MPLS SD&AI NET WORLD22

Reactive In-situ Flow Information Telemetry for IPv6 and SRv6

Giuseppe Fioccola
Standardization Specialist at Huawei Technologies
giuseppe.fioccola@huawei.com

MPLS SD&AI NET WORLD22
5/6/7 APRIL

HUAWEI

IFIT Introduction

In-situ flow information telemetry (**IFIT**) is a family of passive and hybrid data-plane telemetry technologies defined by IETF.

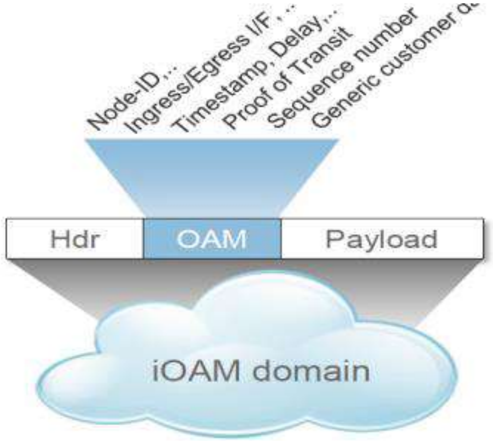
- It includes **In-situ OAM** (**IOAM**) and **Alternate Marking Method** (**AltMark**).
  - These on-path telemetry techniques enable performance measurements on live traffic
- Packet loss, delay and delay variation metrics can be measured in **real time**, at **flow level** and with a **per-packet granularity**.
  - IOAM and AltMark provide high accuracy that is not possible to achieve through measurements done by injecting synthetic traffic.
- Performance Measurements should also **adapt to variations in network conditions**, changes in user needs and business goals.
  - The use of a **closed control loop** helps to optimize network resources through automation and smart application of network monitoring.
  - **Network intelligence** allows to start without examining in depth and, in case of problems in a network portion it can be possible to start an in-depth analysis where and when is necessary.

IFIT Tool: In-situ OAM

IOAM (**draft-ietf-ippm-ioam-data**) records operational and telemetry information in the packet while the packet traverses a path in the network.

In-situ OAM data fields can be encapsulated into a variety of protocols.

- An "IOAM encapsulating node" incorporates one or more IOAM-Option-Types into IOAM enabled packets.
- An "IOAM transit node" reads and/or writes and/or processes one or more of the IOAM-Data-Fields.
- An "IOAM decapsulating node" removes IOAM-Option-Type(s) from packets.

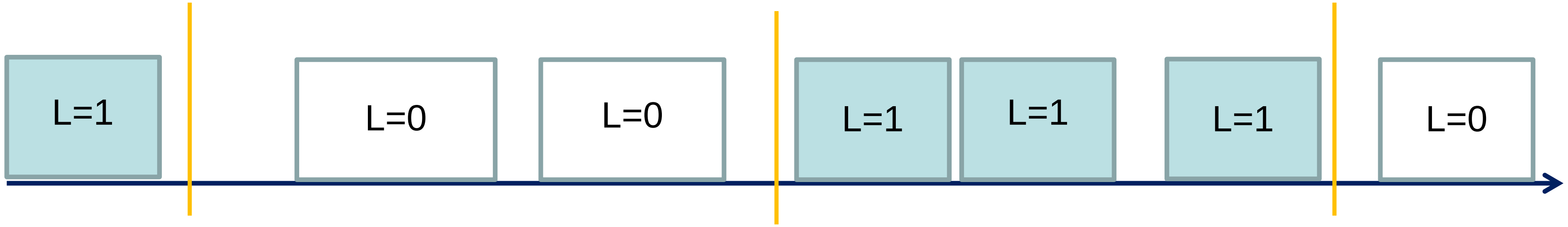


IOAM processes data in Passport mode (since each node records the collected data in packets), it may impact the forwarding plane efficiency of devices and the amount of data to be collected.
IOAM-DEX (IOAM Direct Exporting) can also work in Postcard mode (since each node sends the collected data to the collector)

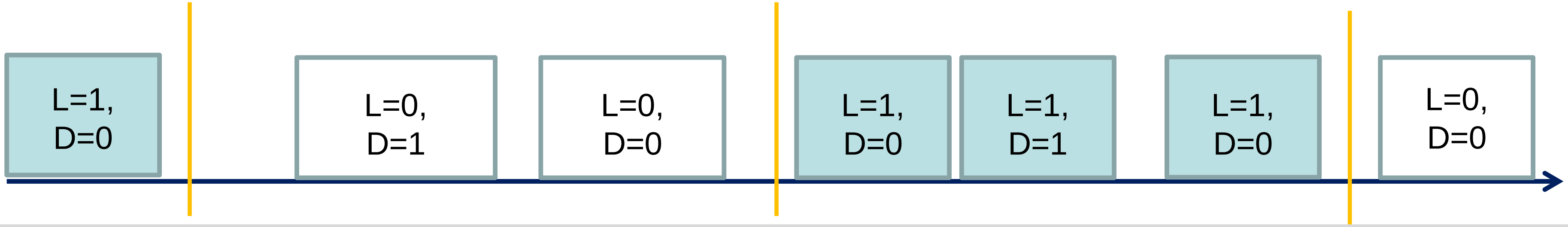
IFIT Tool: Alternate-Marking

Alternate Marking methodology enables Packet Loss, Delay and Delay Variation measurements. The reference document is **RFC 8321**

- Batching packets based on time interval to measure Packet Loss by switching value of L flag.
- First/Last Packet Delay calculation and Average Packet Delay and Delay Variation calculations are possible



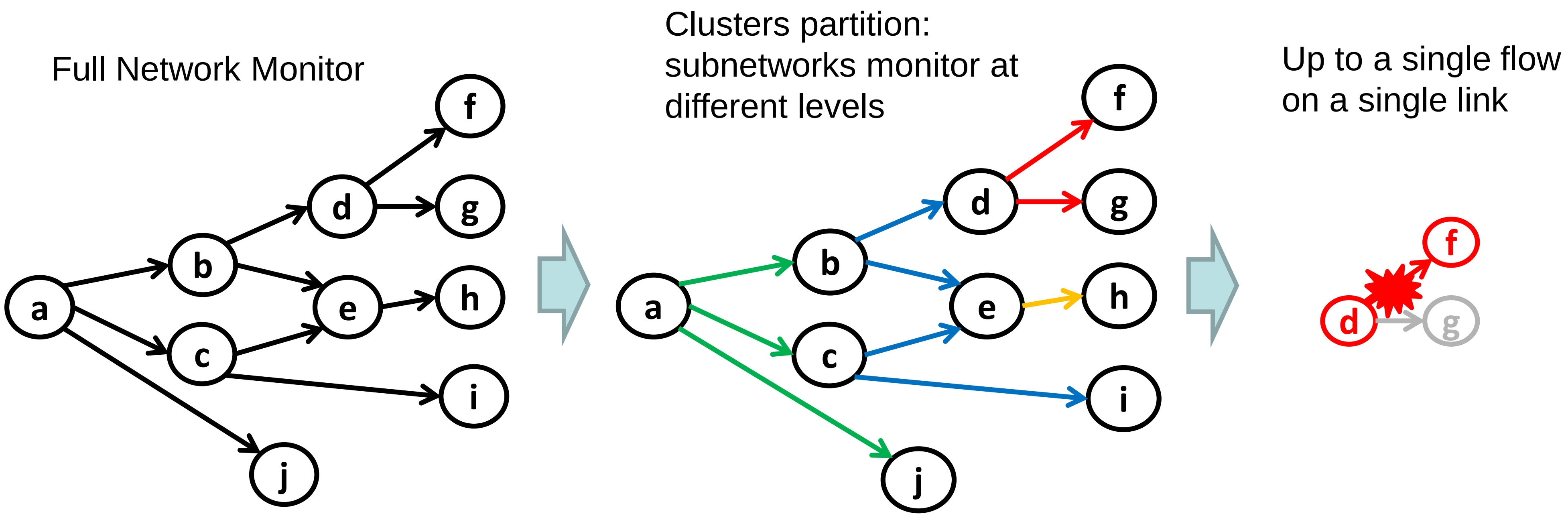
- Use D flag to create a new set of marked packets fully identified over the network. D-marked packets to calculate more informative Packet Delay Metrics



AltMark is a straightforward method but it requires marking fields and works mainly in Postcard mode to collect and correlate data

IFIT Tool: Multipoint Alternate-Marking

Multipoint Alternate Marking methodology generalizes the application of RFC 8321 for multipoint unicast flows. The reference document is **RFC 8889**



Full Network Monitor

Clusters partition: subnetworks monitor at different levels

Up to a single flow on a single link

- Packet Loss can be measured on multipoint path basis (on Cluster basis) or considering the borderline cases of single flows and whole network.
- Delay measurements can be done on multipoint path basis or on single packet basis

Multipoint AltMark enables a closed control loop performance management and a network intelligence approach

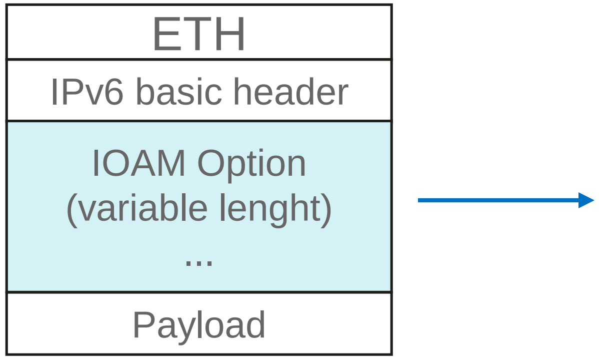
IFIT Tools: AltMark and/or IOAM

IOAM or AltMark can be used together or alternatively according to the specific needs:

IOAM	AltMark
IOAM is a very detailed packet level monitoring with more overhead (i.e. data specified by the IOAM-Trace-Type)	AltMark is a flexible flow monitoring solution and can be encapsulated with less overhead
IOAM is less resilient to losses since it works in Passport mode and if a packet is lost, therefore all the data are lost.	AltMark is more resilient, indeed it can detect where the packet is lost because it works only in Postcard mode
IOAM data are carried within the packet. With IOAM-DEX, data can eventually be exported by each node.	AltMark data require an NMS to correlate counters and timestamps
IOAM architecture is more static and cannot be adapted to the network conditions	AltMark includes a dynamic approach and can be adapted to the network conditions (i.e. Multipoint AltMark)

IFIT for IPv6
How IOAM and AltMark Data Fields are carried in IPv6

- For the IPv6 data plane the IOAM Metadata can be encapsulated as Hop-by-Hop Options Header (HBH) or Destination Options Header (DOH). See draft-ietf-ippm-ioam-ipv6-options



ETH

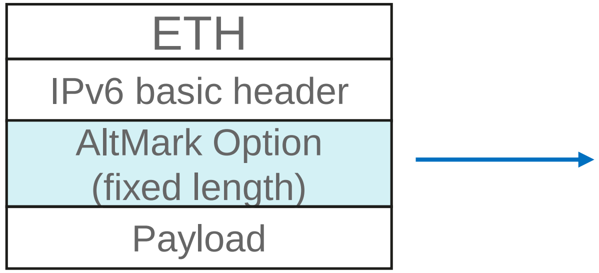
IPv6 basic header

IOAM Option
(variable lenght)
…

Payload

- ➢ Pre-allocated Trace Option represented as HBH
- ➢ Incremental Trace Option represented as HBH
- ➢ Proof of Transit Option represented as DOH
- ➢ Edge to Edge Option represented as HBH
- ➢ Direct Export (DEX) Option represented as DOH

- For the IPv6 data plane the AltMark data can be encapsulated as Hop-by-Hop Options Header (HBH) or Destination Options Header (DOH). See draft-ietf-6man-ipv6-alt-mark.



ETH

IPv6 basic header

AltMark Option
(fixed length)

Payload

- ➢ A 48-bit Option including few fields:
  - ▪ The Flow Monitoring Identification (**FlowMonID**):
  - ▪ **L** and **D** are the Marking Fields
- ▪ It can be both HBH and DOH. Nodes can skip if they do not recognize and data do not change en route

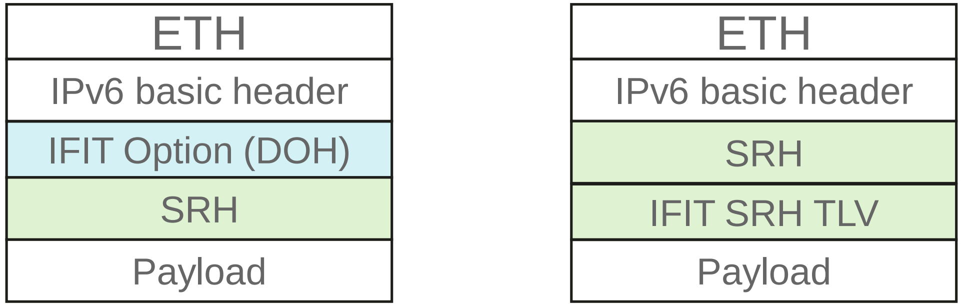
IFIT for SRv6: IOAM and AltMark carried in SRv6

For **IPv6**, IOAM and AltMark can be carried through HBH and DOH.

For **SRv6**, there are two possibilities: DOH + SRH and SRH TLV.
See draft-fz-spring-srv6-alt-mark and draft-ali-spring-ioam-srv6

1. Because SRH is a routing header (RH), DOHs before the RH are processed by each destination in the route list. Therefore, it is possible to apply both IOAM and AltMark by using **DOH + SRH**

2. IOAM and AltMark data could also be carried as **SRH TLV** and be can be piggybacked in the packet and transported as part of the SRH



ETH
IPv6 basic header
IFIT Option (DOH)
SRH
Payload

ETH
IPv6 basic header
SRH
IFIT SRH TLV
Payload

The approach with **DOH + SRH** requires two extension headers and this may have operational implications in comparison with the use of **SRH TLV**

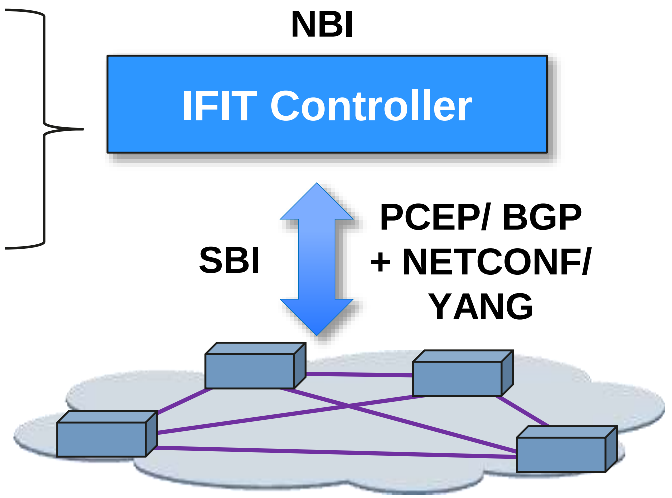
IFIT Management and Control mechanisms

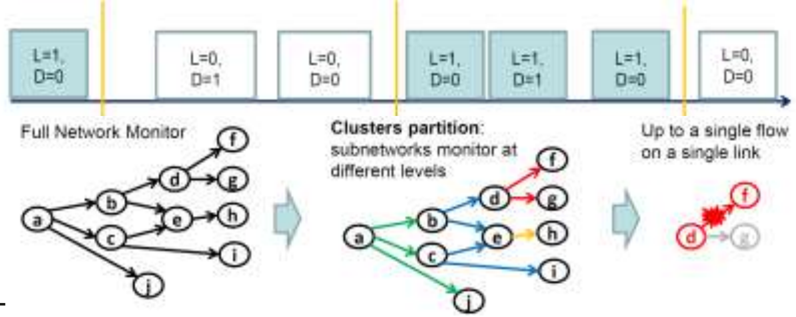
PCEP and BGP extensions can be used to enable automatically IFIT when the path is established.
See draft-ietf-idr-sr-policy-ifit and draft-chen-pce-pcep-ifit

These extensions to PCEP and BGP complements the **SR Policy Architecture**:

- A headend can be informed about the multiple candidate paths for an SR Policy via BGP or PCEP
- IFIT attributes can be included at the candidate path level by using BGP or PCEP
- The best candidate path for an SR Policy is selected and installed in the forwarding plane
- IFIT tools can therefore be activated

Controller-Network interaction:
1. Configuration (Intelligent Flow, Packet and Data selection)
2. Telemetry Data (Intelligent Data Export)
3. Dynamic and Flexible network monitoring




L=1, D=0
L=0, D=1
L=0, D=0
L=1, D=0
L=1, D=1
L=1, D=0
L=0, D=0
Full Network Monitor
Clusters partition: subnetworks monitor at different levels
Up to a single flow on a single link
a
b
c
d
e
f
g
h
i
j

IFIT Controller enables an Intelligent Performance Measurement with Closed Loop Automation

IFIT Deployment Use Cases

With the rapid development of 5G and Cloud era, higher requirements on network quality imply:

- effective user traffic monitoring and real-time metrics
- reactive and flexible approach

Therefore, IFIT has been successfully applied in several scenarios which include:

- ✓ Mobile transport network
- ✓ Enterprise private line services
- ✓ Enterprise WAN
- ✓ 5G services
- ✓ Cloud services

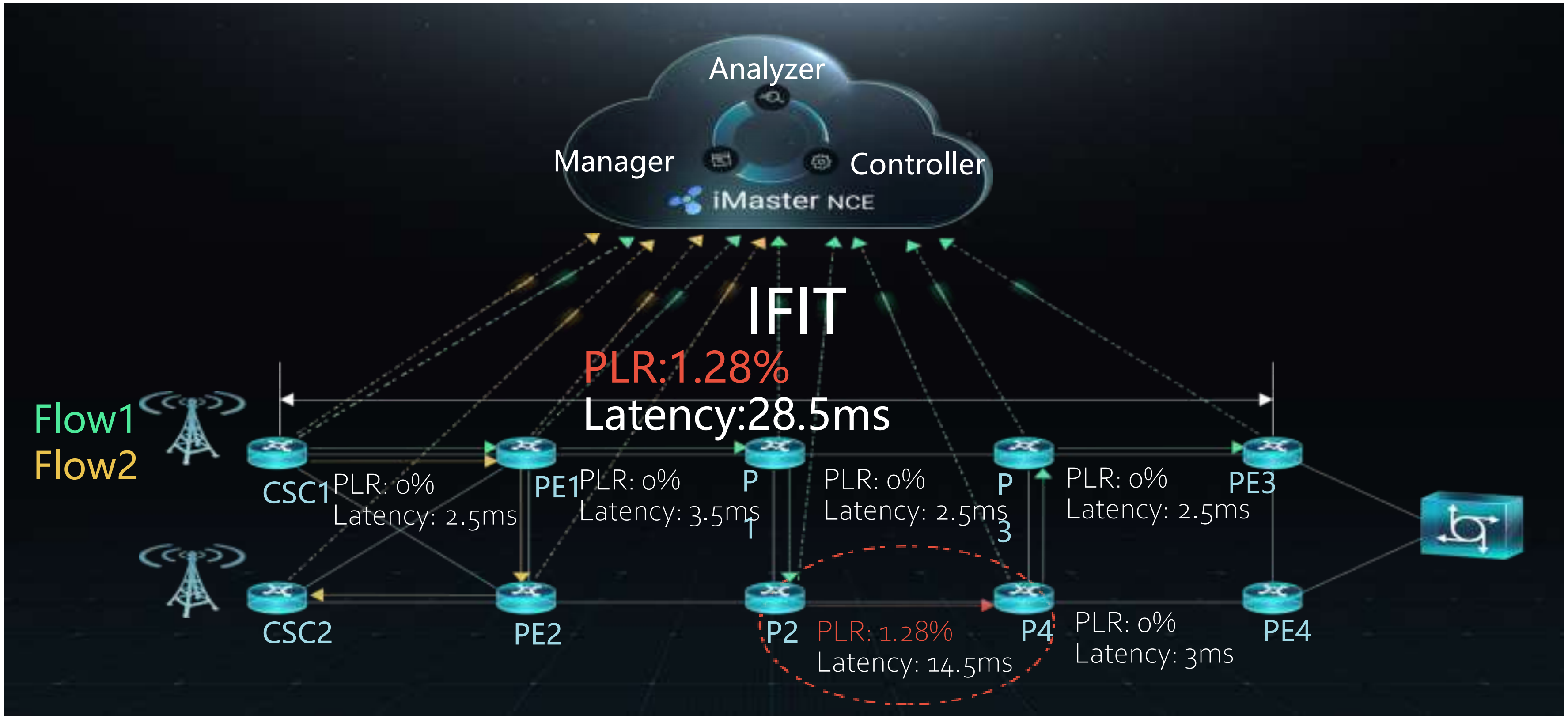
There has been **10+** commercial deployment of IFIT.

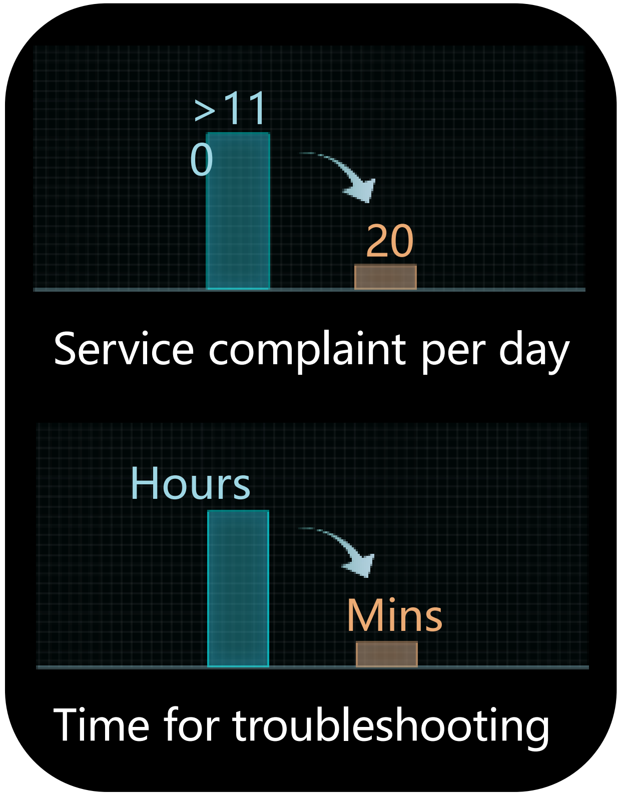
Till the end of 2022, the deployment will increase to **25+**.

An IFIT Deployment Scenario: China Unicom

IFIT deployment for IP RAN Mobile Transport Network:

- Detailed service flows performance parameters and data monitoring
- If a fault occurs IFIT can demarcates and locates faults
- Intelligent O&M system can improve SLA experience and O&M efficiency in real time. It can also evaluate potential network risks and optimize network resources.





Summary

IFIT is a **key technology** for ensuring the SLA of **future network services** and for implementing automated and intelligent IP networks.

- IFIT tools analyze **real-time performance measurement** data of the entire network
- IFIT tools can be **activated dynamically** and where/when needed to save network resources
- IFIT controller changes the traditional network OAM mode driven by faults to a **proactive and predictive** one.
- IFIT controller **intervenes, adjusts and optimizes** network behavior in advance

IFIT offers many benefits over other measurement technologies.

Several technical specifications in IETF have already been defined to set the basis of the whole framework.

MPLS SD&AI NET WORLD22

Thank you