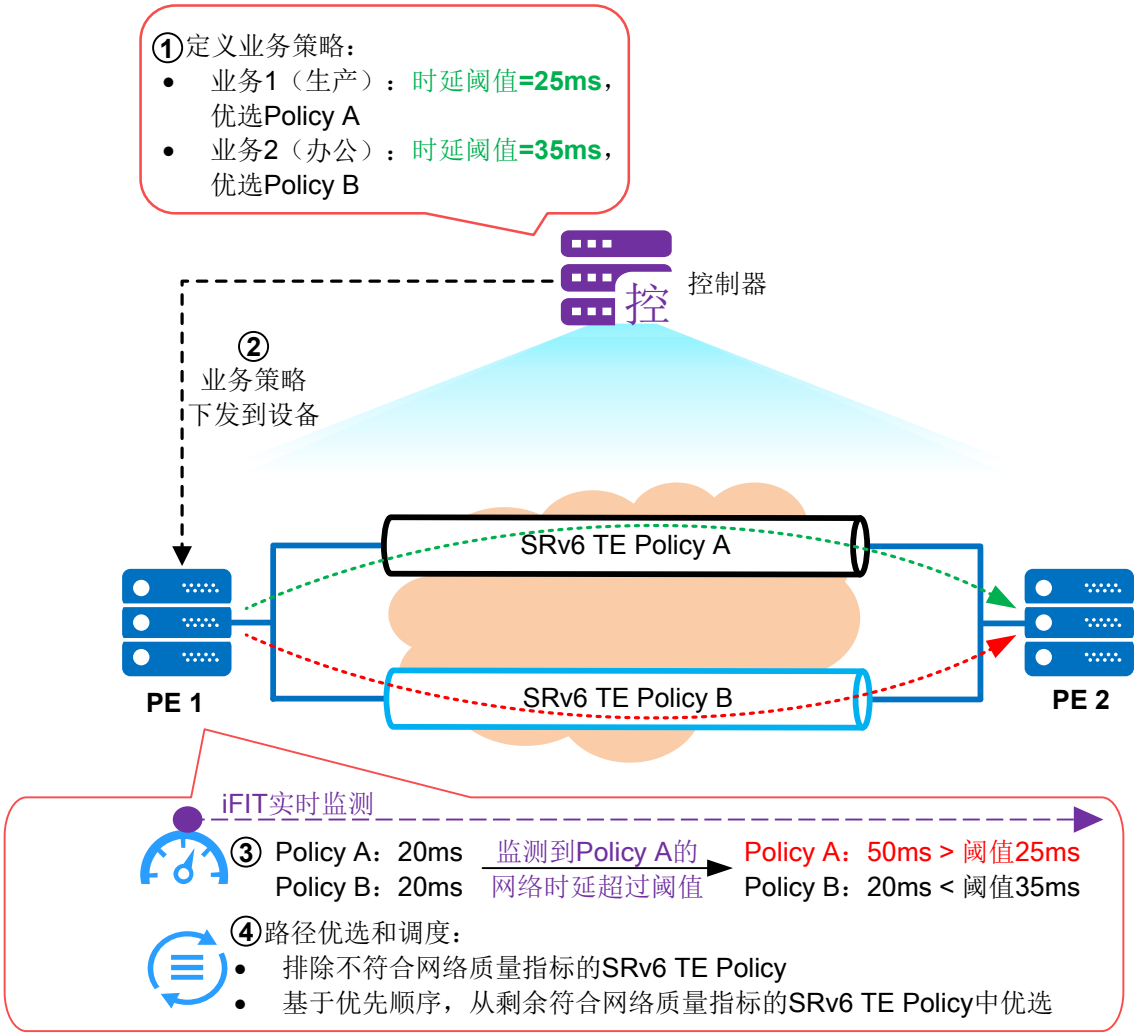
(1) **定义业务策略**：管理员在 SD-WAN 控制器上，根据五元组/DSCP 等字段，对不同应用业务进行区分，并定义业务策略。例如：
   - 业务 1（生产）：时延阈值=25ms，优选 Policy A。
   - 业务 2（办公）：时延阈值=35ms，优选 Policy B。

(2) **业务策略下发到设备**：将定义好的业务策略通过控制器下发到设备。业务策略在设备上生效，由设备自主进行实时网络质量监测和调度。

(3) **设备实时监测网络质量与自主调度**：PE 1 上开启 iFIT（In-situ Flow Information Telemetry，随流检测）检测 SRv6 TE Policy 功能，实时检测 SRv6 TE Policy 中最优候选路径中所有转发路径的时延、丢包率、抖动信息。当设备检测到当前路径的质量不再符合业务需求时，自动触发路径切换。例如，当检测到 SRv6 TE Policy A 的时延增加到 50ms（超过 25ms 的阈值），而 SRv6 TE Policy B 保持在 20ms 时，设备会自动将流量从 SRv6 TE Policy A 切换到 SRv6 TE Policy B。

(4) **动态路径优选**：PE 1 基于测量的实时数据，排除不符合网络质量指标的 SRv6 TE Policy，并周期性地从多个候选的 SRv6 TE Policy 中选择最优的路径来承载业务。设备根据实时监控数据动态调整传输路径，确保选择的路径始终满足业务的 SLA 需求。

图20 根据网络质量优选转发路径调度流量示意图



相比于控制器集中调度，通过这种分布式调度机制，显著减少了对中心处理能力的依赖，降低了复杂度和潜在的延迟，提高了网络的整体实时性和可靠性。通过这种设备自主决策和及时响应机制，设备能够在检测到网络质量下降或带宽压力增大时，迅速进行路径优化和切换，确保服务质量。

基于带宽选路

在当前金融 SRv6 SD-WAN 环境中，尽管已支持基于网络质量的智能路径选择，但缺乏基于实际带宽利用情况的动态路径选择功能。这限制了在链路空闲时段的带宽资源利用，导致带宽利用率不足和成本效率问题。为了优化带宽总体利用率，H3C 增强了金融 SRv6 SD-WAN 的调度能力，引入了基于实时出端口带宽的路径选择新功能。如图 21 所示，假设 SRv6 TE Policy A 和 SRv6 TE Policy B 的出接口的总带宽分别为 10 Mbps 和 15 Mbps，采用 SRv6 TE Policy 智能策略路由 IPR 技术，实现根据网络带宽对流量进行灵活路径调度的简要流程如下：

(1) **定义业务策略**：管理员在 SD-WAN 控制器上定义不同应用业务的隧道出接口带宽利用率上限，并选择合适的 SRv6 TE Policy 进行优选。例如，对于业务 1：
   - Policy A 和 Policy B 的出接口带宽利用率阈值均为 80%，即 Policy A 的出接口带宽上限为 8 Mbps，Policy B 的出接口带宽上限为 12 Mbps。
   - 业务 1 优选 Policy A，但当 Policy A 的使用带宽超过 8 Mbps 时，需要做路径切换。

(2) **业务策略下发到设备**：将定义好的业务策略通过控制器下发到设备。业务策略在设备上生效，由设备自主进行实时网络带宽监测和路径调度。

(3) **带宽监测与统计**

a. **实时统计**：PE 1 上开启所有 SRv6 TE Policy 流量统计功能，实时采集和统计各 SRv6 TE Policy 流量所使用的带宽。例如，当前 SRv6 TE Policy A 已经使用了 7 Mbps 的带宽。

b. **周期性采集**：同时，PE 1 上周期性采集 SRv6 TE Policy 出接口的数据流量所占带宽，并计算其带宽利用率。例如，SRv6 TE Policy A 当前的带宽利用率为 70%（7 Mbps / 10 Mbps）。

c. **触发路径调优**：当 SRv6 TE Policy A 的隧道出接口带宽利用率超过设定上限 80%（即带宽上限 8 Mbps）时，设备将主动触发路径调优流程。

(4) **动态路径优选**

PE 1 评估当前所有 SRv6 TE Policy 的带宽利用情况，选择符合业务带宽需求且利用率最优的路径。具体如下：

a. **计算预期带宽利用率**：PE 1 将当前 SRv6 TE Policy A 的业务流量带宽与 SRv6 TE Policy B 出接口的已使用带宽求和，然后除以 SRv6 TE Policy B 的总带宽，得到流量切换到 SRv6 TE Policy B 后的预期带宽利用率。

b. **比较带宽上限**：如果预期带宽利用率低于设置的上限，则 SRv6 TE Policy B 符合带宽要求，否则不符合。

c. **优选路径**：PE 1 在所有符合带宽要求的 SRv6 TE Policy 中选择最合适的路径转发业务流量。

示例操作：

a. **触发调优**：假设 SRv6 TE Policy A 的实际使用带宽达到 8.5 Mbps，超过设定的利用率上限（8 Mbps），触发路径调优机制。

b. **计算路径**：计算 SRv6 TE Policy B 的隧道出接口当前带宽使用情况，假设已使用 2 Mbps。

c. **预期利用率**：预计将 SRv6 TE Policy A 的流量（8.5 Mbps）切换到 SRv6 TE Policy B 后，SRv6 TE Policy B 的隧道出接口总使用带宽为 10.5 Mbps（8.5 Mbps + 2 Mbps）。

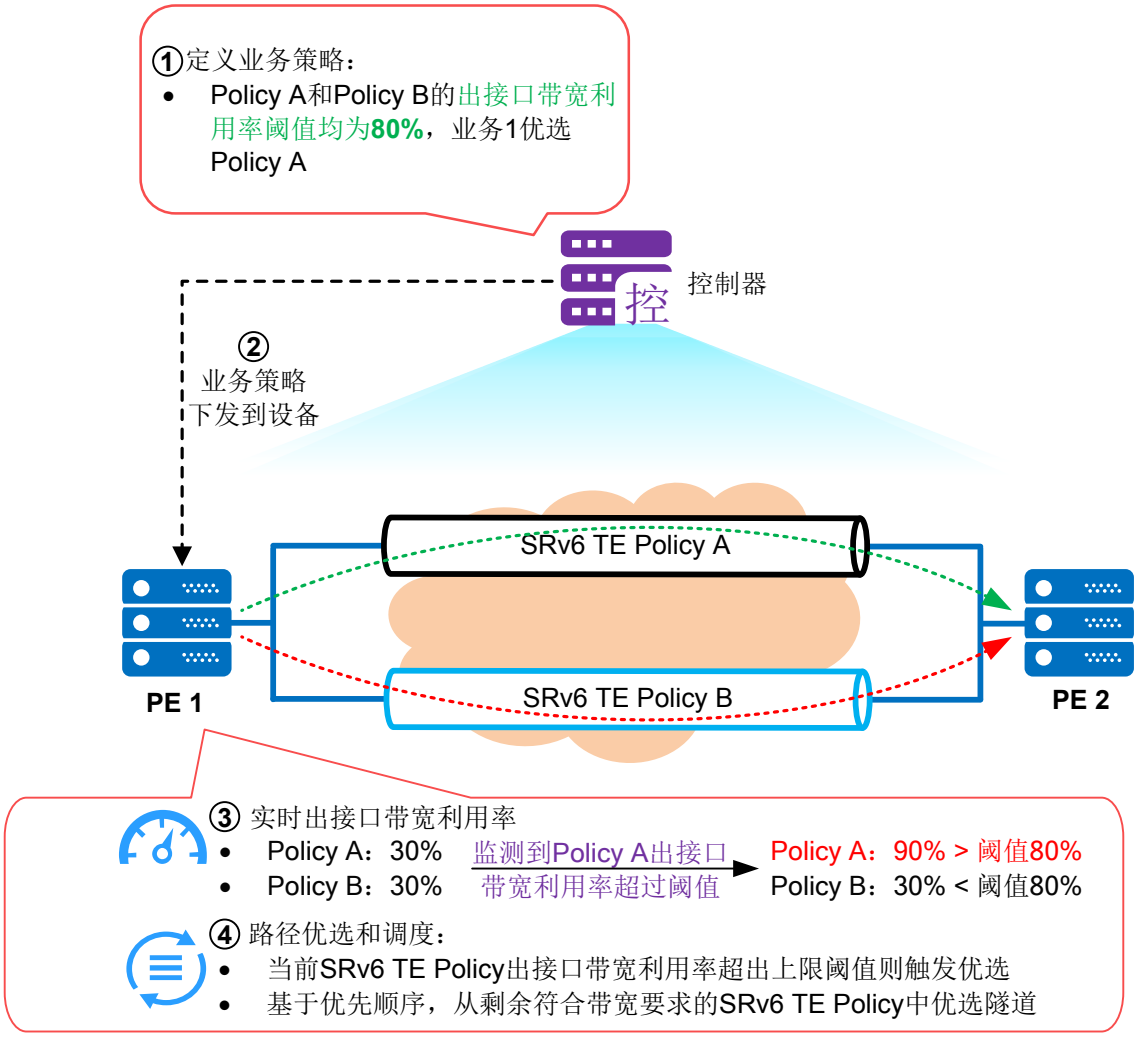
d. **结果分析**：SRv6 TE Policy B 的预期带宽利用率为 70%（10.5 Mbps / 15 Mbps）。

e. **选择路径**：如果 SRv6 TE Policy B 的隧道出接口预期带宽利用率低于预设上限（例如 80%），则 SRv6 TE Policy B 适合承载 SRv6 TE Policy A 的流量，否则不适合。

f. **切换策略**：PE 1 在所有符合要求的路径中选择最合适的 SRv6 TE Policy，如 Policy B，将流量切换至此路径。

通过这种路径调优机制，能够确保在充分利用带宽资源的同时，保障网络的高效性和可靠性。

图21 根据带宽优选转发路径调度流量示意图

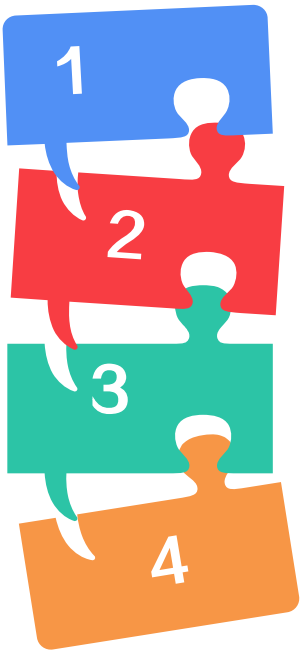


客户价值

SRv6 TE Policy 的智能策略路由技术为金融行业带来显著的价值：

- **高效的性能保障与设备自主决策**：IPR 根据不同业务流量的需求（链路质量、链路带宽）为其选择最适合的链路。如果当前链路由于状态变化不再符合要求，IPR 可以自动将流量切换到另一条链路。通过这种实时监控和动态调整网络路径的机制，IPR 确保网络性能始终满足金融业务的严格 SLA 要求，减少因路径故障导致的业务中断。同时，相较于控制器集中调度方式，分布式调度在设备上进行，设备自主决策和调度使网络反应速度更快、可靠性更高。
- **增强的网络适应性和业务连续性**：灵活的路径调度能力使网络能够迅速适应不同的网络状态变化，优化数据流的传输路线，避免拥塞和性能瓶颈。同时，快速的故障恢复和动态的带宽管理确保关键业务应用的连续性和可靠性，增强企业运营的稳定性。
- **提高成本效益和带宽利用率**：通过优化路径利用和降低故障响应时间，帮助企业降低运营成本，提高网络资源的使用效率。智能管理业务流量还能更高效地利用主备链路的带宽资源，实现所有可用带宽的最大化利用，从而降低整体网络成本。
- **提升用户体验**：优化后的带宽管理和降低的传输延迟直接加快了业务应用的响应速度和可靠性，提高了用户的满意度和服务体验。

图22 客户价值



高效的性能保障与设备自主决策
实时监控和动态调整，自主决策，满足严格SLA，减少中断

增强的网络适应性和业务连续性
灵活路径调度、快速恢复与动态带宽管理，确保关键业务持续运行

提高成本效益和带宽利用率
优化路径和故障响应，智能流量管理，最大化带宽利用，降低成本

提升用户体验
优化带宽管理和降低延迟，加快应用响应，提高用户满意度

综上所述，这些技术不仅提升了网络的智能化管理水平，还确保了企业关键应用的高性能和高可用性，为现代金融网络环境提供了强大的支持。

6.2 业务隔离与质量保障技术

Slice ID 源地址切片：网络切片的简化部署与高效运维

技术背景

随着网络技术的发展，网络切片成为确保数据传输质量和效率的关键技术之一。传统的子接口切片方法要求配置大量的子接口、IP 地址和路由邻居，这不仅增加了网络的复杂度，还提高了运维的难度，导致客户在部署子接口切片时存在顾虑。为了简化操作并提升效率，引入了一种新的 Slice ID 源地址切片方案。该方案旨在优化网络管理和数据转发，从而简化网络切片的部署和运维。

技术简介

源地址切片方案是一种基于 IPv6 报文源地址的创新切片技术，使用 IPv6 报文源地址中的低 32 位来携带 Slice ID。这样，设备仅需解析 IPv6 基本头即可获取 Slice ID 信息，无需额外增加报文长度，报文头开销较小。

如图 23 所示，在物理网络划分为虚拟切片网络的方法为：

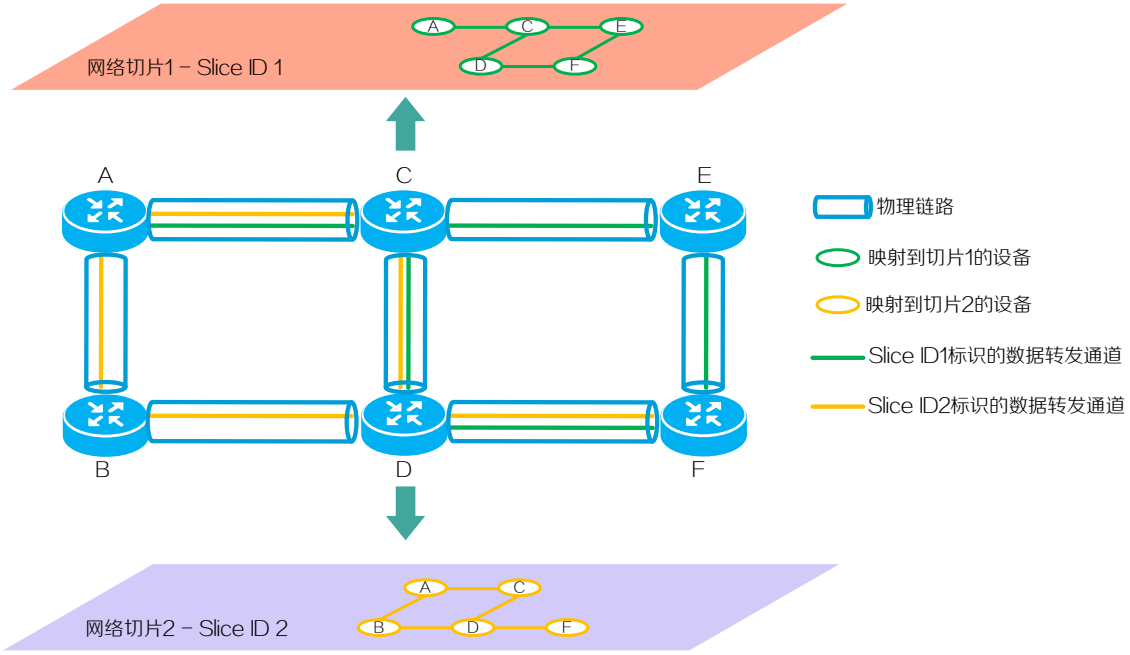
(1) **规划 Slice ID**：根据业务需求，为不同切片网络分配不同的 Slice ID。

(2) **根据 Slice ID 将物理设备映射到虚拟切片网络**：在物理设备上创建网络切片实例，网络切片实例的标识为 Slice ID。这样，就可以将该物理设备映射到 Slice ID 对应的虚拟切片网络。

(3) **根据 Slice ID 将物理接口映射到虚拟切片网络**：在物理接口上开启切片功能并创建网络切片通道，网络切片通道的标识是 Slice ID。这样，就可以将该物理接口映射到 Slice ID 对应的虚拟切片网络。同一物理接口下的不同网络切片通道具有独立的队列调度机制和带宽保障机制，因此，不同网络切片通道中的业务转发互不影响。

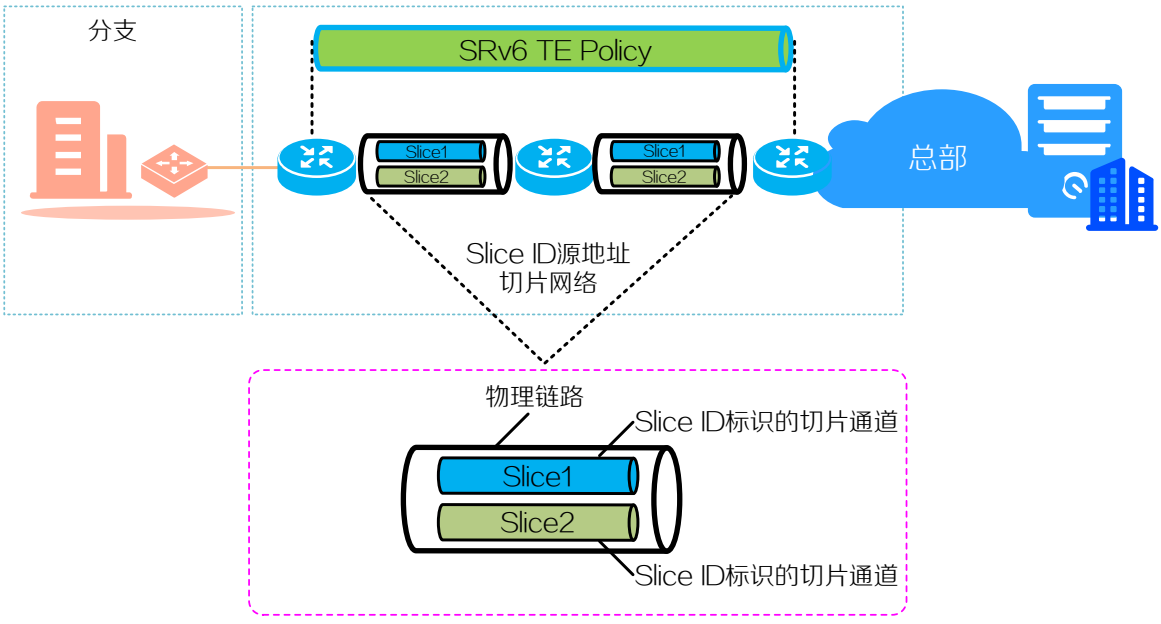
(4) **构成虚拟切片网络**：具有相同 Slice ID 的网络切片实例和网络切片通道构成一个虚拟切片网络。

图23 Slice ID 源地址切片方案示意图



如图 24 所示，在 SRv6 组网场景中，通过全局唯一的 Slice ID 来标识切片网络中的设备和数据转发通道，并以此来划分切片网络。在切片网络中转发的业务报文携带 Slice ID 信息。设备转发该报文时，先查询 FIB 表找到出接口，再根据 Slice ID 从对应出接口上的数据转发通道转发报文。

图24 Slice ID 源地址切片组网示意图



如表 3 所示，与传统的 HBH（Hop-by-Hop Extension Header）扩展头方式相比，Slice ID 源地址切片方案不增加额外的开销或带宽资源消耗。传统的 HBH 扩展头方法需要解析 HBH 的 TLV，而某些 ASIC 芯片设备无法支持这一点。相反，Slice ID 源地址切片方案基本不影响转发性能，因为任何支持 IPv6 转发的中间设备都天然支持此方案，无需额外的报文格式要求或处理。

表3 不同切片方案对比

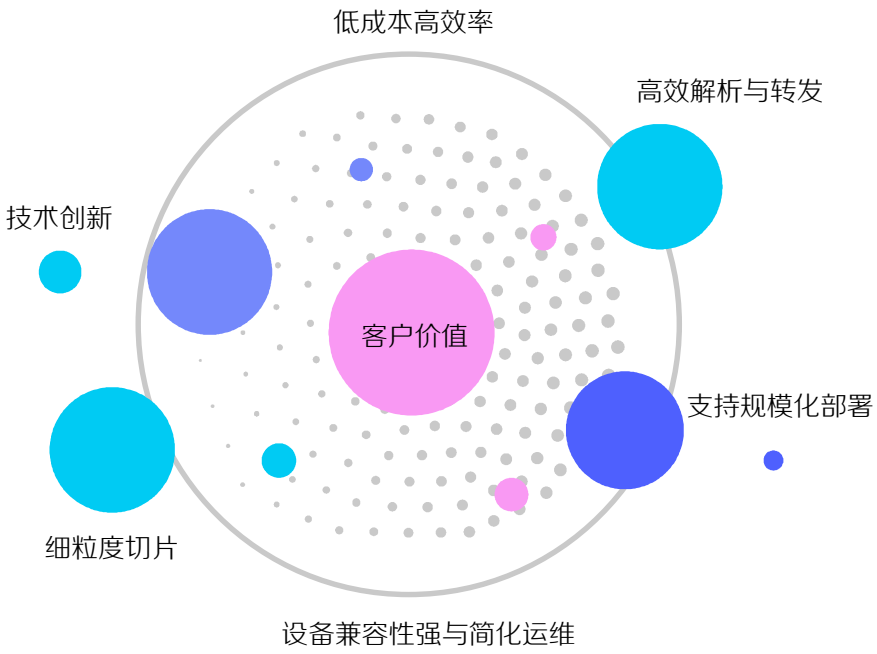
封装方式	HBH 扩展头	源地址切片方案
开销/带宽	扩展头增加开销	无额外开销
转发效率	需解析HBH的TLV，需要芯片支持	基本不影响转发性能
报文格式要求	HBH头须位于首位	无特殊要求

客户价值

Slice ID 源地址切片方案带来了显著的客户价值：

- **低成本高效率**：随着切片数量的增长，IP 地址、路由数量和收敛性能保持不变，大幅减少了资源消耗和管理成本。此外，由于无需额外开销和带宽资源消耗，Slice ID 源地址切片方案在成本效率方面具有显著优势。
- **高效解析与转发**：由于没有额外的扩展头，无需增加报文长度且不占用额外的带宽资源，设备仅需解析 IPv6 基本头即可获取 Slice ID 信息，从而实现更快的解析速度和更高的转发效率。
- **支持规模化部署**：该方案确保 IP 地址和路由数量的需求不会随着切片数量的增加而增长，从而支持更大规模的网络切片部署，保持网络的收敛性能稳定。
- **设备兼容性强与简化运维**：中间网络设备仅需支持 IPv6 基本转发功能即可天然支持此方案，这种嵌入式 Slice ID 方案避免了额外的报文开销和带宽资源消耗，极大地简化了网络设备的要求和运维工作，提高了网络设备的兼容性，便于在现有网络中快速部署。
- **细粒度切片**：支持高达 1M 的细粒度切片，规模可达 K 级。通过全网整体规划，为每个 Slice ID 在设备上预配置必要的资源，能够满足不同业务和应用场景的需求，实现精确的资源分配和灵活的网络管理。
- **技术创新**：作为 H3C 与运营商共同主导的草案，Slice ID 源地址切片方案在转发效率和网络设备兼容性方面表现更优，可以为客户提供一个更可靠和高效的网络切片解决方案。

图25 客户价值



总之，IPv6+的 Slice ID 源地址切片方案不仅解决了传统子接口切片技术的复杂性和运维难度问题，还提供了一个高效、可扩展且低成本的解决方案，使其在金融、云服务等多个行业中具有广泛的应用前景。

支持细粒度 FlexE 切片网络：提升网络资源管理的灵活性与精确性

技术背景

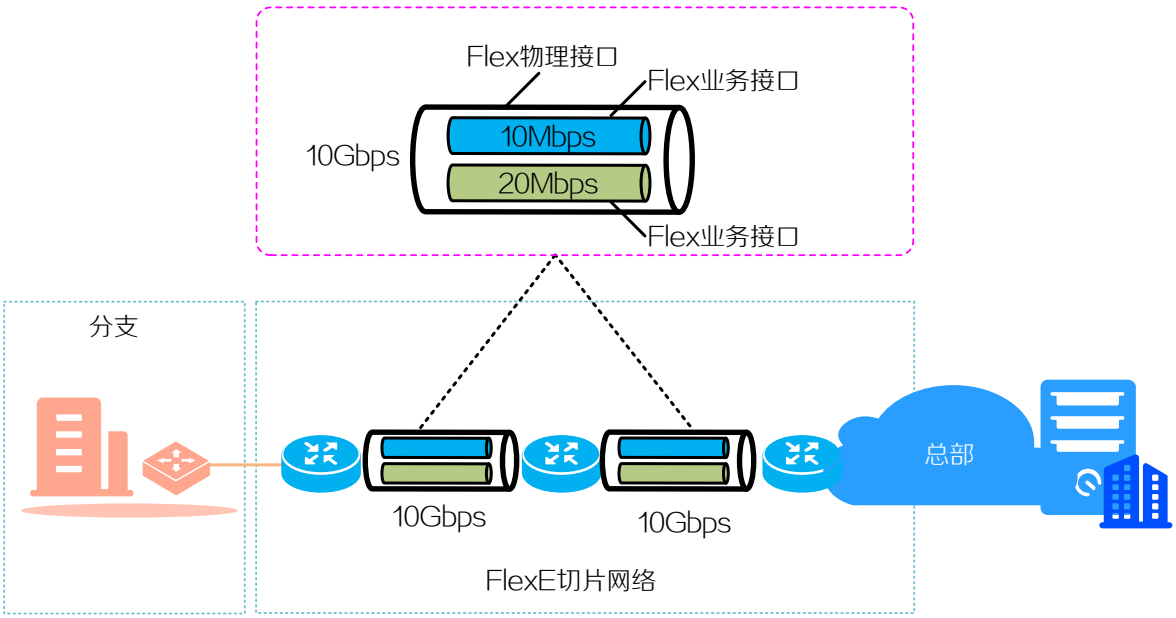
随着 5G 网络和垂直行业应用的蓬勃发展，客户对网络承载能力提出了新的要求。特别是在专线业务等场景中，对于小带宽、高隔离性和高安全性的需求日益迫切。这些场景需要高度定制化的解决方案，能够支持差异化的业务承载，同时在成本和效率上达到最佳平衡。在这种背景下，细粒度的网络切片功能成为关键技术，它允许更细致和灵活的网络资源管理。

技术简介

为响应这一需求，细粒度 FlexE 切片网络技术应运而生。FlexE 是一种将一组物理接口捆绑在一起，并按时隙交叉复用后灵活划分成不同带宽的 FlexE 业务接口的切片技术。FlexE 业务接口作为网络切片方案中的数据转发接口，用于承载大带宽高附加值的行业切片业务。该技术将传统的切片颗粒度从 5Gbps 细化到 10Mbps，极大地提高了网络资源的利用率和灵活性。通过这种小颗粒度的承载管道，网络可以实现硬隔离，确保数据传输的安全性和稳定性。这种细粒度的调整不仅降低了网络部署的成本，还提供了更高的配置灵活性，使得网络运营商能够为不同业务需求提供定制化的服务。

如图 26 所示，可根据业务需要将 10Gbps 物理带宽按需划分成多个大于或等于 10Mbps 粒度的 FlexE 业务接口，以满足不同应用的精细化需求。

图26 细粒度 FlexE 切片网络示意图



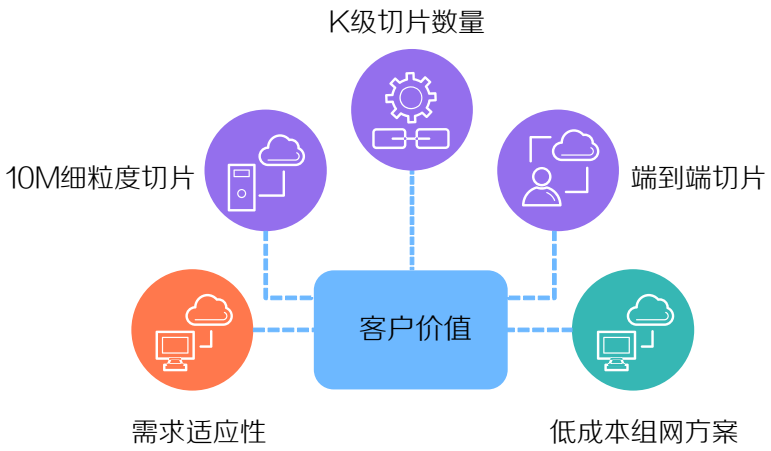
客户价值

部署细粒度 FlexE 切片网络为客户带来了显著的价值：

- **10M 细粒度切片**：超细颗粒度的切片能力，满足客户对差异化业务承载的精细需求，特别适合于对带宽要求不高但需高隔离性和安全性的应用。

- **K 级切片数量**：支持数千级别的切片数量，保证多种业务可以同时承载，提高网络的扩展性和多样性。
- **端到端切片**：从网络核心直接延伸至末端用户，实现业务的端到端完整连接，提供直接且高效的服务体验。
- **低成本组网方案**：在提供同等传输能力的条件下，为客户提供更经济的组网选项，显著降低企业运营成本。
- **需求适应性**：H3C 的细粒度 FlexE 切片网络方案，通过提供 10M 粒度的切片，有效地满足了市场对高精细度网络切片日益增长的需求，从而使客户能够更灵活地应对各种网络场景。

图27 客户价值



切片弹性扩缩容：网络切片带宽的智能自适应调整

技术背景

在传统的网络环境中，网络切片通常被配置为严格专享特定的带宽资源，以确保数据传输的可靠性和服务质量。然而，这种方法会导致链路带宽的利用率下降，特别是在数据流量分布不均匀的场景中，一些链路可能出现资源闲置的情况。这种低效的资源利用率影响了客户对网络切片技术的部署意愿。因此，客户希望能够更高效地使用带宽资源，以降低成本和提高网络性能。

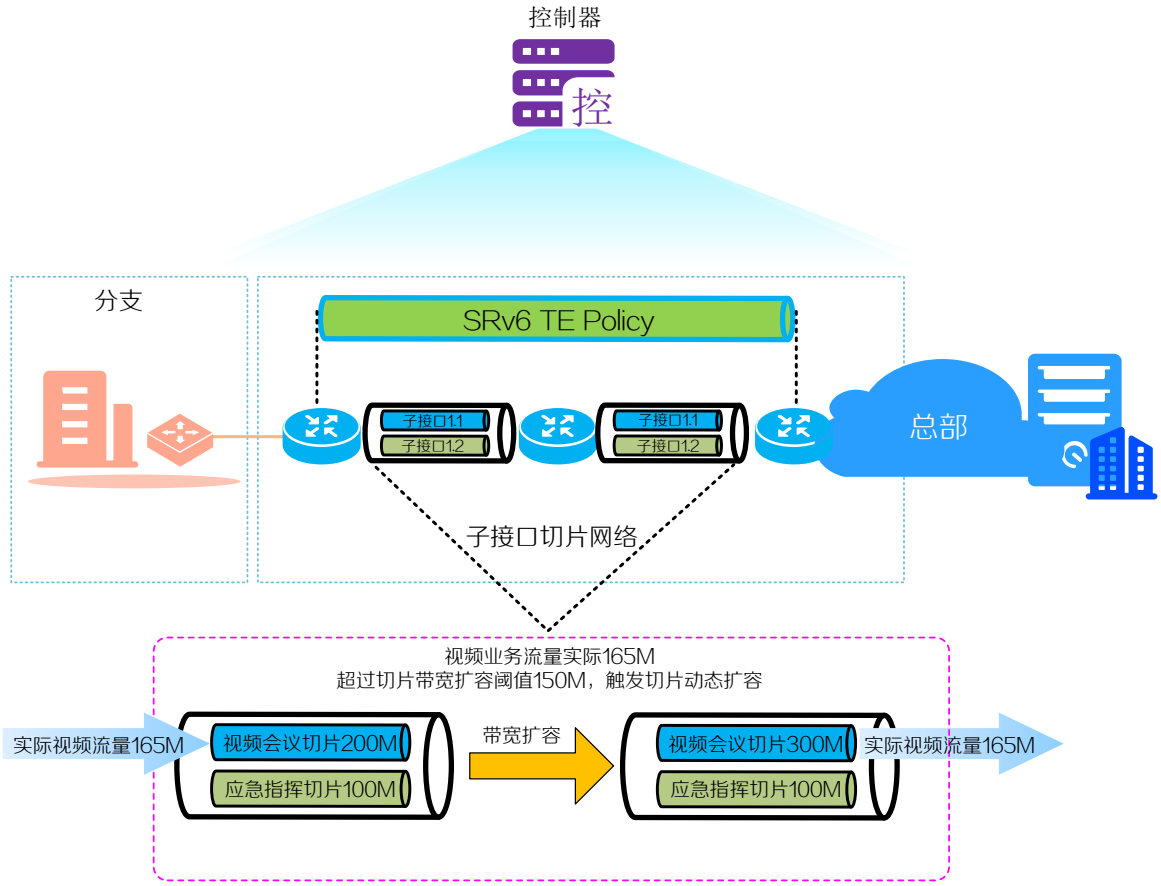
技术简介

如图 28 所示，为了解决上述客户痛点，H3C 提出了一种切片弹性扩缩容方案。该方案的核心是通过智能策略动态地监控切片的带宽使用率，并根据设定的扩容（增加带宽）或缩容（减少带宽）阈值自动调整带宽分配。具体实现步骤如下：

- **监控**：控制器持续实时监控各切片的带宽使用情况。一旦带宽使用率达到或超过预设的扩容或缩容阈值，控制器将向设备下发指令，以触发相应的调整动作。
- **执行**：设备根据控制器的指令进行带宽调整。
  - 扩容：在网络流量需求增加时，增加切片带宽，确保服务质量不受影响。
  - 缩容：当流量需求减少时，减少切片带宽分配，释放未被使用的带宽资源给其他服务。

这种智能化的自适应调整机制不仅使网络资源使用更加高效，而且可以根据实际需求灵活调整资源，有效提升整个网络的带宽利用率，并确保关键业务的连续性和性能。

图28 切片弹性扩缩容方案示意图



客户价值

切片弹性扩缩容方案为客户带来了显著的经济和技术价值：

- **节省带宽与提高利用率**：通过智能化管理，方案在保障必要服务质量的同时，避免不必要的带宽浪费，并根据实际使用情况调整带宽，显著提高网络链路的带宽利用率。
- **成本效益**：更高的带宽利用率意味着相同的网络资源可以支持更多的业务需求，从而减少对额外带宽资源的需求，降低单位业务的网络成本。
- **灵活性与可扩展性**：自动的扩缩容机制使得网络能够灵活适应业务需求的变化，支持业务增长或减少，无需人工干预，提供更高的业务灵活性和网络可扩展性。
- **技术创新**：H3C 的切片弹性扩缩容方案通过支持子接口切片的弹性扩缩容，展示了对网络动态需求的先进适应能力。这种创新性的技术应用不仅提升了网络的灵活性和可扩展性，还为客户提供了更加高效和定制化的网络管理解决方案。

图29 客户价值

综上所述，切片弹性扩缩容方案通过控制器智能监控和自动调整带宽分配，解决了客户对带宽资源利用的痛点，为网络运营商提供了一个成本效益高、灵活性强的网络管理工具，这在金融、云服务和大数据等对网络性能要求极高的行业中具有特别的价值。

前向纠错技术（FEC）：确保广域网中音视频数据的高效传输与可靠性

技术背景

在数字化时代，实时音视频的传输成为了日常通信的重要组成部分，尤其是在金融网点等关键领域。这些应用对网络的稳定性和可靠性有着极高的要求。然而，在广域网环境中，由于网络拥塞、不稳定的链路等因素，数据传输过程中的丢包问题成为了一大挑战，严重影响了音视频流的质量。为了解决这一问题，前向纠错（FEC）技术应运而生，它通过增加冗余数据包来恢复丢失的报文，显著提高了数据传输的可靠性。

技术简介

前向纠错（FEC）技术是一种关键的数据传输错误控制方法，它基于 Reed-Solomon（RS）算法增强数据流的可靠性。RS 算法允许发送端在数据包中加入额外的冗余包，使得即使在网络出现丢包的情况下，接收端也能利用这些冗余信息恢复丢失的数据包。

在 FEC 的应用中，关键是平衡冗余包的数量，以防止过多冗余数据占用带宽，同时确保足够的冗余包以有效恢复数据。这一平衡取决于编码块的大小、编码算法和预期的抗丢包率。

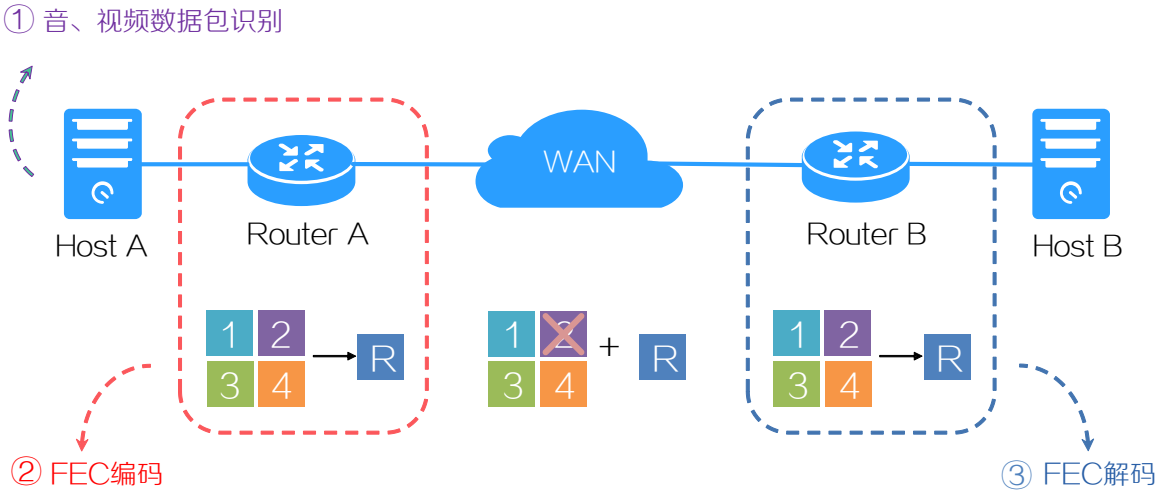
如图 30 所示，FEC 对报文的处理流程如下：

(1) **音视频数据包识别**：对 RTP 类匹配 WAAS 策略，如果匹配到策略，则创建 FEC 的快速转发表项并设置快速转发业务标记；若未匹配到策略，则正常转发。

(2) **FEC 编码**：缓存数据包直到达到编码块包数或超时，进行 FEC 编码生成冗余包 R，并同时发送原始数据包和冗余包。

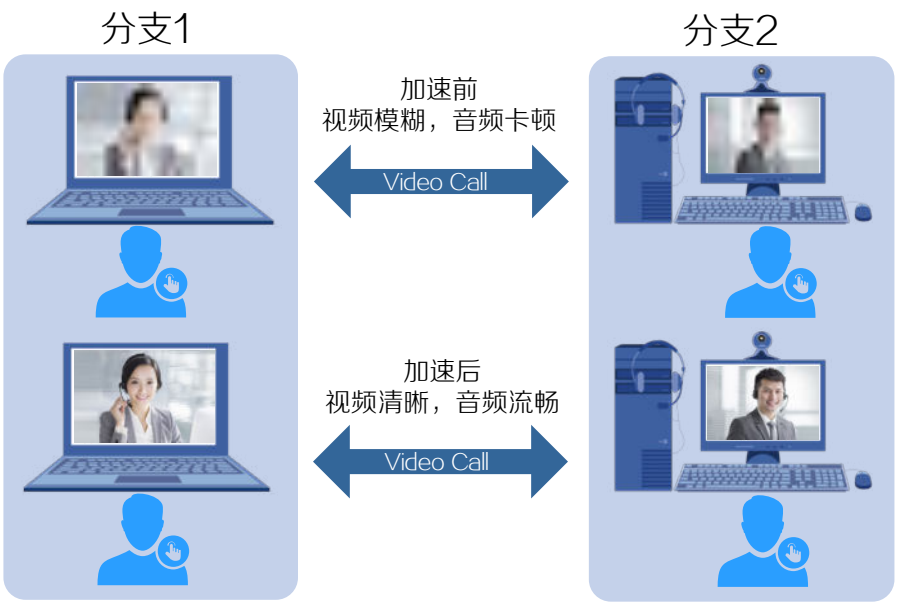
(3) **FEC 解码**：缓存接收的数据包，在解码超时时间内，如果原始数据包和冗余包之和等于或大于分组数据包数，进行 FEC 解码；否则直接发送原始数据包，丢弃冗余包 R。

图30 FEC 工作原理示意图



如图 31 所示，应用流量高质量传输的场景中，全面 WAN 加速利用 FEC 前向冗余纠错技术将数据复制传输、去重排序，可以提升应用流量的抗丢包能力和传输质量。

图31 FEC 加速



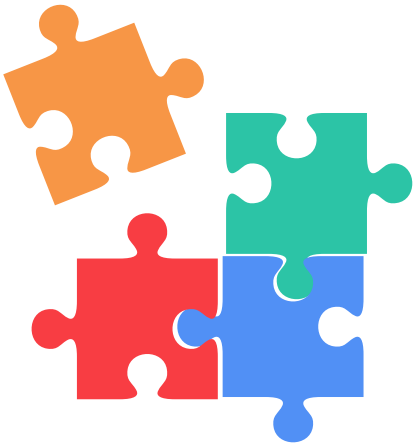
客户价值

FEC 技术的引入，为金融机构提供了一种有效的解决方案来应对网络公共接入带来的安全威胁。具体的客户价值包括：

- **保障关键数据传输的安全性**：FEC 确保金融数据在公共网络上的传输得到高级别的安全保护，这对于金融网点至关重要。
- **优化音视频流的传输质量**：通过 FEC 技术，即使在高丢包率环境下，音视频流仍能流畅播放，提供无卡顿、无花屏的会议体验。

- **提高传输效率与网络稳定性**：FEC 通过动态调节冗余包的数量，在确保通信质量的同时，尽量减少带宽占用，提升了整体网络的效率和稳定性。
- **增强客户信任度**：高性能的网络安全措施增强了客户对金融机构的信任，进而提升了服务评价和满意度。

图32 客户价值



数据传输更安全
确保金融数据在公共网络上传输时的高级别安全保护

音视频质量优化
提供无卡顿、无花屏的流畅会议体验

传输效率和稳定
动态调节冗余包数量，提升整体网络的效率和稳定性

增强客户信任度
高性能网络安全措施提升了客户对金融机构的信任和满意度

多发选收技术：增强数据传输可靠性

技术背景

多发选收技术是另一项关键的确定性网络技术，旨在提升广域网链路异常中断下的传输可靠性。
在高可靠性网络环境中，关键业务不仅需要网络切片技术来保证零丢包环境，而且还必须具备应对链路中断的保护机制。特别是对于可靠性要求极高但流量相对较小的业务（如远程操作、电子支付、紧急呼叫、VoIP 等），采用多发选收技术来增强传输的可靠性成为一种理想的方案。

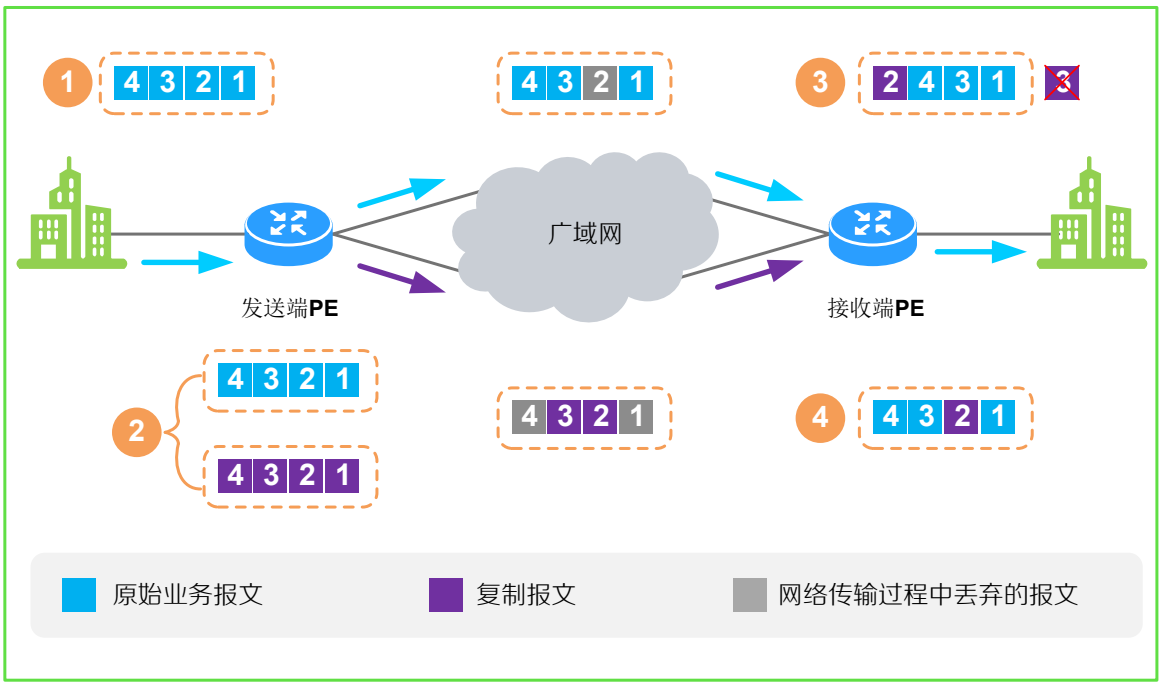
技术简介

多发选收技术通过在发送端复制数据包并通过多条路径转发，再在接收端进行排序和去重，确保数据包的完整性和一致性。
如图 33 所示，通过多发选收技术实现广域网链路异常中断时的零丢包保护基本原理如下：

- **发送端处理**：发送端的 PE（Provider Edge）设备为启用多发选收技术的接口添加重组头，其中包含了报文 ID、时间戳等重要信息，用于报文的重组和排序。PE 设备将数据包复制，并为每个副本封装重组头信息后，通过不同的链路发送。
- **接收端处理**：接收端的 PE 设备负责对收到的所有数据包（包括原始包和复制包）进行排序和去重操作，确保数据包的完整性和一致性。接收端还会设置数据包重组的等待时间和抖动容忍度，以优化基于丢包、时延或抖动的传输效果。

多发选收技术通过提供冗余的传输路径和对接收端数据包处理的细节优化，确保了即使主链路发生中断，关键业务流的数据包也能通过备选路径安全到达接收端。这种方法不仅保障了数据的完整性和无损传输，也满足了关键业务对于高可靠性网络的需求。

图33 多发选收技术原理示意图



客户价值

多发选收技术为金融业务广域网带来了显著的客户价值，主要包括：

- **零丢包保障**：在链路发生丢包时，通过等待其他备份链路上具有相同序号的数据包，确保多路径传输的丢包率最低。
- **最低时延优化**：通过直接转发从多条链路接收到的首个数据包，确保多路径传输的单数据包传输时延最低。
- **平滑抖动控制**：当超过预设的抖动容忍时间后，发送接收到的缓存数据包，确保多路径传输中的抖动最小化。

图34 多发选收技术的客户价值

6.3 带宽优化与效率提升技术

基于硬件的端到端数据压缩技术：提升带宽利用率

技术背景

在广域网环境中，带宽是极其宝贵的资源，特别是在需要在分支机构与总部或数据中心之间进行大规模数据传输的场景中。尽管基于 IPv6+的灵活选路技术已有效提升了链路的负载分担能力和带宽利用率，但在面对更大规模的数据传输时，进一步减少广域网带宽、降低网络运营成本的需求依然迫切。在这种背景下，硬件加速的高性能数据压缩技术显得尤为重要，它能提供更高的压缩效率和更低的延迟，同时处理更高的数据负载。

技术简介

面对广域网环境中的高带宽需求和运营成本问题，H3C 推出的基于专用硬件的高性能端到端数据压缩技术，旨在最大程度上减少带宽消耗，同时保持数据传输的高效率和低延迟。该技术通过专用硬件压缩卡实现高性能数据压缩，相比传统软件实现的压缩技术，提供了更优的压缩效率和更低的延迟。此外，技术支持 IPPCP（IP Payload Compression Protocol，IP 负载压缩协议）标准协议，能够适用多种压缩算法，如 LZ 和 ZSTD，包括其字典压缩特性和 AI 训练字典特性，以满足不同的数据压缩需求。

H3C 的端到端数据压缩技术包含以下关键步骤：

(1) **业务分类与识别**：通过五元组精细化匹配，系统精确地分类和识别不同的业务数据流，确保数据压缩策略能针对性地应用。

(2) **硬件加速压缩**：使用硬件压缩卡执行特定的压缩算法，如 LZ 或 ZSTD，根据数据类型和需求动态选择算法。

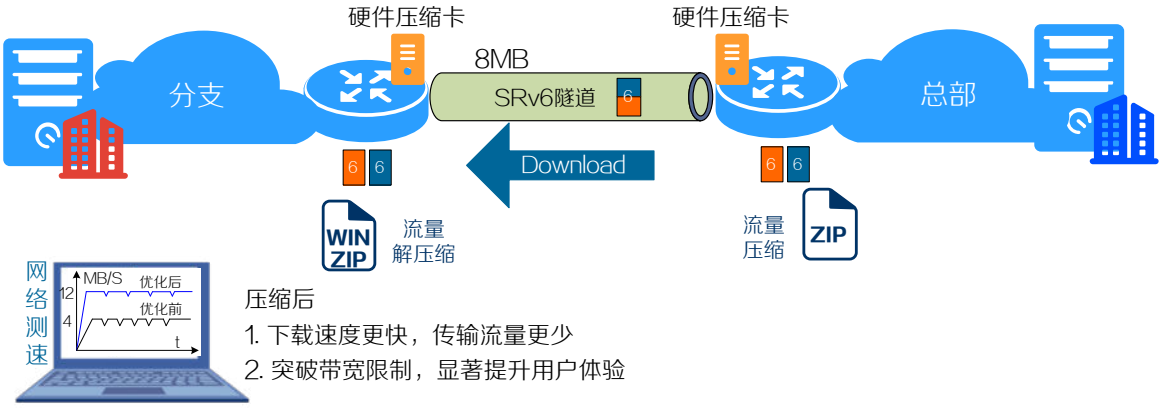
(3) **IPPCP 封装与传输**：压缩后的数据通过 IPPCP 进行封装，优化数据包大小，确保与接收端的兼容性和互操作性。

(4) **隧道引流与传输**：压缩后的数据被引流到预设的隧道（例如 SRv6 隧道）中进行高效传输。

(5) **端到端解压缩**：在数据到达目的地后，使用相同的硬件压缩卡进行解压缩，恢复数据到其原始状态，确保数据的完整性和准确性。

(6) **完整性校验**：每个压缩和解压后的数据包都进行 CRC 校验，以确保数据传输的一致性和无误。

图35 端到端数据压缩，提升带宽利用率



客户价值

采用端到端数据压缩技术，金融机构能够获得以下显著的价值：

- **降低带宽需求**：数据压缩显著减少了传输过程中所需的带宽，减轻了对昂贵专线资源的依赖，降低了相关成本。
- **提升传输效率**：压缩后的数据体积更小，传输速度更快，提高了数据同步和恢复的效率，强化了业务的敏捷性。
- **高效处理能力**：H3C 端到端数据压缩技术以高性能为标准，确保即使在数据高负载情况下也能保持高效的处理能力。
- **广泛的产品兼容性**：从高端到低端的产品线均支持数据压缩功能，使得从网点到分行的端到端数据压缩成为可能，满足不同规模金融机构的需求。

图36 客户价值

降低带宽需求
减少带宽，节省成本

提升传输效率
传输更快，业务敏捷

高效处理能力
高性能单卡，能力高效

广泛兼容性
全线兼容，满足需求

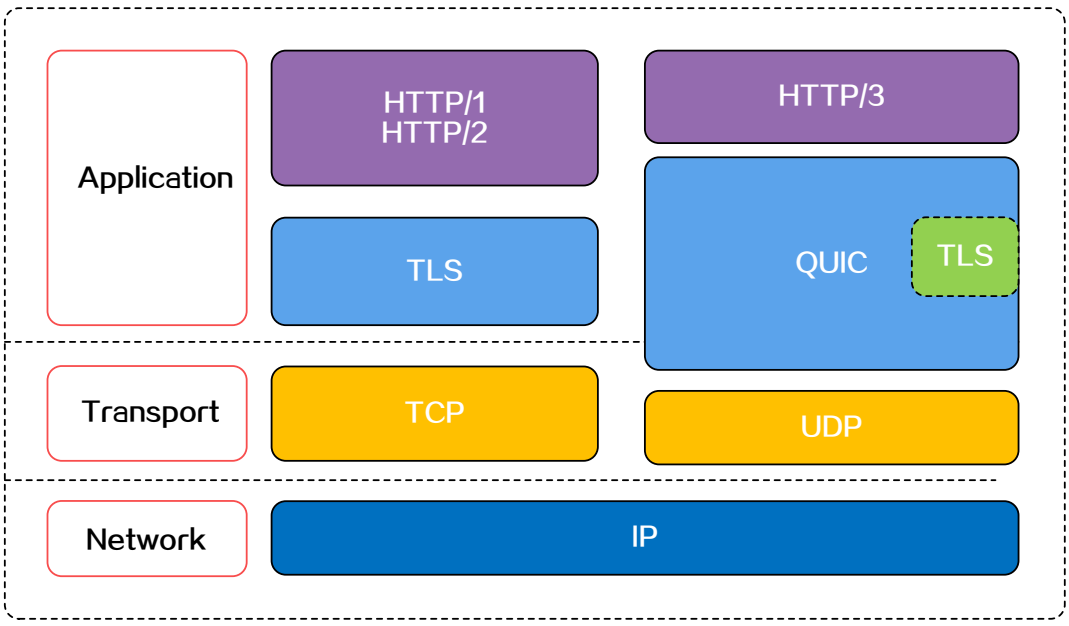
QUIC 传输技术：更快、更稳、更高效的网络传输

技术背景

随着互联网技术的快速发展，传统的 TCP/IP 网络传输协议在处理高并发、低延迟和高效数据传输方面遇到了诸多挑战。特别是在移动网络和高延迟环境下，TCP 协议的三次握手过程和严格的顺序传输要求常常导致显著的延迟以及不理想的用户体验。此外，由于 TCP 和 TLS/SSL 的握手过程是分开的，这进一步增加了建立安全连接所需的时间。例如，对于采用 SD-WAN 隧道技术的客户来说，从专线切换到互联网链路后，依然希望能够获得高质量的流量传输，提供类似专线的高质量。然而，传统的 TCP 传输协议在面对互联网线路的丢包、时延和抖动问题时，难以保持高效的传输性能。

为了解决这些问题，业界提出了 QUIC（Quick UDP Internet Connections，快速用户数据报协议互联网连接）技术，旨在提高网络传输的效率和安全性。H3C 在 SD-WAN 等隧道中采用 QUIC 进行传输层封装，显著提升了网络传输的效率、安全性和稳定性，尤其是在复杂网络环境下。

图37 TCP 与 QUIC 协议栈层级对比示意图

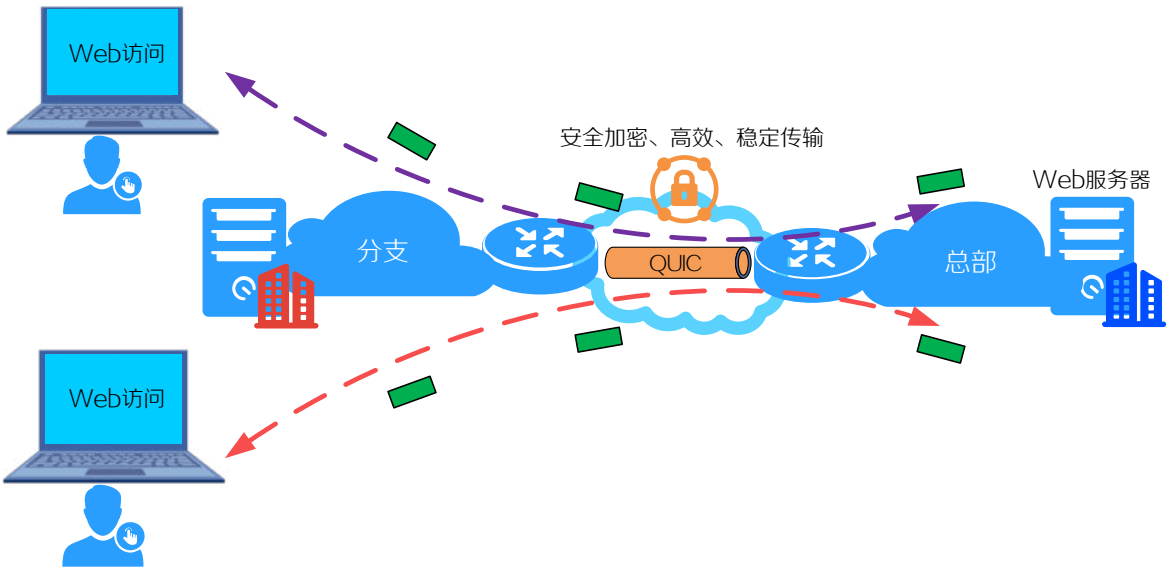


技术简介

QUIC 是一种基于 UDP 的安全多路复用并发传输协议，集成了多路复用、加解密和拥塞控制等功能。它结合了 TCP、TLS/SSL 和 HTTP/2 的优点，在 UDP 上实现面向连接和可靠性特性，从而提供更加可靠、安全且高效的网络传输服务。QUIC 的核心特性包括：

- **多路复用与流量控制**：QUIC 允许通过单个连接并行传输多个数据流，减少了头部阻塞问题，从而提升数据传输效率。每个数据流都有独立的流量控制和优先级设置，使一个数据流的延迟不会影响到其他数据流。这不仅提高了网络效率，还显著优化了用户体验，尤其适用于现代网站、应用程序和多媒体流式传输。QUIC 通过消除 HTTP/2 中的队头阻塞问题，进一步提升了多路复用性能。
- **快速连接建立与握手**：QUIC 支持零往返时间（0-RTT）连接建立，使客户端和服务器在握手阶段即可开始数据传输，显著减少连接建立时间。通过预共享密钥（PSK）或先前连接信息，QUIC 减少了握手次数，实现快速重连。这不仅提高了初次连接的响应速度，也在高频交易和频繁登录环境中显著减少了延迟。
- **内置加密**：QUIC 协议内嵌 TLS 1.3 加密，保障数据传输安全。与 TCP+TLS 相比，QUIC 整合了加密握手过程，提高了安全连接建立的速度和效率，从而确保数据在传输过程中始终保持高度加密状态，预防中间人攻击和数据劫持，保障数据隐私和完整性。
- **连接迁移**：QUIC 连接具有唯一标识，即使客户端的 IP 地址发生变化，连接也能保持活跃。通过维护连接的唯一标识符，QUIC 允许在网络环境变化时保持连接不变，用户可以无缝继续当前操作。这确保了移动金融应用的稳定性和连续性，提升了网络切换时的用户体验。这一特性对移动设备尤其重要，避免了频繁的连接中断。
- **改进的拥塞控制**：QUIC 引入新的拥塞控制算法，通过动态调整数据传输速率并响应网络拥塞情况，优化网络资源利用。这样，QUIC 有效管理网络流量，减少延迟，提高整体传输效率。这在处理金融市场交易高峰期和大量并发请求时尤为重要，确保服务传输高效稳定。

图38 QUIC 传输技术：优化传输效率和带宽利用



如表 4 所示，为了更直观地了解 QUIC 与传统 TCP 在各方面的具体区别，详细列出了传统 TCP 与 QUIC 的区别。

表4 传统 TCP 与 QUIC 的技术对比

特性	传统 TCP	QUIC
连接建立时间	三次握手，耗时较长（至少一个RTT）	支持0-RTT和1-RTT握手，显著加快连接建立速度

特性	传统 TCP	QUIC
多路复用与丢包处理	存在头部阻塞问题，丢包影响整个连接	原生支持多路复用，无头部阻塞，单一流的丢包不影响其他流，快速恢复
TLS/加密	独立于TCP进行，多个RTT增加握手时间	内置TLS 1.3，简化加密处理且提高安全性
连接迁移	基于IP地址和端口，IP变化导致连接中断	使用唯一标识符，支持IP变化下的无缝连接迁移
拥塞与流控性能	依赖TCP版本的算法,单一流量控制机制	使用新算法优化拥塞控制，每个数据流有独立的流量控制，更高效
快速重连	重新连接需要多次握手	通过预共享密钥快速重连
数据传输与网络适应性	受RTT和头部阻塞影响,适用于稳定网络环境	优化的多路复用和快速握手提高数据传输效率，更好适应不稳定和移动网络环境
安全性与中间人攻击风险	独立TLS配置和验证，存在一定风险	内置TLS 1.3加密，减少中间人攻击风险
广域网和移动网络支持	受到延迟和丢包影响较大，IP变化需重建连接	提供快速、稳定、安全的数据传输，支持连接迁移，移动网络切换更平滑
对用户体验的影响	高延迟和丢包可能影响体验	提供流畅和稳定的用户体验，特别适合延迟敏感应用

综上所述，QUIC 技术通过其独特的高安全性、高性能和可扩展性，正迅速成为未来互联网传输协议的重要选择。其在高延迟和高丢包网络环境中的显著优势，使其特别适用于延迟敏感的应用场景。H3C 将 QUIC 应用于 SD-WAN 等隧道技术中，不仅提升了网络传输效率和稳定性，还为用户提供了更稳健的网络体验。

客户价值

应用 QUIC 技术后，金融机构能够显著提升其网络性能和用户体验，带来以下客户价值：

- **提升传输性能与用户体验**：QUIC 通过减少连接建立时间和解决 TCP 头阻塞问题，显著提升了 Web 应用和服务的加载速度，特别是在高延迟网络环境下。此外，在视频会议和在线交易等对网络延迟敏感的应用中，QUIC 提供了更为流畅和稳定的体验。
- **增强安全性与支持移动网络**：QUIC 默认启用加密，提供更强的安全保障，减少中间人攻击的风险。同时，凭借其连接迁移特性，QUIC 能够在移动设备网络切换过程中维持稳定的连接，减少了连接断开和重连所需的时间，从而大幅改善了移动网络的用户体验。
- **优化广域网长距传输**：QUIC 通过其快速、稳定和安全的数据传输服务，满足了广域网长距离传输对带宽和协议效率的需求，从而优化了长距离数据传输的性能和可靠性。

图39 客户价值

Web Cache 技术：提升业务访问速度

技术背景

在金融行业，分支网点经常遇到专线带宽资源紧张和成本高昂的双重挑战。随着业务量的不断增长，这些网点迫切需要提高带宽的利用效率。客户期望能够在不牺牲业务连续性的前提下，减轻文件下载和网页浏览对带宽资源的压力。因此，存在一个突出的需求，即在维持甚至降低成本的同时，优化带宽的分配和使用，以保证关键业务的顺畅进行。

针对金融分支网点的特定需求，Web Cache 技术在以下应用场景中发挥了其最大潜力：

- **金融网点数据访问**：在金融网点日常操作中，职员和客户频繁访问银行的内部系统和公共金融信息网站。通过 Web Cache 技术，这些常访问的页面被缓存在本地，当再次请求相同数据时可直接从缓存中提供，从而加速数据的检索速度，提升用户体验。
- **高峰时段的流量管理**：在业务高峰时段，如工资发放日或促销活动期间，金融网点面临巨大的数据访问压力。Web Cache 技术帮助平衡这些峰值流量，确保网络的稳定性和响应速度。
- **远程地区网点**：对于位于带宽资源较为有限的远程地区网点，Web Cache 技术特别有益，因为它能显著降低对中央数据中心的依赖，提高数据访问速度，同时降低带宽成本。

技术简介

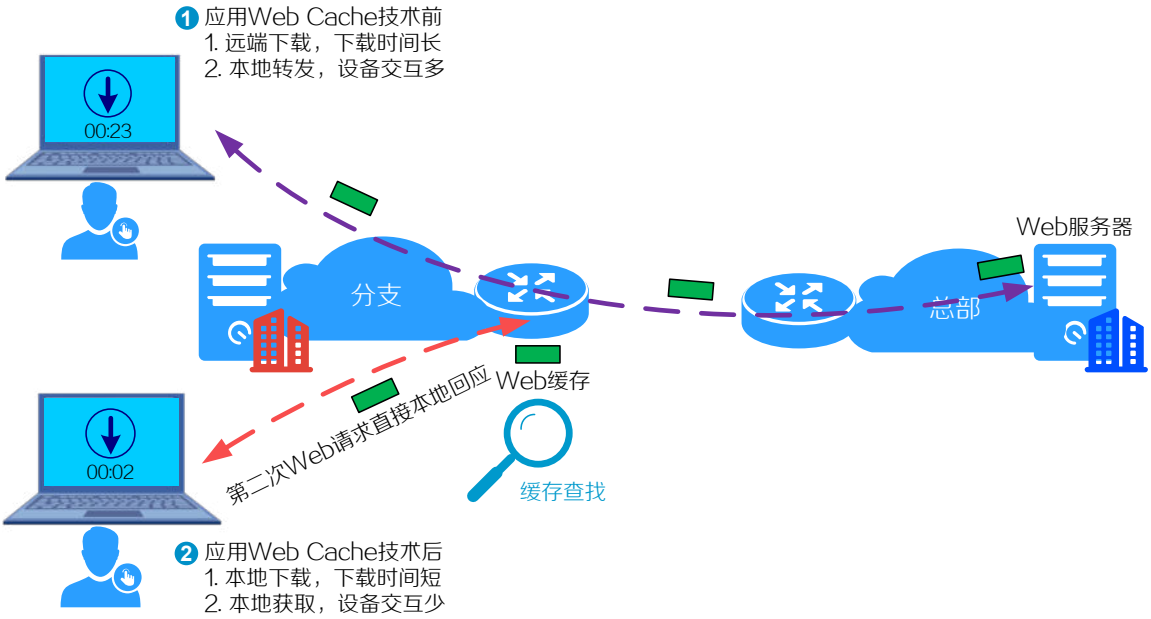
为响应金融分支网点对带宽资源优化和成本控制的迫切需求，H3C 引入了 Web Cache 技术。此技术充分利用本地缓存机制，直接对应提升带宽效率和降低网络相关成本的挑战。具体实现步骤包括：

- **创建本地缓存**：当用户首次访问某个 Web 页面时，Web Cache 技术将页面内容储存到本地设备，减少了因重复请求相同内容而产生的带宽消耗。
- **缓存更新与维护**：为确保内容的新鲜度和准确性，系统将按照设定的策略定期更新本地缓存，或在内容发生变更时及时刷新。
- **快速响应请求**：当用户再次请求先前访问过的 Web 页面时，系统能够迅速从本地缓存中提供数据，避免了对远程数据中心的额外访问，从而减少了对主要带宽的依赖。
- **优化带宽使用**：通过消减重复数据传输，Web Cache 技术显著提升了带宽的利用率，特别是在高流量的业务高峰期，有助于平滑带宽使用曲线，避免出现瓶颈。

通过应用 Web Cache 技术，金融分支网点能够更高效地管理其带宽资源，确保了业务的持续性和响应速度，同时有效控制了运营成本。

如图 40 所示，在应用数据高频访问的场景中，利用 Web Cache 技术将应用数据缓存到本地。当再次访问时，数据可以直接从本地缓存获取，从而减少设备与服务器之间的交互压力，并提高应用的访问速度。

图40 Web Cache 加速



客户价值

应用 Web Cache 技术后，金融机构能够实现以下显著的价值提升：

- **提高业务效率**：通过本地快速获取缓存的网页内容，显著减少了数据检索时间，从而加快业务流程，提升整体工作效率。
- **降低运营成本**：通过优化带宽利用率和减少对远程数据中心的数据传输需求，Web Cache 技术有助于显著降低网络运营成本。
- **增强用户体验**：数据访问速度的加快减少了客户等待的时间，增强了客户满意度和忠诚度，用户体验得到显著提升。
- **提升网络稳定性**：在高流量时段，通过本地缓存减轻了对网络的压力，保障了网络的稳定性和可靠性，避免了潜在的服务中断。

图41 客户价值

通过这种方式，Web Cache 技术不仅解决了金融分支网点面临的带宽和成本问题，还为金融机构带来了具体的业务效益和客户价值，支持了其业务的发展和数字化转型。

6.4 网络可靠性增强技术

4G/5G 备份与电子围栏：提升网络可靠性与安全

技术背景

在当前数字化快速发展的时代，银行、保险等金融行业的网点和分支机构越来越依赖于稳定且灵活的网络连接。这些机构通常会采用具有 4G/5G 接入能力的路由器，并采购运营商的 5G VPDN 专线作为广域网线路的热备或冷备，以确保关键业务的连续性。对于地理位置偏远的站点，如离行 ATM，利用 4G/5G 网络进行连接不仅是一种便捷的解决方案，也是实现稳定接入的关键手段。随着 4G/5G 技术在广域网分支网络场景中的广泛应用，极大提升了网络的可用性，同时也带来了新的运维挑战。设备监控与管理成为网络运维的关键环节，对于确保设备的安全性和运行效率至关重要。

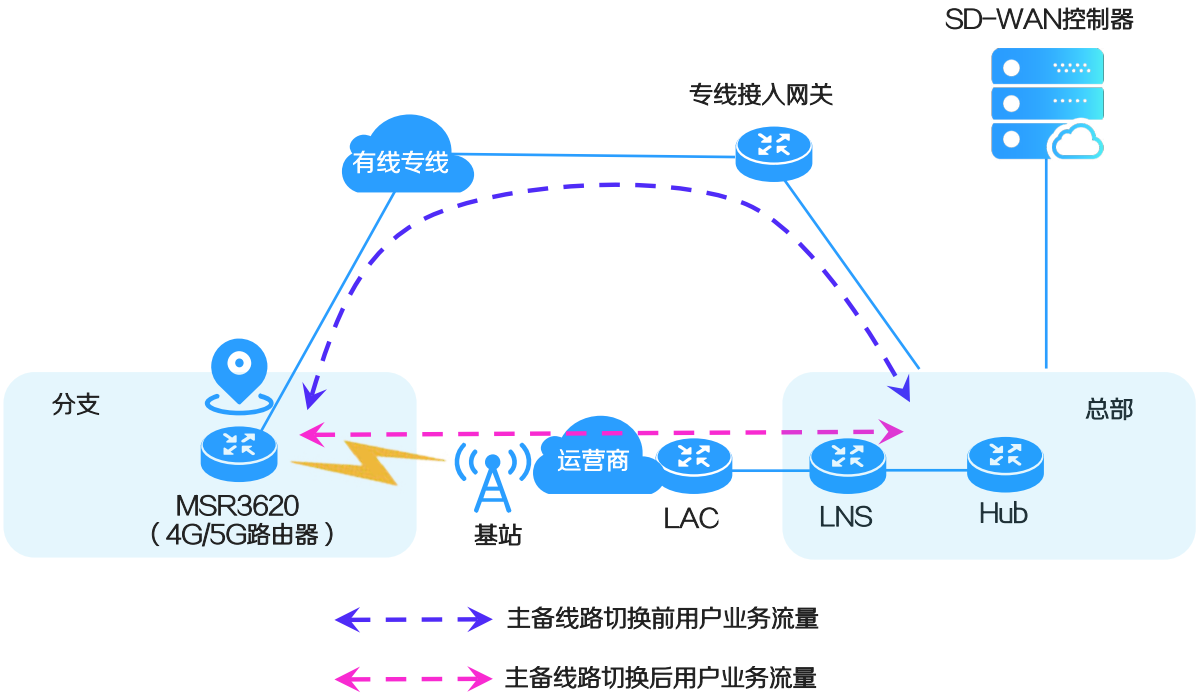
技术简介

在金融行业的分支网络中，有效管理和保护 4G/5G 设备至关重要。为此，H3C 结合 SRv6 SD-WAN 技术，提出了一套综合解决方案，旨在通过精确控制和增强安全性来管理 4G/5G 设备。其中，4G/5G 路由器是一种高度集成的设备，既支持传统的有线专线连接，又内置了 4G/5G 模块，以便同时兼容 4G/5G 无线网络和有线专线连接。这种设备通过其双重连接功能实现了无缝的网络切换能力，允许用户在有线专线和 4G/5G 无线网络之间自由切换，确保网络连接的持续稳定性和高效性能。

4G/5G 备份线路

如图 42 所示，为保证业务连续性和网络可靠性，在分支机构和总部之间部署了一条有线专线作为主线路，并配置了 4G/5G 线路作为备份。在主线路出现故障或通信质量不符合预设标准时，系统会自动切换到 4G/5G 线路。

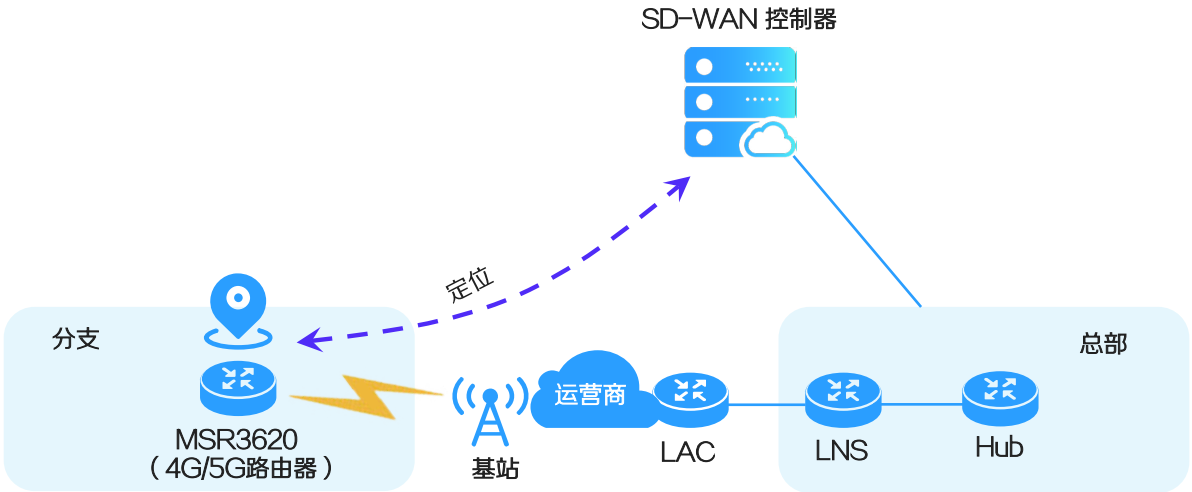
图42 4G/5G 线路备份



设备定位

如图 43 所示，通过集成 SD-WAN 的控制功能，实现设备位置的实时监控和管理。一旦 4G/5G 设备上线，即可利用 SD-WAN 控制器上的基站信息查询设备的经纬度和地理位置。

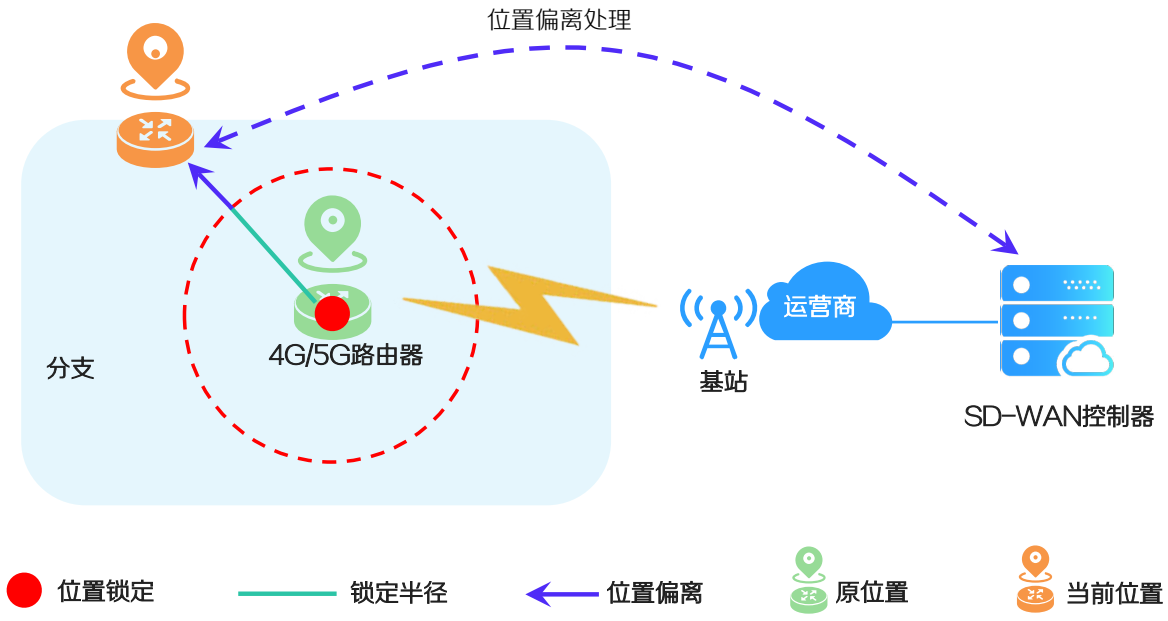
图43 设备定位示意图



电子围栏

如图 44 所示，通过设置电子围栏策略，确保设备仅在授权的地理范围内操作。设备若偏离预定位置，系统将自动触发安全告警并采取必要措施。

图44 电子围栏示意图



综合使用 SRv6 SD-WAN 的先进技术和 4G/5G 的快速接入能力，本方案不仅满足了金融机构对于网络稳定性和安全性的要求，同时也为决策者和技术人员提供了一个清晰、高效的网络管理工具。这种集成化管理不仅简化了运维过程，还提供了对未来网络发展的强大适应性。

客户价值

该技术方案的客户价值主要体现在以下几个方面：

- **提高网络可靠性**：采用 4G/5G 技术作为广域网线路的热备或冷备，确保在主线路发生故障时，业务能够无缝切换并继续运行，从而最小化了潜在的中断对金融业务运营的影响。
- **增强设备安全与监控**：通过实时的设备定位与位置锁定，确保所有接入的 4G/5G 设备在任何时候都处于网络管理员的监控之下，大幅降低了设备被非法移动或在未授权区域使用的风险。同时，电子围栏的划定为设备活动设定了明确的地理边界，增强了对敏感或偏远地区设备的安全防护。
- **优化设备管理效率**：基于 SD-WAN 的 4G/5G 融合管理使得网络操作更加精确和高效。网络运维人员可以实时掌握设备状态和位置信息，快速响应并解决可能的问题，从而维持网络的高效运行。

图45 客户价值

综上所述，这种基于 4G/5G 的设备管理方案不仅提高了企业对其分支网络的控制和安全性，也为企业提供了一个高效、灵活的网络管理工具，使其能够更好地适应快速发展的网络技术和业务需求。

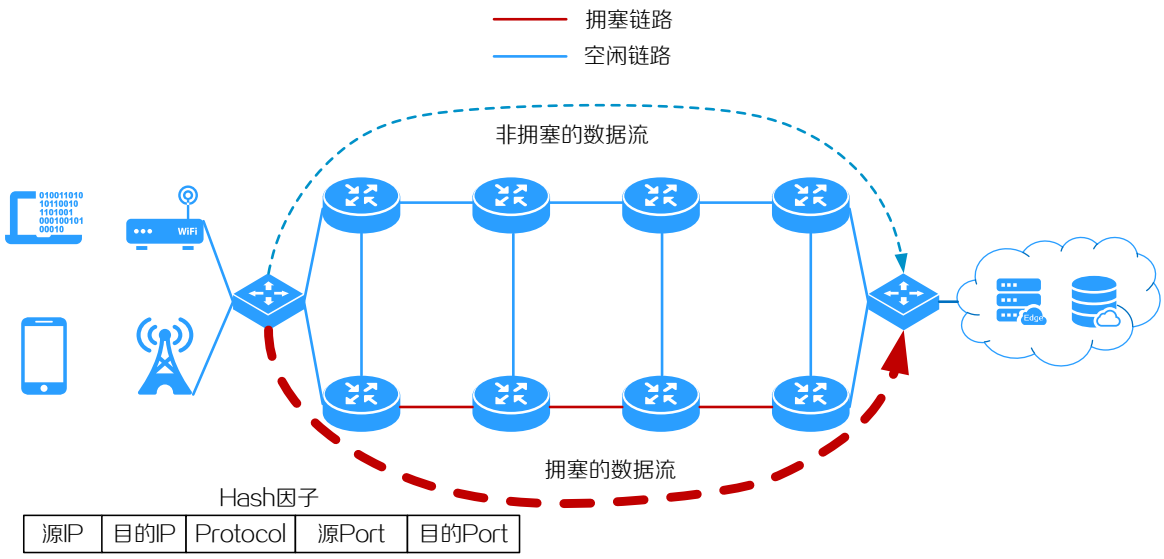
SRv6 TE Policy 高可靠性：高效路径管理与故障快速切换保障

技术背景

在金融行业，数据的稳定传输和高效处理至关重要。银行、证券和保险等金融机构不仅需要处理大量的交易数据，还需确保数据传输的可靠性和业务连续性。伴随着网络应用数据量的不断增长，传统的 IP 网络通常依赖于 ECMP（Equal Cost Multi Path routing，等价多路径路由）技术来实现高效的流量分配。ECMP 技术通过使用网络设备的五元组 Hash 计算来分配流量，但在面对大规模数据传输时，ECMP 存在一些局限性：

- **业务流负载波动**：ECMP 的流量分配依赖于静态的 Hash 计算，这可能导致在网络条件变化时（如链路故障或拥塞）流量分配不均，从而影响金融交易的稳定性。
- **对网络故障的响应较慢**：当网络故障发生时，ECMP 可能需要较长时间来重新计算和稳定流量分配，这可能导致业务中断或性能下降，影响金融服务的连续性。

图46 Hash 算法进行逐流负载分担



技术简介

为了解决上述问题，H3C 的 SRv6 SD-WAN 解决方案采用了 SRv6 TE Policy 高可用传输技术。这项技术不仅通过在多条 SRv6 TE Policy 隧道之间均衡分担业务流量来细化流量管理，还能在任何链路发生故障时，迅速自动将流量转移到其他健康链路。这种快速、动态的流量管理和故障响应机制显著提升了业务的连续性和网络的稳定性。与 ECMP 相比，SRv6 TE Policy 提供了：

- **更智能的路径管理**：SRv6 TE Policy 通过先进的算法控制路径选择和调整，将大流量数据更均匀地分配在多条并行路径中。与传统的 Hash 算法相比，这种方法显著提高了数据传输的稳定性，满足金融行业对高并发和低时延的需求。
- **业务级保护与快速故障恢复**：通过 VPN FRR 和 SRv6 TE FRR 技术，SRv6 SD-WAN 解决方案提供了业务级保护和路径热备份功能。这些技术支持在多条有效路径间快速切换，当主路径故障时，数据流可快速切换到备用路径或 SRv6 BE 路径，确保业务的连续性。
- **灵活的路径保护和流量调度**：SRv6 TE Policy 支持多种路径保护和流量调度机制，例如 BFD 检测机制和 TI-LFA FRR 绕行故障节点或链路的功能。通过 SRv6 的 SID 列表管理，网络管理员可以灵活定义和管理数据流的转发路径，提高网络的可维护性和扩展性。

综上，流量通过 SRv6 TE Policy 转发时，高可靠性机制能够实现多层次、多级别的业务保护（例如节点链路级保护、路径级保护等）。如图 47 和图 48 所示，展示了 SRv6 TE Policy 高可用传输机制，通过应用 SID 列表和备份路径设计，实现了数据流的可靠传输与保护。

图47 多 SRv6 TE Policy 多转发路径分担业务流量逻辑示意图

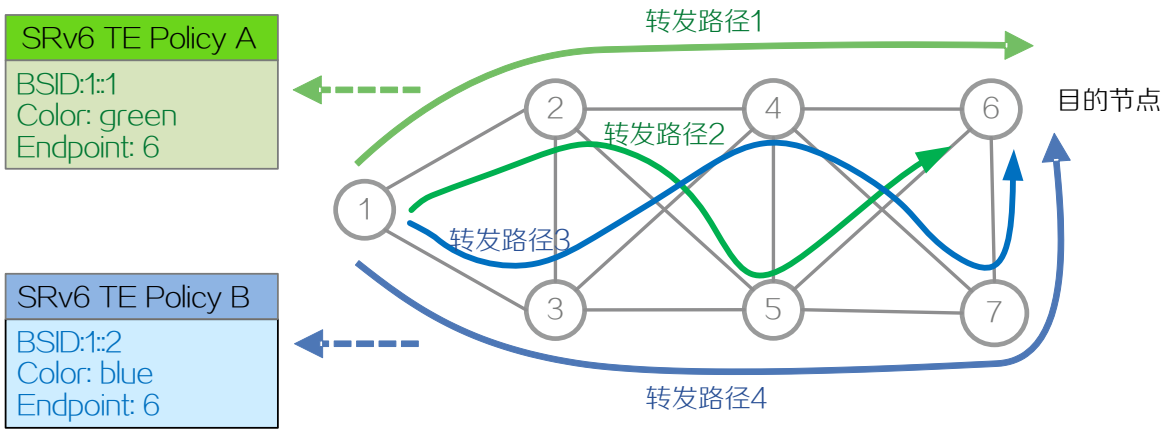
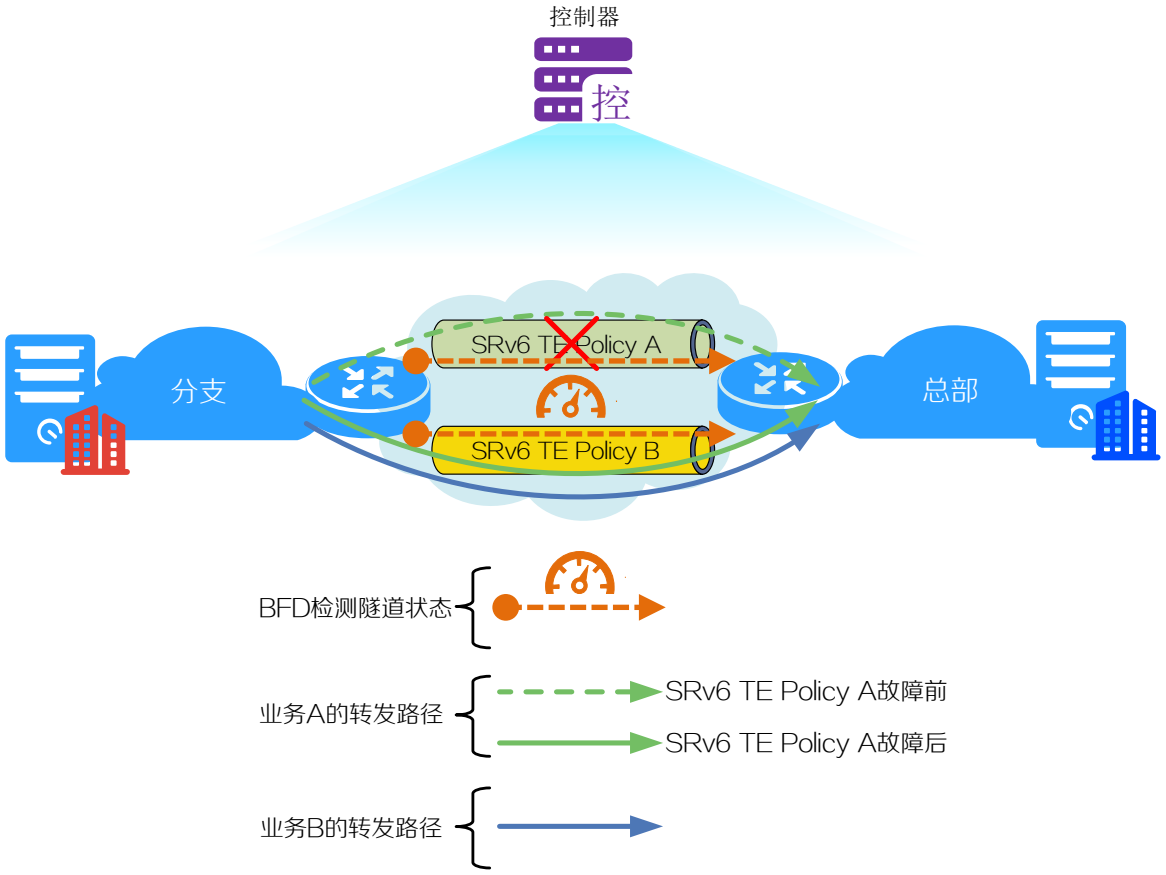


图48 SRv6 TE Policy 故障切换保护功能示意图



客户价值

通过采用 H3C 的 SRv6 TE Policy 高可用传输技术，金融行业客户可获得以下显著价值：

- **高效稳定的数据传输**：SRv6 TE Policy 显著提升了流量分配的灵活性和稳定性，避免传统负载波动问题，在高并发和大流量业务场景中提供一致的传输性能。

- **快速故障切换**：通过 FRR 和 BFD 技术实现快速故障切换和检测，大大缩短了故障恢复时间，确保业务的连续性和可靠性。
- **优化的网络资源利用**：灵活的路径定义和流量调度机制均衡数据传输，避免路径过载，提高全网资源利用效率。
- **增强的网络可维护性**：通过 SID 列表和可定义的路径策略，管理员可以动态调整和优化网络结构，无需更改底层硬件。

图49 客户价值

H3C 的 SRv6 TE Policy 高可用传输技术，通过优化路径选择、增强网络架构灵活性以及改进故障恢复机制，实现了高效、稳定的数据传输，并具备快速故障恢复和优化网络资源利用的优势。该技术为金融行业提供了一个高效、可靠的大规模网络解决方案，支持金融机构的稳定运营和高效管理，确保关键业务数据的安全和连续性。

6.5 业务安全保障技术

跨 Internet 安全链路技术：保障连接安全

技术背景

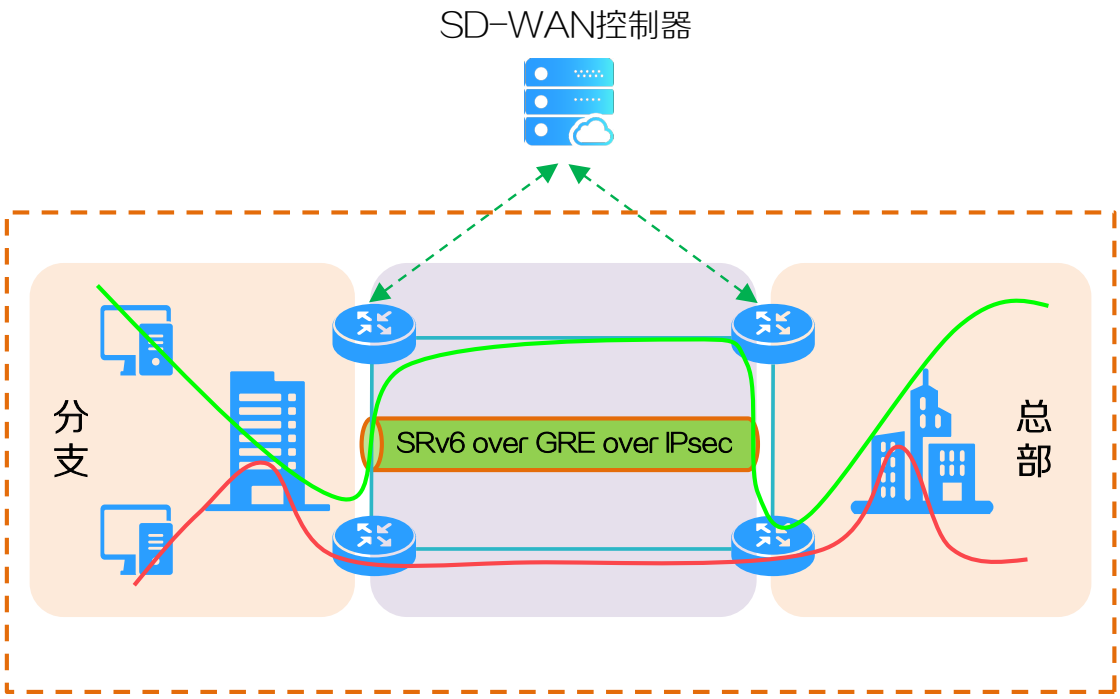
在当前的金融领域，随着网点和服务的数字化转型，对 Internet 和 5G 链路的依赖日益增加。这种转变带来了对网络安全性的高需求，特别是在数据传输过程中。金融数据的高度敏感性要求每次数据传输都必须高度安全，尤其是在使用公共网络如 Internet 或 5G 链路进行数据传输时，保护这些数据免受未授权访问或泄露的挑战更为严峻。因此，确保金融机构的数据安全，对防止金融欺诈、保护客户隐私和维护机构声誉至关重要。

技术简介

如图 50 所示，为应对这些安全挑战，H3C 采用了先进的 SRv6 over GRE 和 SRv6 over GRE over IPsec 技术，以加强在 Internet 及 5G 链路上的数据传输安全。具体来说：

- SRv6 over GRE：此技术通过封装原始数据包，在传输过程中隐藏了数据的原始信息，从而提升数据传输的安全性。
- SRv6 over GRE over IPsec：在 GRE 的基础上增加了 IPsec 层，提供了端到端的加密服务。这种双重保护机制确保了即使数据被截获，信息也因为加密而无法被解读。

图50 跨 Internet 安全链路，保障连接安全



客户价值

通过应用跨 Internet 安全链路技术，金融机构可以有效解决由于网络公共接入带来的安全威胁，从而保障关键业务数据的安全传输，支持业务的可持续发展和数字化转型。具体优势包括：

- **保障连接安全**：确保金融分支网点通过公共网络进行的所有数据传输都得到高级安全保护，防止数据泄露和篡改。
- **高性能加密**：H3C 提供的智能 IPsec 加密引擎性能支持高达 IMIX 35Gbps，确保即使在高数据流量下也能保持优秀的加密性能，不影响传输效率。
- **提升信任度**：增强客户对金融机构网络安全管理能力的信任，有助于提升机构的整体服务评价和客户满意度。

图51 客户价值

综上所述，这一技术方案不仅提高了企业对其分支网络的控制和安全性，也为金融行业提供了一个高效、灵活的网络管理工具，使其能够更好地适应快速发展的网络技术和业务需求。

iSec：面向大规模网络的随路加密技术

技术背景

随着现代网络架构的不断扩展和复杂化，传统的网络加密方法如 IPsec 显现出其局限性，尤其是在处理大规模网络和动态路由环境中的加密需求时。在金融等行业，业务规模的急剧扩张和对网络可靠性的高要求使得传统加密技术的短板变得尤为明显。例如，IPsec 作为点对点的加密技术，涉及复杂的配置和协商，尤其在大型网络中效率低下。此外，传统技术通常支持基于隧道的协商，不足以灵活处理针对路由和业务的加密需求。

为应对这些挑战，特别是在新兴的 SRv6 网络环境中，iSec 技术应运而生。iSec，作为一种基于 IPsec 技术框架和 BGP 扩展协议的新型自适应加密技术，支持点到多点的加密需求，并显著提高了部署的简便性和网络的可靠性。

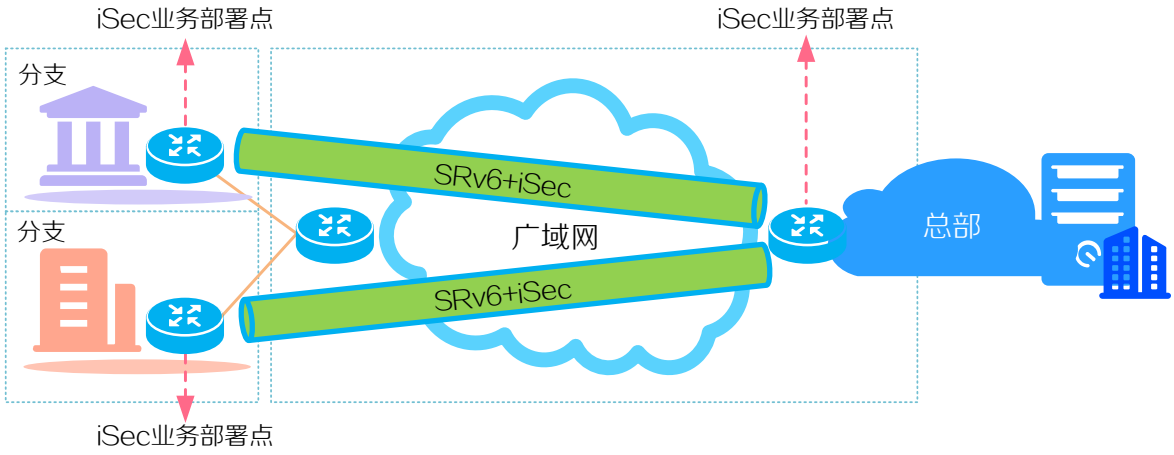
技术简介

什么是 iSec?

iSec 可以被视为一种更灵活、更智能的“安全隧道”。它基于 IPsec 和 BGP 扩展协议，自动为网络数据传输提供高级别的加密保护，无需复杂的手动配置。这一技术不仅简化了配置和增强了自动化，还实现了高效的加密部署和增强的网络可靠性。

在金融行业的应用中，随着银行分支网点和总行之间逐渐升级为 SRv6 网络，现网设备常采用 IPsec 对业务数据进行加密。然而，众多分行网点和总行之间的通信需要逐一部署，增加了管理复杂性。如图 52 所示，通过 iSec 随路加密技术对总行和分支网点之间的流量进行加密，只需单点配置加密成员列表，即可实现对加密节点的增减，极大地降低了配置和运维复杂度。

图52 组网示意图



iSec 如何工作?

想象您的网络是一个高效的智能快递系统，而 iSec 则是这个系统中保护每个“包裹”（即数据）安全、高效传输的智能快递箱。iSec 工作原理的简明解释如下：

(1) **建立安全快递服务（iSec 安全联盟）**

就像快递服务需要知道发件人和收件人的地址一样，iSec 通过建立“安全联盟”来确保数据包能够安全送达其目的地。这个过程自动化地确认了数据的发送和接收方，并确保传输途中的保护措施。这一过程中，iSec 在通信双方建立唯一的安全参数，确保入站和出站 IP 报文的安全处理。

(2) **包裹打包与安全检查（报文封装与加密验证）**

每个数据包在发送前都会被仔细打包，并加上特殊的安全锁（加密）和身份标签（验证），确保数据即使在传输途中被截获，也无法被未授权人员打开或篡改。这一过程中，iSec 使用强大的加密技术（如 AES）和数据验证方法（如 HMAC）来确保数据在传输过程中既安全又完整，不会被篡改或窃取。

(3) **智能钥匙的交换与管理（密钥交换与动态管理）**

iSec 采用 Diffie-Hellman 算法自动在发件人和收件人之间交换一把特殊的“钥匙”，使得只有正确的接收方才能解锁并阅读数据。这个过程完全自动化，通过 BGP 协议安全高效地管理密钥交换，极大简化了密钥管理

的复杂性。在这一过程中，iSec 通过 Diffie-Hellman 算法和 BGP 协议自动生成和管理这些“钥匙”，确保只有收件人能解密数据，整个过程自动化且高效，减少人为干预和错误。

(4) **提高快递系统的可靠性（高可靠性设计）**

iSec 确保即使在网络传输路径出现意外（如道路封闭）时，也能迅速找到新的传输路径继续送达数据包，保障数据传输的连续性和安全性。这得益于 iSec 的随路加密技术，它将业务隧道和 IPsec 加密隧道分离，允许快速路径切换和自动故障恢复，即使网络某个节点或链路出现问题，数据也能快速切换到新的传输路径，保持高可靠性。

通过这种方式，iSec 像一个智能且自动化的快递系统，确保了在互联网这个庞大网络中，数据包的传输既安全又可靠。无论对于大型网络还是对于有特殊安全需求的环境，iSec 提供了一种简单、高效且安全的数据保护解决方案。

表5 IPsec 与 iSec 的技术对比

特性 / 技术	IPsec	iSec
基本定义	一种端到端的安全协议，用于在IP网络中安全地传输数据	基于IPsec和BGP扩展，提供点到多点的自适应加密技术
主要优点	• 成熟稳定，广泛使用 • 提供强大的端到端加密 • 支持多种加密和认证算法	• 支持点到多点加密，适合大规模部署 • 简化配置和维护 • 提高网络的可靠性和灵活性
技术挑战	• 配置复杂，尤其在大规模网络中 • 点对点加密，难以扩展到大规模多点网络	• 需要现代化的网络基础设施支持 • 对 BGP 和 SRv6 的依赖性较高
加密方式	端到端加密	点到多点加密，适用于大规模网络
适用场景	• 小型至中型企业网络 • 端到端通信安全 • VPN 连接	• 大型网络组网，如云数据中心 • 高可靠性要求场景，如金融服务 • 跨域网络连接
部署复杂度	高，需要详细的配置和密钥管理	低，通过BGP实现自动化加密配置和管理
安全性	高，但需要正确配置来保证	高，且通过自动化减少人为配置错误的可能性
SRv6适用性	限制性较高，需要通过特定配置实现SRv6支持	高度兼容SRv6，特别优化以适应SRv6组网场景的需求

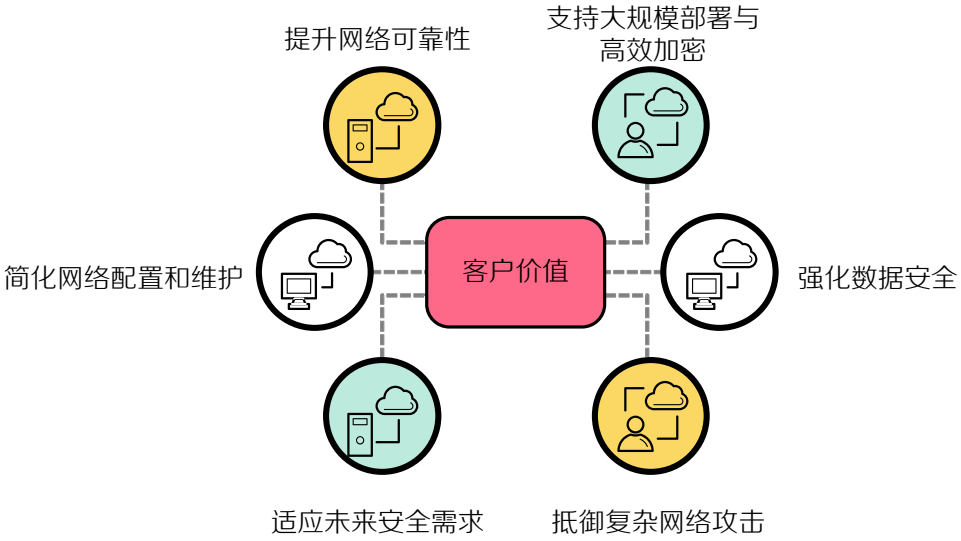
客户价值

iSec 技术为现代大规模和高要求的网络环境带来了以下关键的客户价值：

- **简化网络配置和维护**：通过利用 BGP 协议的点到多点发布机制，大幅简化了网络加密配置的复杂性，自动化配置和管理显著降低了维护成本。
- **提升网络可靠性**：支持业务随路加密，使加密过程与业务承载隧道解耦，即使在节点、单板、链路级别的故障情况下，网络依然能够保持高度的稳定性和可靠性。
- **支持大规模部署与高效加密**：点到多点加密能力使 iSec 非常适合 SRv6 组网场景，满足现代网络架构的大规模部署需求。
- **强化数据安全**：自动化的密钥管理和加密配置减少人为配置错误的可能性，提高网络安全性。

- **抵御复杂网络攻击**：借助 BGP 的动态和自适应特性，iSec 能够有效抵御复杂和先进的网络攻击，保护网络免受恶意侵害。
- **适应未来安全需求**：iSec 的设计考虑了未来网络发展的趋势，如对 SRv6 技术的支持，展示了其适应未来安全需求的潜力。

图53 客户价值



综上所述，iSec 为客户提供了一种既安全又高效的网络加密解决方案，尤其适用于大规模网络部署和高可靠性要求的场景。

SRv6 SFC 技术：简单、灵活、高效的安全保障

技术背景

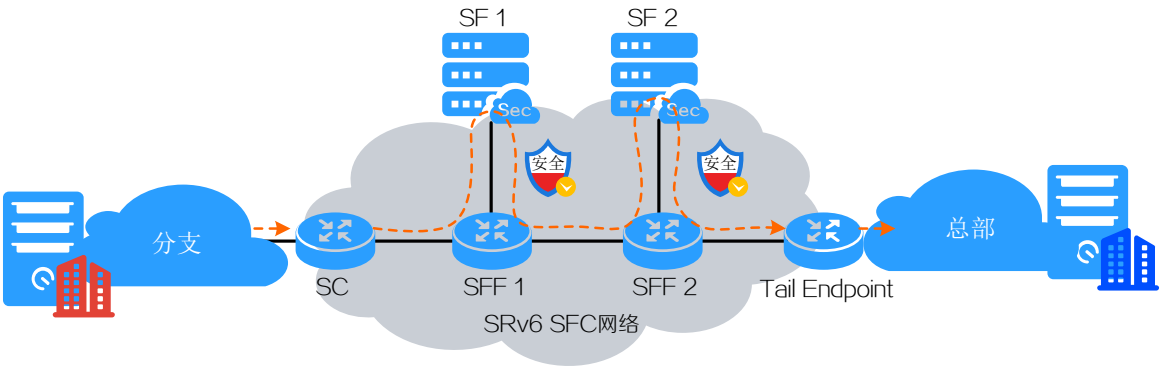
在数字化转型的加速过程中，金融机构正面临前所未有的网络安全和稳定性挑战。随着业务的全球化和互联网化，数据传输的需求不仅局限于高效率，而且需要保障业务的安全性。业务流量需要通过一系列精密的安全设施，如深度包检测 DPI、防火墙 FW、入侵防御系统 IPS 等，并遵循严格的业务逻辑顺序处理，以确保每一个数据包的安全。在传统的网络架构中，安全服务节点往往与特定的网络拓扑和硬件紧密结合，导致网络配置和安全策略变得僵化。这种硬件依赖性不仅限制了网络的灵活性，还使得对新兴安全威胁的响应速度变慢，同时也加大了新业务部署和维护的复杂性及成本。因此，迫切需要一种新的方法来克服这些挑战，提供更加灵活和可扩展的网络安全解决方案。

技术简介

针对上述挑战，SRv6 SFC 技术应运而生，为网络安全领域带来了创新的解决方案。SRv6 SFC 技术通过整合服务功能链（SFC）的思想和 SRv6 的高度可编程性，使得安全服务得以在网络中灵活部署和动态管理。这种技术利用了软件定义网络（SDN）和网络功能虚拟化（NFV）的核心优势，实现了服务与硬件的解耦，极大地提升了网络对安全威胁的适应能力，并优化了业务流量的管理和控制流程，为保障业务连续性和数据安全提供了坚实的技术基础。通过这种方式，SRv6 SFC 技术突破了传统网络安全解决方案的局限，提供了一种更加动态、灵活的方法来应对日益增长的网络安全需求，从而成为现代网络安全架构的关键组成部分。
简而言之，SRv6 SFC 技术就像为网络安全服务提供了一个“智能导航系统”，允许管理员根据业务需要灵活地将安全功能（如 DPI、FW 和 IPS）部署在网络中，确保数据沿着预设的安全路线传输，从而大幅提升网络的安全性、可管理性和可控制性。如图 54 所示，业务流量安全传输的基本流程如下：

- **流量分类与封装**：在网络边缘，SC 节点根据预设的安全策略将业务流量封装进 SRv6 报文，并引导至第一个 SFF 节点。
- **安全处理**：SFF 节点根据服务链路由，将流量按顺序转发至相应的 SF 节点进行安全处理。每个 SF 节点根据其配置执行特定的安全任务，比如 DPI、FW、IPS 等。
- **服务链顺序执行**：每经过每一个 SF 节点的处理后，流量通过 SFF 节点继续按顺序转发至下一个服务节点，直到完成所有安全检查。
- **流量返回**：经过全部安全处理后，业务流量在最后一个 SFF 节点被解封装，并转发至目标网络。

图54 SRv6 SFC 网络模型



客户价值

SRv6 SFC 技术为金融机构带来了显著的价值，主要体现在：

- **加强数据安全与业务连续性**：SRv6 SFC 技术使金融机构能够灵活部署和调整安全服务节点，如动态添加防火墙或入侵防御系统，以应对不断变化的安全威胁，从而加强对敏感数据的保护。此外，凭借可靠的服务链部署，即使某个安全服务节点发生故障，业务流量也能自动切换到备用路径或节点，确保服务不中断，从而提高业务连续性。
- **降低运营成本与增强网络灵活性**：利用 SRv6 SFC 技术，安全服务的部署和维护不再依赖专用硬件，金融机构现可在通用硬件上部署安全服务，降低了设备投资和运维成本。同时，SRv6 SFC 允许金融机构根据实时安全分析和策略调整，快速重构服务链中的节点顺序或功能，迅速响应网络安全威胁，确保金融网络防护能力始终保持在高度可靠的状态。
- **高度可编程性、动态管理与解耦服务**：SRv6 SFC 技术允许网络管理员精确控制数据包的路径，无缝集成安全策略与业务逻辑，实现了对网络流量的灵活控制。同时，网络功能虚拟化（NFV）的应用使得网络服务与底层硬件解耦，简化了网络设计和管理流程，进一步降低了成本。
- **增强可视化管理与配置的灵活性**：SRv6 SFC 服务链支持在控制器上可视化管理，显著提高了网络管理的透明度和可控性。此外，它提供的灵活配置选项（包括静态代理和伪代理），确保了在多样化的应用场景下依然能够有效增强网络的安全性和管理效率。

图55 SRv6 SFC 技术的客户价值

6.6 极简开局与智能运维技术

零配置开局技术：简化网络部署，提升运维效率

技术背景

在当今的企业网络环境中，特别是对于地理位置分散且设备数量众多的网络如金融机构和大型零售连锁，部署和维护分支网络设备面临着巨大挑战。传统方式部署新的分支网络时，设备安装完成后，需要专业 IT 人员到安装现场，对设备逐台进行手工配置，才能将设备接入网络，这不仅耗时且容易出错。为应对这些问题，H3C 推出了零配置开局（Zero Touch Provisioning，ZTP）技术，这种自动化网络部署方案能显著简化部署过程，降低成本，并提高部署效率。

图56 传统开局方式的痛点

技术简介

零配置开局是 H3C 推出的自动化网络部署方案。网络管理人员将基础连通性配置远程发送给设备，设备加电启动后自动完成配置加载，然后自动注册到 SD-WAN 控制器，由 SD-WAN 控制器完成设备纳管及网络业务配置下发。整个过程无需管理人员到现场进行开局配置，大大简化了开局过程，极大降低了开局成本。

零配置开局技术实现了设备的自动配置和部署，主要通过以下步骤实现：

(1) **基础配置准备**：网络管理员在远程服务器上预先配置新网关的基本设置，例如 WAN 接口的 IP 地址和拨号上网的账号/密码。

(2) **设备信息导入**：通过 SD-WAN 控制器导入新网关的信息，如设备名称、序列号和 Router ID 等。

(3) **现场简化操作**：开局人员在现场仅需进行简单的物理连接和设备上电操作。

(4) **自动注册与配置加载**：设备启动后自动从远程服务器加载配置，接入网络，并自动注册到 SD-WAN 控制器。

如图 57 所示，为适应不同网络环境和需求，零配置开局支持多种方式。

图57 零配置开局支持多种方式

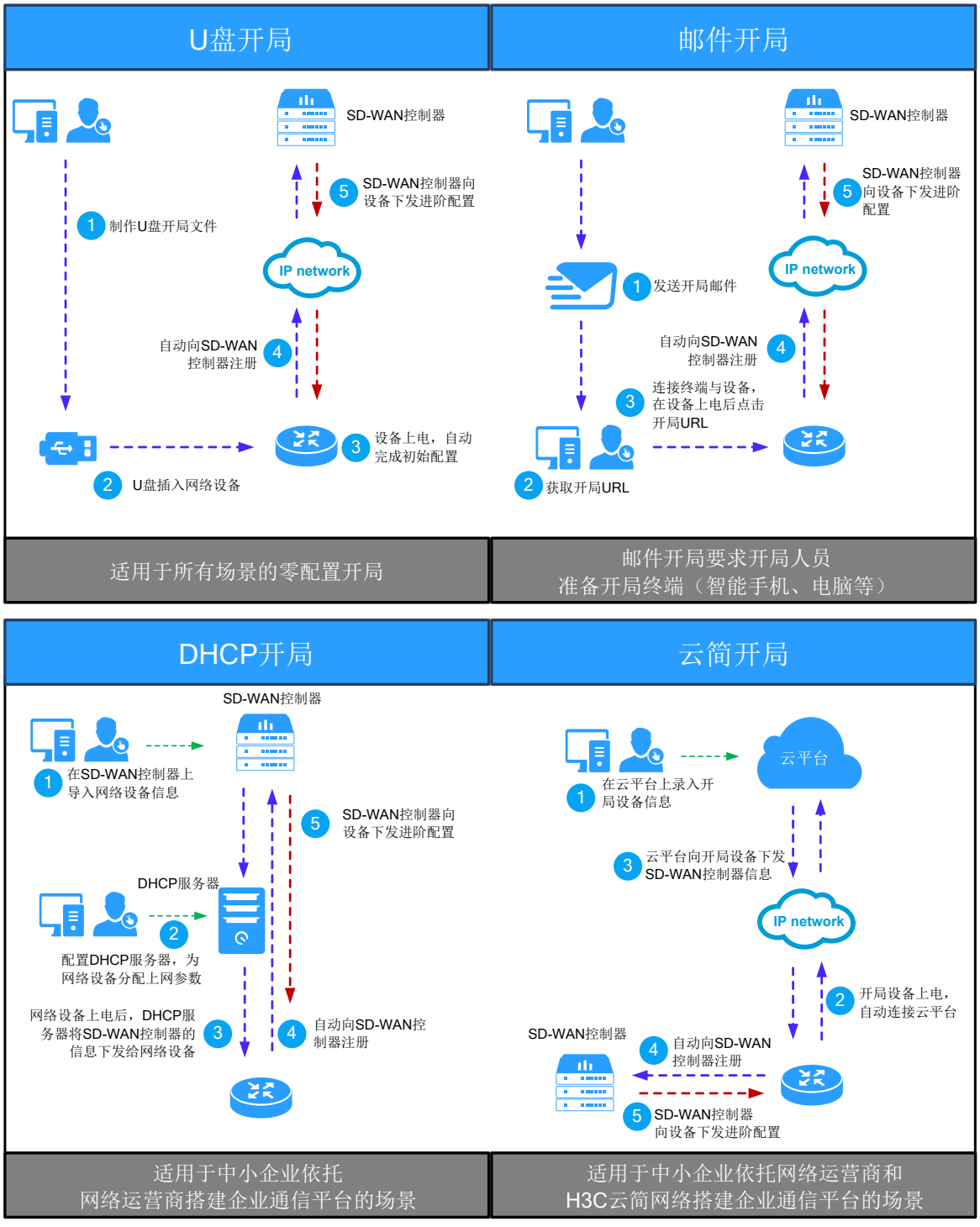


表6 不同开局方式功能和使用场景描述表

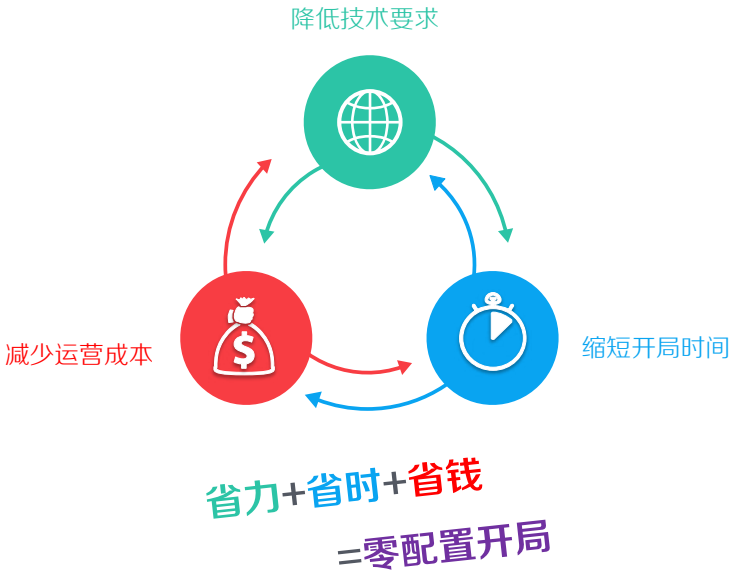
开局技术	功能概述	使用场景
U盘开局	通过在设备上插入U盘的方式来完成设备开局的一种技术	• 开局人员需携带开局 U 盘至现场，将 U 盘插入设备 • 即插即用，对开局人员的专业技能零要求
邮件开局	通过开局邮件下发配置来完成设备开局的一种技术	• 开局人员需准备开局终端（智能手机、平板电脑、笔记本电脑和 PC 等）来接收开局邮件，并将开局终端连接到设备 • 对开局人员的专业技能要求较低
DHCP开局	通过DHCP服务器下发配置来完成设备开局	• 要求管理员具有 DHCP 服务器的配置权限，且 DHCP 服务器支持 Option 253 • 即插即用，对开局人员的专业技能零要求
云简开局	通过H3C的云简管理平台自动下发配置来完成设备开局	• 要求在云简管理平台导入设备信息 • 要求设备能连接云简网络 • 即插即用，对开局人员的专业技能零要求

客户价值

零配置开局技术为企业带来以下核心价值：

- **极简部署与缩短开局时间**：通过最小化现场操作，利用远程管理和批量部署技术，显著简化网络设备的部署过程，将传统的按天部署缩短为分钟级，加快部署速度。
- **成本效率**：减少现场配置所需的技术人员数量和技术水平要求，降低人工成本、错误率以及人员差旅和食宿等费用，从而节省人力、物力和财力。
- **灵活性和自适应性**：支持多种开局方式，确保在各种网络环境下均能高效部署，增强适应性。
- **运维效率提升**：通过 SD-WAN 控制器进行集中管理和智能运维，提高运维效率和网络稳定性。
- **降低技术要求**：实现远程设备部署，界面向导式操作简化流程，使非专业技术人员也能进行现场操作，形成“0”门槛部署。

图58 客户价值



总之，零配置开局技术不仅优化了网络设备的部署流程，减少了错误，还提升了配置一致性，从而增强了网络的整体性能和可靠性。对于需要快速部署和轻松管理广泛网络设备的金融分支网络，这是一个极具吸引力的解决方案。

智能运维：大数据和 AI 驱动自动化网络运维

技术背景

随着互联网的快速发展进入大数据时代，网络业务的规模和数据流量都经历了显著的增长。这种增长带来了巨大的压力，尤其是在网络运维方面，传统的运维手段已经难以应对日益复杂的网络环境。问题的发现、定位和解决变得更加困难，需要更智能、更高效的解决方案。为了应对这些挑战，引入了智能网络分析和可视化运维解决方案，利用大数据和 AI 技术，提高网络运维的自动化和智能化水平。

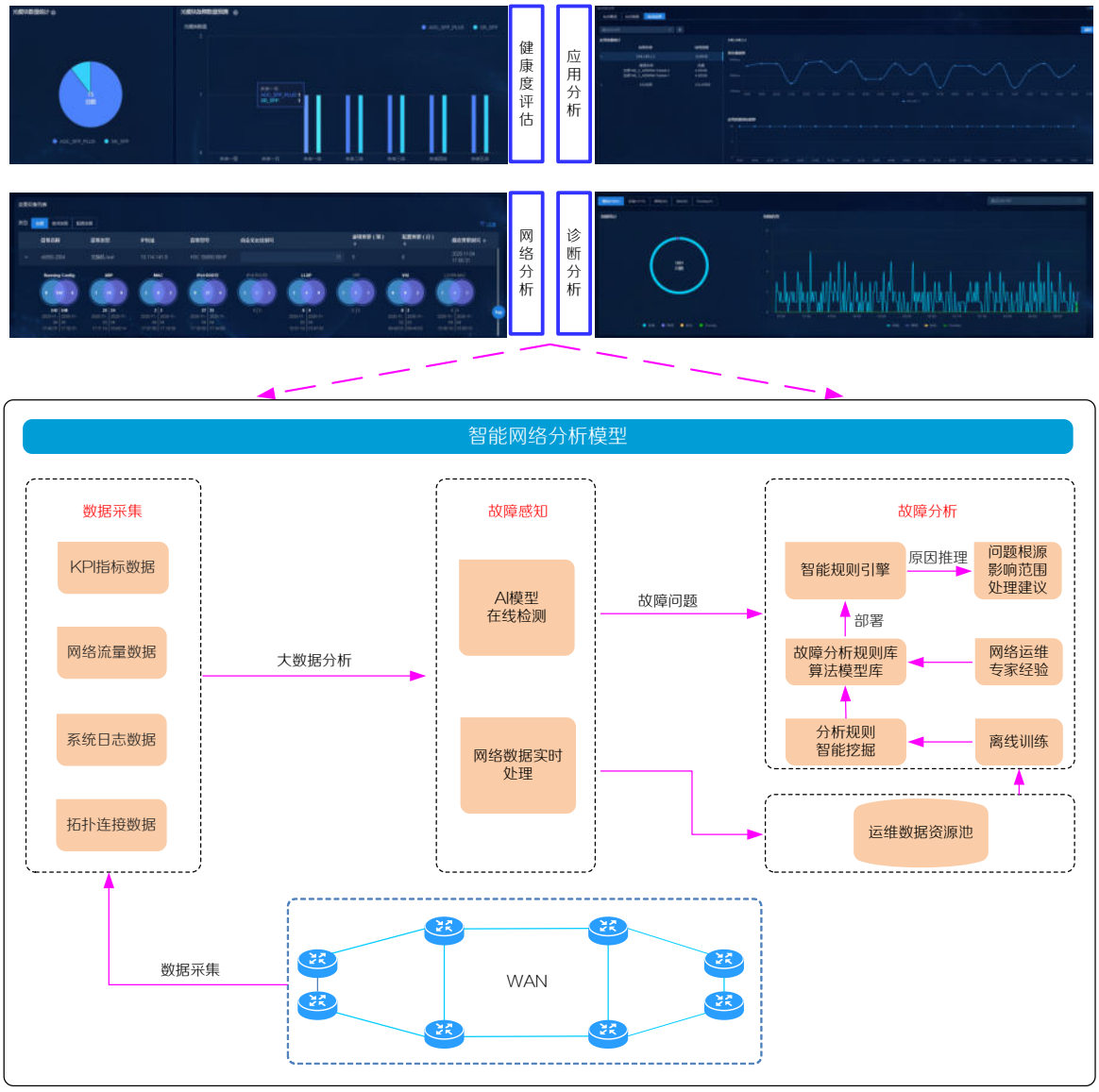
技术简介

智能网络分析

智能网络分析是指使用大数据和 AI 技术，实现对网络的实时监控和自动优化。主要步骤如下：

- 数据采集：采集网络和流量数据，支持秒级和分钟级的粒度。
- 故障感知：基于 AI 模型检测关键性能指标（KPI）的异常，实现分钟级的故障感知。
- 故障分析：利用 AI 算法和模型分析故障原因，实现分钟级的故障定位。
- 故障处置：根据分析结果，自动执行预设的故障处理方案，如 iFIT 随流检测技术实现秒级故障定位，并通知相关人员。

图59 智能网络分析



智能网络分析的主要维度包括：

- 健康度评估：全网健康可视化，主动运维。
- 网络分析：链路带宽和质量预测，网络变更分析，辅助故障定位。
- 应用分析：Netstream 流分析、SRv6 隧道流分析、iFIT 随流分析等，精准问题界定。
- 诊断分析：针对网络、设备、协议、Overlay 等常见故障，分钟级问题发现与定位，并提供处理建议。

可视化运维

如图 60 所示，可视化运维通过结合相关信息采集技术、流采集技术以及网络质量采集技术，实现基于全局的多维度可视呈现能力，以提供全网多维可视化服务，降低运维难度，减少运维成本。

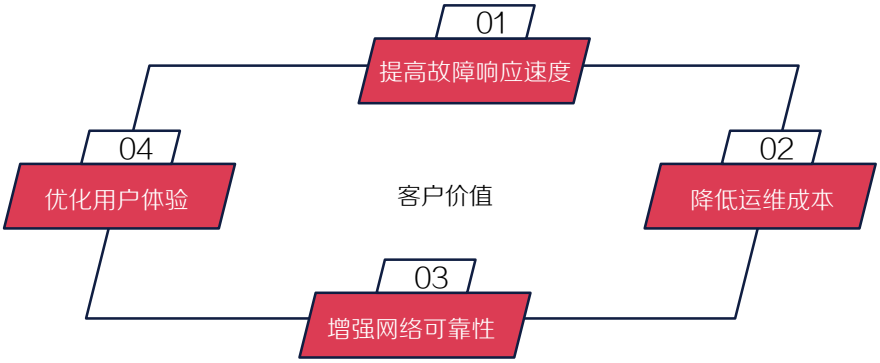
图60 可视化运维

客户价值

智能网络分析和可视化运维技术为客户带来了显著的价值：

- **提高故障响应速度**：通过 AI 模型的快速故障感知和定位，大幅缩短了从问题发现到解决的时间，提升了业务连续性。
- **降低运维成本**：自动化的故障分析和处置减少了对专业技术人员的依赖，降低了人力成本。
- **增强网络可靠性**：通过全面的健康度评估和连续的性能监控，提前发现并解决潜在的网络问题，增强了网络的整体可靠性。
- **优化用户体验**：多维度的网络可视化提供了清晰的网络运行状态，帮助管理员及时优化网络配置，改善最终用户的网络体验，提升用户满意度。

图61 客户价值



全景运维地图：全局视图实现网络可视化与预测

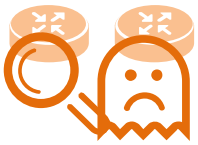
技术背景

随着越来越多业务上线和网络规模不断扩大，网络复杂性呈现指数级增长，传统网络运维已无法满足业务需求，运维管理面临诸多挑战：

- 多菜单入口、数据孤岛
  手动切换菜单监视网络状态不仅效率低下，还耗费大量时间和精力，排查故障和处理问题的过程高度依赖于管理员的专业经验和技能，增加了人为错误的风险，在遇到复杂问题时，往往难以及时、有效地解决。
- 策略固化，调优缺少有效反馈
  依赖人工分析制定策略存在偏差。在网络中实施后成效无法得到及时反馈，网络状况发生变化时，调整策略的响应速度滞后。人工分析和调优网络策略在复杂网络管理中显得过于繁琐和低效。
- 网络变化黑盒，被动响应
  无法清晰呈现网络流量的变化过程，网络管理更多地依赖于被动响应，问题发生后才采取行动进行解决，不仅延误了问题处理的时机，还可能导致更严重的网络中断和性能下降。由于缺乏预警机制和主动管理，运维团队往往只能在网络故障已经对业务造成影响时才得知问题存在。

冗余
多菜单入口、数据孤岛

低效
策略固化，调优缺少有效反馈



滞后
网络变化黑盒，被动响应

技术简介

如图 62 所示，“全景运维地图”通过类比现实世界的交通地图，整合网络相关的数据并呈现为统一的运维地图，以满足广域网运维的需求。

图62 全景运维地图

该技术通过采集网络流量、设备状态、链路质量等多维数据，并将其智能化处理后展示在一张数字化地图上，提供实时的网络运行情况视图。具体来说，全景运维地图利用数据采集、数据处理和可视化技术，将分散的网络信息整合并通过图形界面呈现，从而实现对全网数据的统一管理与监控。此外，该地图还具备秒级故障定位能力，支持快速故障排查，通过直观的可视化方式展示故障源及其影响范围。

客户价值

全景运维地图技术为客户带来显著的价值，通过精确的实时监控、智能资源优化和快速问题溯源，全面提升网络运维效率和可靠性。

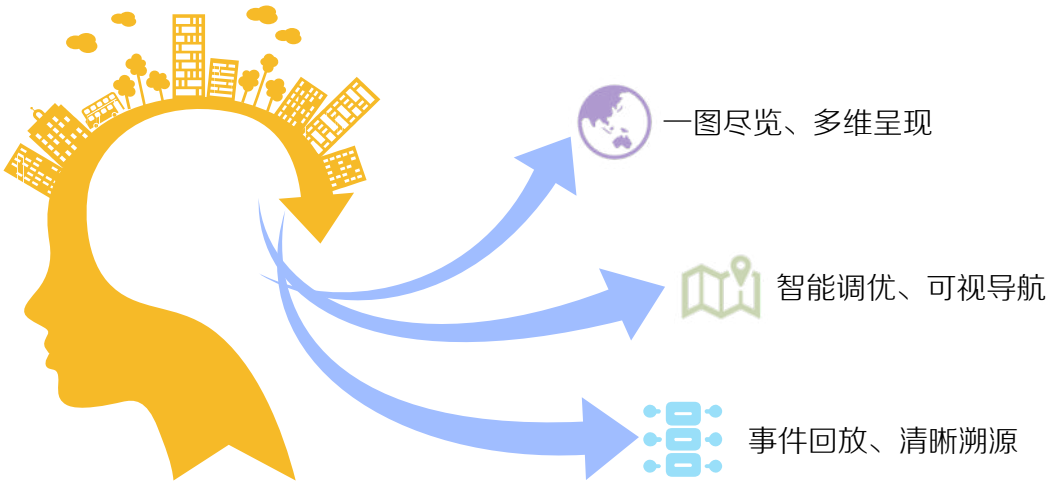
- **一图尽览、多维呈现**

  基于 GIS 地图的实时和直观展示功能，运维人员可以全面掌握全网状态，涵盖带宽、时延、抖动、丢包等多维度信息。这不仅简化了网络监控工作，还提升了监控的效率和准确性。
- **智能调优、可视导航**

  通过基于业务的可视化路径导航，系统能定期自动优化网络路径，从全局视角进行 SR/SRv6 TE Policy 的智能调度，使网络资源的利用更为高效，保障业务的顺畅运行。
- **事件回放、清晰溯源**

  隧道路径的全程展示使得运维人员能够全面了解事件发生的详细过程，快速定位问题根源，并为策略优化提供可靠依据。这不仅缩短了故障排除时间，还提高了网络的整体稳定性。

图63 客户价值



总而言之，H3C 的全景运维地图功能为网络管理带来了革命性的改变，通过全网数据可视和故障秒级定位两大关键能力，达到了统一可视化运维的目标。这不仅使网络管理更加高效、直观，也提供了一种解决复杂网络环境中运维挑战的有效方法。

AIGC 智能运维：AIGC 对话式运维提升运维响应与决策

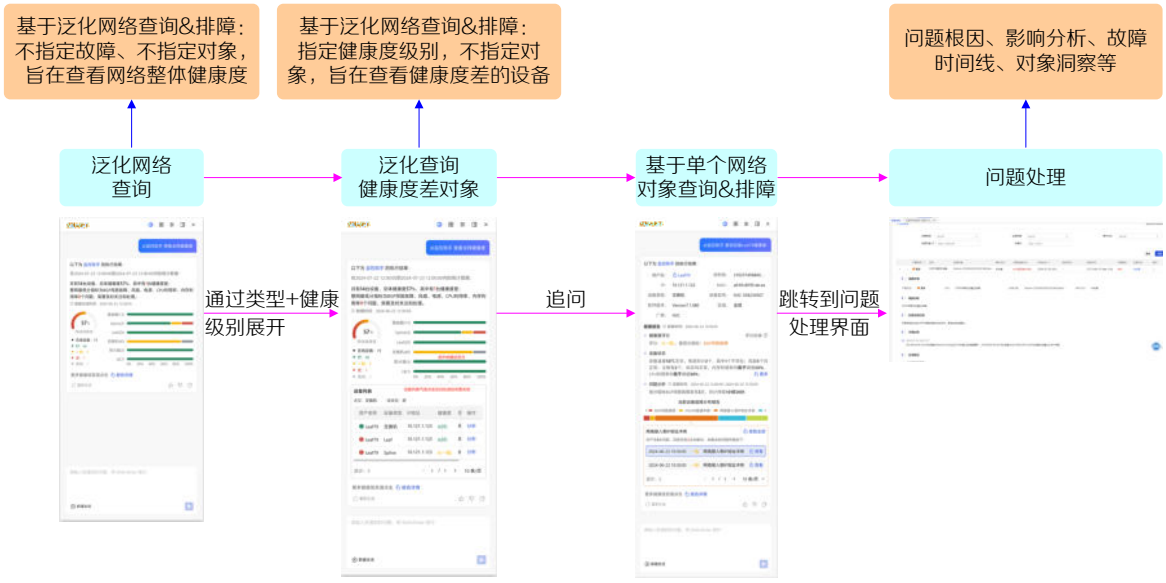
技术背景

在传统网络运维过程中，运维人员往往需要面对错综复杂的网络环境和海量的数据，这种情况极大地制约了运维效率。同时，现有的运维工具通常对用户的专业知识要求较高，新手很难快速掌握。因此，行业亟需一种更智能、更易用的运维解决方案来提高运维效率，减轻运维负担，帮助各类用户更快速地解决问题。

技术简介

AIGC 智能运维功能通过对话式交互，革新了运维体验。用户可以通过自然语言对话快速获取相关领域的知识，系统基于 AI 大模型进行意图识别，精准理解用户需求，给予相应的操作指引。这不仅大大降低了运维的门槛，还显著提升了故障定位和业务调优的效率。技术上通过 AI Agent 等技术手段对产品接口进行代理，充分利用了大模型的自然语言处理能力，从而实现对用户意图的精确理解和响应。

图64 AIGC 智能运维交互流程示意图



AIGC 智能运维功能涵盖了多个核心操作场景，通过对话式交互提供精确且高效的运维支持，包括以下几个主要功能：

- 专家知识问答

  通过对话式交互，用户可以快速获取相关领域知识，辅助高效运维。系统精准识别用户意图，给出对应操作菜单，方便用户进行后续操作。
- 分支链路查询

  用户提问后，系统启动查询分析，采集时延、抖动、丢包率、链路状态等信息，并通过 AI 助手展示，帮助用户快速获取链路数据。
- 分支链路故障分析

  IT 部门根据用户反馈，向 AI 大模型询问链路故障原因。系统分析现网环境，采集链路信息并提供处理建议，协助快速解决问题。
- 承载 VPN 排障

  用户提问后，系统启动分析，调用 AI Agent 采集专线质量信息，进行 SLA 分析并提供原因结果，帮助 IT 运维人员有针对性地进行故障恢复。
- 承载 SRv6 调优

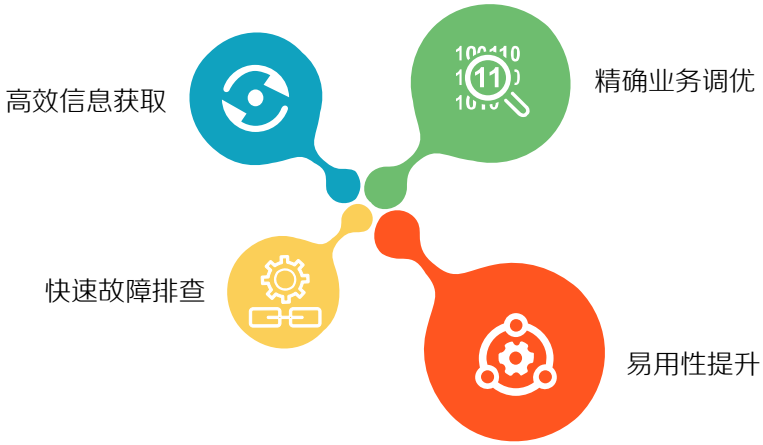
  用户提问后，系统启动思考分析，采集业务质量信息并进行 SLA 分析，列出不符合 SLA 的业务并提供调优入口，方便管理员快速进行业务调优。

客户价值

AIGC 智能运维功能通过其高效的信息交互和智能化的操作方式，为客户带来了多方面的显著价值。

- **高效信息获取**：通过自然对话形式，智能运维功能可以理解客户意图，快速呈现链路相关信息，使运维人员能够迅速掌握网络状态和问题所在。
- **快速故障排查**：系统能够迅速理解客户的故障描述，通过精准指导帮助用户快速定位问题，缩短故障排查时间。
- **精确业务调优**：智能运维功能进一步理解客户需求，帮助用户定位到需要调优的业务模块，并提供详细的调优原因说明，使业务性能优化变得更加科学有效。
- **易用性提升**：通过统一的助手界面入口，无论是初学者还是资深运维人员都可以在一个简洁的界面上完成复杂的运维操作，显著提升了运维工作的易用性和效率。

图65 客户价值



综上所述，AIGC 智能运维功能通过创新的对话式交互，彻底改变了传统高门槛、高难度的网络运维模式。利用 AI 大模型和 AI Agent 技术，该功能不仅提升了运维效率和准确性，还极大地降低了学习和操作成本。因此，AIGC 智能运维功能在提高运维效率、降低运维复杂度、快速解决故障和优化业务表现方面，具有显著的市场价值和应用前景。

7 方案优势

SRv6 SD-WAN 方案在敏捷部署、智能运维、网络承载、安全保障、性能提升、成本优化及未来技术支持等方面展现出显著优势。通过这些自动化和智能化的技术，方案不仅提升了网络性能和安全性，也极大地简化了部署和运维流程，满足了金融行业多样化的业务需求和复杂的网络环境需求，为金融行业的快速发展提供了坚实的技术支撑和安全保障。

图66 方案优势概览

7.1 敏捷部署与智能运维

敏捷的网络建设和智能化的运维机制，显著提高了网络部署和管理的效率：

- **零配置开局**：通过 ZTP（Zero Touch Provisioning）技术，实现设备自动注册和配置，大幅简化分支节点的部署流程，减少现场人工配置操作。
- **快速业务上线**：支持快速业务上线，保障网络的动态扩展和灵活调整，应对不断变化的业务需求。
- **远程维护与集中管理**：通过远程维护和集中控制，实现便捷高效的日常运维操作，减轻运维人员的负担。
- **自动化配置与故障处理**：通过 AI 和大数据技术，实现自动化配置和智能故障诊断，减少人为干预，提升运维效率。
- **实时故障检测与处理**：基于实时数据分析和监控，秒级故障检测和快速定位，实现自动化修复，减少故障影响时间。

7.2 统一承载与灵活调度

SRv6 SD-WAN 方案在网络承载和调度方面提供了高度灵活性和效率：

- **端到端统一承载**：利用 IPv6+技术，实现端到端统一承载，简化网络架构，提升网络效率和扩展能力。
- **动态路径控制**：结合强弱路径控制和智能调度算法，根据实时网络状况动态调整路径和资源分配，确保最佳网络性能和可靠性。
- **业务感知与优化**：通过 APN6 和 iFIT 技术，实现业务感知和路径选择，保障关键业务流的优先级和服务质量。

7.3 网络质量与安全保障

SRv6 SD-WAN 方案提供全面的质量监控和优化措施，并强化了安全保障：

- **实时业务质量监控**：通过 iFIT 技术，实现业务流的实时监控和分析，及时发现和处理潜在的网络问题。
- **服务级别协议（SLA）保障**：提供精细化的 SLA 管理和监控机制，确保关键业务的高可靠性和稳定性。
- **端到端加密与安全防护**：通过 IPsec 和 iSec 技术，实现数据传输的端到端加密，结合多层次的安全防护机制，确保网络和数据安全。

7.4 性能提升与可扩展性

SRv6 SD-WAN 方案不仅提升了现有网络的性能，还具备高度的可扩展性：

- **高效数据处理**：简化数据路径和提高数据处理能力，显著提升传输效率，支持金融业务的高速增长。
- **动态网络扩展**：支持动态的网络扩展，能够根据业务需求快速调整网络资源，保障服务的持续性和可靠性。

7.5 客户体验与成本优化

通过可靠的网络设计和运维效率的提升，SRv6 SD-WAN 方案显著提升了客户体验并优化了成本：

- **服务连续性**：通过高可靠性的网络设计，确保金融服务的持续可用，提升客户满意度。
- **业务质量监控**：利用先进的监测工具，持续监控服务质量，快速响应业务需求变化。
- **智能运维与成本效益**：集成 AI 技术，实现网络故障的快速诊断和自动修复，提高运维效率；自动化配置和管理，减少人力成本，通过优化的网络设计降低整体运营成本。

7.6 未来演进与业务创新

面对未来的发展需求，SRv6 SD-WAN 方案在技术兼容性和创新驱动方面具备突出的优势：

- **兼容未来发展**：SRv6 SD-WAN 技术具备向未来技术过渡的能力，如支持接入云服务和边缘计算等新兴技术。
- **创新驱动**：技术方案的灵活性和高效性为金融服务的创新提供基础，如支持新兴的金融科技应用和服务。

案例研究：SRv6 SD-WAN 助力某银行分支网络创新应用

在金融行业中，采用 SRv6 SD-WAN 创新技术解决方案有效提升了网络效率、安全性以及运维管理的灵活性。本节将通过一个具体案例——某银行分支网络的 SRv6 SD-WAN 应用，深入探讨该方案如何增强其分支网络的性能，并展示技术创新（如 SRv6 Policy 和 iFIT 随流检测）在提升网络效率和安全性方面的应用。
通过这一案例，将展示 SRv6 SD-WAN 在金融网络环境中如何提供更高效、安全和智能化的解决方案，以及它对某银行分支网络架构和业务运营的积极影响。

背景概述

在国家政策的引导下，例如国家两办发布的《推进互联网协议第六版（IPv6）规模部署行动计划》和中国人民银行发布的《金融科技发展规划（2022-2025 年）》，金融机构正迎来网络技术升级的关键时刻。这不仅带来了相当的挑战，也提供了前所未有的机遇。对此，某大型银行作为行业的先行者，积极响应政策号召，率先在全国范围内推广 IPv6+技术，旨在实现网络的现代化升级。该银行采取了包括增强网络安全措施、提升数据处理能力等在内的全面策略，目标是构建一个“一体化、全面覆盖、跨越式发展”的新一代网络基础设施，以支持未来金融服务的发展需求。通过这种技术革新，银行希望增强网络的可靠性、安全性和可管理性，从而更好地支持金融科技创新和业务扩展。

客户痛点

银行在广域骨干网络中已经成功部署了 SRv6 技术，构建了支持灵活路径控制的 IPv6 单栈骨干网，实现了网络简化和部分自治化，极大提升了网络运营效率和业务响应速度。然而，分支网络仍未全面进行 SRv6 改造，依然依赖复杂的传统路由手段进行业务数据分流，无法支持智能调度来保障关键业务的传输质量。这种技术滞后，不仅限制了关键业务活动的及时性和可靠性，还可能影响最终客户体验，从而在扩展新业务和提高服务效率方面带来了多项挑战。

- **智能调度能力不足**：目前分支网络仍在使用传统的 IPv4 架构，通过复杂的传统路由手段实现生产和办公数据的分流。由于无法根据链路健康状态智能调度流量，关键业务的传输质量得不到保障，且无法自动适应不断变化的业务需求，快速调整数据路由。这限制了关键业务活动的及时性和可靠性，可能影响最终客户体验。
- **网络扩展能力受限**：当前业界通常采用控制器与 SRv6 Policy 相结合的集中式调度方案，该方案在面对大规模分支网络时遇到了适应性挑战。这种方案的集中管理特性，使得在扩展新的分支站点时变得复杂且成本上升。随着业务快速增长，这种传统的网络架构逐渐显现出其扩展性的局限。
- **运维管理复杂度高**：在传统网络架构中，由于缺少实时的网络状态监控和业务分析工具，难以实时掌握分支网络的业务状态和运维信息，当网络出现问题时，分支网络的故障响应和维护都很困难，这直接影响了客户的服务质量。

图67 客户痛点

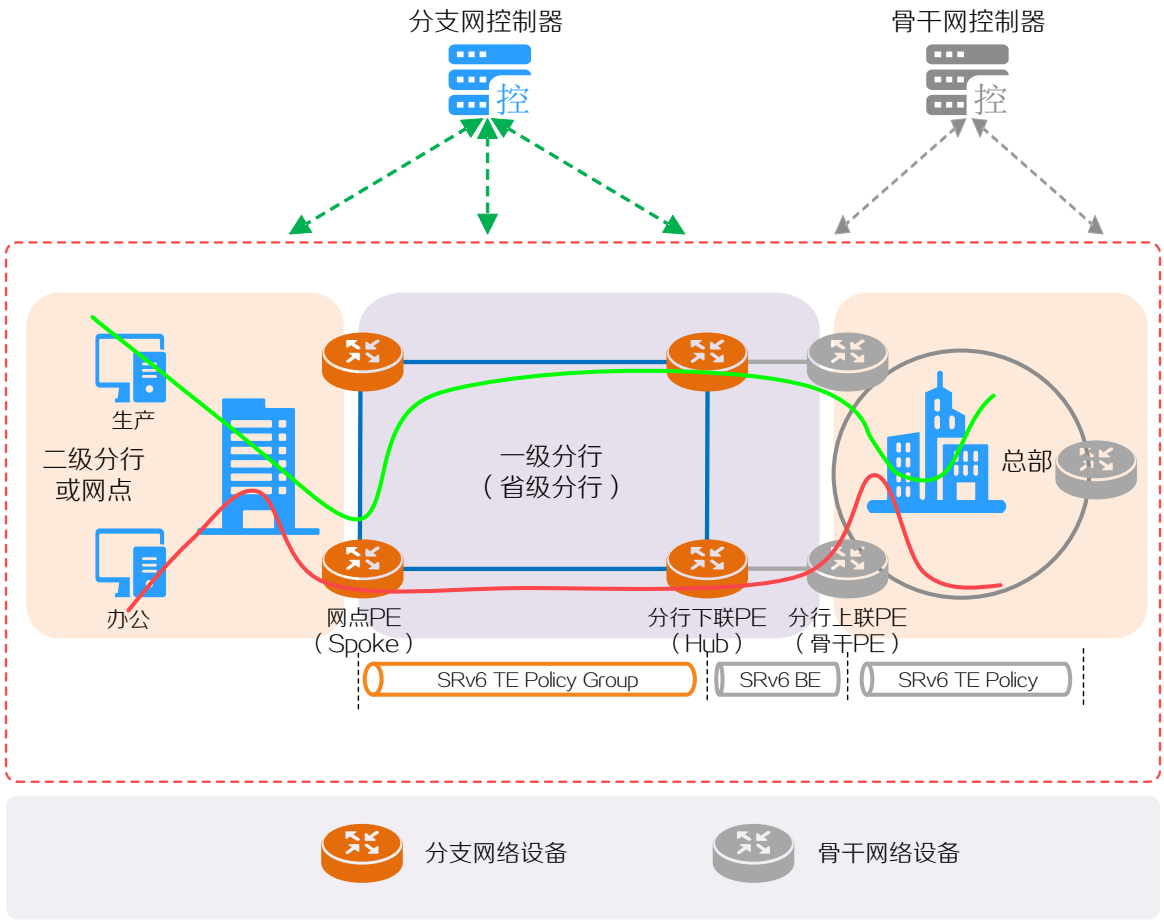
针对这些挑战，银行迫切需要对分支网络进行升级改造，引入新技术来提高网络的可靠性、安全性和易管理性，从而更好地适应业务增长和支持金融科技创新。通过网络升级，银行希望能够更好地适应业务增长，满足对高效运营和安全性的要求，从而更好地支持金融科技创新和业务扩展。

案例简介

为了解决上述客户痛点，本案例通过一系列的网络架构重构和技术升级，实现了省级分行的网络升级改造。如图 68 所示，主要网络改造思路包括以下几个方面：

- **标准组网**：分支 SRv6 SD-WAN 采用 Hub/Spoke 两级标准组网，支持集中管理、智能调度、业务可视、安全隔离等功能。具体实现方式是在骨干网边缘部署两台骨干 PE（作为分行上联 PE），与分行的一对 Hub 节点（即分行下联 PE）之间建立口字型连接，在骨干 PE 与 Hub 节点之间部署 SRv6 BE 实现跨域。这些 Hub 节点管理数百个 Spoke 节点，每对 Hub 代表一个省级分行，每个 Spoke 节点则代表该分行下的二级分行或网点。
- **分段管理与高效运维**：通过在分支网络和骨干网络各自部署独立控制器实现分段管理与高效运维。分支接入网由分支控制器管理，骨干 SRv6 网络由承载控制器管理，确保了网络的灵活性和可扩展性。头节点根据 iFIT 检查结果智能选择 SRv6 Policy 隧道转发报文。
- **技术替换**：采用标准的 EVPN+SRv6 协议替换了之前基于 IPv4 的 SDN-WAN 协议，显著提高了网络的互操作性和未来兼容性。这种技术替换不仅改善了网络性能，确保了新技术在现有架构中的顺利应用，还为未来技术升级奠定了坚实的基础。
- **智能路径管理**：在骨干 PE 和 Hub 节点上进行路由重生成，形成分层的 SRv6 路由，实现分支网络与骨干网的结构解耦。同时，结合 iFIT 和分布式智能调度 IPR 技术对 Hub 和 Spoke 间的隧道进行调度，优化数据流的动态管理，提高网络的灵活性和性能，实现高效且自适应的路径选择。
- **业务可视化**：为了实现全面的业务可视化，部署了基于 iFIT 系统与 IPv6+技术的可视化运维解决方案。通过数据采集、故障感知与分析、健康度评估、网络和应用分析、诊断分析等功能，实现了网络的实时监控和故障自动化处理。业务可视化的实现为网络运维提供了全面支持，有助于更快速地响应和解决潜在问题。

图68 某银行的 SRv6 SD-WAN 应用组网示意图



客户价值

通过应用 SRv6 SD-WAN，银行成功地实现了网络的端到端构建、智能调度和运维，显著提升了网络的运营效率、安全性和灵活性。如图 69 所示，具体价值体现在以下几个方面：

- **智能调度与设备快速响应**：利用 SDN 控制器下发的 SRv6 Policy，银行能够快速开通临时测试业务，实现设备快速响应和智能选路策略的隧道调度。同时，结合 IPR 智能选路策略和基于隧道的 iFIT 功能，一旦检测到隧道质量劣化，设备能够依据 IPR 调度策略和 iFIT 监测信息迅速做出决策，进行隧道切换，确保业务不间断和网络高效运行，提升网络的可靠性和业务连续性。
- **全面可视化运维**：通过 iFIT 与 IPv6+技术，银行实现了拓扑、链路、业务和质量的全景可视化监控。同时，基于实时监控和分析关键指标，智能分析工具实现了主动运维、故障根因定位、运行状态预测和智能策略推荐，从而大幅提升了运维效率和服务质量，确保网络的稳定运行和客户满意度。
- **增强的网络安全性**：IPv6+技术引入的安全特性为金融交易和数据传输提供了安全保护，有效降低了网络攻击和数据泄露的风险，增强了客户对银行系统安全性的信任度。同时，提供了更为严格的访问控制和更高强度的加密措施，进一步保障了客户数据的隐私和安全。
- **技术标准化进程**：通过骨干网和接入网异构互通的实践，推动 IPv6+技术的标准化进程，构建开放的网络技术生态。这种标准化带来了更大的互操作性和兼容性，有助于未来网络技术的推广和应用。特别是通过 SRv6 技术的改造，分支网络与骨干 SRv6 网络构建了统一的 IPv6+网络，实现了总部与分支之间的无缝连接。

图69 客户价值

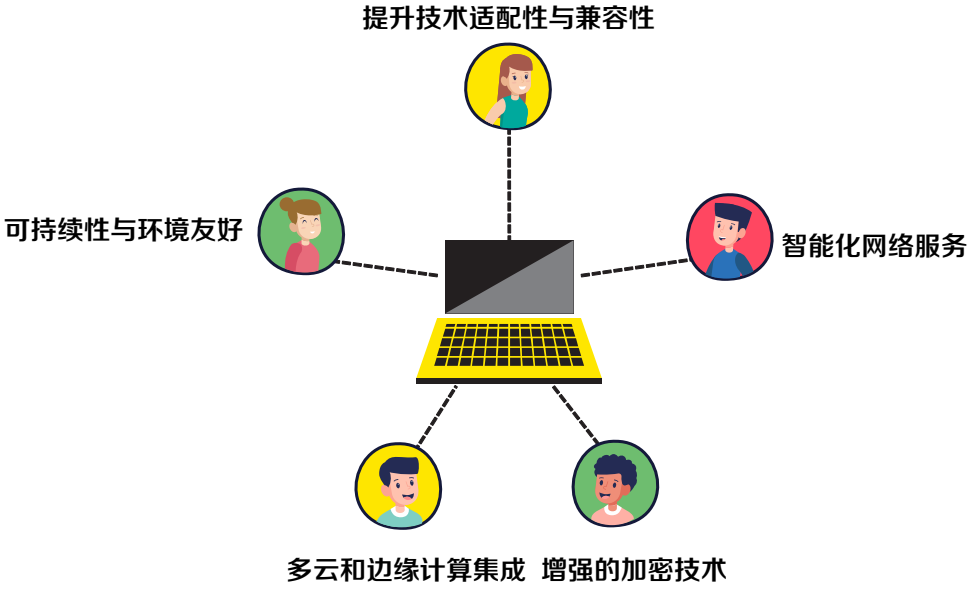
通过以上这些改进，不仅提高了银行网络的技术标准，也为银行的业务运营和客户服务带来了实质性的提升，进一步支持了银行在数字化转型道路上的前行。

未来趋势与展望

SRv6 SD-WAN 的成功应用为金融行业网络的现代化奠定了坚实基础。展望未来，SRv6 SD-WAN 将聚焦以下创新方向，推动金融行业的持续创新和业务扩展：

- **提升技术适配性与兼容性**：增强新技术与现有网络基础设施的兼容性，确保技术过渡过程中的业务连续性。同时，加强行业合作，推动 SRv6 SD-WAN 技术和实现方案的标准化，提高不同设备和服务之间的兼容性和互操作性。
- **智能化网络服务**：利用人工智能和机器学习技术，SRv6 SD-WAN 解决方案可以进一步提升网络的自动化管理和优化性能。智能化服务可以提高网络的响应速度和效率，减少人工干预，提升整体服务质量。
- **增强的加密技术**：为了应对新的安全挑战，未来的 SRv6 SD-WAN 解决方案将集成更先进的端到端加密技术。这将保护数据传输不受侵害，确保金融交易和客户数据的安全。
- **多云和边缘计算集成**：随着金融服务越来越多地采用云计算和边缘计算，SRv6 SD-WAN 解决方案将发展出更优的多云管理能力和边缘计算支持，提高数据处理速度和降低延迟。
- **可持续性与环境友好**：面对全球环境和能源挑战，未来的 SRv6 SD-WAN 解决方案将更加注重能效和减少碳排放，支持绿色运营和可持续发展。不仅有助于降低运营成本，还提升了资源利用效率，符合全球可持续发展的趋势。

图70 创新和发展方向



通过这些技术前景的展望，可以看出 SRv6 SD-WAN 解决方案在金融行业中的应用将继续展现其强大的潜力。该技术不仅能够帮助金融机构克服当前的挑战，还将开辟创新的发展道路，为金融行业的未来增添更多可能性。通过应对困难和技术挑战，抓住技术创新和发展方向的机遇，金融机构将能够提升网络性能、安全性和灵活性，实现业务模式创新和客户体验提升，从而在激烈的市场竞争中保持领先地位，确保业务的长期稳健发展。

缩略语

缩略语	英文全称	中文全称
4G	4th Generation	第四代移动通信技术
5G	5th Generation	第五代移动通信技术
AES	Advanced Encryption Standard	高级加密标准
AH	Authentication Header	认证头
AI	Artificial Intelligence	人工智能
APN6	Application-aware IPv6 Networking	应用感知型IPv6网络

缩略语	英文全称	中文全称
BE	Best Effort	尽力而为
BGP	Border Gateway Protocol	边界网关协议
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DPI	Deep Packet Inspection	深度包检测
EBGP	External Border Gateway Protocol	外部边界网关协议
ECMP	Equal Cost Multi Path routing	等价多路径路由
ESP	Encapsulating Security Payload	封装安全负载
EVPN	Ethernet Virtual Private Network	以太网虚拟专用网络
FEC	Forward Error Correction	前向纠错
FIB	Forwarding Information Base	转发信息库
FlexE	Flexible Ethernet	灵活以太网
FW	Firewall	防火墙
GRE	Generic Routing Encapsulation	通用路由封装
HBH	Hop-by-Hop Extension Header	IPv6逐跳扩展头
HMAC	Hash-based Message Authentication Code	基于哈希的消息认证码
IETF	Internet Engineering Task Force	互联网工程任务组
iFIT	in-situ Flow Information Telemetry	原位流信息遥测
IGP	Interior Gateway Protocol	内部网关协议
IKE	Internet Key Exchange	互联网密钥交换
IP	Internet Protocol	互联网协议
IPPCP	IP Payload Compression Protocol	IP负载压缩协议
IPR	Intelligent Policy Route	智能策略路由
IPS	Intrusion Prevention System	入侵防御系统
IPsec	Internet Protocol Security	互联网协议安全
IPv6	Internet Protocol Version 6	互联网协议第6版
IPv6+	IPv6 Enhanced	IPv6增强技术
LZ	Lempel-Ziv compression	LZ压缩
LTE	Long Term Evolution	长期演进

缩略语	英文全称	中文全称
MPLS	Multiprotocol Label Switching	多协议标签交换
MV	Multiprotocol Label Switching VPN	多协议标签交换虚拟专用网络
PE	Provider Edge	提供商边缘
QoS	Quality of Service	服务质量
QUIC	Quick UDP Internet Connections	快速UDP互联网连接协议
RFC	Request for Comments	技术建议书请求评议
RIB	Routing Information Base	路由信息库
RS	Reed-Solomon	里德-所罗门算法
RTP	Real-time Transport Protocol	实时传输协议
RTT	Round-Trip Time	往返时间
SDN	Software-Defined Networking	软件定义网络
SD-WAN	Software Defined Wide Area Network	软件定义广域网
Slice ID	Slice Identifier	切片标识符
SLA	Service Level Agreement	服务级别协议
SRH	Segment Routing Header	段路由扩展头
SRv6	Segment Routing over IPv6	IPv6段路由
SSL	Secure Sockets Layer	安全套接字层
TE	Traffic Engineering	流量工程
TLS	Transport Layer Security	传输层安全协议
VPDN	Virtual Private Dial-up Network	虚拟专用拨号网络
VPN	Virtual Private Network	虚拟专用网络
WAAS	Wide Area Application Services	广域网应用服务
WAN	Wide Area Network	广域网
ZSTD	Zstandard	Z标准压缩算法
ZTP	Zero Touch Provisioning	零配置

专业引领： 智联未来金融服务

安全保障： 构建稳定可靠网络

高效创新： 推动金融科技发展