ETSI GS F5G 011 V1.1.1 (2022-11)

Fifth Generation Fixed Network (F5G); Telemetry Framework and Requirements for Access Networks

Disclaimer

The present document has been produced and approved by the Fifth Generation Fixed Network (F5G) 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
DGS/F5G-0011Telemetry

Keywords
F5G; telemetry; YANG

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 Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Fifth Generation Fixed Network (F5G).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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 defines the F5G Telemetry Framework and Requirements for the F5G Access Network. The framework specifies the key functions and interfaces. The F5G Access Network telemetry requirements include requirements for the functions, the overall system, and the interfaces with their data models (configuration and streaming/collection).

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

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 necessary for the application of the present document.

[1] ETSI GS F5G 004 (V1.1.1): "Fifth Generation Fixed Network (F5G); F5G Network Architecture".

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] IEEE 802.3™-2008: "IEEE Standard for information technology".

[i.2] Recommendation ITU-T G.988: "ONU management and control interface (OMCI) specification".

[i.3] Google® Developers | Protocol Buffers | Encoding.

NOTE: Available at https://developers.google.com/protocol-buffers/docs/encoding.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GS F5G 004 [1] and the following apply:

Access Network Telemetry (ANT): monitoring technology that remotely collects data in push mode from the OLT

alignment error packet: packet with bad FCS and with a non-integral number of octets

NOTE: The definition of this term comes from IEEE 802.3 [i.1].

ANT object: specific physical or logical entity in the OLT or ONU (e.g. a PON port, a service flow, etc.)

equipment sampling capability: minimum time interval for the OLT to gather the target telemetry data

NOTE: This time interval can be shorter than the sample interval.

EXAMPLE: The equipment sampling capability is x seconds, and the sample interval is y seconds. (x can be shorter than y). A single ANT object is created from the equipment sampled data according to the configuration rules.

error packet: include the following data frames:

- Correct and incorrect data frames with a frame length less than 64 bytes.
- Correct and incorrect data frames whose frame size is greater than the maximum MTU.
- Data frames with FCS errors whose frame length ranges from 64 to the maximum MTU.
- Data frames with alignment errors whose frame length ranges from 64 to the maximum MTU.

NOTE: The definition of this term comes from IEEE 802.3 [i.1].

fragment packet: packets with less than 64 octets in length, excluding framing octets but including FCS octets

NOTE 1: These packets have, and had either a bad FCS with an integral number of octets (FCS error) or a bad FCS with a non-integral number of octets (alignment error).

NOTE 2: The definition of this term comes from IEEE 802.3 [i.1].

jabber packet: packet that is greater than 1 518 octets in length, excluding framing octets but including FCS octets

NOTE 1: These packets have, and had either a bad FCS with an integral number of octets (FCS error) or a bad FCS with a non-integral number of octets (alignment error).

NOTE 2: The definition of this term comes from IEEE 802.3 [i.1].

oversized packet: packet with length greater than 1 518 octets

NOTE: The definition of this term comes from IEEE 802.3 [i.1].

sample interval: time interval for the ANT object in the Telemetry message reported by the OLT to the collector

NOTE: This value is configured by the configuration module of the telemetry system.

sample timestamp: timestamp at which the current ANT object was sampled

sensor group: group of multiple sensor paths

sensor path: data model path of the sensor, which describes the specific ANT objects for collection

service flow: service flow is a consequence of traffic classification based on the identifiers in the Ethernet packets on a physical port or logical port

NOTE 1: For example, an identifier can be a VLAN ID, which means Ethernet packets are classified based on VLANs.

NOTE 2: A service flow can also be a Layer 2 logical channel that carries services between an access node (OLT) and a subscriber (ONU).

undersized packet: packet with length less than 64 octets

NOTE: The definition of this term comes from IEEE 802.3 [i.1].

3.2 Symbols

Void.

3.3 Abbreviations

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

10G-EPON	10 Gbit/s Ethernet Passive Optical Network
AI	Artificial Intelligence
ANT	Access Network Telemetry
BER	Bit Error Ratio
BIP	Bearer Independent Protocol
CLI	Command-Line Interface
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DG	Dying Gasp
DOW	Drift Of Window
DPU	Data Pre-processing Unit
EPON	Ethernet Passive Optical Network
FCS	Frame Check Sequence
FEC	Forward Error Correction
GEM	GPON Encapsulation Mode
GNMI	gRPC® Network Management Interface
GPB®	Google® Protocol Buffer
GPON	Gigabit-Capable Passive Optical Networks
gRPC®	Google® Remote Procedure Call
HEC	Hybrid Error Correction
HTTP	Hyper Text Transfer Protocol
ID	Identity Document
IP	Internet Protocol
IPTV	Internet Protocol Television
JSON	Java Script Object Notation
LOF	Loss Of Frame
LOS	Loss Of Signal
LP	Line Protocol
MAC	Message Authentication Code
MIB	Management Information Base
ML	Machine Learning
MSB	Most Significant Bit
MTU	Maximum Transmission Unit
NE	Network Entity
NETCONF	Network Configuration Protocol
ODN	Optical Distribution Network
OLT	Optical Line Terminal
ONU	Optical Network Unit
P2MP	Point to Multipoint
PON	Passive Optical Network
RPC	Remote Procedure Call
SNI	Service Node Interface
SNMP	Simple Network Management Protocol
TCONT	Transmission - Container
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSDB	Time Series Database
UDP	User Datagram Protocol
UNI	User Network Interface
VLAN	Virtual Local Area Network
XG	10 GigabitMAC
XG-PON	10-Gigabit-capable Passive Optical Network
XGS-PON	10-Gigabit-capable Symmetric Passive Optical Network
YANG	Yet Another Next Generation data modelling language

4 Framework of Telemetry in Access Network

4.1 Motivation and Business Drivers

Figure 1 depicts the current Access Network deployment. A traditional data pulling methods is used, such as SNMP, syslog and CLI to pull data from the OLT to monitor Access Network and troubleshoot any issues. The interface uses proprietary MIBs from different OLT equipment vendors which are difficult to automate. So, each request to pull data is resource intensive and impact the performance of the OLT, and adds complexity because there is more than one pull request per OLT. The pulling method does not efficiently scale.

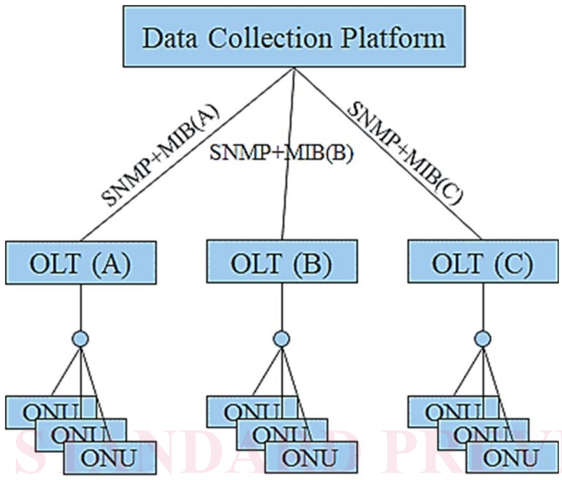


Figure 1: Traditional Access Network architecture

As the complexity of the Access Network increases, it is crucial to maintain the network health. To achieve this, the Access Network can provide better visibility compared to existing methods via automated real-time data collection. Telemetry replaces the pull method, and uses the push method to continuously stream data from the OLT and provides notifications to the data collection platform. Telemetry has the advantages of scale, speed and automation. With the flexibility of telemetry, the data of interest can be selected from the OLT and the OLT can transmit it in a structured format to a data collection platform for monitoring. In addition, the data collection platform can expose F5G Access Network information to the application layer.

Telemetry introduces finer granular data points and more frequent data streaming in the Access Network. It enables better performance monitoring and therefore better control over large Access Network. Telemetry data can assist in the prediction of network problems and take preventative actions without impacting the performance of the OLT. The operators can gain better visibility and insight into the network. The operator can enhance the network operational performance by using data analytics. Telemetry technology opens the door to big data and machine learning methods in the Access Network.

4.2 Telemetry Architecture Overview

Figure 2 illustrates the F5G Access Network architecture of the telemetry technologies. The Access Network equipment supports the telemetry collection function, which adopts the active push mode, supports structured data and has higher execution efficiency and real-time collection accuracy. To meet the needs of refined, visualized, intelligent monitoring of operation and maintenance, telemetry provides the basis of big data analysis for the rapid locating of network problems and network quality optimization and adjustment.

In the deployment scenario of Access Network equipment which supports telemetry technology, the telemetry architecture can be partitioned into the telemetry system and the OLT. The telemetry system is responsible for the subscription configuration, receiving telemetry collection data reported from the OLT, and data processing, storage and analysis. The OLT is responsible for reporting telemetry collection data according to the subscription configuration.

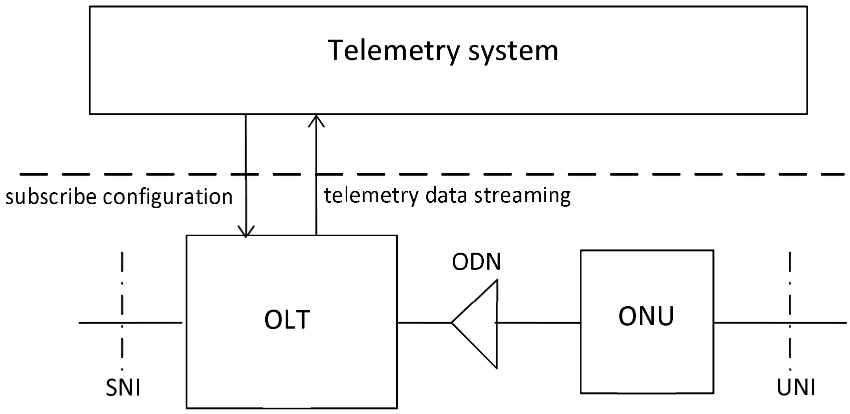


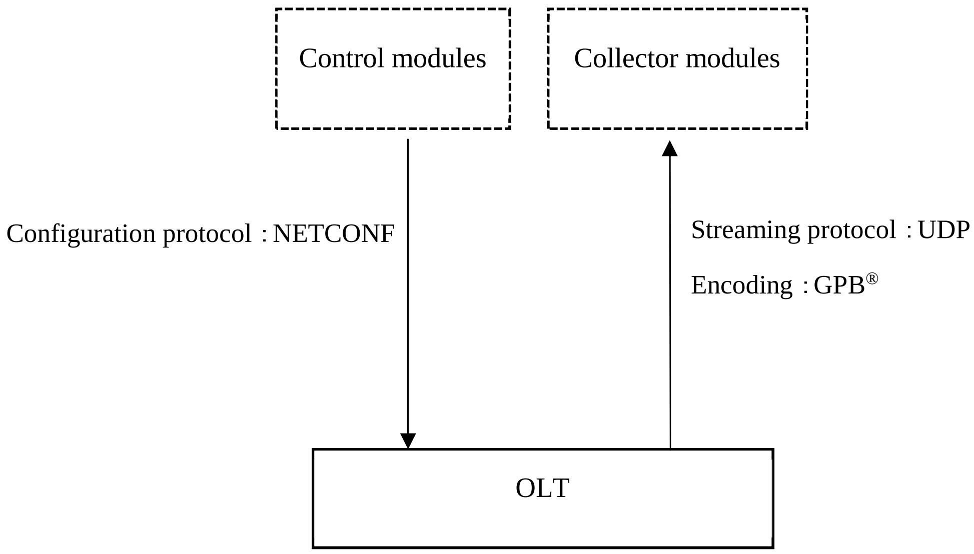
Figure 2: Telemetry architecture in the Access Network

5 Technical Solutions

5.1 UDP Streaming Telemetry Mode

The telemetry system shall support both control and collection features. The control modules should support the NETCONF protocol to send subscription configuration. The corresponding parameters are described in Clause 6 of the present document. If UDP streaming telemetry mode is chosen, the OLT equipment should support UDP encapsulated data reporting. The serialization of the data is based on GPB®.

If UDP streaming telemetry mode is chosen for the telemetry collection, the OLT shall continuously stream the data to the several collectors, once the subscriptions are created as part of the configuration of the OLT and it shall remain the OLT configuration until the subscription is removed. The schematic diagram of UDP streaming telemetry mode is shown in Figure 3.



NOTE: Encoding methods other than GPB® are possible.

Figure 3: UDP streaming telemetry mode

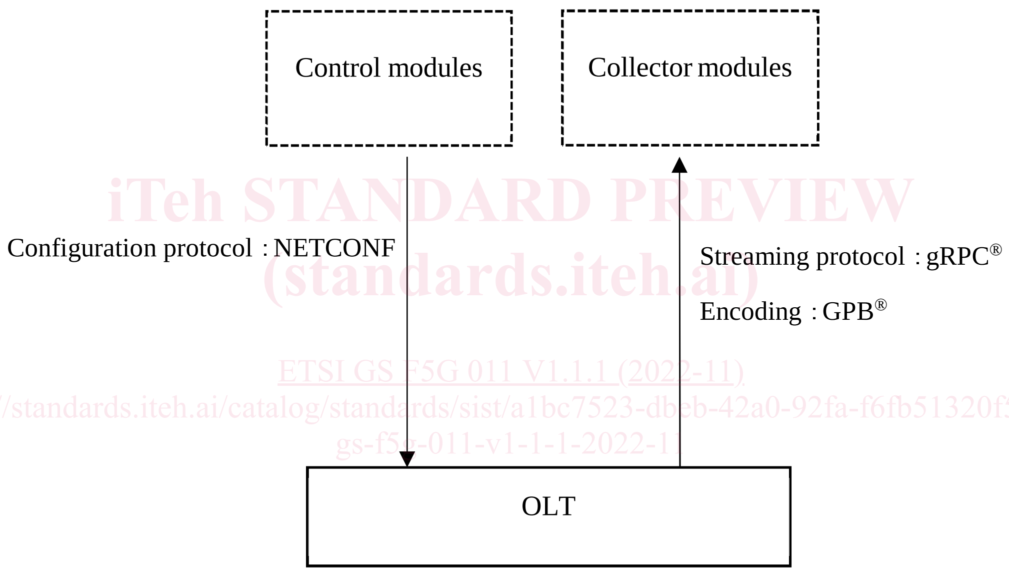
The specific protocol stack layer is shown in Table 1.

Table 1: The telemetry stack layer and requirements of UDP telemetry mode

Telemetry Stack		Requirements
Data layer	Collection data layer	Carries encoded telemetry collection data.
	Telemetry layer	Defines the data header when telemetry data is sent, including sampling path, sampling timestamp, etc. The specific parameters are defined in clause 6.3 of the present document.
Message header layer		Optional support for fragmentation and encoding format indication through the message header layer.
UDP transport layer		UDP provides simple information transmission service, but information might be lost.

5.2 gRPC® Static Telemetry Mode

The telemetry system shall support both control and collection features. The control modules should support the NETCONF protocol to send subscription configuration. The corresponding parameters are described in clause 6. If gRPC® static telemetry mode is chosen, the OLT equipment should support data encapsulation and reporting as a gRPC® client. The schematic diagram of gRPC® static telemetry mode is shown in Figure 4.



NOTE: Encoding methods other than GPB® are possible.

Figure 4: gRPC® Static Telemetry Mode

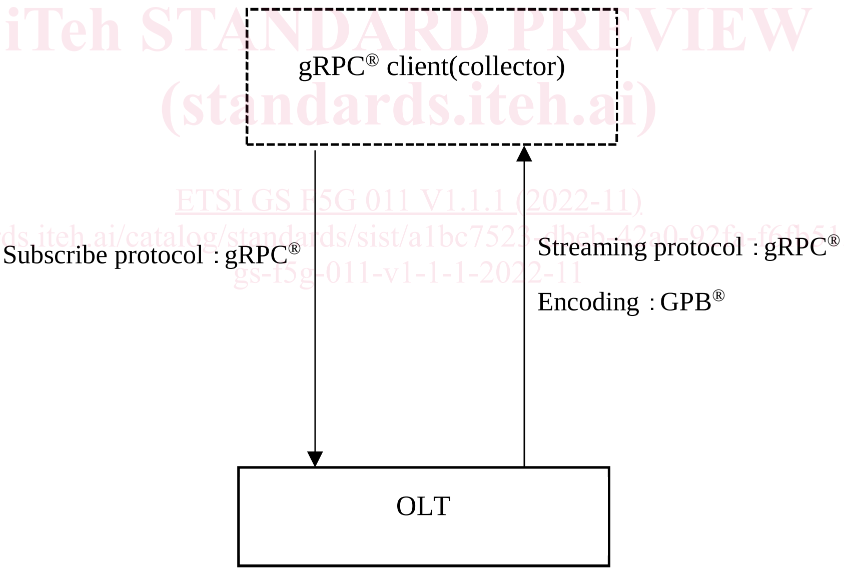
If gRPC® static telemetry mode is chosen for the telemetry collection, the OLT shall continually stream the telemetry data to the several collectors once the subscriptions are created as part of the configuration and it shall remain the OLT configuration until the configuration is removed. The specific protocol stack layer is shown in Table 2.

Table 2: The telemetry stack layer and requirements of gRPC® Static Telemetry Mode

Telemetry Stack		Requirements
Data Layer	Collection data layer	Carries encoded telemetry collection data.
	Telemetry layer	Defines the data header when telemetry data is sent, including sampling path, sampling timestamp, etc. The specific parameters are defined in clause 6.3 of the present document.
	RPC layer	Defines the RPC interfaces when the OLT equipment is reporting telemetry data as a client.
gRPC® layer		Defines the gRPC® protocol interaction format of remote procedure calls.
HTTP 2.0 layer		gRPC® is carried on the HTTP 2.0 protocol.
TLS transport layer		Optional. OLT and telemetry system can perform channel encryption and mutual authentication based on the TLS protocol to realize secure transmission.
TCP transport layer		TCP provides a connection-oriented, reliable information transmission service.
NOTE: The UDP Streaming mode is similar to the gRPC® static mode.		

5.3 gRPC® Dynamic Telemetry Mode

The telemetry system shall support both subscription and collection features. The telemetry system should support creating subscriptions to the OLT as a gRPC® client and receiving streaming data. If gRPC® dynamic telemetry mode is chosen, the OLT equipment should support data encapsulation and reporting as a gRPC® server which supports gRPC® Network Management Interface (gNMI). The schematic diagram of gRPC® static telemetry mode is shown in Figure 5.



NOTE: Encoding methods other than GPB® are possible.

Figure 5: gRPC® Dynamic Telemetry Mode

If gRPC® dynamic telemetry mode is chosen for the telemetry collection, the OLT shall continually stream the telemetry data to the one certain collector when this collector sends the subscriptions to the OLT. This dynamic subscription shall terminate when the collector cancels the subscription or when the session terminates. The dynamic telemetry mode is suitable when the collector exactly knows its telemetry requirements. This mode is convenient as a centralized way of configuring the network and requesting operational data. The specific protocol stack layer is shown in Table 3.

Table 3: The telemetry stack layer and requirements of gRPC® Dynamic Telemetry Mode

Telemetry Stack		Requirements
Data Layer	Collection data layer	Carries encoded telemetry collection data.
	Telemetry layer	Defines the data header when telemetry data is sent, including sampling path, sampling timestamp, etc. The specific parameters are defined in clause 6.3 of the present document.
	RPC layer	Defines the RPC interfaces when the OLT equipment is reporting telemetry data as a server.
gRPC® layer		Defines the gRPC® protocol interaction format of remote procedure call.
HTTP 2.0 layer		gRPC® is carried on the HTTP 2.0 protocol.
TLS transport layer		Optional. OLT and telemetry system can perform channel encryption and mutual authentication based on the TLS protocol to realize secure transmission.
TCP transport layer		TCP provides a connection-oriented, reliable information transmission service.

6 Interface Requirements

6.1 Overview

The gRPC® layer, the telemetry layer and the collection data layer play different roles in the telemetry system. The gRPC® layer shall only exist when the streaming protocol is gRPC®. The telemetry layer and the collection data layer shall always exist in telemetry messages and carries the main contents.

Clause 6 of the present document specifies the technical requirements and the key parameters of the gRPC® layer, the telemetry layer and collection data layer.

6.2 gRPC® Layer Requirements

6.2.1 gRPC® Static Telemetry mode

When the streaming protocol is gRPC® and it is gRPC® Static Telemetry mode, the OLT shall stream collection data through an RPC interface to the telemetry system as a gRPC® client according to the telemetry configuration. The structure of this RPC interface has been defined in this layer.

The RPC structure shall contain the following elements:

- Request ID.
- Streaming telemetry data structure and its elements are defined by the Telemetry layer. The telemetry layer requirements are defined in clause 6.3.

6.2.2 gRPC® Dynamic Telemetry mode

When the streaming protocol is gRPC® and it is gRPC® Dynamic Telemetry mode, the telemetry system shall send a subscription request through an RPC interface to the OLT. The structure of this subscribe RPC interface has been defined in this layer.

The subscribe RPC interface structure shall contain the following elements:

- Request ID.
- Encoding method.
- Data model path of the sensor which describes the specific ANT objects for collection.
- Sample interval.