

Clarification Request

References: 12.1.13 MS/TP Data Link Layer

Date of BTL-WG Response: 10-Oct-2018

☒ All Actions Necessitated have been Completed

Background:

There is currently no test for validation of an MS/TP packet w/out data.

Problem:

A BTL certified device is transmitting 2 extra bytes at the end of every MS/TP frame that it transmits. These bytes are transmitted after the HeaderCRC and are not preceded by the "sacrificial" 0xFF. See following export from Wireshark.

This packet is the first 8 bytes (token pass as an example):

No.	Time	Source	Destination	Protocol
81421	968.220391	0x08	0x12	BACnet
BACnet MS/TP Token				

Frame 81421: 8 bytes on wire (64 bits), 8 bytes captured (64 bits)

BACnet MS/TP, Src (8), Dst (18), Token

Preamble 55: 0x55

Preamble FF: 0xff

Frame Type: Token (0)

Destination Address: 18

Source Address: 8

Length: 0

Header CRC: 0xaf [correct]

[Checksum status: Good]

0000 55 ff 00 12 08 00 00 af

Uÿ.....-

These are the extra two bytes:

No.	Time	Source	Destination	Protocol
Length	Info			
81422	968.220417			2
[Malformed Packet]				

Frame 81422: 2 bytes on wire (16 bits), 2 bytes captured (16 bits)

[Malformed Packet: BACnet MS/TP]

[Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]

[Malformed Packet (Exception occurred)]

[Severity level: Error]

[Group: Malformed]

0000 01 20

If viewing this packet in a “non processing” analyzer, the packet looks as follows:

0000 55 ff 00 12 08 00 00 af 01 20

Question:

Should the testing organizations catch and flag this type of issue? If so, should this result in a test failure?

Response:

YES.

YES.