



(11) **EP 2 692 080 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention
of the grant of the patent:
09.05.2018 Bulletin 2018/19

(51) Int Cl.:
H04L 1/00^(2006.01) H04J 14/00^(2006.01)
H04L 9/00^(2006.01)

(21) Application number: **12711260.5**

(86) International application number:
PCT/IB2012/051218

(22) Date of filing: **14.03.2012**

(87) International publication number:
WO 2012/131517 (04.10.2012 Gazette 2012/40)

(54) **ERROR HANDLING IN A PASSIVE OPTICAL NETWORK**

FEHLERHANDHABUNG IN EINEM PASSIVEN OPTISCHEN NETZWERK

TRAITEMENT D'ERREUR DANS UN RÉSEAU OPTIQUE PASSIF

(84) Designated Contracting States:
**AL AT BE BG CH CY CZ DE DK EE ES FI FR GB
GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO
PL PT RO RS SE SI SK SM TR**

(30) Priority: **30.03.2011 US 201113076377**

(43) Date of publication of application:
05.02.2014 Bulletin 2014/06

(73) Proprietor: **Telefonaktiebolaget LM Ericsson
(publ)
164 83 Stockholm (SE)**

(72) Inventor: **HOOD, David
Palo Alto, CA 94301 (US)**

(74) Representative: **Brann AB
P.O. Box 3690
Drottninggatan 27
103 59 Stockholm (SE)**

(56) References cited:
EP-A1- 1 755 248 WO-A1-2010/142853

- "3av_0811_anslow_1 ; 3av_0811_anslow_1",
IEEE DRAFT; 3AV_0811_ANSLOW_1, IEEE-SA,
PISCATAWAY, NJ USA, vol. 802.3, 26 November
2008 (2008-11-26), pages 1-17, XP017634469,
[retrieved on 2008-11-26]
- "10-Gigabit-capable passive optical networks
(XG-PON): Transmission convergence (TC)
specifications; G.987.3 (10/10)", ITU-T
STANDARD, INTERNATIONAL
TELECOMMUNICATION UNION, GENEVA ; CH,
no. G.987.3 (10/10), 7 October 2010 (2010-10-07),
pages 1-134, XP017588393, [retrieved on
2011-09-30]

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 2 692 080 B1

Description

BACKGROUND

[0001] The present invention relates generally to error detection in a communications network and, more particularly, to a method and apparatus for signaling error events between layers of a layered protocol stack.

[0002] The Gigabit Passive Optical Network (G-PON) uses a layered protocol stack to implement the communication protocols. Each layer of the protocol stack represents a set of protocols or processes needed for communication between the network nodes. These protocols or processes are typically implemented by hardware or firmware, with exceptions typically handled by firmware or software. The organization of the protocols into a layered protocol stack enables modifications in one layer without affecting the applications in other layers.

[0003] When data is sent from one node to another, it is passed down through the layers of the protocol stack at the originating node, transmitted over the physical medium to the destination node, and passed back up the protocol stack at the destination node. As the data travels down the protocol stack at the originating node, each layer adds a header containing information used by the protocols at that layer. As the data travels up the protocol stack at the destination node, the header information is stripped off at each layer.

[0004] It is typical for one or more layers of the protocol stack to implement an error detection and/or error correction capability. Error detection and/or correction is implemented by embedding redundant information in the data that is transmitted by the particular protocol layer. The redundant information enables the detection and/or correction of errors at the receiver. If an uncorrectable error is detected, the general practice is to silently discard the data containing the error without any notification to the higher layer protocols. For some applications, a retransmission protocol may be implemented at a higher protocol level to repeat a previously-transmitted request or to request retransmission of missing data.

[0005] The typical practice of silently discarding data packets by lower protocol layers and using retransmission protocols at the higher protocol layers has several drawbacks. First, retransmission is not useful for many real-time applications in which timeliness is as important as correctness. Second, for non real-time applications, additional delay is introduced by requiring the higher protocol layer to wait for expiration of a timer before initiating the retransmission. Third, some of the discarded data may still be useful to the higher protocol layer. Discarding such means that system throughput will be reduced by unnecessary retransmissions. Fourth, the loss of part of a structured data stream may cause loss of synchronization, leading to further losses in portions of the data stream that contain no errors, but whose structure cannot be deduced until the receiving device regains synchronization.

[0006] Accordingly, there is a need for new techniques to prevent or mitigate data loss when unrecoverable data errors occur.

[0007] "3av-0811-anslow-1", a Draft Amendment to IEEE Std 802.3-2008 from 7th October 2008 discloses physical layer specifications and management parameters for 10G-EPON on point-to-multipoint passive optical networks. As such, the 10G-EPON extends the network architecture of P802.3ah 1G-EPON, providing support for both symmetric and asymmetric data rates while maintaining complete backward compatibility with already deployed equipment. The objectives of this amendment are: 1) Support subscriber access networks using point to multipoint topologies on optical fiber, 2) PHY(s) to have a BER better than or equal to 10^{-12} at the PHY service interface, 3) Provide physical layer specification: - PHY for PON, 10 Gb/s downstream/1 Gb/s upstream, single SM fiber, - PHY for PON, 10 Gb/s downstream/10 Gb/s upstream, single SM fiber, 4) Define up to 3 optical power budgets that support split ratios of 1:16 and 1:32, and distances of at least 10 and at least 20 km.

[0008] WO-A1-2010/142853 discloses a digital video broadcasting (DVB) receiver that processes baseband (BB) frames at both a baseband (BB) block level and a terminal block level. At the BB block, the DVB receiver synchronizes BB frames from synchronization information inserted in the BB frame headers. The BB block configures the error indicator based on whether an error is detected in the BB frame. The DVB receiver also processes signaling information in the preamble of the T2 physical layer frame only if indicated by the signal changed field. The BB passes the processed BB frame to the terminal block of the DVB receiver for processing network packets that is contained in the BB frame. A DVB transmitter inserts a synchronization field and payload type field in the BB frame header of the BB frame and also determines whether there has been a change in the signaling information at the physical layer and configures the signaling changed indicator accordingly.

[0009] EP-A1-1 755 248 discloses indicating lost segments across layer boundaries with an application encoder which generates independently accessible symbols, these symbols are aggregated by symbol aggregation means into a packet payload, the aggregated symbols in the packet payload are transported in a defined packet structure whereby the packet structure is defined by anyone of at least one packet header, a block-check sequence, and a payload of variable length of aggregated independent symbols, these packets are transported over a channel by a packet transmitter segmenting the packets into different segments by segmentation means, a segment receiver included in a first entity has the ability to detect whether a certain segment is lost and also knows the length of the lost segment, the segments are aggregated in the first entity to form at least one packet conforming to the packet stream, the one or more packets are delivered to a packet receiver in another, second entity by means of a normalized interface between the two

entities which allows to pass packets according to the specified format from the first entity to the second entity, a symbol parser entity recovers the symbols and passes the individual symbols to an application decoder, whereby either correct symbols or erased symbols can be forwarded to the application decoder, the segment receiver in the first entity inserts a certain pattern at the position where the lost or defective segment would be which indicates the loss or defect of segment and the length of the lost or defect segment in the aggregated packet, the packet receiver; in the second entity knows the format, the syntax and the semantics of the inserted pattern, means in the second entity search for specific patterns in the received packet and interpret each found pattern to recover all reliable non-lost information within the packet, and a symbol parser in the second entity recovers from the recovered non-lost information of each received packet individual symbols.

[0010] "10-Gigabit-capable passive optical networks (XG-PON): Transmission convergence (TC) specifications; G.987.3 (10/10)", ITU-T STANDARD, INTERNATIONAL TELECOMMUNICATION UNION, GENEVA; CH, no. G.987.3 (10/10), 7 October 2010 (2010-10-07), pages 1-134, XP017588393, describes the transmission convergence layer for 10-gigabit-capable passive optical network systems.

SUMMARY

[0011] The present invention provides a method implemented in a node of a passive optical network according to Claim 1.

[0012] The present invention also provides a network node according to Claim 4.

[0013] The present invention also provides a method implemented in a node of a passive optical network according to Claim 7.

[0014] The present invention also provides a network node according to Claim 11.

[0015] Preferred embodiments are set out in the dependent claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016]

Figure 1 illustrates an exemplary protocol stack for a passive optical network.

Figure 2 illustrates a data transmission error detected by a server layer affecting a message received by a client layer.

Figure 3 illustrates a data transmission error detected by a server layer affecting two or more data frames at a client layer.

Figure 4 illustrates an exemplary method of receiving data having an uncorrectable error and parsing the received data to recover a portion unaffected by the error.

Figure 5 illustrates an exemplary method for parsing data to recover data frames having valid frame headers according to a background example.

Figure 6 illustrates an exemplary method for parsing data to recover a control message not affected by the error.

Figure 7 illustrates an exemplary procedure for processing a control message with a check code that indicates uncorrectable errors in the message.

Figure 8 illustrates an exemplary network node configured according to one embodiment of the present invention.

DETAILED DESCRIPTION

[0017] The present invention provides methods and apparatus for processing data that contains unrecoverable errors. Instead of discarding the data when an uncorrectable error occurs, a lower protocol layer delivers the data to a higher protocol layer and provides an indication that the data contains an uncorrected error. The higher protocol layer can parse the data to recover portions that are not affected by the error. For example, the higher protocol layer can parse the data to recover one or more data frames having valid frame headers. As another example, the higher layer protocol can parse the received data to recover a control message protected by a higher layer protocol check code. The check code can be used to validate the control message if the control message itself is not affected by the error. In another aspect of the invention, a control message with an invalid check code can be accepted if certain acceptance criteria are met, whether or not the lower layer indicates the presence of uncorrectable errors.

[0018] The present invention enables data to be recovered that might otherwise be lost due to uncorrectable errors.

[0019] Referring now to the drawings, Fig. 1 illustrates an exemplary protocol stack 10 for an Gigabit Passive Optical Network (G-PON or X-GPON). The G-PON network is described by the International Telecommunication Union (ITU) in the G.984.3 specification. The XG-PON network is described by the International Telecommunication Union (ITU) in the G.987.3 specification. The protocol stack for both G.987.3 and G.984.3 networks is essentially the same (distinguished by the prefix X in G.987, the distinction not being essential for purposes of this description) and includes three main layers: the network layer 12, G-PON/XG-PON Transmission Convergence (GTC/XGTC) layer 14, and the physical layer 16. The network layer 12 implements a networking protocol such as the Ethernet, Internet Protocol (IP), or Multiprotocol Label Switching (MPLS). On the transmitter side, the network layer 12 generates data packets, referred to herein as service data units (SDUs), for transmission and delivers the SDUs to the GTC/XGTC layer 14. On the receiver side, the network layer 12 receives the SDUs from the GTC layer 14.

[0020] The GTC layer 14 comprises three main sub-layers: the service adaptation sublayer 18, the framing sublayer 20, and the physical adaptation sublayer 22. On the transmitter side, the GTC service adaptation sublayer 18 accepts the upper layer SDUs and applies the G-PON encapsulation method (GEM) to obtain GEM/XGEM frames. The GEM header 24 of each GEM frame includes a length indicator (LI) information element to indicate the length of the GEM frame. The GEM frame header 24 also includes redundant information that permits detecting and/or correcting errors within the header 24 itself. A series of GEM frames forms a payload of a GTC frame in the downstream direction or a GTC burst in the upstream direction. On the receiver side, the GTC service adaptation layer 18 accepts the payload of the GTC frames, decapsulates the GEM frames, and reassembles the SDUs for delivery to the network layer 12.

[0021] The GTC framing sublayer 20 is responsible for adding and parsing headers to the GTC payload to support the PON management functions. The GTC header contains zero or more physical layer operations and maintenance (PLOAM) messages, which are used for low-level control communications between the nodes. On the transmit side, a header is added to the GTC payload to form a GTC frame (downstream) or GTC burst (upstream). On the receiver side, the GTC framing sublayer 20 accepts the GTC frames or GTC bursts from the physical adaptation sublayer 22, parses the GTC header to extract the PLOAM messages contained therein, and delivers the GTC payload to the service adaptation sublayer 18. The incoming PLOAM messaging channel flow is delivered to the PLOAM processing engine (not shown).

[0022] The physical adaptation sublayer 22 is responsible for generating a bit stream suitable for transmission over the transmission medium. The functions performed at the physical adaptation sublayer 22 include physical layer error detection and correction. On the transmitter side, the physical adaptation sublayer 22 accepts the GTC frame (downstream direction) or GTC burst (upstream direction) from the GTC framing sublayer 20, partitions the GTC frames into FEC data blocks, and computes and appends the FEC parity field to each FEC data block to generate a FEC codeword. Several FEC codewords are concatenated to form a payload for the physical layer frames, which are transmitted over the physical medium. The bits of the physical layer frame payload are scrambled to increase robustness against repeated identical bits and a header including synchronization information is added to the payload to create the physical layer frame or physical layer burst. On the receiver side, the physical adaptation sublayer 22 receives data transmitted over the physical medium, performs synchronization and descrambles the physical layer frames, decodes the FEC codewords to detect and correct errors within its capabilities, and reassembles the GTC frames or GTC bursts. If no errors occur during transmission, the GTC frames or GTC bursts are delivered to the framing sub-

layer 20. If an uncorrectable error occurs in a GTC frame or burst, the remainder of the GTC frame or burst is in current implementations discarded by the FEC decoder. In this case, a retransmission protocol implemented at a higher layer may request retransmission of the discarded data or take other steps to mitigate the loss of data. The discarding of a partial or complete GTC frame or burst is referred to herein as an erasure.

[0023] The physical layer 16 comprises the physical medium over which the data is transmitted.

[0024] In current implementations of the protocol stack 10, an erasure by the physical adaptation sublayer 22 due to an unrecoverable error is not signaled to the higher layers. Instead, the data containing the error is silently discarded. In the particular case of a GTC frame or burst, the discarded data includes not only the FEC data block containing the error, but all subsequent FEC data blocks that are part of the same GTC frame or burst. To recover from error events, a protocol may be implemented at a higher protocol layer for non-real time data to request retransmission of any data that is discarded at a lower layer. Typically, the higher layer protocol sets a timer when a missing data packet is detected. If the missing packet is not received before the timer expires, the higher layer protocol can request retransmission of the missing data packet. One problem with this approach is that the wait period before requesting retransmission of missing data packets increases the latency of the data transmission. For real time data, the lost data typically cannot be recovered in time to be useful.

[0025] According to exemplary embodiments of the present invention, a mechanism is provided to enable a lower protocol layer to signal an error event to a higher protocol layer. The term "layer" is used in this context in its broadest sense, to include sublayers. In response to the error indication, the higher protocol layer can use knowledge about the structure of the data to recover a portion of the data that is not affected by the error. Thus, at least some of the data that would otherwise be discarded can be saved.

[0026] Fig. 2 illustrates an application of the present invention to the transmission of PLOAM messages as specified by the International Telecommunication Union (ITU) in the G.987.3 and G.984.3 specifications. The PLOAM message is exchanged between an optical line terminal (OLT) and optical network unit (ONU). Each PLOAM message is protected by a check code 26, such as an error-detecting and -correcting cyclic redundancy check code (CRC) for G.984.3 systems and a cryptographically-derived message integrity check (MIC) code for G.987.3 systems, which detects message alterations. In current implementations PLOAM messages with invalid check codes are silently discarded.

[0027] The PLOAM channel in G-PON networks is message based and is carried in a designated field of the GTC frame header (downstream) and the GTC burst header (upstream). In the event that an FEC codeword contains an uncorrectable error, the current practice is

to discard the entire GTC frame/burst, which may include one or more PLOAM messages. In contrast, embodiments of the present invention use knowledge of the frame and header structure to recover PLOAM messages that would otherwise be discarded when an unrecoverable error is detected in an FEC codeword. As long as frame synchronization is maintained, the receiving node can determine the location of PLOAM messages in the data stream. More particularly, flags or counters at specific locations in the data stream indicate the presence of one or more PLOAM messages. Assuming these flags or counters are received without error, the receiving node can extract the PLOAM messages from the data stream, possibly containing embedded uncorrected errors. The PLOAM message can then be verified by its check code 26. If after a possible error correction step the check code is valid, the PLOAM message can be assumed to be valid.

In the prior art, a PLOAM message containing an invalid check code (e.g. CRC or MIC) is silently discarded. According to another aspect the present invention, it may be appropriate to accept the PLOAM message even with an invalid check code. For example, if the message comprises an emergency stop message, the PLOAM application may accept the message. Other criteria may also be taken into account before deciding whether to discard the PLOAM message. For example, G.987.3 requires a PLOAM message to contain an incrementing and therefore predictable message sequence number, which may be used as additional validation. If the sequence number is correct, the PLOAM application may accept the message despite the error. Also, the PLOAM application may evaluate the consequences of accepting the message. A PLOAM message deemed to be harmless may be accepted despite the error. As an example, a request to read back data from the device may be accepted.

[0028] Fig. 3 illustrates another application of the present invention to avoid error propagation that could otherwise occur when data is discarded and synchronization is lost. Error propagation occurs when a data error in a lower layer frame results in the loss of two or more higher layer frames. Fig. 3 illustrates an unrecoverable error in an FEC codeword received at the physical adaptation sublayer 22. FEC codewords typically comprise not more than 255 bytes (XG-PON FEC codewords are 248 bytes), while Ethernet frame SDUs are often 500 or more bytes long, and not infrequently as much as 1500 bytes. An uncorrectable FEC codeword that falls into the middle of a GEM frame may cause no damage whatever to the synchronization mechanism, which uses the frame length indicator field of the GEM header 24. However, if the uncorrectable errors span a GEM header, the synchronization mechanism is lost. Because the location of the uncorrectable error is not exploited by current implementations, the typical practice as specified by the ITU recommendations is to discard the remainder of the frame/burst following the uncorrectable FEC codeword. Thus, an FEC error affecting one GEM frame can lead

to further data losses because the synchronization information in the header of the GEM frame is not used, even though it might have been valid.

[0029] According to one embodiment of the present invention, rather than being discarded, the GTC frame containing the uncorrectable FEC codeword is delivered by the physical adaptation sublayer 22 to the framing sublayer 20, along with an indication that the GTC frame contains an error within a specific range of byte locations. The framing sublayer 20 passes the GTC payload to the service adaptation sublayer, along with the error information that the GTC payload includes an error within a specific range of byte locations. In the example shown in Fig. 3, it is presumed that the data error occurs in the payload of GEM frame 1 and that the GEM headers 24 of both GEM frames 1 and 2 are received error free. While there is no way to avoid the loss of GEM frame 1, the length indicator contained in the GEM header 24 of GEM frame 1 allows the service adaptation sublayer 18 to determine the starting point of GEM frame 2. By using data that would otherwise have been discarded, the service adaptation sublayer 16 can avoid the loss of GEM frame 2 and subsequent GEM frames.

[0030] Fig. 4 illustrates an exemplary method 50 of receiving data containing unrecoverable data transmission errors. The method begins when a data block containing an uncorrectable error is received at a first protocol layer (e.g., PAS 22 or framing sublayer 20) (block 52). Rather than discard the received data, the first protocol layer delivers the data block to a second protocol layer (e.g. framing sublayer 20 or SAS 18) with an error indication (block 54). The second protocol layer may then parse the received data block responsive to the error indication to recover a portion of the received data stream that is unaffected by the error or errors (block 56). The second protocol layer may, for example, verify that a portion of the received data block is free of errors, parse the received data block to extract the error free portion, and use the error free portion. It should be appreciated that the second protocol layer is above the first protocol layer. However, other protocol layers may exist between the first and second protocol layers.

[0031] In one background example, the received data comprises multiple data frames. The second protocol layer parses the received data to recover data frames having frame headers 24 that are free from errors. As one example, the received data may comprise a GTC frame containing two or more GEM frames. The GTC frame is received in one or more FEC codewords. An error in the FEC codeword can be detected by a decoder and an error indication can be provided to the service adaptation sublayer 18 and/or framing sublayer 20.

[0032] In an exemplary embodiment, the received data contains a control message with a check code. The second protocol layer parses the received data to recover the control message and verifies that the control message after possible error correction contains a valid check code. If the check code is valid, it is presumed that the

control message is not affected by the error and the control message can be used.

[0033] FIG. 5 illustrates an exemplary method 100 according to a background example. The physical adaptation sublayer (PAS) receives data over the physical medium (block 102). The data is protected by a forward error correction (FEC) code. The physical adaptation sublayer 18 decodes the received data and checks for uncorrected errors (block 104). If the data has no uncorrected errors, the PAS 22 delivers the data to the framing sublayer (FS) 20, which in turn delivers the data to the service adaptation sublayer (SAS) 18 (block 106). The service adaptation sublayer 18 processes the data normally. If the received data includes a block that contains an uncorrectable error, rather than discard the block, the physical adaptation sublayer 22 delivers the data block to the framing sublayer 20 (block 108) together with an indication that the particular data block contains an uncorrectable error. More particularly, the received data is assembled into one or more GTC frames or bursts and delivered to the framing sublayer 20 along with the error indication. The framing sublayer 20 in turn delivers the data to the service adaptation sublayer 18 retaining the error indication. The service adaptation sublayer 18 parses the GEM frame headers 24 and determines whether the GEM frame headers contain any errors (block 110, 112). If the GEM frame headers are error free, the service adaptation sublayer 18 continues parsing the GEM frame headers (block 114). However, if an error is detected in a GEM frame header, the service adaptation sublayer 18 generates a hypothesis about the start position of the next GEM frame (block 116). As one example, the service adaptation sublayer 18 may use the frame length indicator in the GEM frame header on the assumption that the frame length indicator is unaffected by the error. Using the hypothesized or estimated start position, the service adaptation sublayer 18 parses the next header and checks the hypothetical next GEM header 24 for errors (block 118). If no errors are detected, the service adaptation sublayer 18 continues parsing headers as previously described (block 120). If an error is detected in the hypothetical next GEM header 24, it is presumed that synchronization has been lost and the service adaptation sublayer waits for resynchronization by the framing sublayer (block 122).

[0034] FIG. 6 illustrates an exemplary procedure 150 for recovering PLOAM messages when an uncorrectable error is detected at the physical adaptation sublayer 22 according to an embodiment of the invention. The physical adaptation sublayer 22 receives data protected by a forward error correcting code as previously described (block 152). Each FEC block in the received data is decoded and checked for errors (block 154). If no uncorrected errors occur, the data is assembled into GTC frames and delivered to the framing sublayer for normal processing (block 156). If a received FEC block contains an uncorrected error, rather than discard the remainder of the GTC frame, the physical adaptation sublayer de-

livers the GTC frame to the framing sublayer 20 with an error indication (block 158). The framing sublayer 20 parses the GTC frame header and extracts any PLOAM messages from the GTC frame header (block 160). The GTC payload may be discarded, or delivered to the service adaptation sublayer 18 with an error indication. The service adaptation sublayer 18 may then process the GTC payload as previously described in FIG. 5. The extracted PLOAM messages are delivered to the PLOAM client (block 162). After a possible error-correcting step, the PLOAM client can verify the PLOAM message using the MIC or CRC 26 appended to the PLOAM message (block 164). If the check code is valid, the message is accepted (block 166). If the check code is not valid, the PLOAM message may be discarded (block 168). Alternatively, additional testing may be applied to determine whether the PLOAM message can be accepted with an invalid check code.

[0035] FIG. 7 illustrates an exemplary procedure 170 for processing a PLOAM message that contains a check code 26. The procedure begins when the PLOAM client receives a message containing a check code (block 172). The PLOAM client verifies the check code (block 174). If the check code is valid, the message is accepted (block 176). If the check code is not valid, rather than discard the message, the PLOAM client may apply additional acceptance criteria to determine whether to accept or reject the message (block 178, 182, 186). For the case where a PLOAM message is protected by an MIC code generated with a security key, the invalid check code 26 may be due to use of an unsynchronized or stale key. The PLOAM client may attempt to validate the PLOAM message with a previous security key (block 178). If the validation using the previous security key is successful, the PLOAM client can accept the message and initiate a security key update procedure to re-synchronize the security key (block 180). If the validation with the previous security key is not successful, the PLOAM client may determine a priority of the message (block 182). If the priority is above a threshold, the PLOAM client may accept the message (block 184). If the priority is below the threshold, the PLOAM client may determine whether the message is usable (block 186). A message may be considered usable if it contains errors that are deemed to be harmless. If the message is usable, the PLOAM client may accept the message (block 188). Other acceptance criteria can also be applied. If none of the acceptance criteria are satisfied, the PLOAM client may discard the message or take additional recovery steps (block 190). The additional recovery steps may comprise repeating a previously transmitted request, sending a negative acknowledgement or requesting retransmission from a peer PLOAM client. It will be appreciated that the method shown in Fig. 7 is applicable even in the absence of errors indicated by a server layer.

[0036] Fig. 8 illustrates an exemplary network node 200 according to one exemplary embodiment. The network node 200 comprises a receiver front end 210 to

receive data over the passive optical network and a processing circuit 220 to process the received data. The receiver 210 may comprise any receiver capable of receiving data over a passive optical network. The received data is delivered to the processing circuit 220 for processing as herein described. The processing circuit 220 implements a layered protocol stack. The processing circuit 220 may comprise one or more microprocessors, hardware, firmware, or a combination thereof. The processing circuit 220 comprises a lower layer processor 230 for implementing lower layer protocols and a higher layer processor 240 to implement higher layer protocols. The same microprocessor, hardware, firmware, or combination thereof may be used to implement both the lower layer processor 230 and higher layer processor 240. Alternatively, different microprocessors, hardware, firmware, or a combination thereof may be used to implement the lower layer processor 230 and higher layer processor 240. The lower layer processor 230 and higher layer processor 240 are configured to execute the methods shown in Figs. 4-7 respectively.

[0037] The present invention may, of course, be carried out in other specific ways than those herein set forth without departing from the scope and essential characteristics of the invention. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive, and all changes coming within the scope of the appended claims are intended to be embraced therein.

Claims

1. A method (50) implemented in a node (200) of a passive optical network for processing data containing uncorrected errors, said method (50) comprising:

receiving (52), by a first protocol layer, data containing one or more uncorrectable errors;
delivering (54) the data to a second protocol layer with an error indication; and
parsing (56), by the second protocol layer, the received data responsive to the error indication to recover a portion of the received data unaffected by the error(s),
wherein said received data includes a control message protected by a check code and wherein parsing (56) the received data comprises parsing said received data to recover the control message,
wherein said control message is protected by a check code and further comprising:

validating (164) the check code; and
accepting (166) the message if the check code is valid,

and wherein the check code is generated with

a security key and wherein validating (164) the check code comprises:

validating the check code with a current security key;
if the validation with the current security key is unsuccessful, validating the check code with a prior security key;
if the validation with the prior security key is successful, initiating a security key update.

2. The method (50) of claim 1 further comprising accepting the control message with an invalid check code if it is determined that the error is harmless.
3. The method (50) of claim 1 further comprising accepting the control message with an invalid check code if the control message specifies a function regarded as high priority.
4. A network node (200) in a passive optical network, said node comprising:

a receiver front end (210) for receiving data over a passive optical network;
a processing circuit (220) for processing received data, said processing circuit (220) comprising:

a first processor (230) configured to provide an error indication indicating that received data has one or more uncorrected errors;
a second processor (240) configured to parse, responsive to the error indication, the received data to recover a portion of the received data not affected by the error(s),

wherein the received data includes a control message protected by a check code and wherein the second processor (240) is configured to parse the received data to recover a control message in a frame header,
wherein said control message is protected by a check code and wherein the second processor (240) is further configured to:

validate the check code; and
accept the message if the check code is valid,

wherein the check code is generated with a security key and wherein the second processor (240) is configured to:

validate the check code with a current security key;
if the validation with the current security key is unsuccessful, validate the check code

with a prior security key;
if the validation with the prior security key is successful, initiate a security key update.

5. The network node of claim 4 wherein the second processor (240) is further configured to accept the control message with an invalid check code if it is determined that the error is harmless. 5
6. The network node of claim 4 wherein the second processor (240) is further configured to accept the control message with an invalid check code if the control message specifies a function regarded as high priority. 10
7. A method (170) implemented in a node (280) of a passive optical network for processing a message containing unrecoverable errors, said method (170) comprising: 15
receiving (172) a message having a message check code;
validating (174) the check code;
accepting (176) the message if the check code is valid; 20
accepting the message with an invalid check code if a predetermined acceptance criterion is satisfied;
wherein the check code is generated with a security key and wherein validating (174) the check code comprises validating the check code with a current security key, 25
wherein accepting the message with an invalid check code comprises:
validating (178) the check code with a prior security key;
accepting the message if the validation with the prior security key is successful; wherein the method further comprises: initiating (180) a security key update if the validation with the prior security key is successful. 30
8. The method (170) of claim 7 wherein accepting the message with an invalid check code comprises accepting the message if it is determined that the error is harmless. 35
9. The method of claim 7 wherein accepting (184) the message with an invalid check code comprises accepting the message if a priority of the message is a predetermined priority level. 40
10. The method of claim 7 wherein the message comprises a physical layer, administration, and maintenance, PLOAM, message. 45
11. A network node (200) in a passive optical network, 50

said network node (200) comprising:

a receiver (210) to receive data over a passive optical link;
a processor (220) configured to:

receive a message having a message check code;
validate the check code;
accept the message if the check code is valid;
accept the message with an invalid check code if a predetermined acceptance criterion is satisfied;

wherein the check code is generated with a security key and wherein the processor (220) is configured to validate the check code with a current security key, and
wherein the processor (220) is configured to:

validate the check code with a prior security key if the validation with the current security key fails; and
accept the message if the validation with the prior security key is successful;

wherein the processor (220) is further configured to: initiate a security key update if the validation with the prior security key is successful.

12. The network node (200) of claim 11 wherein the processor (220) is configured to accept the message if it is determined that the error is harmless. 35
13. The network node (200) of claim 11 wherein the processor (220) is configured to accept the message if a priority of the message is a predetermined priority level. 40
14. The network node (200) of claim 11 wherein the message comprises a physical layer, administration, and maintenance, PLOAM, message. 45

Patentansprüche

1. Verfahren (50), das in einem Knoten (200) eines passiven optischen Netzwerks implementiert ist, zum Verarbeiten von Daten, die nicht korrigierte Fehler enthalten, wobei das Verfahren (50) Folgendes umfasst:

Empfangen (52), durch eine erste Protokollschicht, von Daten, die einen oder mehrere nicht korrigierbare Fehler enthalten;
Abgeben (54) der Daten an eine zweite Protokollschicht mit einer Fehlerangabe; und

- Parsen (56), durch die zweite Protokollschicht, der empfangenen Daten als Reaktion auf die Fehlerangabe, um einen Teil der empfangenen Daten, der nicht durch den/die Fehler betroffen ist, wiederherzustellen, 5
wobei die empfangenen Daten eine Steuerungsnachricht beinhalten, die durch einen Prüfcode geschützt ist, und wobei Parsen (56) der empfangenen Daten Parsen der empfangenen Daten zum Wiederherstellen der Steuerungs- 10
nachricht umfasst,
wobei die Steuerungsnachricht durch einen Prüfcode geschützt ist und ferner umfassend:
- Validieren (164) des Prüfcodes; und 15
Akzeptieren (166) der Nachricht, wenn der Prüfcode gültig ist, und wobei der Prüfcode mit einem Sicherheitsschlüssel erzeugt wird und wobei Validieren (164) des Prüf-
codes Folgendes umfasst: 20
- Validieren des Prüfcodes mit einem aktuellen Sicherheitsschlüssel;
wenn die Validierung mit dem aktuellen Sicherheitsschlüssel nicht erfolgreich 25
ist, Validieren des Prüfcodes mit einem vorhergehenden Sicherheitsschlüssel;
wenn die Validierung mit dem vorhergehenden Sicherheitsschlüssel erfolg-
reich ist, Einleiten einer Sicherheits- 30
schlüsselaktualisierung.
2. Verfahren (50) nach Anspruch 1, ferner umfassend Akzeptieren der Steuerungsnachricht mit einem ungültigen Prüfcode, wenn bestimmt wird, dass der Fehler harmlos ist. 35
3. Verfahren (50) nach Anspruch 1, ferner umfassend Akzeptieren der Steuerungsnachricht mit einem ungültigen Prüfcode, wenn die Steuerungsnachricht eine Funktion hoher Priorität spezifiziert. 40
4. Netzwerkknoten (200) in einem passiven optischen Netzwerk, wobei der Knoten Folgendes umfasst: 45
- ein Empfänger-Frontend (210) zum Empfangen von Daten über ein passives optisches Netzwerk;
eine Verarbeitungsschaltung (220) zum Verarbeiten der empfangenen Daten, wobei die Ver- 50
arbeitungsschaltung (220) Folgendes umfasst:
- einen ersten Prozessor (230), der zum Bereitstellen einer Fehlerangabe konfiguriert ist, die angibt, dass die empfangenen Daten 55
einen oder mehrere nicht korrigierte Fehler aufweisen;
einen zweiten Prozessor (240), der als Re-

aktion auf die Fehlerangabe zum Parsen der empfangenen Daten konfiguriert ist, um einen Teil der empfangenen Daten, der nicht durch den/die Fehler betroffen ist, wiederherzustellen,
wobei die empfangenen Daten eine Steuerungsnachricht beinhalten, die durch einen Prüfcode geschützt ist, und wobei der zweite Prozessor (240) zum Parsen der empfangenen Daten konfiguriert ist, um eine Steuerungsnachricht in einem Frame Header wiederherzustellen,
wobei die Steuerungsnachricht durch einen Prüfcode geschützt ist und wobei der zweite Prozessor (240) ferner konfiguriert ist zum:

Validieren des Prüfcodes; und
Akzeptieren der Nachricht, wenn der Prüfcode gültig ist,

wobei der Prüfcode mit einem Sicherheitsschlüssel erzeugt wird und wobei der zweite Prozessor (240) konfiguriert ist zum:

Validieren des Prüfcodes mit einem aktuellen Sicherheitsschlüssel;
wenn die Validierung mit dem aktuellen Sicherheitsschlüssel nicht erfolgreich ist, Validieren des Prüfcodes mit einem vorhergehenden Sicherheitsschlüssel;
wenn die Validierung mit dem vorhergehenden Sicherheitsschlüssel erfolgreich ist, Einleiten einer Sicherheits-
schlüsselaktualisierung.

5. Netzwerkknoten nach Anspruch 4, wobei der zweite Prozessor (240) ferner zum Akzeptieren der Steuerungsnachricht mit einem ungültigen Prüfcode konfiguriert ist, wenn bestimmt wird, dass der Fehler harmlos ist.
6. Netzwerkknoten nach Anspruch 4, wobei der zweite Prozessor (240) ferner zum Akzeptieren der Steuerungsnachricht mit einem ungültigen Prüfcode konfiguriert ist, wenn die Steuerungsnachricht eine Funktion hoher Priorität spezifiziert.
7. Verfahren (170), das in einem Knoten (280) eines passiven optischen Netzwerks implementiert ist, zum Verarbeiten einer Nachricht, die einem nicht wiederherstellbaren Fehler enthält, wobei das Verfahren (170) Folgendes umfasst:
- Empfangen (172) einer Nachricht mit einem Nachrichtenprüfcode; Validieren (174) des Prüf-
codes;
Akzeptieren (176) der Nachricht, wenn der Prüf-
code gültig ist;

- Akzeptieren der Nachricht mit einem ungültigen Prüfcode, wenn ein vorbestimmtes Akzeptanzkriterium erfüllt wird;
wobei der Prüfcode mit einem Sicherheits-
schlüssel erzeugt wird und wobei Validieren
(174) des Prüfcodes Validieren des Prüfcodes
mit einem aktuellen Sicherheitsschlüssel um-
fasst,
wobei Akzeptieren der Nachricht mit einem un-
gültigen Prüfcode Folgendes umfasst: 5 10
- Validieren (178) des Prüfcodes mit einem
vorhergehenden Sicherheitscode;
Akzeptieren der Nachricht, wenn die Vali-
dierung mit dem vorhergehenden Sicher-
heitsschlüssel erfolgreich ist; 15
wobei das Verfahren ferner Folgendes um-
fasst: Einleiten (180) einer Sicherheits-
schlüsselaktualisierung, wenn die Validie-
rung mit dem vorhergehenden Sicherheits-
schlüssel erfolgreich ist. 20
8. Verfahren (170) nach Anspruch 7, wobei Akzeptie-
ren der Nachricht mit einem ungültigen Prüfcode Ak-
zeptieren der Nachricht umfasst, wenn bestimmt
wird, dass der Fehler harmlos ist. 25
9. Verfahren nach Anspruch 7, wobei Akzeptieren
(184) der Nachricht mit einem ungültigen Prüfcode
Akzeptieren der Nachricht umfasst, wenn eine Prio-
rität der Nachricht ein vorbestimmtes Prioritätsni-
veau ist. 30
10. Verfahren nach Anspruch 7, wobei die Nachricht eine
Nachricht für Verwaltung und Wartung auf der
physischen Schicht (physical layer, administration
and maintenance - PLOAM) umfasst. 35
11. Netzwerkknoten (200) in einem passiven optischen
Netzwerk, wobei der Netzwerkknoten (200) Folgen-
des umfasst: 40
- einen Empfänger (210) zum Empfangen von
Daten über eine passive optische Verbindung;
einen Prozessor (220), der konfiguriert ist zum: 45
- Empfangen einer Nachricht mit einem
Nachrichtenprüfcode; Validieren des Prüf-
codes;
Akzeptieren der Nachricht, wenn der Prüf-
code gültig ist; 50
Akzeptieren der Nachricht mit einem ungül-
tigen Prüfcode, wenn ein vorbestimmtes
Akzeptanzkriterium erfüllt wird;
wobei der Prüfcode mit einem Sicherheits-
schlüssel erzeugt wird und wobei der Pro-
zessor (220) zum Validieren des Prüfcodes
mit einem aktuellen Sicherheitsschlüssel
- konfiguriert ist, und
wobei der Prozessor (220) konfiguriert ist
zum:
- Validieren des Prüfcodes mit einem
vorhergehenden Sicherheitscode,
wenn die Validierung mit dem aktuellen
Sicherheitsschlüssel fehlschlägt; und
Akzeptieren der Nachricht, wenn die
Validierung mit dem vorhergehenden
Sicherheitsschlüssel erfolgreich ist;
- wobei der Prozessor (220) ferner konfigu-
riert ist zum: Einleiten einer Sicherheits-
schlüsselaktualisierung, wenn die Validie-
rung mit dem vorhergehenden Sicherheits-
schlüssel erfolgreich ist.
12. Netzwerkknoten (200) nach Anspruch 11, wobei der
Prozessor (220) zum Akzeptieren der Nachricht kon-
figuriert ist, wenn bestimmt wird, dass der Fehler
harmlos ist.
13. Netzwerkknoten (200) nach Anspruch 11, wobei der
Prozessor (220) zum Akzeptieren der Nachricht kon-
figuriert ist, wenn eine Priorität der Nachricht ein vor-
bestimmtes Prioritätsniveau ist.
14. Netzwerkknoten (200) nach Anspruch 11, wobei die
Nachricht eine Nachricht für Verwaltung und War-
tung auf der physischen Schicht (physical layer, ad-
ministration and maintenance - PLOAM) umfasst.

Revendications

1. Procédé (50) mis en oeuvre dans un noeud (200)
d'un réseau optique passif pour le traitement de don-
nées contenant des erreurs non corrigées, ledit pro-
cédé (50) comprenant :

la réception (52), par une première couche de
protocole, de données contenant une ou plu-
sieurs erreurs non corrigibles ;
la fourniture (54) des données à une deuxième
couche de protocole avec une indication
d'erreur ; et
l'analyse syntaxique (56), par la deuxième cou-
che de protocole, des données reçues en ré-
ponse à l'indication d'erreur pour récupérer une
portion des données reçues non affectées par
l'erreur ou les erreurs,
dans lequel lesdites données reçues compren-
nent un message de commande protégé par un
code de vérification et dans lequel l'analyse syn-
taxique (56) des données reçues comprend
l'analyse syntaxique desdites données reçues
pour récupérer le message de commande,

dans lequel ledit message de commande est protégé par un code de vérification et comprenant en outre :

la validation (164) du code de vérification ; 5
et
l'acceptation (166) du message si le code de vérification est valide,

et dans lequel le code de vérification est généré 10
avec une clé de sécurité et dans lequel la validation (164) du code de vérification comprend :

la validation du code de vérification avec 15
une clé de sécurité actuelle ;
si la validation avec la clé de sécurité actuelle échoue, la validation du code de vérification avec une clé de sécurité précédente ;
si la validation avec la clé de sécurité précédente réussit, le lancement d'une mise à 20
jour de clé de sécurité.

2. Procédé (50) selon la revendication 1, comprenant 25
en outre l'acceptation du message de commande avec un code de vérification invalide s'il est déterminé que l'erreur est inoffensive.

3. Procédé (50) selon la revendication 1, comprenant 30
en outre l'acceptation du message de commande avec un code de vérification invalide si le message de commande spécifie une fonction considérée comme hautement prioritaire.

4. Noeud de réseau (200) dans un réseau optique passif, ledit noeud comprenant :

un dispositif frontal de récepteur (210) pour recevoir des données sur un réseau optique passif ; 40
un circuit de traitement (220) pour traiter des données reçues, ledit circuit de traitement (220) comprenant :

un premier processeur (230) configuré pour 45
fournir une indication d'erreur indiquant que des données reçues comportent une ou plusieurs erreurs non corrigées ;
un deuxième processeur (240) configuré 50
pour analyser syntaxiquement, en réponse à l'indication d'erreur, les données reçues pour récupérer une portion des données reçues non affectées par l'erreur ou les erreurs,
dans lequel les données reçues comprennent 55
un message de commande protégé par un code de vérification et dans lequel le deuxième processeur (240) est configuré

pour analyser syntaxiquement les données reçues pour récupérer un message de commande dans une en-tête de trame, dans lequel ledit message de commande est protégé par un code de vérification et dans lequel le deuxième processeur (240) est configuré en outre pour :

valider le code de vérification ; et
accepter le message si le code de vérification est valide,

dans lequel le code de vérification est généré avec une clé de sécurité et dans lequel le deuxième processeur (240) est configuré pour :

valider le code de vérification avec une clé de sécurité actuelle ;
si la validation avec la clé de sécurité actuelle échoue, valider le code de vérification avec une clé de sécurité précédente ;
si la validation avec la clé de sécurité actuelle réussit, lancer une mise à jour de clé de sécurité.

5. Noeud de réseau selon la revendication 4, dans lequel le deuxième processeur (240) est configuré en outre pour accepter le message de commande avec un code de vérification invalide s'il est déterminé que l'erreur est inoffensive.

6. Noeud de réseau selon la revendication 4, dans lequel le deuxième processeur (240) est configuré en outre pour accepter le message de commande avec un code de vérification invalide si le message de commande spécifie une fonction considérée comme hautement prioritaire.

7. Procédé (170) mis en oeuvre dans un noeud (280) d'un réseau optique passif pour le traitement d'un message contenant des erreurs irrécupérables, ledit procédé (170) comprenant :

la réception (172) d'un message ayant un code de vérification de message ;
la validation (174) du code de vérification ;
l'acceptation (176) du message si le code de vérification est valide ;
l'acceptation du message avec un code de vérification invalide si un critère d'acceptation prédéterminé est satisfait ;
dans lequel le code de vérification est généré avec une clé de sécurité et dans lequel la validation (174) du code de vérification comprend la validation du code de vérification avec une clé de sécurité actuelle,

dans lequel l'acceptation du message avec un code de vérification invalide comprend :

la validation (178) du code de vérification avec une clé de sécurité précédente ;
l'acceptation du message si la validation avec la clé de sécurité précédente réussit ;
dans lequel le procédé comprend en outre : le lancement (180) d'une mise à jour de clé de sécurité si la validation avec la clé de sécurité précédente réussit.

8. Procédé (170) selon la revendication 7, dans lequel l'acceptation (du message avec un code de vérification invalide comprend l'acceptation du message s'il est déterminé que l'erreur est inoffensive.

9. Procédé selon la revendication 7, dans lequel l'acceptation (184) du message avec un code de vérification invalide comprend l'acceptation du message si une priorité du message est un niveau de priorité prédéterminé.

10. Procédé selon la revendication 7, dans lequel le message comprend un message de couche physique d'administration et de maintenance, PLOAM.

11. Noeud de réseau (200) dans un réseau optique passif, ledit noeud de réseau (200) comprenant :

un récepteur (210) pour recevoir des données sur un réseau optique passif ;
un processeur (220) configuré pour :

recevoir un message ayant un code de vérification de message ; valider le code de vérification ;
accepter le message si le code de vérification est valide ;
accepter le message avec un code de vérification invalide si un critère d'acceptation prédéterminé est satisfait ;
dans lequel le code de vérification est généré avec une clé de sécurité et dans lequel le processeur (220) est configuré pour valider le code de vérification avec une clé de sécurité actuelle, et
dans lequel le processeur (220) est configuré pour :

valider le code de vérification avec une clé de sécurité précédente si la validation avec la clé de sécurité actuelle échoue ; et
accepter le message si la validation avec la clé de sécurité précédente réussit ;

dans lequel le processeur (220) est configuré en outre pour : lancer une mise à jour de clé de sécurité si la validation avec la clé de sécurité précédente réussit.

12. Noeud de réseau (200) selon la revendication 11, dans lequel le processeur (220) est configuré pour accepter le message s'il est déterminé que l'erreur est inoffensive.

13. Noeud de réseau (200) selon la revendication 11, dans lequel le processeur (220) est configuré pour accepter le message si une priorité du message est un niveau de priorité prédéterminé.

14. Noeud de réseau (200) selon la revendication 11, dans lequel le message comprend un message de couche physique d'administration et de maintenance, PLOAM.

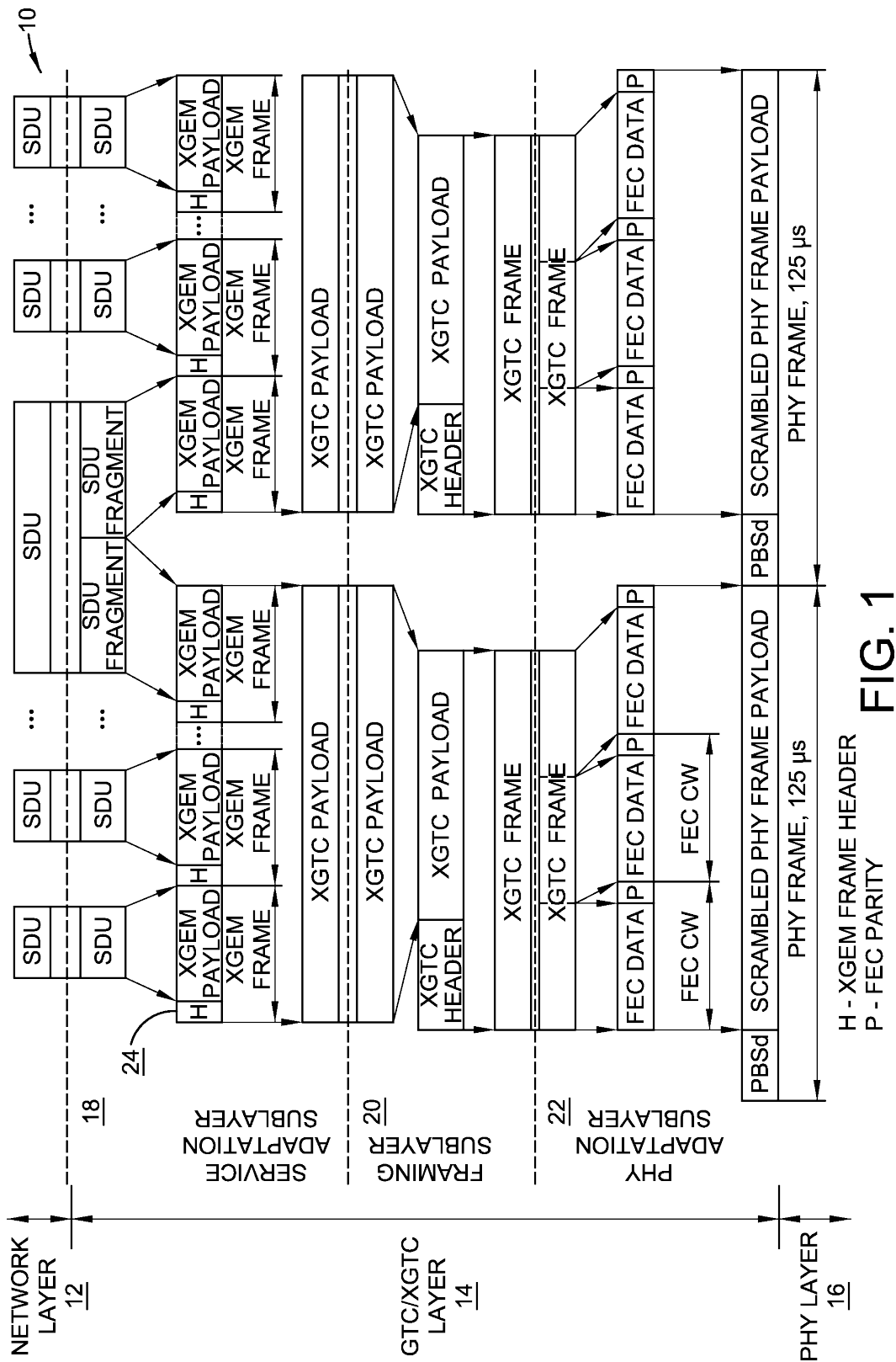


FIG. 1

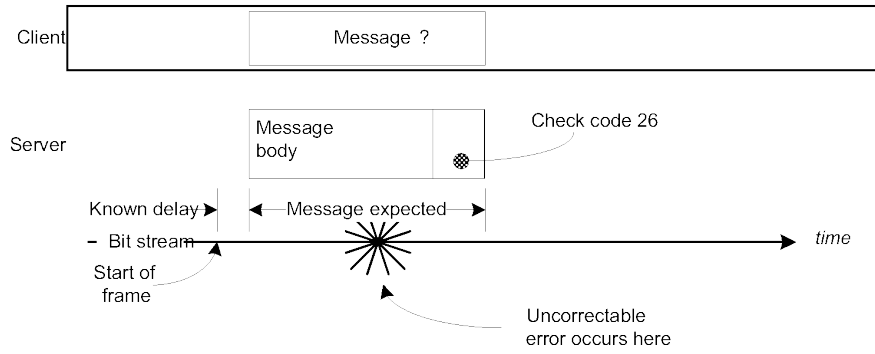


FIG. 2

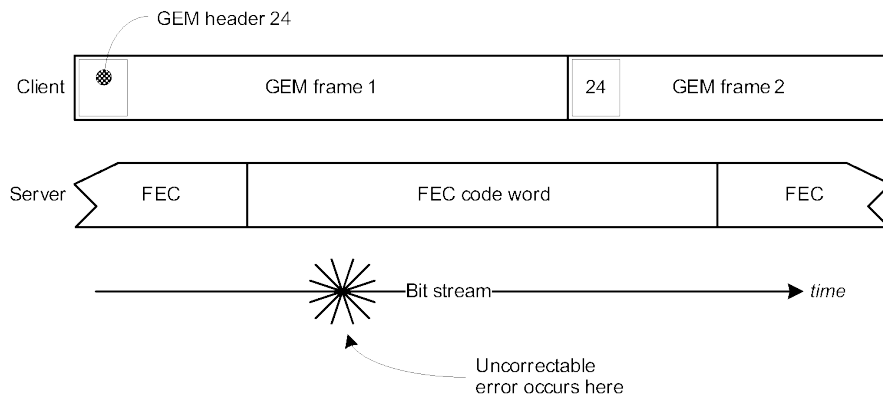


FIG. 3

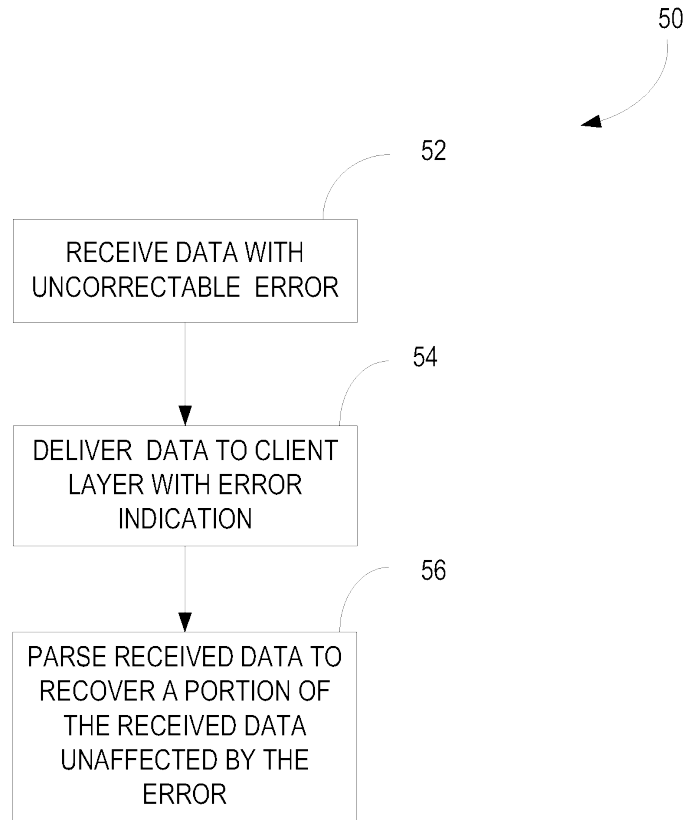


Fig. 4

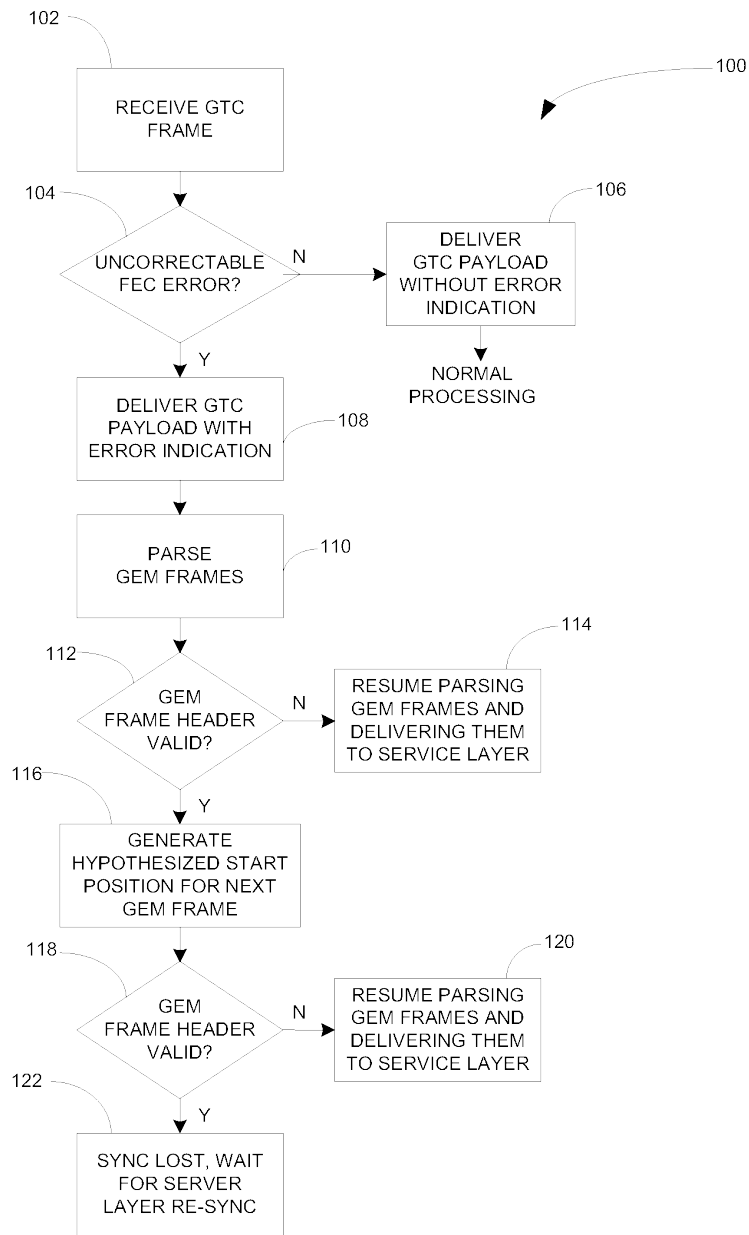


Fig. 5

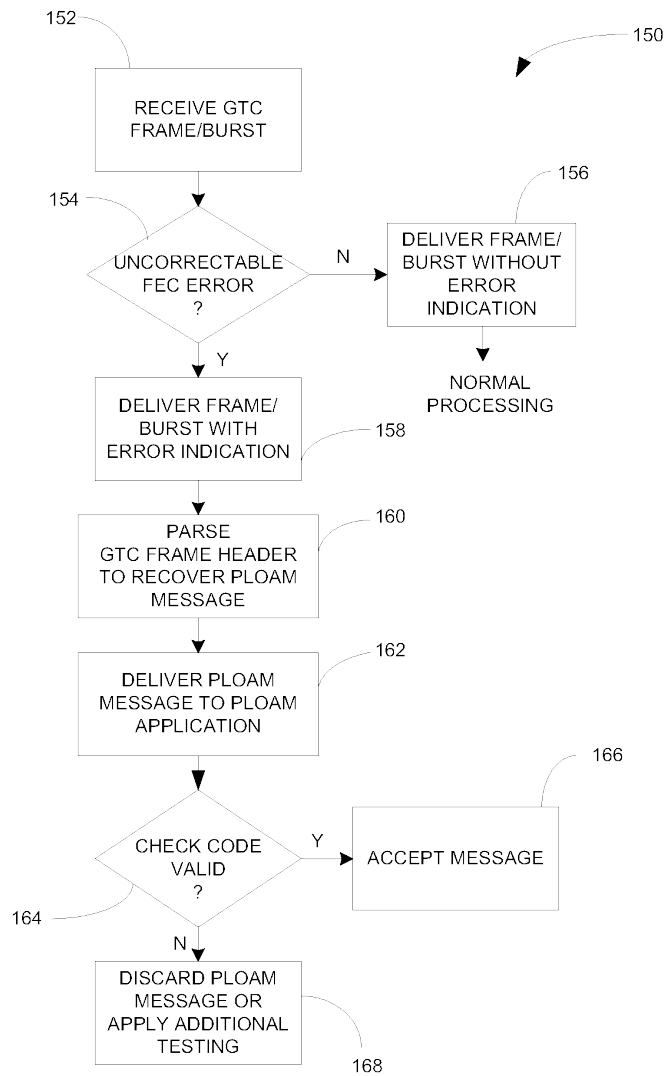


FIG. 6

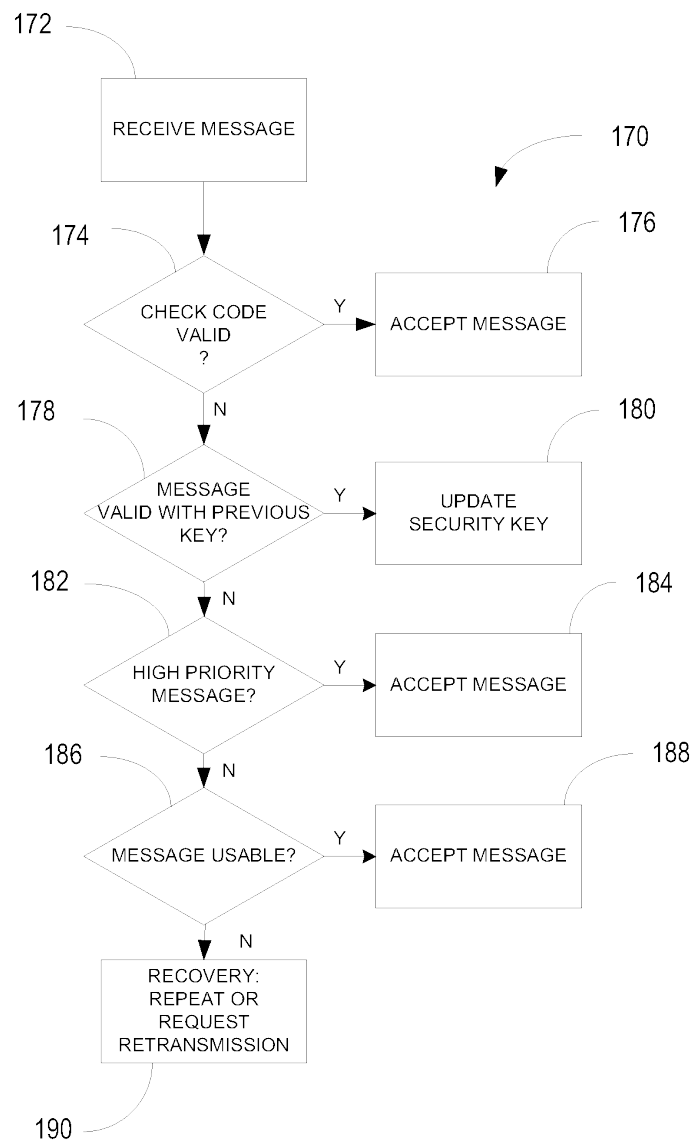


FIG. 7

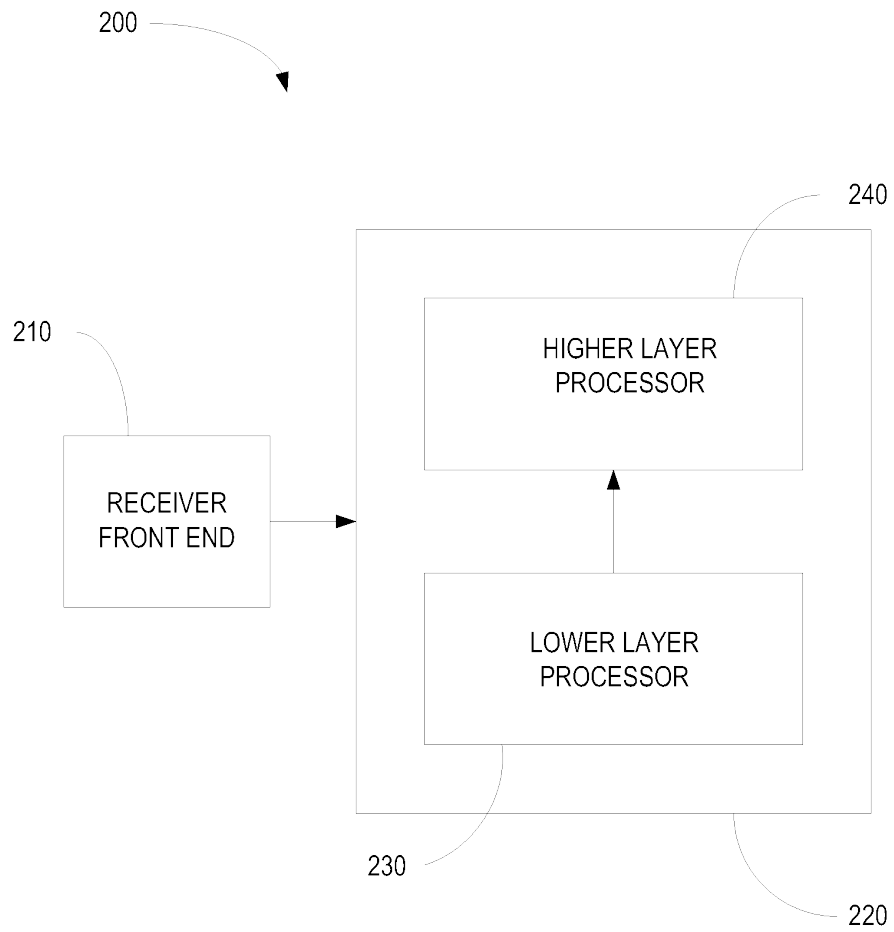


Fig. 8

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- WO 2010142853 A1 [0008]
- EP 1755248 A1 [0009]

Non-patent literature cited in the description

- 3av-0811-anslow-1. *Draft Amendment to IEEE Std 802.3-2008*, 07 October 2008 [0007]
- 10-Gigabit-capable passive optical networks (XG-PON): Transmission convergence (TC) specifications; G.987.3 (10/10). ITU-T STANDARD. INTERNATIONAL TELECOMMUNICATION UNION, 07 October 2010, 1-134 [0010]