



IPv6+



IP网络系列丛书

IFIT

主编：陈婧怡 王雅莉

数据通信数字化信息和内容体验部 出品



版权声明

主编：陈婧怡 王雅莉
主要参与人员：骆兰军 魏跃云
发布日期：2021-05-10
发布版本：01

版权所有© 华为技术有限公司 2021。保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

前言

主编简介

陈婧怡，华为数据通信产品资料工程师，2019 年加入华为，一直从事检测特性的资料开发工作，致力于推动相关技术的传播。

王雅莉，华为数据通信研究与标准工程师，2018 年加入华为，曾参与撰写 IFIT 控制平面协议扩展的多篇 IETF 标准草案，主导撰写《电信运营商网络带内流信息自动化质量测量技术要求》CCSA 行标和《Reactive In-situ Flow Information Telemetry》ETSI 报告。

本书内容

本书重点介绍 IFIT 的产生背景，揭示 IFIT 备受瞩目的原因，阐述 IFIT 独特的技术价值，展示 IFIT 多样的应用场景和广阔的发展空间。本书还在第 4 章简要介绍 IFIT 的实现原理，理解这些内容，会帮助大家更深刻地理解 IFIT 的技术优势。



读者对象

本书主要适用于网络工程师等 ICT 从业人员，也适合想了解前沿 IP 网络技术的读者阅读。阅读本书需要有一定的 IP 网络技术基础，例如了解 IP 网络架构、网络运维以及传统检测技术等。



目录

第1章 IFIT 简介	1
第2章 IFIT 的产生背景	2
2.1 网络业务与架构演进	2
2.2 传统网络运维的痛点	3
2.3 优质运维手段的缺失	4
2.4 IFIT 随流检测的诞生	5
第3章 IFIT 的技术价值	9
3.1 高精度多维度检测真实业务质量	9
3.2 灵活适配大规模多类型业务场景	10
3.3 提供可视化的运维界面	11
3.4 构建闭环的智能运维系统	13
第4章 IFIT 的基础原理	15
4.1 IFIT 如何精准定位故障	15
4.2 IFIT 如何自动触发检测	19



4.3 IFIT 如何实时上送数据	21
第 5 章 IFIT 的成功应用	22
5.1 IPRAN 移动承载网	22
5.2 智能云网专线业务	24
5.3 金融广域一张网	25
第 6 章 IFIT 推动 IPv6+时代的智能运维发展	27



第1章

IFIT 简介

IFIT (In-situ Flow Information Telemetry, 随流检测) 是一种通过对网络真实业务流进行特征标记, 以直接检测网络的时延、丢包、抖动等性能指标的检测技术。随着移动承载、专网专线以及云网架构的快速发展, 承载网面临着超大带宽、海量连接及高可靠低时延等新需求与新挑战。IFIT 通过在真实业务报文中插入 IFIT 报文头进行性能检测, 并采用 Telemetry 技术实时上送检测数据, 最终通过 iMaster NCE-IP 可视化界面直观地向用户呈现逐包或逐流的性能指标。IFIT 可以显著提高网络运维及性能监控的及时性和有效性, 保障 SLA (Service Level Agreement, 服务水平协议) 可承诺, 为实现智能运维奠定坚实基础。



第2章

IFIT 的产生背景

摘要

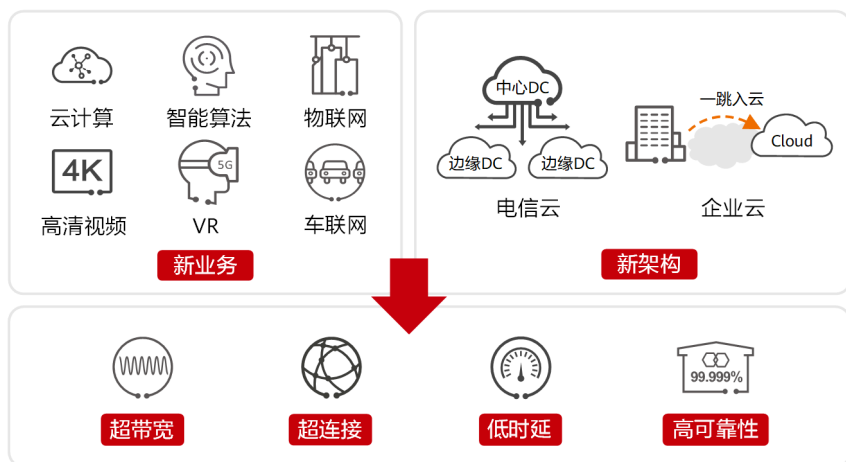
IFIT是华为公司为了应对5G和云时代网络业务不断提高的SLA要求和网络运维面临的挑战提出的IETF（Internet Engineering Task Force，因特网工程任务组）标准化检测协议，是业界首个完整体系的随流质量感知与故障定界方案。IFIT从提出到现在短短几年已受到国内外的广泛关注，它在2019年斩获Interop东京国际网络电信展览会“Best of Show Award”特别奖，相关学术文稿也被网络通信顶级会议SIGCOMM收录。本章将从网络业务与架构演进、传统网络运维的痛点以及优质运维手段的缺失三个方面切入，揭秘IFIT随流检测的诞生过程。

2.1 网络业务与架构演进

面向 5G 和云时代，IP 网络的业务与架构都产生了巨大变化，这些变化给网络运维带来了巨大挑战。一方面，5G 的发展带来了如高清视频、VR（Virtual Reality，虚拟现实）、车联网等丰富新业务的兴起；另一方面，为方便统一管理、降低维护成本，网络设备和服务的云化已经成为必然趋势。如图 2-1 所示，新业务与新架构对目前的承载网提出了诸多挑战：

- 超带宽：为承载庞大体量的业务数据交互，要求带宽持续增加，带宽利用率最大化以及带宽增长可预测。
- 超连接：为支撑海量智能终端接入网络，需要实现按需动态连接和业务自动部署，同时针对不同的业务连接实现差异化的 SLA 保障。
- 低时延：为优化用户及时流畅的网络体验，需要实现网络时延从 20ms 到 2ms 的显著降低，并且保证时延的确定性。例如，远程医疗要求时延不超过 10ms，车联网要求时延不超过 5ms，工业控制网络则要求时延不超过 2ms。
- 高可靠性：为提升网络的可靠性，需要提供故障主动感知及快速定界定位的运维手段，并进一步开发网络的自我修复能力。

图2-1 新业务与新架构提出的新挑战



2.2 传统网络运维的痛点

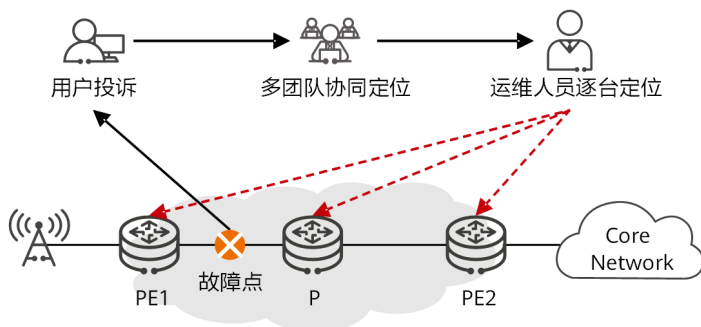
传统的网络运维方法并不能满足 5G 和云时代新应用的 SLA 要求，突出问题是业务受损被动感知和定界定位效率低下，如图 2-2 所示：

- 业务受损被动感知：运维人员通常只能根据收到的用户投诉或周边业务部门派发的工单判断故障范围，在这种情况下，运维人员故障感知延后、故障处理被动，

导致其面临的排障压力大，最终可能造成不好的用户体验。因此，当前网络需要能够主动感知业务故障的业务级 SLA 检测手段。

- 定界定位效率低下：故障定界定位经常需要多团队协同，团队间缺乏明确的定界机制会导致定责不清；人工逐台设备排障找到故障设备进行重启或倒换的方法，排障效率低下；此外，传统 OAM（Operation, Administration and Maintenance，操作、管理和维护）技术通过测试报文间接模拟业务流，无法真实复现性能劣化和故障场景。因此，当前网络需要基于真实业务流的高精度快速检测手段。

图2-2 传统网络运维的痛点



2.3 优质运维手段的缺失

面对传统网络运维的痛点，业界一直在进行探索改进，先后提出了几种不同的 OAM 技术，这些技术按照测量类型不同，可分为带外测量和带内测量两种模式。带外测量技术通过间接模拟业务数据报文并周期性发送报文的方法，实现端到端路径的性能测量与统计；带内测量技术则是通过对真实业务报文进行特征标记或在真实业务报文中嵌入检测信息，实现对真实业务流的性能测量与统计。

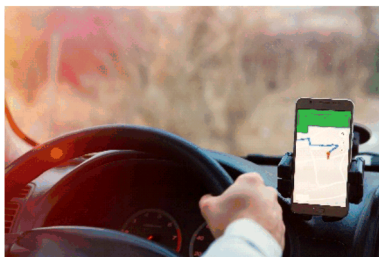
为了帮助大家理解这两种测量模式的区别，我们举一个例子。如图 2-3 所示，如果把网络中的业务流看作车道上行驶的车辆，那么带外测量技术就好比在道路两旁定点设置的监控探头，收集的数据有限且存在盲区，不足以还原车辆完整的运行轨迹；带内测量技术则好比车辆安装了定位模块，车辆的行驶信息都将被收集，可以实现对车辆的实时定位以及准确的路径还原。

图2-3 带外测量与带内测量的对比

带外测量模式



带内测量模式



现有的带外测量技术代表是 TWAMP (Two-Way Active Measurement Protocol, 双向主动测量协议), 带内测量技术包括早期的 IP FPM (IP Flow Performance Measurement, IP 流性能监控) 和近些年提出的 IOAM (In-situ Operation, Administration and Maintenance, 随流操作、管理和维护), 这些测量方法各有优点, 但对于新的网络业务与架构要求, 仍旧不能很好地满足, 具体表现在:

- TWAMP 作为早期主流的带外测量技术, 由于其部署简单, 受到广泛应用, 但是其通过在业务报文中插入测量探针并间隔发包的方法导致统计精度较低, 无法定位具体故障点及呈现真实业务路径。
- IP FPM 的出现带来了带内测量的新思想, 它通过直接对 IP 报文头进行染色显著提高了检测精度, 但是由于其无法感知业务流的转发路径导致部署难度较高, 不适合在现网中进行大规模应用。
- IOAM 无需路径发现即可部署, 它的出现解决了配置复杂的问题, 但是其采用 Passport 数据处理模式, 即每个节点都将采集数据记录在报文中并在尾节点集中上报, 会对设备的转发平面效率造成影响。

2.4 IFIT 随流检测的诞生

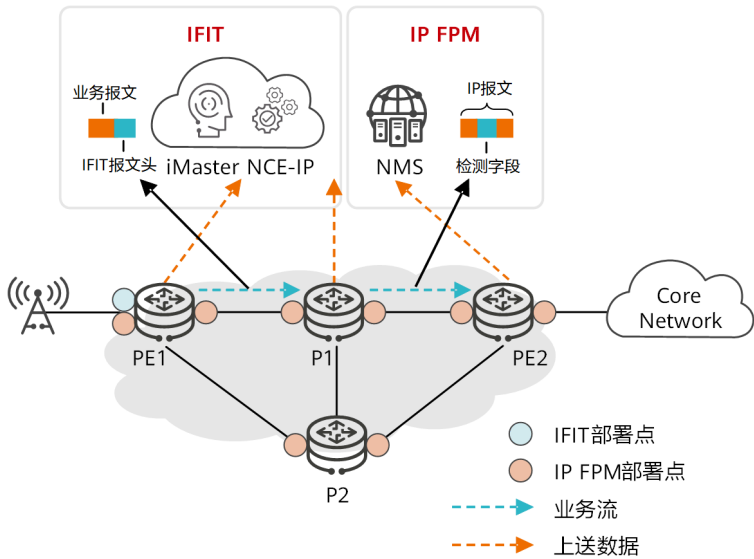
2018 年, 在世界移动大会 (MWC 2018) 上, 华为正式发布意图驱动的智能网络解决方案, 通过在物理网络和商业意图之间构建一个数字孪生世界, 驱动网络从 SDN (Software-Defined Networking, 软件定义网络) 向智能网络演进, 使能

商业价值最大化。为了满足智简网络不仅能够准确识别用户意图、实现网络的端到端自动化配置，还能够实时感知用户体验并进行预测性分析和主动优化的需求，IFIT 随流检测技术应运而生。IFIT 也是一种带内测量技术，它能够弥补 IP FPM 和 IOAM 的不足。

IFIT 与 IP FPM 的对比如图 2-4 所示，二者的主要差异表现在：

- 在业务部署方面，IFIT 支持控制器事先获取全网拓扑结构，通过将上报节点的设备标识、接口标识等信息映射到网络拓扑上实现路径的自动发现。IFIT 只需在头节点配置，降低了 IP FPM 逐点配置带来的部署难度，将部署效率提升 80%。
- 在扩展性方面，IFIT 通过为业务流增加 IFIT 报文头实现随流检测的方法，相较于 IP FPM 基于 IP 报文现有字段的实现，提高了可扩展性，可以满足未来网络的长期演进。

图2-4 IFIT 与 IP FPM 的对比



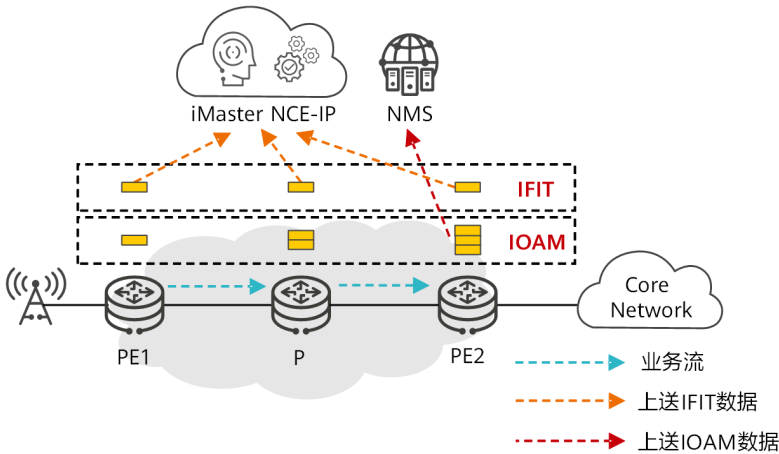
IFIT 与 IOAM 的对比如图 2-5 所示，二者的主要差异表现在：

- 在转发效率方面，IFIT 采用 Postcard 数据处理模式，相较于 IOAM 采用的 Passport 模式，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。在这种情况下，IFIT 报文头长度短且固定，降低了对设备转发平面效率的影响。

- 在检测范围方面，IFIT 通过上报每一跳信息支持逐跳的丢包检测，可以对具体的丢包位置进行解析。

图2-5 IFIT 与 IOAM 的对比



如表 2-1 所示，进一步总结了上述不同类型 OAM 技术的对比，从中可以看出，IFIT 在多个方面均展现出优势。

表2-1 不同 OAM 技术的对比

对比项	IP FPM	IOAM	IFIT
部署难度	高	低	低
逐跳检测	支持	不支持逐跳丢包检测	支持
转发平面效率	中等	低	高
数据采集压力	小	大	仅使用染色功能：小 使用扩展功能：大



对比项	IP FPM	IOAM	IFIT
可扩展性	基于 IP 报文头现有字段，扩展能力差	扩展能力强	扩展能力强

结合大数据分析和智能算法，IFIT 可以进一步构建智能运维系统，使网络具有预测性分析和自愈能力，通过提前识别网络故障主动进行故障修复和体验优化，为网络的自动化和智能化提供保障。

目前，IETF、ETSI、CCSA 等国内外标准组织正在加紧制定 IFIT 的各项标准，以便更好地促进 IFIT 的规模商用。IFIT 的主要标准介绍如下：

- IFIT 框架和染色原理在 IETF 草案 In-situ Flow Information Telemetry Framework (draft-song-opsawg-ifit-framework)、IETF 标准 Alternate-Marking Method for Passive and Hybrid Performance Monitoring (RFC8321) 和 Multipoint Alternate-Marking Method for Passive and Hybrid Performance Monitoring (RFC8889) 这三篇文稿中制定。
- IFIT 转发平面的 IPv6 和 MPLS 封装机制分别在 IETF 草案 IPv6 Application of the Alternate Marking Method (draft-fz-6man-ipv6-alt-mark) 和 Encapsulation For MPLS Performance Measurement with Alternate Marking Method (draft-cheng-mpls-inband-pm-encapsulation) 这两篇文稿中制定。
- IFIT 控制平面的能力通告机制和借助 SR Policy 实现的 IFIT 自动化部署机制分别在 IETF 草案 IGP Extensions for In-situ Flow Information Telemetry (IFIT) Capability Advertisement (draft-wang-lsr-igp-extensions-ifit) 和 BGP SR Policy Extensions to Enable IFIT (draft-qin-idr-sr-policy-ifit) 这两篇文稿中制定。
- 分布式 Telemetry 机制以及基于 UDP 的数据上送机制分别在 IETF 草案 Subscription to Distributed Notifications (draft-unyte-netconf-distributed-notif) 和 UDP-based Transport for Configured Subscriptions (draft-unyte-netconf-udp-notif) 这两篇文稿中制定。

第3章

IFIT 的技术价值

摘要

IFIT通过在真实业务报文中插入IFIT报文头的方法进行检测，这种方法可以反映业务流的实际转发路径，配合Telemetry高速数据采集能力实现高精度、多维度的真实业务质量检测。IFIT基于设备透传、转发路径自动学习等能力，可以实现对大规模多类型业务场景的灵活适配。IFIT支持通过iMaster NCE-IP定制多种监控策略，可视化呈现检测结果，可以给用户带来良好的运维体验。此外，IFIT结合大数据分析和智能算法能力，能够进一步构建闭环的智能运维系统。

3.1 高精度多维度检测真实业务质量

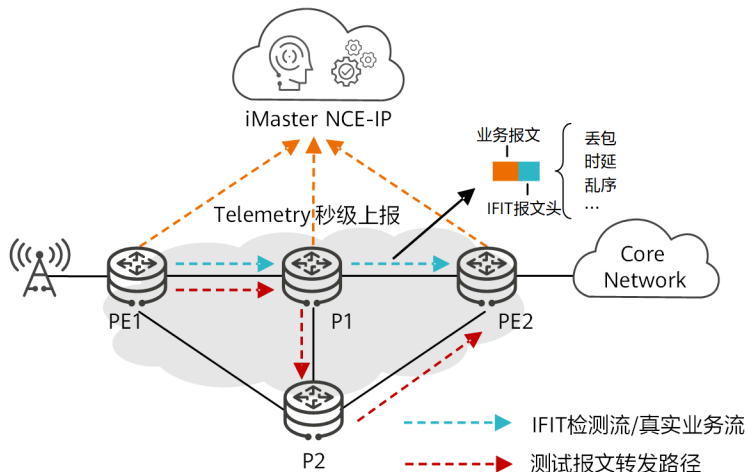
传统 OAM 技术的测试报文转发路径可能与真实业务流转发路径存在差异，IFIT 提供的随流检测能力基于真实业务报文展开，如图 3-1 所示，这种检测方式存在很大优势，具体描述如下：

- IFIT 可以真实还原报文的实际转发路径，精准检测每个业务的时延、丢包、乱序等多维度的性能信息，丢包检测精度可达 10^{-6} 量级，时延检测精度可达微秒级。
- IFIT 配合 Telemetry 秒级数据采集功能，能够实时监控网络 SLA，快速实现故障定界和定位。



- IFIT 可以实现对静默故障的完全检测、秒级定位。静默故障是指业务体验受损但没有达到触发告警门限且缺乏有效定位的故障，现网中 15% 的静默故障常常需要耗费超过 80% 的运维时间，危害较大。IFIT 能够识别网络中的细微异常，即使丢 1 个包也能检测到，这种高精度丢包检测率可以满足金融决算、远程医疗、工业控制和电力差动保护等“零丢包”业务的要求，保障业务的高可靠性。

图3-1 IFIT 基于真实业务流检测



3.2 灵活适配大规模多类型业务场景

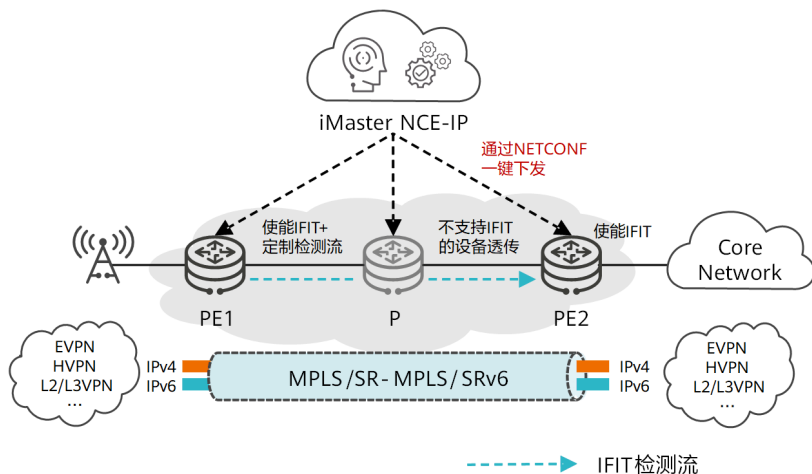
网络的发展并非是一蹴而就的，随着网络需求的不断增长，一张网络中可能同时存在多种网络设备并且承载多样的网络业务。在这种情况下，IFIT 凭借其部署简单的特点可以灵活适配大规模、多类型的业务场景，如图 3-2 所示，具体表现在：

- IFIT 支持用户一键下发、全网使能。只需在头节点按需定制端到端和逐跳检测，中间节点和尾节点一次使能 IFIT 即可完成部署，可以较好地适应设备数量较大的网络。
- IFIT 检测流可以由用户配置生成（静态检测流），也可以通过自动学习或由带有 IFIT 报文头的流量触发生成（动态检测流）；可以是基于五元组等信息唯一创建

的明细流，也可以是隧道级聚合流或 VPN 级聚合流。在这种情况下，IFIT 能够同时满足检测特定业务流以及端到端专线流量的不同检测粒度场景。

- IFIT 对现有网络的兼容性较好，不支持 IFIT 的设备可以透传 IFIT 检测流，这样能够避免与第三方设备的对接问题，可以较好地适应设备类型较多的网络。
- IFIT 无需提前感知转发路径，能够自动学习实际转发路径，避免了需要提前设定转发路径以及对沿途所有网元逐跳部署检测所带来的规划部署负担。
- IFIT 适配丰富的网络类型，适用于二、三层网络，也适用于多种隧道类型，可以较好地满足现网需求。

图3-2 IFIT 适配多种应用场景



3.3 提供可视化的运维界面

在可视化运维手段产生之前，网络运维需要通过运维人员先逐台手工配置，再多部门配合逐条逐项排查来实现，运维效率低下。可视化运维可以提供集中管控能力，它支持业务的在线规划和一键部署，通过 SLA 可视支撑故障的快速定界定位。IFIT 可以提供可视化的运维能力，如图 3-3 所示，用户可以通过 iMaster NCE-IP 可视

化界面根据需要下发不同的 IFIT 监控策略，实现日常主动运维和报障快速处理，具体介绍如下：

- 日常主动运维：日常监控全网和各区域影响基站最多的 TOP5 故障、基站状态统计、网络故障趋势图以及异常基站趋势图等数据，通过查看性能报表及时了解全网、重点区域的 TOP 故障以及基站业务状态的变化趋势；在 VPN 场景下，通过查看端到端业务流的详细数据，帮助提前识别并定位故障，保证专线业务的整体 SLA。
- 报障快速处理：在收到用户报障时，可以通过搜索基站名称或 IP 地址查看业务拓扑和 IFIT 逐跳流指标，根据故障位置、疑似原因和修复建议处理故障；还可以按需查看 7*24 小时的拓扑路径和历史故障的定位信息。

图3-3 iMaster NCE-IP 可视化界面



从图 3-3 中可以看出，IFIT 的监控结果可以在 iMaster NCE-IP 上直观生动地图形化呈现，能够帮助用户掌握网络状态，快速感知和排除故障，为用户带来更好的运维体验。



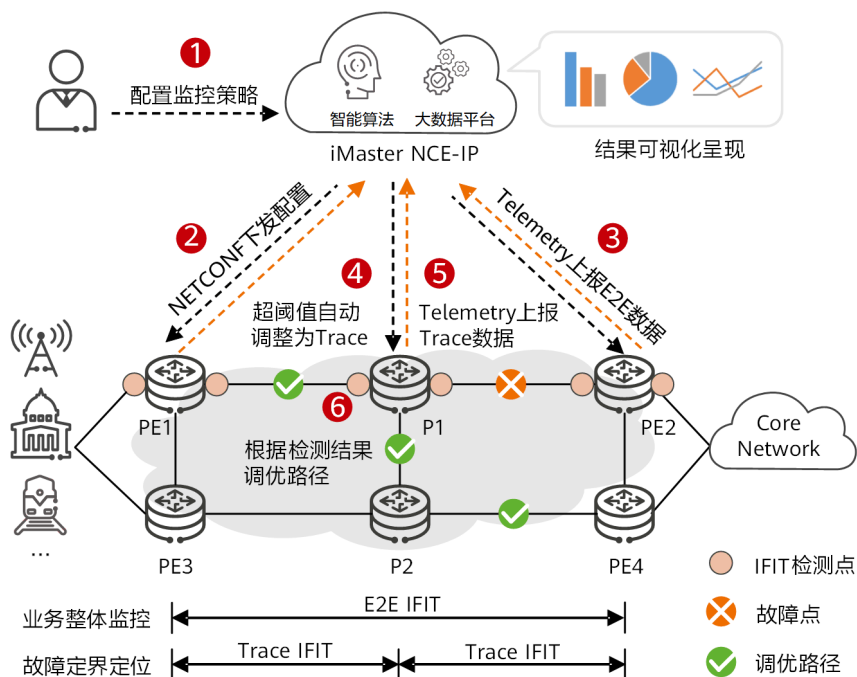
3.4 构建闭环的智能运维系统

为应对网络架构与业务演进给承载网带来的诸多挑战，满足传统网络运维手段提出的多方面改进要求，实现用户对网络的端到端高品质体验诉求，需要将被动运维转变为主动运维，打造智能运维系统。智能运维系统通过真实业务的异常主动感知、故障自动定界、故障快速定位和故障自愈恢复等环节，构建一个自动化的正向循环，适应复杂多变的网络环境。

如图 3-4 所示，IFIT 与 Telemetry、大数据分析和智能算法等技术相结合，共同构建智能运维系统，该系统的具体工作流程描述如下：

1. 通过 iMaster NCE-IP 全网使能 IFIT 能力并进行 Telemetry 订阅，根据需要选择业务源宿节点及链路并配置 IFIT 监控策略。
2. iMaster NCE-IP 将监控策略转换为设备命令，通过 NETCONF 下发给设备。
3. 设备生成 IFIT 端到端监控实例，源宿节点分别通过 Telemetry 秒级上报业务 SLA 数据给 iMaster NCE-IP，基于大数据平台处理可视化呈现检测结果。
4. 设置监控阈值，当丢包或时延数据超过阈值时，iMaster NCE-IP 自动将监控策略从端到端检测调整为逐跳检测并通过 NETCONF 下发更新后的策略给设备。
5. 设备根据新策略将业务监控模式调整为逐跳模式，并逐跳通过 Telemetry 秒级上报业务 SLA 数据给 iMaster NCE-IP，基于大数据平台处理可视化呈现检测结果。
6. 基于业务 SLA 数据进行智能分析，结合设备 KPI、日志等异常信息推理识别潜在根因，给出处理意见并上报工单；同时，通过调优业务路径保障业务质量，实现故障自愈。

图3-4 基于 IFIT 构建闭环的智能运维系统



从上述过程中可以看出，IFIT 端到端（E2E）和逐跳（Trace）检测的上送结果是大数据库平台和智能算法分析的数据来源，也是实现智能运维系统故障精准定位和故障快速自愈能力的基石。除了 IFIT 随流检测以及 Telemetry 高速采集外，大数据平台拥有秒级查询、高效处理海量 IFIT 检测数据的能力，并且单节点故障不会导致数据丢失，可以保障数据高效可靠地分析转化；智能算法支持将质差事件聚类为网络群障（即计算同一周期内质差业务流的路径相似度，将达到算法阈值的质差业务流视为由同一故障导致，从而定位公共故障点），识别准确率达 90% 以上，可以提升运维效率，有效减少业务受损时间。以上四大技术共同保障智能运维系统闭环，推进智能运维方案优化，可以很好地适应未来网络的演进。

第4章

IFIT 的基础原理

摘要

本章主要介绍IFIT的基础原理，描述基于交替染色法的IFIT检测指标、端到端和逐跳的统计模式、IFIT自动触发检测能力以及基于Telemetry的数据上送功能，从转发平面、控制平面和管理平面的不同维度来诠释IFIT的技术价值。

4.1 IFIT 如何精准定位故障

IFIT 通过在真实业务报文中插入 IFIT 报文头实现故障定界和定位，这里以 IFIT over SRv6 场景为例，展示 IFIT 报文头结构，再通过对染色标记位和统计模式位这两个关键字段功能的介绍，说明 IFIT 如何实现故障的精准定位。

IFIT 报文头结构

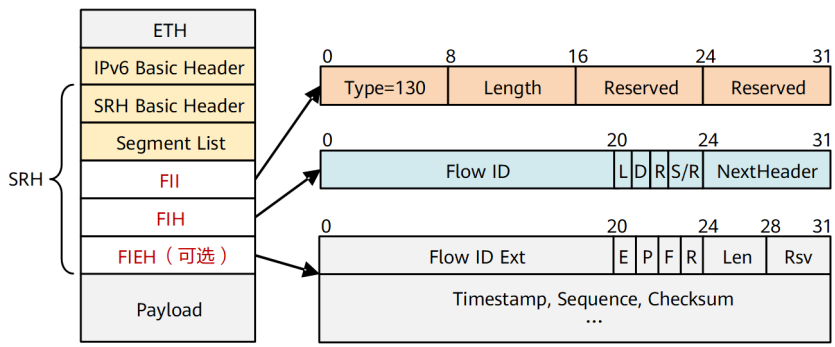
在 IFIT over SRv6 场景中，IFIT 报文头封装在 SRH（Segment Routing Header，段路由扩展头）中，如图 4-1 所示。在该场景中，IFIT 报文头只会被指定的 SRv6 Endpoint 节点（接收并处理 SRv6 报文的任何节点）解析。运维人员只需

在指定的、具备 IFIT 数据收集能力的节点上进行 IFIT 检测，从而有效地兼容传统网络。

IFIT 报文头主要包含以下内容：

- FII (Flow Instruction Indicator，流指令标识)：FII 标识 IFIT 报文头的开端并定义了 IFIT 报文头的整体长度。
- FIH (Flow Instruction Header，流指令头)：FIH 可以唯一地标识一条业务流，L 和 D 字段提供了对报文进行基于交替染色的丢包和时延统计能力。
- FIEH (Flow Instruction Extension Header，流指令扩展头)：FIEH 能够通过 E 字段定义端到端或逐跳的统计模式，通过 F 字段控制对业务流进行单向或双向检测。此外，还可以支持如逐包检测、乱序检测等扩展功能。

图4-1 IFIT 报文头结构



基于交替染色法的 IFIT 检测指标

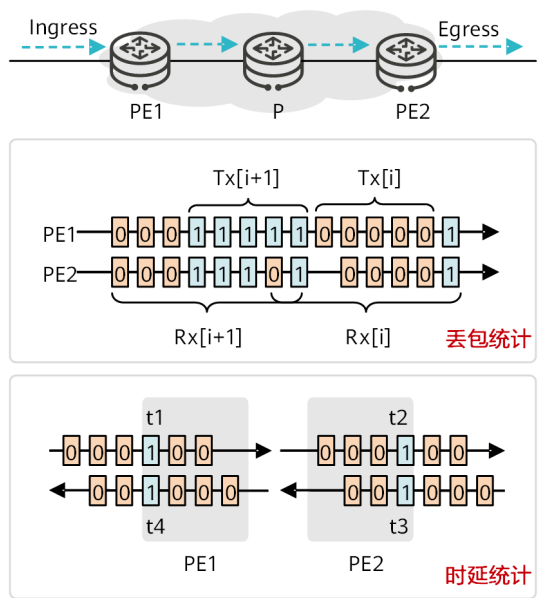
丢包率和时延是网络质量的两个重要指标。丢包率是指在转发过程中丢失的数据包数量占所发送数据包数量的比率，设备通过丢包统计功能可以统计某一个测量周期内进入网络与离开网络的报文差。时延则是指数据包从网络的一端传送到另一端所需要的时间，设备通过时延统计功能可以对业务报文进行抽样，记录业务报文在网络中的实际转发时间，从而计算得出指定的业务流在网络中的传输时延。

IFIT 的丢包统计和时延统计功能通过对业务报文的交替染色来实现。所谓染色，就是对报文进行特征标记，IFIT 通过将丢包染色位 L 和时延染色位 D 置 0 或置 1 来



实现对特征字段的标记。如图 4-2 所示，业务报文从 PE1 进入网络，从 PE2 离开网络，通过 IFIT 对该网络进行丢包统计和时延统计。

图4-2 基于交替染色法的 IFIT 检测指标



从 PE1 到 PE2 方向的 IFIT 丢包统计过程描述如下：

1. PE1 在 Ingress 端标记每个业务报文的 L 染色位为 0 或 1，每个周期翻转一次，统计周期内的 0 或 1 并计算报文数 $Tx[i]$ 。
2. PE2 在 Egress 端延长统计周期（避免报文乱序影响统计结果），每个周期独立统计周期内的 0 或 1 并计算报文数 $Rx[i]$ 。
3. 计算第 i 个周期内的丢包数 $= Tx[i] - Rx[i]$ ，第 i 个周期内的丢包率 $= (Tx[i] - Rx[i]) / Tx[i]$ 。

PE1 和 PE2 间的 IFIT 时延统计过程描述如下：

1. PE1 在 Ingress 端对某一业务报文的 D 染色位置 1，并获取时间戳 $t1$ 。
2. PE2 在 Egress 端接收到经历网络转发与时延的 D 染色位置 1 的业务报文，并获取时间戳 $t2$ 。



3. 计算 PE1 至 PE2 的单向时延= t_2-t_1 ，同理可得出 PE2 至 PE1 的单向时延= t_4-t_3 ，双向时延= $(t_2-t_1)+(t_4-t_3)$ 。

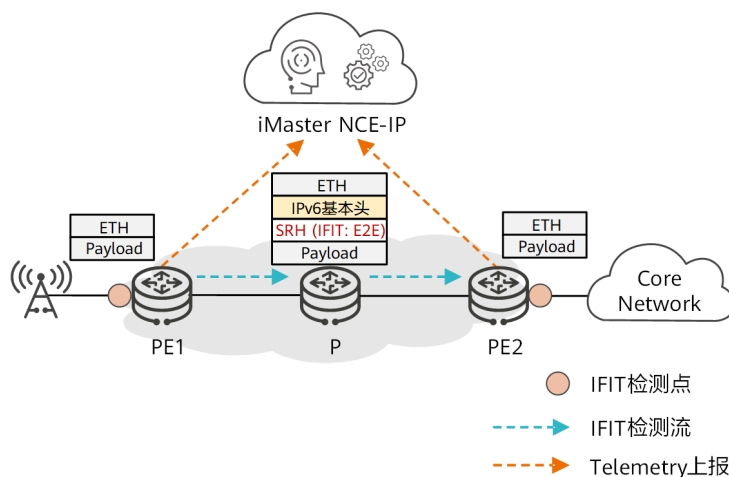
通过对真实业务报文的直接染色，辅以部署 1588v2 等时间同步协议，IFIT 可以主动感知网络细微变化，真实反映网络的丢包和时延情况。

端到端和逐跳的统计模式

现有检测方法中常见的数据统计模式一般分为端到端（E2E）和逐跳（Trace）两种，E2E 统计模式适用于需要对业务进行端到端整体质量监控的检测场景，Trace 统计模式则适用于需要对低质量业务进行逐跳界定或对 VIP 业务进行按需逐跳监控的检测场景。IFIT 同时支持 E2E 和 Trace 两种统计模式。

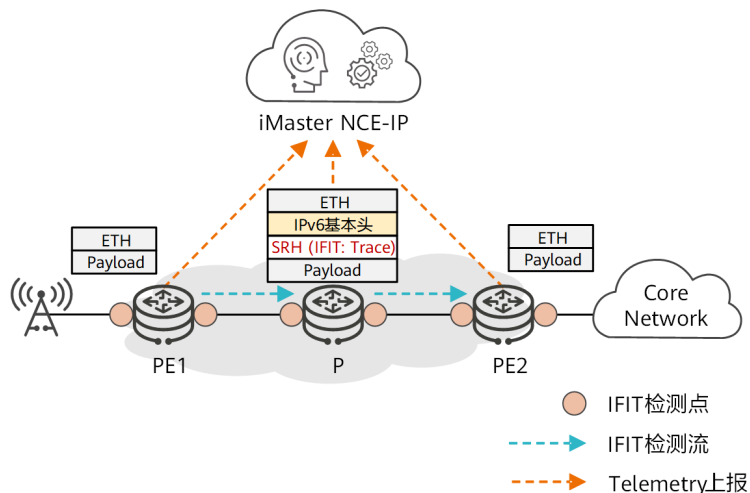
E2E 统计模式仅需在头节点部署 IFIT 检测点触发检测，在尾节点使能 IFIT 能力即可实现。在这种情况下，仅头尾节点感知 IFIT 报文并上报检测数据，中间节点则做 Bypass 处理，如图 4-3 所示。

图4-3 E2E 统计模式



Trace 统计模式需要在头节点部署 IFIT 检测点触发检测，同时在业务流途经的所有支持 IFIT 的中间节点上使能 IFIT 能力，如图 4-4 所示。

图4-4 Trace 统计模式



在实际应用中，一般是 E2E IFIT+Trace IFIT 组合使用，当 E2E IFIT 的检测数据达到阈值时会自动触发 Trace IFIT，在这种情况下，可以真实还原业务流转发路径，并对故障点进行快速定界和定位。

4.2 IFIT 如何自动触发检测

为了自动触发 IFIT 检测，控制器需要能感知网络中设备对 IFIT 的支持情况，可以通过扩展 IGP/BGP 通告网络设备支持 IFIT 的能力，并通过扩展 BGP-LS (BGP-Link State, BGP 链路状态) 协议将设备支持情况汇总通告给控制器，控制器可以根据上报的信息确定是否可以在指定网络域中使能 IFIT。

下面以 BGP 扩展为例进行介绍。如图 4-5 所示，是扩展 BGP 团体属性所定义的 IPv6-Address-Specific IFIT Tail Community，IFIT 尾节点可以使用该团体属性将其支持的 IFIT 能力通告给对端设备（即 IFIT 头节点）。

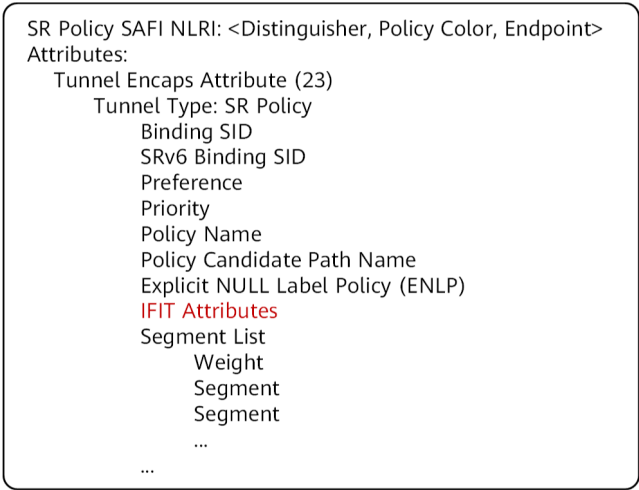
图4-5 IPv6-Address-Specific IFIT Tail Community 结构

0	8	16	31
Type	Sub-Type	Originating IPv6 Address	
Originating IPv6 Address (cont.)			
Originating IPv6 Address (cont.)			
Originating IPv6 Address (cont.)			
Originating IPv6 Address		IFIT Capabilities	

在图 4-5 中，Originating IPv6 Address 字段携带了 IFIT 尾节点的 IPv6 单播地址；IFIT Capabilities 字段则标识了该节点支持的 IFIT 能力，包括端到端和逐跳检测能力，以及基于交替染色法的检测能力等。

当需要快速检测已部署业务的 SLA 劣化情况以及及时进行业务调整时，可以通过在扩展 BGP/PCEP 协议分发 SR Policy 时增加携带 IFIT 信息来实现。在这种情况下，下发 SR Policy 的同时 IFIT 将自动激活并运行，如图 4-6 所示。

图4-6 携带 IFIT 信息的 SR Policy 结构



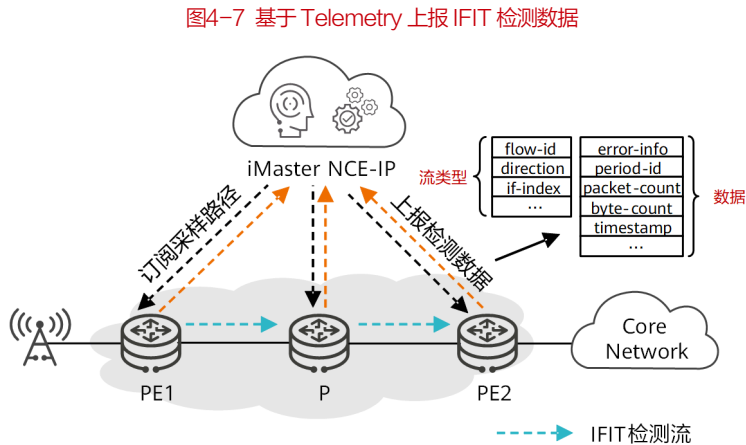
在 BGP 扩展下发 SR Policy 时，可以通过 IFIT Attributes 字段携带 IFIT 属性信息，这样 IFIT 可以以相同方式检测 SR Policy 的所有候选路径。其中，候选路径

包含多个 SR 路径，每个路由由一个段列表指定，IFIT 属性作为子 TLV 附加在候选路径层面。

4.3 IFIT 如何实时上送数据

在智能运维系统中，IFIT 通常采用 Telemetry 技术实时上送检测数据至 iMaster NCE-IP 进行分析。Telemetry 是一项远程的从物理设备或虚拟设备上高速采集数据的技术，设备通过推模式（Push Mode）周期性地主动向采集器上送设备的接口流量统计、CPU 或内存数据等信息，相对传统拉模式（Pull Mode）的一问一答式交互，提供了更实时更高速的数据采集功能。Telemetry 通过订阅不同的采样路径灵活采集数据，可以支撑 IFIT 管理更多设备以及获取更高精度的检测数据，为网络问题的快速定位、网络质量的优化调整提供重要的大数据基础。

如图 4-7 所示，用户在 iMaster NCE-IP 侧订阅设备的数据源，设备根据配置要求采集检测数据并封装在 Telemetry 报文中上报，其中包括流 ID、流方向、错误信息以及时间戳等信息。iMaster NCE-IP 接收并存储统计数据，再将分析结果可视化呈现。



在 Telemetry 秒级高速数据采集技术的配合下，IFIT 能够实时将检测数据上送至 iMaster NCE-IP，实现高效的性能检测。

第5章

IFIT 的成功应用

摘要

随着5G的不断深化，运营商用户面对的网络质量要求不断提高，对移动承载网的有效监控显得尤为重要；同时，随着云计算的不断发展，业务上云已成为企业用户首要考虑的服务部署方式，智能云网、广域一张网等方案不断涌现，在云网场景下的高效运维显得迫在眉睫。IFIT可以很好地满足上述场景，本章从IPRAN移动承载网、智能云网专线业务以及金融广域一张网三个具体场景展现IFIT的成功应用。

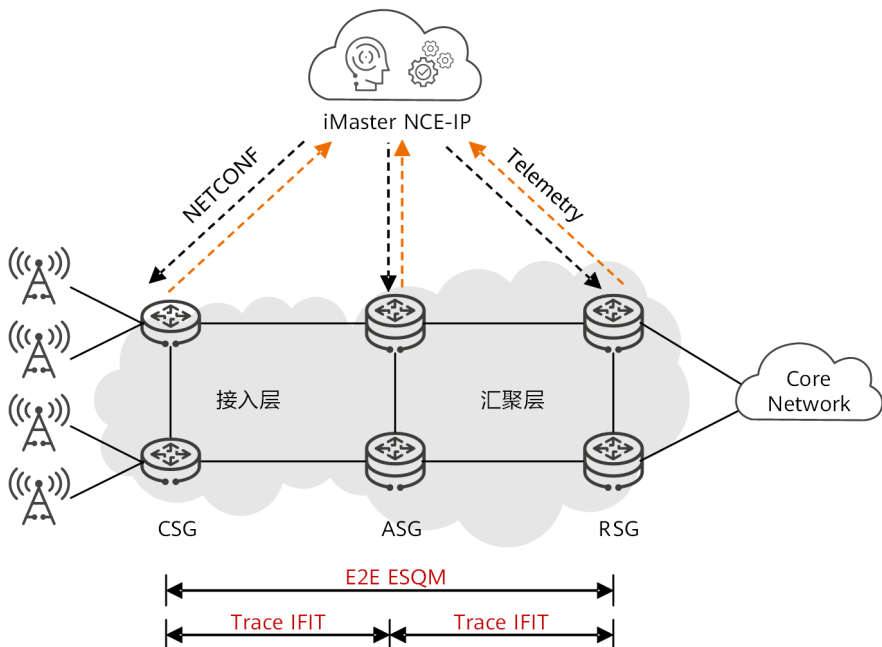
5.1 IPRAN 移动承载网

为了最大限度地保护运营商的投资成本、减少建网投资以及保障网络的平滑演进，诞生了在RAN（Radio Access Network，无线接入网络）中引入IP的IPRAN解决方案。IPRAN移动承载网具有接入方式丰富，网络规模庞大等特点，各种移动承载业务诸如高清视频等都对链路连通性与性能指标提出了更高的要求。

在这种情况下，华为提出了E2E ESQM（Enhanced Stream Quality Monitoring，增强型流质量监控）+ Trace IFIT的混合检测方案。如图5-1所示，IFIT通过对故障的快速定界定位和按需回放复现，提升SLA体验和运维效率。



图5-1 IFIT 在 IPRAN 移动承载网中的应用



ESQM 是一种基于五元组信息对 TCP、SCTP 或 GTP 报文信息进行统计的检测技术，在该场景中，先进行端到端的 ESQM 性能检测，当基站流性能指标超过设定阈值时触发逐跳的 IFIT 检测，iMaster NCE-IP 汇总上报的逐跳检测数据进行路径还原和故障定位。该方案具有如下特点：

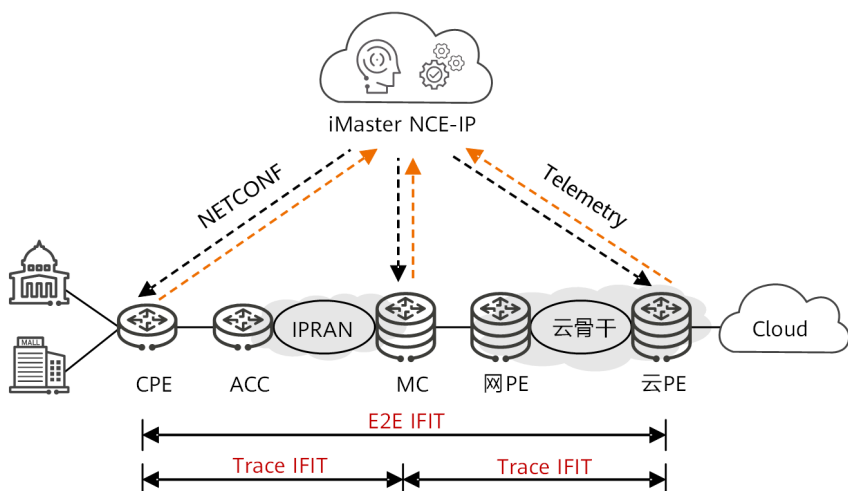
1. 一方面支持从基站流、数据流、信令流的不同维度监控业务流的详细指标数据；另一方面支持聚类处理基站流故障，对质差业务进行快速定界，防止大量基站流同时故障触发超过转发规格的 Trace IFIT 检测。
2. 当故障来自 IPRAN 网络外部时，IFIT 可以帮助网络快速准确地自证清白；当故障来自 IPRAN 网络内部时，IFIT 可以帮助网络快速定位到故障网元或链路，提升网络运维效率。
3. 基于全网基站的实时性能数据可以构建大数据智能运维系统，实现基站业务的高精度、业务级的 SLA 实时感知、多维可视，对网络可能发生的风险进行分析评估和调整优化，实现自动化、智能化运维。

5.2 智能云网专线业务

智能云网技术以智能 IP 网络为基础，实现自动化、智能化的云网运营和云网运维，支撑包括运营商 2B（To Business，面向企业客户）业务、政府、医疗等企业业务在内的千行百业的数字化转型。智能云网专线业务是智能云网技术的重要一环，它利用移动承载网广覆盖的优势更加便捷地提供企业专线业务，通过端到端的协同管理提高网络的部署、运营及运维效率。

IFIT 支持在智能云网专线业务中提供 VPN 业务分析保障，包括组网专线、上云专线以及云网互联三大场景。这里以上云专线为例，介绍 E2E IFIT + Trace IFIT 的检测方案。如图 5-2 所示，IFIT 可以保障端到端的高可靠性，通过可视化运维实现分钟级故障定位。

图5-2 IFIT 在智能云网专线业务中的应用



在该场景中，先进行端到端的 IFIT 性能检测，当 VPN 流的性能指标超过设定阈值时触发逐跳的 IFIT 性能检测，iMaster NCE-IP 汇总上报的逐跳检测数据进行路径还原和故障定位。该方案具有如下特点：

1. 可针对某一条 VPN 流进行流故障分析定位，支持按分钟到年多粒度查询 VPN 业务流端到端的性能指标，包括最大流速、最大单向时延、最大丢包率等。

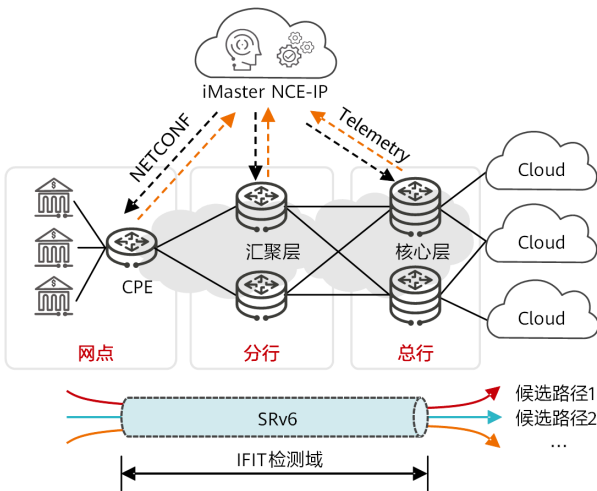
- 2. 支持按 VPN 名称、VPN 类型及业务状态查询 VPN 整体端到端的业务信息，并在存在多段业务流的情况下以质量最差段的状态值为准。
- 3. 实现端到端多维度异常识别、网络健康可视、智能故障诊断以及故障自愈闭环。

5.3 金融广域一张网

为了方便统一管理，产生了广域一张网的概念，它是一种通过对不同网络进行协同，提供跨域网络服务的技术。在金融行业中，二级行、网点、子公司、外联单位等机构首先接入一级行，通过一级行汇聚业务流量后进而和银行核心网打通，最终实现和总行数据中心的互访。广域一张网的集中管理理念在这里显得尤为重要。

一方面，金融广域一张网依靠 SRv6 技术简单快速地打通云和各种接入点之间的基础网络连接，确保业务高效开通；另一方面，金融行业本身就对 SLA 质量有很高的要求，而随着银行业务的发展，网点的业务类型呈现多样化特征，除了传统的生产办公业务外，还有安防、物联网、公有云等业务，这对金融广域一张网的运维能力提出了更高的要求。在这种情况下，华为提出了 IFIT 隧道级检测方案，如图 5-3 所示，IFIT 可以简化运维流程，优化运维体验。

图5-3 IFIT 在金融广域一张网中的应用



该方案具有如下特点：

1. 支持在 SRv6 场景中使能 IFIT 隧道级检测，能够检测 SRv6 各个 Segment List 的质量并选出最优链路，通过周期性地对比当前链路和最优链路进行选路调优，实现智能选路。
2. 全网一个核心控制器，可以对整个金融网络进行集中式运维，实现端到端的管理和调度。



第6章

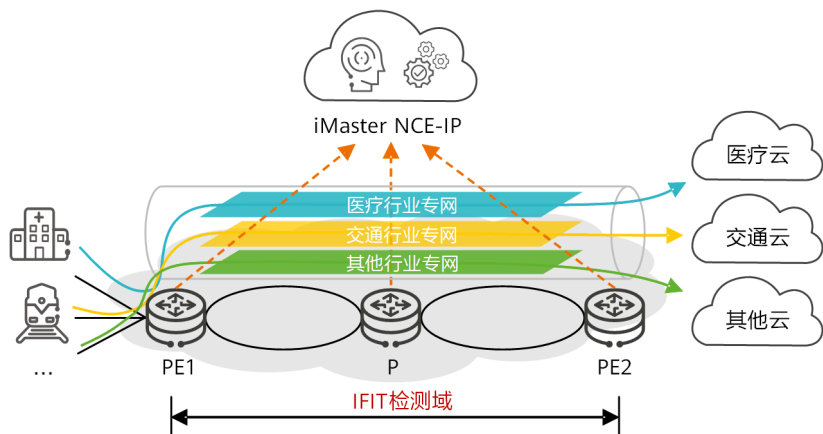
IFIT 推动 IPv6+时代的智能运维发展

5G 和云时代都在驱动 IP 网络朝着 IPv6+ 发展，未来 IP 网络需要具备智能超宽、智能联接、智能运维三大特征。其中，智能运维是保障未来网络业务 SLA 的重要手段，是实现自动化、智能化 IP 网络的关键。智能运维通过分析全网实时性能检测数据，对网络可能发生的风险进行提前干预、调整和优化，将“由故障推动的传统网络运维方式”转变为“主动预测性运维”。

IPv6+ 是智能 IP 网络的最佳选择，IFIT 作为智能运维方面的核心代表技术之一，是 IPv6+ 的重要组成部分。IFIT 的设计目标是构筑完整体系的随流检测，实现快速故障感知和自动修复，满足 5G 和云时代背景下的智能运维需求。如图 6-1 所示，面向未来，IFIT 将进一步迎来物联网、车联网、工业互联网等千行百业上云以及万物智联带来的新的智能运维需求与挑战。



图6-1 IFIT 未来发展



基于此，IFIT 也需要进一步完善，例如，提升技术能力，增加更多测量参数，有效提升测量精度；更大程度实现自动化部署和简易部署，通过减少数据上送提升性能等。为了实现这个目标，华为也将进一步推动产业合作，积极开展联合创新和验证，挖掘新需求和应用潜力，促进技术应用发挥更大价值。



联系我们

networkinfo@huawei.com

获取更多 IP 网络系列丛书

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

