INTERPRETATION IC 135-2008-18 OF
ANSI/ASHRAE STANDARD 135-2008 BACnet® -
A Data Communication Protocol for Building
Automation and Control Networks

Approval Date: January 29, 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 24.2.8, 24.2.9, 24.3.7, 24.12.1, S.1 (pages 12, 29, 39, 98), relating to Security Applied to Request-Master-Key message.

Background: Consider an undeployed secure BACnet device having no keys and having a non-battery-backed RTC, and which is deployed on an encrypted network. Such a device starts out its life with no means to discover its time stamp or network number.

When such a device emits its Request-Master-Key request, the request would need to have a zero time stamp.

Clause 24.3.7 makes a provision for routers to allow routing this message even if it does not meet the local network policy.

Clauses 24.2.8 and 24.2.9 talk about allowing for the SNET to be zero.

Clause 24.12.1 allows a router to validate the source MAC, time stamp, and message ID of a message that is passing through.

Annex S, Clause S.1 seems to imply that a bad time stamp is a possibility here, but that's only informative.

The problem here is that some router vendor might decide to apply time stamp check (or perhaps other checks that are destined to fail) to the Request-Master-Key message, without realizing that is defeats the entire mechanism. This is apparently allowed by 24.12.1 (maybe even encouraged for the overachieving router vendor).

However, vendors of non-routing devices depend on the routers to support the mechanism correctly and consistently, as defined by the standard.

Interpretation No.1: A router should not apply any security checks to Request-Master-Key, but should rather just route it according to Clause 6. The easiest error to make here would be to try to validate the time stamp or SNET fields.

Question No.1: Is this interpretation correct?

Answer No.1: Yes.

Interpretation No.2: The only security a router applies to Request-Master-Key is to refuse to route it altogether, and only then if explicitly configured to do so (which must not be its default configuration).

Question No.2: Is this interpretation correct?

Answer No.2: Yes.

Interpretation No.3: A key server needs to accept a Request-Master-Key message with a bad (or zero) time stamp.

Question No.3: Is this interpretation correct?

Answer No.3: Yes.