INTERPRETATION IC 135-2008-22 OF
ANSI/ASHRAE STANDARD 135-2008 BACnet® -
A Data Communication Protocol for Building
Automation and Control Networks

Approval Date: 10/27/2011

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, Clauses 24.12.1, 24.13.6 and 24.15.2.1 (pages 39, 40, 44-46), relating to validation of time stamp and message ID routers.

Background: Clause 24.12.1 states "When routing messages without changing the security of the packet, a router may optionally validate the security protocol control octet, signature and timestamp, and verify uniqueness of the Message Id across the timestamp window."

Clause 24.13.6 states "Routers shall not validate the Timestamp of a message unless the router changes or removes the security wrapper of the message, or the router is the final destination for the message."

Clause 24.15.2.1 describes a method for creating pseudo-random and/or never previously used message IDs and it also describes sending Challenge-Request messages with an "all zeros" time stamp.

Clause 24.15.2.1 states "If the secure device does not have the current key set, the Challenge request will have to be aimed at the Key Server and use the device's Distribution or Device Master key"

This leads to the following issues:

1. Clauses 24.12.1 and 24.13.6 appear to contradict each other with regard to routers validating the time stamp (barring cases where the router is both the FINAL destination and the message is also to be routed, which would seem to be a separate contradiction).

2. If routers try to validate the message IDs of any messages generated as described in 24.15.2.1, their message ID tables will become cluttered with random-ish message IDs, whereas the validation mechanism is really only defined to work well with the normal message IDs (specifically, ones that increase monotonically). When the device does finally discover the correct time stamp, its ability to communicate could be affected by the cluttered message ID tables in the nearby routers.

3. In would seem very likely that in most installations, many devices would have to go through routers to communicate with the key server. If routers were to validate the time stamp and/or message ID, this would prevent the time stamp challenges described in 24.15.2.1 from being

successfully "aimed at" and actually reaching the key server, in the case where a device has no valid key set.

Interpretation No.1: Clause 24.12.1 is incorrect in saying a router may validate the time stamp when routing without changing security. At least in the case of a Challenge-Request message, it cannot validate the time stamp when routing without changing security.

Question No.1: Is this interpretation correct?

Answer No.1: No. Clause 24.13.6 is incorrect. Routers may optionally validate the timestamps of routed messages. But as noted, there are cases where the validation shall not be applied.

Interpretation No.2: Clause 24.12.1 is incorrect in saying a router may optionally validate the message ID when routing without changing security. At least in the case of a Challenge-Request messages, it cannot validate the message ID when routing without changing security.

Question No.2: Is this interpretation correct?

Answer No.2: No. Routers may optionally validate the Message Ids of routed messages. But as noted, there are cases where the validation shall not be applied.

Interpretation No.3: The challenge described in Clause 24.15.2.1 should be sent encrypted and with the "do-not-decrypt" and "do-not-unwrap" flags set, so that intermediate routers will not attempt to change the security of the message en route, consequently subjecting them to time stamp and/or message ID validation, and also cluttering up the message ID tables of the routers.

Question No.3: Is this interpretation correct?

Answer No.3: No.

Comments:

Note that the method which uses special message IDs described in 24.15.2.1 also mandates that the device wait 2 * Security_Time_Window which will result in the purging of past Message Ids in receiving devices. Thus the problem of “cluttering” will not occur.

In 24.15.2.1, the device that does not have a clock will generate a Challenge request with an all 0 timestamp. Routers shall not drop these requests due to a timestamp validation failure.

In clauses 24.15.2.1.1 and 24.15.2.1.2, it should be noted that the time to use in the Challenge request should be based on the time in the original message and not an all 0 time. These clauses should also note the need to wait 2 * Security_Time_Window or to remember the last used Message Id across a reset.