GPON 984.3

Section 12-14

Reporter: 王依盈

94.10.26

Outline

- Security
- Forward Error Correction
- OMCI Transport Mechanism

- Security
  - Basic Threat Model
  - Encryption System
  - Key exchange and switch-over
- Forward Error Correction
- OMCI Transport mechanism

Basic Threat Model

- PON is highly directional
- Any ONU cannot observe the upstream traffic from the other ONUs on the PON
- Downstream data is broadcast to all ONUs
  - Eavesdropping threat: A malicious user wants to re-program his ONU such that he could listen to all the downstream data
  - Other exotic threats are not considered practically

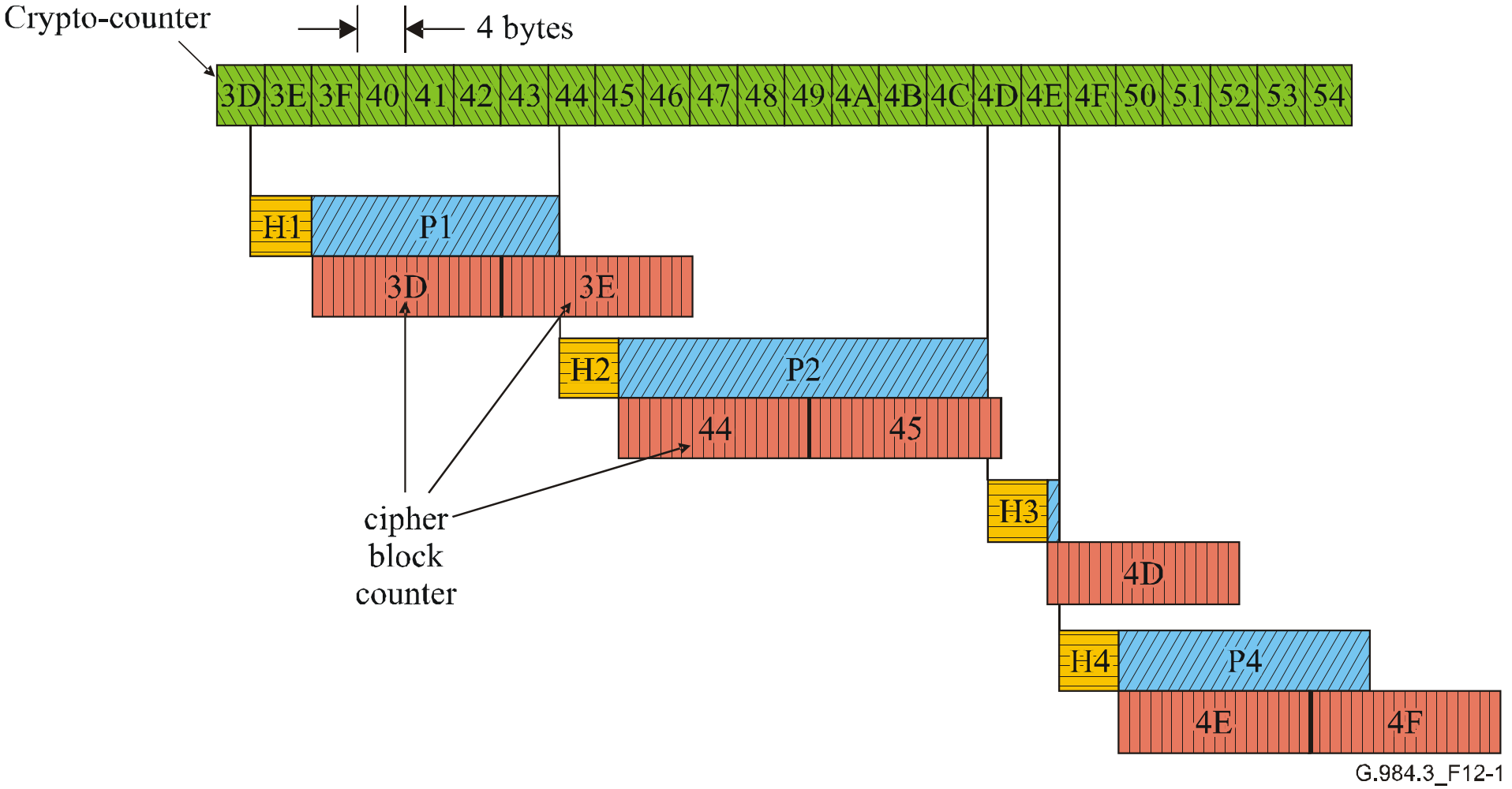
Encryption system

- Advanced Encryption Standard (AES)
  - 128, 192, and 256 byte keys work with16-byte blocks of data
- Counter mode: a synchronized crypto-counter that is common to the OLT and all ONUs
  - Counter is 46 bits –upper 30 bits as inter-frame counter, lower 16 bits as intra-frame counter
  - Intra-frame counter is reset to 0 at the beginning of downstream frame, and is incremented every 4 bytes
  - Inter-frame counter is the same as the super-frame counter, ONU implements a synchronized counter in case of error

Encryption system (con’t)

- In the case of ATM data: 48 bytes = 16 bytes * 3 (blocks)
- In the case of GEM fragments: the port-id header is not encrypted, the last data block (1-16 bytes in length) is also OK
- Generation of cipher-text
  - The cipher generates a stream of 16-byte pseudo-random cipher blocks
  - XOR with input text

- The relationship between cipher block sequence and crypto-counter sequence



Key Exchange

- Initiate by the OLT sending *key_request_msg* in the PLOAM channel (divided into 2 pieces and sent 3 times)
- ONU responds by generating, storing, and sending the key
- All ONU transmissions of a particular key have the same value of Key_index
- Key_index is incremented for each key that the ONU generates upon request from OLT

Switch over

- Once OLT receives the key, it stores the key in the *shadow_key_reg*
- OLT chooses a frame number to be the first frame to use the new key
- OLT tells ONU the super-frame number of this frame using *Key_switching_time* msg (sent 3 times)
- At the beginning of the chosen frame, ONU will copy its *shadow_key_reg* into the *active_key_reg,* so OLT and ONU begin using the new key at precisely the same frame

- Security
- Forward Error Correction
  - Reed-Solomon (Block based FEC)
  - Downstream FEC
  - Upstream FEC
  - Last Codeword
  - FEC synch and control
- OMCI Transport mechanism

Forward Error Correction

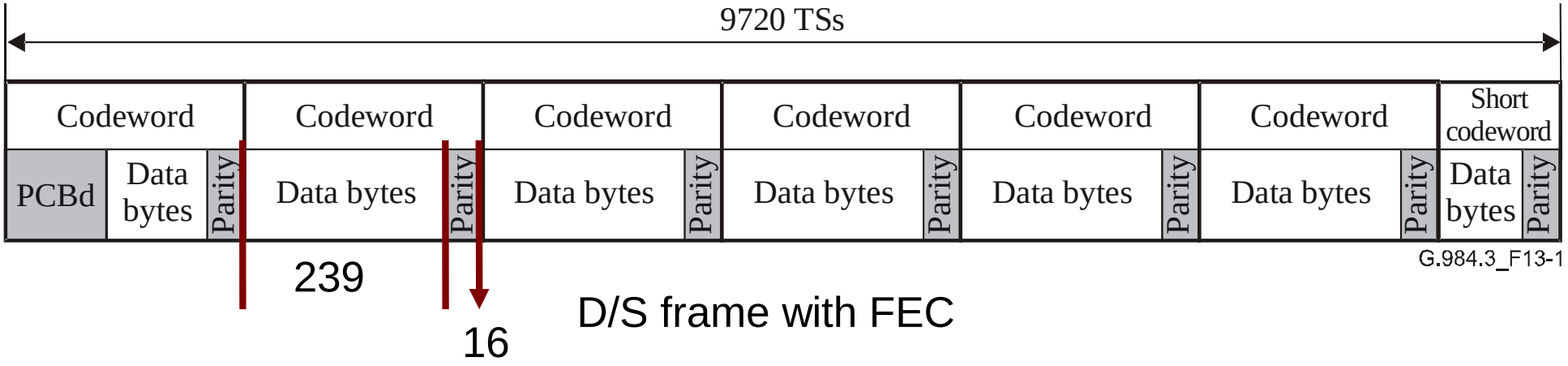
- Used by the transport layer in communication system
- Based on transmitting data in encoded format
- Encoding redundancy can decrease BER
- FEC results in an increased link budget, so higher bit rate and longer distance can be supported

Reed-Solomon

- RS is a block based code
- It takes a data block of constant size and adds extra ‘redundant’ bits at the end
- Detail is specified in ITU-T Rec. J.81
- RS(255,239)
  - Codeword is 255 bytes long, consists of 239 data bytes followed by 16 parity bytes
- Not efficient for very high BER

Downstream FEC

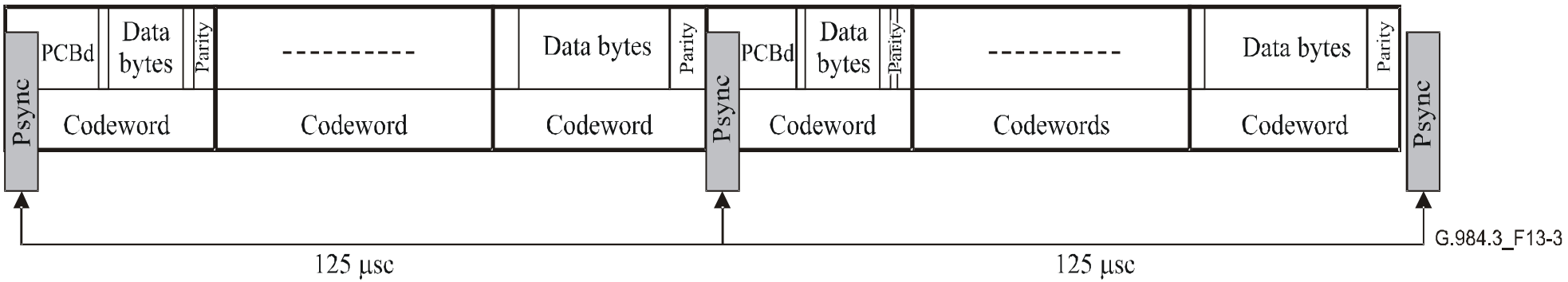
- The codeword begins with the framing section (PCBd), which is the first byte
- The next codeword will start after the 255th byte and will be repeated every 255 bytes
- When FEC is used, less bandwidth is available for user data



D/S frame with FEC

D/S FEC code synchronization

- Frame sync at ONU
  - The Psync field of the PCBd remains unchanged during the encoding process



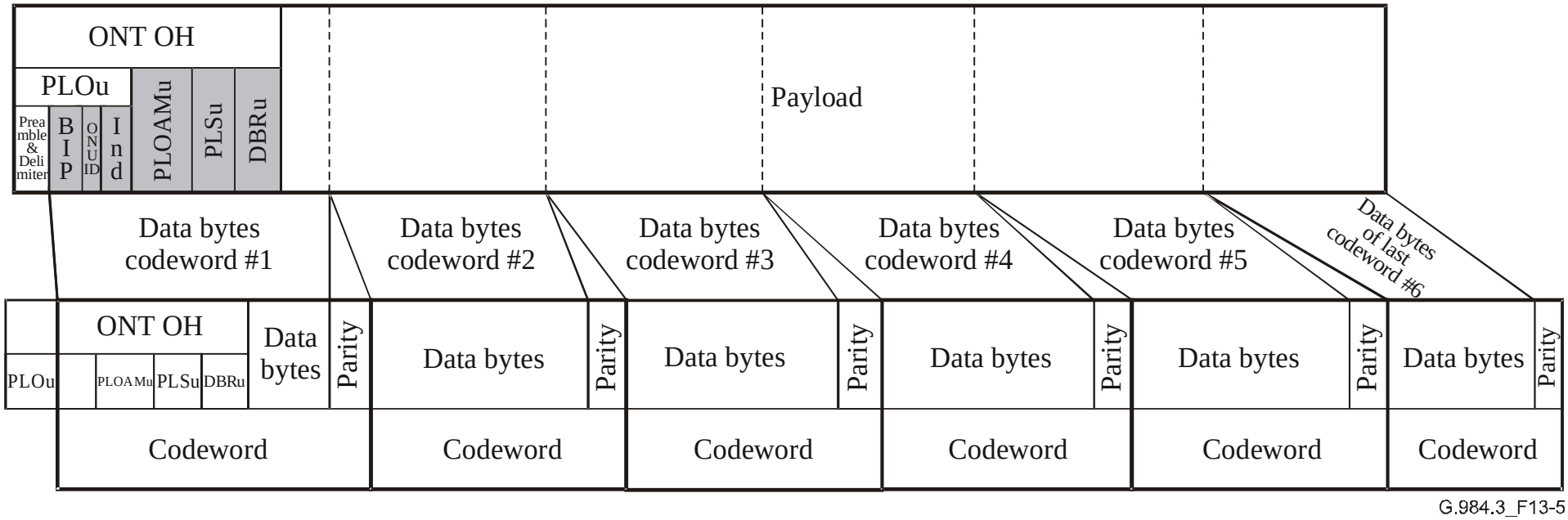
- Codeword sync
  - Once frame sync is achieved, codeword sync is also achieved

D/S FEC On/Off control

- The D/S FEC function can be activated/ deactivated at the OLT by operation system
  - FEC indication bit is located in the IDENT field
- FEC detection at ONU receiver
  - Default value is off.
  - Four consecutive On/Off indication bits will change the FEC status at ONU

Upstream FEC

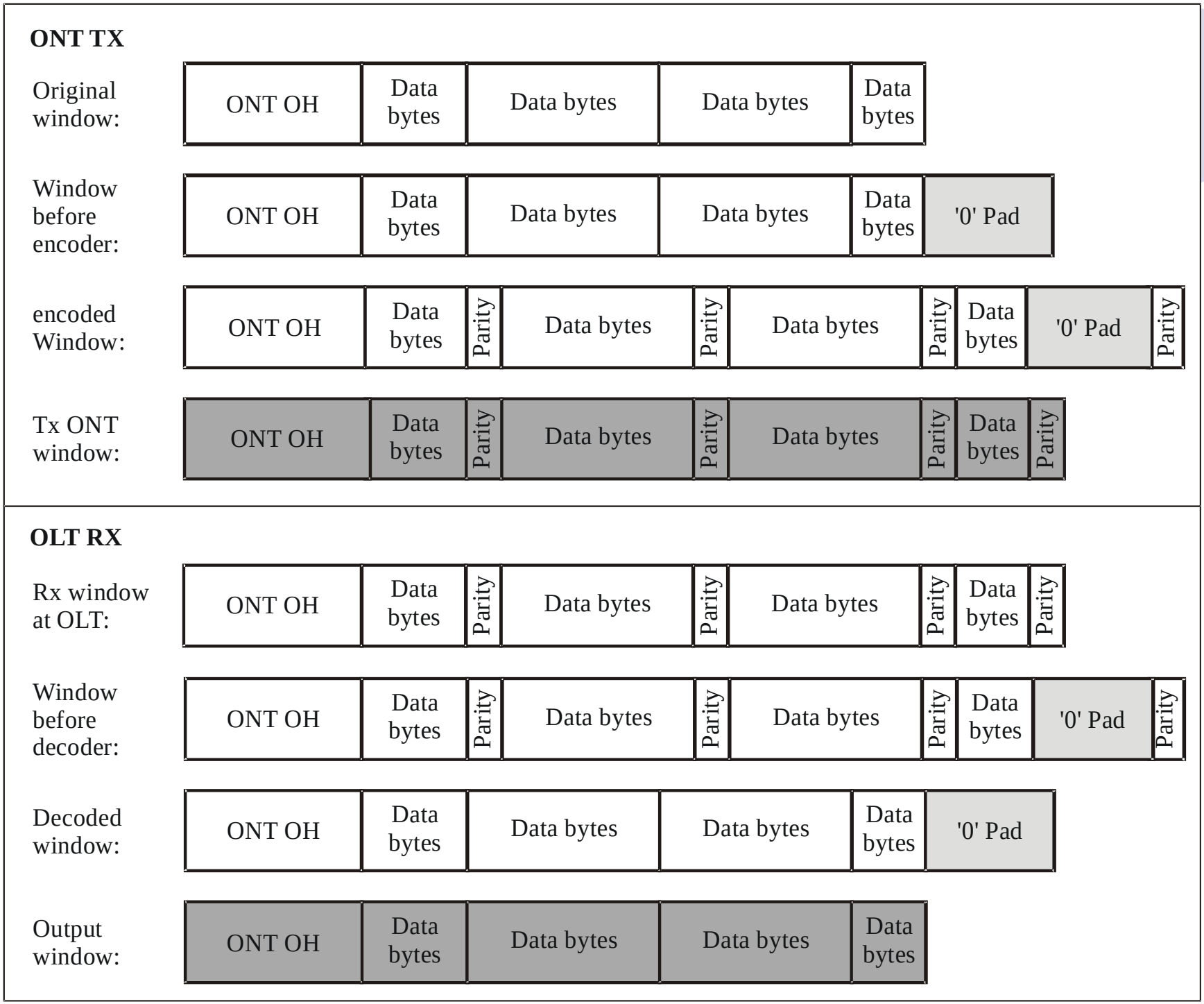
- RS(255,239) is used
- The Preamble and Delimiter fields of the PLOu are not included in the first codeword



U/S frame with FEC

Last codeword

- Pad extra zeros at the end of the last codeword
- Calculate parity bytes
- Remove the ‘0’ pad bytes and transmit the codeword
- While receiving, OLT will reinsert the extra ‘0’ bytes before decode it
- Following the decoding process, the extra bits are once again removed


ONT TX
Original window:
ONT OH
Data bytes
Data bytes
Data bytes
Data bytes
Window before encoder:
ONT OH
Data bytes
Data bytes
Data bytes
Data bytes
'0' Pad
encoded Window:
ONT OH
Data bytes
Parity
Data bytes
Parity
Data bytes
Parity
Data bytes
'0' Pad
Parity
Tx ONT window:
ONT OH
Data bytes
Parity
Data bytes
Parity
Data bytes
Parity
Data bytes
Parity
OLT RX
Rx window at OLT:
ONT OH
Data bytes
Parity
Data bytes
Parity
Data bytes
Parity
Data bytes
Parity
Window before decoder:
ONT OH
Data bytes
Parity
Data bytes
Parity
Data bytes
Parity
Data bytes
'0' Pad
Parity
Decoded window:
ONT OH
Data bytes
Data bytes
Data bytes
Data bytes
'0' Pad
Output window:
ONT OH
Data bytes
Data bytes
Data bytes
Data bytes

G.984.3_F13-6

U/S FEC code synchronization

- Transmission sync
  - The preamble and delimiter fields are received unchanged at the OLT
  - Codeword sync is not needed
- Framing-word error
  - Up to three or four errored bits are allowed in the delimiter (framing) word, if the delimiter is 16 or 20 bits long, respectively

U/S FEC On/Off control

- The U/S FEC function of the ONU can be activated/deactivated by the operation system via the OLT
  - OLT sets the ONU FEC status using the UseFEC bit in the FLAGS field
- FEC detection at OLT
  - Same as D/S
- For all special ONU-activation transmissions, no FEC will be applied

- Security
- Forward Error Correction
- OMCI Transport Mechanism

OMCI Transport Mechanism

- ONU Management and Control Interface
- Basic framework is given in ITU-T Rec. G.983.2
- OMCI operates on a dedicated bidirectional virtual channel between the management station and the ONU
- The management station can be the OLT itself or other network element

OMCI Transport Mechanism (2)

- Two transport modes: ATM and GEM
- OLT and ONU may support both or either one
- The OMCI primitive data units are 48-bytes in length
  - ATM mode: datagrams are carried in the ATM cell payloads
  - GEM mode: payloads are encapsulated with a GEM header

OMCI Transport Mechanism (3)

- OMCI adapter at the ONU is responsible for
  - In the D/S: filtering and de-encapsulation either cells **or** frames
  - In the U/S: encapsulating the PDUs
- OMCI adapter at the control station is responsible for
  - In the D/S: encapsulating the PDUs from control logic to ONU
  - In the U/S: filtering and de-encapsulation cells **and** frames