**Date:** February 3, 2022
**To:** FC-FS-6 Project Ad-hoc
**RE**: ESP End-to-end Protection CRC Proposal (T11-2022-00027-v000 replacing T11-2021-00022-v00))
**Proposer Contacts:** David Kwak <dkwak@marvell.com>, Ali Khwaja <akhwaja@marvell.com>, Craig W. Carlson <cwcarlson@marvell.com>

This proposal contains detailed text for the ideas contained in T11-2020-223 and T11-2021-00021.

Below are the proposed changes for the ESP End-to-end Protection CRC proposal. New text added for the proposal is indicated in blue.

# 14 Optional headers

## 14.1 Scope

Optional headers are a function of the FC-2V sublevel.

## 14.2 Introduction

Optional headers defined within the Data_Field of a frame are:

a) ESP_Header and ESP_Trailer;
b) Network_Header; and
c) Device_Header.

Control bits in the DF_CTL field of the Frame_Header define the presence of optional headers (see 12.9). The sum of the length in bytes of the Payload, the number of fill bytes, and the lengths in bytes of all optional headers shall not exceed 2 112. The sequential order of the optional headers, Payload, and their sizes are indicated in figure 73, figure 74, and figure 75.

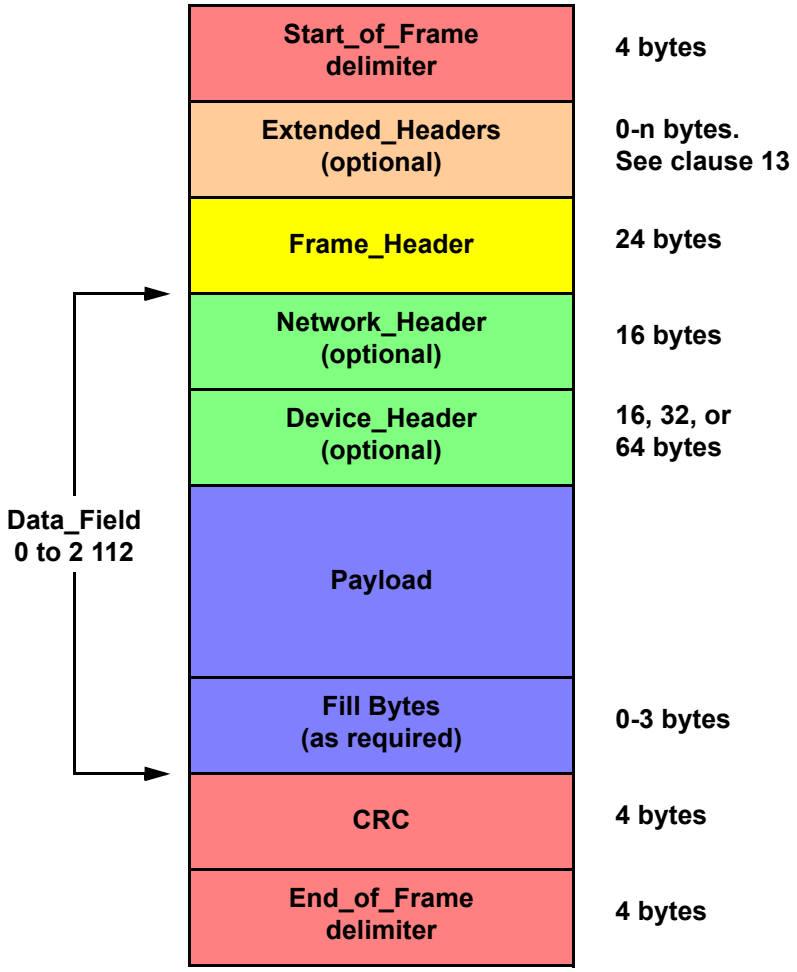


**Figure 73 - Frame structure when ESP_Header is not used**

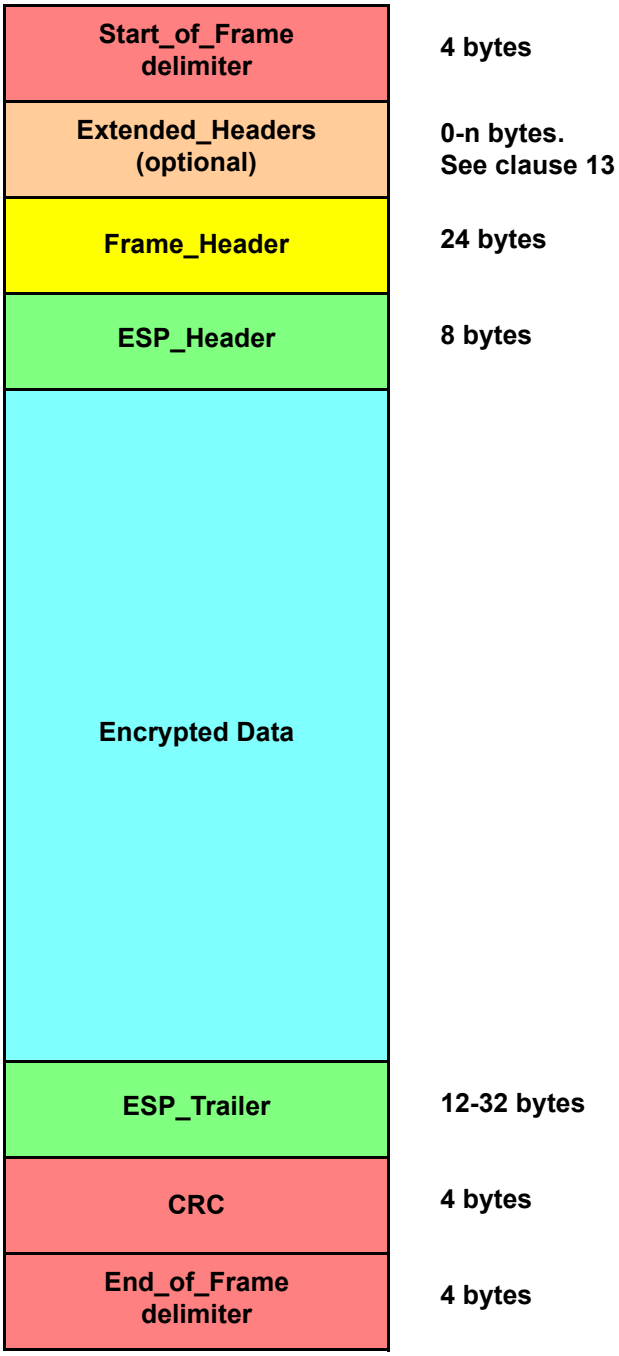


**Figure 74 - Frame structure with End-to-end ESP_Header and ESP_Trailer**

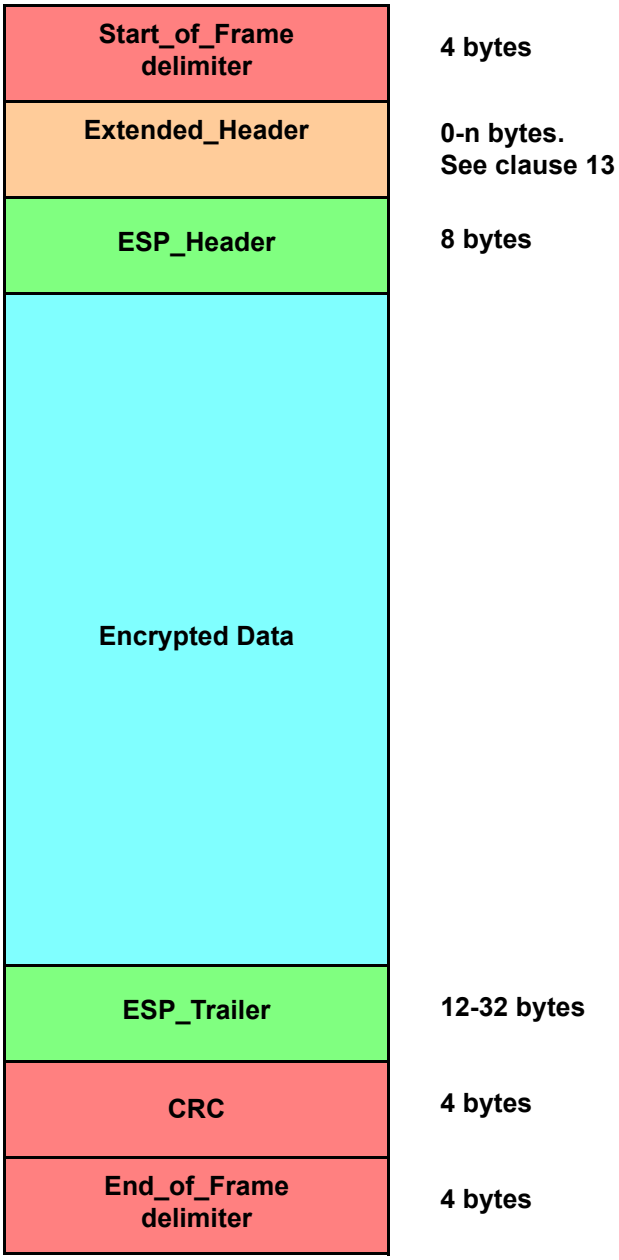


**Figure 75 - Frame structure with Link-by-link ESP_Header and ESP_Trailer**

Optional headers are provided for use of the FC-4 level. The use of the optional headers is not defined by this standard.

If the Payload is not a multiple of four bytes, fill bytes shall be appended to the Payload as necessary (see 12.7.13).

## 14.3 ESP_Header

### 14.3.1 Overview

The Encapsulating Security Payload (ESP) is defined in the IETF document RFC 4303. It is a generic mechanism to provide confidentiality, data origin authentication, and anti-replay protection to IP packets. FC-SP-2 defines how to use ESP in Fibre Channel, including any negotiation procedure, additional encryption/authentication algorithm and processing requirements. This clause defines the structure of a Fibre Channel frame conveying an ESP_Header.

End-to-end ESP_Header processing shall be applied to FC frames in transport mode (see RFC 4303), and Link-by-link ESP_Header processing shall be applied to FC frames in tunnel mode (see RFC 4303). The Authentication option shall be used, Confidentiality may be negotiated by the two communicating FC_Ports (see FC-SP-2).

ESP_Header processing may be applied End-to-end, Link-by-link, or both. End-to-end ESP_Header processing is indicated in the Frame_Header of the frame, is applied by the Nx_Port identified in the S_ID of the frame, and is removed by the Nx_Port identified in the D_ID of the frame. Link-by-link ESP_Header may be indicated in an Extended_Header of the frame, is applied to a frame at the transmitting end of a link, and removed at the receiving end of the link.

NOTE 27 - An intended application of Link-by-link ESP_Header processing is to secure a link in a Fabric or between Fabrics without requiring use of ESP by every Nx_Port.

This specification adheres to RFC 4303 except for the ICV coverage. Variations of ICV coverage are defined for each header in which a Fibre Channel ESP_Header is indicated.

### 14.3.2 Application of End-to-end ESP_Header processing

Table 56 shows the format of an FC frame to which End-to-end ESP_Header processing is applied. Presence of an End-to-end ESP_Header is indicated in the DF_CTL field of the Frame_Header. A sender shall apply End-to-end ESP_Header processing to an FC frame as follows:

1) Compute the ESP End-to-end Protection CRC if the feature is enabled (see 14.3.5);
2) Add a fixed length ESP_Header (8 bytes) following the Frame_Header, specifying a Security Parameter Index (SPI) and an ESP Sequence Number;
3) Pad the concatenation of any other optional headers, the Payload, and any required fill bytes to the block size required by the negotiated encryption/authentication algorithms. The Pad Length field shall contain the length of this ESP padding, if ESP End-to-end Protection is enabled, place the CRC calculated in 1) into the ESP padding (see 14.3.5);
4) Apply the negotiated encryption algorithm to the data resulting from item 3);
5) Compute an Integrity Check Value (ICV), using the negotiated authentication algorithm and parameters, covering:
   i) the Frame_Header, with the S_ID, D_ID, and CS_CTL/Priority fields set to zero for the purpose of the ICV computation;
   ii) the ESP_Header; and
   iii) the data resulting from item 4);

   and
6) Add an ESP_Trailer containing the ICV computed in item 5). The length of the ESP_Trailer shall be negotiated (see FC-SP-2) and shall be a multiple of 32 bits. {CWC: This reference is confusing, there is NO mention of ESP_Trailer in FC-SP-2.}

NOTE 28 - In step 5), the CS_CTL/Priority field is excluded because it is a mutable field, and the S_ID field and D_ID field are excluded to permit address translation.

A receiver shall apply End-to-end ESP_Header processing to an FC frame as follows:

1) Check the ESP_Header, using the SPI to retrieve the negotiated parameters required to interpret the received FC frame, and the ESP Sequence Number to avoid replay attacks (see RFC 4303). The length of the ESP_Trailer is one of the retrieved parameters;
2) Compute an ICV, using the retrieved parameters, covering:
   i) the Frame_Header, with the S_ID, D_ID, and CS_CTL/Priority fields set to zero for the purpose of the ICV computation;
   ii) the ESP_Header; and
   iii) the encrypted data;
3) Check the computed ICV with the content of the ESP_Trailer. If they are equal the authentication is successful, otherwise not;
4) Apply the negotiated decryption algorithm to the encrypted data;
5) Remove the ESP padding and process the resulting optional headers, Payload, and fill bytes that are present; and
6) Check the ESP End-to-end Protection CRC against the decrypted data if the feature is enabled (see 14.3.5).

Processing of the ESP_Header and ESP_Trailer shall be performed before removing any fill bytes determined by the F_CTL Fill Bytes field in the Frame_Header.

The End-to-end ESP_Header processing shall be transparent to the FC-4. On the sending side the End-to-end ESP_Header processing shall be applied to every frame of a sequence to be protected. On the receiving side, the End-to-end ESP_Header processing shall be applied to every frame that carries an ESP_Header, and only after that the sequence shall be reassembled and sent to the FC-4.

The ESP_Header and ESP_Trailer, if used, shall be present in every frame of a Sequence. If the receiving FC_Port does not support the ESP_Header function, it shall discard the FC frame.

**Table 56 - End-to-end ESP_Header and ESP_Trailer**

| Word \ Bits | 31 .. 24 | 23 .. 16 | 15 .. 08 | 07 .. 00 |
|---|---|---|---|---|
| **0** | R_CTL | D_ID | | |
| **1** | CS_CTL / Priority | S_ID | | |
| **2** | TYPE | F_CTL | | |
| **3** | SEQ_ID | DF_CTL | SEQ_CNT | |
| **4** | OX_ID | | RX_ID | |
| **5** | Parameter | | | |
| **6** | Security Parameter Index (SPI) | | | |
| **7** | ESP Sequence Number | | | |
| **8 .. M** | Other Optional Headers (if present) | | | |
| **M+1 .. N** | Payload (variable length) | | | |
| | | Fill Bytes (if present) | | |
| **N+1 .. P** | ESP Padding (2-254 bytes) | | | |
| | | | Pad Length | Not meaningful |
| **P+1 .. Q** | Integrity Check Value | | | |
| **Q+1** | CRC | | | |

NOTE 1 The D_ID, S_ID, and CS_CTL/Priority fields zeroed for the purposes of ICV computation.
NOTE 2 The ESP_Header consists of words 6 and 7.
NOTE 3 The ESP_Trailer consists of words P+1 through Q. {CWC: This appears to be the ONLY place that ESP_Trailer is defined. We probably need a better definition.}
NOTE 4 Confidentiality covers words 8 through P.
NOTE 5 Authentication covers words 0 through P.
NOTE 6 Other Optional Headers are possibly present in words 8 to M as specified in 12.9.

### 14.3.5 ESP End-to-end Protection

#### 14.3.5.1 Overview

This sub-clause defines an optional mechanism for providing end-to-end data integrity protection while ESP encryption is enabled. The purpose of this mechanism is to provide for method of detecting bit errors introduced during the encryption/decryption process.

For ESP End-to-end Protection, there are the following components:

a) During Security Association negotiation, use of the ENCR_AES_GCM with end-to-end encryption protection or ENCR_AES_AUTH_AES_GMAC with end-to-end encryption protection indicates support of the feature (see FC-SP-2 AM2);
{CWC: I used the names proposed in T11-2022-00022-v000. Perhaps a more concise name for the end-to-end feature code-points would be good.}
b) a 16-bit CRC is put in place of the first 16 bytes of the ESP Padding (see 14.3.5.2); and
c) processing rules for the ESP Padding CRC (see 14.3.5.3).

ESP End-to-end Protection is defined for the End-to-end ESP_Header (see 14.3.2).

#### 14.3.5.2 ESP Padding CRC Placement

The format of the ESP Padding field when the ESP End-to-end protection feature is enabled is shown in table 57.

**Table 57 - ESP Padding field when ESP End-to-end protection enabled**

| Bits / Word | 31 .. 24 | 23 .. 16 | 15 .. 08 | 07 .. 00 |
|---|---|---|---|---|
| 0 | ESP Padding CRC | | | |
| .. | ESP Padding (0-252 bytes) | | | |
| P | | | Pad Length | Not meaningful |

**ESP Padding CRC:** When the ESP End-to-end protection feature is enabled, the ESP Padding CRC shall replace the first 16 bits of the ESP Padding field (see 14.3.5.3).

**ESP Padding:** If there are more than two ESP Padding bytes, this field shall be set as defined in RFC 4303. As specified by RFC 4303, an increasing count is placed in each byte of the ESP Padding. If there are any ESP Padding field bytes beyond two, the count shall start at 03h (i.e., the CRC replaces the first two bytes of the padding field which are defined to have the values 01h and 02h respectively).

**Pad Length**: The total length, in bytes, of the ESP Padding field including the ESP Padding CRC.

#### 14.3.5.3 ESP End-to-end protection processing

After building a frame for transmission, but before encrypting the data (see 14.3.2), the transmitting port shall:

1) Compute CRC, using the T10 Protection Information CRC (see SBC-5), covering:
   i) the Frame_Header, with the S_ID, D_ID, and CS_CTL/Priority fields set to zero for the purpose of the CRC computation;

ii) optional headers other than the ESP_Header, if present; and

iii) the Payload; and

2) place the computed CRC into the first 2 bytes of the ESP Padding field (see 14.3.5.2).

After decrypting the received data (see 14.3.2), the receiving port shall:

1) Compute CRC, using the T10 Protection Information CRC (see SBC-5), covering:

   i) the Frame_Header, with the S_ID, D_ID, and CS_CTL/Priority fields set to zero for the purpose of the CRC computation;

   ii) optional headers other than the ESP_Header, if present; and

   iii) the Payload; and

2) compare the CRC computed in 1) with the CRC received in the first 2 bytes of the ESP Padding field (see 14.3.5.2), if the values don't match an error should be indicated.

NOTE 29 - The mechanism by which a CRC mismatch is indicated is outside the scope of this standard.