PolarSoft® Inc.
914 South Aiken Ave
Pittsburgh PA 15232-2212
412-683-2018 voice
info@polarsoft.com
www.polarsoft.com

Source: **Brian Conroy on BACnet-L (9-Jun-2003)**

Question: *What is everyone's policy about responding to a BACnet service request from a device that we have not yet received an I-am from? Would we discard the request or fulfill it anyway?*

This brings up another question - how do you tell which device sent the request - in the case of bacnet4linux (using raw ethernet, no BACnet/IP) it says that if the SA in the MPDU matches an SA from an I-am request and the slen = 0 (therefore we are on the same BACnet network) or the SA in the MPDU matched an SA from an I-am request, and if the slen >0 the saddr in the request matches the saddr in the original I-am request and the snet matches the original snet, then we have seen this device before so it's ok to respond to the request.

Is the assumption that if the slen = 0 then the MAC in the MPDU must be actual MAC for the device and not a router a correct assumption - I'm not questioning bacnet4linux …just trying to clarify.

Also, how does this play out for BACnet/IP? Can we tell which device sent the request from the IP? what about cases when the requesting device is behind a router?

Answer: **David Fisher**

No question about it. You should answer every request, period.

As a server, in general you don't care about I-Ams. I-Ams are generated by servers to report their device instance, vendor ID etc.

The only reason for servers to track I-Ams is if they have also a client component, and you want to remember peer device bindings.

Just because you haven't heard an I-Am from a peer, doesn't mean they are illegitimate (and why would you care if they were, and why does sending an I-Am make them legitimate?).

There are lots of reasons why a client/server device might not have sent an I-Am prior to trying to talk to your device:

1. He wants to find out something from you, but no one has yet asked him Who-Is
2. He has replied to a Who-Is, but you never saw his I-Am because: it got lost due to collisions or router congestion, or it hasn't yet made it to you because of routing, or your device missed it because you were too busy, out of buffer space etc.

I could go on...

Anyway, the short version is: always answer requests targeted to you.

> how do you tell which device sent the request

You can't and there is generally no reason to care.

QUESTION

If you must know, there are only two cases:

1. The client is on the same BACnet network segment that you are, this is known if the network layer header has the bit 3==0 in the NPCI. In this case the source MAC address is the client address.
2. The client is on another network segment. This is the case when the bit 3 of NPCI==1. In this case then SNET field is present and tells you the client's BACnet network number and the SADR is the client's MAC address. SLEN would never be zero in this scenario.

A MAC address is just a byte array that is SLEN long.

This is consistent across all BACnet MAC layers including BACnet/IP.

So your BACnet application layer doesn't really know or care about the kind of MAC media the client uses. You identify the client as a 16 bit network number (0=local) and SLEN length MAC address.

> Also, how does this play out for BACnet/IP? can we tell which device sent the request from the IP? What about cases when the requesting device is behind a router?

The same concepts apply to BACnet/IP. In this MAC, the "MAC address" is 6 bytes, the first 4 of which are the IP address and the last 2 are the UDP port number (big endian). Usually the UDP port number is 0xBAC0 but can be other numbers in some circumstances.

