International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.7041/Y.1303

(08/2016)

SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

Data over Transport – Generic aspects – General

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet protocol aspects – Transport

Generic framing procedure

Recommendation ITU-T G.7041/Y.1303

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TRANSMISSION MEDIA AND OPTICAL SYSTEMS CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
MULTIMEDIA QUALITY OF SERVICE AND PERFORMANCE – GENERIC AND USER-RELATED ASPECTS	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DATA OVER TRANSPORT – GENERIC ASPECTS	G.7000–G.7999
General	**G.7000–G.7099**
Transport network control aspects	G.7700–G.7799
PACKET OVER TRANSPORT ASPECTS	G.8000–G.8999
ACCESS NETWORKS	G.9000–G.9999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T G.7041/Y.1303

Generic framing procedure

Summary

Recommendation ITU-T G.7041/Y.1303 defines a generic framing procedure (GFP) to delineate octet-aligned, variable-length payloads from higher-level client signals for subsequent mapping into octet-synchronous paths, such as those defined in Recommendations ITU-T G.707/Y.1322, ITU-T G.8040/Y.1340 and ITU-T G.709/Y.1331. This Recommendation defines:

– frame formats for protocol data units (PDUs) transferred between GFP initiation and termination points;

– the mapping procedure for the client signals into GFP;

– responses to certain defect conditions.

This edition adds the information from Amendment 1 (2012), Amendment 2 (2012) and Amendment 3 (2015) to Recommendation ITU-T G.7041 (2011), in addition to new material and text enhancements from contributions to the February 2016 meeting.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T G.7041/Y.1303	2001-12-14	15	11.1002/1000/5644
1.1	ITU-T G.7041/Y.1303 (2001) Amd. 1	2002-06-13	15	11.1002/1000/6062
1.2	ITU-T G.7041/Y.1303 (2001) Cor. 1	2003-03-16	15	11.1002/1000/6285
1.3	ITU-T G.7041/Y.1303 (2001) Amd. 2	2003-03-16	15	11.1002/1000/6284
2.0	ITU-T G.7041/Y.1303	2003-12-14	15	11.1002/1000/7082
2.1	ITU-T G.7041/Y.1303 (2003) Amd. 1	2004-10-07	15	11.1002/1000/7352
2.2	ITU-T G.7041/Y.1303 (2003) Amd. 2	2004-06-13	15	11.1002/1000/7353
2.3	ITU-T G.7041/Y.1303 (2003) Cor. 1	2005-01-13	15	11.1002/1000/7476
2.4	ITU-T G.7041/Y.1303 (2003) Amd. 3	2005-01-13	15	11.1002/1000/7475
3.0	ITU-T G.7041/Y.1303	2005-08-22	15	11.1002/1000/8528
3.1	ITU-T G.7041/Y.1303 (2005) Amd. 1	2006-03-29	15	11.1002/1000/8769
3.2	ITU-T G.7041/Y.1303 (2005) Cor. 1	2006-12-14	15	11.1002/1000/8997
3.3	ITU-T G.7041/Y.1303 (2005) Amd. 2	2007-07-29	15	11.1002/1000/9170
4.0	ITU-T G.7041/Y.1303	2008-10-07	15	11.1002/1000/9399
4.1	ITU-T G.7041/Y.1303 (2008) Amd. 1	2009-01-13	15	11.1002/1000/9655
4.2	ITU-T G.7041/Y.1303 (2008) Amd. 2	2010-07-29	15	11.1002/1000/10893
5.0	ITU-T G.7041/Y.1303	2011-04-13	15	11.1002/1000/11133
5.1	ITU-T G.7041/Y.1303 (2011) Amd. 1	2012-02-13	15	11.1002/1000/11506
5.2	ITU-T G.7041/Y.1303 (2011) Amd. 2	2012-10-29	15	11.1002/1000/11799
5.3	ITU-T G.7041/Y.1303 (2011) Amd. 3	2015-01-13	15	11.1002/1000/12378
6.0	ITU-T G.7041/Y.1303	2016-08-06	15	11.1002/1000/12801

Keywords

Generic framing procedure, optical transport network, synchronous digital hierarchy

---

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

© ITU 2017

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

Page

Introduction

A generic framing procedure (GFP) provides a generic mechanism to adapt traffic from higher-layer client signals over a transport network. Client signals may be protocol data unit- (PDU)-oriented [such as Internet protocol/point-to-point protocol (IP/PPP) or Ethernet media access control (MAC)] or block-code oriented constant bit rate stream [such as fibre channel or enterprise systems connection/single-byte command code sets connection (ESCON/SBCON)].

The GFP specification consists of both common and client-specific aspects. Common aspects of GFP apply to all GFP-adapted traffic and they are specified in clause 6. Client-specific aspects of GFP are specified in clauses 7 and 8. Currently, two modes of client signal adaptation are defined for GFP.

– A PDU-oriented adaptation mode, referred to as frame-mapped GFP (GFP-F), is specified in clause 7.

– A block-code oriented adaptation mode, referred to as transparent GFP (GFP-T), is specified in clause 8.

Figure 1 illustrates the relationship between the higher-layer client signals, GFP and GFP transport paths.

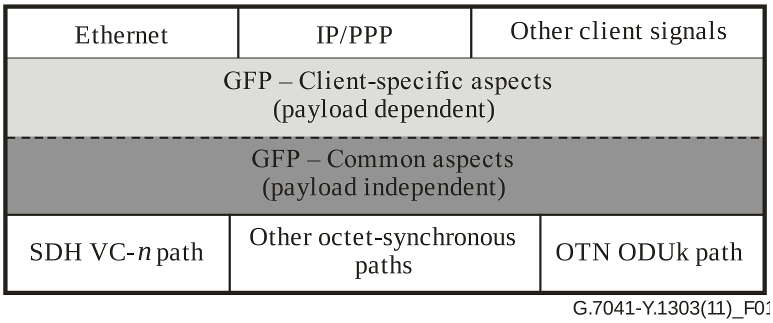


Figure 1 – GFP relationship to client signals and transport paths

Figure 2 illustrates the environment in which GFP operates.

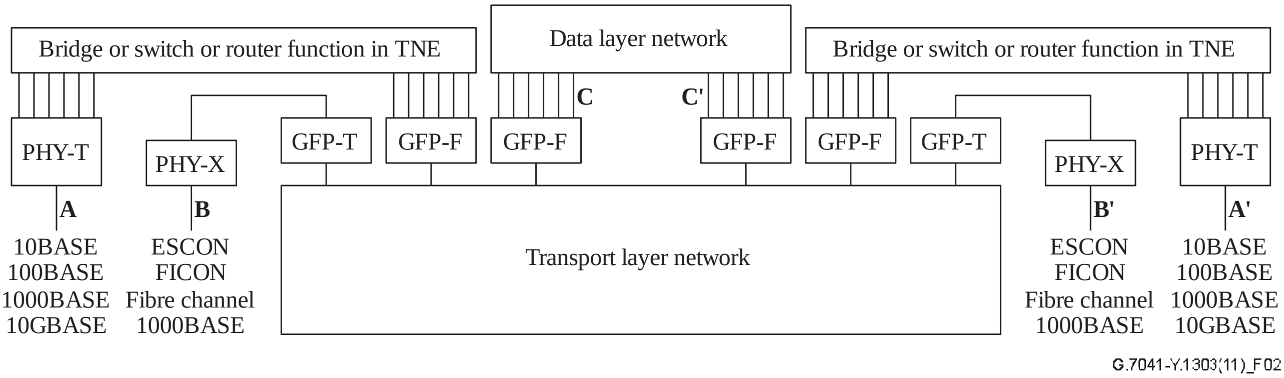


Figure 2 – GFP functional model (single client)

In the frame-mapped adaptation mode, the client/GFP adaptation function may operate at the data link layer (or higher layer) of the client signal. Client PDU visibility is required. This visibility is obtained when the client PDUs are received from either the data layer network [e.g., Internet protocol (IP) router fabric or Ethernet switch fabric (C/C' in Figure 2)] or, e.g., a bridge, switch or router function in a transport network element (TNE). In the latter case, the client PDUs are received via, e.g., an Ethernet interface (A/A' in Figure 2).

For the transparent adaptation mode, the client/GFP adaptation function operates on the coded character stream rather than on the incoming client PDUs. Thus, processing of the incoming codeword space for the client signal is required (B/B' in Figure 2).

Typically, interconnections can be set up between ports A and A', B and B', C and C', A and C', and C and A'. Note that the physical port type of B and B' must be the same to support an interconnection, while the physical port type of A and A' may be different.

Some high-level functional models associated with the above GFP processing can be found in Appendix I.

Recommendation ITU-T G.7041/Y.1303

Generic framing procedure

1 Scope

This Recommendation defines a generic framing procedure (GFP) to encapsulate variable-length payload of various client signals for subsequent transport over synchronous digital hierarchy (SDH), plesiochronous digital hierarchy (PDH) and optical transport network (OTN) networks as defined in [ITU-T G.707], [ITU-T G.8040] and [ITU-T G.709]. This Recommendation defines the:

- frame formats for protocol data units (PDUs) transferred between GFP initiation and termination points;
- mapping procedure for the client signals into GFP.

The framing procedure described in this Recommendation can be applied to both the encapsulation of entire client frames (frame-mapped GFP), in which a single client frame is mapped into a single GFP frame, and to character-mapped transport (transparent GFP), in which a number of client data characters are mapped into efficient block codes for transport within a GFP frame.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T G.707]	Recommendation ITU-T G.707/Y.1322 (2007), *Network node interface for the synchronous digital hierarchy (SDH)*.
[ITU-T G.709]	Recommendation ITU-T G.709/Y.1331 (2016), *Interfaces for the optical transport network (OTN)*.
[ITU-T G.781]	Recommendation ITU-T G.781 (2008), *Synchronization layer functions*.
[ITU-T G.783]	Recommendation ITU-T G.783 (2006), *Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks*.
[ITU-T G.798]	Recommendation ITU-T G.798 (2012), *Characteristics of optical transport network hierarchy equipment functional blocks*.
[ITU-T G.806]	Recommendation ITU-T G.806 (2012), *Characteristics of transport equipment – Description methodology and generic functionality*.
[ITU-T G.8021]	Recommendation ITU-T G.8021/Y.1341 (2016), *Characteristics of Ethernet transport network equipment functional blocks*.
[ITU-T G.8040]	Recommendation ITU-T G.8040/Y.1340 (2005), *GFP frame mapping into plesiochronous digital hierarchy (PDH)*.
[ITU-T G.8264]	Recommendation ITU-T G.8264/Y.1364 (2013), *Distribution of timing information through packet networks*.
[ITU-T G.8275.1]	Recommendation ITU-T G.8275.1/Y.1369.1 (2016), *Precision time protocol telecom profile for phase/time synchronization with full timing support from the network*.

[ITU-T H.222.0] Recommendation ITU-T H.222.0 (2014)|ISO/IEC 13818-1:2015, *Information technology – Generic coding of moving pictures and associated audio information: Systems*.

[ITU-T I.363.1] Recommendation ITU-T I.363.1 (1996), *B-ISDN ATM Adaptation Layer specification: Type 1 AAL*.

[ITU-T I.432.1] Recommendation ITU-T I.432.1 (1999), *B-ISDN user-network interface – Physical layer specification: General characteristics*.

[ITU-T X.233] Recommendation ITU-T X.233 (1997)|ISO/IEC 8473-1:1998, *Information technology – Protocol for providing the connectionless-mode network service: Protocol specification*.

[ANSI INCITS 230] ANSI INCITS 230-1994 (R1999), *Information Technology – Fibre Channel – Physical and Signaling Interface (FC-PH).*

[ANSI INCITS 296] ANSI INCITS 296-1997 (R2007), *Information Technology – Single-Byte Command Code Sets CONnection (SBCON) Architecture*.

[EN 50083-9] EN 50083-9:2002, *Cable networks for television signals, sound signals and interactive services – Part 9: Interfaces for CATV/SMATV headends and similar professional equipment for DVB/MPEG-2 transport streams*.

[ETSI TR 101 290] ETSI TR 101 290 (2014), *Digital Video Broadcasting (DVB); Measurement guidelines for DVB systems*.

[IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol*.

[IETF RFC 1661] IETF RFC 1661 (1994), *The Point-to-Point Protocol (PPP)*.

[IETF RFC 1662] IETF RFC 1662 (1994), *PPP in HDLC-like Framing*.

[IETF RFC 2460] IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Specification*.

[IETF RFC 3032] IETF RFC 3032 (2001), *MPLS Label Stack Encoding*.

[IEEE 802.3] IEEE 802.3-2015, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*.

[IEEE 802.17] IEEE 802.17-2011, *IEEE standard for information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 17: Resilient packet ring (RPR) access method and physical layer specifications*.

[ISO 9542] ISO 9542:1988, *Information processing systems – Telecommunications and information exchange between systems – End system to Intermediate system routeing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473).*

[ISO/IEC 10589] ISO/IEC 10589:2002, *Information technology – Telecommunications and information exchange between systems – Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473).*

[ISO/IEC 13239]	ISO/IEC 13239:2002, *Information technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures*.
[ISO/IEC 13818-9]	ISO/IEC 13818-9:1996, *Information technology – Generic coding of moving pictures and associated audio information – Part 9: Extension for real time interface for systems decoders*.
[ISO/IEC 14165-241]	ISO/IEC 14165-241:2005, *Information technology – Fibre Channel – Part 241: Backbone 2 (FC-BB-2).*

3 Terms and definitions

This Recommendation defines the following terms:

3.1 channel identifier (CID): An 8-bit binary number used to indicate one of 256 communication channels at a generic framing procedure (GFP) initiation/termination point.

3.2 client data frame: A generic framing procedure (GFP) frame that contains payload data from a client signal.

3.3 client defect clear indication (DCI): A fast explicit indication from the client that a client signal fail, reverse defect or forward defect event has cleared. The DCI allows the generic framing procedure (GFP) sink adaptation function to respond to the fault clearing immediately rather than detecting the clearing through a time out in the arrival of Client Signal Fail (CSF), reverse defect indication (RDI) or forward defect indication (FDI) frames.

3.4 client forward defect indication (FDI): A generic framing procedure (GFP) client management frame (CMF) used to communicate client forward defect information from the GFP-F source to the sink adaptation functions. Some clients transmit an indication of local faults affecting the forward signal direction, with the indication encoded into the client physical layer signal.

3.5 client management frame (CMF): A generic framing procedure (GFP) frame containing information associated with the management of the GFP connection between the GFP source and sink.

3.6 client reverse defect indication (RDI): A generic framing procedure (GFP) client management frame (CMF) used to communicate this client reverse defect information from the GFP-F source to the sink adaptation functions. Some clients transmit an indication of faults in the reverse signal direction, with the indication encoded into the client physical layer signal.

3.7 control frame: A generic framing procedure (GFP) frame used to control the GFP connection. The only control defined at this time is the idle frame.

3.8 frame-mapped GFP: A type of generic framing procedure (GFP) mapping in which a client signal frame is received and mapped in its entirety into one GFP frame.

3.9 management communications frame (MCF): A generic framing procedure (GFP) frame used to provide a management communications channel (MCC) capability across the GFP link. The definition of this channel and its applications are beyond the scope of this Recommendation.

3.10 maximum transmission unit (MTU): Maximum size of the generic framing procedure (GFP) payload area, in octets.

3.11 running disparity (RD): A procedure used by block line codes, such as 8B/10B, to balance the total of number of 1s and 0s transmitted over time. The running disparity at the end of a line code sub-block is positive if more 1s than 0s have been sent up to that point, and negative if more 0s than 1s have been sent. The encoder uses the running disparity value to choose which of the two possible codes to transmit for the next character mapping in order to balance the number of transmitted 1s and 0s.

3.12 source port/destination port (SP/DP): A logical addressable entity on a physical interface.

3.13 superblock: A transparent generic framing procedure (GFP) structure that combines multiple 64B/65B codes along with a CRC-16 for the purposes of providing payload octet alignment and error control over the bits in the superblock.

NOTE – See Figure 8-3.

3.14 transparent GFP: A type of generic framing procedure (GFP) mapping in which block-coded client characters are decoded and then mapped into a fixed-length GFP frame and may be transmitted immediately without waiting for the reception of an entire client data frame.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

1GbE	1 Gbit/s Ethernet
ACFC	Address-and-Control-Field-Compression
AIS	Alarm Indication Signal
ASI	Asynchronous Serial Interface
ATM	Asynchronous Transfer Mode
BBW	Backbone WAN
cHEC	core Header Error Check
CID	Channel Identifier
CLNP	Connectionless Network Protocol
CMF	Client Management Frame
CoS	Class of Service
CRC	Cyclic Redundancy Check
CSF	Client Signal Fail
DCI	Defect Clear Indication
DE	Discard Eligibility
DP	Destination Port
DVB	Digital Video Broadcast
eHEC	extension Header Error Check
ES-IS	End System-to-Intermediate System
EOF	End of Frame
ESCON	Enterprise Systems Connection
EXI	Extension header Identifier
FC	Fibre Channel
FCS	Frame Check Sequence
FDI	Forward Defect Indication
FEFI	Far-End Fault Indication
FICON	Fibre Connection

FIFO	First-In, First-Out
GFP	Generic Framing Procedure
GFP-F	Generic Framing Procedure, Frame-mapped
GFP-T	Generic Framing Procedure, Transparent
HDLC	High-level Data Link Control
HEC	Header Error Check
IFG	Inter-Frame Gap
IP	Internet Protocol
IPG	Inter-Packet Gap
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System-to-Intermediate System
LCC	Last Control Character
LCP	Link Control Protocol
LF	Local Fault
LOL	Loss of Light
LOS	Loss of Signal
LSB	Least Significant Bit
MAC	Media Access Control
MAPOS	Multiple Access Protocol Over Synchronous optical network/synchronous digital hierarchy
MCC	Management Communications Channel
MCF	Management Communications Frame
MPEG	Moving Picture Expert Group
MPLS	Multiprotocol Label Switching
MSB	Most Significant Bit
MTU	Maximum Transmission Unit
NE	Network Element
OSI	Open Systems Interconnection
OTN	Optical Transport Network
PCS	Physical Coding Sublayer
PDH	Plesiochronous Digital Hierarchy
PDU	Protocol Data Unit
pFCS	payload Frame Check Sequence
PFI	Payload Frame check sequence Indicator
PLI	Payload Length Indicator
PLL	Phase-Locked Loop
PPP	Point-to-Point Protocol
PTI	Payload Type Identifier

PTP	Precision Time Protocol
RD	Running Disparity
RDI	Reverse Defect Indication
RF	Remote Fault
RPR	Resilient Packet Ring
RS	Reed-Solomon
SBCON	Single-Byte command code sets Connection
SBW	Spare Bandwidth
SDH	Synchronous Digital Hierarchy
SFD	Start of Frame Delimiter
SOF	Start of Frame
SONET	Synchronous Optical Network
SP	Source Port
SSF	Server Signal Failure
SSM	Synchronization Status Message
tHEC	type Header Error Check
TS	Transport Stream
TSF	Trail Signal Fail
UPI	User Payload Identifier
VC-*n*	Virtual Container-*n*

5 Conventions

Transmission order: The order of transmission of information in all the figures in this Recommendation is first from left to right and then from top to bottom. Within each byte, the most significant bit (MSB) is transmitted first. The MSB is shown at the left of all the figures.

Undefined field values: The default value for any undefined header fields is 0, unless otherwise stated.

6 Aspects common to both frame-mapped and transparent-mapped modes of GFP

This clause discusses the common (protocol-independent) aspects of GFP for octet-aligned payloads. The mapping of the framed payloads into an SDH VC-*n* is specified in [ITU-T G.707]. The mapping of the framed payloads into an OTN ODUk payload is specified in [ITU-T G.709].

GFP uses a variation of the HEC-based frame delineation mechanism defined for asynchronous transfer mode (ATM) (see [ITU-T I.432.1]). Two kinds of GFP frames are defined: GFP client frames and GFP control frames. Frame formats for GFP client and control frames are defined in clauses 6.1 and 6.2. GFP also supports a flexible (payload) header extension mechanism to facilitate the adaptation of GFP for use with diverse transport mechanisms. Currently defined payload extension header types are specified in clause 6.1.2.1.3.

6.1 Basic signal structure for GFP client frames

The format for GFP frames is shown in Figure 6-1. GFP frames are octet-aligned and consist of a GFP core header and, except for GFP idle frames, a GFP payload area.

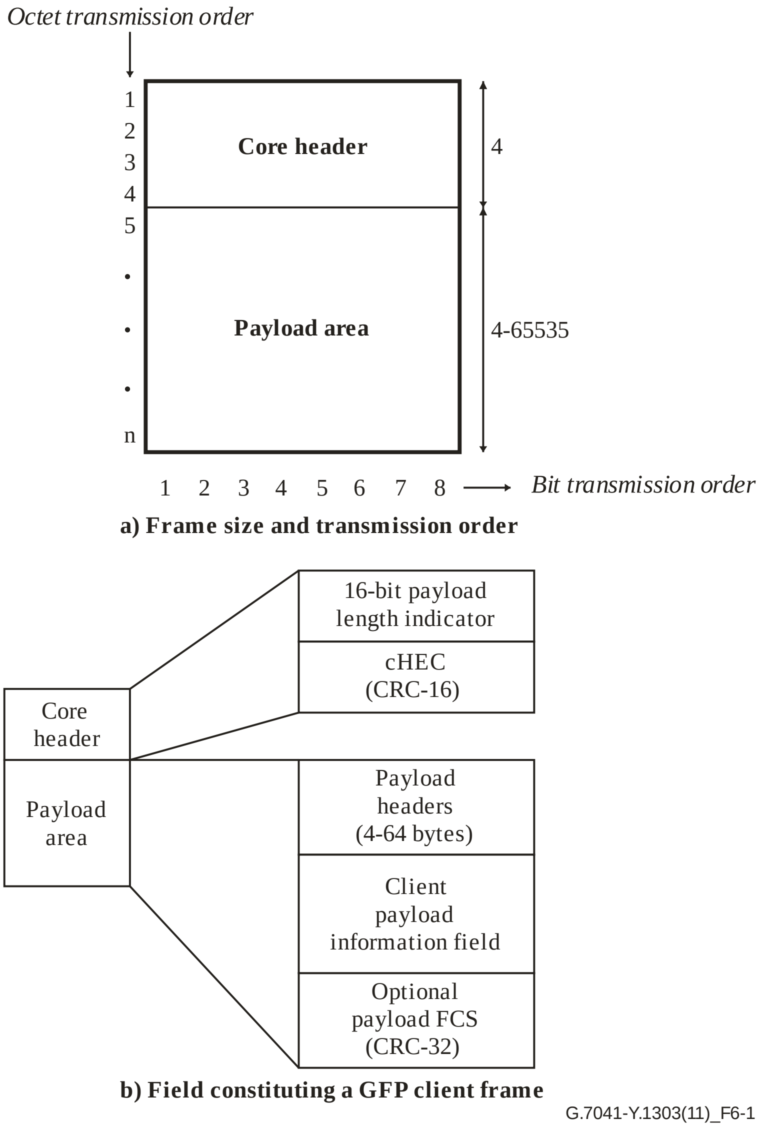
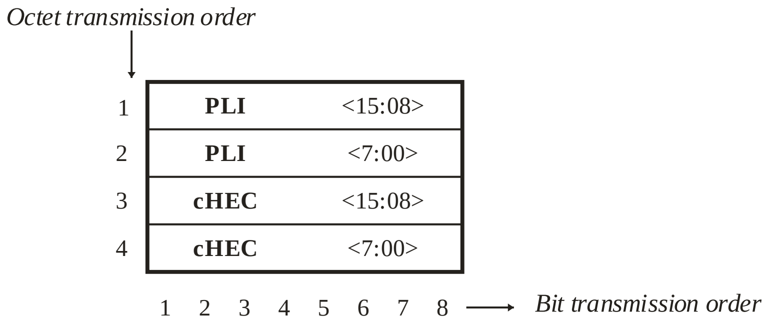


Figure 6-1 – Frame format for GFP client frames

6.1.1 GFP core header

The GFP core header format is shown in Figure 6-2. The four octets of the GFP core header consist of a 16-bit payload length indicator (PLI) field and a 16-bit core header error check (cHEC) field. This header allows GFP frame delineation independent of the content of the higher layer PDUs.



G.7041-Y.1303(11)_F6-2

Figure 6-2 – GFP core header format

6.1.1.1 Payload length indicator field

The two-octet PLI field contains a binary number representing the number of octets in the GFP payload area. The absolute minimum value of the PLI field in a GFP client frame is four octets. PLI values 0–3 are reserved for GFP control frame usage (see clause 6.2).

6.1.1.2 Core header error control field

The two-octet cHEC field contains a cyclic redundancy check-16 (CRC-16) error control code that protects the integrity of the contents of the core header by enabling both single-bit error correction and multi-bit error detection. The cHEC sequence is calculated over the octets of the core header as specified in clause 6.1.1.2.1.

6.1.1.2.1 HEC processing

The header error check (HEC) generating polynomial is $G(x) = x^{16} + x^{12} + x^5 + 1$, with an initialization value of zero, where x^{16} corresponds to the MSB and x^0 corresponds to the least significant bit (LSB).

The cHEC field is generated by the source adaptation process using the following steps (see Appendix I of [b-ITU-T V.41]).

1) The first two octets of the GFP frame are taken in network octet order, MSB first, to form a 16-bit pattern representing the coefficients of a polynomial $M(x)$ of degree 15.
2) $M(x)$ is multiplied by x^{16} and divided (modulo 2) by $G(x)$, producing a remainder $R(x)$ of degree 15 or less.
3) The coefficients of $R(x)$ are considered to be a 16-bit sequence, where x^{15} is the MSB.
4) This 16-bit sequence is the CRC-16 where the first bit of the CRC-16 to be transmitted is the coefficient of x^{15} and the last bit transmitted is the coefficient of x^0.

The sink adaptation process performs steps 1)–3) in the same manner as the source adaptation process, except that here, the $M(x)$ polynomial of step 1) includes the CRC-16 bits in received order, and has degree 23. In the absence of bit errors, the remainder shall be 0000 0000 0000 0000.

This single error correction shall be performed on the core header. The GFP sink adaptation process shall discard any of those GFP frames where multi-bit errors are detected. The sink adaptation process also updates any relevant system records for performance monitoring purposes.

6.1.1.3 Core header scrambling

The core header is scrambled for DC balance by an exclusive-OR operation (modulo 2 addition) with the hexadecimal number B6AB31E0. This number is the maximum transition, minimum side-lobe, Barker-like sequence of length 32. The scrambling of the GFP core header improves the robustness of the GFP frame delineation procedure and provides a sufficient number of 0-1 and 1-0 transitions during idle transmission periods.

6.1.2 GFP payload area

The GFP payload area, which consists of all octets in the GFP frame after the GFP core header, is used to convey higher-layer specific protocol information. This variable length area may include from 4 to 65 535 octets. As shown in Figure 6-3, the GFP payload area consists of two common components: a payload header and a payload information field. An optional payload frame check sequence (pFCS) field is also supported.

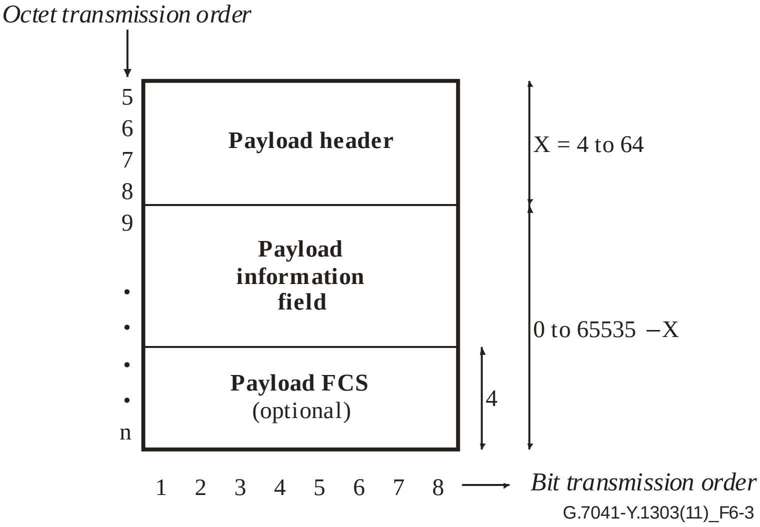


Figure 6-3 – GFP payload area format

Practical GFP maximum transmission unit (MTU) sizes for the GFP payload area are application specific. An implementation should support transmission and reception of GFP frames with GFP payload areas of at least 2 000 octets. By prior arrangement, consenting GFP implementations may use other MTU values. Implementations supporting frame-mapped fibre channel (FC) should support GFP payload areas of at least 2 156 octets.

6.1.2.1 Payload header

The payload header is a variable-length area, 4 to 64 octets long, intended to support data link management procedures specific to the higher-layer client signal. The structure of the GFP payload header is illustrated in Figure 6-4. The area contains two mandatory fields, the type and the type header error check (tHEC) fields, and a variable number of additional payload header fields. This group of additional payload header fields is referred to as the extension header. The presence of the extension header, and its format, and the presence of the optional pFCS are specified by the type field. The tHEC protects the integrity of the type field.

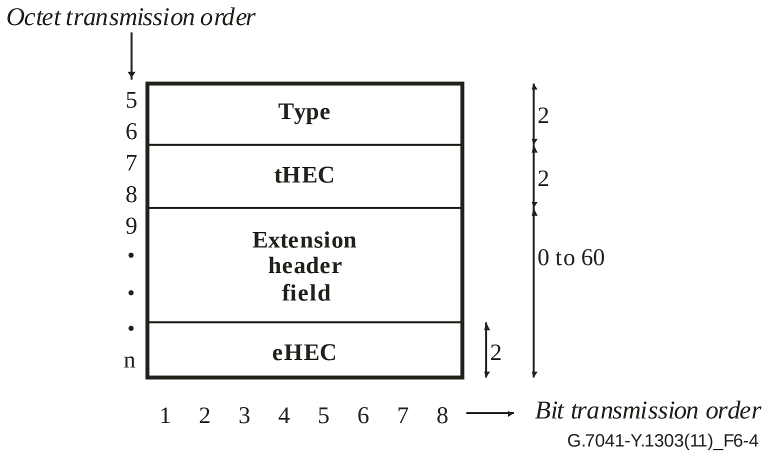


Figure 6-4 – GFP payload header format

An implementation shall support reception of a GFP frame with a payload header of any length in the range 4 to 64 octets.

6.1.2.1.1 GFP type field

The GFP type field is a mandatory two-octet field of the payload header that indicates the content and format of the GFP payload information field (see clause 6.1.2.2). The type field distinguishes between GFP frame types and between different services in a multi-service environment. As shown in Figure 6-5, the type field consists of a payload type identifier (PTI), a pFCS indicator (PFI), an extension header identifier (EXI) and a user payload identifier (UPI).

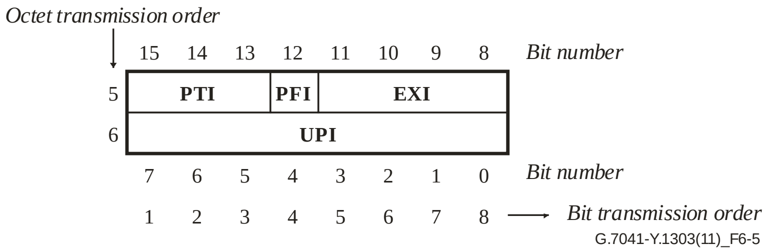


Figure 6-5 – GFP type field format

The interpretation of the UPI field for PTI values different from 000 or 100 is for further study. Sample type field values are illustrated in Appendix II.

6.1.2.1.1.1 Payload type identifier

This 3-bit subfield of the type field identifies the type of GFP client frame. Three kinds of client frames are currently defined, user data frames (PTI = 000), CMFs (PTI = 100) and management communication frames (PTI = 101). PTI codepoints are given in Table 6-1.

Table 6-1 – GFP payload type identifiers

Type bits <15:13>	Usage
000	User data
100	Client management
101	Management communications
Others	Reserved

6.1.2.1.1.2 Payload frame check sequence indicator

This one-bit subfield of the type field indicates the presence (PFI = 1) or absence (PFI = 0) of the pFCS field.

6.1.2.1.1.3 Extension header identifier (EXI)

This 4-bit subfield of the type field identifies the type of extension header GFP. Three kinds of extension headers are currently defined: a null extension header; a linear extension header; and a ring extension header. EXI codepoints are given in Table 6-2.

Table 6-2 – GFP extension header identifiers

Type bits <11:8>	Usage
0000	Null extension header
0001	Linear frame
0010	Ring frame
Others	Reserved

6.1.2.1.1.4 User payload identifier

This 8-bit field identifies the type of payload conveyed in the GFP payload information field. Interpretation of the UPI field is relative to the type of GFP client frame as indicated by the PTI subfield. UPI values for client data frames are specified in clause 6.1.3.1 and UPI values for CMFs are specified in clause 6.1.3.2.

6.1.2.1.2 Type headererror control field

The two-octet tHEC field contains a CRC-16 error control code that protects the integrity of the contents of the type field by enabling both single-bit error correction and multi-bit error detection. The type header consists of the type field and the tHEC.

The content of the tHEC field is generated using the same steps as the cHEC (see clause 6.1.1.2.1) with the following exception:

– for the tHEC, step 1 is modified such that $M(x)$ is formed from all the octets in the type field, excluding the tHEC field itself at the source, but including the tHEC field at the sink.

The GFP sink adaptation process shall perform single-bit error correction on the type field, which is protected by a tHEC field. The GFP sink adaptation process shall discard any of those GFP frames where multi-bit errors are detected. The sink adaptation process also updates any relevant system records for performance monitoring purposes.

6.1.2.1.3 GFP extension headers

The payload extension header is a 0-to-60 octet extended field [including the extension header error check (eHEC)] that supports technology-specific data link headers such as virtual link identifiers, source/destination addresses, port numbers, class of service (CoS) and extension header error control. The type of the extension header is indicated by the content of the EXI bits in the type field of the payload header.

Three extension header variants are currently defined to support client-specific data over a logical ring or logical point-to-point (linear) configurations.

This clause describes the various fields in each extension header. The default value for any undefined fields is 0 unless otherwise stated.

6.1.2.1.3.1 Null extension header

The payload header for a frame with a null extension header is shown in Figure 6-6. This extension header applies to a logical point-to-point configuration. It is intended for scenarios where the transport path is dedicated to one client signal.

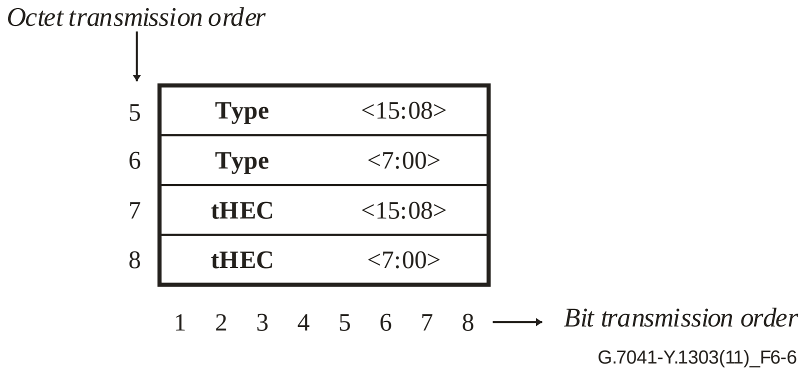


Figure 6-6 – Payload header for a GFP frame with a null extension header

6.1.2.1.3.2 Extension header for a linear frame

The payload header for a linear (point-to-point) frame with an extension header, shown in Figure 6-7, is intended for scenarios where there are several independent links requiring aggregation on to a single transport path.

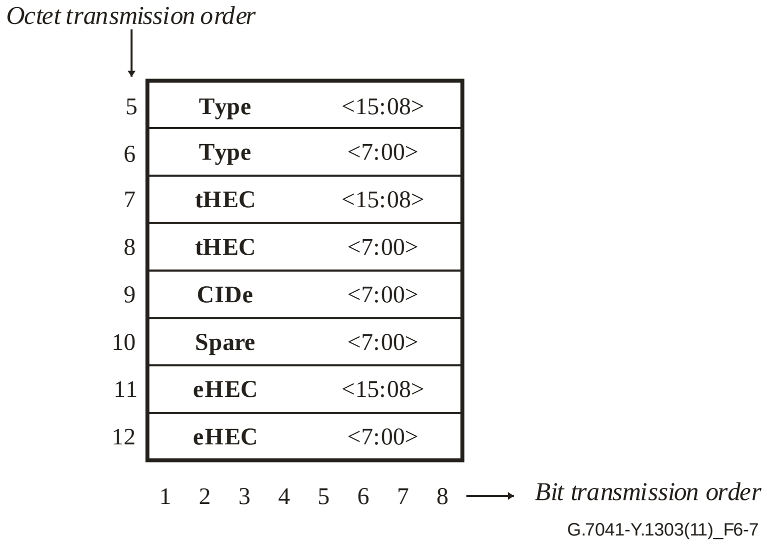


Figure 6-7 – Payload header for a linear (point-to-point) frame including the extension header

6.1.2.1.3.2.1 Channel ID field

The CID is an 8-bit binary number used to indicate one of 256 communication channels at a GFP termination point.

6.1.2.1.3.2.2 Spare field

The 8-bit spare field is reserved for future use.

6.1.2.1.3.2.3 Extension header error check field

See clause 6.1.2.1.4.

6.1.2.1.3.3 Extension header for a ring frame

For further study.

6.1.2.1.4 Extension header error check field

The two-octet eHEC field contains a CRC-16 error control code that protects the integrity of the contents of the extension headers by enabling both single-bit error correction (optional) and multi-bit error detection.

The content of the eHEC field is generated using the same steps as the cHEC (see clause 6.1.1.2.1) with the following exception:

– for the eHEC, step 1 is modified such that $M(x)$ is formed from all the octets in the extension header, but excluding the eHEC field itself.

The GFP sink adaptation process may perform single-bit error correction on all of the fields protected by a tHEC field. Single error correction is optional for the extension header. The GFP sink adaptation process shall discard any of those GFP frames where multi-bit errors are detected or where any error occurs in a header field that does not make use of single error correction. The sink adaptation process also updates any relevant system records for performance monitoring purposes.

6.1.2.2 Payload information field

The payload information field contains the framed PDU for frame-mapped GFP or, in the case of transparent GFP, a group of client signal characters. This variable-length field may include from 0 to 65 535 − X octets, where X is the size of the payload header. This field may include an optional pFCS field. The client PDU/signal is always transferred into the GFP payload information field as an octet-aligned packet stream.

6.1.2.2.1 Payload frame check sequence field

The GFP pFCS, as shown in Figure 6-8, is an optional, four-octet long, FCS. It contains a CRC-32 sequence that protects the contents of the GFP payload information field. The FCS generation process is defined in clause 6.1.2.2.1.1. A value of 1 in the PFI bit within the type field identifies the presence of the pFCS field.

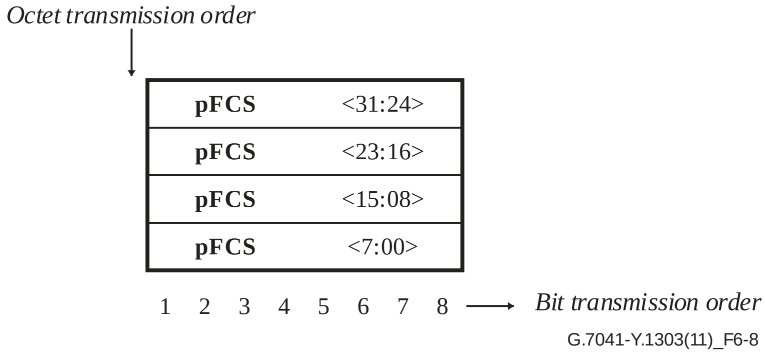


Figure 6-8 – GFP payload frame check sequence format

6.1.2.2.1.1 Payload frame check sequence generation

The pFCS is generated using the CRC-32 generating polynomial [ISO/IEC 13239] $G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x^{1} + 1$, where x^{32} corresponds to the MSB and x^{0} corresponds to the LSB.

The pFCS field is generated using the following steps.

1) The N octets from the GFP payload information field, excluding the FCS are taken in network octet order, MSB first, to form a $8N$-bit pattern representing the coefficients of a polynomial $M'(x)$ of degree $8N - 1$.

2) $M'(x)$ is multiplied by x^{32}, added to the product of x^{8N} and the all-1s polynomial $U(x) = 1 + x^1 + x^2 + ... + x^{31}$, and divided (modulo 2) by $G(x)$, producing a remainder $R(x)$ of degree 31 or less.

   NOTE – The addition of x^{8N} $[1 + x^1 + x^2 + ... + x^{31}]$ is equivalent to presetting the shift register to all-1s for typical shift register implementations using presets. Either method is equivalent to complementing the 32 MSBs of the GFP payload information field for the purpose of calculating the FCS.

3) The coefficients of $R(x)$ are considered to be a 32-bit sequence, where x^{31} is the MSB.

4) The complement of this 32-bit sequence is the CRC-32.

The sink adaptation process performs steps 1)–3) in the same manner as the source adaptation process. In the absence of errors, the remainder shall be 11000111_00000100_11011101_01111011, in the order x^{31} to x^0.

6.1.2.3 Payload area scrambling

Scrambling of the GFP payload area is required to provide security if the payload information happens to be the same as the scrambling word (or its inverse) from a frame-synchronous scrambler, such as those used in the SDH Reed-Solomon (RS) layer or in an OTN OPU*k* channel. Figure 6-9 illustrates the scrambler and descrambler processes.

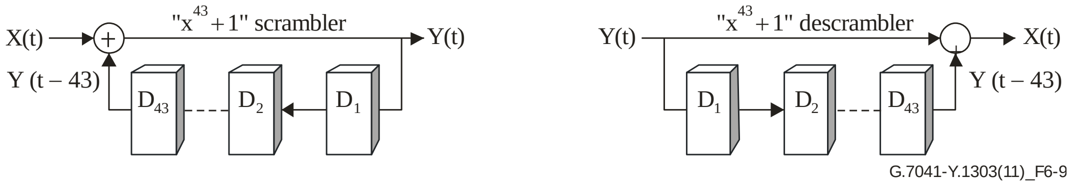


Figure 6-9 – x^{43}+1 scrambler and descrambler processes for GFP

All octets in the GFP payload area are scrambled using a $1 + x^{43}$ self-synchronous scrambler. Scrambling is done in network bit order.

At the source adaptation process, scrambling is enabled starting at the first transmitted octet after the cHEC field, and is disabled after the last transmitted octet of the GFP frame. When the scrambler or descrambler is disabled, its state is retained. Hence, the scrambler or descrambler state at the beginning of a GFP frame payload area will thus be the last 43 payload area bits of the GFP frame transmitted in that channel immediately prior to the current GFP frame.

The activation of the sink adaptation process descrambler also depends on the present state of the cHEC check algorithm:

a) in the HUNT and PRESYNC states, the descrambler is disabled;

b) in the SYNC state, the descrambler is enabled only for the octets between the cHEC field and the end of the candidate GFP frame.

NOTE – The GFP sink adaptation process can reliably forward GFP frames to the higher-layer entity only when the sink adaptation process is in the SYNC state.

6.1.3 GFP client frames

Two types of GFP client frames are currently defined, client data and client management. GFP client data frames are used to transport data from the client signal. GFP CMFs are used to transport information associated with the management of the client signal or GFP connection.

6.1.3.1 Client data frames

Client data is transported over GFP using client data frames. Client data frames are GFP client frames consisting of a core header and a payload area. The type field of the client data frames uses the following Type subfield values:

– PTI = 000
– PFI = Payload specific
– EXI = Payload specific
– UPI = Payload specific

The PFI shall be set as required depending on whether FCS is enabled or not. The EXI shall be set consistently with the frame multiplexing and topology requirements for the GFP connection. The UPI shall be set according to the transported client signal type. Defined UPI values for client data frames are given Table 6-3.

Table 6-3 – User payload identifiers for GFP client frames

PTI = 000 and 101 (See Notes 2 and 3)	
Type bits <7:0>	**GFP frame payload area**
0000 0000 and 1111 1111	Reserved and not available
0000 0001	Frame-mapped Ethernet
0000 0010	Frame-mapped PPP
0000 0011	Transparent fibre channel
0000 0100	Transparent FICON
0000 0101	Transparent ESCON/SBCON
0000 0110	Transparent Gbit Ethernet
0000 0111	Reserved for future use
0000 1000	Frame-mapped multiple access protocol over SDH (MAPOS)
0000 1001	Transparent DVB ASI
0000 1010	Framed-mapped IEEE 802.17 resilient packet ring
0000 1011	Frame-mapped fibre Channel FC-BBW
0000 1100	Asynchronous transparent fibre channel
0000 1101	Frame-mapped MPLS
0000 1110	See Note 6
0000 1111	Frame-mapped OSI network layer protocols (IS-IS, ES-IS, CLNP)
0001 0000	Frame-mapped IPv4
0001 0001	Frame-mapped IPv6
0001 0010	Frame-mapped DVB ASI
0001 0011	Frame-mapped 64B/66B encoded Ethernet, including the Ethernet frame preamble (see Note 4)
0001 0100	Frame-mapped 64B/66B encoded Ethernet ordered set information (see Note 5)
0001 0101	Transparent transcoded FC-1200 (see clause 17.8.2 of [ITU-T G.709])

Table 6-3 – User payload identifiers for GFP client frames

PTI = 000 and 101 (See Notes 2 and 3)	
Type bits <7:0>	**GFP frame payload area**
0001 0110	Precision time protocol (PTP) message
0001 0111	Synchronization status message (see clause 7.11 and Note 7)
0001 1000 through 1110 1111	Reserved for future standardization
1111 0000 through 1111 1110	Reserved for proprietary use (See Note 1)

NOTE 1 – The use of proprietary code values is described in Annex A of [ITU-T G.806].

NOTE 2 – The UPI value applies to the PDU in the payload area of that GFP frame.

NOTE 3 – Not all of these UPI types are applicable with PTI = 101.

NOTE 4 – The former [b-ITU-T G-Sup.43] description of this mapping recommended using UPI = 1111 1101.

NOTE 5 – The former [b-ITU-T G-Sup.43] description of this mapping recommended using UPI = 1111 1110.

NOTE 6 – This UPI value had been assigned to multicast MPLS frames, which is a mapping that is no longer applicable. This UPI value should not be used.

NOTE 7 – The same UPI is used for the both types of messages in 7.11. Both include a synchronization status message (SSM) octet, with the extended SSM appending additional message fields.

6.1.3.2 GFP client management frames

CMFs provide a generic mechanism for the GFP client-specific source adaptation process to optionally send CMFs to the GFP client-specific sink adaptation process. As illustrated in Figure 6-10, the CMFs are GFP client frames consisting of a core header and a payload area. The type field of the client data frames uses the following Type subfield values:

- PTI = 100
- PFI = Payload specific
- EXI = Payload specific
- UPI = Payload specific

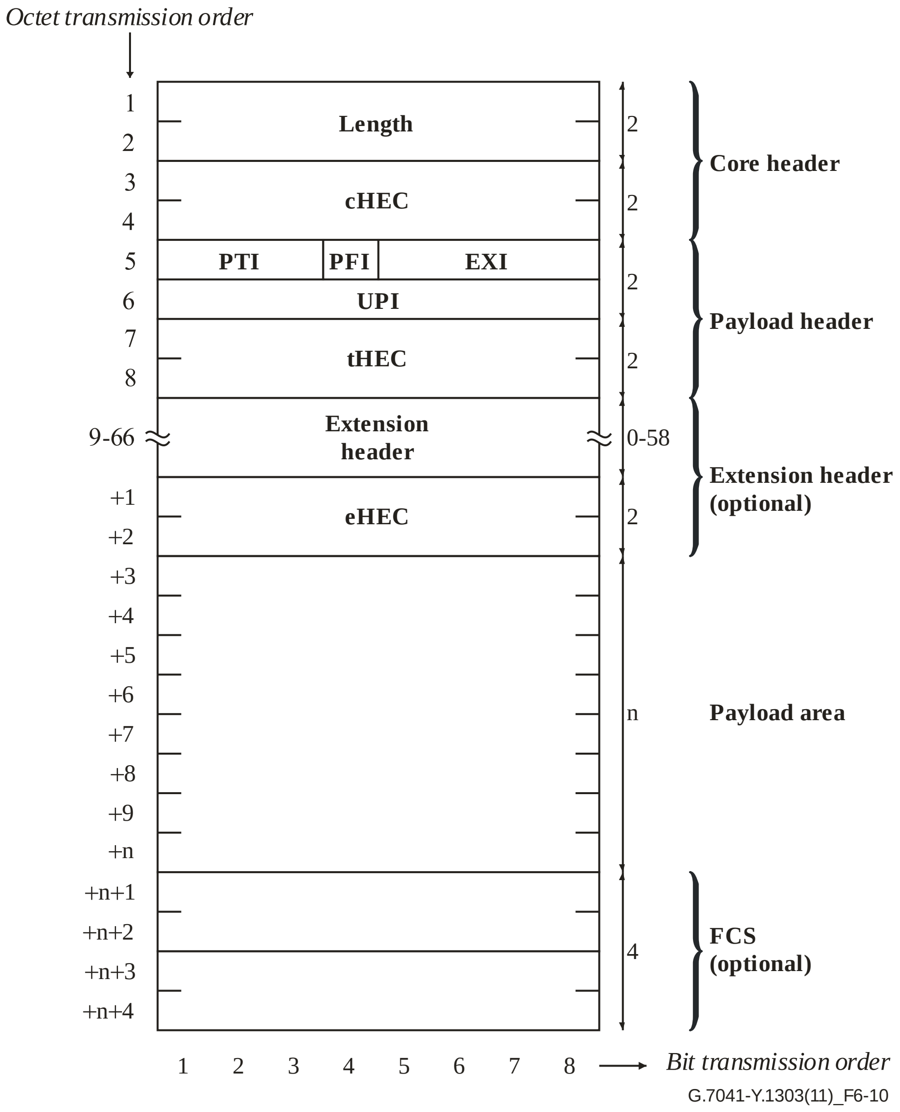


Figure 6-10 – GFP client management frame

For use as a GFP CMF, the PFI shall be set as required depending on whether FCS is enabled [note that the use of FCS in GFP CMFs reduces the amount of spare bandwidth (SBW) that can be used for such frames]. The extension header indicator (EXI) shall be set as required depending on whether the extension header is employed (note that the use of an extension header in the GFP CMF will significantly reduce the amount of SBW that can be used for such frames).

The UPI defines the use of the GFP CMF payload. In this way, the GFP CMF may be used for multiple purposes. Table 6-4 defines the GFP CMF payload uses.

Table 6-4 – GFP client management frame user payload identifier

PTI = 100	
UPI value	**Usage**
0000 0000 1111 1111	Reserved
0000 0001	Client signal fail (loss of client signal)
0000 0010	Client signal fail (loss of character synchronization)
0000 0011	Client defect clear indication (DCI)
0000 0100	Client forward defect indication (FDI)
0000 0101	Client reverse defect indication (RDI)
0000 0110 through 1101 1111	Reserved for future use
1110 0000 through 1111 1110	Reserved for proprietary use (Note)
NOTE – The use of proprietary code values is described in Annex A of [ITU-T G.806].	

6.2 GFP control frames

GFP control frames are used in the management of the GFP connection. The only control frame specified at this time is the GFP idle frame.

6.2.1 GFP idle frames

The GFP idle frame is a special four-octet GFP control frame consisting of only a GFP core header with the PLI and cHEC fields (see clause 6.1.1) set to 0, and no payload area. The idle frame is intended for use as a filler frame for the GFP source adaptation process to facilitate the adaptation of the GFP octet stream to any given transport medium where the transport medium channel has a higher capacity than required by the client signal. The GFP idle frame format is shown in Figure 6-11, with the parenthetical values indicating the values after the Barker-like scrambling has been performed.

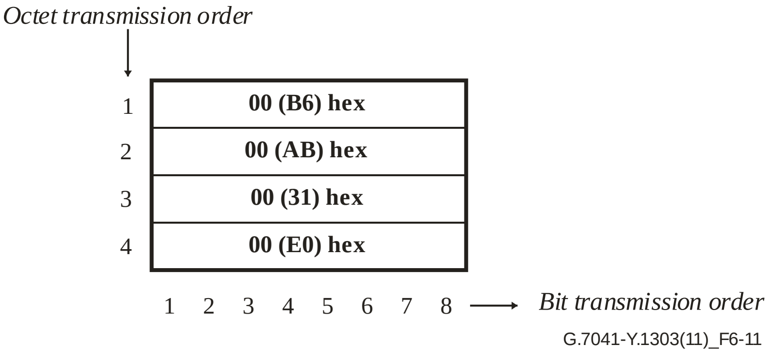


Figure 6-11 – GFP idle frame (Barker-like scrambled frame)

6.2.2 Other control frames

Control frames with PLI = 1, 2 or 3 are for further study.

6.3 GFP frame-level functions

This clause discusses frame-level processes common to all payloads that are framed via GFP. Processes specific to particular payloads are discussed in clauses 7 and 8. The relationships among these processes are illustrated in Figure 6-12.

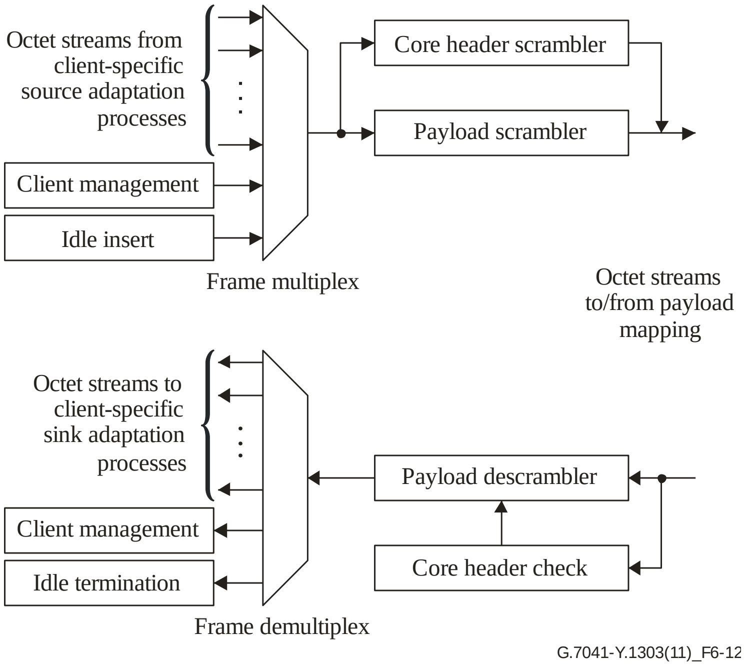


Figure 6-12 – GFP common (protocol-independent) procedures

6.3.1 GFP frame delineation algorithm

The GFP uses a modified version of the HEC algorithm specified in clause 7.3.3.2 of [ITU-T I.432.1] to provide GFP frame delineation. The frame delineation algorithm used in the GFP differs from that in [ITU-T I.432.1] in two basic ways:

a) the algorithm uses the PLI field of the GFP core header to find the end of the GFP frame; and

b) HEC field calculation uses a 16-bit polynomial and, consequently, generates a two-octet cHEC field.

GFP frame delineation is performed based on the correlation between the first two octets of the GFP frame and the embedded two-octet cHEC field. There are two alternative frame delineation methods, 6.3.1.1 and 6.3.1.2.

6.3.1.1 Frame delineation alternative using only the core header

Figure 6-13 shows the state diagram for the GFP frame delineation method based on only using the core header.

The state diagram works as follows:

1) In the HUNT state, the GFP process performs frame delineation by searching, octet-by-octet, for a correctly formatted core header over the last received sequence of four octets. The core header single error correction is disabled while in this state. Once a correct cHEC match is detected in the candidate PLI and cHEC fields, a candidate GFP frame is identified and the receive process enters the PRESYNC state.

2) In the PRESYNC state, the GFP process performs frame delineation by checking, frame-by-frame, for a correct cHEC match in the presumed core header of the next candidate GFP frame. The PLI field in the core header of the preceding GFP frame is used to find the beginning of the next candidate GFP frame. Core header single error correction remains disabled while in this state. The process repeats until DELTA consecutive correct cHECs are confirmed, at which point the process enters the SYNC state. If an incorrect cHEC is detected, the process returns to the HUNT state. The total number of consecutive correct cHECs required to move from the HUNT state to the SYNC state is therefore DELTA + 1.

3) In the SYNC state, the GFP process performs frame delineation by checking for a correct cHEC match on the next candidate GFP frame. The PLI field in the core header of the preceding GFP frame is used to find the beginning of the next candidate GFP frame. Single-bit core header error correction is enabled while in this state. Frame delineation is lost whenever multiple bit errors are detected in the core header by the cHEC. In this case, a GFP loss of frame delineation event is declared, the framing process returns to the HUNT state, and a client server signal failure (SSF) is indicated to the client adaptation process.

4) Idle GFP frames participate in the delineation process and are then discarded.

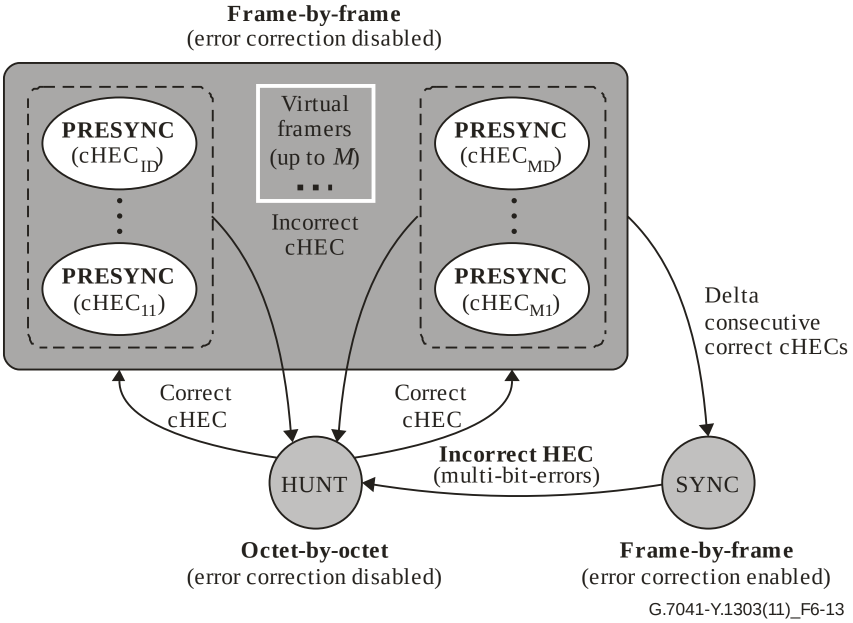


Figure 6-13 – GFP frame delineation state diagram

Robustness against false delineation in the re-synchronization process depends on the value of DELTA. A value of DELTA = 1 is suggested.

Frame delineation acquisition speed can be improved by the implementation of multiple "virtual framers", whereby the GFP process remains in the HUNT state and a separate PRESYNC sub-state is spawned for each candidate GFP frame detected in the incoming octet stream, as depicted in Figure 6-13.

6.3.1.2 Frame delineation alternative using both the core and type headers

An alternative algorithm uses both the core and type headers, as illustrated in Figure 6-14. This algorithm can be advantageous for high-speed interfaces that are typically protected by FEC and where circuit implementations often use wide data bus structures. The state machine works similarly to that shown in Figure 6-13, except for the PRESYNC state operation. That operation works as follows:

– In the PRESYNC state, the four octets following the candidate cHEC are checked:

  - if the candidate cHEC corresponds to a GFP Idle frame (i.e., PLI=0), and the subsequent four octets contain a valid cHEC, proceed to the SYNC state;
  - if the candidate cHEC does not correspond to a GFP Idle frame (i.e., PLI≠0), and the subsequent four octets contain a valid tHEC, proceed to the SYNC state;
  - otherwise, go back to the HUNT state.

  Error correction continues to be disabled for both the core and type headers during this state. The tHEC check requires retaining the 43 data bits immediately prior to the candidate cHEC, so that the tHEC value can be properly descrambled.

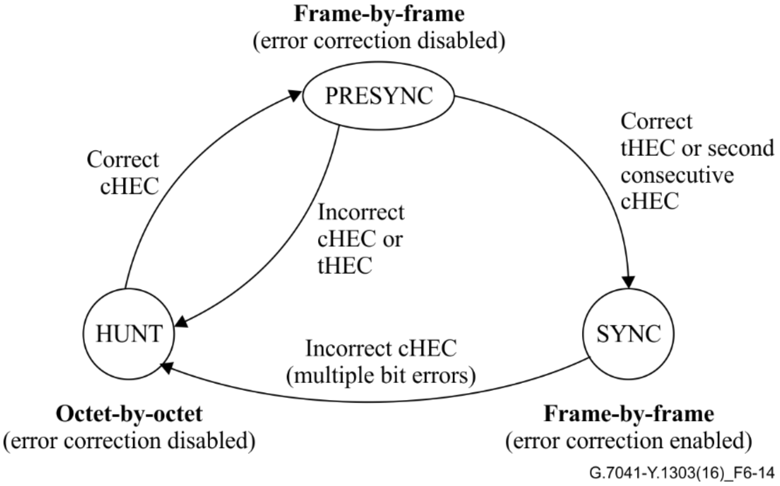


Figure 6-14 – GFP frame delineation state diagram using cHEC and tHEC

NOTE – The choice between the frame delineation algorithm alternatives is left to the implementer and shall not be a provisional option. Equipment developed prior to the 2012 version of this Recommendation used the frame delineation algorithm method based on only using the core header. Equipment developed subsequently may use either alternative.

6.3.2 Frame multiplexing

GFP frames from multiple ports and multiple client types are multiplexed on a frame-by-frame basis. The choice of scheduling algorithms is outside the scope of this Recommendation.

When there are no other GFP frames available for transmission, GFP idle frames shall be inserted, thus providing a continuous stream of frames for mapping into an octet-aligned physical layer.

6.3.3 Client signal fail and defect indications

The GFP provides a generic mechanism for a GFP client-specific source adaptation process to propagate indications of a client signal fail (CSF) or a local or remote client defect to the far-end GFP client-specific sink-adaptation process on detection of the condition.

6.3.3.1 Client signal fail indication

Detection rules for CSF events are, by definition, client-specific (see clauses 7 and 8). Upon detection, a GFP source adaptation process should generate a CMF (PTI = 100). The PFI subfield is set to 0 (no payload information field FCS) and the EXI subfield is set to the appropriate extension header type as applicable. The two types of CSF use the following UPI field values:

– loss of client signal (UPI = 0000 0001);

– loss of client character synchronization (UPI = 0000 0010).

Upon detection of the CSF condition, the GFP client-specific source adaptation process should send CSF indications to the far-end GFP client-specific sink adaptation process once every 100 ms $\leq T \leq$ 1 000 ms, beginning as soon as possible. When no client frames are available, GFP idle frames shall be transmitted before and between CSF frames.

Upon reception of the CSF indication, the GFP client sink adaptation process declares a sink CSF. Defect handling is discussed in clause 6.3.4.

The GFP client-specific sink adaptation process should clear the defect condition upon one of the following conditions:

1) no CSF frame is received in $N \times 1\,000$ ms (a value of 3 is suggested for N); or
2) upon receiving a valid GFP client data frame; or
3) upon receiving a DCI.

Handling of incomplete GFP frames at the onset of a CSF event should be consistent with the error handling procedures specified in clause 8.3 for transparent-mapped GFP and in clause 7.4 for frame-mapped GFP. The use of CSF with frame-mapped GFP is client-specific, as specified in clause 7.

6.3.3.2 Client link fault status indications

Two types of GFP CMF frames are defined to communicate the explicit client fault indication signals:[1]

- client reverse defect indication (RDI);
- client forward defect indication (FDI).

Detection rules for local and remote defect indications are client-specific and specified in clause 7. The format of these client link fault status signals is specified in the associated standards for the client signal. Upon detection of the explicit forward (reverse) client link fault status signal, the GFP client-specific source adaptation process should send an FDI (RDI) signal to the far-end GFP client-specific sink adaptation process. The FDI/RDI signal shall be sent once every 100 ms $\leq T \leq$ 1 000 ms, beginning as soon as possible. When no client frames are available, GFP idle frames shall be transmitted before and between FDI and RDI frames.

Upon reception of the FDI (RDI) signal, the GFP client sink adaptation process should regenerate the native forward (reverse) client link fault status signal towards the near-end client port to communicate the remote client link fault status information to the near-end client signal sink. The format of the egress client fault status signal is specified in the associated standards for that client signal interface.

The GFP client-specific sink adaptation process should clear the defect condition upon one of the following conditions:

1) no FDI (RDI) CMF frames are received in $N \times 1\,000$ ms (a value of 3 is suggested for N); or
2) receiving a valid GFP client data frame; or
3) receiving a DCI.

For the FDI and RDI, the PFI subfield is set to 0 (no payload information field FCS) and the EXI subfield is set to the appropriate extension header type, as applicable.

The process of client link fault status propagation is illustrated in Figure 6-15 (reverse fault) and Figure 6-16 (forward fault). The figures depict a typical link connection scenario between two client network elements (NE A and NE D) interconnected through a generic transport network. Client NE A connects to transport node NE B and client NE D connects to transport node NE C. Figure 6-15 depicts a scenario where client NE A detects a link fault in the D-to-A receive path and transmits a

---

[1] Note that neither loss of client signal nor loss of client synchronization are considered "explicit" client fault indications, since they are detected by the GFP client-specific source adaptation process.

well-defined client (reverse) link fault status indication for the reverse path over the A-to-D link connection towards NE D. Similarly, Figure 6-16 depicts a scenario where client NE D detects a link fault in its D-to-A transmit path and transmits a well-defined client (forward) link fault status indication for the transmit path over the D-to-A link connection towards NE A. The client link fault status indications are propagated by GFP-capable NEs by mapping the signalled client link fault indications into a corresponding RDI (Figure 6-15) or FDI (Figure 6-16) GFP CMF frame.

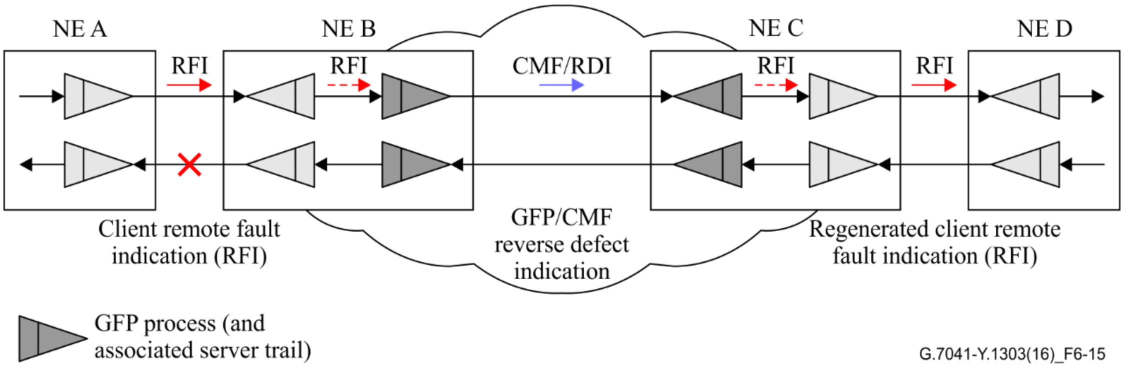


Figure 6-15 – Examples of a reverse defect indication of a client link fault status indication

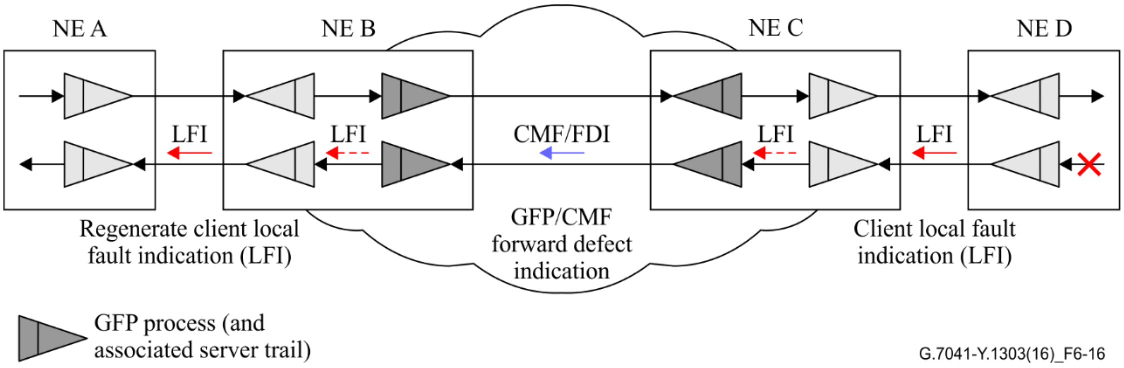


Figure 6-16 – Examples of a forward defect indication of a client link fault status indication

For instance, in Figure 6-15, the native client link fault status indication at transport node NE B is received by the GFP source adaptation process, mapped into a CMF RDI and then forwarded to the GFP sink adaptation process in transport node NE C. At NE C, the CMF RDI is extracted, mapped back into native client link fault status indication and regenerated in the port towards the near-end client NE D. Similarly, in Figure 6-16, the native client link fault status indication at transport node NE C is forwarded to the GFP source adaptation process, mapped into a CMF FDI client link fault status and then forwarded to the GFP sink process in transport node NE B. At NE B, the CMF FDI is extracted, mapped into the native client link fault status indication and regenerated back in the port toward NE A.

Note that processing of native client link fault status indications and its mapping into a GFP CMF for client link fault status indication can be based solely on near-end client link fault status information.

6.3.3.3 Client defect clear indications

In addition to the implicit defect clearance mechanisms in clause 6.3.3, the GFP also provides an explicit event-driven mechanism to help expedite clearance of native client link fault conditions called the client defect clear indication (DCI).

Clearance rules for native client link fault events are client-specific.

Upon detection of the native client link fault clearance event condition, the GFP client-specific source adaptation process may send a DCI signal to the GFP client-specific sink adaptation process. The

DCI should be sent as soon as possible upon detection of the defect clearing. Subsequent DCI frames may be transmitted. Interim frames shall be GFP idle frames when no client data frames are available.

Upon reception of the DCI signal, the GFP client sink adaptation process should stop inserting the native reverse (forward) client link fault clearance signal. If the standard for the associated client signal interface specifies a link fault clearance signal, the GFP client sink adaptation process should regenerate and transmit it to the near-end client port.

6.3.4 Defect handling in GFP

Figure 6-17 depicts the causal relationship between various defects detected or indicated by the GFP process. Trail signal fail (TSF) events refer to failure events detected in the SDH or OTN transport network as defined in [ITU-T G.783] and [ITU-T G.798]. GFP server signal fail events refer to GFP loss of frame delineation events as defined in the GFP state machine (clause 6.3.1) or propagation of TSF events to the GFP clients. CSF events refer to failure events detected in the client signal on ingress (communicated to the far-end by a CSF CMF) or egress (client-specific mapping defects such as payload errors, see clauses 7 and 8).

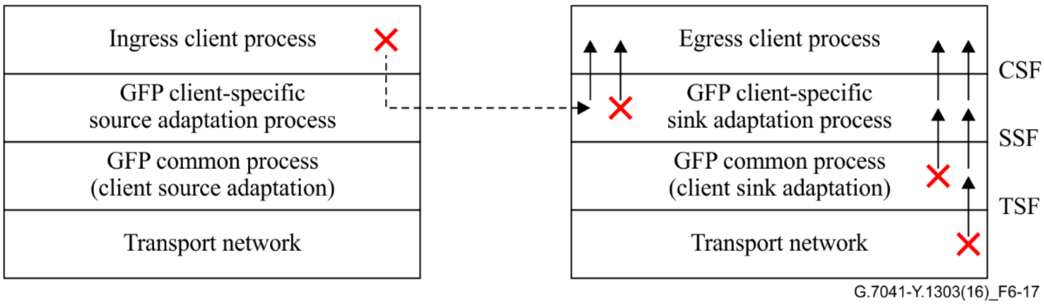


Figure 6-17 – Defect signal propagation in GFP

Upon detection of a TSF event or a GFP loss of frame delineation event, the GFP sink adaptation process generates a GFP SSF indication to its client-specific sink adaptation processes. These failure events are cleared as soon as the GFP process regains link synchronization.

Upon detection of CSF events other than a far-end CSF indication, the GFP client-specific sink adaptation processes should take client-specific (as well as server-specific) actions to deal with those failure events.

6.4 Management communications frame

Management communications frames (MCFs), which use PTI = 101, are used to provide an in-band management communications channel (MCC) capability between a GFP source and sink. The type of PDU s carried in these frames are identified by the UPI values specified in Table 6-3. The MCFs are for further study.

7 Payload-specific aspects for frame-mapped GFP

This clause describes those aspects of the generic encapsulation specific to the adaptation of client signals using a frame-by-frame mapping of the client payload into GFP.

7.1 Ethernet media access control payload

The format of Ethernet media access control (MAC) frames is defined in clause 3.1 of [IEEE 802.3]. There is a one-to-one mapping between a higher-layer PDU and a GFP PDU. Specifically, the boundaries of the GFP PDU are aligned with boundaries of the framed higher layer PDUs. This relationship between Ethernet MAC frames and GFP frames is illustrated in Figure 7-1.

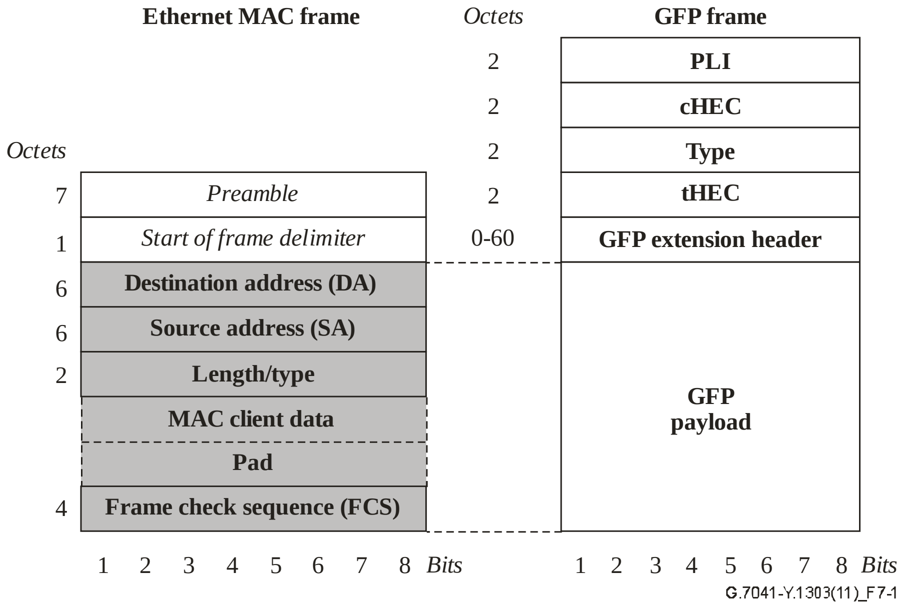


Figure 7-1 – Ethernet and GFP frame relationships

7.1.1 Ethernet media access control encapsulation

The Ethernet MAC octets from destination address through FCS, inclusive, are placed in the GFP payload information field. Octet alignment is maintained and bit identification within octets is maintained. Specifically, on an octet-by-octet basis, bits 0 and 7 in clause 3 of [IEEE 802.3] correspond to bits 8 and 1, respectively, in this GFP Recommendation.

7.1.2 Ethernet inter-packet gap deletion and restoring

The following rules apply to the deletion and restoration of Ethernet inter-packet gaps (IPGs) when the client is not a native frame-mapped GFP client.

1) IPGs are deleted before the Ethernet MAC frame is processed by the GFP source adaptation process and restored after the GFP frame is processed by the GFP sink adaptation process.

2) IPGs are deleted as the Ethernet MAC frame is extracted from the client bit stream. The extracted (decoded) Ethernet MAC frame is then forwarded to the GFP source adaptation process for subsequent encapsulation into a GFP frame.

3) IPGs are restored after the Ethernet MAC frame is extracted from the GFP frame by the GFP termination element. The extracted (uncoded) Ethernet MAC frame is then forwarded to the client layer for subsequent processing. IPGs are restored by ensuring that sufficient octets containing an idle pattern of 00 hex are present between consecutive received Ethernet MAC frames to meet the minimum receiver inter-frame gap (IFG) requirements. Minimum receiver IFG requirements are stated in clause 4.4 of [IEEE 802.3].

7.1.3 Client-specific signal fail aspects

Clauses 7.1.3.1 to 7.1.3.6 identify various client link fault conditions and define actions that should be taken at client signal egress in response to a corresponding CMF signal, or any client adaptation or transport defects that make it impossible to regenerate a client signal.

NOTE – For further details of processing these signals and consequent action, refer to [ITU-T G.8021] and [ITU-T G.806].

7.1.3.1 Common aspects for Ethernet clients

Upon detection of a loss of client signal by the GFP source adaptation process, CSF (loss of client signal) is transmitted until the client signal is restored, as described in clause 6.3.3.1.

Upon detection of a loss of client synchronization by the GFP source adaptation process, CSF (loss of client synchronization) is transmitted until character synchronization is regained, as described in clause 6.3.3.1.

NOTE – The insertion of RDI and FDI CMFs is specific to certain IEEE 802.3 physical layers, and is only applicable for GFP-F.

7.1.3.2 10BASE-FB client

The remote fault (RF) signal is defined in clause 17 of [IEEE 802.3]. When this signal is detected by the GFP source adaptation process, it causes CMF RDI frames to be inserted until the RF signal is no longer detected, as described in clause 6.3.3.2. When CMF RDI is received by the GFP sink adaptation process, it causes the RF signal to be output on the egress client signal.

7.1.3.3 100BASE-FX client or 100Base-TX over shielded twisted pair client

The far-end fault indication (FEFI) is defined in clauses 24.3.2.1 and 24.3.4 of [IEEE 802.3]. When this signal is detected by the GFP source adaptation process, it causes CMF RDI frames to be inserted until the FEFI signal is no longer detected, as described in clause 6.3.3.2. When CMF RDI is received by the GFP sink adaptation process, it is recommended that the FEFI signal be output on the egress client signal in order to cause far-end fault detection and the associated action at the downstream Ethernet receiver.

When the GFP sink adaptation process receives a CSF (loss of client signal) or any other transport failure events, the client adaptation process should transmit nothing, forcing loss of signal (LOS) detection and associated action at the downstream Ethernet receiver.

7.1.3.4 10/100/1000BASE-TX over unshielded twisted pair client

A link enabled to support the IEEE auto-negotiation process, defined in clause 28 of [IEEE 802.3], is considered failed if it fails to reach completion of the auto-negotiation process after it has started. The common behaviour for LOS described in clause 7.1.3.1 applies.

7.1.3.5 1000BASE-X client

Gigabit Ethernet physical media dependent (PMD) signal detect requirements are specified in clauses 38.2.4 and 39.2.3 of [IEEE 802.3] for fibre and copper interfaces, respectively. Conditions for declaring a client signal in or out of 8B/10B codeword synchronization are specified in clause 36.2.5.2.6 and Figure 36-9 of [IEEE 802.3].

When the GFP sink adaptation process receives a CSF (loss of client signal) or any other transport failure events, the GFP adaptation sink process should transmit nothing, forcing LOS detection and associated action at the downstream 1 Gbit/s Ethernet (1GbE) receiver.

A link enabled to support the IEEE auto-negotiation process, defined in clause 37 of [IEEE 802.3], is considered failed if it fails to reach completion of the auto-negotiation process after it has started. The common behaviour for LOS described in clause 7.1.3.1 applies.

When the GFP sink adaptation process receives a CSF (loss of character synchronization), it is recommended that the egress 1GbE transmitter continuously output the /V/ ordered set per clause 36.2.4.16 of [IEEE 802.3]. Alternatively, in response to the CSF (loss of character synchronization) condition, the client adaptation process may transmit nothing, forcing LOS detection and associated action at the downstream 1GbE receiver.

7.1.3.6 10G client

The local fault (LF) and RF signals are defined in clause 46.3.4 of [IEEE 802.3].

When the RF signal is detected by the GFP source adaptation process, it causes CMF RDI frames to be inserted until the RF signal is no longer detected, as described in clause 6.3.3.2. When CMF RDI is received by the GFP sink adaptation process, it is recommended that the RF signal be output on the 10 Gbit Ethernet egress client signal.

When the LF signal is detected by the GFP source adaptation process, it causes CMF FDI frames to be inserted until the LF signal is no longer detected, as described in clause 6.3.3.2. When a CMF FDI is received by the GFP sink adaptation process, it is recommended that the LF signal be output on the 10 Gbit Ethernet egress client signal.

Note that clause 46.3.4.3 of [IEEE 802.3] specifies that the LF or RF should go away within 0.7 µs of the fault clearing. Consequently, it is appropriate to send a DCI immediately after detecting that the link is healthy again.

10GBASE-R client signals use ordered sets to communicate detected remote and LF indications. The 10GBASE-R mapping specified in this clause (UPI = 0000 0001) does not preserve ordered set information and consequently communicates the 10GBASE-R remote and LF information between the GFP source and sink through GFP CMF RDI and FDI frames. The 10GBASE-R mapping specified in 7.9 (UPI = 0001 0011 and 0001 0100) preserves the ordered set information. Consequently, it does not use GFP CMF RDI or FDI frames, but passes the client signal's ordered sets for this purpose.

7.2 HDLC/PPP payload

The direct mapping of high-level data link control/point-to-point protocol (HDLC/PPP) into GFP is intended for applications that wish to transport HDLC/PPP frames in their native mode. HDLC/PPP payloads are natively encapsulated into an HDLC-like frame. The format of a PPP frame is defined in clause 2 of [IETF RFC 1661]. The format of the HDLC-like frame is defined in clause 3 of [IETF RFC 1662]. Unlike [IETF RFC 1662], no octet stuffing procedure is performed to identify flag or control escape characters during the GFP adaptation process. There is a one-to-one mapping between a higher-layer PPP/HDLC PDU and a GFP PDU. Specifically, the boundaries of the GFP PDU are aligned with boundaries of the framed higher layer HDLC/PPP PDUs. This relationship between the HDLC/PPP frame and the GFP frame is illustrated in Figure 7-2.

Similar clients, such as MAPOS, are mapped in the same manner as PPP frames.

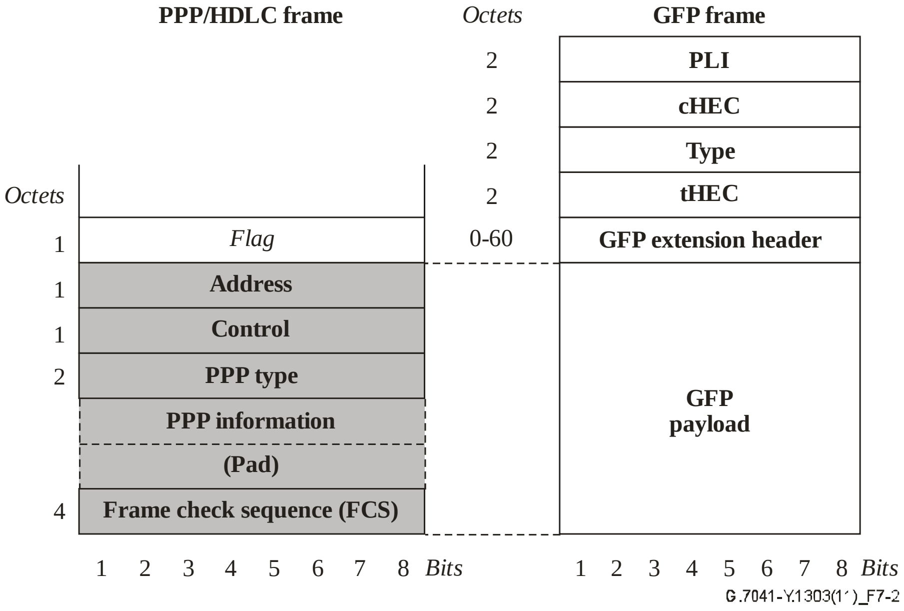


Figure 7-2 – HDLC/PPP and GFP frame relationships

7.2.1 PPP frame encapsulation

All octets from the PPP/HDLC frame, including any optional PPP information field padding, are placed in the payload information field of a GFP frame. Octet alignment is maintained and bit identification within octets is also maintained. Bits 0 and 7 of the PPP/HDLC byte (see [ISO/IEC 13239]) correspond to bits 8 and 1 of the GFP payload byte, respectively.

7.2.2 GFP/HDLC delineation interworking

GFP does not rely on flag characters, and associated control escape octet, for frame delineation purposes. The following rules apply to the processing of octet-synchronous HDLC frames by a GFP/HDLC interworking function:

1) Flags and associated control escape octets are removed (as specified in clause 4.2 of [IETF RFC 1662]) as the PPP/HDLC frame is extracted from the incoming client octet stream. The extracted (decoded) PPP/HDLC frame is then forwarded to the GFP source adaptation process for subsequent encapsulation into a GFP frame.
2) The GFP extracts the PPP/HDLC frame from the GFP frame. The extracted (uncoded) PPP/HDLC frame is then forwarded to the client layer for subsequent processing. Flags and control escape characters are then restored by inserting flag characters (e.g., hexadecimal 0x7e) and escape control characters (e.g., hexadecimal 0x7d) as specified in clause 4 of [IETF RFC 1662].

7.2.3 PPP payload configuration options

Modifications to the PPP/HDLC-like frame format may be negotiated using the link control protocol (LCP) configuration option procedures as defined in clause 6 of [IETF RFC 1661]. For example, the format of the GFP frame after a successful negotiation of the address-and-control-field-compression (ACFC) configuration option is illustrated in Figure 7-3. Such configuration procedures are client-specific and transparent to the GFP process.

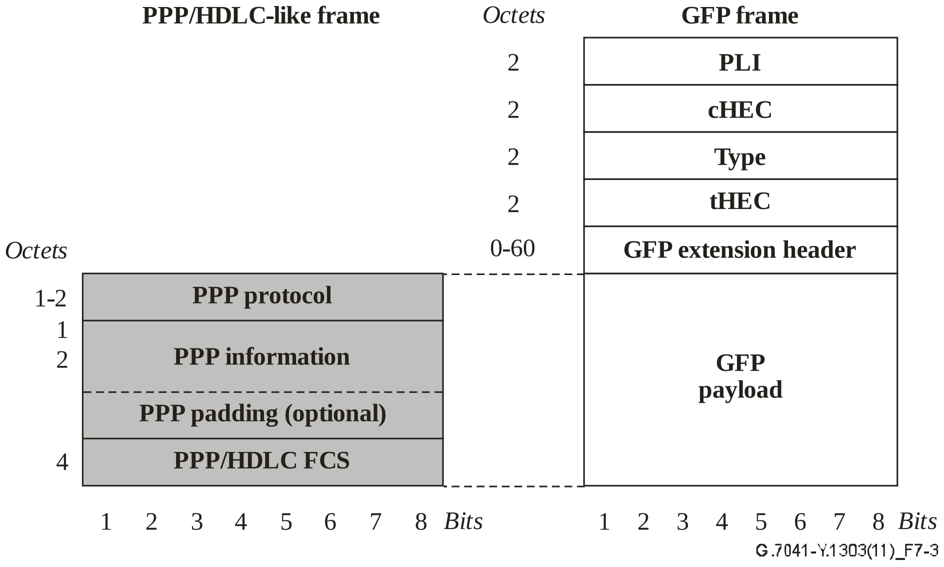


Figure 7-3 – PPP/HDLC and GFP frame relationships (with PPP's ACFC configuration option)

7.3 Fibre channel payload via FC-BBW_SONET

The format of an FC broadband-2_SONET (FC-BBW_SONET) PDU is defined in clause 6 of [ISO/IEC 14165-241]. For the purposes of GFP-F-based adaptation, a one-to-one mapping is assumed between FC PDUs and FC-BBW_SONET PDUs (as per the FC-BB specification), and between FC-BBW_SONET PDUs and GFP PDU (as per this Recommendation). Only the mapping relationship between the FC-BBW_SONET PDU and the GFP PDU is specified in this Recommendation.

7.3.1 FC-BB-2_SONET PDU encapsulation

All octets in the FC-BBW_SONET PDU, starting from the LLC/SNAP_Header to the backbone WAN (BBW) message payload, inclusive, are placed in the payload information field of a GFP frame. Both octet alignment and bit identification within octets are maintained within the GFP PDU. The construction of the BBW_Header and the BBW message payload (if present) for the FC-BBW_SONET PDUs are specified in [ISO/IEC 14165-241]. This relationship between FC-BBW_SONET frames and GFP frames is illustrated in Figure 7-4.

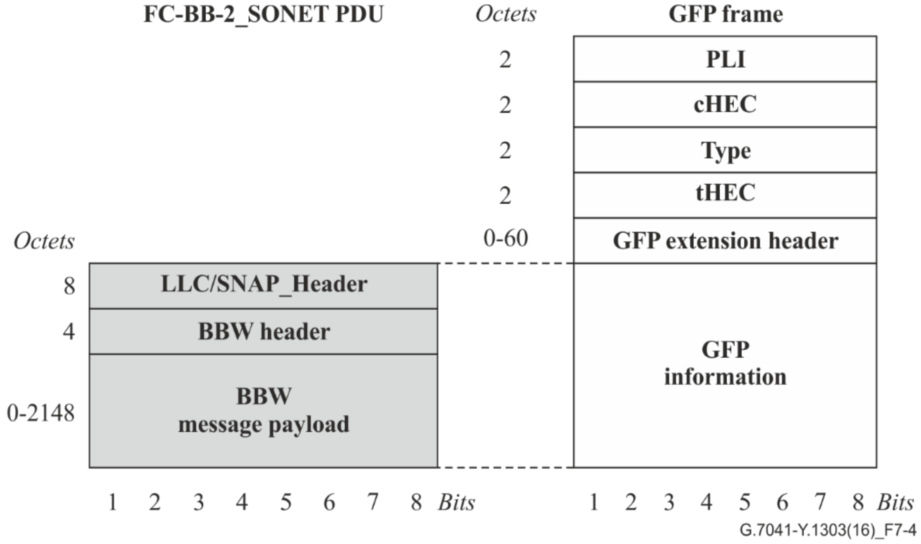


Figure 7-4 – Fibre channel broadband-2 SONET (FC-BBW_SONET) and GFP frame relationships

7.4 Error handling in frame-mapped GFP

On ingress, PDUs detected in error before transmission by the client source adaptation process should be discarded. PDUs detected in error while in transmission by the client source adaptation process should be padded with an all-1s bit sequence and transmitted with a pFCS that has all 32-bits complemented, when present. These actions ensure that the termination GFP process, or the client end, will drop the errored PDU.

7.4.1 Client-specific signal fail aspects

When frame-mapped GFP source adaptation process detects a CSF at ingress, the preferred action is to output the appropriate client signal AIS if available.

In the case where no client alarm indication signal (AIS) is available, it is possible to generate a CMF[csf] at the GFP-F source adaptation process, which may send a "client signal fail" indication as described in clause 6.3.3. Other implementation-dependent indications of a failed client signal (e.g., loss-of-clock from an interface between integrated circuits) may be encoded as client signal fail.

NOTE – For further details of processing this signal and consequent action, refer to [ITU-T G.8021] and [ITU-T G.806].

7.5 IEEE 802.17 resilient packet ring payload

The format of resilient packet ring (RPR) frames is defined in clause 8 of [IEEE 802.17]. There is a one-to-one mapping between a RPR frame and a GFP PDU. For clarity, this relationship between RPR frames and GFP frames is illustrated in Figure 7-5.

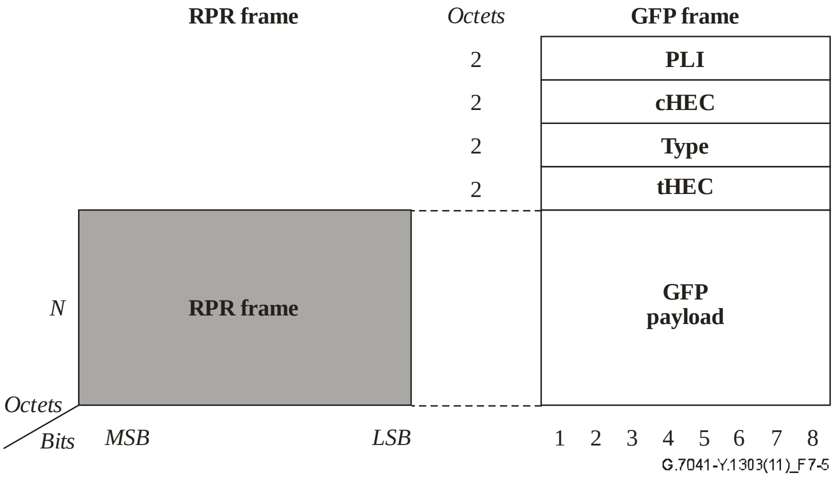


Figure 7-5 – RPR and GFP frame relationships

7.5.1 RPR encapsulation

All of the RPR frame octets (as defined in clause 8 of [IEEE 802.17]) are placed in the GFP payload information field. The default is no header extension and the pFCS field is not used. Octet alignment is maintained and bit identification within octets is maintained. Specifically, on an octet-by-octet basis, the LSB and MSB in clause 8 and Annex C of [IEEE 802.17] correspond to bits 8 and 1, respectively, in this GFP Recommendation. A complete definition of this encapsulation is contained in Annex C of [IEEE 802.17].

7.6 Direct mapping of multiprotocol label switching into GFP-F frames

The direct mapping of multiprotocol label switching (MPLS) into GFP is intended for applications that wish to transport MPLS-shim PDUs directly over a transport network such as OTN, SDH, or PDH. The MPLS PDU contains one or more MPLS-specific label stack entries (as specified in [IETF RFC 3032]) and an MPLS payload information field. All octets in the MPLS PDU are placed in the payload information field of a GFP-F frame. Both octet alignment and bit identification within octets are maintained within the GFP-F PDU. This direct mapping of MPLS into GFP is intended to be the default mapping when MPLS client signals are directly carried over a transport network.

The GFP pFCS is required and is computed as specified in clause 6.1.2.2.1.1 and inserted into the pFCS field. The PFI field is set to 1.

This relationship between MPLS PDU and GFP-F frames is illustrated in Figure 7-6.

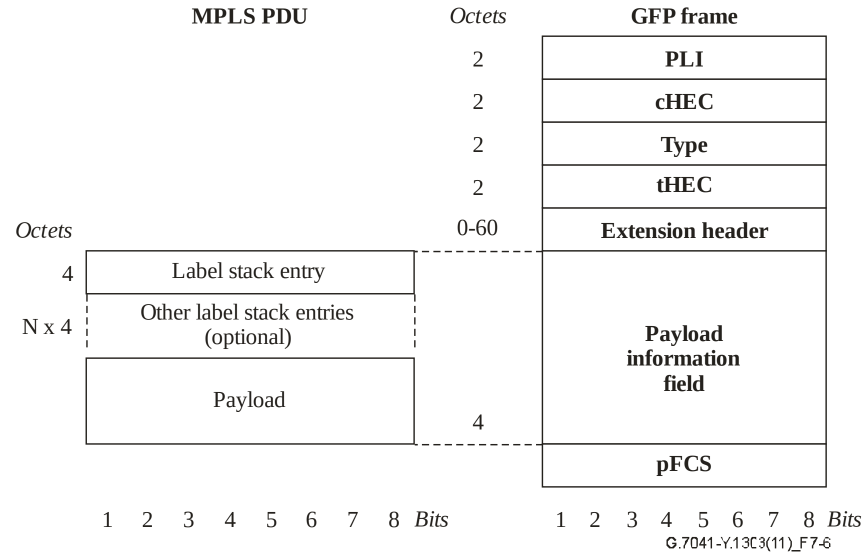


Figure 7-6 – MPLS PDU and GFP frame relationships

7.7 Direct mapping of IP and OSI network layer PDUs into GFP-F frames

The direct mapping of IPv4, IPv6 and open systems interconnection (OSI) network layer PDUs into GFP is intended for applications that wish to transport IP/OSI PDUs directly over SDH containers. The IPv4 PDU [IETF RFC 791], IPv6 PDU [IETF RFC 2460], CLNP PDU [ITU-T X.233], end system-to-intermediate system (ES-IS) PDU [ISO 9542] and intermediate system-to-intermediate system (IS-IS) PDU [ISO/IEC 10589] contain one or more client-specific header entry and a client payload information field. All octets in the client PDU are placed in the payload information field of a GFP-F frame. Both octet alignment and bit identification within octets are maintained within the GFP-F PDU.

The GFP pFCS is required and is computed as specified in clause 6.1.2.2.1.1 and inserted in the pFCS field. The PFI field is set to 1. This relationship between the IPv4, IPv6 or OSI network layer PDUs and GFP-F frame is illustrated in Figure 7-7.

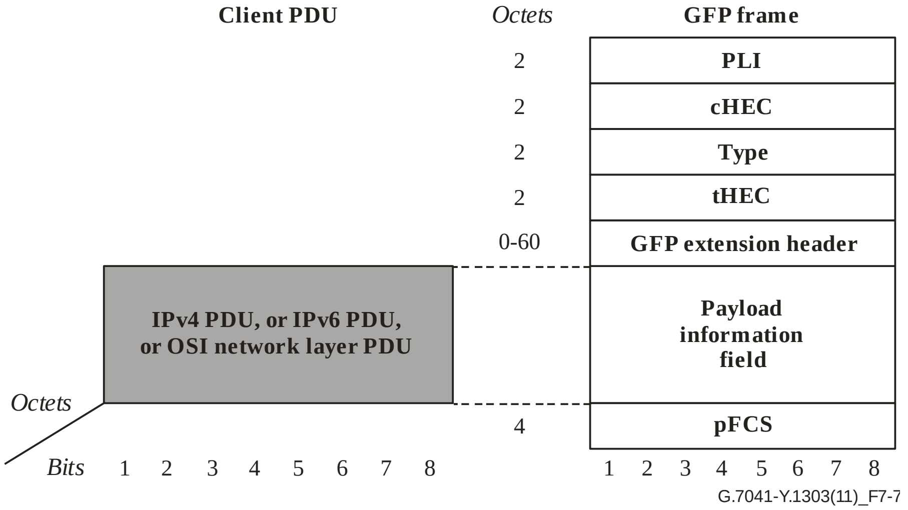


Figure 7-7 – IPv4/IPv6/OSI network layer PDUs and GFP frame relationships

7.8 DVB ASI payload

The formats of transport stream (TS) packets are defined in [EN 50083-9] as either 188 bytes or 204 bytes, the latter being referred to as RS-coded TS packets. There is a one-to-one mapping between a TS packet (or a RS-coded TS packet) and a GFP PDU. Specifically, the boundaries of the GFP PDU are aligned with boundaries of the TS packet (or of the RS-coded TS packet). This relationship between TS packets (or RS-coded TS packets) and GFP frames is illustrated in Figure 7-8.

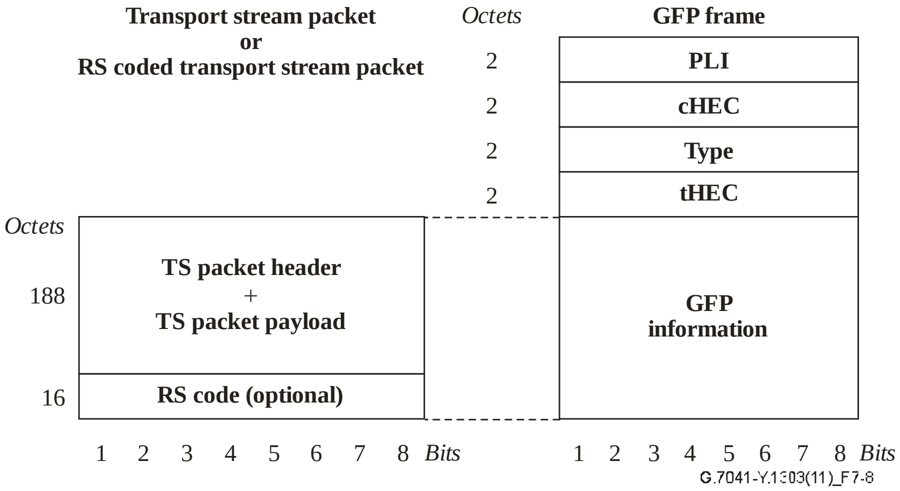


Figure 7-8 – TS packet and GFP frame relationships

7.8.1 DVB ASI encapsulation

The 188 or 204 TS packet octets are placed in the GFP payload information field. Octet alignment is maintained and bit identification within octets is maintained with respect to [ITU-T H.222.0]. Specifically, on an octet-by-octet basis, data bits d7 and d0 (corresponding to 8B information characters H and A) in [EN 50083-9] for a digital video broadcast asynchronous serial interface (DVB ASI) correspond to GFP payload byte bits 1 and 8, respectively.

7.8.2 DVB ASI operations

7.8.2.1 DVB ASI ingress interface operations

At the ingress interface, the data bytes and their clock are recovered from the received DVB ASI signal; the processing includes: optical receiver (for fibre-optic-based links) or coupling/impedance matching (for coaxial cable), amplifier/buffer, clock/data recovery and serial-to-parallel conversion, FC comma deletion, 8B/10B decoding, as specified in Annex B of [EN 50083-9].

7.8.2.1.1 DVB ASI loss of light

By reference to FC standards, DVB ASI LOS is an implementation-dependent option. When supported, applicable loss of light (LOL) and signal detect requirements are found in clauses 5.6, 6.2.3.2 and H.10 of [ANSI INCITS 230].

7.8.2.1.2 DVB ASI 8B/10B loss of synchronization

Per Appendix B of [EN 50083-9], DVB ASI codeword synchronization shall be achieved on receipt of two /K28.5/ characters having the same alignment within five consecutive received characters. Enterprise systems connection/single-byte command code sets connection (ESCON/SBCON) character-based codeword loss-of-synchronization criteria should be those specified in clause 7.1 of [ANSI INCITS 296].

NOTE – [EN 50083-9] does not specify criteria for declaring loss of codeword synchronization. FC criteria may not be applied since DVB ASI codeword synchronization and transmission is character based, rather than 4-character transmission word based.

7.8.2.2 TS packet ingress operations

The function realizes the synchronization acquisition of the MPEG-2-TS packets or of the RS-coded MPEG-2 TS packets, on the basis of the method proposed in clause 5.2 of [ETSI TR 101 290] (five consecutive correct synchronization bytes for synchronization acquisition; two or more consecutive corrupted synchronization bytes should indicate synchronization loss).

The packet size (188 bytes or 204 bytes) may be recovered from the received signals on the basis of the periodicity of the synchronization bytes.

In the case of ingress client failure (either LOS or loss of character synchronization or loss of packet synchronization) it is not possible to delineate any packet; in fact, the impossibility to delineate packets causes the generation of GFP idle frames only.

GFP-F encapsulation function uses PFI = "0" (no pFCS) and EXI = "0000" (null extension header).

7.8.2.3 TS packet egress operations

At the egress interface, the GFP-F de-encapsulation function removes the core header, de-scrambles the payload area, then passes the TS packet (or the RS-coded TS packet) to the next block also in the case of uncorrectable tHEC assuming the default type conditions. The type of packet (MPEG-2 TS packet or RS-coded MPEG-2 TS packet) is determined on the basis of the length of the received GFP frame.

In order to recover the TS packet (or RS-coded TS packet) timing information and to remove received packet jitter (due to GFP idle frames, pointer movements, etc.), an end-to-end synchronization method is required. The method to be used is the adaptive clock method described in [ITU-T I.363.1].

NOTE – This method is appropriate because it is not necessary in the case of the transport of compressed video programmes to comply with the wander specifications of [b-ITU-T G.823]. Furthermore, the adaptive clock method does not rely on the availability of an external reference clock. End-to-end synchronization of the TS packets (or of the RS-coded TS packets) can be recovered on the basis of arrival time of received GFP frames.

The transport packet jitter shall meet the jitter requirements specified in [ISO/IEC 13818-9].

7.8.2.4 DVB ASI egress interface operations

The processing includes 8B/10B coding, FC comma symbols insertion, parallel-to-serial conversion, amplifier buffer and optical emitter (for fibre-optic-based links) or coupling/impedance matching (for coaxial cable), as specified in Annex B of [EN 50083-9].

The running disparity (RD) aspects shall adhere to the FC standard, which are found in clause 11 of [ANSI INCITS 230].

When the receiving buffer underflows, the egress DVB ASI transmitter should continuously output the 10B neutral disparity codeword, depending on the beginning running disparity (RD– or RD+), following the rules described in clause 8.1.1.1, forcing loss-of-synchronization detection and any associated action at the downstream DVB ASI receiver.

7.9 Transporting Ethernet 10GBASE-R payloads with preamble transparency and ordered set information

The mapping of this clause is defined for applications where there is a requirement to preserve the Ethernet frame preamble and ordered set information when the 10GBASE-R signal is carried by GFP-F in addition to the Ethernet frames. This preamble and ordered set information is not defined to be part of the Ethernet frame by [IEEE 802.3], and consequently is not carried by GFP-F in the Ethernet frame-based mapping defined in clause 7.1.

7.9.1 Using 64B/66B information to delimit data and ordered sets

A 10GBASE LAN signal is made up of several layers:

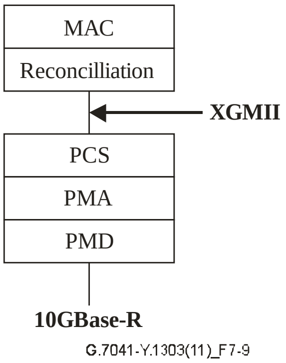


Figure 7-9 – 10GBASE-R LAN model

The physical coding sublayer (PCS) is described in clause 49.2 of [IEEE 802.3], including the delimiting of data frames and ordered sets.

7.9.2 GFP-F encapsulation

As shown in [IEEE 802.3] Figure 46-3, the Ethernet data stream at the XGMII consists of: <inter-frame><preamble><sfd><data><efd>. For the purposes of these mappings, the client data frames include the <preamble><sfd><data> information, and the ordered sets include specific information carried in the <inter-frame> characters. The mapping of both client data frames and ordered sets into GFP-F frames is described in this clause. Each GFP-F frame uses the core header and type header. The GFP type field is shown in Figure 6-5. The UPI field indicates data or ordered sets. The rest of the fields are static:

- PTI = 000 (client data)
- PFI = 0 (no FCS)
- EXI = 0000 (null extension header)

The functional model of the mapping is illustrated in Figure 7-10. EthPP represents the Ethernet PDU with its preamble and EthOS represents the Ethernet ordered set information. Note that there is no Ethernet MAC termination function. Consequently, since no error checking is performed on the Ethernet MAC frames, errored MAC frames are forwarded at both the ingress and egress to the GFP adaptation functions.

NOTE 1 – Since no MAC function exists at the GFP source or sink, Ethernet auto-negotiation is performed between Ethernet terminals across the GFP link rather than between the Ethernet terminal and the GFP source/sink equipment.

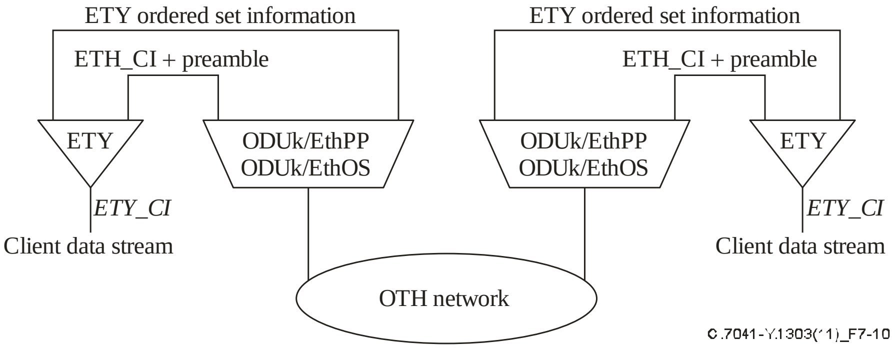


Figure 7-10 – Functional model for mapping 10GBASE-R information into the ODUk

NOTE 2 – The Ethernet control codes such as idle, error and the reserved codes are not transferred.

At the egress from the GFP sink adaptation process, the IEEE 802.3 rules shall be observed in the reconstituted Ethernet data stream, including the appropriate insertion of IFG characters.

7.9.2.1 Client data frame encapsulation

Unlike the Ethernet frame mapping specified in clause 7.1, this mapping includes the Ethernet frame preamble information in the GFP-F payload area along with the client Ethernet data frame. See Figure 7-11. As specified in clause 46.2 of [IEEE 802.3], the preamble consists of seven octets beginning with the /S/ (start) control character and followed by the start of frame delimiter (SFD) character. Since the /S/ control character is always present at the beginning of the preamble, as shown in Figure 7-11, it is mapped as a fixed value of 0x55 when it is inserted into the GFP-F frame. The SFD character is included, however, to ensure there is no ambiguity regarding the beginning of the client data frame. Specifically, the six preamble octets and the SFD are pre-pended to the Ethernet data frame in their network octet transmission order. Consistent with the Ethernet data mapping into GFP, the bit order of each octet is mapped such that preamble/SFD octet bit 7 corresponds to GFP octet bit 1 and preamble/SFD octet bit 0 corresponds to GFP octet bit 8.

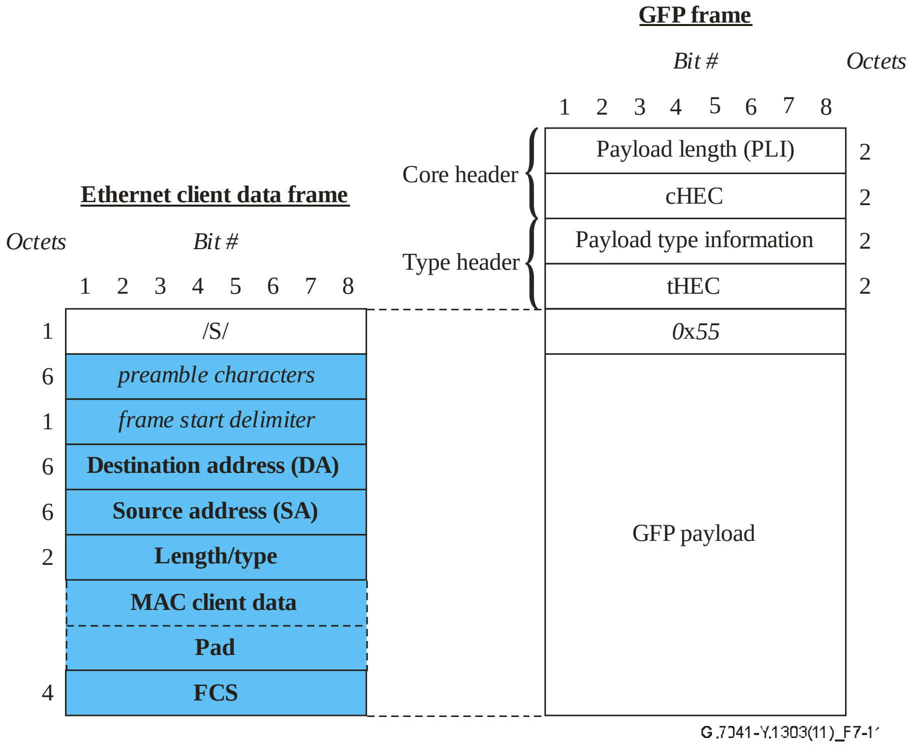


Figure 7-11 – Ethernet client data frame and preamble mapping into GFP-F

7.9.2.2 Ordered set encapsulation

The 10 Gbit Ethernet ordered set is defined in clause 49.2.4 of [IEEE 802.3]. An ordered set consists of four octets, beginning with a special character (/O/) followed by three data octets. Each ordered set is mapped into its own GFP-F frame, as shown in Figure 7-12. The first octet of the ordered set has the four MSBs set to all-zeros and the four LSBs equal to the O code. This way both sequence ordered sets (O code = 0000) and signal ordered sets (O code = 1111) can be transferred. The next three octets contain the three data bytes of the ordered set. The ordered set octets are mapped into the GFP payload area in network octet transmission order. Consistent with the Ethernet data mapping into GFP, the bit order of each octet is mapped such that ordered set octet bit 7 corresponds to GFP octet bit 1 and ordered set octet bit 0 corresponds to GFP octet bit 8.

During a link fault condition, clause 46.3.4 of [IEEE 802.3] specifies that the fault be signalled by continuously transmitting the appropriate fault status ordered set. The additional bandwidth required for the GFP encapsulation prevents all of the ordered sets from being transmitted. However, since the stream of ordered sets is continuous, [IEEE 802.3] allows some of these ordered sets to be discarded as long as some are passed to the Ethernet sink to communicate the link status. The GFP source adaptation process shall encapsulate and transmit these link status ordered sets as bandwidth allows, and discard others. In the same manner as for all ordered sets, the GFP sink adaptation process shall convert the ordered set information it receives in a GFP frame into an ordered set that is transmitted on the 10GBASE-R egress link.

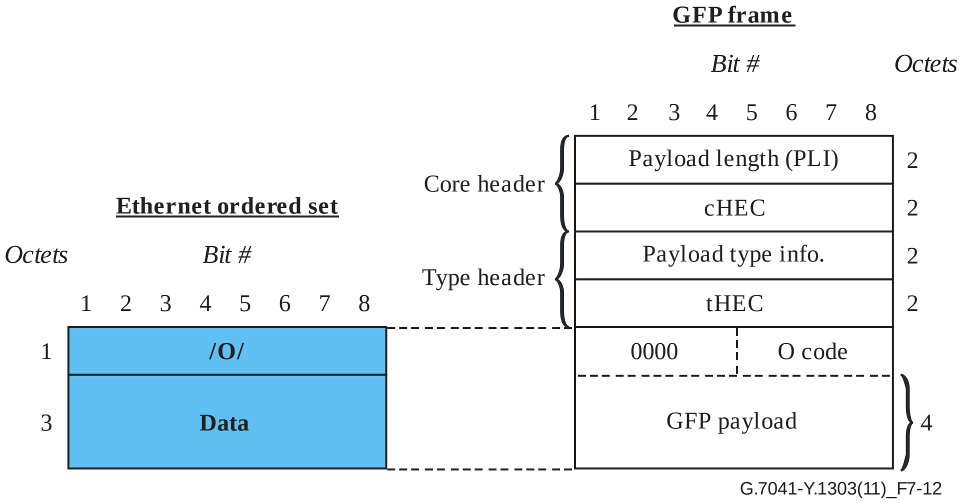


Figure 7-12 – Ethernet ordered set mapping into GFP-F

7.9.2.3 Fault handling

There are three types of Ethernet PCS faults that can be detected at the ingress to the GFP source adaptation process:

- LOS
- loss of codeword synchronization
- high bit error rate

When any of these conditions is detected, GFP client signal fail frames are sent from the GFP source to the GFP sink as specified in clause 6.3. The consequent action of the 10GBASE-R source at the egress of the GFP sink adaptation function is for further study.

NOTE – The response to the reception of /E/ error termination characters is not defined.

7.10 Precision time protocol

The precision time protocol (PTP) uses packets to communicate highly accurate frequency, phase and time-of-day information. PTP messages are encapsulated in GFP-F frames as illustrated in Figure 7-13. The content of the PTP common message header and message fields are specified in [ITU-T G.8275.1]. The types of PTP messages used for a given application are defined in the Recommendation associated with that application.

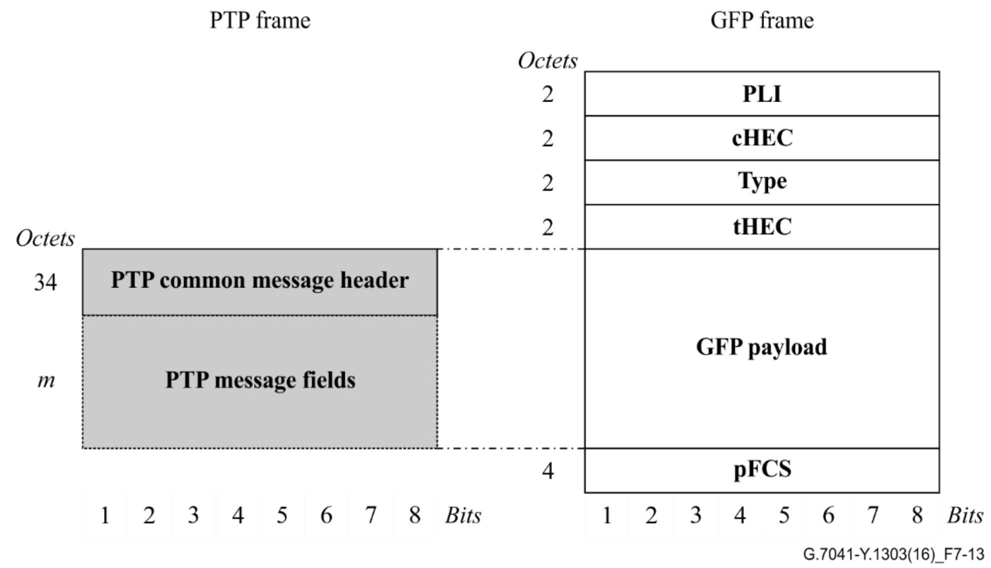


Figure 7-13 – PTP message mapping into GFP-F

7.11 Synchronization status messages

A synchronization status message (SSM) provides information regarding the quality of the clock source being used by the SSM source.

An SSM is encapsulated in GFP-F frames as illustrated in Figure 7-14. The contents of the SSM are specified in [ITU-T G.781]. The basic SSM is a single octet message, using only the first octet of the SSM message field shown in Figure 7-14.

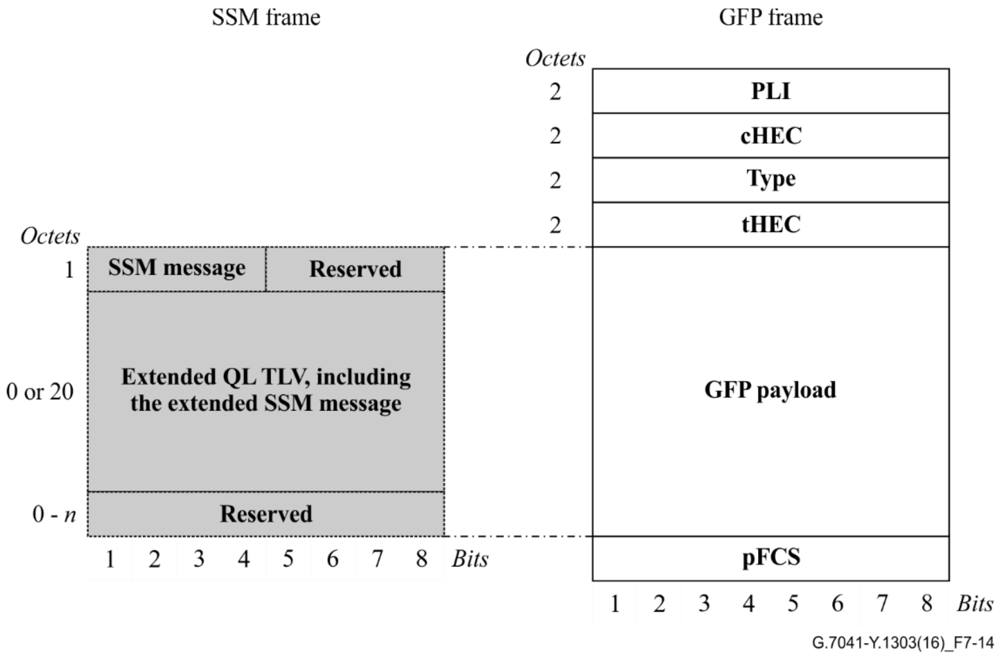


Figure 7-14 – SSM mapping into GFP-F

In order to support enhanced clocks and new functionality, an extended SSM is defined in Figure 7-14. The contents of the extended SSM are defined in clause 11.3.1.3 of [ITU-T G.8264]. The Extended SSM includes the 20-byte field after the SSM octet, and may optionally include other TLVs as they are defined in the future. Consistent with [ITU-T G.8264] and [IEEE 802.3], on an octet-by-octet bases, bits 0 and 7 of the extended SSM correspond to bits 8 and 1 in the GFP frame.

8 Payload-specific aspects for transparent mapping of 8B/10B clients into GFP

Transparent mapping of 8B/10B payloads into GFP is intended to facilitate the transport of 8B/10B block-coded client signals for scenarios that require very low transmission latency. Examples of such client signals include FC, ESCON, fibre connection (FICON) and gigabit Ethernet. Rather than buffering an entire frame of the client data into its own GFP frame, the individual characters of the client signal are demapped from the client block codes and then mapped into periodic, fixed-length GFP frames. The mapping occurs regardless of whether the client character is a data or a control character, which thus preserves the client 8B/10B control codes. Frame multiplexing is not precluded with transparent GFP.

NOTE – Throughout this clause, the term "ESCON" is used to refer to both the ESCON and SBCON client signals.

8.1 Common aspects of GFP-T

The transparent GFP frame uses the same frame structure as the frame-mapped GFP, including the required payload header. The pFCS is optional. The transparent GFP frame format is depicted in Figure 8-1.

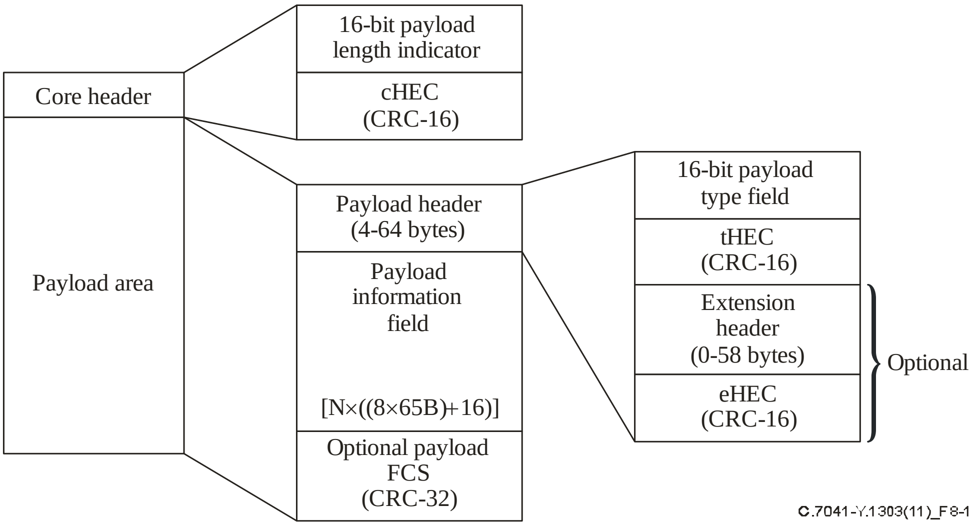


Figure 8-1 – Transparent GFP frame format

8.1.1 Adapting 8B/10B client signals via 64B/65B block codes

As depicted in the functional model in Figure 2, the first step in the client adaptation process is to decode the physical layer of the client signal. For 8B/10B line codes, the received 10-bit character is decoded into its original 8-bit value, if it is an 8B/10B data codeword, or into a control character if it is an 8B/10B control codeword. The 8B/10B control codewords are mapped into one of the 16 possible 4-bit control code indicators for the 8-bit control characters available in transparent GFP (see Table 8-1).

Table 8-1 – Mapping between 8B/10B control characters and the 64B/65B control code indicators

Name	Octet value	10B codeword (RD–) abcdei fghj	10B codeword (RD+) abcdei fghj	64B/65B 4-bit mapping
/K28.0/	1C	001111 0100	110000 1011	0000
/K28.1/	3C	001111 1001	110000 0110	0001
/K28.2/	5C	001111 0101	110000 1010	0010
/K28.3/	7C	001111 0011	110000 1100	0011
/K28.4/	9C	001111 0010	110000 1101	0100
/K28.5/	BC	001111 1010	110000 0101	0101
/K28.6/	DC	001111 0110	110000 1001	0110
/K28.7/	FC	001111 1000	110000 0111	0111
/K23.7/	F7	111010 1000	000101 0111	1000
/K27.7/	FB	110110 1000	001001 0111	1001
/K29.7/	FD	101110 1000	010001 0111	1010
/K30.7/	FE	011110 1000	100001 0111	1011
10B_ERR	01	Unrecognized RD–	Unrecognized RD+	1100
65B_PAD	02	N/A	N/A	1101
Spare	03	N/A	N/A	1110
Spare	04	N/A	N/A	1111

NOTE 1 – While all 256 data characters must be supported, only 12 special 8B/10B control codewords are recognized and used for 64B/65B control characters in gigabit Ethernet, FC, FICON and ESCON. Hence, the compression of special 8B/10B control codewords into 4-bit values is possible without restricting client signals, or providing protocol-specific handling of 8B/10B control codewords.

NOTE 2 – The re-coding process is entirely unaware of the meaning of control words or ordered sets. It simply generically recodes data and control words into 65B blocks. No knowledge of start-of-frame, end-of-frame, errors, idles, control codes, ordered sets, etc., is required.

The decoded 8B/10B characters are then mapped into a 64B/65B block code. The structure of the 64B/65B block code is shown in Figure 8-2. The leading bit of the 65-bit block, the flag bit, indicates whether that block contains only 64B/65B 8-bit data characters or whether client control characters are also present in that block (flag bit = 0 indicates data octets only and flag bit = 1 indicates at least one control octet in the block). Client control characters, which are mapped into 8-bit 64B/65B control characters, are located at the beginning of the 64-bit block payload if they are present in that block. The first bit of the 64B/65B control character contains a last control character (LCC) flag bit which indicates whether this control character is the last one in this block (LCC = 0), or whether there is another control character in the next octet (LCC = 1). The next three bits contain the control code locator, which indicates the original location of the 8B/10B control code character within sequence of the eight client characters contained in the block. The last 4 bits, the control code indicator, give the 4-bit representation of the 8B/10B control code character. The explicit mapping of 8B/10B control code characters into the 4-bit control codes is defined in Table 8-1. The control codes are mapped into the payload bytes of the 64B/65B code in the order in which they were received. Note that, as a result, the control code addresses aaa-hhh in Figure 8-2 will be in ascending order.

Input client characters	Flag bit	64-bit (8-octet) field							
All data	0	D1	D2	D3	D4	D5	D6	D7	D8
7 data, 1 control	1	0 aaa C1	D1	D2	D3	D4	D5	D6	D7
6 data, 2 control	1	1 aaa C1	0 bbb C2	D1	D2	D3	D4	D5	D6
5 data, 3 control	1	1 aaa C1	1 bbb C2	0 ccc C3	D1	D2	D3	D4	D5
4 data, 4 control	1	1 aaa C1	1 bbb C2	1 ccc C3	0 ddd C4	D1	D2	D3	D4
3 data, 5 control	1	1 aaa C1	1 bbb C2	1 ccc C3	1 ddd C4	0 eee C5	D1	D2	D3
2 data, 6 control	1	1 aaa C1	1 bbb C2	1 ccc C3	1 ddd C4	1 eee C5	0 fff C6	D1	D2
1 data, 7 control	1	1 aaa C1	1 bbb C2	1 ccc C3	1 ddd C4	1 eee C5	1 fff C6	0 ggg C7	D1
8 control	1	1 aaa C1	1 bbb C2	1 ccc C3	1 ddd C4	1 eee C5	1 fff C6	1 ggg C7	0 hhh C8

– Leading bit in a control octet (LCC) = 1 if there are more control octets and = 0 if this payload octet contains the last control octet in that block.

– aaa = 3-bit representation of the first control code's original position (first control code locator).

– bbb = 3-bit representation of the second control code's original position (second control code locator).

...

– hhh = 3-bit representation of the eighth control code's original position (eighth control code locator).

– Ci = 4-bit representation of the i-th control code (control code indicator).

– Di = 8-bit representation of the i-th data value in order of transmission.

Figure 8-2 – Transparent GFP 64B/65B code components
(see Figure 8-3 for actual superblock structure)

For example, if there is a single 64B/65B control character in a block, and it was originally located between 8B/10B data codewords D2 and D3, the first octet of the 64B/65B block will contain 0.010.C1. The LCC value of 0 indicates that this 64B/65B control character is the last one in that block and the value of aaa = 010 indicates C1's location between D2 and D3. At the demapper, the 64B/65B data characters are remapped as 8-bit data octets and then encoded back into the 8B/10B data codewords. For 64B/65B control characters, the four-bit control code indicators are remapped into the appropriate 8B/10B control codewords with their positions within the original character stream restored based on the three-bit control code locator.

8.1.1.1 10B_ERR code

Certain client signal defects may produce 8B/10B codewords on ingress to the GFP source adaptation process that cannot be recognized by the 64B/65B adaptation process (e.g., a CSF, an illegal 8/10B codeword or a legal codeword with an RD error, see clause 8.2). A special 64B/65B control character, the 10B_ERR code, is provided to convey such "unrecognized 8B/10B codeword" client signal defects.

When reconstructing the client signal on egress from the transport network, it is recommended that received 10B_ERR codes be typically recoded by the demapper into an invalid transmission character of either 001111 0001 (RD–) or 110000 1110 (RD+) (fixed, illegal 8B/10B codewords with neutral disparity, containing a transition within both the first three bits and last three bits of the codeword), depending on RD (see clause 8.2.3 for other client-specific RD considerations). Although the actual value of the unrecognized 8B/10B codeword is not retained, the occurrence and location of the client signal defect are preserved.

In addition to the recommended invalid transmission character (whose construction minimizes the possible creation of aliased commas when combined with adjacent characters), 10B_ERR events may also be demapped into alternate invalid transmission characters, provided that these alternate invalid transmission characters also meet all 8B/10B coding rules, are of neutral disparity and contain a minimum of one transition within both the first four bits and last four bits of the codeword.

8.1.1.2 Insertion of 65B_PAD code and GFP client management frames

Since the transparent GFP application requires that the available path (channel) capacity is at least that of the client signal base (pre-encoding) data rate, the input receive (ingress) buffer at the mapper will regularly approach underflow. For rate adaptation purposes, if a transparent GFP frame is currently being transmitted and if there are no client characters ready for transmission by the transparent GFP mapper, the mapper shall insert a 65B_PAD padding character. The pad character is mapped into the GFP frame in the same manner as a control character and is recognized and removed by the GFP demapper. Client-specific considerations for 65B_PAD code handling are given in clause 8.4.1.

Client data frames are transmitted with priority over CMFs. If a GFP CMF is available to transmit, and the ingress buffer is nearly empty (e.g., if a 65B_PAD character has been sent during the current client data frame), then the CMF may be sent after the current client data frame. In order to maintain low latency, it is recommended that, for a right-sized channel, only a single CMF be sent between client data frames. It is also recommended that CMFs used with transparent GFP be limited to a payload information field of eight bytes or less. Note that low latency may also be maintained by increasing the channel size to allow the exchange of additional CMFs.

8.1.2 Adapting 64B/65B code blocks into GFP

To preserve the octet alignment of the transparent GFP signal with the transport SDH/ODUk frame, the first step in the adaptation process is to group eight 64B/65B codes into a superblock as shown in Figure 8-3. The leading (flag) bits of each of the eight 64B/65B codes are grouped together into a first trailing octet. The 16 bits of the last two trailing octets are used for a CRC-16 error check over the bits of this superblock.

<table>
<tr><td colspan="8">Octet 1, 1</td></tr>
<tr><td colspan="8">Octet 1, 2</td></tr>
<tr><td colspan="8">Octet 1, 3</td></tr>
<tr><td colspan="8">.
.
.</td></tr>
<tr><td colspan="8">Octet 8, 7</td></tr>
<tr><td colspan="8">Octet 8, 8</td></tr>
<tr><td>L1</td><td>L2</td><td>L3</td><td>L4</td><td>L5</td><td>L6</td><td>L7</td><td>L8</td></tr>
<tr><td>CRC-1</td><td>CRC-2</td><td>CRC-3</td><td>CRC-4</td><td>CRC-5</td><td>CRC-6</td><td>CRC-7</td><td>CRC-8</td></tr>
<tr><td>CRC-9</td><td>CRC-10</td><td>CRC-11</td><td>CRC-12</td><td>CRC-13</td><td>CRC-14</td><td>CRC-15</td><td>CRC-16</td></tr>
<tr><td colspan="8">where: Octet <i>j</i>, <i>k</i> is the <i>k</i>-th octet of the <i>j</i>-th 64B/65B code in the superblock
L<i>j</i> is the leading (flag) bit <i>j</i>-th 64B/65B code in the superblock
CRC-<i>i</i> is the <i>i</i>-th error control bit where CRC-1 is the MSB of the CRC</td></tr>
</table>

Figure 8-3 – Superblock structure for mapping 64B/65B code components into the GFP frame

NOTE – To minimize latency, the transparent GFP mapper can begin transmitting data as soon as the first 64B/65B code in the group has been formed rather than waiting for the entire superblock to be formed.

Assuming no pFCS and a null extension header, the resulting GFP frame is $\{N \times [(65 \times 8) + 16] + (8 \times 8)\}$ bits long, where N is the number of superblocks in the GFP frame. The value of N depends on the base, uncoded rate of the client signal and on the transport channel capacity. Suggested SDH virtually concatenated channel capacities and the associated minimum values for N are shown in Appendix IV. Suggested channel capacities for other transport paths are for further study. The minimum value of N depends on the data rate of the client signal, the number of GFP frame overhead octets (e.g., 8 with no optional pFCS and a null extension header), and the size of the payload envelope, as shown in Appendix IV. Specifically, $N_{\min}$ must be chosen such that for the fastest tolerance client clock rate and slowest tolerance SDH/OTN clock rate, the time required to transmit the GFP frame containing the $N \times 8 \times 8$ client characters is less than the time in which the client can deliver these $N \times 8 \times 8$ characters to the GFP mapper.

Note that N may be optionally configurable according to SBW requirements for the transport of CMFs (see Appendix IV).

8.1.2.1 Error control with transparent GFP

The 16-error control bits in a superblock (see Figure 8-3) contain a CRC-16 error check code over the 536 bits in that superblock. If the demapper detects an error, it should output either 10B error characters or unrecognized 10B characters in place of all of the client characters contained in that superblock. The 10B error and unrecognized characters are described for disparity errors in the client-specific aspects (see clause 8.2). This replacement guarantees that the client receiver will be able to detect the presence of the error.

The generator polynomial for the CRC-16 is $G(x) = x^{16} + x^{15} + x^{12} + x^{10} + x^4 + x^3 + x^2 + x + 1$ with an initialization value of zero, where x^{16} corresponds to the MSB and x^0 to the LSB. The superblock CRC is generated by the source adaptation process using the following steps:

1) the first 65 octets of the superblock are taken in network octet order (see Figure 8-3), MSB first, to form a 520-bit pattern representing the coefficients of a polynomial $M(x)$ of degree 519;
2) $M(x)$ is multiplied by x^{16} and divided (modulo 2) by $G(x)$, producing a remainder $R(x)$ of degree 15 or less;
3) The coefficients of $R(x)$ are considered to be a 16-bit sequence, where x^{15} is the MSB;
4) This 16-bit sequence is the CRC-16.

NOTE – Single error correction is also possible with this CRC-16. However, since the sink adaptation process performs the CRC-16 check after the payload descrambling is performed, the error correction circuit should account for single bit errors, as well as double errors spaced 43 bits apart coming out of the descrambler.

The sink adaptation process performs steps 1)–3) in the same manner as the source adaptation process, except that here, the $M(x)$ polynomial of step 1 includes the CRC-16 bits in received order, and has degree 535. In the absence of bit errors, the remainder shall be 0000 0000 0000 0000.

8.2 Running disparity in 64B/65B codes

8B/10B codewords are designed to facilitate error-free transmission by maintaining DC balance, providing significant transitions for clock recovery and limiting run-length of consecutive 1s or 0s. DC balance is measured on a codeword-by-codeword basis by keeping track of RD. RD is either positive (indicating more 1s than 0s have been sent), or negative (more 0s than 1s sent).

In order to maintain DC balance in 8B/10B codewords, each 8-bit data character and each of the 12 recognized "special control characters" have two 10-bit encodings. Depending on current RD, the 8B/10B encoder will select which of the two encodings to transmit for next data or control character in order to either flip the RD, or to maintain the current RD. Specifically, the new codeword flips the RD from negative to positive if there have been more 0s than 1s transmitted, from positive to negative if there have been more 1s than 0s transmitted or maintains the RD if there has been an equal number of 1s and 0s.

Transmission bit errors may cause a received 8B/10B codeword to have the wrong disparity for the current beginning RD state. In these cases, an RD error is detected. Independent of the received character's validity, the received transmission character shall be used to calculate a new value of RD. The new value shall be used as the receiver's current RD for the next received transmission character.

NOTE – Transmission bit errors may also result in the errored codeword being received with correct disparity and a corrupted but legal 8B/10B codeword that results in some later non-errored codeword being detected with an RD error. In some cases, protocol-specific RD rules have been created to ensure each data packet begins or ends with defined disparity so that errors will not be propagated across data packets.

8.2.1 Handling of running disparity on ingress

On ingress, the initial RD, upon power-on, reset or transition from an LOS or loss of codeword synchronization phase, may be assumed to be either positive or negative.

A match to the received 10B character is searched for in the appropriate RD+ or RD– column of the 8B/10B valid codeword lookup table, depending on the current beginning RD. If no match is found, either an illegal codeword or a legal codeword with a RD error has been detected. Both are treated as 8B/10B code violations, and are replaced with the 10B_ERR code in the 64B/65B mapping process.

8.2.2 Handling of running disparity on egress

On egress, the initial RD upon power-on, reset or transition from an LOS or loss of codeword synchronization phase shall be assumed to be negative.

Transparent transport implementations must generate correct RDs using any applicable protocol-specific rules. References are provided in clause 8.2.3 to the standard(s) that define each currently applicable protocol's disparity rules.

10B_ERR codes are recoded into client signals either as an unrecognized codeword with valid RD or as a protocol-specific error, depending on the protocol, as described in clause 8.2.3.

8.2.3 Client-specific running disparity aspects

This clause describes the client-specific RD rules for each of the identified, supported 8B/10B client protocols.

8.2.3.1 Fibre channel payload

RD rules for a FC are found in clause 11 of [ANSI INCITS 230]. In addition to the "generic" RD rules specified in clause 11.2 of [ANSI INCITS 230] FC-specific rules in clause 11.4 of [ANSI INCITS 230] provide two versions of each end of frame (EOF) ordered set, and dictate their use to ensure that a negative RD will result after processing of the final character of the EOF ordered set. Ordered sets defined for the primitive signals and primitive sequences preserve this negative disparity, ensuring that the ordered sets associated with start of frame (SOF) delimiters (SFDs), primitive signals and primitive sequences will also always be transmitted with a negative beginning RD. This restriction allows FC idle words to be removed and added from an encoded bit stream one word at a time without altering the beginning RD.

To prevent subsequent valid FC frames from being declared invalid, the K28.5 character associated with all ordered sets except EOF should be generated assuming a beginning negative RD. In the event that a previous transmission error results in an incorrect EOF for the current RD, the next ordered set will be generated with RD− K28.5, forcing the ending RD to be negative. As a result, transmission errors will not cause a RD error to be propagated across frames.

For "transparent transport" of FC payloads, 10B_ERR shall be recoded into an unrecognized 10B neutral disparity codeword, depending on the beginning running disparity (RD− or RD+), following the rules described in clause 8.1.1.1.

8.2.3.2 ESCON payload

RD rules for ESCON are found in clause 6.2.2 of [ANSI INCITS 296]. Since ESCON does not define an error code to substitute for code violations, on egress, 10B_ERR shall be recoded into an unrecognized 10B neutral disparity codeword, depending on the beginning running disparity (RD− or RD+), following the rules described in clause 8.1.1.1.

8.2.3.3 FICON payload

For purposes of mapping into transparent GFP, the RD rules for FICON are identical to those specified for FC in [ANSI INCITS 230].

8.2.3.4 Gigabit Ethernet payload

RD rules for gigabit Ethernet are found in clause 36.2.4 of [IEEE 802.3]. Two idle encodings are provided, indicated as /I1/ and /I2/. The first /I/ following a packet or configuration ordered set restores the current RD to a negative value. All subsequent /I/s are /I2/ to ensure a negative ending RD. This restriction allows single /I2/s to be inserted/removed for rate adaptation without altering the beginning RD associated with the code-group subsequent to the inserted or removed /I2/.

In order to ensure beginning negative RD for each SOF, all /I2/ idles should be generated with RD− K28.5, ensuring a beginning negative RD for the next idle or SOF.

As per clause 36.2.4.16 of [IEEE 802.3], RD errors detected on ingress (and replaced with 10B_ERR codeword in 64B/65B encoding process) should be replaced with /V/ codeword (K30.7) having correct disparity on egress. As an option, it is also permissible to recode received 10B_ERR into one of the following unrecognized 10B neutral disparity codewords, depending on beginning running disparity: 001111 0001 (RD−) or 110000 1110 (RD+). As an option, it is also permissible to recode received 10B_ERR into an unrecognized 10B neutral disparity codeword, depending on the beginning running disparity (RD− or RD+), following the rules described in clause 8.1.1.1.

It should be noted that such optional introduction of demapped 10B_ERR codes into the data stream is only appropriate when the attached Ethernet system is not using error logging for system maintenance support.

NOTE – In [ITU-T G.709], two replacement signals are defined for GbE:

– the failed GbE signal is replaced by a stream of 10B blocks, with a bit rate of 1 250 000 kbit/s ± 100 ppm, each carrying a link fault indication as specified in [IEEE 802.3] (applicable at ingress and egress side), or

– the GFP-T signal is replaced by a stream of GFP client signal fail (CSF) and GFP-idle frames with a bit rate of 15/16 × 1 250 000 kbit/s ± 100 ppm (applicable at the ingress side only).

8.2.3.5 DVB ASI payload

The RD aspects of the DVB ASI mapping in GFP shall adhere to the FC standard, which are found in clause 11 of [ANSI INCITS 230]. On egress, 10B_ERR shall be recoded into an unrecognized 10B neutral disparity codeword, depending on the beginning running disparity (RD– or RD+), following the rules described in clause 8.1.1.1.

8.3 Client-specific signal fail aspects

When transparent GFP mapping detects a CSF at ingress, it may send a "client signal fail" indication as described in clause 6.3.3. Client signal fail conditions include, as a minimum, loss of 8B/10B synchronization and, in some cases, LOS. Other implementation-dependent indications of a failed client signal (e.g., loss-of-clock from an interface between integrated circuits) may be encoded as client signal fail.

Since client signals are provided as a continuous serial stream of 10-bit characters, it is necessary to find codeword alignment. Special characters containing the "comma" delimiter provide the information necessary to achieve and maintain codeword alignment. While all 8B/10B client signals employ the same bit alignment technique, conditions for detecting and clearing loss of 8B/10B synchronization are protocol-specific, and are identified in the following protocol-specific clauses.

Server layer failures in the GFP process itself, in the 64B/65B adaptation process or in the transport network, may induce a CSF indication to the client adaptation process.

If the onset of CSF occurs within a GFP client data frame, the remainder of the 64B/65B blocks of that GFP frame shall be filled with 10B_ERR codes. At the far-end, these shall be decoded as errors.

At the far-end of a transport network, transparently transported client signals must still be reconstructed and output in a manner that is compliant with the physical and coding interface requirements specific to each protocol. The following client-specific clauses define what action should be taken at client signal egress in response to a received far-end client signal fail indication, or any adaptation or transport defects that make it impossible to extract a client signal.

8.3.1 Fibre channel payload

8.3.1.1 Fibre channel loss of light

FC LOS is an implementation-dependent option. When supported, applicable LOL and signal detect requirements are found in clauses 5.6, 6.2.3.2 and H.10 of [ANSI INCITS 230].

Other implementation-dependent indications of a failed client signal (e.g., loss-of-clock from a SerDes) may be encoded as client signal fail.

8.3.1.2 Fibre channel 8B/10B loss of synchronization

FC conditions for declaring in/out of 8B/10B codeword synchronization are specified in clause 12.1 of [ANSI INCITS 230].

8.3.1.3 Fibre channel output due to ingress or transport signal fail

Since the goal of transparent GFP mapping is to transport client signals as transparently as possible, it is not appropriate to initiate link initialization or link recovery procedures on egress due to client signal fail or transport failures. It is recommended that the egress FC transmitter generate the Not_Operational primitive sequence per clause 16.4.2 of [ANSI INCITS 230].

NOTE – Older equipment was allowed to continuously output the neutral disparity decoding for 10B_ERR, forcing loss-of-synchronization detection and the associated action at the downstream FC receiver.

If the CSF condition persists, the client adaptation process may transmit nothing, forcing LOS detection and associated action at the downstream FC receiver.

8.3.2 ESCON payload

8.3.2.1 ESCON loss of signal

Optical LOS detection requirements are specified in clauses 5.2 and 5.3 of [ANSI INCITS 296], respectively.

8.3.2.2 ESCON 8B/10B loss of synchronization

ESCON conditions for declaring being in or out of 8B/10B codeword synchronization are specified in clause 7.1 of [ANSI INCITS 296].

8.3.2.3 ESCON output due to ingress or transport signal fail

Since the goal of transparent GFP mapping is to transport client signals as transparently as possible, it is not appropriate to initiate link initialization or link recovery procedures on egress due to client signal fail or transport failures. It is recommended that the egress ESCON transmitter generate the not-operational sequence per clause 7.4.2 of [ANSI INCITS 296].

NOTE – Older equipment was allowed to continuously output the neutral disparity decoding for 10B_ERR, forcing loss-of-synchronization detection and the associated action at the downstream ESCON receiver.

If the CSF condition persists, the client adaptation process may transmit nothing, forcing LOS detection and associated action at the downstream ESCON receiver.

8.3.3 FICON payload

The CSF handling requirements for FICON are identical to those for FC, as specified in [ANSI INCITS 230].

8.3.4 Full-duplex gigabit Ethernet payload

8.3.4.1 Gigabit Ethernet loss of signal

Gigabit Ethernet physical media dependent (PMD) signal detect requirements are specified in clauses 38.2.4 and 39.2.3 of [IEEE 802.3] for fibre and copper interfaces, respectively.

8.3.4.2 Gigabit Ethernet 8B/10B loss of synchronization

Gigabit Ethernet conditions for declaring being in or out of 8B/10B codeword synchronization are specified in clause 36.2.5.2.6 and Figure 36-9 of [IEEE 802.3].

8.3.4.3 Gigabit Ethernet output due to ingress or transport signal fail

Since the goal of transparent GFP mapping is to transport client signals as transparently as possible, it is not appropriate to initiate link initialization or link recovery procedures on egress due to client signal fail or transport failures. It is recommended that the egress GbE transmitter continuously output the /V/ ordered set per clause 36.2.4.16 of [IEEE 802.3].

If the CSF condition persists, the client adaptation process may transmit nothing, forcing LOS detection and associated action at the downstream GbE receiver.

NOTE – In [ITU-T G.709], two replacement signals are defined for GbE:

- the failed GbE signal is replaced by a stream of 10B blocks, with a bit rate of 1 250 000 kbit/s ± 100 ppm, each carrying a link fault indication as specified in [IEEE 802.3] (applicable at ingress and egress side); or
- the GFP-T signal is replaced by a stream of GFP client signal fail (CSF) and GFP-idle frames with a bit rate of (15/16) × 1 250 000 kbit/s ± 100 ppm (applicable at the ingress side only).

8.3.5 DVB ASI payload

8.3.5.1 DVB ASI loss of light

By reference to FC standards, DVB ASI LOS is an implementation-dependent option. When supported, applicable LOL and signal detect requirements are found in clauses 5.6, 6.2.3.2 and H.10 of [ANSI INCITS 230].

Other implementation-dependent indications of a failed client signal (e.g., loss-of-clock from a SerDes) may be encoded as client signal fail.

8.3.5.2 DVB ASI 8B/10B loss of synchronization

As per Appendix B of [EN 50083-9], DVB ASI codeword synchronization shall be achieved on receipt of two /K28.5/ characters having the same alignment within five consecutive received characters. [EN 50083-9] does not specify criteria for declaring loss of codeword synchronization. FC criteria may not be applied since DVB ASI codeword synchronization and transmission are character based, rather than 4-character transmission word based. In the absence of guidance from [EN 50083-9], ESCON/SBCON character-based codeword loss-of-synchronization criteria should be those specified in clause 7.1 of [ANSI INCITS 296].

8.3.5.3 DVB ASI output due to ingress or transport signal fail

The egress DVB ASI transmitter should continuously output the neutral disparity decoding for 10B_ERR, forcing loss-of-synchronization detection and any associated action at the downstream DVB ASI receiver. If the CSF condition persists, the client adaptation process may transmit nothing, forcing LOS detection and associated action at the downstream DVB ASI receiver.

8.4 Synchronous full-rate transparent mapping of 8B/10B clients into GFP

Transparent mapping of 8B/10B block-coded clients can be accomplished via a synchronous (full-rate) mapping of all received client characters. This transparent mapping utilizes common character-based mapping described in clause 8.1 as well as client-specific processes described in clauses 8.2.3 and 8.3. In addition, client-specific requirements described in the following clauses are applied before mapping and encapsulating (in the ingress direction) and after de-mapping, extracting 64B/65B blocks and decoding them into 8B/10B block codes (in the egress direction).

8.4.1 Rate adaptation in 64B/65B codes

On ingress, rate adaptation to the output payload data rate occurs in the 64B/65B encoding process. If there is not an 8B/10B codeword available for the mapper to recode into 64B/65B block code, the mapper inserts a 65B_PAD as described in clause 8.1.1.2. Essentially, this 65B_PAD is a non-client-idle that is used to pad 64/65B blocks for rate adaptation purposes. On egress, the demapper removes these non-client-idle signals. Since fixed-length GFP frames are used, and frames may be padded with 65B_PADs for rate adaptation, there is no need to buffer an entire GFP frame prior to inserting it into the payload of the outgoing transport signal, thus reducing buffering and delay in the mapping process.

8.4.1.1 Egress rate adaptation procedures

There are two approaches for generating the client egress data interface clock at the GFP client-specific sink-adaptation process. One approach is to adapt the client signal to a clock source that is local to the GFP sink adaptation process. The other approach is to generate the client signal egress clock by deriving it from the received GFP signal and transport clock.

Should a failure occur in either the ingress client signal or during SDH/OTN transport, a protocol-specific local reference clock is still required at the client data egress point if the client expects a client rate link failure signal to replace the failed client.

8.4.1.1.1 Rate adaptation to a local reference clock

The currently supported 8B/10B client signals specify operating frequencies with clock-offset requirements of ±100 ppm to ±200 ppm, which are significantly relaxed compared to SDH or OTN. Each of these client signals is designed to allow rate adaptation to a local reference clock, either at repeaters or at the far-end, through client idle (or fill-word) insertion or removal. To facilitate this rate adaptation, each of these client signals impose minimum IPG rules, which specify the minimum number of idle codewords that must be inserted between data packets. Each of these client signals also specifies the maximum data packet size. Minimum IPG rules have been established to ensure that where rate adaptation to a local clock is required, even under the worst-case condition where a fast input clock and slow output clock require some IPG idles to be deleted, a sufficient IPG will remain between packets for successful client frame delineation.

This scheme may be employed equally well when reconstructing transparent-mapped client data on egress. With this approach, a local reference clock is supplied at the GFP sink adaptation process. As client data is demapped from GFP frames and recoded into 8B/10B codewords, it is rate adapted to the local reference clock through idle insertion/removal. Client-specific processing is required to recognize legal opportunities to insert/remove idle codewords, generate proper idle codes and insert such codes in the egress bit stream. An example of a client-specific parameter is the minimum and maximum number of idles that are allowed to be inserted or removed.

Even in links containing multiple repeaters, if all "local" clocks meet the accuracy requirements for the specific protocol, sufficient opportunities for idle insertion or removal will occur, since aggregate timing offsets through cascaded repeaters cannot exceed worst-case clock offset requirements.

With this approach, timing characteristics such as the jitter and wander of the reconstructed client signal depend primarily on the quality of the local reference clock. The local reference clock is protocol rate-specific (e.g., gigabit Ethernet, FC and ESCON do not share common frequencies).

8.4.1.1.2 Rate adaptation from the transported client signal

Client signals are provided at a smooth protocol-specific clock rate on ingress. While there may be gaps in the client data packets themselves, these are filled with an IPG at a constant clock rate. Transparent mapping preserves all of the client data, control and IPG information when re-coding it using 64B/65B (assuming no client LOS or loss of character synchronization occurs). However, the recoded data is then mapped into GFP frames with 65B_PAD stuffing to rate-adapt to the higher bandwidth transport payload channel. GFP client management or control frames may also be inserted periodically or opportunistically between GFP client data frames. Transport frames add their own overhead (section and path overhead plus fixed stuff bytes in the case of SDH). No alignment between client data, stuffing bytes or blocks, GFP frames or transport overhead is maintained.

On egress, clock recovery is expected to require a first-in, first-out (FIFO) and desynchronizer, where the desynchronizer would require a reference clock, phase-locked loop (PLL) and filter. Recovered clock timing would depend on some filtered version of the FIFO fill level. The FIFO itself would be subject to fairly dramatic changes in level under normal operating conditions due to the occurrence of large blocks of section/transport overhead, GFP frame overhead and GFP CMFs. Under worst-case conditions, it is possible that all of the client data "gapping" mechanisms will align into one contiguous "no client data" block. The relatively non-periodic nature of some of the gaps combined with the relative large client data source clock frequency tolerance complicate the FIFO and PLL design.

The advantage of this desynchronizer approach is that no protocol-specific knowledge is required to recover the client clock on egress.

The jitter and wander timing characteristics of the reconstructed client signal depend primarily on the design of the clock recovery system. With a more complex design, a wide range of client rates may be supported with a single design.

8.4.1.2 Client-specific rate adaptation aspects

On egress, transparently transported client signals must be reconstructed and output in a manner that is compliant with the physical interface requirements specific to each protocol. Regardless of the selected client egress timing approach, protocol-specific timing requirements must be met, as defined in applicable standards for each client protocol. Clauses 8.4.1.2.1 to 8.4.1.2.5 identify key applicable requirements, but other protocol-specific requirements may apply.

8.4.1.2.1 Fibre channel payload

FC full rate output data rate (after 8B/10B encoding) shall be 531.25, 1 062.5, 2 125 or 4 250 Mbit/s ± 100 ppm, as specified in clause 5.1 of [ANSI INCITS 230]. Output signal timing requirements are further specified in clauses 6.1.1 (single-mode optical output interface), 6.2.1 (multi-mode optical output interface) and 7 (electrical cable interface) of [ANSI INCITS 230]. Output signals will normally be generated with a minimum of six primitive signals (idles and R_RDY) between frames, as specified in clause 17.1 of [ANSI INCITS 230]. If rate adaptation is performed using FC idle insert/removal, rate adaptation shall be applied such that the destination receives at least two idles preceding each frame, as specified in clause 17.1 of [ANSI INCITS 230].

Rate adaptation may also be required when a continuous stream of FC primitive sequences is received, where primitive sequences are defined in Table 26 of [ANSI INCITS 230]. Since a minimum of three consecutive identical primitive sequences are required to be received before the sequence is recognized (per clause 16.4.1 of [ANSI INCITS 230]), rate adaptation by inserting one replica of the received four-character sequence, or deleting a received sequence, shall only occur after three consecutive identical sequences have been received and retransmitted.

Depending on implementation, a continuous stream of 10B_ERR neutral disparity characters could be generated at egress, although rate adaptation is still required here. In this case, rate adaptation may be performed by removing or inserting a 10B_ERR neutral disparity character after 12 consecutive 10B_ERR characters have been received and retransmitted.

8.4.1.2.2 ESCON payload

ESCON output data rate (after 8B/10B encoding) shall be 200 Mbit/s ± 0.04 Mbit/s, as specified in clause 5.1.2 of [ANSI INCITS 296]. Output signal timing requirements are further specified in clauses 5.2.1 (multi-mode output interface) and 5.3.1 (single-mode output interface) of [ANSI INCITS 296]. Output signals will normally be generated with a minimum of four idle characters (K28.5) between data frames, as specified in clause 6.3 of [ANSI INCITS 296]. According to the rules of clause 7.2 of [ANSI INCITS 296], if rate adaptation is performed using ESCON idle insert/removal, such adaptation is limited to one insert/removal event between any two frames, and said insert/removal event consists of the addition or removal of either one or two idle characters. However, one insert/removal event between frames may not provide for sufficient rate correction capability when the interval between frames becomes sufficiently large. Therefore, for GFP-T egress adaptation purposes, any number of insert/removal events is permitted between frames, provided that such events occur no more frequently than once every 2 500 characters on average and do not result in fewer than two idles remaining between frames. Rate adaptation may also be required when a continuous stream of ordered set sequences is received, where ordered set sequences are defined in Table 15 of [ANSI INCITS 296]. Since a minimum of eight consecutive sequences are required to be received before the sequence is recognized (per clause 6.3 of [ANSI INCITS 296]), rate adaptation by inserting a replica of the received two-character sequence, or deleting a received sequence shall only occur after eight consecutive identical sequences have been received and retransmitted.

Depending on implementation, a continuous stream of 10B_ERR neutral disparity characters could be generated at egress, although rate adaptation is still required here. In this case, rate adaptation may be performed by removing or inserting a 10B_ERR neutral disparity character after 12 consecutive 10B_ERR characters have been received and retransmitted.

8.4.1.2.3 FICON payload

The timing requirements for FICON are the same as those specified for FC in [ANSI INCITS 230].

8.4.1.2.4 Full-duplex gigabit Ethernet payload

GbE output data rate (after 8B/10B encoding) shall be 1 250 Mbit/s ± 100 ppm, as specified in [IEEE 802.3]. Output signal timing requirements are further specified in clauses 38.5 and 38.6

(1000BASE-LX optical fibre interfaces) and clauses 39.3.1 and 39.3.3 of [IEEE 802.3] [1000BASE-CX (short-haul copper interface)]. Output signals will normally be generated with a minimum IPG of 12 octets, per clause 4.4.2.3 of [IEEE 802.3], GbE idle characters are two octets, as defined in clause 36.2.4.12 of [IEEE 802.3]. If rate adaptation is performed using full-duplex GbE Idle insert/removal, any number of /I2/s may be removed in any IPG, such that their removal shall not result in no /I/ and not less than 8 octets including /T/, /R/ and /I/ remaining between frames (see Note), as required for successful frame delineation according to Figures 36-7a and 36-7b of [IEEE 802.3]. Any number of /I2/s may be added in any IPG. Rate adaptation may also be required when a continuous stream of eight-character configuration ordered sets (consisting of alternating /C1/C2/) is received. Since a minimum of three consecutive /C1/C2/ configuration ordered sets are required to be received before the configuration set is recognized, rate adaptation, by inserting a replica of the received /C1/C2/ sequence, or deleting a received /C1/C2/ sequence shall only occur after three consecutive identical /C1/C2/ sequences have been received and retransmitted. Depending on implementation, a continuous stream of 10B_ERR neutral disparity or transmission error (/V/) characters could be generated at egress, which still requires rate adaptation. In this case, rate adaptation may be performed by removing or replicating a 10B_ERR or /V/ character after 12 consecutive 10B_ERR or /V/ characters have been received and retransmitted.

NOTE – The 8-octet limit is described in Note 3 of clause 4.4.2 of [IEEE 802.3]. Note that [IEEE 802.3] does not specify the amount of IPG shrinkage that the receiver must tolerate without frame loss.

8.4.1.2.5 DVB ASI payload

DVB ASI output data rate (after 8B/10B encoding) shall be 270 Mbit/s ± 100 ppm, as specified in Appendix B of [EN 50083-9]. Output signal timing requirements are further specified by reference to FC specification [ANSI INCITS 230].

A minimum of two /K28.5/ characters must occur between Moving Picture Expert Group (MPEG) packets. Additional rate-adapting /K28.5/ characters may occur within or between packets. If rate adaptation is performed using /K28.5/ removal, rate adaptation shall be applied such that the destination receives at least two /K28.5/ characters preceding each frame, as specified in Appendix B of [EN 50083-9]. If rate adaptation requires insertion of /K28.5/ characters, they may be inserted either between or within MPEG packets.

Depending on implementation, a continuous stream of 10B_ERR neutral disparity characters could be received or generated at egress (e.g., in response to received client signal fail). In this case, rate adaptation may be performed by removing or inserting a 10B_ERR neutral disparity character after 12 consecutive 10B_ERR characters have been received and retransmitted.

8.5 Asynchronous (full- or sub-rate) mapping of 8B/10B clients into GFP

Sub-rate transport of 8B/10B block-coded clients can be accomplished via an asynchronous (full- or sub-rate) mapping of received client characters. Asynchronous transparent mapping utilizes common character-based mapping described in clause 8.1 as well as the client-specific processes of clauses 8.2.3 and 8.3. However, asynchronous mapping is typically a less transparent character-based mapping in which client-specific processing (on ingress) deletes client idle characters from the codeword stream. Flow control may be applied to ensure lossless client signal transport over transport paths offering less bandwidth than full-rate client signals support. Client-specific requirements described in 8.5.1 are applied before mapping and encapsulating (in the ingress direction) and after de-mapping, extracting 64B/65B blocks and decoding them into 8B/10B block codes (in the egress direction).

8.5.1 Fibre channel specific aspects for asynchronous GFP-T mapping

FC client-specific aspects for asynchronous GFP-T mapping are for further study.

Appendix I

Examples of functional models for GFP applications

(This appendix does not form an integral part of this Recommendation.)

This appendix presents some examples of functional models for GFP applications. In the absence of layer network architectures for data layer networks (e.g., IP and Ethernet), the models presented are for illustration purposes only.

GFP can be deployed in transport NEs (e.g., SDH) and in data NEs (e.g., IP, Ethernet).

In the former case, a physical data interface (Ethernet or storage area network type) is provided as a tributary interface port on the transport NE. If the physical data signal is an 8B/10B coded signal, it can be transported through the transport network as a transparent stream using GFP-T mapping (Figure I.1). If only a part of the physical interface bandwidth is carrying traffic and only this traffic is to be transported through the transport network, the physical data interface signal is terminated, data PDUs are extracted and forwarded via GFP-F mapping over a VC-m-Xv, VC-n, VC-n-Xc or VC-n-Xv signal (Figure I.2).

In the latter case, GFP processing is performed between the IP router (Ethernet switch) fabric and the, e.g., STM-N interface port functions (Figures I.3 and I.4). The FC tributary interface port using FC-BBW_SONET and GFP-F mapping in an SDH NE is shown in Figure I.5.

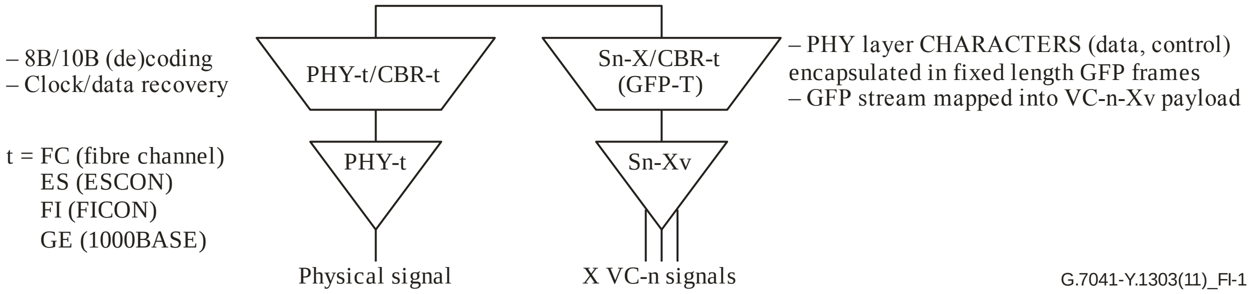


Figure I.1 – FC/ES/FI/GE tributary interface port using full-rate GFP-T mapping in an SDH network element

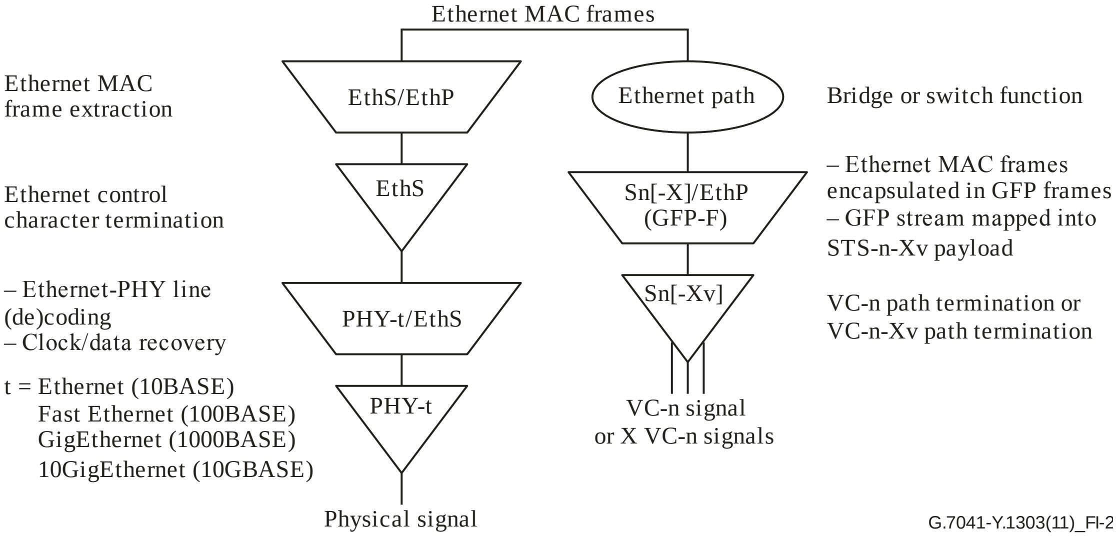


Figure I.2 – Ethernet tributary interface port using GFP-F mapping in an SDH network element

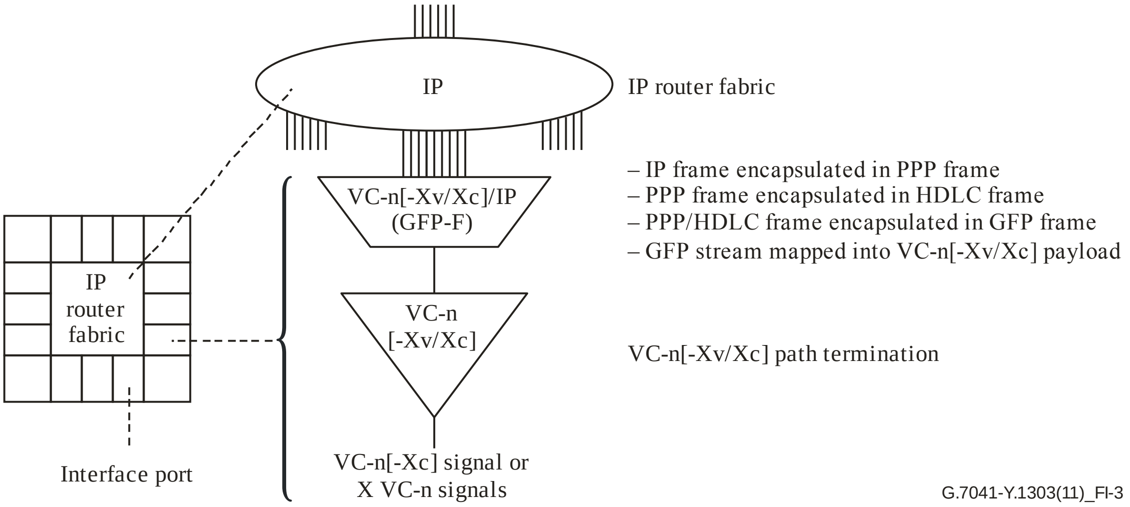


Figure I.3 – VC-n/VC-n-Xv/VC-n-Xc port on IP router or IP router function embedded in hybrid SDH/IP equipment

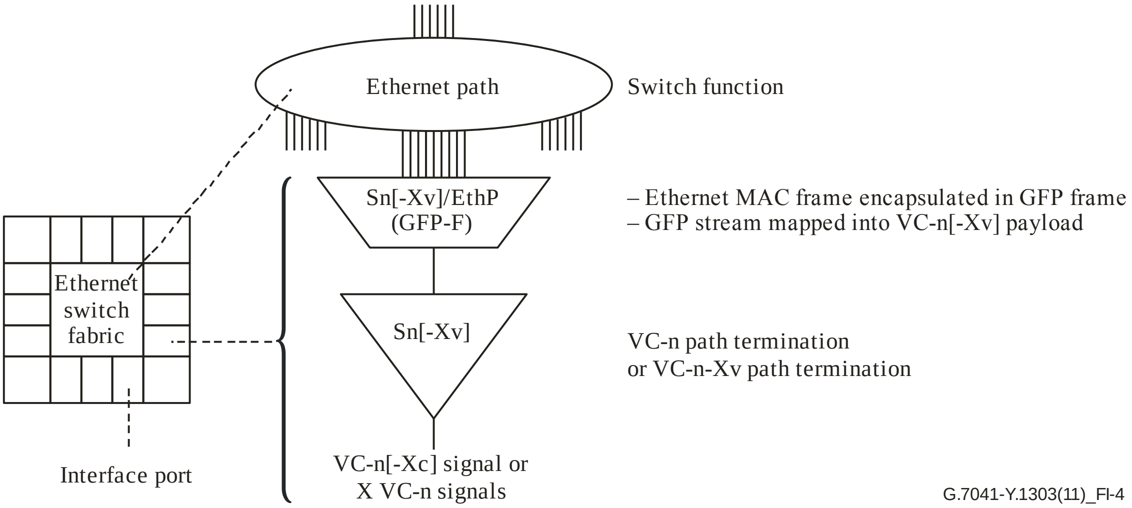


Figure I.4 – VC-n-Xv port on Ethernet switch or Ethernet switch function embedded in hybrid SDH/Ethernet equipment

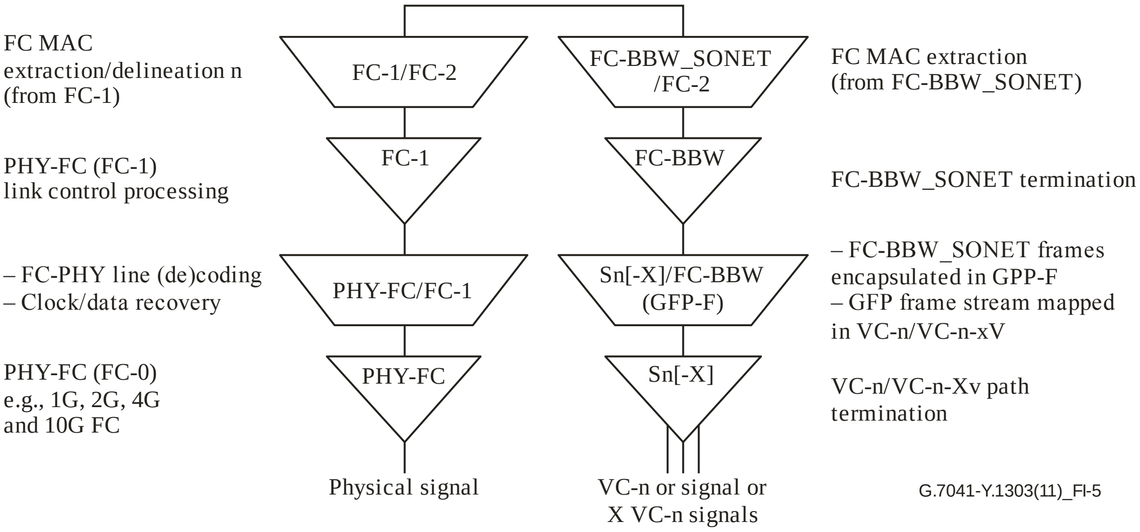


Figure I.5 – Fibre channel tributary interface port using FC-BBW_SONET and GFP-F mapping in an SDH network element

Appendix II

Sample GFP payload types

(This appendix does not form an integral part of this Recommendation.)

Table II.1 – GFP payload types

Payload type identifier (binary) **Type bits <15:13>**	**Payload frame check sequence identifier (binary)** **Type bit <12>**	**Extension header identifier (binary)** **Type bits <11:8>**	**User payload identifier (binary)** **Type bits <7:0>**	**Type** **(HEX)**	**GFP frame payload area**	**Length of extension headers** **(No. octets)**
000	0	xxxx	0000 0000	0x00	Reserved	
000	1	xxxx	0000 0000	1x00	Reserved	
000	0	0000	0000 0001	0001	Ethernet with null extension header and no pFCS	0
000	0	0000	0000 0010	0002	PPP with null extension header and no pFCS	0
000	0	0001	0000 0001	0101	Ethernet with linear extension header and no pFCS	4
000	0	0001	0000 0010	0102	PPP with linear extension header and no pFCS	4
000	0	0010	0000 0001	0201	Ethernet with ring extension header and no pFCS	18
000	0	0010	0000 0010	0202	PPP with ring extension header and no pFCS	18
000	0	0000	0000 0011	0003	Transparent fibre channel with null extension header and no pFCS	0
000	0	0000	0000 0100	0004	Transparent FICON with null extension header and no pFCS	0
000	0	0000	0000 0101	0005	Transparent ESCON with null extension header and no pFCS	0
000	0	0000	0000 0110	0006	Transparent gigabit Ethernet with null extension header and no pFCS	0
1xx	x	xxxx	xxxx xxxx	–	Reserved	–
x1x	x	xxxx	xxxx xxxx	–	Reserved	–
xx1	x	xxxx	xxxx xxxx	–	Reserved	–

Appendix III

GFP frame example illustrating transmission order and CRC calculation

(This appendix does not form an integral part of this Recommendation.)

III.1 Worked example for a GFP-F frame

Transmit:

User_data → GFP_source adaptation → scramble and DC_balance → SDH

Receive:

SDH → un_DC_balance and unscramble → GFP_sink decapsulation → client data

The following worked example shows the encapsulation of a 64-byte Ethernet frame with linear header and FCS, before DC balancing and self-synchronous scrambling. The Ethernet data octets are mapped to the GFP octet according to a reversed transmission bit order relative to the Ethernet transmission bit order (i.e., bit 0 in clause 3 of [IEEE 802.3] corresponds to GFP octet bit 8, and bit 7 in clause 3 of [IEEE 802.3] corresponds to GFP octet bit 1). The hex values in this example are oriented such that the MSB is on the left and the LSB right.

Byte	Field	Value (hex)	Comment
1	PLI[15:8]	00	; PLI = Length { payload header + payload information field }
2	PLI[7:0]	48	; = 8 + 64 = 72 bytes
3	cHEC[15:8]	C9	;
4	cHEC[7:0]	CC	;
5	TYPE[15:8]	01	; [15:13] = '000' (client data)
6	TYPE[7:0]	01	; [12] = '0' (pFCS disabled)
7	tHEC[15:8]	23	; [11:8] = '0001' (linear header)
8	tHEC[7:0]	10	; [7:0] = '00000001' (Ethernet)
9	EHDR[15:8]	80	; CID[07:00] = 0x8000 (the value is just an example)
10	EHDR[7:0]	00	; SPARE[7:0]
11	eHEC[15:8]	1B	; eHEC calculated over CID,SPARE
12	eHEC[7:0]	98	; End extension header
13	DATA	FF	; 1d Ethernet DA = 0xFFFFFFFFFFFF
14	DATA	FF	; 2d
15	DATA	FF	; 3d
16	DATA	FF	; 4d
17	DATA	FF	; 5d
18	DATA	FF	; 6d
19	DATA	06	; 7d Ethernet SA = 0x060504030201
20	DATA	05	; 8d
21	DATA	04	; 9d
22	DATA	03	; 10d
23	DATA	02	; 11d

Byte	Field	Value (hex)	Comment
24	DATA	01	; 12d
25	DATA	00	; 13d Ethernet TYPE/LENGTH
26	DATA	2E	; 14d
27	DATA	00	; 15d Ethernet payload
28	DATA	01	; 16d
29	DATA	02	; 17d
30	DATA	03	; 18d
31	DATA	04	; 19d
32	DATA	05	; 20d
33	DATA	06	; 21d
34	DATA	07	; 22d
35	DATA	08	; 23d
36	DATA	09	; 24d
37	DATA	0A	; 25d
38	DATA	0B	; 26d
39	DATA	0C	; 27d
40	DATA	0D	; 28d
41	DATA	0E	; 29d
42	DATA	0F	; 30d
43	DATA	10	; 31d
44	DATA	11	; 32d
45	DATA	12	; 33d
46	DATA	13	; 34d
47	DATA	14	; 35d
48	DATA	15	; 36d
49	DATA	16	; 37d
50	DATA	17	; 38d
51	DATA	18	; 39d
52	DATA	19	; 40d
53	DATA	1A	; 41d
54	DATA	1B	; 42d
55	DATA	1C	; 43d
56	DATA	1D	; 44d
57	DATA	1E	; 45d
58	DATA	1F	; 46d
59	DATA	20	; 47d
60	DATA	21	; 48d
61	DATA	22	; 49d
62	DATA	23	; 50d
63	DATA	24	; 51d
64	DATA	25	; 52d

Byte	Field	Value (hex)	Comment
65	DATA	26	; 53d
66	DATA	27	; 54d
67	DATA	28	; 55d
68	DATA	29	; 56d
69	DATA	2A	; 57d
70	DATA	2B	; 58d
71	DATA	2C	; 59d
72	DATA	2D	; 60d
73	DATA	DE	; 61d Ethernet FCS computed over 60 bytes
74	DATA	E1	; 62d
75	DATA	90	; 63d
76	DATA	D0	; 64d

The core header is XORed with the DC Barker code, the rest of the GFP frame is unchanged.

Byte	Field	Value (hex)	Comment
1	PLI[15:8]	B6	; 00 XOR B6
2	PLI[7:0]	E3	; 48 XOR AB
3	cHEC[15:8]	F8	; C9 XOR 31
4	cHEC[7:0]	2C	; CC XOR E0
5	...		

The following example shows the calculation of the cHEC for PLI[15:0] = 0x0048. The polynomial is $G(x) = x^{16} + x^{12} + x^5 + 1$. The PLI is shifted into the CRC-16 calculator with PLI[15:8] first, then PLI[7:0], MSB first for each octet.

		x^{15} ... x^0
		0000000000000000 ← CRC-16 initial state
Input bit	1	0001000000100001 ← CRC-16 after input bit
	0	0010000001000010
	0	0100000010000100
	1	1001000100101001
	0	0011001001110011
	0	0110010011100110
	0	1100100111001100

Transmit the CRC-16 starting from x^{15} gives the GFP octets cHEC[15:0] = 0xC9CC.

The GFP frame is input to the x^{43}+1 scrambler in network bit order (MSB first). Starting with the first byte of the TYPE field (the core header is not scrambled):

Bit #1	TYPE[15]
Bit #2	TYPE[14]
Bit #3	TYPE[13]
...	

III.2 Worked example for a GFP-T superblock CRC calculation

This clause provides a worked example calculation of the CRC-16 for a GFP-T superblock. For this example, the first octet of the superblock (octet 1,1) contains the value 80 hex (i.e., a 1 in the MSB position), and all other octets in the superblock, including the L-bit octet, contain all 0s. The resulting CRC-16 value will be 1001 1010 1010 0010 (9AA2 hex) in bits CRC-1-CRC-16, respectively.

III.3 Worked example for a GFP-F encapsulated MPLS frame

The following worked example shows the encapsulation of a 28-byte MPLS frame with null extension header and FCS, before DC balancing and self-synchronous scrambling. The same methods as in clause III.1 are used for core and type header CRC calculation and the core header encoding. The hex values in this example are oriented such that the MSB is on the left and the LSB right.

Byte	Field	Value (hex)	Comment
1	PLI[15:8]	00	; PLI = Length { payload header + payload information field + pFCS }
2	PLI[7:0]	24	; = 4 + 28 + 4 = 36 bytes
3	cHEC[15:8]	64	;
4	cHEC[7:0]	E6	;
5	TYPE[15:8]	10	; [15:13] = '000' (client data)
6	TYPE[7:0]	0D	; [12] = '1' (pFCS enabled)
7	tHEC[15:8]	D2	; [11:8] = '0000' (null extension header)
8	tHEC[7:0]	DE	; [7:0] = '00001101' (MPLS)
9	DATA	00	; 1d MPLS headers
10	DATA	01	; 2d
11	DATA	70	; 3d
12	DATA	FE	; 4d
13	DATA	00	; 5d
14	DATA	01	; 6d
15	DATA	21	; 7d
16	DATA	FF	; 8d
17	DATA	49	; 9d MPLS payload
18	DATA	54	; 10d
19	DATA	55	; 11d
20	DATA	2D	; 12d
21	DATA	54	; 13d

Byte	Field	Value (hex)	Comment
22	DATA	20	; 14d
23	DATA	52	; 15d
24	DATA	65	; 16d
25	DATA	63	; 17d
26	DATA	20	; 18d
27	DATA	47	; 19d
28	DATA	2E	; 20d
29	DATA	37	; 21d
30	DATA	30	; 22d
31	DATA	34	; 23d
32	DATA	31	; 24d
33	DATA	20	; 25d
34	DATA	47	; 26d
35	DATA	46	; 27d
36	DATA	50	; 28d
37	FCS[31:24]	87	; First byte of GFP pFCS
38	FCS[23:16]	64	; Covers only payload information field
39	FCS[15:8]	8B	; (i.e., 28 bytes)
40	FCS[7:0]	BB	; Last byte of GFP pFCS.

The core header is XORed with the DC Barker code, the rest of the GFP frame is unchanged.

Byte	Field	Value (hex)	Comment
1	PLI[15:8]	B6	; 00 XOR B6
2	PLI[7:0]	8F	; 24 XOR AB
3	cHEC[15:8]	55	; 64 XOR 31
4	cHEC[7:0]	06	; E6 XOR E0
5	...		

Appendix IV

Number of superblocks used in transparent GFP

(This appendix does not form an integral part of this Recommendation.)

IV.1 Introduction

In GFP-T, there is an integer number (N) of 536-bit superblocks in a client data frame. The value of N must be chosen so that the efficiency of the client data bits relative to the GFP frame overhead bits allows enough bandwidth to transport the client data signal. The value of N can be chosen to allow enough additional SBW in the channel for the transport of CMFs and MCFs. The minimum values of N are shown here as a function of the various overhead bits and the number of CMFs (CMFs) or MCFs that are allowed to be transmitted between successive GFP-T client data frames.

IV.2 Calculation of spare bandwidth

The SBW in a GFP-T channel is specified as:

SBW = (minimum bit rate for carrying client bits in the channel) − (client data bit rate)

= (minimum channel bit rate) (ratio of client data bits to total bits) − (client data bit rate)

where:

the client data bit rate is the data rate after decoding the block line code (e.g., 8B/10B), and the total number of bits in the channel is the client data bits plus all GFP-T overhead bits.

SBW as a function of N is:

$$\mathrm{SBW}(N) = (\mathrm{Min.Chan.rate})\left(\frac{\text{client data bits/GFP-T frame}}{\text{total bits/GFP-T frame}}\right) - (\text{Max. client data rate})$$

$$\mathrm{SBW}(N) = \frac{(512)(N)(\mathrm{ChBW}_{\min})}{\mathrm{GFPOH} + (536)(N)} - \mathrm{CSBW}_{\max}$$

where:

$\mathrm{ChBW}_{\min}$ = transport channel bandwidth with slowest end of the transport clock tolerance

$\mathrm{CSBW}_{\max}$ = client signal data rate with fastest end of the client clock tolerance

GFPOH = the number of GFP overhead bits

The minimum value of N is the smallest N such that SBW(N) > 0:

$$N_{\min} = \left\lceil \frac{(\mathrm{CSBW}_{\max})(\mathrm{GFPOH})}{(512)(\mathrm{ChBW}_{\min}) - (536)(\mathrm{CSBW}_{\max})} \right\rceil$$

where the notation $\lceil x \rceil$ represents the smallest integer that is $\geq x$.

The minimum VC path sizes with their associated $N_{\min}$ values are shown in Table IV.1.

Table IV.1 – SDH path capacity and number of superblocks per transparent GFP frame

Client unencoded data rate	Example client signal	VC path size	Min. number of superblocks/GFP frame
160 Mbit/s	ESCON	VC-3-4v	1
216 Mbit/s	DVB ASI	VC-4-2v	1
425 Mbit/s	Fibre channel	VC-4-3v	13
850 Mbit/s	Fibre channel/FICON	VC-4-6v	13
1 000 Mbit/s	Gigabit Ethernet	VC-4-7v	95
1 700 Mbit/s	Fibre channel	VC-4-12v	13
3 400 Mbit/s	Fibre channel	VC-4-24v	13
NOTE – The minimum number of superblocks shown here assumes a null extension header and no optional pFCS.			

IV.3 Calculation of available bandwidth for CMFs and MCFs

For compactness, CMF is used in this clause to indicate either CMFs or MCFs. The bandwidth available to be used for CMFs is the SBW subject to the constraints on the number of CMFs that can be transmitted between two client data frames. If there were no restrictions on the number of CMFs that could be transmitted, then the largest allowable value of *N* would give the largest amount of bandwidth available for CMFs, where:

$N_{\max}$ = (65 536 – GFPOH)/67
= 978 with no extension header or pFCS; and
= 977 with extension header or pFCS

In order to minimize the latency and buffering requirements associated with the ingress to the GFP-T source adaptation process, it is desirable to send no more than one CMF between client data frames. The longer the client data frames are, the fewer the opportunities per second exist for transmitting CMFs (i.e., the fewer inter-client data frame gaps exist for sending CMFs). As a result, as *N* increases, the number of CMF transmission opportunities decreases, and hence the available CMF bandwidth decreases. With this restriction, the optimum value of *N* is the one that fills the entire bandwidth with exactly one CMF per client data frame. A smaller value of *N* would reduce the SBW such that it is not adequate to allow a CMF between each client data frame. A larger value of *N* would result in fewer CMFs per second. In general, if *m* CMFs are allowed to be transmitted between client data frames, the available CMF bandwidth is:

$$\mathrm{CMFBW}(N,m) = (\mathrm{CMF/second})(\mathrm{bits/CMF})$$

$$\mathrm{CMFBW}(N,m) = \frac{(\mathrm{ChBW}_{\min})(\mathrm{CMFL})(m)}{(m)(\mathrm{CMFL}) + \mathrm{GFPOH} + (536)(N)}$$

where:

CMFL = CMF frame length

m = the number of CMFs that can be transmitted between client data frames, and there is a constraint that:

$$\frac{(512)(N)(\mathrm{ChBW}_{\min})}{\mathrm{GFPOH} + (536)(N) + (m)(\mathrm{CMFL})} \geq \mathrm{CSBW}_{\max}$$

The actual payload bandwidth of the CMFs is the ratio of the CMF payload area to the total CMF frame length:

$$\mathrm{CMPLBW} = [\mathrm{CMFBW}(N, m)]\left(\frac{\mathrm{CMFPAL}}{\mathrm{CMFL}}\right)$$

where:

CMPLBW = the CMF usable payload bandwidth

CMFPAL = the number of bits in the CMF payload area used for CMF payload (i.e., the payload area minus the pFCS, if it is used)

For a given value of *m*, the value of *N* that gives the most useable CMF bandwidth will be the integer closest to:

$$N_{\mathrm{opt}} = \frac{(\mathrm{CSBW}_{\mathrm{max}})[\mathrm{GFPOH} + (m)(\mathrm{CMFL})]}{(512)(\mathrm{ChBW}_{\mathrm{min}}) - (536)(\mathrm{CSBW}_{\mathrm{max}})}$$

Appendix V

Bandwidth requirements for Ethernet transport

(This appendix does not form an integral part of this Recommendation.)

This appendix shows the transport bandwidth requirements for client data over Ethernet over GFP over a synchronous optical network (SONET) as a function of the Ethernet MAC rate, the client payload field length, whether the network has inserted a VLAN tag, and whether the GFP pFCS is used. This information is shown in Tables V.1 to V.4.

NOTE – The MAC bit rate in Tables V.1 to V.3 is the actual bit rate of the Ethernet MAC frames after the removal of the 12-byte IPG plus 7-byte preamble + 1-byte SFD. In other words, MAC bit rate = (Ethernet interface rate) (No. of bits in the MAC frame)/(No. of bits in the MAC frame + 12-byte IPG + 7-byte preamble + 1-byte SFD). The calculations in Table V.4 are the same, except that the 10 Gbit Ethernet uses a 5-byte minimum IPG instead of 12 bytes.

Table V.1 – Maximum (un)tagged MAC bit rate per "10 Mbit/s" MAC server signal

			Payload bit rate (nominal bit rate for Ethernet)								
			10 000	**9 600**		**11 200**		**8 704**		**10 880**	
			MAC bit rate (kbit/s), throughput (%) relative to maximum MAC bit rate								
GFP-FCS	**VLAN tag**	**MAC-size (bytes)**	**10Base-T**	**VC-11-6v**	**Throughput**	**VC-11-7v**	**Throughput**	**VC-12-4v**	**Throughput**	**VC-12-5v**	**Throughput**
0	0	64	7 619	8 533	112.0	9 956	131	7 737	101.5	9 671	127
0	0	128	8 649	9 055	104.5	10 541	122	8 192	94.7	10 240	118
0	0	256	9 275	9 309	100.4	10 861	117	8 440	91.0	10 550	114
0	0	512	9 624	9 452	98.2	11 028	115	8 570	89.0	10 713	111
0	0	1 024	9 808	9 526	97.1	11 113	113	8 637	88.1	10 796	110
0	0	1 518	9 870	9 550	96.8	11 141	113	8 658	87.7	10 823	110
0	0	9 618	9 979	9 592	96.1	11 191	112	8 697	87.1	10 871	109
0	1	64	7 727	8 589	111.2	10 021	130	7 788	100.8	9 735	126
0	1	128	8 684	9 051	104.2	10 560	122	8 207	94.5	10 258	118
0	1	256	9 286	9 313	100.3	10 866	117	8 444	90.9	10 555	114
0	1	512	9 627	9 453	98.2	11 029	115	8 571	89.0	10 714	111
0	1	1 024	9 809	9 526	97.1	11 114	113	8 637	88.0	10 796	110
0	1	1 518	9 870	9 550	96.8	11 141	113	8 658	87.7	10 823	110
0	1	9 618	9 979	9 592	96.1	11 191	112	8 697	87.1	10 871	109

NOTE 1 – GFP-FCS; no = 0, yes = 1. VLAN tag; value gives the number of VLAN tags (no VLAN tag = 0).

NOTE 2 – Encapsulation overhead; 20 bytes for physical Ethernet interface (7-byte preamble, 1-byte SFD and 12-byte minimum IPG). 8-byte encapsulation overhead for GFP without GFP-FCS and 12-byte encapsulation overhead for GFP with GFP-FCS.

Table V.2 – Maximum (un)tagged MAC bit rate per "100 Mbit/s" MAC server signal

			Payload bit rate (nominal bit rate for Ethernet)				
			100 000	**96 768**		**149 760**	
			MAC bit rate (kbit/s), throughput (%) relative to maximum MAC bit rate				
GFP-FCS	**VLAN tag**	**MAC-size (bytes)**	**100Base-T**	**VC-3-2v**	**Throughput**	**VC-4**	**Throughput**
0	0	64	76 190	86 016	100.0	133 120	100.0
0	0	128	86 486	91 076	100.0	140 951	100.0
0	0	256	92 754	93 836	100.0	145 222	100.0
0	0	512	96 241	95 279	99.0	147 456	100.0
0	0	1 024	98 084	96 018	97.9	148 599	100.0
0	0	1 518	98 700	96 261	97.5	148 975	100.0
0	0	9 618	99 792	96 688	96.9	149 636	100.0
0	1	64	77 273	86 582	100.0	133 996	100.0
0	1	128	86 842	91 238	100.0	141 202	100.0
0	1	256	92 857	93 879	100.0	145 290	100.0
0	1	512	96 269	95 291	99.0	147 474	100.0
0	1	1 024	98 092	96 021	97.9	148 604	100.0
0	1	1 518	98 703	96 262	97.5	148 977	100.0
0	1	9 618	99 793	96 688	96.9	149 636	100.0

NOTE 1 – GFP-FCS; no = 0, yes = 1. VLAN tag; value gives the number of VLAN tags (no VLAN tag = 0).

NOTE 2 – Encapsulation overhead; 20 bytes for physical Ethernet interface (7-byte preamble, 1-byte SFD and 12-byte minimum IPG). 8-byte encapsulation overhead for GFP without GFP-FCS and 12-byte encapsulation overhead for GFP with GFP-FCS.

Table V.3 – Maximum (un)tagged MAC bit rate per "1 Gbit/s" MAC server signal

			Payload bit rate (nominal bit rate for Ethernet)				
			1 000 000	**898 560**		**1 048 320**	
			MAC bit rate (kbit/s), throughput (%) relative to maximum MAC bit rate				
GFP-FCS	**VLAN tag**	**MAC-size (bytes)**	**1000Base-X**	**VC-4-6v**	**Throughput**	**VC-4-7v**	**Throughput**
0	0	64	761 905	798 720	100.0	931 840	100.0
0	0	128	864 865	845 704	97.8	986 654	100.0
0	0	256	927 536	871 331	93.9	1 016 553	100.0
0	0	512	962 406	884 736	91.9	1 032 192	100.0
0	0	1 024	980 843	891 594	90.9	1 040 193	100.0
0	0	1 518	986 996	893 849	90.6	1 042 824	100.0
0	0	9 618	997 925	897 813	90.0	1 047 449	100.0
0	1	64	772 727	803 975	100.0	937 971	100.0
0	1	128	868 421	847 214	97.6	988 416	100.0
0	1	256	928 571	871 737	93.9	1 017 027	100.0
0	1	512	962 687	884 842	91.9	1 032 315	100.0
0	1	1 024	980 916	891 621	90.9	1 040 225	100.0
0	1	1 518	987 030	893 862	90.6	1 042 839	100.0
0	1	9 618	997 926	897 814	90.0	1 047 449	100.0

NOTE 1 – GFP-FCS; no = 0, yes = 1. VLAN tag; value gives the number of VLAN tags (no VLAN tag = 0).

NOTE 2 – Encapsulation overhead; 20 bytes for physical Ethernet interface (7-byte preamble, 1-byte SFD and 12-byte minimum IPG). 8-byte Encapsulation overhead for GFP without GFP-FCS and 12-byte encapsulation overhead for GFP with GFP-FCS.

Table V.4 – Maximum (un)tagged MAC bit rate per "10 Gbit/s" MAC server signal

			Payload bit rate (nominal bit rate for Ethernet)						
			10 000 000	**9 884 160**		**9 953 280**		**9 995 277**	
			MAC bit rate (kbit/s), throughput (%) relative to maximum MAC bit rate						
GFP-FCS	**VLAN tag**	**MAC-size (bytes)**	**10GBase-R**	**VC-4-66v**	**Throughput**	**ODU1-4v**	**Throughput**	**ODU2**	**Throughput**
0	0	64	8 311 688	8 785 920	100.0	8 847 360	100.0	8 884 691	100.0
0	0	128	9 078 014	9 302 739	100.0	9 367 793	100.0	9 407 319	100.0
0	0	256	9 516 729	9 584 640	100.0	9 651 665	100.0	9 692 390	100.0
0	0	512	9 752 381	9 732 096	99.8	9 800 153	100.0	9 841 503	100.0
0	0	1 024	9 874 638	9 807 539	99.3	9 876 123	100.0	9 917 794	100.0
0	0	1 518	9 915 088	9 832 343	99.2	9 901 100	99.9	9 942 877	100.0
0	0	9 618	9 986 502	9 875 945	98.9	9 945 008	99.6	9 986 970	100.0
0	1	64	8 395 062	8 843 722	100.0	8 905 566	100.0	8 943 143	100.0
0	1	128	9 103 448	9 319 351	100.0	9 384 521	100.0	9 424 118	100.0
0	1	256	9 523 810	9 589 110	100.0	9 656 167	100.0	9 696 910	100.0
0	1	512	9 754 253	9 733 257	99.8	9 801 322	100.0	9 842 677	100.0
0	1	1 024	9 875 120	9 807 834	99.3	9 876 421	100.0	9 918 093	100.0
0	1	1 518	9 915 309	9 832 478	99.2	9 901 237	99.9	9 943 014	100.0
0	1	9 618	9 986 508	9 875 949	98.9	9 945 011	99.6	9 986 974	100.0

NOTE 1 – GFP-FCS; no = 0, yes = 1. VLAN tag; value gives the number of VLAN tags (no VLAN tag = 0).

NOTE 2 – Encapsulation overhead; 13 bytes for physical Ethernet interface (7-byte preamble, 1-byte SFD and 5-byte minimum IPG). 8-byte encapsulation overhead for GFP without GFP-FCS and 12-byte encapsulation overhead for GFP with GFP-FCS.

Appendix VI

Ethernet physical layer defect signals

(This appendix does not form an integral part of this Recommendation.)

Ethernet defines a number a PHY-specific signals to indicate local and remote defects. These signals fall into two broad categories that are useful to communicate across the GFP-F link: remote defect indications and FDIs.

Tables VI.1 and VI.2 summarize these PHY-specific signals, the conditions under which they are inserted and the PHY layer responses to receiving them. The information in these tables is provided for information only. [IEEE 802.3] is the standard for the complete specification of these signals. GFP RDI frames are sent in response to the remote defect signals of Table VI.1, and GFP FDI frames are sent in response to the local defect signals of Table VI.2.

Table VI.1 – Ethernet PHY remote defect signals

PHY	Remote defect	Condition(s) for insertion	Response when received (per [IEEE 802.3])
10BASE-FB (clause 17 of [IEEE 802.3])	Remote_fault is indicated continuously via a specific pattern of code violations.	Receive jabber, low light or invalid data detected, or continuous clock recovery not met.	Send idle on the link, indicate link is idle.
100BASE-FX, 100BASE-TX over shielded twisted pair (clause 24.3.2.1 of [IEEE 802.3])	Far-end fault indication (FEFI) is indicated continuously via a specific pattern that can be detected but does not cause carrier detect.	PMD sub-layer detects a loss of signal.	Send idle on the link, indicate link is failed.
10/100/1000BASE-TX over UTP (clause 28.2.3.5 of [IEEE 802.3])	Remote fault can be communicated via auto-negotiation. A single bit indicates the presence of a remote fault. The 'next page' capability can further indicate the type of fault as test, link loss or jabber.	Auto-negotiation is invoked immediately when a local failure is detected. The remote fault information is included in the auto-negotiation signalling. The auto-negotiation process will not complete while the local failure exists. When the local failure clears, auto-negotiation stops signalling the remote failure.	Continue auto-negotiation until it completes successfully. The remote fault is indicated in the status register. The link is considered failed until auto-negotiation is complete.

Table VI.1 – Ethernet PHY remote defect signals

PHY	Remote defect	Condition(s) for insertion	Response when received (per [IEEE 802.3])
1000BASE-X (clause 37.2.1.5 of [IEEE 802.3])	Remote fault is detected if the received configuration register information is all zeros for longer than the expected amount of time. The configuration register also includes bits to indicate a remote fault, but those bits are not set until the fault has cleared, so they are not useful as an indication that a remote fault exists (the fault has cleared by the time the bits are set).	Auto-negotiation is invoked immediately when a failure is detected. In the absence of character synchronization, the state machine remains in the an_enable state, which fixes the configuration register information at all zeros.	Continue auto-negotiation until it completes successfully. The link is considered failed until auto-negotiation is complete.
All 10G PHYs (clauses 46.3.4 and 66.3 of [IEEE 802.3])	Remote fault is indicated continuously via an ordered set.	The receive reconciliation sub-layer detects a local fault.	Send idle on the link.

Table VI.2 – Ethernet PHY local defect signals

PHY	local defect	Inserted when…	Response when received (per [IEEE 802.3])
1000Base-X (clause 37.2.1.5 of [IEEE 802.3])	Offline can be communicated via auto-negotiation.	When a management action causes the link to be administratively out of service, the link can be renegotiated with the offline signal included. Having sent this indication, the local end can then take the link out of service without waiting for auto-negotiation to complete.	No direct response to receiving offline, but the link will be considered failed until auto-negotiation completes successfully and the offline status will be set in the status register.
All 10G PHYs (clauses 46.3.4 and 66.3 of [IEEE 802.3])	Local fault is indicated continuously via an ordered set.	A local fault in the transmitter is detected.	Generate remote fault.

Appendix VII

Ethernet throughput of ODUflex for GFP-F mapped client signals

(This appendix does not form an integral part of this Recommendation.)

While the normal application of ODUflex for GFP-F mapped client signals is to provide a sub-rate or VLAN service, it is instructive to examine the Ethernet packet throughput available for various ODUflex sizes.

The sizes of ODUflex for various tributary slot sizes are shown in Table VII.1.

Table VII.1 – ODUflex(GFP) capacity per tributary slot

	ODUflex(GFP) capacity	**OPUflex(GFP) capacity**
ODUflex(GFP) of n tributary slots, $1 \leq n \leq 8$	$n \times 1\ 249\ 177.230$	$n \times 1\ 243\ 950.547$
ODUflex(GFP) of n tributary slots, $9 \leq n \leq 32$	$n \times 1\ 254\ 470.354$	$n \times 1\ 249\ 221.524$
ODUflex(GFP) of n tributary slots, $33 \leq n \leq 80$	$n \times 1\ 301\ 467.133$	$n \times 1\ 296\ 021.664$

Figure VII.1 indicates packet data throughput against packet size for ODUflex(GFP) as well as Ethernet PHYs (1000BASE-X, 10GBASE-R).

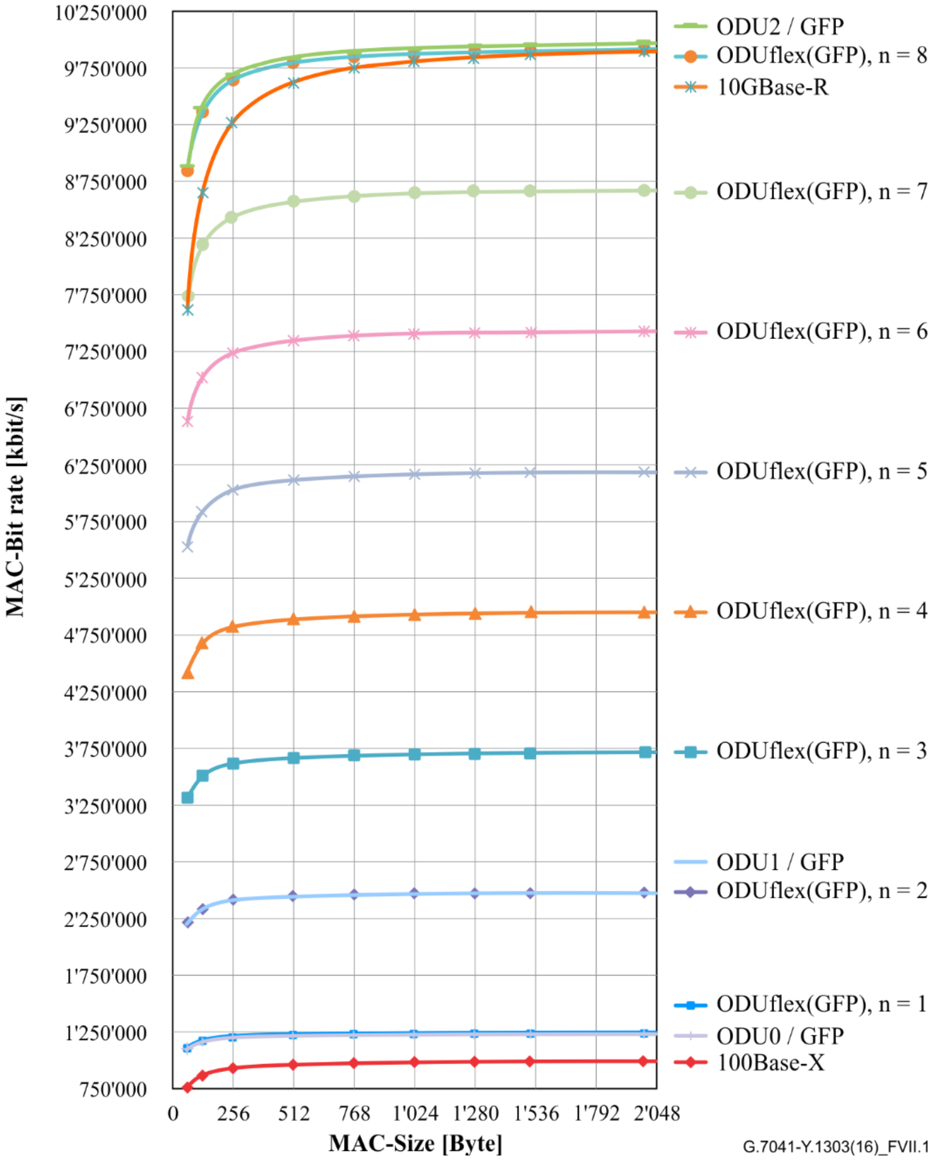


Figure VII.1 – Packet data throughput for ODUflex(GFP), *n* = 1,…,8, ODUk (*k* = 0,1,2), 1000Base-X, 10GBase-R

Bibliography

[b-ITU-T G.823] Recommendation ITU-T G.823 (2000), *The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy*.

[b-ITU-T V.41] Recommendation ITU-T V.41 (1988), *Code-independent error-control system*.

[b-ITU-T G-Sup.43] Supplement ITU-T G-Sup.43 (2011), *Transport of IEEE 10GBASE-R in optical transport* networks *(OTN)*.

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	**Y.1300–Y.1399**
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2017