ICS 33.040.40
CCS L 78

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 44887.11-2024

IPv6 evolution technical requirements-Part 11: IPv6 in-situ flow information telemetry

IPv6演进技术要求 第11部分：IPv6随流检测技术

Issued on: November 28, 2024 **Implemented on: March 1, 2025**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

1 Scope

This document specifies the technical requirements for IPv6 in-situ flow information telemetry, and describes the architecture of in-situ flow information telemetry, its key technologies, and the data encapsulation formats and methods.

This document applies to the measurement of data-plane in-situ flow information in multi-service bearer scenarios, and is used for the development, testing and deployment of the in-situ flow information telemetry function of IP network devices.

2 Normative references

The contents of the following documents constitute indispensable provisions of this document through normative reference in the text. For dated references, only the version corresponding to that date applies to this document; for undated references, the latest version (including all amendments) applies to this document.

IETF RFC 8200 Internet protocol, version 6 (IPv6) specification; IETF RFC 9341 Alternate-marking method.

3 Terms and definitions

The following terms and definitions apply to this document.

3.1 in-situ flow information telemetry: a telemetry technique that marks the characteristics of real service traffic in the network so that network performance indicators are measured directly.

3.2 postcard-based telemetry: an in-band flow quality measurement method that, along the packet forwarding path, collects data hop by hop and reports it hop by hop.

3.3 passport mode telemetry: an in-band flow quality measurement method that, along the packet forwarding path, collects data hop by hop and reports it at the tail node. Note: in passport mode telemetry, the flow quality information collected hop by hop is encapsulated in the data packet and forwarded with the flow.

3.4 alternate marking (colouring): a quality detection technique that marks service packets directly in order to measure indicators such as packet loss and delay.

3.5 in-situ operations, administration and maintenance: an OAM implementation method that carries network operation and measurement information within service packets and forwards it along the service path.

4 Abbreviations

The following abbreviations apply to this document. ACL: access control list. BGP: border gateway protocol. DNP: dynamic network probe. DoH: destination option header. DSCP: differentiated services code point. FIEH: flow instruction extension header. IFIT: in-situ flow information telemetry. IGP: interior gateway protocol. IOAM: in-situ OAM. IPFIX: IP flow information export. OAM: operations, administration and maintenance. PBT: postcard-based telemetry. PMT: passport mode telemetry. SRH: segment routing header. SRv6: segment routing over IPv6. VxLAN: virtual extensible local area network.

5 Architecture of in-situ flow information telemetry

In-situ flow information telemetry (IFIT) provides an architecture and a method for network performance measurement that achieve automated quality measurement of high-performance flow information. Its architecture is shown in Figure 1 and mainly comprises the IFIT application and management system, the IFIT controller, and the forwarding devices inside the IFIT domain.

IFIT application and management system: responsible for the input of the measurement intent and the presentation of the measurement results. On one side it receives the network quality measurement intent coming from service applications and from operation and maintenance systems, and converts it into a network configuration policy that is delivered to the IFIT controller; the IFIT network configuration policy includes the flow objects to be measured, the performance indicators to be collected and the way the test data is to be reported. On the other side it receives the IFIT quality measurement data and the analysis results reported by the collection and analysis function module of the IFIT controller, and presents them visually.

IFIT controller: it contains two functional components, the network configuration function module and the collection and analysis function module. The network configuration function module supports gRPC and UDP protocol interfaces, receives the network configuration policy delivered by the IFIT application and management system, and converts it into device configuration commands for monitoring and quality measurement that are delivered to the network forwarding devices. The collection and analysis function module receives and stores the telemetry quality measurement data reported by the network devices and performs computation and analysis of the measurement data, such as forwarding delay and packet loss analysis and fault location; at the same time it reports the relevant measurement data and analysis results to the IFIT application and management system. The collection and analysis function module supports the JSON encoding format, supports a structured way of describing data, and supports standardized data encoding and convenient format conversion.

Forwarding devices inside the IFIT domain: network devices that support the IFIT function. During flow quality measurement they are divided, according to their IFIT role, into IFIT head node, IFIT transit node and IFIT tail node. The IFIT head node encapsulates the IFIT instruction header into the data packets of the designated flow object. The IFIT transit node collects measurement data according to the IFIT instruction and reports it to the IFIT controller as required. The IFIT tail node extracts the quality measurement data carried in the data packet and reports it to the IFIT controller, and at the same time removes the IFIT instruction header from the data packet before forwarding it.

Forwarding devices inside the IFIT domain shall support: the IFIT function, that is the encapsulation and decapsulation of the IFIT packet header and the addition and reading of the IFIT collected information; the flow identification function, identifying the traffic to be monitored or measured by means of ACLs or of algorithms such as Count-Min Sketch; the gRPC protocol, the JSON encoding format and the YANG modelling language, so that the collected flow information is reported quickly; the IPFIX protocol, for standardized export of IP flow information; pre-processing of the IFIT collected data, such as removal of redundant data, buffered batch processing and subscription to abnormal events; the dynamic network probe (DNP) technique, which achieves on-demand information probing through flexible configuration of the measurement data; the postcard mode and passport mode ways of reporting IFIT data; the unified mode and pipe mode ways of processing IFIT data.

In the implementation of IFIT, the IFIT controller configures the forwarding nodes and collects and analyses the quality measurement data, so that the forwarding quality information of the network flows is monitored in real time; the IFIT application and management system dynamically adjusts, on the basis of the measurement results, the flow quality measurement indicators and parameters that are monitored or measured, so that the quality measurement information is adjusted and optimized according to the real-time operating state of the network and network operation becomes finer grained.

The IFIT architecture supports several techniques for collecting in-situ flow information and for exporting data, so as to suit the measurement needs of different networks and applications. For the collection of performance test data, IFIT can be implemented in postcard-based telemetry (PBT) mode or in passport mode telemetry (PMT); for delimiting packet loss of an application, the PBT mode is required. In addition, IFIT can further integrate several data-plane monitoring and measurement techniques, providing network operation and maintenance with a complete method for automated quality measurement of data-plane flow information.

6.1 General

The key IFIT technologies mainly include intelligent flow selection, intelligent data reporting, dynamic network probing, and encapsulation and tunnelling. Intelligent flow selection achieves quality measurement of a specific flow for a specific service need; intelligent data reporting improves the transmission efficiency of the collected information on the basis of redundancy removal and efficient compression; dynamic network probing allows the measurement information to be customized flexibly and probes to be deployed on demand, either programmable hardware probes or hardware plus programmable software probes, improving the efficiency of network quality measurement; the use of different encapsulation and tunnelling techniques achieves end-to-end performance measurement in cross-domain network scenarios.

The IFIT application and management system needs to designate the corresponding measurement technique on the basis of the measurement needs of the application or of the operation and maintenance, and to deliver the relevant policy to the IFIT head node through the IFIT controller. On the basis of the configuration instruction the IFIT head node selects the target flow to be monitored or measured and the set of measurement information, and determines the corresponding header encapsulation format and tunnel mode according to the type of bearer layer. The IFIT forwarding devices collect the relevant measurement data according to the configuration instruction and determine the reporting mode of the measurement data, so that in-situ flow quality measurement is achieved.

In addition, on the basis of the real-time operating state of the network and of the services, the IFIT application and management system shall, without affecting the normal operation of the network, dynamically designate the loading or unloading of the DNP, adjust the