

**INTERPRETATION IC 135-2008-10 OF
ANSI/ASHRAE STANDARD 135-2008 BACnet® -
A Data Communication Protocol for Building
Automation and Control Networks**

Approval Date: October 28, 2010

Request from: Dean Matsen (dean.matsen@honeywell.com), Alerton Dealer Business
Honeywell Automation & Control Solutions, 6670 185th Ave. NE, Redmond, WA 98052.

Reference: This request for interpretation refers to the requirements presented in Addendum g to ANSI/ASHRAE Standard 135-2008, Section 24.16.1, relating to APDU and NPDU sizes.

Background: Section 24.16.1 (page 46 of Addendum g to 135-2008) lists some new APDU sizes that leave extra room for the security header. However, for whatever reason, different amounts of space for the security information appear to be assumed for each media without any explanation of justification as to why they are different.

The BACnet/Ethernet max APDU size has been reduced from 1476 to 1420. This seems to reserve 56 extra bytes for security overhead.

The MS/TP and PTP max APDU size has been reduced from 480 to 412. This seems to reserve 68 extra bytes for security overhead.

The BACnet/IP APDU size is left as-is, but the limit for the next lower layer has been raised from 1497 (I think) to 1562. This seems to reserve 65 extra bytes for security overhead.

The LonTalk max APDU has been reduced from 206 to 140. This seems to reserve 66 extra bytes for security overhead.

No rationale is given for the numbers 56, 65, 66, and 68, nor is any explanation given for why they are different for each media type.

This does not give a clear guideline for what max NPDU sizes to assume in order to support APDU sizes other than those shown in Table 24-28 (page 47 of Addendum g to 135-2008).

Interpretation No.1: Before security was proposed, the difference between max_APDU and max_NPDU was always 21 bytes (1476 vs. 1497 and 480 vs. 501). So this implies that 21 bytes should be reserved for the NPCI.

Question No.1: Is this interpretation correct?

Answer No.1: YES.

Interpretation No.2: The security overhead differs for each media type for some unstated reason. For BACnet/Ethernet, it is 56 bytes. For PTP and MS/TP, it is 68 bytes.

Question No.2: Is this interpretation correct?

Answer No.2: NO. See comments.

Interpretation No.3: When implementing BACnet/Ethernet with a maximum APDU limit of max_APDU, assume max_NPDU = max_APDU + 21 + 56 = max_APDU + 77

Question No.3: Is this interpretation correct?

Answer No.3: NO. See comments.

Interpretation No.4: When implementing MS/TP or PTP with maximum APDU limit of max_APDU, assume max_NPDU = max_APDU + 21 + 68 = max_APDU + 89

Question No.4: Is this interpretation correct?

Answer No.4: NO. See comments.

Comments:

The max APDU values in clause 24.16.1 are incorrectly calculated; they are based on an earlier draft of the addendum.

The max APDU values vary by datalink due to the requirement that the encrypted portion of the packet be a multiple of the encryption block size which in this case is 16 octets. To calculate the max secure APDU for a given max APDU size the following formula is used:

$$\text{max-secure-apdu} = \text{floor}((\text{max-apdu} - s1) / \text{bs}) * \text{bs} - s2$$

where:

max-apdu is the max-apdu size for a non-secured packet on the datalink

s1 is the number of octets of security information that is not encrypted and is 32

s2 is the number of octets of security information that is encrypted and is 27

bs is the size of the encryption algorithm's block size and is 16 for the encryption algorithms used by the current security addendum

This results in the following max-secure-apdu sizes for the current datalinks:

LON: 131
MS/TP: 419
PTP: 419
ARCNET: 419
Ethernet: 1411
ZigBee: 1411

The B/IP max-secure-apdu is not subject to these constraints and remains 1476.