Harder, Better, Faster, Stronger*

Improving BACnet® MS/TP

By Steve Karg, Member ASHRAE

More BACnet MS/TP devices probably are installed than any other kind, considering that MS/TP is used in small, inexpensive devices that are plentiful in buildings. In the last several years, changes to the BACnet standard have made this popular field bus even more robust.

A Slave-Proxy was added to free the MS/TP slaves and reduce site configuration. Some benign quirks in the state machine were corrected. Speed enhancements were made with the addition of two standard baud rates (57600 bps and 115200 bps). An addendum full of wiring diagrams, and details about proper isolation, grounding, and reference connections for nearly any type of installation was added in 2010. The MS/TP working group is exploring standard ways to automatically address MS/TP devices.

MS/TP Overview

BACnet MS/TP is a data link protocol unique to BACnet that is commonly used as a field bus. The acronym MS/TP stands for Master-Slave/Token-Passing. The protocol uses EIA-485 as the physical layer. The protocol is defined using three state machines: Master Node Finite State Machine, Slave Node Finite State Machine, and Receive Frame Finite State Machine. A device is either a Master Node or a Slave Node.

MS/TP Master Nodes are similar to those of other peer-to-peer protocols. At power up, each Master Node waits for its timeslot (based on the Medium Access Control [MAC] address range of 0–127) to begin searching for peers. When a peer is found, the token is passed to the peer, and that peer begins looking for its peer. Once a node has its peer identified, it participates in Token passing and only searches for a peer every 50 Token passes, and only if there are gaps in the MAC addresses between the nodes. If a Master Node receives a token, it can send one or more frames (defined by Max_Info_Frames).

A Slave Node (MAC address range of 0–254) simply waits for a Master Node to query it using a "Data Expecting Reply" message, and it responds. It does not participate in the Token passing. A Slave Node can also receive "Data Not Expecting Reply" frames, such as a Broadcast TimeSynchronization service, but cannot send any messages on its own.

Work it Harder

Because a Slave Node does not receive a Token, it does not respond to a Who-Is service request with an I-Am, and is unable to participate in dynamic device binding (discovering a device based on its Device instance number). Addendum 135-2001a added the capability to issue I-Am responses on behalf of MS/TP slave devices.

Automatic Slave detection is accomplished by a proxy device using ReadProperty or ReadPropertyMultiple services to read the Device object's Protocol_Services_Supported property of the slave to see if it supports execution of the Who-Is service. The proxy device reads using the special wildcard device

About the Author

Steve Karg is a senior engineer at Watt Stopper, in Birmingham, Ala. He has been an active member of the BACnet standards committee since 2001, and convenes its Lighting Applications working group. He wrote the open source BACnet Protocol Stack hosted on SourceForge.net, and continues to help maintain the BACnet decoder in Wireshark.

* "Harder, Better, Faster, Stronger" is a song by French duo Daft Punk.

object instance of 4194303, which is treated as if the Object Identifier correctly matched the local Device object of the slave. If the slave device does not support the execution of the Who-Is service, then it is added to a list in the proxy device. Manual Slave address binding is also supported with the addition of a new List property, Manual_Slave_Address_Binding, for Slave devices that do not support the special object instance of 4194303.

If the Slave proxy device receives a Who-Is request, it will respond with an I-Am for each of the slave devices on the MS/TP network that it has listed, and that match the device range parameters.

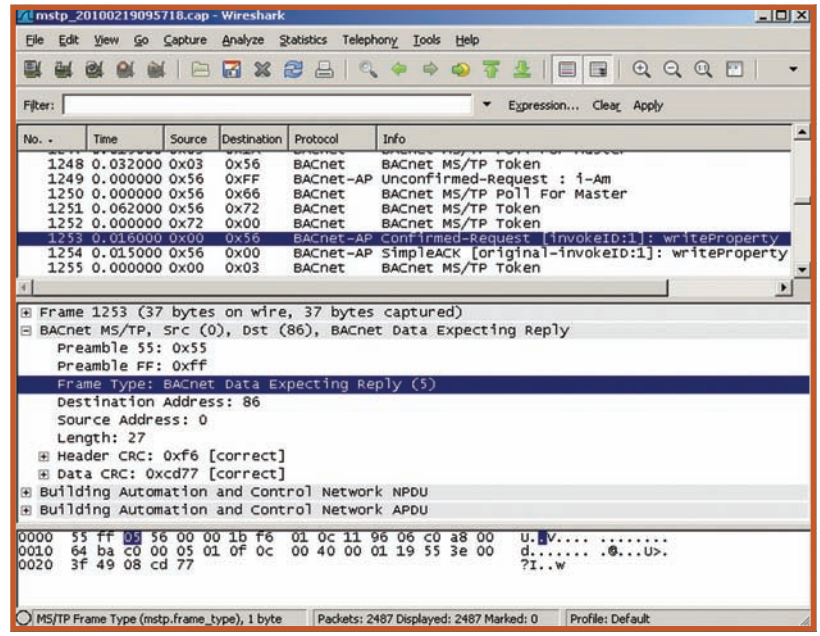

Figure 1: A protocol analyzer displays a BACnet MS/TP frame in all its gory detail.

Make it Better

Occasionally, there is an ambiguity in the language of the BACnet standard, and someone will ask for an interpretation of the language. The resulting Interpretation Request is reviewed by the BACnet committee (SSPC 135), and the language is then clarified in subsequent releases of the standard. Addendum 135-2004b-9 is such a case, and it permits MS/TP "Data Expecting Reply" frames to be broadcast when they were originally considered an invalid frame. This adds consistency with the other data link layers since the network layer allows a device to broadcast on its local LAN a message to be routed to a device on some other network.

Sometimes a small anomaly is noticed in an MS/TP state machine, where some condition occurs that was not accounted for the in the original design. Although there are no visible changes on the MS/TP wire, one subtle error was found and corrected in Addendum 135-2004d-8. The MS/TP Master Node State Machine handling of the variable EventCount could cause unnecessary transitions between the IDLE and NO_TOKEN states if there was no Token.

Another Master Node state machine error was discovered in a real-world installation when a node received an unexpected frame under certain conditions. In that rare situation, an MS/TP Master Node would send a Token addressed to itself. As a result, the Token was dropped and was re-generated after a short delay. Addendum 135-2008v-1 fixes the TokenCount value to prevent this from occurring.

The Receive Frame state machine was designed to be very efficient, and discarded frames that were not addressed to itself without needing to fully process them. However, if such discarded frames contained data that indicated the start of a new frame, the Receive Frame state machine would begin processing as if another frame was being received. This new frame would eventually be deemed invalid since the CRC (checksum) would fail or the frame would time out. In some cases, the subsequent frame would be lost. After several attempts to fix the problem, the MS/TP working group finally proposed Addendum 135-2008z-3 to modify the MS/TP Receive State Machine so that it will consistently ignore data that is not addressed to itself. This addendum is undergoing public review.

Do it Faster

Addendum 135-2008ab-1 added new standard baud rates of 57600 bps and 115200 bps. Those values were chosen since they are common standard baud rates on personal computers. Concern about the reduced maximum distance of 3,280 ft (1000 m) when running the 115200 bps baud rate (3,937 ft [1200 m] for all other standard baud rates) had the proposal delayed for some time, but consensus won out. The addendum also requires that the 38400 bps baud rate be implemented in all MS/TP devices in addition to the 9600 bps currently required by the standard. Baud rates 19200, 57600, 76800, and 115200 remain optional.

Makes Us Stronger

For many years, there has been debate about how to wire an MS/TP network. Installers would ask, "Should we use two wire or three wire, or two wire and a shield?" 2010 brought an addendum full of guidance that defined deployment options for MS/TP. The rational from the addendum sums things up:

Although EIA-485 practice allows for a third wire to connect transceiver common or reference points together so the receiver common mode rejection voltage limit is not exceeded, the BACnet specification in Clause "9.2.1 Medium" only mentions "shielded, twisted-pair cable."

Due to electrical noise issues, some hardware applications cannot successfully communicate over EIA-485 without a remote common or reference connection and internal isolation. This has been particularly noticed in variable speed drive controllers that can produce local ground noise in excess of the EIA-485 common mode voltage limit.

BACnet MS/TP also requires 1500 volt isolation when crossing buildings, but does not specify any mechanism for doing this.

This proposed change is designed to describe wiring topologies for a reference wire in EIA-485 and to specify

acceptable topologies for interoperable connections for both single-building and multiple-building installations.

Addendum 135-2008y is filled with wiring diagrams, and details about the proper isolation, grounding, and reference connections for just about any type of installation.

Our Work is Never Over

The MS/TP MAC address range is limited from 0 to 254, and is often configured with a DIP switch, jumper links, LCD screen, or configuration tool. To reduce product costs and to provide easy, no-configuration installation, the MS/TP working group has been exploring standard methods to automatically configure the MS/TP MAC address.

One proposed method uses a master device with a fixed MAC address (usually a router) to assign the MAC address for certain MS/TP devices on a single MS/TP segment (similar to the Dynamic Host Configuration Protocol [DHCP]). Another proposed method uses a broadcast message that includes a vendor identifier and a serial number to simply assign the MAC address to a specific device. A third method, that has been discussed, has an MS/TP device monitor the "Poll For Master" frames on the wire to find an unused MAC address, which it uses after verifying that the address is unused (aka zero configuration networking).

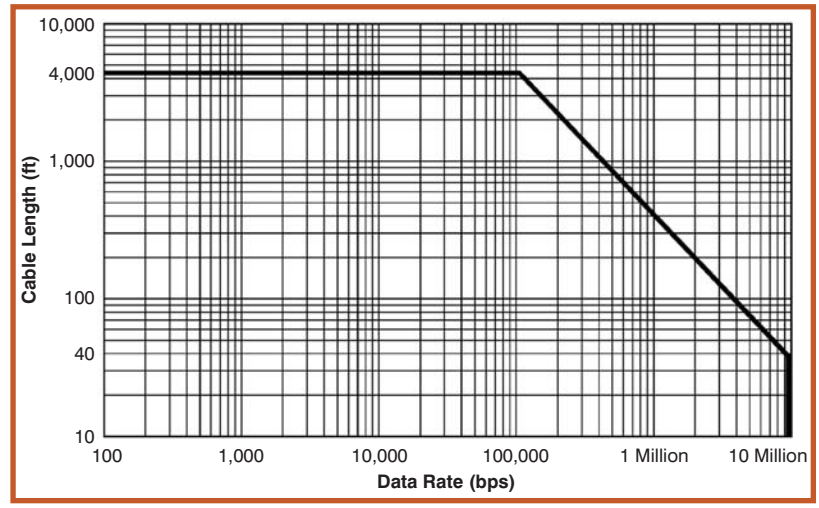

Figure 2: A graph depicting cable length and data rate of RS-485. Source: National Instruments Application Note 1057 "Ten Ways to Bulletproof RS-485 Interfaces."

With improvements in speed, robustness, ease of use, and deployment specifications, and new features on the way, MS/TP is a robust, living, and adapting protocol.