ANSI®

T1.xxx.yy-200x

T1X1.5/2000-024R3 (Draft ANSI T1.xxx.yy-200x)

American National Standard
for Telecommunications —

Generic Framing Procedure —

Secretariat:

Alliance for Telecommunications Industry Solutions

Approved <date>

American National Standards Institute, Inc.

Abstract

<To be supplied>

Contents

Page

Tables

Figures

Foreword (This foreword is not part of American National Standard T1.xxx.yy-200x.)

<To be supplied>

American National Standard
for Telecommunications –

Generic Framing Procedures (GFP) –

1. Scope

This document defines a generic framing procedure (GFP) to delineate octet-aligned, variable-length payloads from higher-level client signals for subsequent mapping into octet-synchronous payload envelopes such as those defined in ANSI T1.105.02 and ITU-T G.709. It also defines the frame formats for protocol data units (PDUs) transferred between GFP initiation and termination points, as well as the mapping procedure for the client signals into GFP.

2. Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this American National Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this American National Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

ANSI T1.105-1995, *Telecommunications – Digital hierarchy – Optical Interface Rates and Formats Specifications (SONET)*

ANSI T1.105.02 –1999, *Telecommunications – Synchronous Optical Networks (SONET) – Payload Mappings*

ANSI X3.230-1994, *Fibre Channel Physical and Signaling Interface (FC-PH), Rev 4.3*, June-1994.

ANSI X3.230-1996, *Single-Byte Command Code Sets Connection Architecture (SBCON), Rev 2.3*, Sep-1996.

ITU-T Draft Recommendation G.709*, ITU-T Network Node Interface for the Optical Transport Network (OTN), February 2001*

ISO/IEC 3309:1993, *Information Technology – Telecommunications and Information Exchange Between Systems – High-level Data Link Control (HDLC) Procedures – Frame Structure*

IEEE 802.3-1998, Part 3:, *Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*, 1998.

IETF RFC 1661, *The Point-to-Point Protocol (PPP),* July 1994

IETF RFC 1662, *PPP in HDLC-like Framing,* July 1994

IETF RFC 2615, *PPP over SONET/SDH,* June 1999

3. Definitions and Classifications

For detailed SONET definitions see ANSI T1.105. For detailed OTN definitions see ITU-T G.709.

3.1 Network Octet Order (NOO): A transport network convention in which the most significant octets from a logical information unit are transmitted first over the network facility.

3.2 Network Bit Order (NBO): A data transport rule in which the most significant bit from a logical information unit are transmitted first over the network facilities.

3.3 Maximum Transmission Unit (MTU): Maximum size of the GFP Payload Area, in octets.

3.4 Source/Destination Port (SP/DP): A logical addressable entity on a physical interface.

3.5 Frame-mapped GFP: A type of GFP mapping in which a client signal frame is received and mapped in its entirety into one or more GFP frames.

3.6 Transparent GFP: A type of 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.

3.7 Running Disparity: A procedure used by block line codes, such as 8B/10B, to balance the total of number of ones and zeros transmitted over time. The running disparity at the end of a line code sub-block is positive if more ones than zeros have been sent up to that point, and negative if more zeros than ones 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 ones and zeros.

4. Abbreviations

ANSI	American National Standards Institute
ATM	Asynchronous Transfer Mode
cHEC	Core HEC
CRC	Cyclic Redundancy Check
CSF	Client Signal Failure
DP	Destination Port
eHEC	Extended HEC
EXI	Extension Header Identifier
FCS	Frame Check Sequence
GFP	Generic Framing Procedure
HDLC	High-level Data Link Control
HEC	Header Error Check
IP	Internet Protocol
IPG	Inter-Packet Gap
ISDN	Asynchronous Transfer Mode

ITU-T International Telecommunication Union – Telecommunication Standardization Sector

LSB Least Significant Bit

MAC Media Access Control

MSB Most Significant Bit

NE Network Element

OA&M Operations, Administration & Maintenance

PDU Protocol Data Unit

PFI Payload FCS Identifier

PLI PDU Length Indicator

PTI Payload Type Identifier

PPP Point-to-Point Protocol

SSF Server Signal Failure

SONET Synchronous Optical Network

SP

SPE Synchronous Payload Envelop

STS Synchronous Transport Signal

tHEC Type HEC

TTL Time-to-Live

UPI User Payload Identifier

5. Introduction

GFP provides a generic mechanism to adapt traffic from higher-layer client signals over an octet synchronous transport network. Client signals may be PDU-oriented (such as IP/PPP or Ethernet MAC), block-code oriented (such as Fibre Channel or ESCON), or a constant bit rate stream.

GFP consists of both common and client-specific aspects. Common aspects of GFP apply to all GFP adapted traffic and they are specified in clause 5. Client-specific aspects of GFP are specified in clauses 6 & 7. Currently, two modes of client signal adaptation are defined for GFP. A PDU-oriented adaptation mode, referred to as Frame-Mapped GFP, is specified in clause 6. A block-code oriented adaptation mode, referred to as Transparent GFP, is specified in clause 7. Client-specific aspects of GFP are specified in clauses 6 & 7. Figure 1 illustrates the relationship between the higher-layer client signals, GFP, and its transport paths.

GFP consists of both common and client-specific aspects. Common aspects of GFP are specified in clause 5. Client-specific aspects of GFP are specified in clauses 6 & 7. Figure 1 illustrates the relationship between the higher-layer client signals, GFP, and its transport paths.

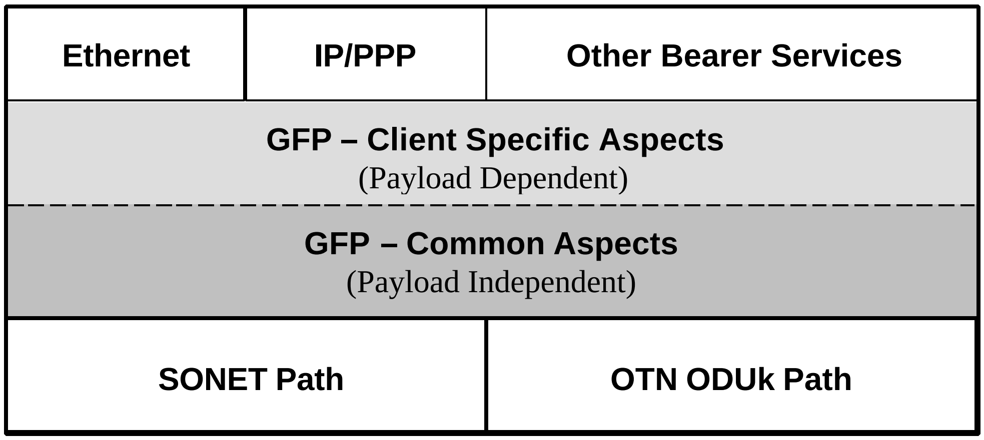


Figure 1: GFP Relationship to Client Signals and Transport Paths

Figure 2 shows a high-level functional model for GFP. In the Frame-Mapped adaptation mode the Client/GFP adaptation function may operate at the physical or data link layer of the client signal. Client PDU visibility is required. 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.

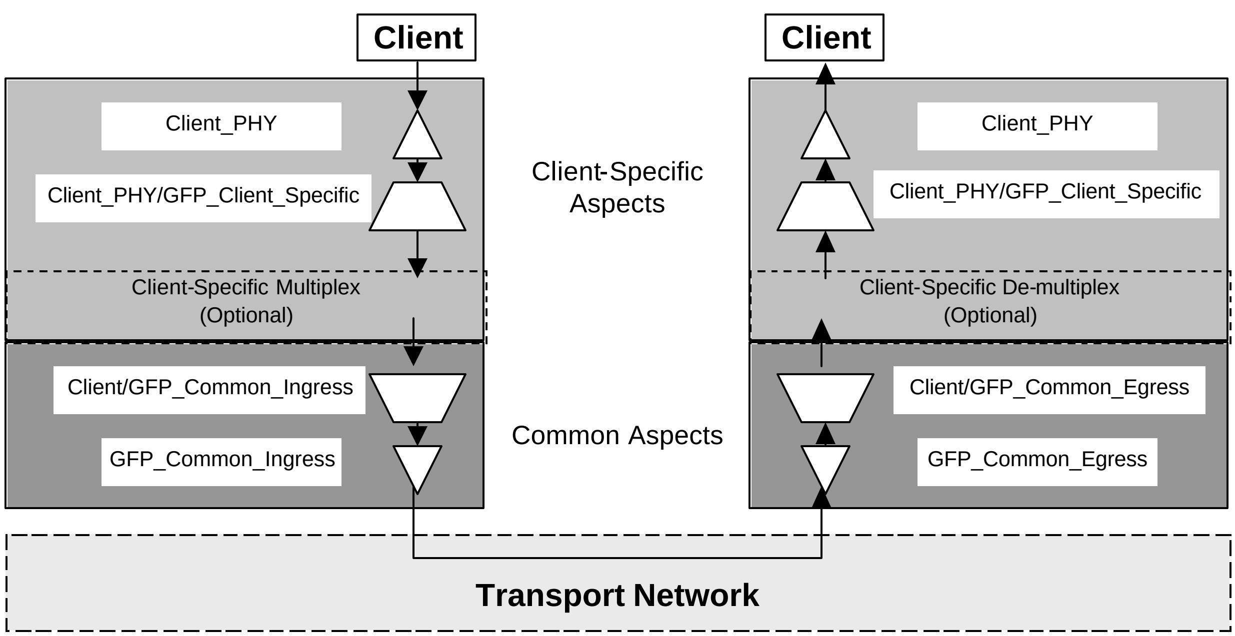


Figure 2: GFP Functional Model (Single Client)

6. Common Aspects of GFP

This clause discusses the common (protocol independent) aspects of GFP for octet-aligned, variable-length payloads. The mapping of the framed payloads into a STS SPE is specified in ANSI T1.105.02. The mapping of the framed payloads into an OTN ODUk payload is specified in ITU-T Recommendation G.709.

GFP uses a variation of the HEC-based frame delineation mechanism defined for ISDN Asynchronous Transfer Mode (ATM) (see ITU-T Recommendation I.432.1-1999). Two kinds of GFP frames are defined: GFP user frames and GFP control frames. Frame formats for GFP user and control frames are defined in clauses 6.1 and 6.2. Common handling procedures for all GFP frames are specified in clause 6.3. GFP also supports a flexible (payload) header extension mechanism to facilitate the adaptation of diverse transport mechanisms via GFP. Currently defined (payload) extension header types are specified in clause 6.4.

Unless otherwise stated all fields in the GFP frame are represented in Network Octet Order (NOO), and all octets are represented in Network Bit Order (NBO), with bit 1 being the most significant bit (MSB) and bit 8 being the least significant bit (LSB).

6.1 GFP User Frames

The format for GFP user frames is shown in Figure 3. GFP user frames are octet-aligned and consist of a GFP Core Header and a GFP Payload Area.

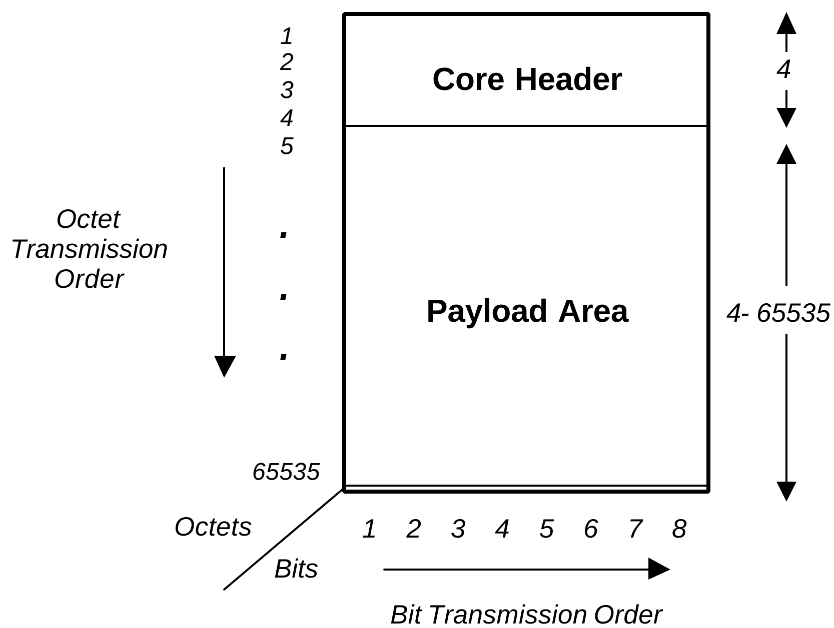


Figure 3: Frame Format for GFP User Frames

6.1.1 GFP Core Header

The GFP Core Header format is shown in Figure 4. The Core Header length is fixed at 4 octets. It is intended to support frame delineation procedures and essential data link operations functions independent of the higher layer PDUs. The GFP Core Header consists of a PDU Length Indicator field and a Core Header Error Check field.

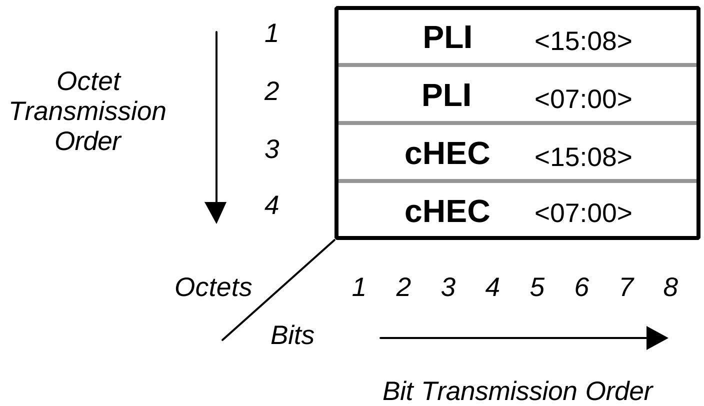


Figure 4: GFP Core Header Format

6.1.1.1 PDU Length Indicator (PLI) Field

The two-octet PLI field contains a binary number representing the number of octets in the GFP Payload Area. PLI values 0-3 are reserved for GFP control frame usage (see clause 6.2).

6.1.1.2 Core HEC (cHEC) Field

The two-octet Core Header Error Control field contains a CRC-16 generated sequence 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 remaining octets of the Core Header. The HEC generation process is defined in clause 6.3.4.

6.1.2 GFP Payload Area

The GFP Payload Area consists of all octets in the GFP frame after the GFP Core Header. This variable length area may include from 4 to 65 535 octets. It is intended to convey higher layer specific protocol information. The GFP Payload Area consists of two common components: a Payload Header and a Payload field. An optional Payload FCS field is also supported. The structure of the GFP Payload Area is depicted in Figure 5.

Practical GFP MTU sizes for the GFP Payload Area are application specific. An implementation should support reception of GFP frames with GFP Payload Areas of at least 1600 octets. By prior arrangement, consenting GFP implementations may use other MTU values.

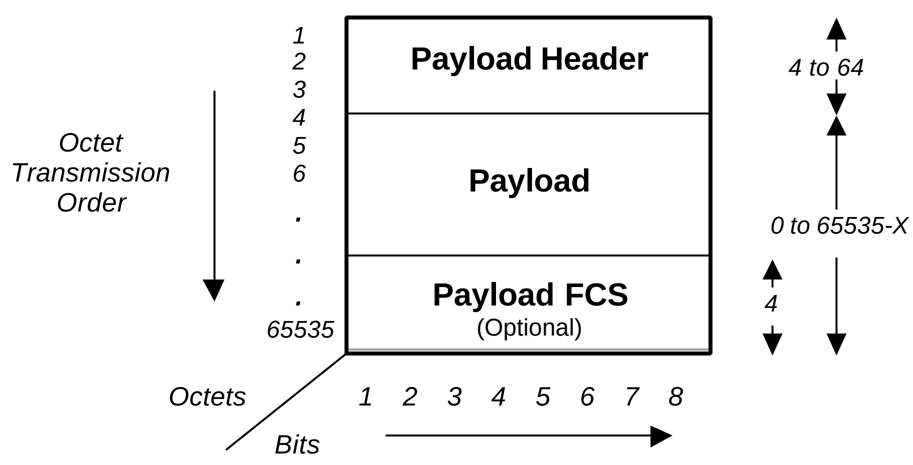


Figure 5: GFP Payload Area Format

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 area contains two mandatory fields, the Type and the tHEC fields, and a variable number of additional payload header fields, referred to as a group as the Extension Header. The presence of the Extension Header, and its format, and the presence of the optional Payload FCS are specified by the Type field. The tHEC protects the integrity of the Type field. The structure of the GFP Payload Header is illustrated in Figure 6.

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

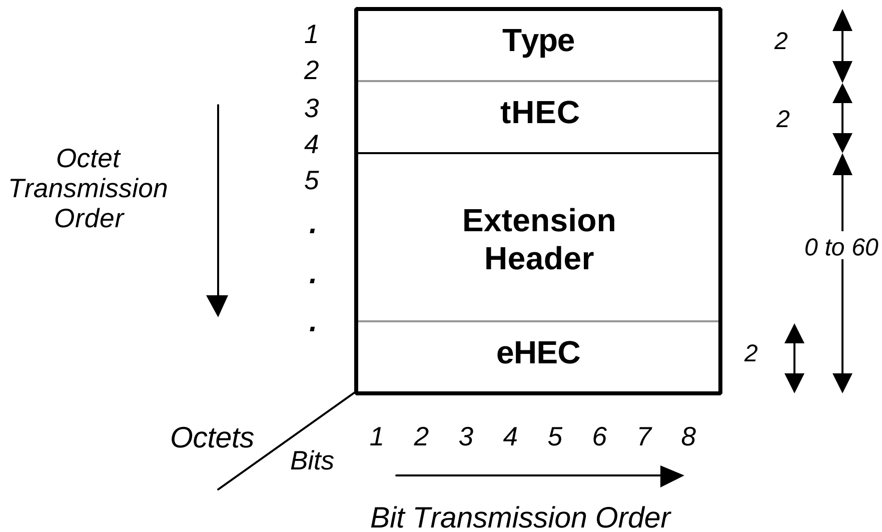


Figure 6: GFP Payload Header Format

.

6.1.2.1.1 GFP Type Field

The GFP Type field is a mandatory 2-octet field of the Payload Header that indicates the content and format of the GFP Payload field (see clause 6.1.2.2). The Type field distinguishes between services in a multi-service environment. The Type field consists of a 3-bit Payload Type Identifier (PTI), a 1-bit Payload FCS Indicator (PFI), a 4-bit Extension Header Identifier (EXI) and an 8-bit User Payload Identifier (UPI). The format of the GFP Type field is illustrated in Figure 7.

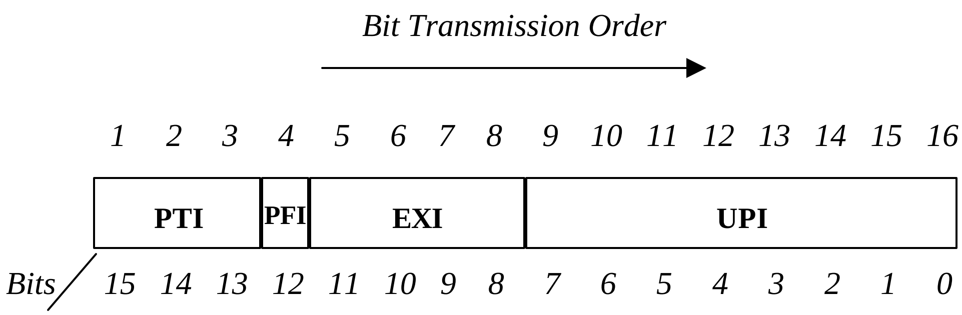


Figure 7: GFP Type Field Format

Defined Payload Type Identifiers, Extension Header Identifiers and Payload Identifiers are given in Tables 1, 2 and 3. PTI is set to zero (PTI=0) for GFP user frames conveying client data. PTI is set to one (PTI=1) for GFP user frames conveying far-end Client Signal Fail indications (clause 6.3.7). The Payload FCS is assumed present whenever PFI is set to one (PFI=1) and absent whenever PFI is set to zero (PFI=0). The interpretation of the UPI field for PTI values different from zero or one is for further study.

6.1.2.1.2 Type HEC (tHEC) Field

The two-octet Type Header Error Control field contains a CRC-16 generated sequence that protects the integrity of the contents of the Type Field by enabling both single-bit error correction and multi-bit error detection. The tHEC generation process is defined in clause 6.3.4.

6.1.2.1.3 GFP Extension Headers

A 0-to-60 octets extended field that supports technology specific data link headers such as virtual link identifiers, source/destination addresses, port numbers, Class of Service, extended header error control, etc. The length and format of the extension header is indicated by the value of the Type field.

6.1.2.1.4 Extension HEC (eHEC) Field

The two-octet Extension Header Error Control field contains a CRC-16 generated sequence that protects the integrity of the contents of the extended headers by enabling both single-bit error correction and multi-bit error detection. The eHEC generation process is defined in clause 6.3.4.

6.1.2.2 Payload Field

The Payload field contains the framed PDU. This variable length field may include from 0 to 65 535 – X octets, where X is the size of the Payload Header. It may include an optional Payload FCS field. The client user/control PDU is always transferred into the GFP Payload field as an octet-aligned packet stream.

6.1.3 Payload Frame Check Sequence (FCS) Field

An optional, four-octet long, frame check sequence. It contains a CRC-32 sequence that protects the contents of the GFP Payload The FCS generation process is defined in 6.4.6. The format of the GFP FCS field is shown in Figure 8. The Type field identifies the presence of the Payload FCS field.

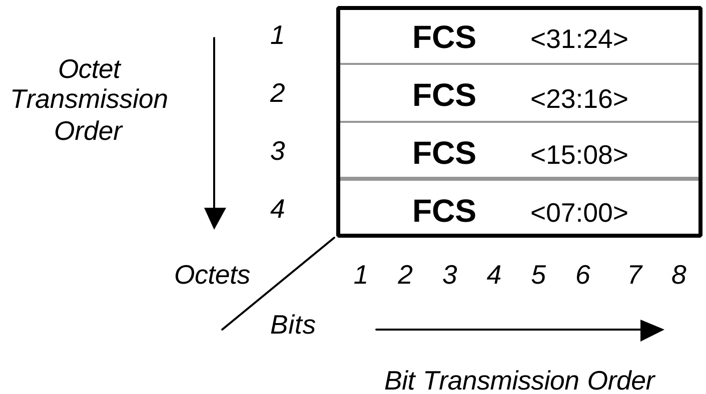


Figure 8: GFP Frame Check Sequence Format

6.2 GFP Control Frames

The lower values of the PLI field are reserved for GFP control purposes. These frames are referred to as GFP control frames. The absolute minimum value of the PLI field in a GFP user frame is 8 octets. GFP assigns special meaning to PLI field values in the 0-3 range. The PDU formats for these messages are depicted in Figure 9. In particular, note that except for the Core Header format GFC control frames do not make use of the same frame fields as the GFP user frames. The CRC-16 for the control message payload is generated using the same general procedure as for the cHEC computation.

All GFP common procedures specified in clause 6.3 apply to GFP control frames.

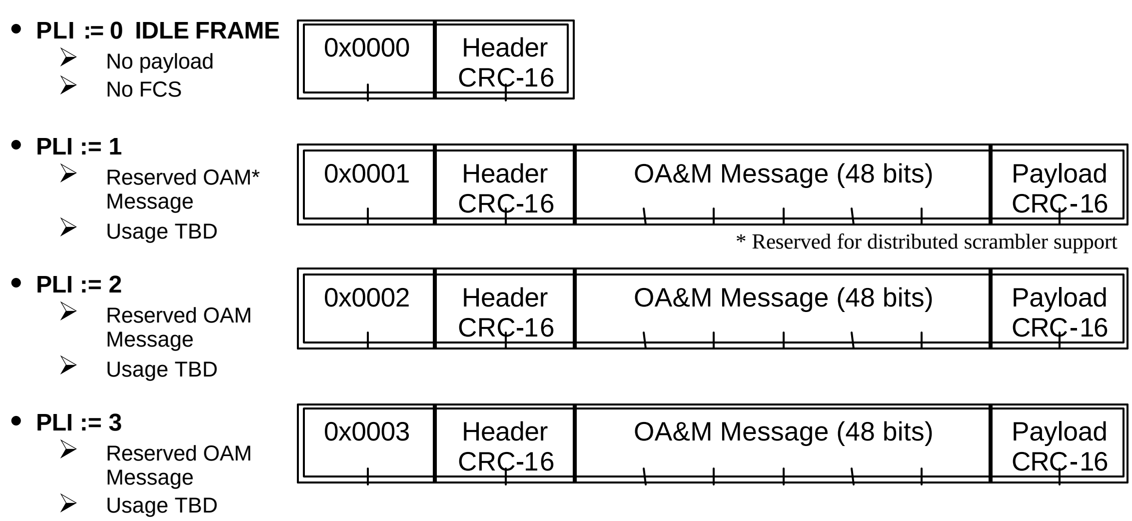


Figure 8: Frame Format for GFP Control Frames

6.2.1 GFP Idle Frames

The GFP Idle frame is a special four-octet GFP control frame. It consists of only a GFP Core Header with the PLI and cHEC fields set to 0. The GFP Idle frame does not contain a Payload Area. It is intended as a filler frame for the GFP transmitter to facilitate the adaptation of the GFP octet stream to any given transport medium. The GFP Idle frame format is shown in Figure 10.

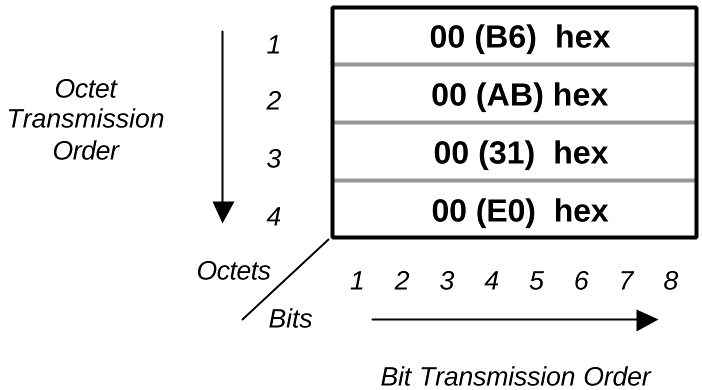


Figure 9: GFP Idle Frame (Barker-like scrambled frame)

6.3 GFP Common Processes

This clause discusses the processes common to all payloads that are framed via GFP. Processes specific to particular payloads are discussed in clauses 6 & 7. The relationships among these processes are illustrated in Figure 11.

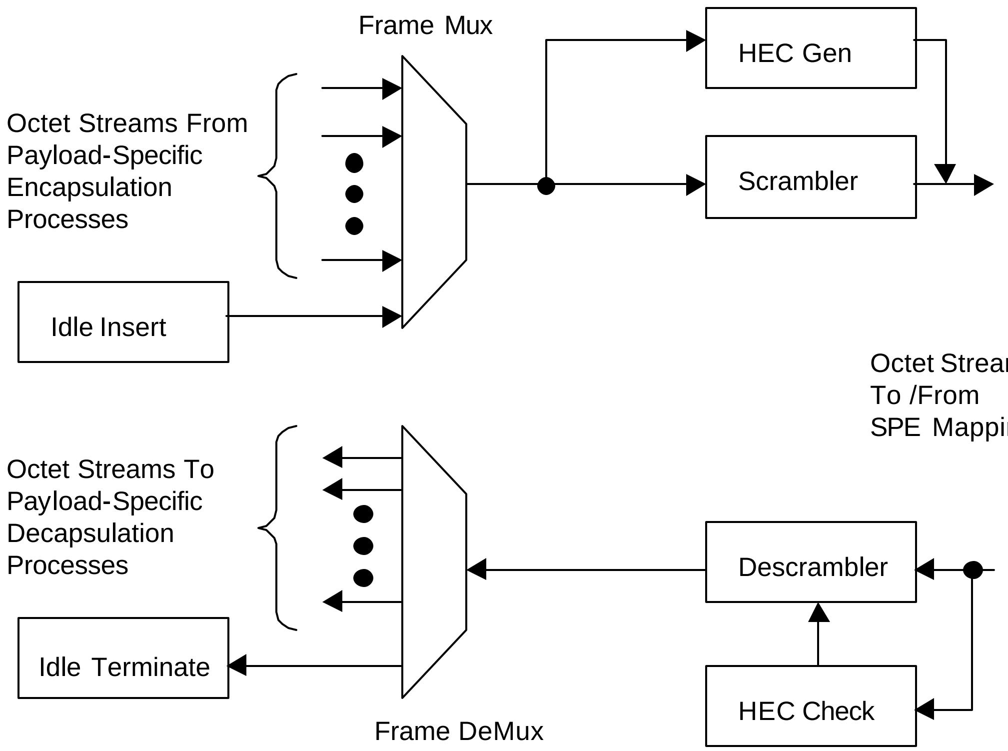


Figure 10: GFP Common (Protocol Independent) Procedures

6.3.1 Frame Multiplexing

GFP frames from multiple ports are multiplexed on a frame-by-frame basis.

When there are no other GFP frames available for transmission, GFP Idle frames must be inserted. This provides a continuous stream of frames for mapping into an octet aligned physical layer.

6.3.2 Payload Area Scrambling

Scrambling of the GFP Payload Area is required to provide security against payload information replicating the frame synchronous scrambling word (or its inverse) (e.g., as used in the SONET Section layer or in an OTN OPUk channel). Figure 12 illustrates the scrambler and descrambler processes.

All octets in the GFP Payload Area are scrambled using a $1 + x^{43}$ self-synchronous scrambler.

At the transmitter, 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.

The activation of the receiver descrambler 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 HEC field and the end of the candidate GFP frame.

When the scrambler/descrambler is disabled its state is retained.

Scrambling is done in network bit order.

Note: the GFP receiver can reliably forward GFP frames to the higher layer entity only when the receiver is in the SYNC state.

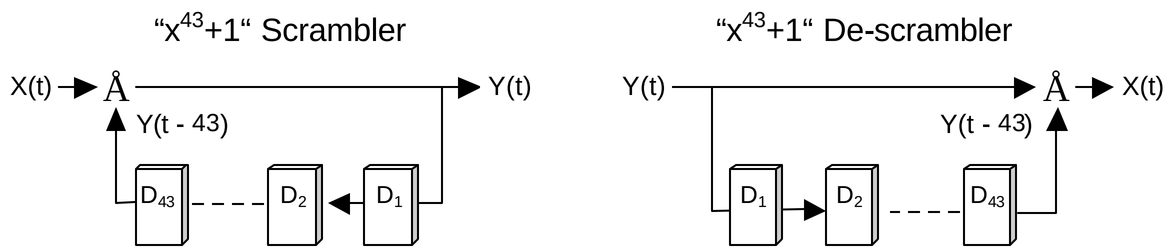


Figure 11: X^{43}+1 Scrambler and De-scrambler Processes for GFP

6.3.3 Core Header Scrambling

The Core Header is DC balanced by an exclusive-OR operation (also known as “modulo 2 addition") with the hex number B6AB31E0. This hex number is the maximum transition, minimum side-lobe, Barker-like sequence of length 32. The scrambling of the GFP Core Header improves robustness of the GFP fame delineation procedure and provides a sufficient number of 0/1 transition density during idle transmission periods.

6.3.4 HEC Processing

The 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 LSB.

The Core HEC (cHEC) field is generated using the following steps (see ITU-T Recommendation V.41, Appendix I):

1. The first two octets of the GFP frame are taken in network octet order, most significant bit 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 most significant bit.
4. This 16-bit sequence is the CRC-16.

The contents of the tHEC and eHEC fields are generated using the same steps, with the following exceptions:

1. For the tHEC step a) is modified such that *M(x)* is formed from all the octets in the Type field, but excluding the tHEC field itself.
2. For the eHEC step a) is modified such that *M(x)* is formed from all the octets in the Extension Header, but excluding the eHEC field itself.

Unless otherwise stated, the GFP receiver performs single-bit error correction on all of the fields protected by a HEC field, and discards any of those GFP frames where multi-bit errors are detected. The receiver also updates any relevant system records for performance monitoring purposes. The first bit of the CRC-16 to be transmitted is the coefficient of x^{15}, the last bit transmitted is the coefficient of x^0.

6.3.5 GFP Frame Delineation Algorithm

GFP uses a modified version of the HEC check algorithm specified in ITU-T I.432, clause 4.5.1.1, to provide GFP frame delineation. The frame delineation algorithm used in GFP differs from that in ITU-T I.432 in two basic ways:

a) The algorithm uses the PDU Length Indicator 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. Figure 13 shows the state diagram for the GFP frame delineation method.

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. Core Header 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 correction is 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 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 Synchronization event is declared and the framing process returns to the HUNT state and a GFP Server Signal Failure (SSF) is indicated to the client adaptation process.

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

Robustness against false delineation in the re-synchronization process depends on the value of DELTA. The parameter DELTA is to be chosen to make the GFP frame delineation process as robust and secure as possible. A value of DELTA=1 is suggested.

Frame delineation robustness can also 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 spawn for each candidate GFP frame detected in the incoming octet stream, as depicted in Figure 13.

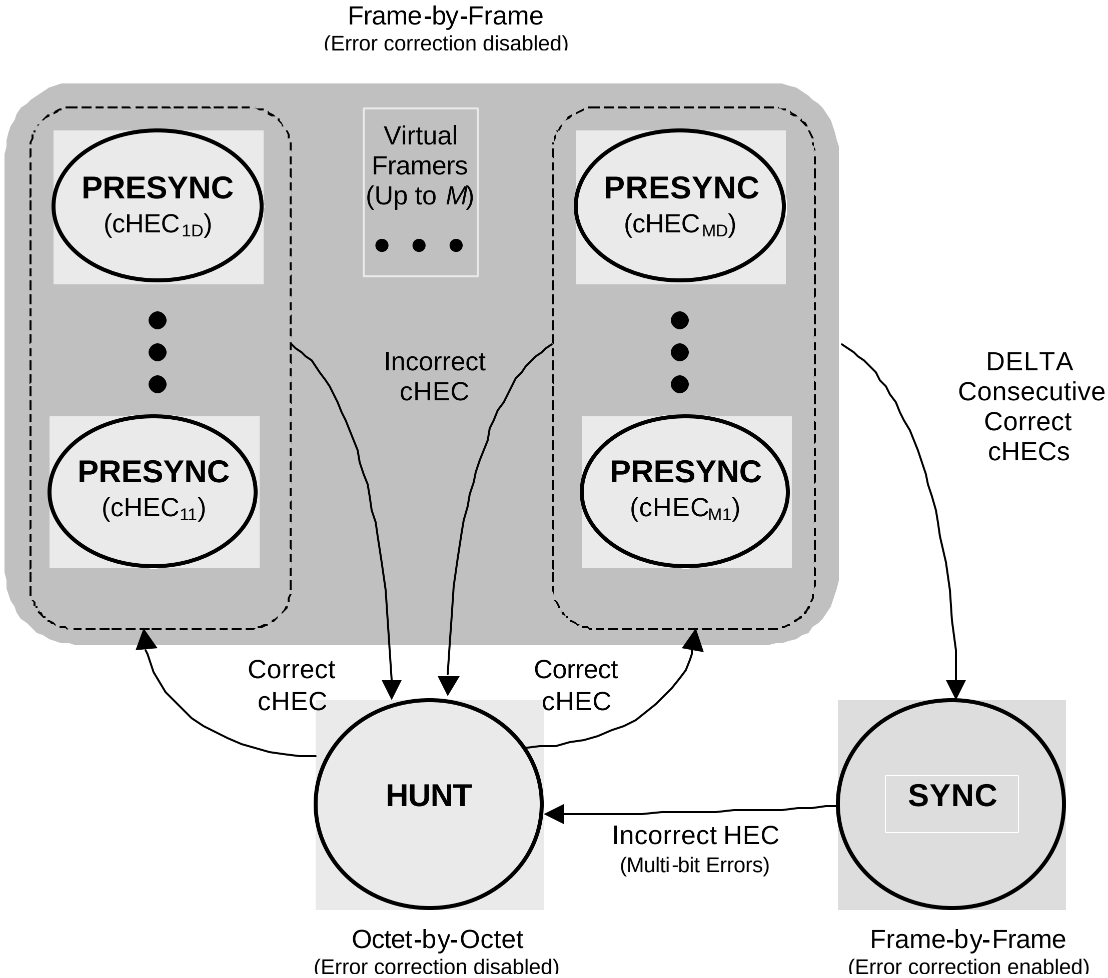


Figure 12: GFP Frame Delineation State Diagram

6.3.6 Payload FCS Generation

The Payload FCS is generated using the ITU-T CRC-32 generating polynomial $G(x)=1 + x^1 + x^2 + x^4 + x^5 + x^7 + x^8 + x^{10} + x^{11} + x^{12} + x^{16} + x^{22} + x^{23} + x^{26} + x^{32}$ where x^{32} corresponds to the MSB and x^0 corresponds to the LSB. The FCS generation procedure uses the initial remainder value of FFFFFFFF hex for calculation and the bits are complemented before transmission.

The Payload FCS field is generated using the following steps:

1. The N octets from the GFP Payload Area, excluding the FCS (when present) are taken in network octet order, most significant bit 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 all-ones polynomial $U(x)=1 + x^1 + x^2 + \ldots + x^{31}$, and divided (modulo 2) by $G(x)$, producing a remainder $R(x)$ of degree 31 or less.
3. The coefficients of $R(x)$ are considered to be a 32-bit sequence, where x^{31} is the most significant bit.
4. The complement of this 32-bit sequence is the CRC-32.

At the receiver, the initial content of the Payload FCS register is initialized to all ones. The final remainder after multiplication by x^{32} and division (modulo 2) by G(x) will be C704DD7B (hex), x^{32} to x^0, respectively.

6.3.7 Far-end Client Signal Fail Indication

GFP provides a generic mechanism for GFP client-specific source adaptation processes to propagate a far-end Client Signal Fail (CSF) indication to the GFP client-specific sink-adaptation process on detection of defects in the ingress client signal.

Detection of client defects is by definition client-specific (see clauses 6 & 7). Upon detection, a GFP transmitter may generate a far-end CSF indication frame as depicted in Figure 14. Far-end CSF indication frames are GFP data frames with the PTI set to User Control (PTI=1). Two generic types of defects can be reported:

- Loss of Client Signal (Control=0)
- Loss of Client Synchronization (Control=1)

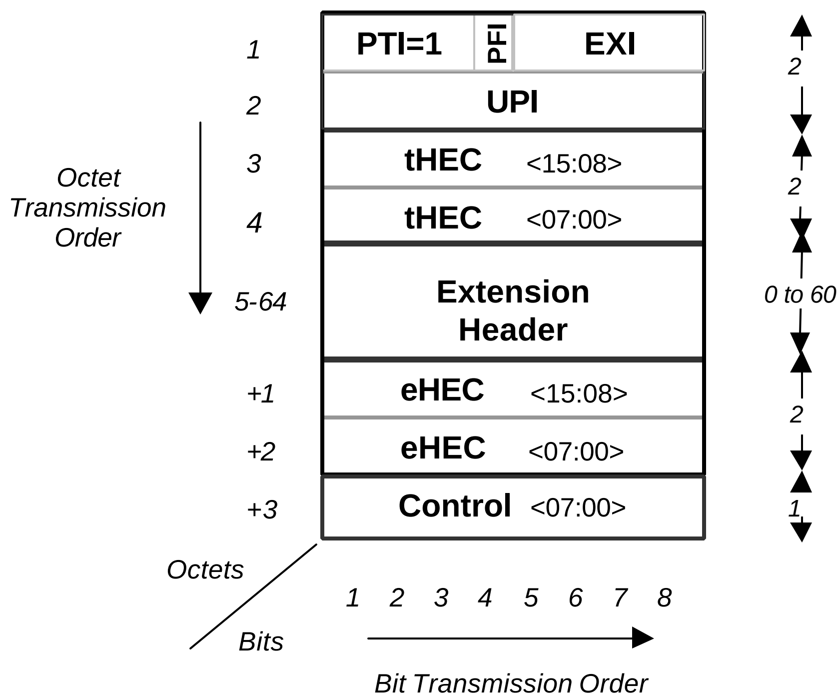


Figure 13: Far-end Client Signal Fail User Frame

Upon detection, the GFP client-specific source adaptation process may send far-end CSF indications at even rate of about one every second. Unless otherwise stated, the GFP client-specific sink adaptation process should clear the defect condition after failing to receive Ncsf consecutive far-end CSF indications. An Ncsf value of 3 is suggested.

6.3.8 Other Defect Handling in GFP

Figure 15 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 SONET or OTN transport network as defined in [REF]. GFP Server Signal Fail events refer to GFP Loss of Synchronization events as defined in the GFP state machine (clause 6.3.5) or propagation of TSF events to the GFP clients. CSF events refer to failure events detected in the client signal on ingress (via a far-end CSF user frame) or egress (client-specific mapping defects such as payload errors, see clauses 6 & 7).

Upon detection of a TSF event or a GFP Loss of Synchronization event, the GFP receiver 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 server-specific) actions to deal with those failure events.

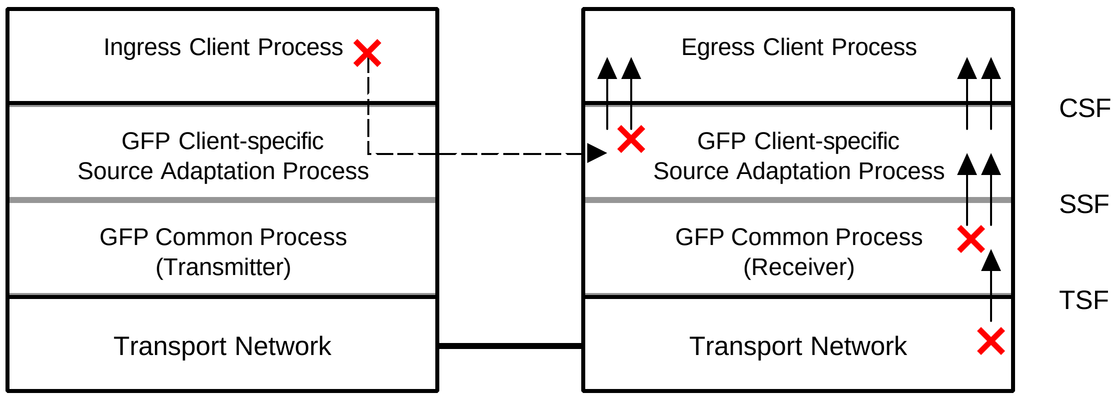


Figure 14: Defect Signal Propagation in GFP

6.4. GFP Extension Header Types

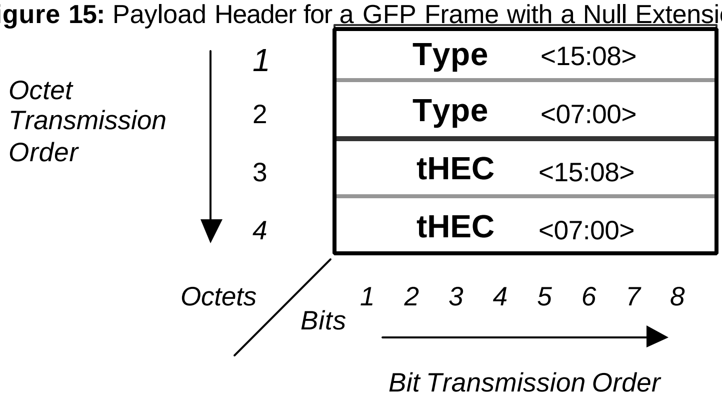
Three Extension Header variants are currently defined to support client specific data over a logical Ring or logical Point-to-Point (Linear) configurations.

Below is a description of the various fields in each Extension Header. The default value for any undefined fields is 0 unless otherwise stated.

6.4.1 Null Extension Header

The Extension Header for a frame with a Null Extension Header is shown in Figure 16. 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 15: Payload Header for a GFP Frame with a Null Extension Header



6.4.2 Extension Header for a Linear Frame

The Extension Header for Linear (Point-to-Point) frame is shown in Figure 17. The following fields are defined within the Extended Header. It is intended for scenarios where the transport path is shared among various client signals.

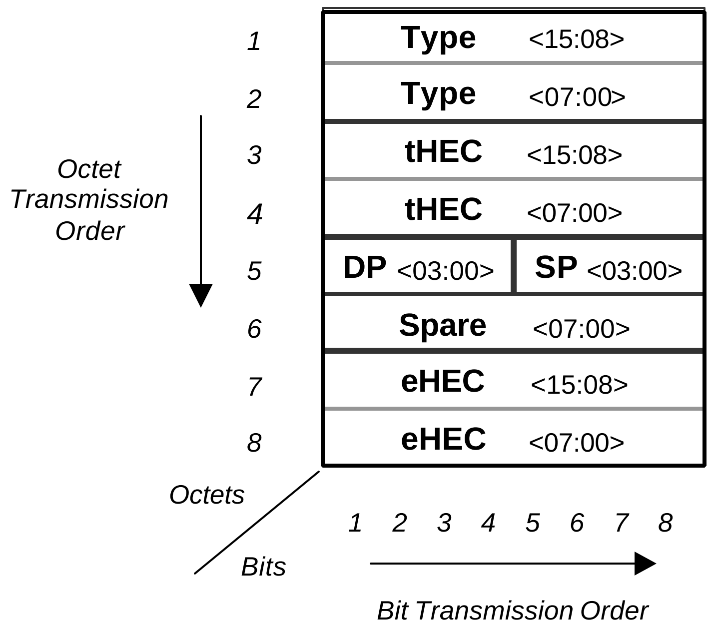


Figure 16: Extension Header for a Linear (Point-to-Point) Frame

6.4.1.1 Destination Port (DP) Field

A 4-bit binary number used to indicate one of 16 destination ports at a GFP termination pointt.

6.4.1.2 Source Port (SP) Field

A 4-bit binary number used to indicate one of 16 source ports at a GFP initiation point.

6.4.1.3 Spare Field

An 8-bit spare field reserved for future use.

6.4.1.4 Extension HEC (eHEC) Field

The two-octet Extension Header Error Control field contains a CRC-16 generated sequence that protects the integrity of the contents of the Extension Header (not including the Type/tHEC fields). The eHEC generation process is defined in clause 6.3.4.

6.4.3 Extension Header for a Ring Frame

The Extension Header for a Ring frame is shown in Figure 18. The following fields are defined within the Extended Header.

6.4.2.1 Spare1 Field

An 8-bit spare field reserved for future use.

6.4.2.2 Priority Field

A 4-bit field used for traffic prioritization purposes. The field is subdivided into 2 components:

- Discard Eligibility (DE) bit
- Class of Service (CoS) bits

6.4.2.3 Time to Live (TTL) Field

An 8-bit binary number representing the remaining number of GFP hops that the GFP PDU will persist. A value of zero indicates that the associated GFP PDU will be terminated at the next GFP termination element.

6.4.2.4 Destination Port (DP) Field

A 4-bit binary number used to indicate one of 16 destination ports at a GFP termination element.

6.4.2.5 Source Port (SP) Field

A 4-bit binary number used to indicate one of 16 source ports at a GFP initiation element.

6.4.2.6 Destination MAC Address Field

A 48-bit binary number that contains the destination MAC address of the GFP termination element.

6.4.2.7 Source MAC Address Field

A 48-bit binary number that contains the source MAC address of the GFP initiation element.

6.4.2.8 Spare2 Field

A 4-bit spare field reserved for future use.

6.4.2.9 Extension HEC (eHEC) Field

The two-octet Extension Header Error Control field contains a CRC-16 generated sequence that protects the integrity of the contents of the Extension Header (not including the Type/tHEC fields). The eHEC generation process is defined in clause 6.3.4.

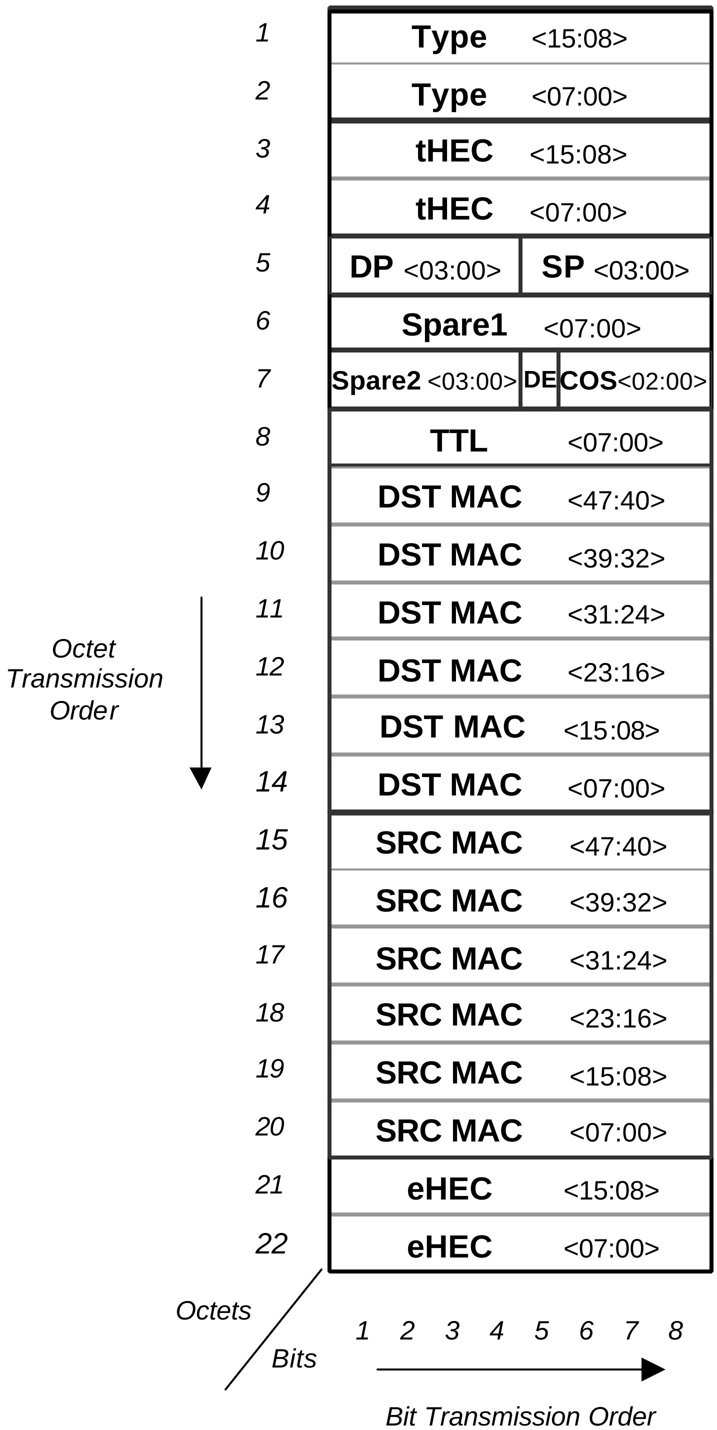


Figure 17: Extension Header for a Ring Frame

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 via GFP.

7.1 Ethernet MAC Payload

The format of Ethernet MAC frames is defined in IEEE 802.3, section 3.1. 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. The relationship between Ethernet MAC frames and GFP frames is illustrated in Figure 19.

7.1.1 Ethernet MAC Encapsulation

The Ethernet MAC octets from Destination Address through Frame Check Sequence, inclusive, are placed in the GFP Payload field. Octet-alignment is maintained. Bit identification within octets is maintained. Specifically, on a octet-by-octet basis, bit 0 in IEEE 802.3 1998 Clause 3 corresponds to bit 8 in this specification and bit 7 in IEEE 802.3 1998 Clause 3 corresponds to bit 1 in this specification.

7.1.2 Ethernet Inter-Packet Gap (IPG) Deletion and Restoring

The following rules apply to the deletion and restoration of IPGs when the client is not a native GFP client:

1. IPGs are deleted before the Ethernet MAC frame is processed by the GFP transmitter and restored after the GFP frame is processed by the GFP receiver.
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 transmitter 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 sufficient octets containing an idle pattern of 00 hex are present between consecutive received Ethernet MAC frames to meet the minimum receiver IFG requirements. Minimum receiver IFG requirements are stated in IEEE 802.3, section 4.4.

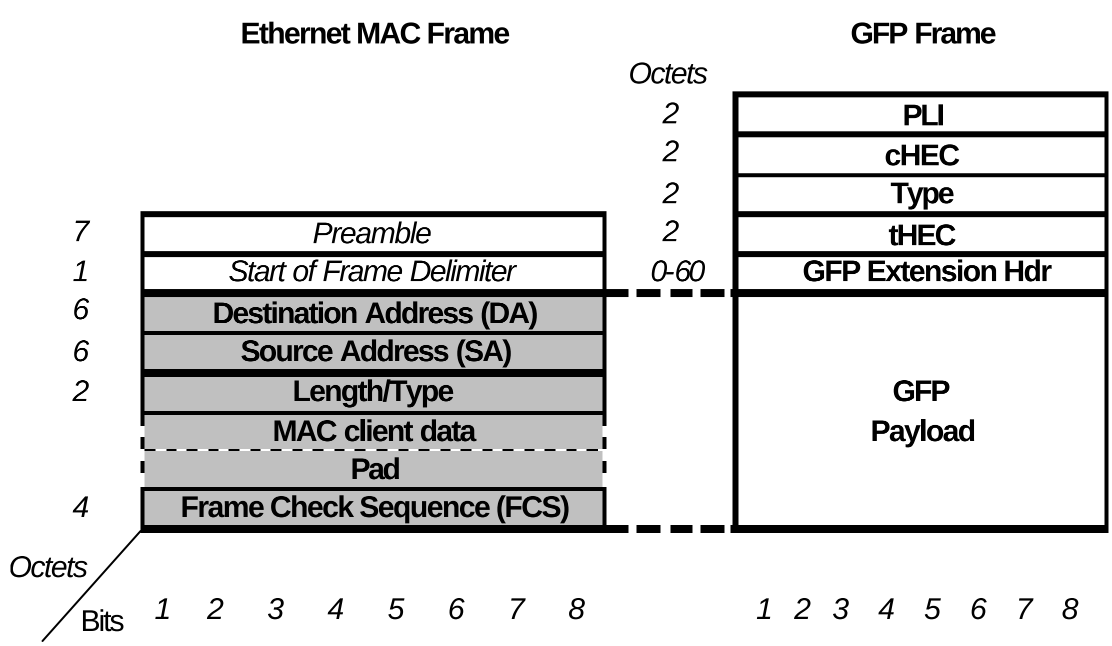


Figure 18: Ethernet and GFP Frame Relationships

7.2 IP/PPP Payload

IP/PPP payloads are first encapsulated in an HDCL-like frame. The format of a PPP frame is defined in the IETF RFC 1661, section 2. The format of the HDLC-like frame is defined in RFC 1662, section 3. 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 PPP/HDLC PDUs. The relationship between PPP/HDLC frame and the GFP frame is illustrated in Figure 20.

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 field of a GFP frame. Octet alignment is maintained. Bit identification within octets is also maintained.

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 the PPP/HDLC frame is extracted from the incoming client octet stream. The extracted (decoded) PPP/HDLC frame is then forwarded to the GFP transmitter for subsequent encapsulation into a GFP frame.
2. The PPP/HDLC frame is extracted from the GFP frame by the GFP reciever. 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 contro characters (e.g., hexadecimal 0x7d) as stated in IETF RFC 1662, section 4.

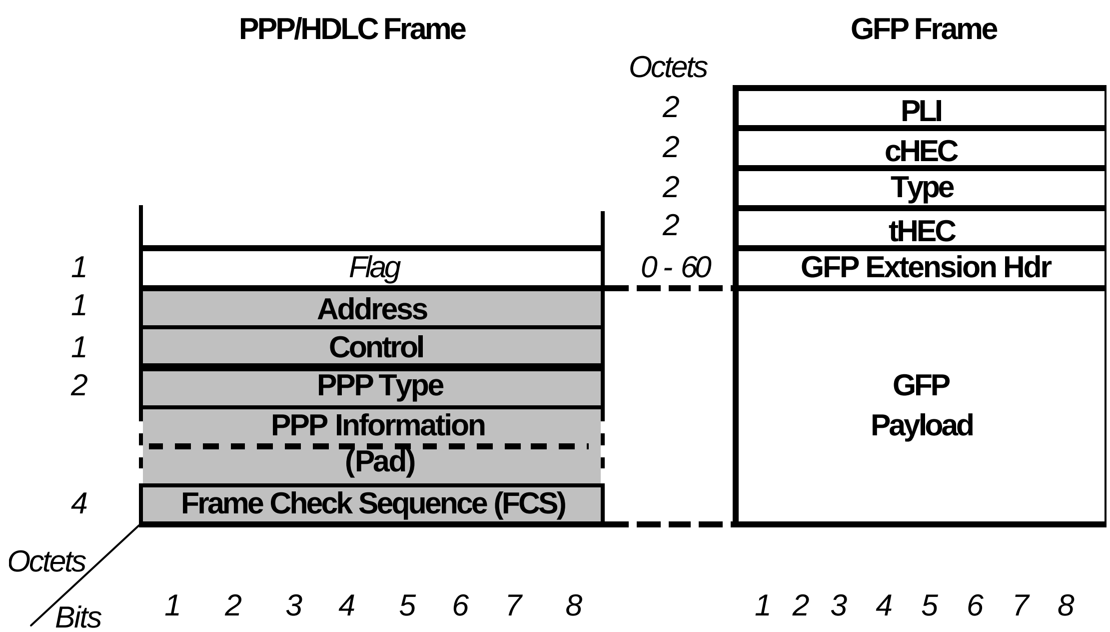


Figure 19: PPP/HDLC and GFP Frame Relationships

7.2.3. PPP Payload Configuration Options

Modifications to the PPP/HDLC-like frame format may be negotiated using the Link Configuration Protocol (LCP) Configuration Options procedures as defined in IETF RFC 1661, section 6. For instance, the format of the GFP frame after a successful negotiation of the Address-and-Control-Field-Compression (ACFC) Configuration Option is illustrated in Figure 21. Such configuration procedures are client-specific and transparent to GFP process.

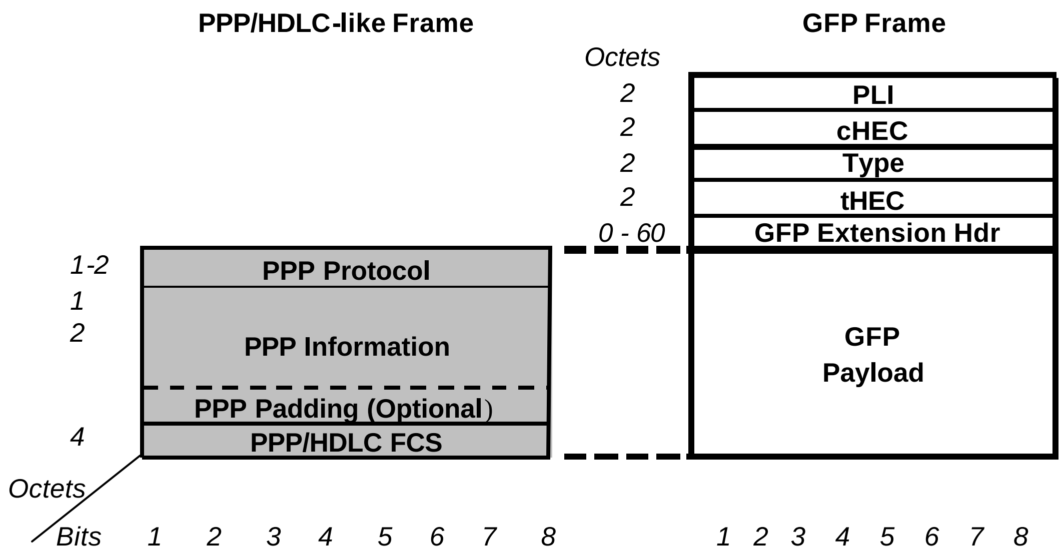


Figure 20: PPP/HDLC/HDLC and GFP Frame Relationships (with PPP's ACFC Configuration Option).

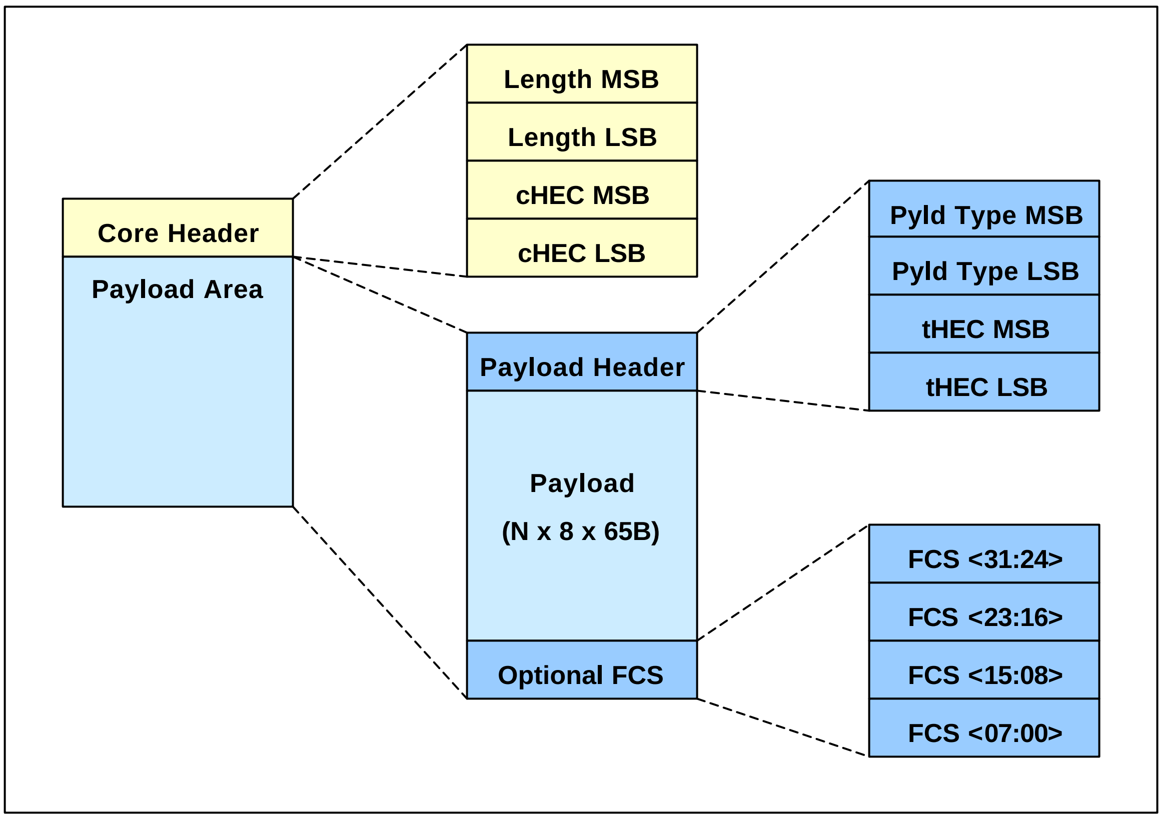
7.3. Error Handling in Frame-Mapped GFP

On ingress, PDUs detected in error before transmission by the client adaptation process should be discarded. PDUs detected in error while in transmission by the client adaptation process should be padded up with an all ones bit sequence, and transmitted with a reversed Payload FCS, when present. These actions ensure that the errored PDU will be dropped by the termination GFP process or the client end system.

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 Fibre Channel, ESCON, 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. Frame multiplexing is not precluded with transparent GFP.

The transparent GFP frame uses the same frame structure as the frame-mapped GFP, including the required Payload Header. The Payload FCS is optional. The transparent GFP frame format is depicted in Figure 22.



8.1. 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 decoding 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 an 8-bit control character if it is a 8B/10B control codeword. The 8B/10B control codewords are mapped into one of the 16 possible 8-bit control characters available in transparent GFP.

The decoded 8B/10B characters are then mapped into a 64-bit/65-bit -64B/65B- block code. The structure of the 64B/65B block code is shown in Figure 23. The leading bit of a 65-bit block, the Sync bit, indicates whether that block contains only 64B/65B 8-bit data characters or whether 64B/65B 8-bit control characters are also present in that block. If 64B/65B control characters are present, they are located at the beginning of the block. The first bit of the 64B/65B control character contains the Flag bit which indicates whether this is the last control character in this block (Flag=1) or whether there is another control character in the next octet (Flag=0). The next three bits contain the Control Code Locator, which indicates the original location of the 8B/10B control code character within the eight character locations of 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 4.

NOTE - 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, Fibre Channel, 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 - The re-coding process is entirely unaware of the meaning of control words or ordered sets. It simply generically re-codes 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.

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 0aaaC1. The flag value of 0 indicates that this 64B/65B control character is the last one in that block and a 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 Indicator is 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.

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

Legend:

- Leading bit in a control octet = 1 if there are more control octets and = 0 if this is the last control octet in that block
- aaa = 3-bit representation of the 1st control code's original position

- bbb = 3-bit representation of the 2nd control code's original position

...

- hhh = 3-bit representation of the 8th control code's original position

- Ci = 4-bit representation of the ith control code
- Di = 8-bit representation of the ith data value in order of transmission

Figure 22: Transparent GFP 64B/65B block coding

8.1.1. 10B_ERR Code

Certain client signal defects may produce 8B/10B codewords on ingress to the GFP transmitter that cannot be recognized by the 64B/65B adaptation process (e.g., an illegal 8/10B codeword or a legal codeword with a running disparity error, see clause 7.3). 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, received 10B_ERR code are typically re-coded by the demapper into either 001111 0001 (RD-) or 110000 1110 (RD+) (fixed illegal 8B/10B codewords with neutral disparity), depending on running disparity (see clause 7.3.3 for other client-specific 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.

8.1.2. 65B_PAD Code

Since this application requires that the available path capacity is at least that of the client signal base (pre-encoding) data rate, the input receive buffer at the mapper will regularly underflow. For rate adaptaion purposes, and if there are no characters ready for transmission by the transparent GFP mapper, the mapper should insert a 65B_PAD padding character. This 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 10B_PAD code handling are given in clause 7.4.

8.1.3. 65B_ESC Code

Escape Sequences in the 64B/65B block code consist of consecutive characters which, when arranged in a particular order, represent a predefined function within a given 64B/65B coding. The first character of all Escape Sequences is always a special "escape" control character, the 65B_ESC code.

To facilitate the conveyance of certain in-band commands/indicators, a two character 'Escape Sequence' is used. This is a sequence of the "escape'" control character followed by a data octet. This is equivalent to a two octet 'Ordered Set' ('K-Char' followed by a 'D-Char') in the client data.

The meaning of the 64B/65B Escape Sequence is defined by the value of the D-octet associated with the 65B_ESC code. The value and meaning of these D-octets are for further study.

8.1.4. Insertion of 64B/65B Escape Sequence

The insertion of 65B_PAD characters is prohibited between the 65B_ESC character and its associated D-Character. This is to prevent complexity at the egress where the inserted 65B_PAD character could be misinterpreted as the D-Character.

8.2. Adapting 64B/65B Code Blocks into GFP

The payload structure of transparent GFP is illustrated in Figure 24. The use of the optional Payload FCS is not required with transparent GFP. To preserve the octet alignment of the GFP signal with the transport SONET/ODUk frame, the first step in the adaptation process is to group seven 64B/65B codes as shown in

Figure 24. The leading bits of each of the seven 64B/65B codes are grouped together into a first trailing octet. The eighth bit of this trailing octet and the eight bits of the second trailing octet are used for a CRC-9 error check over that group

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 group to be formed.

The resulting GFP frame is [(*N* X ((65 X7+9)) + (12 X 8)] bits long. The value of *N* depends on the base rate of the client signal and on the transport channel capacity. Suggested SONET virtually concatenated channel capacities are shown in Table 5. 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., 12 if the optional Payload FCS is included and no Extension Header is present), and the size of the payload envelope, as shown in Table 5. The Payload Header contains a Payload Type Identifier indicating transparent transport of client protocol data type.

Octet 1, 1							
Octet 1, 2							
Octet 1, 3							
. . .							
Octet 7, 7							
Octet 7, 8							
L1	L2	L3	L4	L5	L6	L7	C1
C2	C3	C4	C5	C6	C7	C8	C9

where: Octet j, k is the k^{th} octet of the j^{th} 64B/65B code in the superblock

Lj is the leading bit j^{th} 64B/65B code in the superblock

Ci is the i^{th} error control bit

Figure 23: Group structure for mapping 64B/65B codes into the GFP frame

8.2.1. Error Control with Transparent GFP

The nine error bits in each group of 64B/65B codes (see Figure 24) contain a CRC_9 error check code over the 464 bits in that group. The polynomial for the CRC-9 is {to be determined}. If the demapper detects an error, it should output either a 10B error character or an unrecognized 10B character, as described for disparity errors in the client-specific subclauses of 8.4. This replacement guarantees that the client receiver will be able to detect the presence of the error.

NOTE – Single error correction is also possible with this CRC-9.

8.3. 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 "running disparity." Running disparity 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 characters and each of the 12 recognized "special control characters" have two 10-bit encodings. Depending on current "running disparity," the next data or control character will select which of its two encodings to transmit to either flip running disparity (from negative to positive, or vice versa, if the character to be transmitted has an imbalance of 1s and 0s in its two forms) or to maintain the current running disparity state (if the character to be transmitted has 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 running disparity state. In these cases, a running disparity error is detected. Independent of the received character's validity, the received transmission character shall be used to calculate a new value of running disparity. The new value shall be used as the receiver's current running disparity for the next received transmission character.

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

8.3.1. Handling of Running Disparity on Ingress

On ingress, the initial running disparity, upon power-on, reset, or transition from a loss of signal or loss of codeword synchronization phase, may be assumed 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 running disparity. If no match is found, either an illegal codeword or a legal codeword with a running disparity 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.

8.3.2. Handling of Running Disparity on Egress

On egress, the initial running disparity upon power-on, reset, or transition from a loss of signal or loss of codeword synchronization phase, shall be assumed negative.

Transparent transport implementations must generate correct running disparity using any applicable protocol-specific rules. For each of the supported protocols, references are provided in clause 8.4 to the standard(s) which define each protocol's disparity rules.

10B_ERR codes are re-coded into client signals either as an unrecognized codeword with valid running disparity, or as a protocol-specific error, depending on the protocol, as described in section 8.4, Client Specific Aspects of Transparent Mapping.

8.3.3. Client-Specific Running Disparity Aspects

The following client-specific running disparity rules apply to all of the identified supported 8B/10B client protocols:

8.3.3.1. Fibre Channel Payload

Running disparity rules for Fibre Channel are found in ANSI X3.230-1994, Fibre Channel Physical and Signaling Interface (FC-PH), Rev 4.3, section 11. In addition to the "generic" running disparity rules specified in section 11.2, Fibre Channel specific rules in section 11.4 provide two versions of each EOF ordered set, and dictate their use to ensure that negative running disparity 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 SOF delimiters, primitive signals, and primitive signals will also always be transmitted with negative beginning running disparity. This allows Fibre Channel Idle words to be removed and added from an encoded bit stream one word at a time without altering the beginning running disparity.

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

For “transparent transport” of Fibre Channel payloads, 10B_ERR shall be re-coded into one of the following unrecognized 10B neutral disparity codewords, depending on beginning running disparity: 001111 0001 (RD-) or 110000 1110 (RD+).

8.3.3.2. ESCON Payload

Running disparity rules for ESCON are found in ANSI X3.296-1997, Information Technology--Single-Byte Command Code Sets Connection (SBCON) Architecture, section 6.2.2. Since ESCON does not define an error code to substitute for code violations, on egress, 10B_ERR shall be re-coded into one of the following unrecognized 10B neutral disparity codewords, depending on beginning running disparity: 001111 0001 (RD-) or 110000 1110 (RD+).

8.3.3.3. FICON Payload

FICON, as specified in Draft Proposed ANSI standard FC-SB-2 (T11 Project 1357-D, Rev 2.1), defines an Upper Level Protocol (ULP) at Fibre Channel layer FC-4 utilizing the same physical (FC-0) and coding (FC-1) interfaces as Fibre Channel, which are defined in ANSI X3.230-1994, rev 4.3. The same running disparity requirements described above in section 8.3.1 apply to both Fibre Channel and FICON payloads.

8.3.3.4. Gigabit Ethernet Payload

Running disparity rules for Gigabit Ethernet are found in IEEE 802.3-1998, section 36.2.4. Two Idle encodings are provided, indicated as /I1/ and /I2/. The first /I/ following a packet or Configuration ordered set restores the current running disparity to a negative value. All subsequent /I/s are /I2/ to ensure negative ending running disparity. This allows single /I2/s to be inserted/removed for rate adaptation without altering the beginning running disparity associated with the code-group subsequent to the inserted or removed /I2/.

In order to ensure beginning negative running disparity for each SOF, all /I2/ Idles should be generated with RD- K28.5, insuring beginning negative running disparity for the next Idle or SOF.

Per section 36.2.4.16 of IEEE 802.3-1998, running disparity 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 re-code 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+).

8.3.3.5. Infiniband Payload

Running disparity rules for Infiniband are for further study.

8.4. 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 re-code into 64B/65B block code the mapper inserts a 10B_PAD with its location indicated in the same manner as if a control code had been encountered in that location. Essentially, this 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. Rate Adaptation Procedures

Two possible approaches for rate adapting client signals reconstructed from transparent-GFP-mapped data received at the far-end of transport network are in the next clauses. These two approaches are to either rate-adapt the transported client signal to a client reference clock locally provided at the far end, the currently recommended approach, or recover client clock from the transported signal (for further study).

8.4.1.1. Rate Adaptation to a Local Reference Clock

Currently supported 8B/10B client signals specify operating frequencies with significantly relaxed (compared to SONET or OTN) clock-offset requirements (±100 to 200ppm). 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, each of these client signals impose minimum Inter-Packet Gap (IPG) rules, which specify the minimum number of Idle codewords which 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 insure that where rate adaptation to a local clock is required, even under worst case conditions (fast input clock & slow output clock, requiring some IPG Idles to be deleted), sufficient IPG will remain between packets for them to be successfully delineated.

This scheme may be employed equally well when reconstructing transparent-mapped client data on egress. With this approach, a local reference clock is supplied to the far-end device. As client data is demapped from GFP frames and re-coded 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 (e.g. min/max number of idles allowed to be inserted/removed.

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

With this approach, timing characteristics (jitter / 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. GbE, Fibre Channel, and ESCON do not share common frequencies; 1/2x, 1x, and 2x rates for a specific protocol can be easily derived, however, with no performance penalty).

In the event of ingress client signal failure or SONET/SDH failure, local clock may already be available to generate the protocol-specific link failure signal.

8.4.1.1. Rate Adaptation from the Transported Client Signal

NOTE: This material is under further study.

Client signals are provided at a smooth protocol-specific clock rate on ingress. While there may be gaps in the data packets themselves, these are filled with inter-packet gap (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 Loss of Signal or Loss of Synchronization occurs). However, the re-coded data is then mapped into GFP frames with 65B_PAD stuffing to rate-adapt to the higher bandwidth transport payload space. GFP control frames (as well as user control OA&M frames) may also be inserted periodically or opportunistically between GFP user data frames. Transport frames add their own overhead (Section/Transport and Path Overhead plus fixed stuff bytes in the case of SONET). No alignment between client data, stuffing bytes or blocks, GFP frames, transport overhead is maintained.

On egress, clock recovery is expected to require a FIFO and desynchronizer, where the desynchronizer would require a reference clock, PLL, and filter. Recovered clock timing would depend on some filtered version of 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 OA&M frames. Under worst-case conditions, which will randomly occur due to no alignment constraints, all client data "gapping" mechanisms will align into one contiguous "no client data" block.

No protocol-specific knowledge is required to recover client clock on egress.

Timing characteristics (jitter and wander) 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.

Should a failure occur in either the ingress client signal, or during transport, if a client rate link failure signal is expected to replace the failed client, a protocol-specific local reference clock is still required.

8.4.2. 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. With regards to reconstructed client signal timing, client output clock may either be recovered from the transported data, or transported data may be rate-adapted to a locally provided reference clock. Regardless of the selected output timing approach, protocol-specific timing requirements must be met, as defined in applicable standards for each client protocol. The following subsections identify key applicable requirements, but other protocol-specific requirements may apply.

8.4.2.1. Fibre Channel Payload

Fibre Channel full rate output data rate (after 8B/10B encoding) shall be 1062.5 Mb/s ±100ppm, as specified in ANSI X3.230-1994, Fibre Channel Physical and Signaling Interface (FC-PH), Rev 4.3, section 5.1. Output signal timing requirements are further specified in ANSI X3.230, sections 6.1.1 (Single-mode optical output interface), 6.2.1 (Multi-mode optical output interface), and 7 (Electrical cable interface). Output signals will normally be generated with a minimum of six Primitive Signals (Idles and R_RDY) between frames, as specified in ANSI X3.230, section 17.1. If rate adaptation is performed using Fibre Channel Idle insert/removal, rate adaptation shall be applied such that the receiving destination receives at least two Idles preceding each frame, as specified in ANSI X3.230, section 17.1.

Rate adaptation may also be required when a continuous stream of Fibre Channel primitive sequences is received, where primitive sequences are defined in Table 26 of X3.230-1994. Since a minimum of three consecutive identical primitive sequences are required to be received before the sequence is recognized (per section 16.4.1 of X3.230), rate adaptation by inserting one replica of the received 4-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 which still require rate adaptation. 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.

8.4.2.2. ESCON Payload

ESCON output data rate (after 8B/10B encoding) shall be 200 Mb/s ±0.04 Mb/s, as specified in ANSI X3.296-1996, Information Technology--Single-Byte Command Code Sets Connection (SBCON) Architecture, section 5.1.2. Output signal timing requirements are further specified in ANSI X3.296, sections 5.2.1 (Multi-mode output interface) and 5.3.1 (Single-mode output interface). Output signals will normally be generated with a minimum of 4 idle characters (K28.5) between data frames, as specified in ANSI X3.296, section 6.3. If rate adaptation is performed using ESCON Idle insert/removal, either one or two idle characters may be added or removed between frames, according to the rules of ANSI X3.296, section 7.2.

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 X3.296. Since a minimum of eight consecutive sequences are required to be received before the sequence is recognized (per section 6.3 of X3.296), rate adaptation by inserting a replica of the received 2-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 which still require rate adaptation. 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.

8.4.2.3. FICON Payload

FICON, as specified in Draft Proposed ANSI standard FC-SB-2 (T11 Project 1357-D, Rev 2.1), defines an Upper Level Protocol (ULP) at Fibre Channel layer FC-4. FICON utilizes the same physical (FC-0) and coding (FC-1) interfaces as Fibre Channel, which are defined in ANSI X3.230-1994, rev 4.3. The same timing requirements described above in clause 8.5.1.1 apply to both Fibre Channel and FICON payloads.

8.4.2.4. Full-Duplex Gigabit Ethernet Payload

Gigabit Ethernet output data rate (after 8B/10B encoding) shall be 1250 Mb/s ±100ppm, as specified in IEEE 802.3-1998. Output signal timing requirements are further specified in IEEE 802.3-1998, sections 38.5 and 38.6 (1000BASE-LX optical fiber interfaces), and 39.3.1 and 39.3.3 (1000BASE-CX (short-haul copper interface). Output signals will normally be generated with a minimum IPG of 12 octets, per IEEE 802.3-1998, section 4.4.2.3. GbE Idle characters are two octets, as defined in IEEE 802.3-1998, section 36.2.4.12. If rate adaptation is performed using full-duplex GbE Idle insert/removal, only a single /I2/ should be removed in any IPG, and only when its removal shall not result in no /I/ and not less than 8 octets including /T/, /R/, and /I/ remaining between frames, for successful frame delineation according to IEEE 802.3-1998, figures 36-7a and 36-7b.

Rate adaptation may also be required when a continuous stream of 8-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.

8.4.2.5. Infiniband Payload:

Output timing requirements for Infiniband are for further study.

8.5. Client-Specific Signal Fail Aspects

When transparent GFP mapping detects a client signal failure at ingress, it may send a far-end “Client Signal Fail” indication as described in 6.3.7. Client signal fail conditions include, as a minimum, loss of 8B/10B synchronization and, in some cases, loss of signal. Other implementation-dependent indications of a failed client signal (e.g. loss-of-clock from a SerDes) 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 following protocol-specific subsections.

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.

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 subsections 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.

8.5.1. Fibre Channel Payload

Fibre Channel Loss of Light (LOL)

Fibre Channel Loss of Signal is an implementation-dependent option. When supported, applicable Loss of Light and Signal Detect requirements are found in sections 5.6, 6.2.3.2 and H.10 of ANSI X3.230-1994, Fibre Channel Physical and Signaling Interface (FC-PH), Rev 4.3.

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

Fibre Channel 8B/10B Loss of Synchronization

Fibre Channel conditions for declaring in/out of 8B/10B codeword synchronization are specified in section 12.1 of ANSI X3.230-1994.

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 the egress Fibre Channel transmitter continuously output the neutral disparity decoding for 10B_ERR, forcing Loss-of-Synchronization detection and associated action at the downstream Fibre Channel receiver. Alternatively, the egress transmitter may generate the Not_Operational primitive per section 16.4.2 of X3.230-1994.

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

8.5.2. ESCON Payload

ESCON Loss of Signal (LOS)

Optical Loss of Signal detection requirements are specified in ANSI X3.296-1997, Information Technology--Single-Byte Command Code Sets Connection (SBCON) Architecture, sections 5.2 and 5.3 for multi-mode and single-mode interfaces, respectively.

ESCON 8B/10B Loss of Synchronization

ESCON conditions for declaring in/out of 8B/10B codeword synchronization are specified in ANSI X3.296-1997, section 7.1.

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 the egress ESCON transmitter continuously output the neutral disparity decoding for 10B_ERR, forcing Loss-of-Synchronization detection and associated action at the downstream ESCON receiver. Alternatively, the egress transmitter may generate the Not-operational sequence per section 7.4.2 of X3.296-1997.

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

8.5.3. FICON Payload

FICON, as specified in Draft Proposed ANSI standard FC-SB-2 (T11 Project 1357-D, Rev 2.1), defines an Upper Level Protocol (ULP) at Fibre Channel layer FC-4. FICON utilizes the same physical (FC-0) and coding (FC-1) interfaces as Fibre Channel, which are defined in ANSI X3.230-1994, rev 4.3. The same CSF handling requirements described above in clause 8.5.3.1 apply to both Fibre Channel and FICON payloads.

8.5.4. Full-Duplex Gigabit Ethernet Payload

Gigabit Ethernet Loss of Signal

Gigabit Ethernet Physical Media Dependent (PMD) Signal Detect requirements are specified in sections 38.2.4 and 39.2.3 of IEEE 802.3-1998 for fiber and copper interfaces, respectively.

Gigabit Ethernet 8B/10B Loss of Synchronization

Gigabit Ethernet conditions for declaring in/out of 8B/10B codeword synchronization are specified in IEEE 802.3-1998, section 36.2.5.2.6 and Figure 36-9.

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 the egress GbE transmitter continuously output the /V/ ordered set per section 36.2.4.16 of IEEE 802.3-1998, forcing Loss-of-Synchronization detection and associated action at the downstream GbE receiver.

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

8.5.5. Infiniband Payload

Infiniband Loss of Signal

For further study.

Infiniband 8B/10B Loss of Synchronization

For further study.

Infiniband Output due to Ingress or Transport Signal Fail

For further study.

Table 1: GFP Payload Type Identifiers

Payload Type Identifiers **Type Bits <15:13>**	**Usage**
000	User Data
001	User Control
100	OA&M
110	Resource Management
Others	Reserved

Table 2: GFP Extension Header Identifiers

Payload Type Identifiers **Type Bits <12:9>**	**Usage**
0000	Null Extension Header
0001	Linear Frame
0010	Ring Frame
Others	Reserved

Table 3 – GFP Payload Types

Payload Type Identifier (BIN) **TYPE Bits <15:13>**	**Payload FCS Identifier (BIN)** **TYPE Bit <12>**	**Extension Header Identifier (BIN)** **TYPE Bits <11:8>**	**User Payload Identifier (BIN)** **TYPE Bits <7:0>**	**TYPE** **(HEX)**	**GFP Frame** **Payload Area**	**Length of Extension Headers** **(# 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 & no Payload FCS	0
000	0	0000	0000 0010	0002	PPP with Null Extension Header & no Payload FCS	0
000	0	0001	0000 0001	0101	Ethernet with Linear Extension Header & no Payload FCS	4
000	0	0001	0000 0010	0102	PPP with Linear Extension Header & no Payload FCS	4
000	0	0010	0000 0001	0201	Ethernet with Ring Extension Header & no Payload FCS	18
000	0	0010	0000 0010	0202	PPP with Ring Extension Header & no Payload FCS	18
000	1	0000	0000 0011	1003	Transparent Fiber Channel with Null Extension Header & no Payload FCS	0
000	1	0000	0000 0100	1004	Transparent FICON with Null Extension Header & no Payload FCS	0
000	1	0000	0000 0101	1005	Transparent ESCON with Null Extension Header & no Payload FCS	0
000	1	0000	0000 0110	1006	Transparent Gb Ethernet with Null Extension Header & no Payload FCS	0
000	1	0000	0000 0111	1007	Transparent Infiniband with Null Extension Header & no Payload FCS	0
1xx	x	xxxx	xxxx xxxx	-	Reserved	-
x1x	x	xxxx	xxxx xxxx	-	Reserved	-
xx1	x	xxxx	xxxx xxxx	-	Reserved	=

Table 4: Special control character mapping into 4-bit control value

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	N/A	Unrecognized RD-	Unrecognized RD+	1100
65B_PAD	N/A	N/A	N/A	1101
65B_ESC	N/A	N/A	N/A	1110
Spare	N/A	N/A	N/A	1111

Table 5: SONET VC Path capacity & number of 64B/65B blocks per GFP frame

Client un-encoded data rate	VC Path Size	Min. number of 65B blocks/GFP frame
160 Mbit/s	STS-1-4v / VC-3-4v	8
425 Mbit/s	STS-3c-3v / VC-4-3v	40
850 Mbit/s	STS-3c-6v / VC-4-6v	40
1000 Mbit/s	STS-3c-7v / VC-4-7v	48

NOTE – The minimum number of the 65B blocks shown here assumes that the optional payload FCS is used.

Annex A

(Informative)

Bibliography

ANSI T1.102-1993, *Telecommunications – Digital hierarchy – Electrical interfaces*

ANSI T1.105.01-1994, *Telecommunications – Synchronous optical network (SONET) – automatic protection switching*

ANSI T1.105.03-1994, *Telecommunications – Synchronous optical network (SONET) – Jitter at network interfaces*

ANSI T1.105.04-199x, *Telecommunications – Synchronous optical network (SONET) – Data communication channel protocols and architectures*[1)]

ANSI T1.105.05-1994, *Telecommunications – Synchronous optical network (SONET) – Tandem connection maintenance*

ANSI T1.107-1988, *Telecommunications – Digital hierarchy – Formats specifications*

ANSI T1.627-1993, *Telecommunications – Broadband ISDN – ATM layer functionality and specification*

ITU-T Recommendation G.783-1997, *Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks* [2)]

ITU-T Recommendation G.784-1998, *Synchronous digital hierarchy (SDH) management* [2)]

ITU-T Recommendation I.432.1-1999, *Series I: Integrated Services Digital Network. ISDN user-network interfaces – Layer 1 Recommendations.*

ITU-T Recommendation V.41, Appendix I

IETF RFC 2823, *PPP over Simple Data Link (SDL) using SONET/SDH with ATM-like framing,* May 2000.

1) This standard is part of the set of standards created when ANSI T1.105 was broken into its constituent parts. This part is currently undergoing the approval process. Contact the Secretariat for more recent information.

2) All American National Standards (ANSI), International Standards (ISO), and ITU-T Recommendations, are available from the American National Standards Institute, 11 West 42nd Street, New York, NY 10036. Dual listings of American National Standards and International Standards mean that the two standards are eitheidentical or similar.