ETSI GR ENI 012 V1.1.1 (2022-03)

Experiential Networked Intelligence (ENI); Reactive In-situ Flow Information Telemetry

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-0022_Flow_Info_Tele

Keywords

artificial intelligence, network, 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 present document describes the motivation, issues, and challenges of using flow-oriented on-path telemetry techniques which provide relevant measurement or event reports to the AI-enabled network entities.

The present document outlines a reference framework, named as "In-situ Flow Information Telemetry (IFIT)" and identifies technical issues, including modes of flow-oriented on-path telemetry; IFIT-based reactive telemetry framework and technical issues, including intelligent flow and packet selection, intelligent data export, dynamic network probe, on-demand underlying technique selection.

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] IETF RFC 7276 (June 2014): "An Overview of Operations, Administration, and Maintenance (OAM) Tools".

[i.2] IETF RFC 4443 (March 2006): "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification".

[i.3] IETF RFC 5880 (June 2010): "Bidirectional Forwarding Detection (BFD)".

[i.4] IETF RFC 7799 (May 2016): "Active and Passive Metrics and Methods (with Hybrid Types In-Between)".

[i.5] IETF RFC 4656 (September 2006): "A One-way Active Measurement Protocol (OWAMP)".

[i.6] IETF RFC 5357 (October 2008): "A Two-Way Active Measurement Protocol (TWAMP)".

[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 RFC 8321 (January 2018): "Alternate-Marking Method for Passive and Hybrid Performance Monitoring".

[i.9] draft-ietf-ippm-ioam-data (June 2021): "Data Fields for In-situ OAM".

[i.10] IETF draft-ietf-ippm-ioam-direct-export (August 2021): "In-situ OAM Direct Exporting".

[i.11] IETF RFC 8889 (August 2020): "Multipoint Alternate-Marking Method for Passive and Hybrid Performance Monitoring".

[i.12] IETF draft-song-opsawg-ifit-framework (work in progress): "In-situ Flow Information Telemetry".

[i.13] 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.

NOTE: Available at https://doi.org/10.1145/3342280.3342292.

[i.14] ETSI GR ENI 009 (V1.1.1): "Experiential Networked Intelligence (ENI); Definition of Data Processing Mechanisms".

[i.15] IETF RFC 8639 (September 2019): "Subscription to YANG Notifications".

[i.16] IETF RFC 8640 (September 2019): "Dynamic Subscription to YANG Events and Datastores over NETCONF".

[i.17] IETF RFC 8641 (September 2019): "Subscription to YANG Notifications for Datastore Updates".

[i.18] IETF RFC 8650 (November 2019): "Dynamic Subscription to YANG Events and Datastores over RESTCONF".

[i.19] draft-ietf-ippm-ioam-yang (work in progress): "A YANG Data Model for In-Situ OAM".

[i.20] IETF RFC 7950 (August 2016): "The YANG 1.1 Data Modeling Language".

[i.21] IETF RFC 6241 (June 2011): "Network Configuration Protocol (NETCONF)".

[i.22] IETF RFC 8040 (January 2017): "RESTCONF Protocol".

[i.23] draft-ietf-idr-sr-policy-ifit: "BGP SR Policy Extensions to Enable IFIT".

[i.24] draft-chen-pce-pcep-ifit (work in progress): "Path Computation Element Communication Protocol (PCEP) Extensions to Enable IFIT".

[i.25] ETSI GS ENI 005 (V2.1.1): "Experiential Networked Intelligence (ENI); System Architecture".

[i.26] IETF RFC 5475 (March 2009): "Sampling and Filtering Techniques for IP Packet Selection".

[i.27] Shuping Peng, Jianwei Mao, Ruizhao Hu and Zhenbin Li: "Demo Abstract: APN6: Application-aware IPv6 Networking", IEEE INFOCOM 2020.

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

flow-oriented on-path telemetry: specific class of network forwarding-plane telemetry techniques, including In-situ OAM (IOAM), Enhanced Alternate Marking (EAM), Postcard-Based Telemetry (PBT), and Hybrid Two Steps (HTS)

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

NOTE 1: It can provide flow information on the entire forwarding path on a per-packet basis in real time. "In-situ" is Latin which can be translated as "in the original place".

NOTE 2: See IETF RFC 8321 [i.8].

reactive telemetry: telemetry operation in a dynamic and interactive fashion

3.2 Symbols

Void.

3.3 Abbreviations

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

ACL	Access Control List
AMF	Access and Mobility Management Function
AMM	Enhanced Alternate Marking Method
API	Application Programming Interface
APN	APplication-aware Network
ASG	Aggregation Site Gateway
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BUM	Broadcast, Unknown-Unicast and Multicast
DEX	Direct Exporting
DNP	Dynamic Network Probes
E2E	End-to-End
EAM	Enhanced Alternate Marking
ECMP	Equal-Cost Multipath
ENI	Experiential Networked Intelligence
GPB	Google Protocol Buffer
GPRS	General Packet Radio Service
GTP	GPRS Tunnelling Protocol
HD	High-Definition
HTS	Hybrid Two Steps
IFIT	In-situ Flow Information Telemetry
IOAM	In-situ OAM
IP	Internet Protocol
IPFIX	IP Flow Information eXport
IPFPM	IP Flow Performance Measurement
IPPM	IP Performance Measurement
MDT	Model Driven Telemetry
NBI	North Bound Interface
NMS	Network Management System
NP	Network Processor
OAM	Operation, Administration and Maintenance
OTT	Over The Top
OWAMP	One-Way Active Measurement Protocol
PBT	Postcard-Based Telemetry
PCEP	Path Computation Element communication Protocol
PM	Performance Management
RSG	Radio Service Gateway
SBI	South Bound Interface
SCTP	Stream Control Transmission Protocol
SDN	Software-Defined Network
SD-WAN	Software-defined WAN
SLA	Service Level Agreement
SR	Segment Routing
TM	Traffic Manager
TWAMP	Two-Way Active Measurement Protocol
UPF	User Plane Function
VPN	Virtual Private Network
WAN	Wide Area Network
WG	Working Group
YANG	Yet Another Next Generation

4 Introduction

4.1 Background, Motivation and Benificial Aspests

4.1.1 Background

This clause presents background and deployment challenges of flow-oriented on-path telemetry, as well as the components of a reference framework.

As introduced in ETSI GS ENI 005 [i.25], 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).

In-situ Flow Information Telemetry (IFIT) is a family of 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. This flow quality measurement information that may be carried on a complete forwarding path in real time at a per-packet granularity may include device and interface information as well as a nanosecond-precision cache time of a packet in each network device as well as identification contention queue flow information. In-situ flow information telemetry technologies include e.g. In-situ OAM (IOAM) [i.9], IOAM Direct Exporting (IOAM-DEX) [i.10], and Alternate Marking Method (AMM) [i.8]. This family of In-situ flow information telemetry technologies are currently defined by IETF.

4.1.2 Motivation

Currently there is no efficient and extensible standard-based mechanism to provide smart, context-aware and flexible performance management. In addition, Performance Measurement tools should adapt to variations in network conditions, changes in user needs and business goals. All this will be possible by using In-situ flow information telemetry techniques. Moreover, this approach further enables the use of real-time closed control loops and also helps to optimize network resources through the use of automation and smart application of network monitoring. Network intelligence allows to start without examining in depth and, if there are problems in some network portions these are detected. Then, it can be possible to determine which parts of the network are affected and start an in-depth analysis only where and when is necessary. The resulting telemetry information can be used to understand what is going on and to eventually try to solve it in order to maintain Service Level Agreements (SLAs).

ETSI GS ENI 005 [i.25] 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.

4.1.3 Benificial Aspests

Efficient network OAM increasingly depends on high-quality visualization of network data plane quality. Traditional OAM technologies are widely used, including network fault detection, network fault isolation, network fault reporting, and network performance measurement, IETF RFC 7276 [i.1]. For example, traditional IP Ping, IETF RFC 4443 [i.2] and Bidirectional Forwarding Detection (BFD), IETF RFC 5880 [i.3] are used for connectivity detection. According to IETF RFC 7799 [i.4], performance measurement can be classified into three types, aka active performance measurement, passive performance measurement, and hybrid performance measurement. For example, Two-Way Active Measurement Protocol (TWAMP), IETF RFC 5357 [i.6], is a typical active performance measurement method that operates by injecting proactive probe packets to measure the loss and delay.

Different from active performance measurement, passive performance measurement directly monitors data flows without sending additional probe packets or modifying data packets. For example, the IP Flow Information eXport (IPFIX) protocol [i.7] may transmit IP data flow statistics from a device to a collector by using a pre-defined data output format. 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. For example, IP Flow Performance Measurement (IPFPM) [i.8] directly monitors real data flows by colouring data packets, which is a typical hybrid performance measurement technology. Because the hybrid performance measurement method does not introduce additional probe packets, the accuracy of the performance measurement can be equal to that of the passive measurement.

Traditional network performance measurement technologies (such as TWAMP [i.6] and IPFIX [i.7]) cannot meet the requirements of high-precision and real-time network performance monitoring. A new measurement technology is required to meet the requirements of future network and service development. In addition, intelligence has become the developing trend of network. The new APplication-aware Network (APN) [i.27] architecture describes the ability of the network to acquire and manage current information about users and applications. This information can be used to optimize the use of network resources and improve the quality of service. In addition, the emerging In-situ Flow Information Telemetry (IFIT) technologies provide high-precision visualization of flow quality (such as jitter, delay, packet loss).

Although In-situ flow information telemetry is beneficial, it is to be addressed in the following practical deployment challenges. First, In-situ flow information telemetry incurs extra packet processing which may cause stress on the network data plane. The potential impact on the forwarding performance creates an unfavourable "observer effect". For example, the growing IOAM data per hop can negatively affect service levels by increasing the serialization delay and header parsing delay. Second, In-situ flow information telemetry can generate a considerable amount of data which may consume too much transport bandwidth and the servers used for data collection, storage, and analysis, may collapse. For example, if IOAM is applied to all the traffic, one node may collect a few tens of bytes as telemetry data per packet. Third, as the network operation evolves to be fully automated, and the trends of network virtualization and packet-optical integration continue, more data is needed in an on-demand and interactive fashion. Flexibility and extensibility on data defining, aggregation, acquisition, and filtering, is to be considered. Lastly, as applying only a single underlying in-situ flow information telemetry technique may lead to a defective result, for example, packet drop can cause the loss of the flow telemetry data. Therefore, the reason why the packet drop has occurred remains unknown if only the IOAM trace option [i.9] is used. As such, a comprehensive solution needs the flexibility to switch between different underlying techniques and adjust the configurations and parameters at runtime. Hence, system-level management is needed.

The present document provides an IFIT-based reactive Telemetry framework, which addresses the aforementioned handicaps for deployment. By following this framework, an effectively and implementable automatic data flow quality measurement scheme for data flow becomes possible. IFIT-based reactive Telemetry framework requires intelligent flow selection, efficient data handling, dynamic network probe, and tunnel encapsulation to enable on-demand network performance measurement.

4.2 Modes of Flow-oriented On-path Telemetry

This clause lists various telemetry techniques in the category of flow-oriented on-path telemetry, such as In-situ OAM (IOAM) [i.9], IOAM Direct Exporting (IOAM-DEX) [i.10], Alternate Marking Method (AMM) [i.8], and classifies various modes of flow-oriented on-path telemetry in accordance to IETF RFC 7799 [i.4].

Traditional OAM technologies are widely used in network OAM and management, including network fault detection, network fault isolation, network fault reporting, and network performance detection. According to IETF RFC 7799 [i.4], performance measurement can be classified into three types: active performance measurement, passive performance measurement, and hybrid performance measurement.

In proactive performance measurement, probe packets are sent on the network, and the network performance is deduced by measuring the probe packets. Active performance measurement methods, such as IP Ping [i.2], Bidirectional Forwarding Detection (BFD) [i.3], One-Way Active Measurement Protocol (OWAMP) [i.5], and Two-Way Active Measurement Protocol (TWAMP) [i.6].

Different from active performance measurement, passive performance measurement obtains performance parameters by directly monitoring service data flows. No additional detection packets are sent or service packets need to be modified. Therefore, the performance can be accurately and accurately reflected. Passive performance measurement methods, such asIP Flow Information Export (IPFIX) [i.7], which is a statistical and output standard for IP data flows. IP data flow statistics can be transmitted from one output to the collector through a defined data output format.

Hybrid performance measurement is a combination of active performance measurement and passive performance measurement. It does not need to send additional probe packets on the network. Instead, it only needs to modify some fields of service packets to measure network performance. Because the hybrid performance measurement method does not introduce additional active measurement packets, the accuracy of the performance measurement can be equal to that of the passive measurement, hybrid performance measurement methods, such as IOAM [i.9], IOAM-DEX [i.10], Alternate Marking [i.8], which directly monitors real data flows by inserting instruction header or colouring data packets.

5 Overview of IFIT

5.1 IFIT-based Reactive Telemetry Framework

As a hybrid performance measurement technology, the IFIT technology provides 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 in the future. IFIT encapsulates flow quality measurement information into user data packets to implement real-time and per-packet flow quality measurement.

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

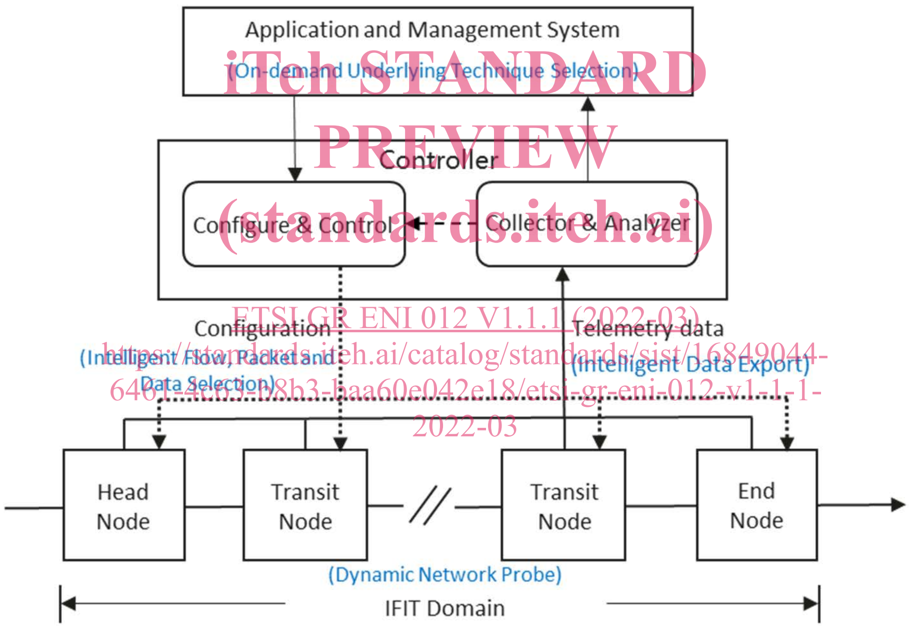

Figure 1: IFIT-based Reactive Telemetry Framework

As shown in the IFIT-based reactive telemetry framework, 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. For example, for different types of information data, IOAM or Alternate Marking may be selected to collect information. In addition, switching from the IOAM mode [i.9] to the IOAM-DEX mode [i.10] for fault location. After the telemetry data is processed and analysed, the analysing results may be used to instruct the controller to modify a configuration of a node in the IFIT domain for adjusting data collected by the IFIT. Therefore, the process may be dynamic and interactive.

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.

In the IFIT-based Reactive Telemetry Framework shown in Figure 1, each 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. The IFIT network configuration policy generated by the application and management system, which includes information such as a specified flow object to be measured, a performance indicator to be collected, and a test data exporting mode (passport mode or postcard mode). 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.

b) The Controller consists of two functional components: Configuration and Control, Collector and Analyzer. 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 receives and stores measurement data exported from network devices, then analyses and processes the data, such as fault location and performance deterioration alarm. At the same time, relevant measurement data and analysis results are reported to the application and management system.

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 the following roles:

- 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.

d) 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.

5.2 Closed-Loop Performance-Management Approach

This clause discusses relevant mechanisms to apply the Closed-Loop approach of the Reactive In-situ Flow Information Telemetry. In particular it is reported how this approach has been introduced in some relevant documents in IETF IPPM WG (e.g. IETF RFC 8321 [i.8] and IETF RFC 8889 [i.11]) to enable flexible and adaptive performance measurement.

IETF RFC 8321 [i.8] applies to point-to-point unicast flows and BUM traffic, while in general it is defined the Clustered Alternate-Marking method that is valid for multipoint-to-multipoint unicast flows, anycast and ECMP flows.

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 8321 [i.8].

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.