IP Network eBook Series

IFIT

Authors: Jingyi Chen, Yali Wang

Information Digitalization and Experience Assurance (IDEA) Department

HUAWEI

Copyright

Authors:	Jingyi Chen, Yali Wang
Key Contributors:	Lanjun Luo, Jun Peng
Release Date:	2021-06-28
Issue:	01

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Preface

Author Introduction

Jingyi Chen: Documentation engineer for Huawei data communication products. She joined Huawei in 2019 and has since been developing documentation for measurement features, helping to promote related technologies.

Yali Wang: Huawei data communication research and standards engineer. She joined Huawei in 2018 and has since developed multiple Internet Engineering Task Force (IETF) standard drafts related to extending the control plane protocols for In-situ Flow Information Telemetry (IFIT) automation and played a leading role in drafting the China Communications Standards Association (CCSA) industry standard *Technical requirement of In-situ Flow Information Telemetry on Telecom Operator Networks* and European Telecommunications Standards Institute (ETSI) report *Reactive In-situ Flow Information Telemetry*.

About This Book

This book focuses on the background of IFIT, reveals why IFIT attracts significant attention, describes the unique technical values of IFIT, and demonstrates the diversified application scenarios and broad development space of IFIT. In addition, this book briefly describes the implementation principles of IFIT, helping you better understand the technical advantages of IFIT.

Intended Audience

This book is intended for ICT practitioners such as network engineers and readers who want to understand cutting-edge IP network technologies. Because IFIT involves many network concepts, readers of this book should have a basic understanding of IP network fundamentals, such as the IP network architecture, network Operation and Maintenance (O&M), and traditional measurement technologies.

Table of Contents

Chapter 1
IFIT Overview

In-situ Flow Information Telemetry (IFIT) is a technology that marks real service flows on a network to directly measure network performance indicators such as the delay, packet loss, and jitter. It adds IFIT packet headers to real service packets in order to measure network performance, and reports measurement data in real time through telemetry. As mobile transport, private networks and lines, and cloud-network architecture continue to develop rapidly, transport networks face new requirements and challenges, such as ultra-high bandwidth, numerous connections, high reliability, and low delay. With the data provided by IFIT, iMaster NCE-IP can display per-packet and per-flow performance indicators on its Graphical User Interface (GUI). IFIT significantly improves the timeliness and effectiveness of network Operation and Maintenance (O&M) and performance monitoring, enables Service Level Agreements (SLAs) to be guaranteed, and lays a solid foundation for intelligent O&M.

Chapter 2
IFIT Background

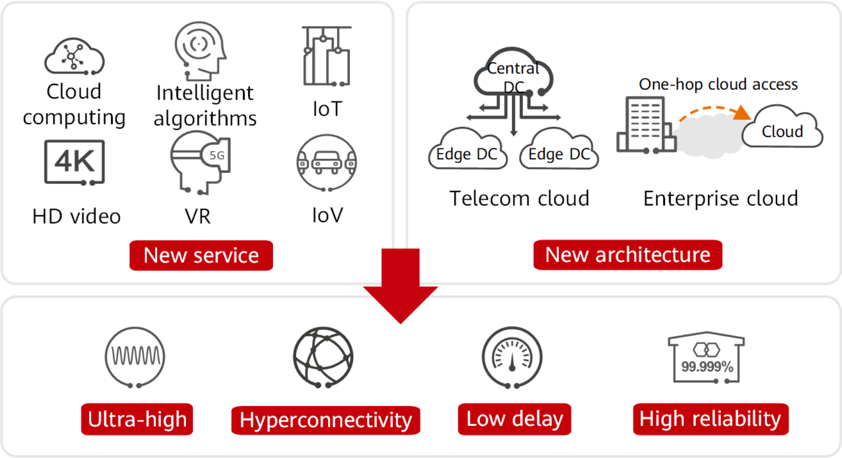
IFIT is a measurement protocol proposed by Huawei to meet the increasingly stringent SLA requirements of network services and address the challenges facing network O&M in the 5G and cloud era. IFIT — an Internet Engineering Task Force (IETF) standardized protocol — is the industry's first complete in-band quality awareness and demarcation solution. Within just a few years of being proposed, IFIT has attracted wide attention around the world. For example, it won the Best of Show Award Special Prize at Interop Tokyo 2019, and related academic documents were included at Association for Computing Machinery's Special Interest Group on Data Communications (SIGCOMM) — a globally leading conference in data communications and networking. This chapter describes the IFIT development process from three aspects: network service and architecture evolution, pain points of traditional network O&M, and lack of high-quality O&M methods.

2.1 Network Service and Architecture Evolution

IP network services and architecture have undergone significant changes in the 5G and cloud era, posing major challenges to network O&M. For example, the development of 5G has given rise to new services such as HD video, Virtual Reality (VR), and Internet of Vehicles (IoV). And, to facilitate unified management and reduce maintenance costs, cloudification of network devices and services has become an inevitable trend. As shown in Figure 2-1, new services and architecture pose the following challenges to the current transport network:

- Ultra-bandwidth: To carry vast amounts of service data, there is a need for bandwidth to be continuously increased, its utilization maximized, and its growth predictable.
- Hyperconnectivity: To support the vast number of intelligent terminals accessing the network, on-demand dynamic connections and automated service deployment are required. Furthermore, differentiated SLA assurance needs to be implemented for different service connections.
- Low delay: To optimize user experience by delivering smooth and responsive network access, the network delay needs to be significantly reduced from ~20 ms to as low as 2 ms, and the delay must be deterministic. For example, delay must be no more than 10 ms for telemedicine, 5 ms for IoV, and 2 ms for industrial control networks.
- High reliability: To improve network reliability, proactive fault detection and fast fault demarcation and locating are required, and the network self-healing capability needs to be further developed.

Figure 2-1 New challenges brought by new services and architecture



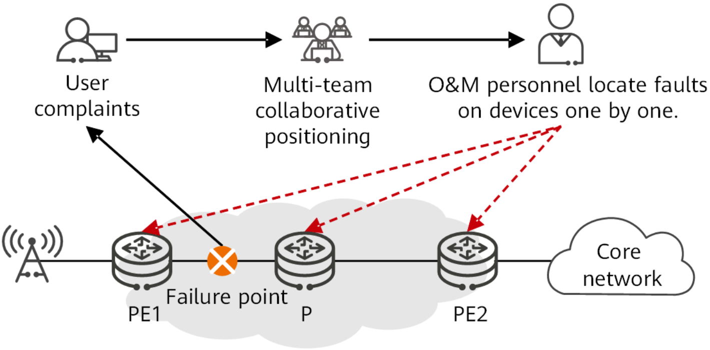
2.2 Pain Points of Traditional Network O&M

In the 5G and cloud era, the methods used for traditional network O&M cannot meet the SLA requirements of new applications. This is mainly due to the passive perception of service loss and the inefficient approach to fault demarcation and locating, as shown in Figure 2-2:

- Passive perception of service loss: In most cases, O&M personnel can determine the fault scope based on only complaints received from users or work orders dispatched by related service departments. This means that O&M personnel cannot perceive faults quickly and can only handle the faults passively, increasing the pressure on troubleshooting and potentially resulting in poor user experience. To resolve this problem, a service-level SLA measurement method that can proactively detect service faults is required on the live network.

- Inefficient fault demarcation and locating: Multiple teams often need to collaborate in order to demarcate and locate faults, and the lack of a clear demarcation mechanism between teams means that their responsibilities are not well defined. Troubleshooting is inefficient because devices must be manually checked one by one to identify the faulty device and the faulty device needs to be restarted or its traffic needs to be switched to another device. In addition, traditional Operations, Administration, and Maintenance (OAM) technologies simulate service flows by using test packets and therefore cannot reproduce performance deterioration or fault scenarios that are exactly the same as those on the live network. To resolve this problem, high-precision fast measurement based on real service flows is required on the live network.

Figure 2-2 Pain points of traditional network O&M

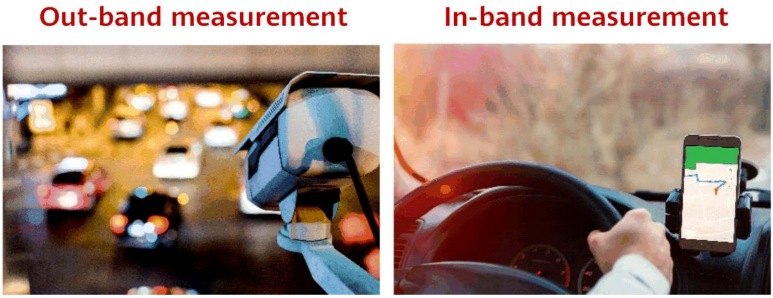

User complaints
Multi-team collaborative positioning
O&M personnel locate faults on devices one by one.
Failure point
PE1
P
PE2
Core network

2.3 Lack of High-Quality O&M Methods

To address the pain points involved in traditional network O&M, the industry keeps exploring and improving OAM technologies. These technologies are classified as out-band measurement or in-band measurement technologies based on the type of measurement they perform. To measure performance, out-band measurement indirectly simulates service data packets and periodically sends packets in order to collect statistics for End-to-End (E2E) paths. Conversely, in-band measurement marks real service packets to collect statistics of real service flows.

The following analogy, shown in Figure 2-3, helps to explain the differences between these two types of technologies. Assume that service flows on a network are like vehicles driving along the lanes of a highway. In this case, out-band measurement is similar to monitoring probes placed at fixed locations on both sides of the highway. Because blind spots may exist between these probes, the collected data is limited and cannot depict the entire journey of vehicles. In contrast, in-band measurement is similar to installing a positioning module on each vehicle. The driving information of each vehicle can then be collected to implement real-time positioning and accurately represent the journey of each vehicle.

Figure 2-3 Comparison between out-band measurement and in-band measurement



In terms of existing technologies, Two-Way Active Measurement Protocol (TWAMP) is representative of out-band measurement, while the earlier IP Flow Performance Measurement (IP FPM) and the more recent In-situ Operations, Administration, and Maintenance (IOAM) technologies are representative of in-band measurement. Although these technologies each offers specific advantages, none of them can completely meet the requirements of new network services and architecture.

- TWAMP is one of the first mainstream out-band measurement technologies. It is easy to deploy and therefore widely used. However, because TWAMP sends measurement probes at intervals between service packets — resulting in low measurement precision — the failure point cannot be located and the real service path cannot be displayed.

- IP FPM draws on the new concept of in-band measurement and directly colors IP packet headers, offering a significant improvement in measurement precision. However, because IP FPM cannot detect the forwarding path of service flows, it is difficult to deploy and therefore unsuitable for large-scale application on live networks.
- IOAM can be deployed without path discovery, making configuration simpler. However, because IOAM processes data in Passport mode (meaning that each node records the collected data in packets and the egress reports the data in a centralized manner), it has a negative impact on the forwarding plane efficiency of devices.

2.4 Emergence of IFIT

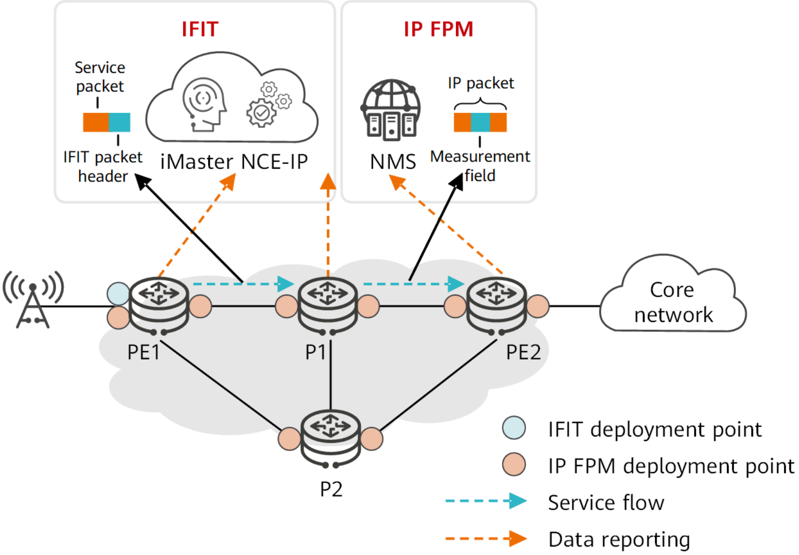
At Mobile World Congress (MWC) 2018, Huawei officially launched the Intent-Driven Network (IDN) solution, which creates a digital twin of the network architecture to bridge the gap between physical networks and business intents. This solution drives the network to evolve from Software-Defined Networking (SDN) to IDN and maximizes business value. IFIT was developed to meet the requirements of IDNs — specifically, their need to accurately identify user intents and implement E2E automated network configuration, real-time perception of user experience, predictive analysis, and proactive optimization. IFIT is an in-band measurement technology that overcomes the disadvantages of IP FPM and IOAM.

The key differences between IFIT and IP FPM are described as follows and shown in Figure 2-4.

- In terms of service deployment, the controller obtains the network-wide topology in advance and maps the reporting node information (such as the device ID and interface ID) to the network topology to implement automatic path discovery for IFIT. IFIT parameters need to be configured only on the ingress, making deployment simpler compared with IP FPM's hop-by-hop configuration and improving deployment efficiency by 80%.

- In terms of scalability, IFIT implements in-band flow measurement by adding IFIT packet headers to service flows. Compared with IP FPM, which uses existing fields in IP packets, IFIT enhances scalability and meets long-term network evolution requirements.

Figure 2-4 Comparison between IFIT and IP FPM



The key differences between IFIT and IOAM are described as follows and shown in Figure 2-5:

- In terms of forwarding efficiency, IFIT processes data in Postcard mode, which offers greater forwarding efficiency compared with the Passport mode used by IOAM. Specifically, upon receiving data packets that contain instruction headers, nodes in the IFIT measurement domain do not record the collected data in these packets (unlike in the Passport mode). Instead, in Postcard mode, each node generates a packet containing the collected data and sends it to the collector. Because the IFIT packet header is short and fixed, the impact on the forwarding plane efficiency is minimized.

- In terms of the measurement scope, IFIT enables packet loss to be measured on a per-hop basis by reporting information about each hop.

Figure 2-5 Comparison between IFIT and IOAM

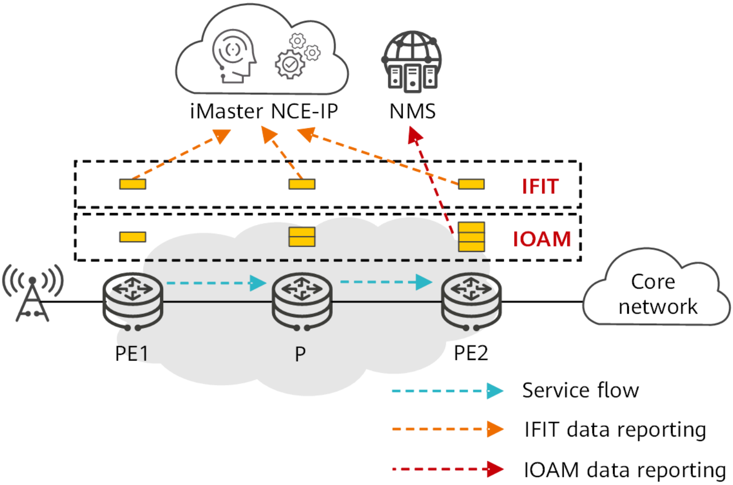


Table 2-1 compares the differences between the preceding OAM technologies, indicating the multiple advantages IFIT offers over other technologies.

Table 2-1 Comparison between different OAM technologies

Item	IP FPM	IOAM	IFIT
Deployment complexity	High	Low	Low
Hop-by-hop measurement	Supported	Hop-by-hop packet loss measurement not supported	Supported
Forwarding plane efficiency	Medium	Low	High

Item	IP FPM	IOAM	IFIT
Data collection pressure	Low	High	Low when only the coloring function is used; High when IFIT extended functions are used
Scalability	Weak (because it is based on existing fields in IP packet headers)	Strong	Strong

Combined with big data analytics and intelligent algorithms, IFIT can further build an intelligent O&M system to enable predictive analysis and self-healing capabilities on networks. This enables faults to be proactively identified and rectified before they affect user experience, and enables the automation and intelligentization of networks.

At present, standards organizations such as IETF, European Telecommunications Standards Institute (ETSI), and China Communications Standards Association (CCSA) are accelerating the development of IFIT standards to facilitate its commercial use on a wider scale. The main IFIT standards are as follows:

- The IETF draft *In-situ Flow Information Telemetry Framework (draft-song-opsawg-ifit-framework)* and the *IETF standards Alternate-Marking Method for Passive and Hybrid Performance Monitoring (RFC 8321)* and *Multipoint Alternate-Marking Method for Passive and Hybrid Performance Monitoring (RFC 8889)* define the IFIT framework and coloring principles.
- The IETF drafts *IPv6 Application of the Alternate Marking Method (draft-fz-6man-ipv6-alt-mark)* and *Encapsulation For MPLS Performance Measurement with Alternate Marking Method (draft-cheng-mpls-inband-pm-encapsulation)* define the IPv6 and MPLS encapsulation mechanisms for the IFIT forwarding plane, respectively.
- The IETF drafts *IGP Extensions for In-situ Flow Information Telemetry (IFIT) Capability Advertisement (draft-wang-lsr-igp-extensions-ifit)* and *BGP SR Policy Extensions to Enable IFIT (draft-qin-idr-sr-policy-ifit)* define the IFIT

control plane capability advertisement mechanism and the IFIT automatic deployment mechanism implemented using SR Policy, respectively.

- The IETF drafts *Subscription to Distributed Notifications (draft-unyte-netconf-distributed-notif)* and *UDP-based Transport for Configured Subscriptions (draft-unyte-netconf-udp-notif)* define the distributed telemetry mechanism and UDP-based data sending mechanism, respectively.

Chapter 3
Technical Benefits of IFIT

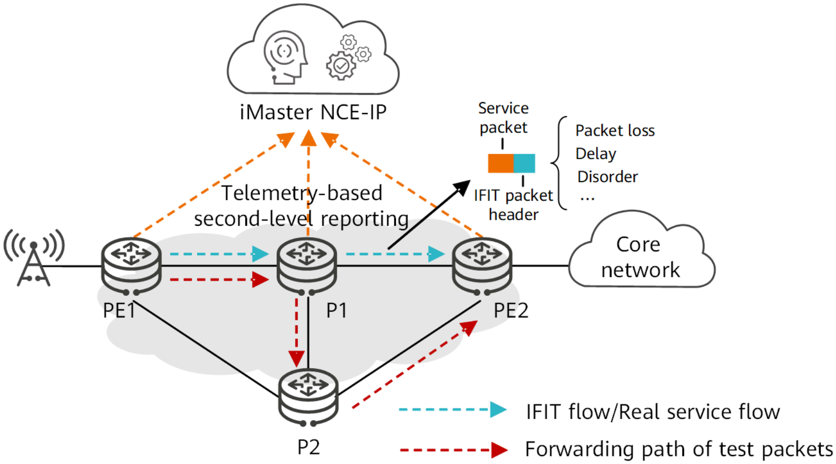
IFIT reflects the actual forwarding paths of service flows by adding IFIT headers to real service packets and leverages telemetry's high-speed data collection capability to implement high-precision and multi-dimensional quality measurement of real services. Integrating capabilities such as transparent transmission and automatic learning of forwarding paths, IFIT can flexibly adapt to large-scale and multi-type service scenarios. And by supporting numerous user-defined monitoring policies and GUI-based display of measurement results on iMaster NCE-IP, IFIT brings tangible improvements to O&M experience. In addition, IFIT combines big data analytics and intelligent algorithm capabilities to build a closed-loop intelligent O&M system.

3.1 High-Precision and Multi-Dimensional Quality Measurement of Real Services

Traditional OAM technologies use test packets that may be forwarded along paths different from those used for real service flows. As shown in Figure 3-1, IFIT eschews this approach and instead provides in-band flow measurement capabilities based on real service packets, offering the following benefits:

- IFIT can restore the actual forwarding path of packets and accurately detect the performance information of each service in multiple dimensions, such as delay, packet loss, and disorder. This means that the precision of packet loss detection can reach 10^{-6}, while that of delay detection can reach microseconds.
- IFIT can monitor network SLAs in real time and quickly demarcate and locate faults by working together with telemetry's data collection function, which enables data to be collected within seconds.
- IFIT can detect all silent faults and locate them within seconds. Silent faults — those that affect service experience but do not reach the alarm triggering threshold and cannot be effectively located — cause significant damage on the live network, as they account for 15% of all faults but consume more than 80% of the time spent on O&M. IFIT can identify minor exceptions on the network and detect the loss of even one packet. This high precision of packet loss detection meets the requirements of "zero-packet-loss" services such as financial final accounting, telemedicine, industrial control, and power differential protection, ensuring high reliability for such services.

Figure 3-1 IFIT based on real service flows


iMaster NCE-IP
Service packet
Packet loss
Delay
Disorder
...
IFIT packet header
Telemetry-based second-level reporting
Core network
PE1
P1
PE2
P2
IFIT flow/Real service flow
Forwarding path of test packets

3.2 Flexible Adaptation to Large-Scale and Multi-Type Service Scenarios

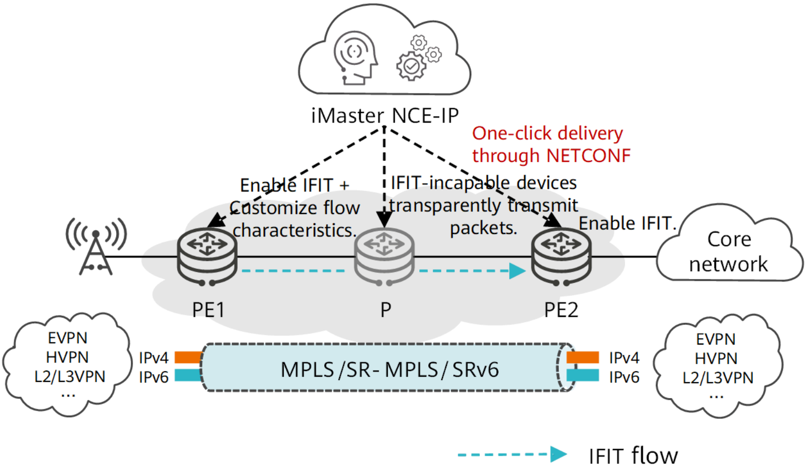
Network development is usually a lengthy process, meaning that multiple types of devices may coexist on a network and carry various types of services as requirements continue to grow and evolve. IFIT is easy to deploy and can flexibly adapt to large-scale and multi-type service scenarios, as shown in Figure 3-2.

- IFIT supports one-click delivery of network-wide configuration. E2E or hop-by-hop measurement can be configured only on the ingress as required, with IFIT simply enabled on transit and egress nodes. In this way, IFIT is applicable to both small networks with few devices and large networks with many devices.
- IFIT flows can be manually configured (static flows), automatically learned, or triggered by traffic with IFIT headers (dynamic flows). Such flows can be specific flows created based on unique information (such as 5-tuple), tunnel-level aggregation flows, or VPN-level aggregation flows. With IFIT,

both specific service flows and E2E private line traffic can be detected at different granularities.

- IFIT has good compatibility with existing networks and can be applied to networks with various types of devices. Devices that do not support IFIT can transparently transmit IFIT flows, avoiding the potential problems involved in interconnection with third-party devices.
- IFIT can automatically learn actual forwarding paths without needing to detect the paths in advance. This eliminates the need to plan or set forwarding paths in advance for hop-by-hop measurement on all NEs along the path, thereby reducing the workload.
- IFIT applies to various types of networks, such as Layer 2 and Layer 3 networks, and multiple types of tunnels, meeting diverse requirements on the networks.

Figure 3-2 IFIT adapts to multiple-type service scenarios

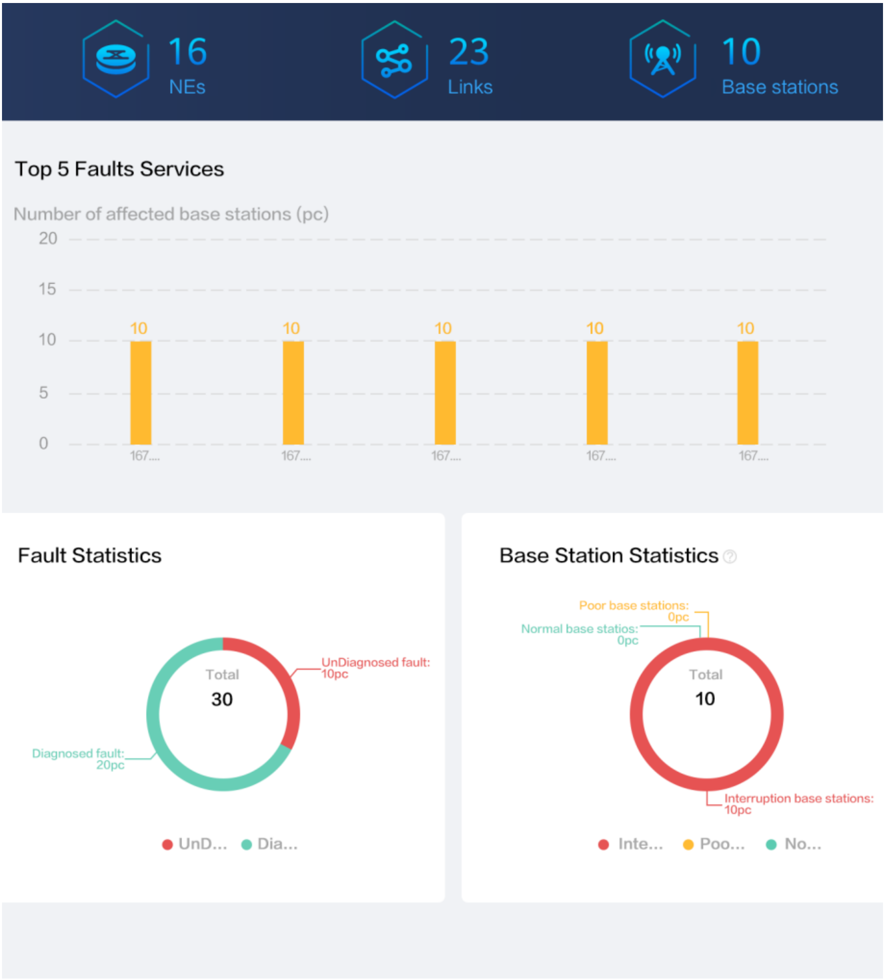

iMaster NCE-IP
One-click delivery through NETCONF
Enable IFIT + Customize flow characteristics.
IFIT-incapable devices transparently transmit packets.
Enable IFIT.
Core network
PE1
P
PE2
EVPN
HVPN
L2/L3VPN
...
IPv4
IPv6
MPLS /SR- MPLS / SRv6
IPv4
IPv6
EVPN
HVPN
L2/L3VPN
...
IFIT flow

3.3 Visualized O&M GUI

Without visualized O&M, network O&M personnel need to manually configure devices one by one, and then multiple departments need to cooperate to check items one by one. As such, the O&M efficiency is low. Visualized O&M brings significant enhancements to the efficiency of O&M. It not only provides centralized management and control capabilities, but also supports online service planning and one-click deployment. Furthermore, it supports quick fault demarcation and locating through SLA visualization. One of the key benefits of IFIT is that it provides visualized O&M capabilities. As shown in Figure 3-3, users can deliver different IFIT monitoring policies through the iMaster NCE-IP GUI as required to implement routine proactive O&M and quick troubleshooting. The details are as follows:

- Routine proactive O&M: O&M personnel can routinely monitor base station status statistics, the network fault trend chart, the abnormal base station trend chart, and the top-5 faults that most affect base stations at the network and area level. This enables O&M personnel to gain actionable insight into the health status of the network through performance reports. In VPN scenarios, detailed information about E2E service flows is provided to help O&M personnel proactively identify and locate faults and ensure the overall SLA of private line services.
- Quick troubleshooting: Upon receiving a fault report, O&M personnel can search for the base station name or IP address to view the service topology and IFIT hop-by-hop flow indicators, and rectify the fault based on the fault location, possible causes, and rectification suggestions. In addition, O&M personnel can view information about topology paths and historical fault locations collected over the past seven days (covering 24 hours per day).

Figure 3-3 iMaster NCE-IP GUI



As shown in Figure 3-3, the IFIT monitoring results can be displayed on iMaster NCE-IP GUI. This helps users learn about the network status and quickly detect and rectify faults, achieving superior O&M experience.

3.4 Closed-Loop Intelligent O&M System

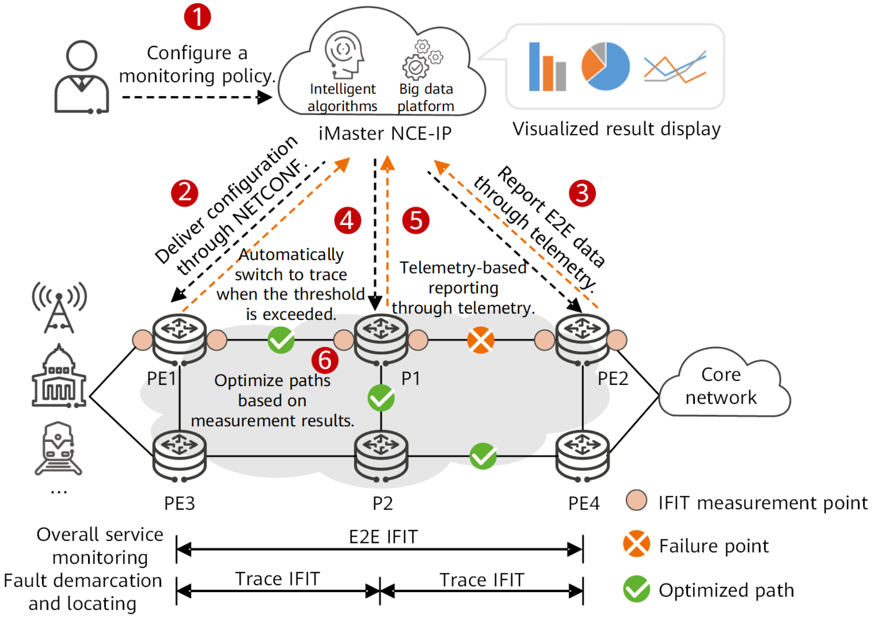
To address the challenges facing the transport network due to network architecture and service evolution, meet the requirements for improving traditional network O&M methods, and meet users' requirements for E2E high-quality network experience, passive O&M needs to be changed to proactive O&M, and an intelligent O&M system needs to be built. Such a system can proactively detect exceptions in real services, automatically demarcate faults, and implement fast fault locating and self-healing, creating automated processes that can adapt to complex and changing network environments.

As shown in Figure 3-4, IFIT works with telemetry, big data analytics, intelligent algorithms, and other technologies to build an intelligent O&M system. The working process of this system is as follows:

1. A user enables the IFIT capability on the entire network through iMaster NCE-IP, performs telemetry subscription, selects the ingress, egress, and links of the service as required, and configures an IFIT monitoring policy.
2. iMaster NCE-IP converts the monitoring policy into device commands that it delivers to devices.
3. Devices generate IFIT E2E monitoring instances. The ingress and egress report service SLA data to iMaster NCE-IP through telemetry within seconds, and iMaster NCE-IP processes the data based on the big data platform and displays the detection results on its GUI.
4. Monitoring thresholds are set. If the packet loss or delay exceeds the threshold, iMaster NCE-IP automatically adjusts the monitoring policy from E2E to hop-by-hop and delivers the updated policy to devices through Network Configuration Protocol (NETCONF).
5. Based on the updated policy, the devices adjust the service monitoring mode to hop-by-hop and report service SLA data to iMaster NCE-IP hop by hop through telemetry within seconds. iMaster NCE-IP then processes the data based on the big data platform and displays the detection results on its GUI.
6. iMaster NCE-IP performs intelligent analysis based on service SLA data, identifies potential root causes based on exception information such as device KPIs and logs, provides handling suggestions, and reports work orders.

In addition, iMaster NCE-IP optimizes service paths to ensure service quality and implement fault self-healing.

Figure 3-4 Building a closed-loop intelligent O&M system based on IFIT


1
Configure a monitoring policy.
Intelligent algorithms
Big data platform
iMaster NCE-IP
Visualized result display
2
Deliver configuration through NETCONF.
4
Automatically switch to trace when the threshold is exceeded.
5
Telemetry-based reporting through telemetry.
3
Report E2E data through telemetry.
PE1
P1
PE2
6
Optimize paths based on measurement results.
Core network
PE3
P2
PE4
...
IFIT measurement point
Failure point
Optimized path
Overall service monitoring
E2E IFIT
Fault demarcation and locating
Trace IFIT
Trace IFIT

The results of E2E and hop-by-hop (trace) IFIT are data sources for the big data platform and intelligent algorithm analysis. These results form the foundation of the intelligent O&M system's ability to implement precise fault demarcation and locating and fast fault self-healing. In addition to providing IFIT for in-band flow measurement and telemetry for high-speed statistics collection, the big data platform enables queries to be performed within seconds and massive IFIT data to be efficiently processed. Furthermore, efficient and reliable data analysis and conversion are ensured if a single node fails, as the failure does not cause data loss. The intelligent algorithm can cluster poor-quality events as mass network faults. That is, the algorithm calculates the path similarity of poor-quality service flows in the same period and considers such flows that reach the algorithm threshold to be caused by the same fault. This enables the common failure point to be located, with an identification accuracy of more than 90%, improving the O&M efficiency and reducing the service interruption time. The combination of IFIT, telemetry, the big data platform, and the intelligent algorithm ensures the intelligent O&M system is a closed-loop one. Furthermore, it promotes the optimization of intelligent O&M solutions that can adapt to future network evolution.

Chapter 4
IFIT Fundamentals

This chapter describes the IFIT fundamentals, including the IFIT indicators based on the alternate coloring method, E2E and hop-by-hop measurement modes, IFIT automatic triggering detection capability, and telemetry-based data sending. It also explains the technical benefits of IFIT on the forwarding plane, control plane, and management plane.

4.1 How Does IFIT Accurately Locate Faults?

IFIT inserts IFIT headers into real service packets to implement fault demarcation and locating. To explain how IFIT accurately locates faults, the following sections use the IFIT over SRv6 scenario as an example to describe the format of the IFIT packet header and the functions of the coloring flag bit and measurement mode bit.

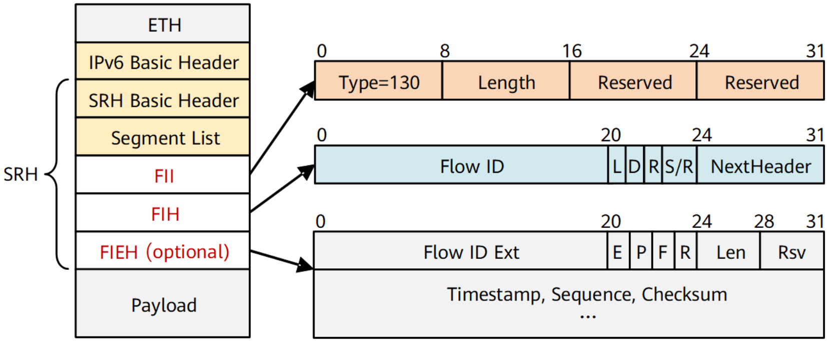
IFIT Packet Header Format

In an IFIT over SRv6 scenario, an IFIT packet header is encapsulated into a Segment Routing Header (SRH), as shown in Figure 4-1. In this scenario, only the specified SRv6 endpoint (any node that receives and processes SRv6 packets) needs to parse the IFIT packet header. O&M personnel need to perform IFIT only on specified nodes that have the IFIT data collection capability, ensuring adaptability to traditional networks.

An IFIT packet header contains the following contents:

- Flow Instruction Indicator (FII): identifies the beginning of an IFIT packet header and defines its overall length.
- Flow Instruction Header (FIH): uniquely identifies a service flow. The L and D bits provide the packet loss and delay measurement capabilities, respectively, based on alternate coloring.
- Flow Instruction Extension Header (FIEH): defines the E2E or hop-by-hop measurement mode using the E bit and performs unidirectional or bidirectional measurement on service flows using the F bit. In addition, extended functions such as per-packet and disorder measurement are supported.

Figure 4-1 IFIT packet header format

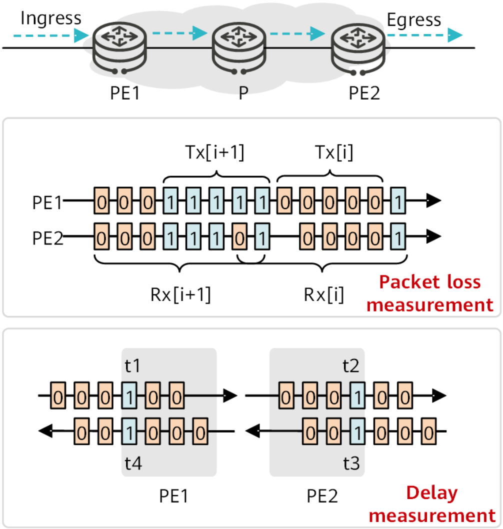


Alternate Coloring-based IFIT Indicators

Packet loss rate and delay are two important indicators of network quality. Packet loss rate refers to the percentage of the number of lost packets to the number of sent packets during packet forwarding. The packet loss measurement function can be used to calculate the difference between the numbers of packets entering and leaving the network within a measurement period. Delay refers to the time required for transmitting data packets from one point to another on a network. The device samples service packets, records the forwarding time of these service packets, and then calculates the transmission delay of the specified service flow on the network.

IFIT implements packet loss and delay measurement by alternately coloring service packets. Coloring refers to marking packets for specific measurement, which IFIT does by setting the packet loss coloring bit L or delay coloring bit D to 0 or 1. On the network shown in Figure 4-2, service packets enter the network through PE1 and leave the network through PE2. IFIT is used to collect statistics about the packet loss and delay on the network.

Figure 4-2 Alternate coloring-based IFIT indicators



IFIT packet loss measurement for packets from PE1 to PE2 is performed as follows:

1. PE1 sets the L bit of each service packet to 0 or 1 on the ingress, flips the L bit value once in each measurement period, and calculates the number (Tx[i]) of packets with the bit value of 0 or 1 in the period.
2. PE2 extends the measurement period on the egress to prevent packet disorder from affecting the measurement result. In each measurement period, PE2 calculates the number (Rx[i]) of packets with the bit value of 0 or 1.
3. The number of lost packets in period i is calculated using the following formula: Tx[i] – Rx[i]. The packet loss rate in period i is calculated using the following formula: (Tx[i] – Rx[i])/Tx[i].

IFIT delay measurement between PE1 and PE2 is performed as follows:

1. PE1 sets the D bit of a service packet to 1 on the ingress and records the timestamp t1.
2. PE2 receives the service packet with the D bit set to 1 and records the timestamp t2.
3. The one-way delay from PE1 to PE2 is calculated as t2 – t1. Similarly, the one-way delay from PE2 to PE1 is calculated as t4 – t3, and the two-way delay is calculated as (t2 – t1) + (t4 – t3).

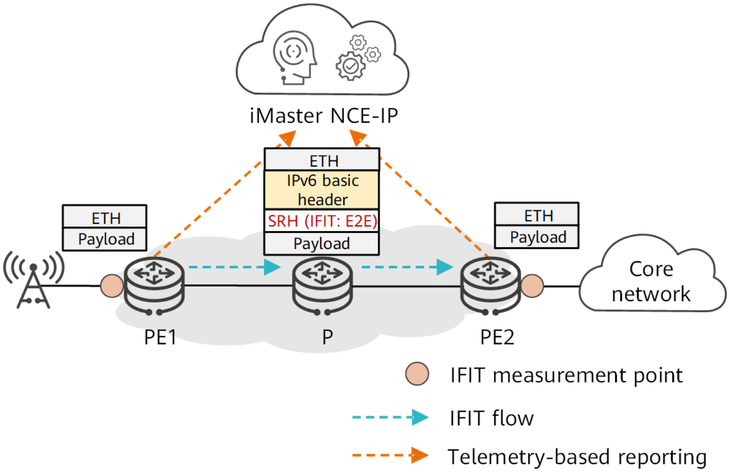
By coloring real service packets and leveraging time synchronization protocols such as 1588v2, IFIT can proactively detect minor network changes and reflect the packet loss and delay on the network.

E2E and Hop-By-Hop Measurement Modes

There are two common modes of measurement: E2E and hop-by-hop (trace). The E2E mode applies to scenarios where E2E overall service quality monitoring is required, whereas the hop-by-hop (trace) mode applies to scenarios where hop-by-hop demarcation is required for low-quality services or on-demand hop-by-hop monitoring is required for VIP services. IFIT supports both E2E and trace modes.

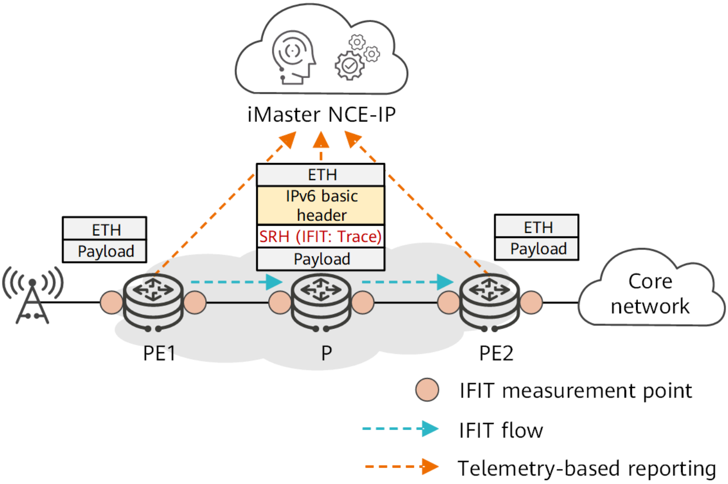
In E2E mode, an IFIT measurement point needs to be deployed only on the ingress to trigger measurement, and IFIT just needs to be enabled on the egress. In this case, only the ingress and egress sense IFIT packets and report measurement data, and transit nodes perform bypass processing, as shown in Figure 4-3.

Figure 4-3 E2E measurement



In hop-by-hop (trace) mode, an IFIT measurement point needs to be deployed on the ingress to trigger measurement, and IFIT needs to be enabled on all IFIT-capable nodes along the service flow path, as shown in Figure 4-4.

Figure 4-4 Trace measurement



In most cases, E2E IFIT and trace IFIT are used together. When the E2E IFIT measurement data reaches the threshold, trace IFIT is automatically triggered. In this case, the service flow forwarding path can be restored, and faults can be quickly demarcated and located.

4.2 How Does IFIT Automatically Trigger Measurement?

To enable automatic triggering of IFIT, the controller needs to know whether devices on the network support IFIT. IGP/BGP extensions can be used to advertise information about network devices' IFIT capabilities, while the Border Gateway Protocol-Link State (BGP-LS) protocol can be used to summarize such information and report it to the controller. Based on the information it receives, the controller then determines whether IFIT can be enabled in a specified network domain.

The following uses BGP extensions as an example. Figure 4-5 shows the IPv6-Address-Specific IFIT Tail Community defined by the extended BGP community attribute. The IFIT egress can use this community attribute to advertise its supported IFIT capabilities to the peer device (IFIT ingress).

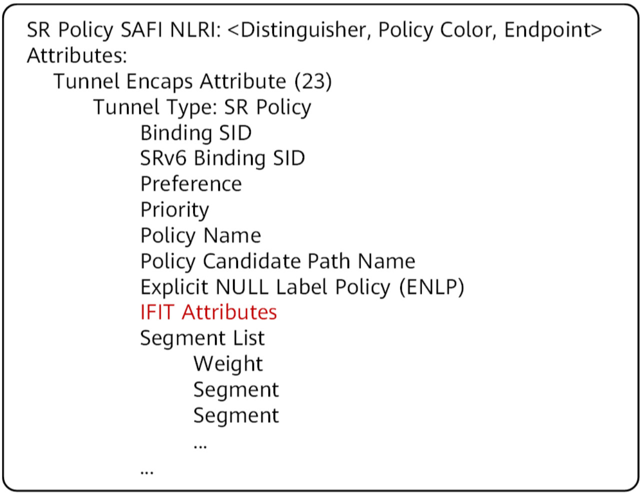
Figure 4-5 IPv6-Address-Specific IFIT Tail Community format

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

As shown in Figure 4-5, the Originating IPv6 Address field carries the IFIT egress's IPv6 unicast address. The IFIT Capabilities field indicates what IFIT capabilities the node supports, including E2E and hop-by-hop measurement capabilities and alternate coloring-based measurement capabilities.

In order to quickly detect SLA deterioration of deployed services for service adjustment, IFIT information can be added to an SR Policy delivered by the extended BGP/PCEP protocol. In this case, IFIT is automatically activated and starts to run when the SR Policy is delivered, and its information is carried in the SR Policy, as shown in Figure 4-6.

Figure 4-6 Structure of an SR Policy that carries IFIT information



```
SR Policy SAFI NLRI: <Distinguisher, Policy Color, Endpoint>
Attributes:
   Tunnel Encaps Attribute (23)
        Tunnel Type: SR Policy
              Binding SID
              SRv6 Binding SID
              Preference
              Priority
              Policy Name
              Policy Candidate Path Name
              Explicit NULL Label Policy (ENLP)
              IFIT Attributes
              Segment List
                    Weight
                    Segment
                    Segment
                    ...
              ...
```

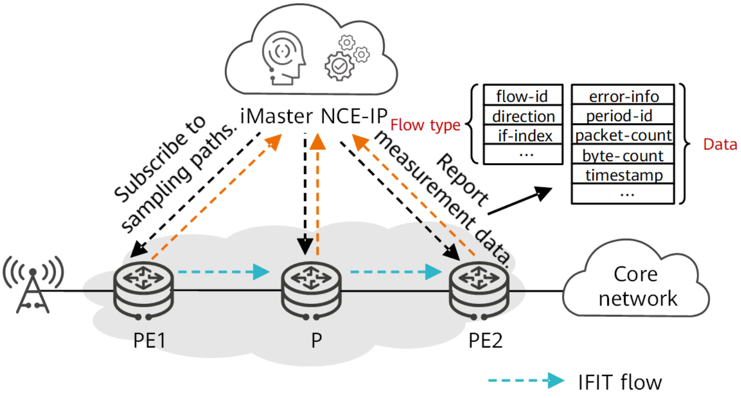
When BGP extensions are used to deliver an SR Policy, the IFIT attribute information can be carried in the IFIT Attributes field. This allows IFIT to measure all candidate paths of the SR Policy in the same way. The candidate paths can be multiple SR paths, and each path is specified by a segment list. The IFIT attribute is attached to the candidate path attributes as a sub-TLV.

4.3 How Does IFIT Send Data in Real Time?

In an intelligent O&M system, IFIT uses telemetry to send measurement data to iMaster NCE-IP for analysis in real time. Telemetry is a technology that remotely collects data from physical or virtual devices at a high speed. Devices periodically send interface traffic statistics, CPU usage, and memory usage to collectors in push mode. Compared with the traditional pull mode (question-answer interaction), the push mode provides data collection in real time. Telemetry flexibly collects data by subscribing to different sampling paths. This allows IFIT to manage more devices and obtain measurement data with higher precision, providing big data to enable fast locating of network faults and the optimization of network quality.

As shown in Figure 4-7, a user subscribes to the data source of a device on iMaster NCE-IP. The device collects measurement data based on the configuration requirements. It then encapsulates the data, such as the flow ID, flow direction, error information, and timestamp, into telemetry packets for reporting. iMaster NCE-IP receives and stores measurement data and displays analysis results on its GUI.

Figure 4-7 Telemetry-based data sending



Working with telemetry's high-speed data collection technology, which can collect data within seconds, IFIT sends measurement data to iMaster NCE-IP in real time to implement efficient performance measurement.

Chapter 5

Successful Applications of IFIT

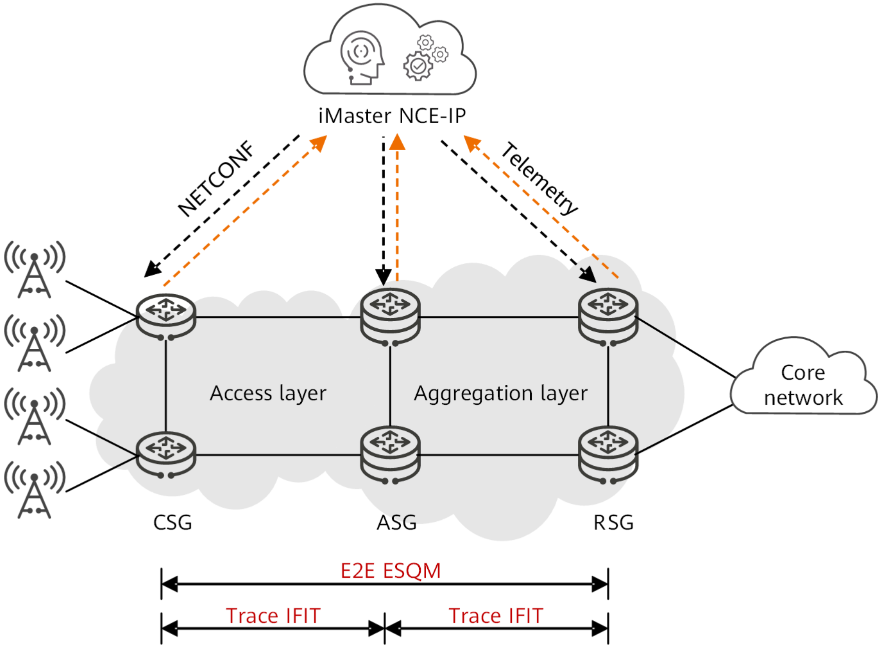
With the rapid development of 5G, carrier users have higher requirements on network quality. This means that effective monitoring for mobile transport networks is especially important. In addition, as cloud computing continues to develop, service cloudification has become the primary mode of service deployment for enterprise users. With solutions such as intelligent cloud-network and one WAN emerging, efficient O&M in cloud-network integration scenarios is urgently required. IFIT can meet the preceding requirements. This chapter describes the successful applications of IFIT in three scenarios: Internet Protocol Radio Access Network (IP RAN) mobile transport network, intelligent cloud-network private line service, and one financial WAN.

5.1 IP RAN Mobile Transport Network

The IP RAN solution is developed to maximize carriers' return on investment (ROI), reduce network construction costs, and ensure smooth network evolution. The IP RAN mobile transport network — a large-scale network — has various access modes and carries various mobile transport services (such as HD video) that pose higher requirements on link connectivity and performance indicators.

In this case, Huawei proposes the E2E Enhanced Stream Quality Monitoring (ESQM) + trace IFIT hybrid measurement solution. As shown in Figure 5-1, IFIT quickly demarcates and locates faults and replays faults on demand, improving SLA experience and O&M efficiency.

Figure 5-1 Application of IFIT on an IP RAN mobile transport network



ESQM is a measurement technology that collects statistics on TCP, SCTP, and GTP packets based on 5-tuple information. In this scenario, E2E ESQM performance measurement is performed first. Hop-by-hop (trace) IFIT is triggered when the base station flow performance indicator exceeds the specified threshold. iMaster NCE-IP summarizes the reported hop-by-hop measurement data for path restoration and fault locating. This solution offers the following benefits:

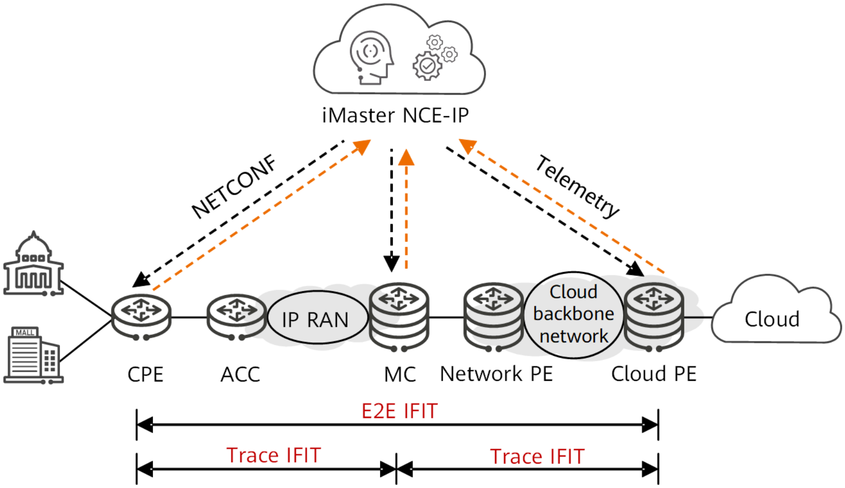
1. Detailed indicator data of service flows can be monitored from different dimensions, such as base station flows, data flows, and signaling flows. In addition, this solution supports clustering to process base station flow faults and quickly demarcate poor-quality services, preventing multiple faults of numerous base station flows from triggering more trace IFIT instances than are supported.
2. If a fault occurs outside the IP RAN, IFIT can quickly and accurately prove that the fault is not due to the network. If a fault occurs on the IP RAN, IFIT can quickly locate the faulty NE or link, improving network O&M efficiency.
3. Based on the real-time performance data of base stations across the entire network, a big data-based intelligent O&M system can be constructed to implement high-precision and service-level SLA awareness in real time and multi-dimensional visualization for base station services. It can also analyze and evaluate potential network risks, and optimize network resources to implement automatic and intelligent O&M.

5.2 Intelligent Cloud-Network Private Line Service

Based on intelligent IP networks, the intelligent cloud-network technology implements automatic and intelligent cloud-network operations and O&M, supporting digital transformation of various industries, including carrier To Business (2B), government, and healthcare. The intelligent cloud-network private line service is an important part of the intelligent cloud-network technology. It leverages the wide coverage of the mobile transport network to provide enterprise private line services more conveniently and improves the network deployment, operations, and O&M efficiency through E2E collaborative management.

IFIT provides VPN service analysis and assurance for intelligent cloud-network private line services, including site-to-site private line, site-to-cloud private line, and cloud-network interconnection scenarios. The following uses the cloud private line as an example to describe the E2E IFIT + trace IFIT solution. As shown in Figure 5-2, IFIT ensures E2E high reliability and implements minute-level fault locating through visualized O&M.

Figure 5-2 Application of IFIT in the intelligent cloud-network private line service



In this scenario, E2E IFIT is performed first. Hop-by-hop IFIT is triggered when the performance indicator of a VPN flow exceeds the specified threshold. iMaster NCE-IP then summarizes the reported hop-by-hop measurement data for path restoration and fault locating. This solution offers the following benefits:

1. Analyzes and locates faults of a VPN flow and queries E2E performance indicators of the VPN service flow by granularity ranging from year to minute, including the maximum traffic rate, maximum one-way delay, and maximum packet loss rate.
2. Queries E2E VPN service information based on the VPN name, VPN type, and service status. If multiple segments of service flows exist, the status value of the segment with the lowest quality is used.

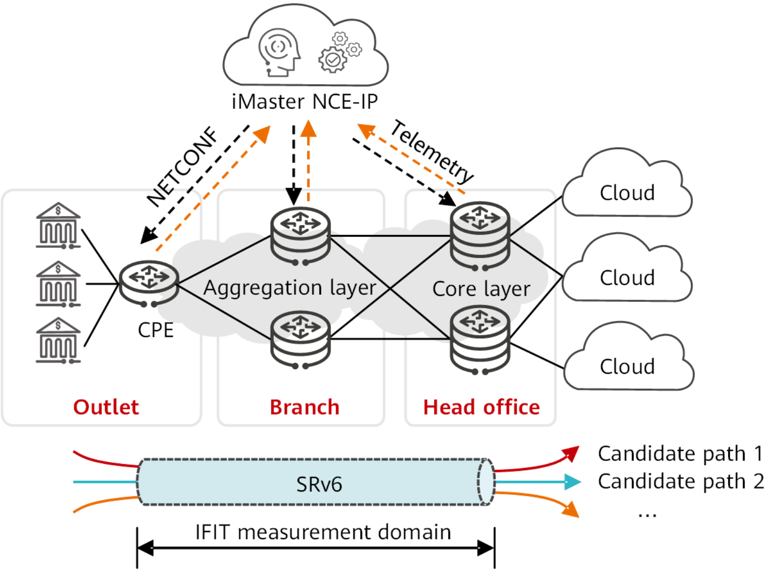
3. Implements E2E multi-dimensional exception identification, network health visualization, intelligent fault diagnosis, and fault self-healing in a closed-loop manner.

5.3 One Financial WAN

The concept of one WAN has been introduced to facilitate unified management. This technology coordinates different networks to provide cross-domain network services. In the financial industry, tier-2 banks, branches, subsidiaries, and external organizations first connect to tier-1 banks, which aggregate service traffic and then connect to the bank core network to implement mutual access between them and the head office data center. In this case, the concept of centralized management for one WAN is of particular importance.

One financial WAN uses SRv6 technology to quickly and easily establish basic network connections between the cloud and various access points, ensuring efficient service provisioning. In terms of O&M capabilities, the financial industry itself has high requirements on the SLA assurance, and one financial WAN faces higher requirements due to the diverse array of branch service types brought about by the development of banking services. For example, in addition to traditional production and office services, other services such as security protection, IoT, and public cloud services are now prevalent. To address this issue, Huawei proposes the tunnel-level IFIT solution. As shown in Figure 5-3, IFIT can simplify the O&M process and optimize O&M experience.

Figure 5-3 Application of IFIT on one financial WAN



This solution offers the following benefits:

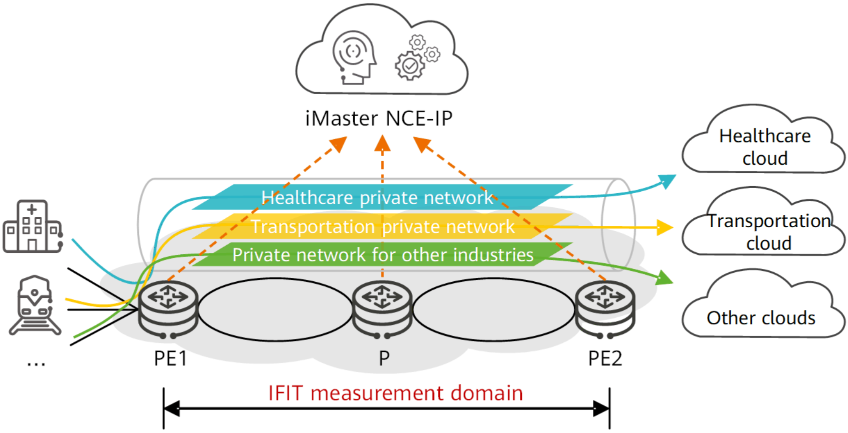
1. In SRv6 scenarios, tunnel-level IFIT can be enabled to measure the quality of each SRv6 segment list and select the optimal link. The link currently in use is periodically compared with the optimal link for path selection and optimization, implementing intelligent traffic steering.
2. One core controller is deployed to perform centralized O&M on the entire financial network and implement E2E management and scheduling.

Chapter 6
IFIT Promotes Intelligent O&M in the IPv6 Enhanced Innovation Era

The 5G and cloud era is driving the development of IP networks toward IPv6 Enhanced Innovation. In the future, IP networks must have three features: intelligent ultra-broadband, intelligent connection, and intelligent O&M. Intelligent O&M is vital for ensuring the SLA of future network services and key to implementing automated and intelligent IP networks. It analyzes real-time performance measurement data of the entire network; intervenes, adjusts, and optimizes possible network risks in advance; and changes the traditional network O&M mode driven by faults to a proactive and predictive one.

IPv6 Enhanced Innovation is the optimal choice for intelligent IP networks. As one of the core technologies for intelligent O&M, IFIT is an important part of IPv6 Enhanced Innovation. IFIT is designed to build a complete in-band flow measurement system to implement fast fault detection and self-healing, meeting intelligent O&M requirements in the 5G and cloud era. As shown in Figure 6-1, IFIT will further embrace new intelligent O&M requirements and challenges brought by the cloudification of various industries, such as the IoT, IoV, and industrial Internet, as well as the intelligent connection of everything.

Figure 6-1 Future development of IFIT



Although IFIT offers many benefits over other measurement technologies, it is still currently a work in progress. For example, technical capabilities need to be improved, more measurement parameters need to be added, and measurement precision needs to be improved. In addition, greater automation is needed to simplify deployment, and the volume of sent data needs to be reduced to improve performance. To achieve these objectives, Huawei will further promote industry cooperation, proactively carry out joint innovation and verification, explore new requirements and application potential, and promote the technology's wider application.

IP Network
eBook Series

Contact Us

networkinfo@huawei.com

More IP Network eBooks

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