ETSI GR ENI 032 V4.1.1 (2024-05)

Experiential Networked Intelligence (ENI); In-situ Flow Information Telemetry (IFIT) Deployment Scenarios

Disclaimer

The present document has been produced and approved by the Experiential Networked Intelligence (ENI) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/ENI-0032v411_IFIT

Keywords
network, performance, telemetry

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Experiential Networked Intelligence (ENI).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The purpose of the present document is to provide guidelines about IFIT deployment use cases and application scenarios. As described in ETSI GR ENI 012 [i.1], IFIT is a key technology for ensuring the SLA of future network services and for implementing automated and intelligent IP networks. Several technical specifications in IETF have already been defined to set the basis and ISG ENI is playing an important role in defining the whole framework. The present document includes a report of IFIT use cases and how they fit the ENI architecture.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GR ENI 012 (V1.1.1): "Experiential Networked Intelligence (ENI); Reactive In-situ Flow Information Telemetry".

[i.2] IETF RFC 9341 (December 2022): "Alternate-Marking Method".

[i.3] IETF RFC 9342 (December 2022): "Clustered Alternate-Marking Method".

[i.4] IETF RFC 9343 (December 2022): "IPv6 Application of the Alternate-Marking Method".

[i.5] IETF RFC 9197 (May 2022): "Data Fields for In Situ Operations, Administration, and Maintenance (IOAM)".

[i.6] IETF RFC 9326 (November 2022): "In-situ OAM Direct Exporting".

[i.7] IETF RFC 7011 (September 2013): "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information".

[i.8] IETF draft-song-opsawg-ifit-framework (work in progress): "In-situ Flow Information Telemetry".

[i.9] Bo Lu, Ling Xu, Yuezhong Song, Longfei Dai, Min Liu, Tianran Zhou, Zhenbin Li and Haoyu Song: "IFIT: Intelligent Flow Information Telemetry". In Proceedings of the ACM SIGCOMM 2019 Conference Posters and Demos (SIGCOMM Posters and Demos '19). Association for Computing Machinery, New York, NY, USA, p15-17.

[i.10] IETF RFC 8639 (September 2019): "Subscription to YANG Notifications".

[i.11] IETF RFC 8640 (September 2019): "Dynamic Subscription to YANG Events and Datastores over NETCONF".

[i.12] IETF RFC 8641 (September 2019): "Subscription to YANG Notifications for Datastore Updates".

[i.13] IETF RFC 8650 (November 2019): "Dynamic Subscription to YANG Events and Datastores over RESTCONF".

[i.14] draft-ietf-ippm-ioam-yang (work in progress): "A YANG Data Model for In-Situ OAM".

[i.15] IETF RFC 7950 (August 2016): "The YANG 1.1 Data Modeling Language".

[i.16] IETF RFC 6241 (June 2011): "Network Configuration Protocol (NETCONF)".

[i.17] IETF RFC 8040 (January 2017): "RESTCONF Protocol".

[i.18] draft-ietf-idr-sr-policy-ifit (work in progress): "BGP SR Policy Extensions to Enable IFIT".

[i.19] draft-ietf-pce-pcep-ifit (work in progress): "Path Computation Element Communication Protocol (PCEP) Extensions to Enable IFIT".

[i.20] ETSI GS ENI 005 (V2.1.1): "Experiential Networked Intelligence (ENI); System Architecture".

[i.21] draft-ietf-ippm-alt-mark-deployment (work in progress): "Alternate Marking Deployment Framework".

[i.22] draft-gfz-opsawg-ipfix-alt-mark (work in progress): "IPFIX Alternate-Marking Information".

[i.23] draft-gfz-ippm-alt-mark-yang (work in progress): "A YANG Data Model for the Alternate Marking Method".

[i.24] draft-fz-spring-srv6-alt-mark (work in progress): "Application of the Alternate Marking Method to the Segment Routing Header".

[i.25] draft-ietf-opsawg-ipfix-on-path-telemetry (work in progress): "Export of On-Path Delay in IPFIX".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

In-situ Flow Information Telemetry (IFIT): network OAM data plane on-path telemetry techniques, including Alternate Marking Method (AMM), In-situ OAM (IOAM), IOAM Direct Exporting (IOAM-DEX), and Postcard-Based Telemetry (PBT)

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AMM	Alternate Marking Method
API	Application Programming Interface
BGP	Border Gateway Protocol
BUM	Broadcast, Unknown-Unicast and Multicast
DEX	Direct Exporting
E2E	End-to-End
ECMP	Equal-Cost Multipath
ENI	Experiential Networked Intelligence
ESQM	Enhanced Stream Quality Monitoring
GTP	GPRS Tunnelling Protocol
GUI	Graphical User Interface
HD	High-Definition
IFIT	In-situ Flow Information Telemetry

IOAM	In-situ OAM
IoT	Internet of Things
IP	Internet Protocol
IPv6	IP version 6
IPFIX	IP Flow Information eXport
MDT	Model Driven Telemetry
MPLS	Multi-Protocol Label Switching
NBI	North Bound Interface
NMS	Network Management System
OAM	Operation, Administration and Maintenance
OWAMP	One-Way Active Measurement Protocol
PBT	Postcard-Based Telemetry
PCEP	Path Computation Element communication Protocol
PM	Performance Management
RAN	Radio Access network
SBI	South Bound Interface
SCTP	Stream Control Transmission Protocol
SDN	Software-Defined Network
SLA	Service Level Agreement
SR	Segment Routing
SRH	Segment Routing Header
TLV	Type Length Value
TCP	Transmission Control Protocol
TWAMP	Two-Way Active Measurement Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
YANG	Yet Another Next Generation

4 Introduction

IFIT [i.8] and [i.9] denote a family of flow-oriented on-path telemetry techniques defined in the Internet Engineering Task Force (IETF). IFIT measurement methods (i.e. AMM, IOAM) insert option headers in the real service packets, thereby directly measuring network performance indicators, such as delay, packet loss rate, and jitter. IFIT uses telemetry technology to report measurement data in real time and displays the results on a Graphical User Interface (GUI).

In contrast with traditional network OAM technologies, IFIT features high precision, real-time performance, and visualization. It can flexibly adapt to multiple service scenarios and promotes intelligent OAM by working with the big data platform and intelligent algorithms.

As introduced in ETSI GS ENI 005 [i.20], current network management and performance measurement functions are not optimized due to the different technologies and implementations from different vendors. The human-machine interaction challenges increase the time to market of innovative and advanced services (including the new performance management tools).

IFIT techniques are hybrid data-plane telemetry technologies, through which the flow quality measurement information is directly recorded and encapsulated in data packets to implement flow quality visualization at a granularity of each data packet.

Differently from active performance measurement, IFIT performance measurement directly monitors data flows without sending additional probe packets or modifying data packets. In addition, hybrid performance measurement combines active performance measurement and passive performance measurement to modify certain fields of data packets without introducing additional probe packets to the network.

Traditional network performance measurement technologies (such as OWAMP, TWAMP) cannot meet the requirements of high-precision and real-time network performance monitoring. While, the In-situ Flow Information Telemetry (IFIT) technologies provide near real time and high-precision visualization of flow quality (such as jitter, delay, packet loss).

IFIT methods, also introduced in ETSI GR ENI 012 [i.1], include:

- Alternate Marking Method (AMM), defined in IETF RFC 9341 [i.2] and IETF RFC 9342 [i.3];
- In-situ OAM (IOAM), IOAM Direct Exporting (IOAM-DEX), defined in IETF RFC 9197 [i.5] and IETF RFC 9326 [i.6].

This family of In-situ flow information telemetry technologies are currently defined by IETF.

ETSI GS ENI 005 [i.20] defines a Functional Block architecture that helps to address the application of In-situ flow information telemetry. The experiential architecture and self-learning principle are key to implement a smart, context-aware and flexible performance management.

5 IFIT Framework

5.1 IFIT-based Reactive Telemetry and ENI integration

As a hybrid performance measurement technology, the IFIT techniques provide high-precision visualization of flow quality and real-time network fault alarms (such as jitter, delay, packet loss) to meet the requirements for high-performance network quality measurement of the emerging applications. IFIT encapsulates flow quality measurement information into user data packets to implement real-time and per-packet flow quality measurement.

Figure 1 shows the IFIT-based reactive telemetry framework within the ENI System, which includes Application and Management System, Controller, and IFIT-enabled forwarding devices.

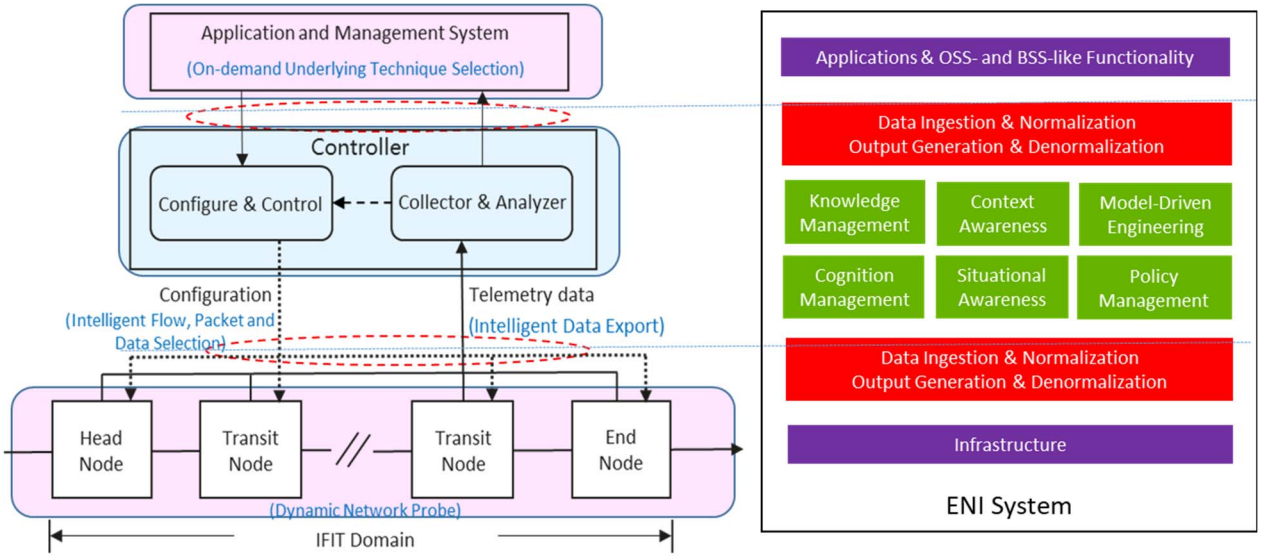

Figure 1: IFIT-based Telemetry Framework within the ENI System

As shown in ETSI GR ENI 012 [i.1], to meet the measurement requirements of different applications, multiple data-plane measurement technologies and data exporting technologies can be flexibility integrated to provide comprehensive performance information for network OAM.

ETSI GS ENI 005 [i.20] specifies in clause 6.3.1.4 and clause 6.3.1.5 that there are six functions (i.e. Knowledge Management, Context Awareness, Cognition Management, Situational Awareness, Model-Driven Engineering and Policy Management). External Reference Points (see clauses 4.4.6.1, 7.2 and 7.3 in ETSI GS ENI 005 [i.20]), and Internal Reference Points (see clauses 4.4.6.2, 7.6 and 7.7 in ETSI GS ENI 005 [i.20]) are used by ENI System to communicate with the Assisted System (or its Designated Entity) and communicate between different ENI System Functional Blocks respectively.

As shown in Figure 1, it is possible to map the functional components of IFIT-based Reactive Telemetry Framework into the ENI Functional Architecture with Domains and Control Loops. In the IFIT-based Reactive Telemetry Framework shown in Figure 1, the functional components are as follows:

a) The Application and Management System is responsible for inputting OAM measurement intent and displaying measurement analysis results. On the one hand, the intent of network quality measurement from service applications and OAM systems is received, converted into network configuration policies, and delivered to the controller. On the other hand, the application and management system receives IFIT quality measurement data and analysis results from the collector and analyser, then displays the results in a visualized manner. The IFIT network configuration policy generated by the application and management system are transmitted to the API Broker, which then communicates the data using one of the designated input External Reference Points. Each input first goes to the Data Ingestion and then to the Normalization Functional Blocks. At this point, the data is in a format that can be understood by the six Internal ENI Functional Blocks. The application and management system receives IFIT quality measurement data and analysis results from the collector and analyser, which are translated into specific formats required by the application and management system through Output Generation Functional Block, then displays the results in a visualized manner.

b) The Controller consists of two functional components: Configuration and Control, Collector and Analyser. The network configuration function module receives network configuration policies delivered by the application and management system, converts the policies into network device configuration for performance measurement, and delivers the instructions to network forwarding devices to enable the IFIT function. The collector and analyser receive and store measurement data exported from network devices, then analyse and process the data, such as fault location and performance deterioration alarm, which is realized within Knowledge Management Functional Block, Context-Aware Management Functional Block, and Model Driven Engineering Functional Block. At the same time, relevant measurement data and analysis results are reported to the application and management system. The network configuration function module receives network configuration policies delivered by the application and management system, converts the policies into network device configuration for performance measurement, and delivers the instructions to network forwarding devices to enable the IFIT function, which are realized within Cognition Management Functional Block, Situational Awareness Functional Block, and Policy Management Functional Block.

c) An IFIT-enabled forwarding devices perform in-band flow quality measurement at the granularity of data packets in the IFIT domain. Based on the roles of the IFIT function, IFIT-enabled nodes (devices) are classified into IFIT Head Node, IFIT Transit Node and IFIT End Node. An IFIT-enabled forwarding devices perform in-band flow quality measurement at the granularity of data packets in the IFIT domain. Similarly, performance measurements metrics are transmitted to the API Broker, which then communicates the data using one (or more) of the designated input External Reference Points. Each input first goes to the Data Ingestion and then to the Normalization Functional Blocks. At this point, the data is in a format that can be understood by the six Internal ENI Functional Blocks.

5.2 Closed-Loop Performance-Management

Alternate Marking Method (AMM) is a key technology for IFIT. IETF RFC 9341 [i.2] is the foundation document for the Alternate Marking and applies to point-to-point unicast flows and BUM traffic, while in general it is defined the Clustered Alternate-Marking method, that is introduced in IETF RFC 9342 [i.3] and is valid for multipoint-to-multipoint unicast flows, anycast and ECMP flows. It adds flexibility to Performance Management (PM), because it can reduce the order of magnitude of the packet counters. This allows an SDN orchestrator to supervise, control, and manage PM in large networks.

Therefore, the Alternate-Marking method can be extended to any kind of multipoint-to-multipoint paths, and the network-clustering approach is the formalization of how to implement this property and allow a flexible and optimized performance measurement support for network management in every situation.

Without network clustering, it is possible to apply Alternate Marking only for all the network or per single flow. Instead, with network clustering, it is possible to use the partition of the network into clusters at different levels in order to perform the needed degree of detail. In some circumstances, it is possible to monitor a multipoint network by analysing the network clustering, without examining in depth. In case of performance degradation, the filtering criteria could be specified more in order to perform a detailed analysis by using a different combination of clusters up to a per-flow measurement as described in IETF RFC 9341 [i.2].

This approach fits very well with the Closed-Loop Network and Software-Defined Network (SDN) paradigm, where the SDN orchestrator and the SDN controllers are the brains of the network and can manage flow control to the switches and routers and, in the same way, can calibrate the performance measurements depending on the desired accuracy. An SDN controller application can orchestrate how accurately the network performance monitoring is set up by applying the Multipoint Alternate Marking as described in the present document.

The monitoring network can be considered as a whole or split into clusters that are the smallest subnetworks (group-to-group segments), maintaining the packet-loss property for each subnetwork. The Network Clusters partition divides the Network Graph into the smallest subnetworks called Clusters. These Clusters can be combined and used at different levels to perform the needed degree of detail.

ETSI GS ENI 005 [i.20] defines an architecture where the centralized Data Collector and Network Management can apply the intelligent and flexible Alternate-Marking algorithm as previously described.

6 IFIT Measurement Domain and Nodes

The Alternate-Marking Method is an example of a solution limited to a controlled domain [i.2] and [i.3]. A controlled domain is a managed network that selects, monitors, and controls access by enforcing policies at the domain boundaries in order to discard undesired external packets entering the domain and to check internal packets leaving the domain. It does not necessarily mean that a controlled domain is a single administrative domain or a single organization. A controlled domain can correspond to a single administrative domain or multiple administrative domains under a defined network management. It should be possible to control the domain boundaries and use specific precautions to ensure authentication, encryption, and integrity protection if traffic traverses the Internet.

IETF RFC 9343 [i.4] and [i.24] describe the application of the Alternate-Marking Method to IPv6 and SRv6 and also discuss the Controlled Domain requirement.

The IFIT domain can cross multiple network domains. The nodes that enter and leave the IFIT domain are called the Head Node and End Node. The ingress node is responsible for encapsulating the IFIT instruction header into data packets. All nodes in the IFIT domain can perform the specified IFIT function. The end node is to be able to capture all packets with IFIT headers and metadata, remove the IFIT headers and IFIT metadata to ensure that any data packet with IFIT-specific headers and metadata does not leak out of the IFIT domain, and then forward them out of the IFIT field.

- The IFIT Head Node is responsible for adding an IFIT instruction header to a data packet of a specified flow object. The instruction header specifies the information to be measured in inband mode.
- IFIT Transit Node, which identifies IFIT-enabled data flow packets, parses IFIT instruction header, and collects measurement data based on the IFIT instruction. Then the data collected in the transit node is stored in data packets or directly exported to the controller as required.
- IFIT End Node identifies IFIT-enabled data flow packets, decapsulates IFIT headers, removes IFIT instruction headers, and extracts the quality measurement data carried in the data packet to the controller. Then end nodes forward the data packet.

7 Manageability

7.1 Introduction

The existing and proposed mechanisms relevant for the IFIT deployment involve the usage of the standard SDN interfaces. The South Bound Interface (SBI), which is the interface used by the Controller to configure and collect telemetry data (e.g. OAM results, statistics, states, etc.) from the network nodes. The North Bound Interface (NBI) is the interface between the Service Orchestrator and the Controllers.

The flexibility and dynamicity of the IFIT applications are given by the use of additional functions on the controller and on the network nodes, and this can be done by adding a telemetry information exchange between the network nodes and the controllers in order to enable the so-called Closed-Loop automation. The IFIT Deployment Framework is presented in [i.21].

7.2 Packet Flow Selection and Configuration

Network quality measurement such as IFIT will inevitably increase the consumption of network bandwidth, and cause an impact on forwarding performance. It is impractical to enable IFIT for all flows or packets in the network. Therefore, it is necessary to select some specific service flows, packets or data according to service or operation and maintenance requirements.

IFIT can implement intelligent flow, packet and data selection and monitoring strategies to meet measurement requirements. In addition, IFIT can dynamically adjust selection and collection strategies in real time based on network load, forwarding processing capabilities, and other criteria.

The YANG module defines a data model for IOAM and Alternate-Marking capabilities using the YANG data modelling language, described in IETF RFC 7950 [i.15]. It is designed to be used by the network management protocols such as NETCONF [i.16] or RESTCONF [i.17] in order to configure the network nodes. It supports Alternate Marking and all the five IOAM options, which are Incremental Tracing Option, Pre-allocated Tracing Option, Direct Export Option, Proof of Transit Option, and Edge-to-Edge Option. IOAM and Alternate Marking YANG data models are described in [i.14] and [i.23].

NETCONF, as showed in Figure 2, gives access to the native capabilities of a device within a network, defines methods to manipulate its configuration database, retrieves operational data, and invokes specific operations. YANG provides the means to define the content carried through NETCONF, for both data and operations.

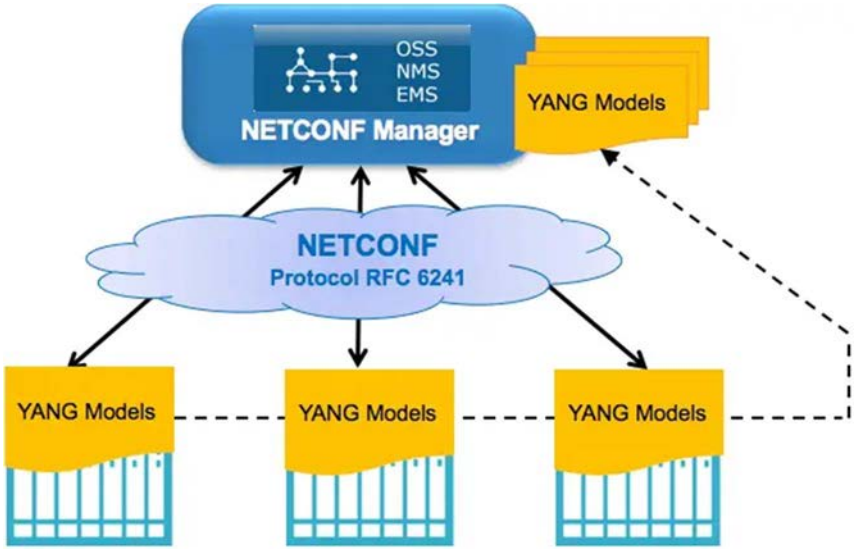

Figure 2: NETCONF and YANG

In addition to YANG models, other protocols can also be used for the communication between the control layer and the network nodes: Path Computation Element communication Protocol (PCEP) and Border Gateway Protocol (BGP).

The definition of the IFIT data plane methods for SR-MPLS and SRv6 imply requirements for various routing protocols, such as BGP and PCEP. [i.18] aims to define BGP extensions to distribute SR policies carrying IFIT information and this allows to signal the IFIT capabilities in order to automatically configure and run IFIT methods when the SR Policy candidate paths are distributed through BGP. Similarly, the PCEP extension defined in [i.19] allows to signal the IFIT capabilities and apply the IFIT attributes for all path types, as long as they support the relevant data plane telemetry method. In this way IFIT methods are automatically activated and running when the path is instantiated.

7.3 Data Export, Collection and Calculation

IFIT can measure and export flow or packet quality information in real time. But there is a lot of redundancy in the collected information, and the high-density service flow quality measurement information uploading will consume a lot of bandwidth and may cause congestion of the exporting channel. Therefore, in order to reduce the transmission bandwidth and reduce the processing burden of the controller, it is necessary to perform de-redundancy and compression processing of the exported data.

In addition, IFIT can also use the general IP data export technology (i.e. IPFIX) to realize the export of measurement data. IPFIX [i.7] is a template format-based information export protocol based on data feature analysis. It can obtain different data formats based on different collection requirements with strong scalability. IPFIX extensions for Alternate Marking are described in [i.22].

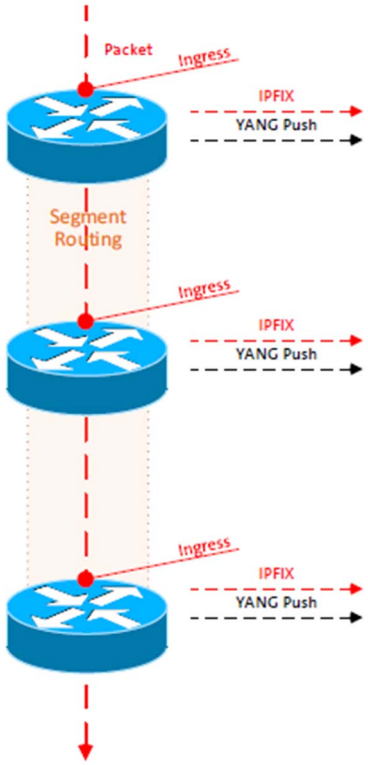

Figure 3: Example of Export of On-Path Delay with IPFIX and YANG Push

[i.25] introduces new IP Flow Information Export (IPFIX) information elements to expose the On-Path Telemetry measured delay. [i.24] defines how the timestamp can be encoded in the encapsulation node and be read at the intermediate and decapsulation node to calculate the on-path delay by using the SRH TLV. Figure 3 describes how the On-Path Delay measured can be exposed on each node of the path.

In this regard it is possible to mention the Model Driven Telemetry (MDT) that enables the Closed Loop Automation. MDT is an approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics. The configuration is done with Data Models and Telemetry is also done with Data Models. Model Driven Telemetry is also known as YANG Push and defined in IETF RFC 8639 [i.10], IETF RFC 8640 [i.11], IETF RFC 8641 [i.12] and IETF RFC 8650 [i.13]. Applications can subscribe to specific data items they need, by using standard-based YANG data models over NETCONF YANG.

IOAM and Alternate Marking can surely leverage YANG Push to achieve flexible telemetry.

An automatic network requires the Service Level Agreement (SLA) monitoring on the deployed service. So that the system can quickly detect the SLA violation or the performance degradation, hence, to change the service deployment. In this regard, [i.18] and [i.19] define extensions to BGP and PCEP respectively in order to distribute IFIT information. So that IFIT behaviour can be enabled automatically when the path is instantiated.

In summary, by combining the use of YANG Push, PCEP and BGP it is possible to obtain the reactive and adaptive telemetry for IFIT methodologies.

8 Examples of Application

8.1 IP RAN Mobile Bearer Network

The IP RAN mobile bearer network is a large-scale network that has various access modes and carries various mobile bearer services (such as HD video) that pose higher requirements on link connectivity and performance indicators. For this, the E2E ESQM + trace IFIT hybrid measurement solution is proposed. ESQM is a measurement technology that collects statistics on TCP, SCTP, or GTP packets based on 5-tuple information. In this solution, E2E ESQM is performed first. Hop-by-hop IFIT is triggered when the performance indicator of a base station flow exceeds the specified threshold. The Controller then summarizes the reported hop-by-hop measurement data for path restoration and fault locating.

This solution monitors detailed indicator data of service flows from different dimensions, such as base station flows, data flows, and signalling flows. Based on the real-time performance data of base stations across the entire network, a big data-based intelligent OAM system can be constructed to implement high-precision and service-level SLA awareness in real time and multi-dimensional visualization for base station services. The system can also analyse and evaluate potential network risks, as well as adjust and optimize network resources to implement automatic and intelligent OAM.

8.2 Intelligent Cloud-Network Private Line Service

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 bearer network to provide enterprise private line services more conveniently and improves the network deployment, operations, and OAM 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 site-to-cloud private line as an example to describe the E2E IFIT + trace IFIT solution, in which E2E IFIT is performed first. Hop-by-hop IFIT is triggered when the performance indicator of a VPN flow exceeds the specified threshold. The Controller then summarizes the reported hop-by-hop measurement data for path restoration and fault locating.

This solution supports the query of VPN service flow performance indicators by granularity ranging from minute to year and the query of overall VPN service information based on the VPN name, VPN type, and service status. In this way, the solution implements E2E multi-dimensional exception identification, network health visualization, intelligent fault diagnosis, and fault self-healing in a closed-loop manner.

8.3 One Financial WAN

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. The financial industry itself has high requirements on SLA assurance, and one financial WAN faces higher requirements on OAM capabilities due to the diverse array of outlet 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. Against this backdrop, the IFIT tunnel-level measurement solution is proposed.

This solution supports IFIT tunnel-level measurement in SRv6 scenarios. The link currently in use is periodically compared with the optimal link for path selection and optimization, implementing intelligent traffic steering. In addition, one core controller is deployed to perform centralized OAM on the entire financial network and implement E2E management and scheduling.

9 Conclusions and Recommendations

The present document describes the IFIT deployment framework for improving traditional network OAM methods and meets users' requirements for E2E high-quality network experience in data-driven intelligent networks.

Furthermore, a synergy between IETF, that is responsible for the definition of IFIT related methodologies, and ETSI, that is working towards achieving an ENI architecture, is also expected.

Annex A:
Change history

Date	Version	Information about changes
2023-05	V0.0.1	Initial early draft with skeleton
2024-03	V0.0.6	Stable draft
2024-04	V0.0.7	Final version

History

Document history		
V4.1.1	May 2024	Publication