LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-JRNL-673285

The BACnet Campus Challenge - Part 2

K. Masica

June 16, 2015

The BACnet Campus Challenge # Part 2

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

The BACnet Campus Challenge – Part 2

< By Ken Masica / Version 2 / June 30th 2015 >

INTRODUCTION: Four Challenges Down, Four to Go

The first part of this two-part article described both the benefits and the challenges of implementing BACnet in large campus environments. Adopting native BACnet as a primary design requirement can be a key strategy in achieving an interoperable and flexible multi-vendor building automation system (BAS) that can scale to large campus installations, integrate with modern campus networking infrastructures, and address legacy equipment issues that can occur when DDC upgrades are done by different contractors using various equipment vendors over different time frames. Inherent in such an approach, however, are certain challenges that include understanding the BACnet protocol model that is based on defined objects, devices, and networks. Part one of the this two-part article explained the BACnet object model so that large system designers can develop object naming conventions and device and network numbering plans so that building automation implementations can scale to large campus or multi-campus environments.

In the second part of this two-part article, the additional challenges of providing BACnet campus connectivity, protecting the BACnet network traffic, and controlling the resulting broadcast traffic will be addressed. The final challenge will be an example BACnet implementation that unifies the concepts presented in both articles.

FIFTH CHALLENGE: Provide BACnet Network Connectivity

Large modern, multi-building campuses will likely already have a data network infrastructure (cabling, switching, and routing equipment) deployed that serves the various IT needs of the institution. A key initial decision in deploying, expanding, or modernizing a campus building automation system will therefore be deciding the degree to which the automation system will use the existing data communications infrastructure to provide the required connectivity between the components of the BAS (automation server, controllers, fieldbus networks, operator workstations, etc.) and the BACnet traffic that is generated. Careful consideration and recognition should be given to the fact that an automation system has different performance, reliability, and security requirements than typical IT systems and applications will have. Both automation systems and IT systems now have many commercial-off-the-shelf (COTS) technologies in common such as ethernet switches, IP routers, workstations for operator HMI access, database software that stores trend/alarm/audit data, and servers that run automation software and supporting engineering tools. However, the approach to designing, implementing, and managing an automation system should be based on system performance requirements in order to maintain operational stability and availability, with particular attention devoted to the area of change control, testing, and configuration management of the BAS components. Therefore, the degree of integration of the building automation system with the campus data network infrastructure should take into account these factors during system design and operation.

Three general approaches to consider regarding BACnet network connectivity across a large campus environment are:

1) *Create a separate building automation network including dedicated cabling, Ethernet switching, and IP routing equipment*.

   This is considered a "Layer-1" solution because it requires rnning separate physical cabling to the automation system components, and cabling in a network corresponds to the Physical Layer (Layer-1) in the ISO 7-layer networking model. It is the most secure approach to providing automation system connectivity and performance but is also the most costly, especially for large campuses because it also involves installing dedicated Ethernet switches and IP routers to provide the required BACnet connectivity between automation system components such as the controllers, automation software server, and operator workstations. Therefore, pursuing a Layer-1 solution will depend on size, cost, and future expansion trade-offs against the strongest security and best performance for the BACnet network. For campuses that have a distributed fiber backbone, a potential cost-saving measure is to use Wave Division Multiplexing (WDM) equipment on existing fiber pairs going to each building to allocate a portion of the bandwidth of those used fibers to the automation system if unused fiber availability is an issue.

2) *Integrate with the existing campus data network infrastructure and utilize the existing cabling, Ethernet switching, and IP routing equipment for BACnet connectivity*.

   This approach is potentially the least costly for a large campus because it utilizes the existing data network infrastructure on the campus. Factors such as the security, performance, and reliability of the current data infrastructure should be considered with this approach.

3) *Develop a hybrid approach that utilizes the existing network infrastructure for some aspects of automation system connectivity and dedicated equipment for other aspects*.

   This approach provides a trade-off between cost and security/performance requirements for providing BACnet connectivity across a large campus. Depending on the size and system architecture of the BAS as well as the security and performance requirements, it may be possible to use dedicated equipment and connectivity of the more critical components (e.g. the controllers and field bus networks in each building) and shared data infrastructure with Layer-2 or Layer-3 isolation for other components such as operator workstations and database servers.

Campus environments will vary based on their size, number of buildings, existing cabling and networking infrastructure, and current performance and security capabilities. Each of the BAS integration options described above should therefore be evaluated based on the size, cost, security, performance, and reliability requirements of the building automation system.

SIXTH CHALLENGE: Protect BACnet Traffic

A comprehensive approach to BAS security involves developing policies and procedures that should be applied systematically to all components, users, and contractors of the system based on a risk assessment and mitigation process. In keeping with the theme of this series of articles,

security will be addressed as it pertains to BACnet networks on large campuses. Different approaches will be listed to give the reader an idea of the security options that exist for securing automation networks. Customer implementations will vary by the size of the automation system, existing network and security infrastructure on the campus, and organizational security policies. Ideally, the organization will have a security plan that outlines the policies and procedures that govern the operational security of the BAS and identifies the network security measures implemented.

Listed below are some options for protecting BAS components and the BACnet traffic that is generated. The most appropriate option will depend on the degree to which the BAS is integrated with the campus data network infrastructure as described in the previous section as well as the existing security, performance, and reliability of the current network. Additionally, organizational security requirements and the automation system performance and reliability requirements will be factors.

1) *Use VLANs and VACLs to protect the automation netw*ork.

   This is considered a Layer-2 solution because it involves creating a logically separate network over shared physical cabling for the automation system traffic among the Ethernet switches that comprise the campus network. (Ethernet corresponds to Layer-2 in the ISO 7-Layer Networking Model.) The protection of the BACnet traffic in this case is achieved by logically separating it from other traffic flowing on the campus data network infrastructure. Unlike a Layer-1 solution, shared cabling is used. VLAN technology is a standard feature in most campus Ethernet switches so implementation does not typically require new equipment but does require configuration of the switches and configuration of VLAN trunks between IP routers that comprise the campus backbone network. VLAN isolation of the automation system is a cost effective option, especially for a campus that already has a VLAN infrastructure in place. The BACnet traffic is not encrypted, but it is logically isolated and can be prevented from being routed to the other campus subnets. VLAN Access Control Lists (VACLs) can also be used as an enhanced security measures to specify and limit the types of traffic that can propagate over the VLAN.

2) Use *VPN tunnel encryption to protect the automation network*.

   This is considered a Layer-3 solution because it involves creating encrypted tunnels at the IP layer. (IP corresponds to Layer-3 in the ISO 7-Layer Networking Model.) The automation system traffic is combined with the other campus network traffic, but because traffic is encrypted, it is protected as it moves across the campus network. Although very secure, VPNs can be complex to implement and maintain, and unless the VPN traffic is prioritized across the backbone router infrastructure, it will be combined with all the other campus traffic so automation system performance might be an issue. Also, establishing encrypted tunnels to each BACnet router of the automation system may require additional equipment such as VPN appliances since BACnet routers do not typically support VPN features.

3) *Use firewalls to protect the automation network*.

   This is considered a Layer-3/Layer-4 solution because it involves filtering network traffic based on the source and destination IP address (Layer-3) as well as filtering on the protocol or service port of the inbound and outbound traffic (Port numbers are specified in the TCP and UDP headers which correspond to Layer-4 in the ISO 7-Layer Networking Model.) Firewalls have an effective and singular purpose to protect the devices behind them from all other traffic

on the campus except the protocols required, which is BACnet in this case. Firewalls are a common security technology and can be a cost effective solution to isolate the automation system. Firewalls packaged in DIN rail enclosures and designed specifically for industrial control systems are available on the market and therefore can be included inside a DDC panel as part of a standard campus automation system implementation. Note, however, that firewalls will perform a filtering function but unless a campus traffic priority scheme is used, the automation traffic will be mixed with the other campus traffic so performance might be an issue depending on channel utilization and available bandwidth.

As noted, the approach to securing the BACnet traffic of the building automation system will vary by the size, budget, existing infrastructure, and site security plan of the organization. Using dedicated cabling is the most secure approach but also the most costly. VLAN separation can be a cost-effective approach for most campus installations, whereas VPN encryption is very secure but can be costly to maintain and suffer from performance issues. Firewalls are a common security technology and can be used to protect the automation system from other campus traffic and also be used as an additional security measure even when VLAN, VPN, or dedicated cabling is utilized.

SEVENTH CHALLENGE: Control BACnet Traffic

As explained previously, BACnet devices must have unique ID's across the entire campus installation. A structured BACnet numbering plan is the most effective way to ensure assignments are unique and avoid conflicts. When two BACnet devices within the same BACnet network need to communicate with each other over the field bus network (e.g. MS/TP, ARCNET, etc.) that interconnects them, the communication will be directly between the devices without the need for a BACnet router to relay the packets to another BACnet network elsewhere on the campus. However, when two devices are located on different BACnet networks on campus, the BACnet routers front-ending each BACnet network must be used to relay the BACnet traffic between the devices as explained in the first part of this article published previously. If the BACnet networks are located within the same IP subnet (LAN), then the BACnet routers will be within the same Ethernet broadcast domain and can perform initial discovery and communication directly using the Ethernet switches that interconnect them. An example of a simple, single Ethernet IP Subnet BAS is shown below in Figure-1 and might be representative of a relatively small installation or an implementation that uses a dedicated network infrastructure or VLAN for the building automation system. In this case, the single LAN architecture uses Ethernet switches to interconnect two buildings that each have a BACnet network installed and also interconnect the other BAS components such as the automation server and operator workstations. The BACnet routers will each have a unique IP address within the same subnet so they can communicate with each other and with the other BAS components in the automation system over a switched Ethernet LAN network infrastructure.

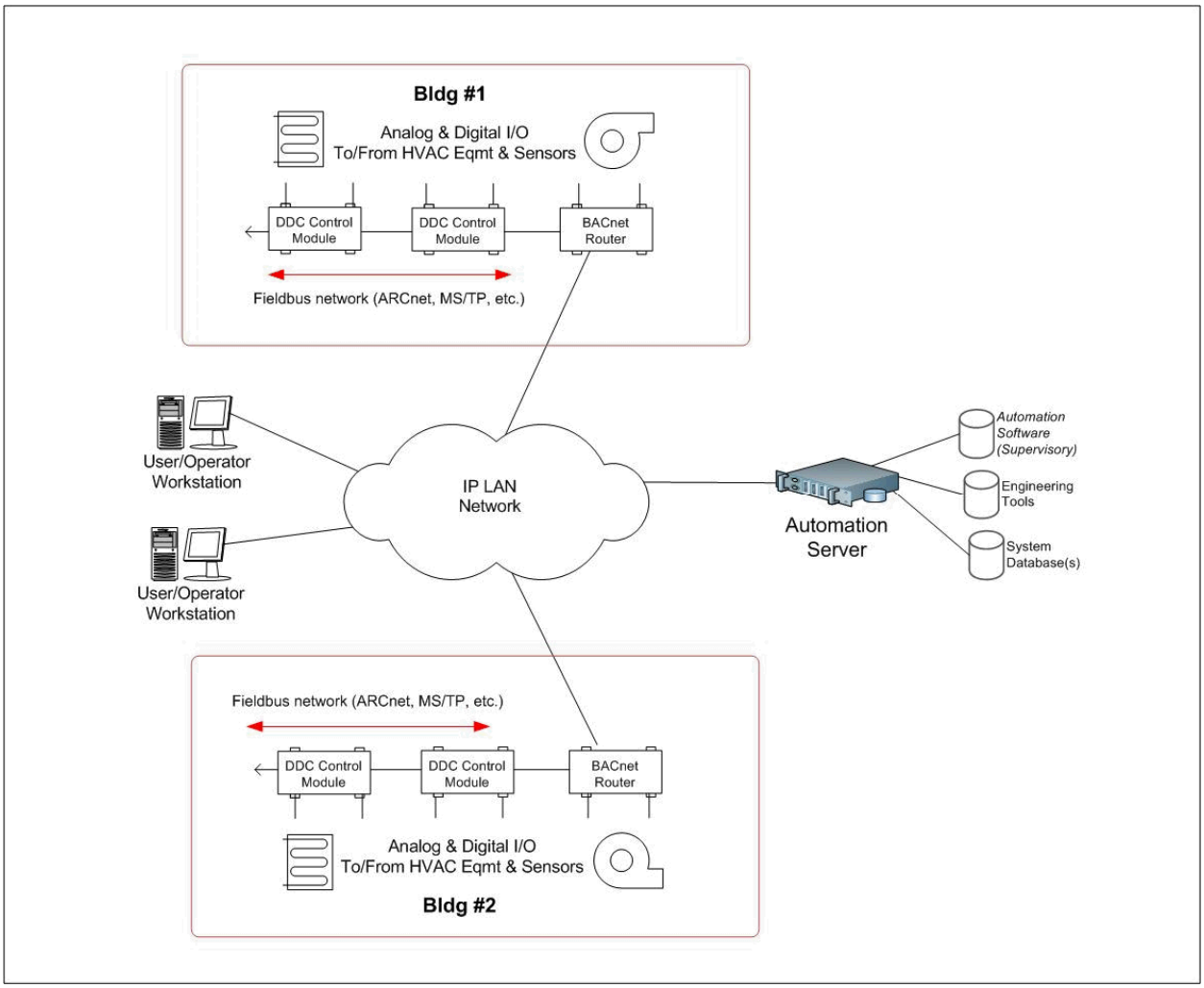

Figure-1: Example building automation system architecture on a single IP Subnet LAN or VLAN.

In contrast to a single physical LAN or logical VLAN implementation, when BACnet networks are located in different IP subnets on a campus IP network (which is typical in large campus implementations), there are additional measures that must be taken in order for the BACnet traffic to be sent between the BACnet routers located on different IP subnets. Note the distinction between BACnet networks and IP networks, which are different types of networks that must co-exist on same network infrastructure. BACnet networks that span different IP subnets will need to use the *BACnet/IP Broadcast Management Device* (BBMD) function within their local BACnet router in order to exchange their broadcast data. This is because IP routers will not forward the Ethernet broadcast traffic generated by a BACnet router during the initial device discovery phase. Instead, the BACnet router must know the IP addresses of one BACnet router in each IP subnet deployed across the campus and send unicast IP packets directly to them across the campus backbone network that interconnects the IP subnets. A *Broadcast Distribution Table*, also referred to as a BBMD table, is used by each BACnet router to record the IP address of the other BACnet routers deployed across the campus. The BBMD functionality described above is most often offered as a feature of BACnet routers, so it usually does not involve the installation of a separate device. Figure-2 below shows a basic example of a BAS that has a BACnet network implemented in two different buildings on campus, with each BACnet network being in a different IP subnet and interconnected through the routed campus backbone network.

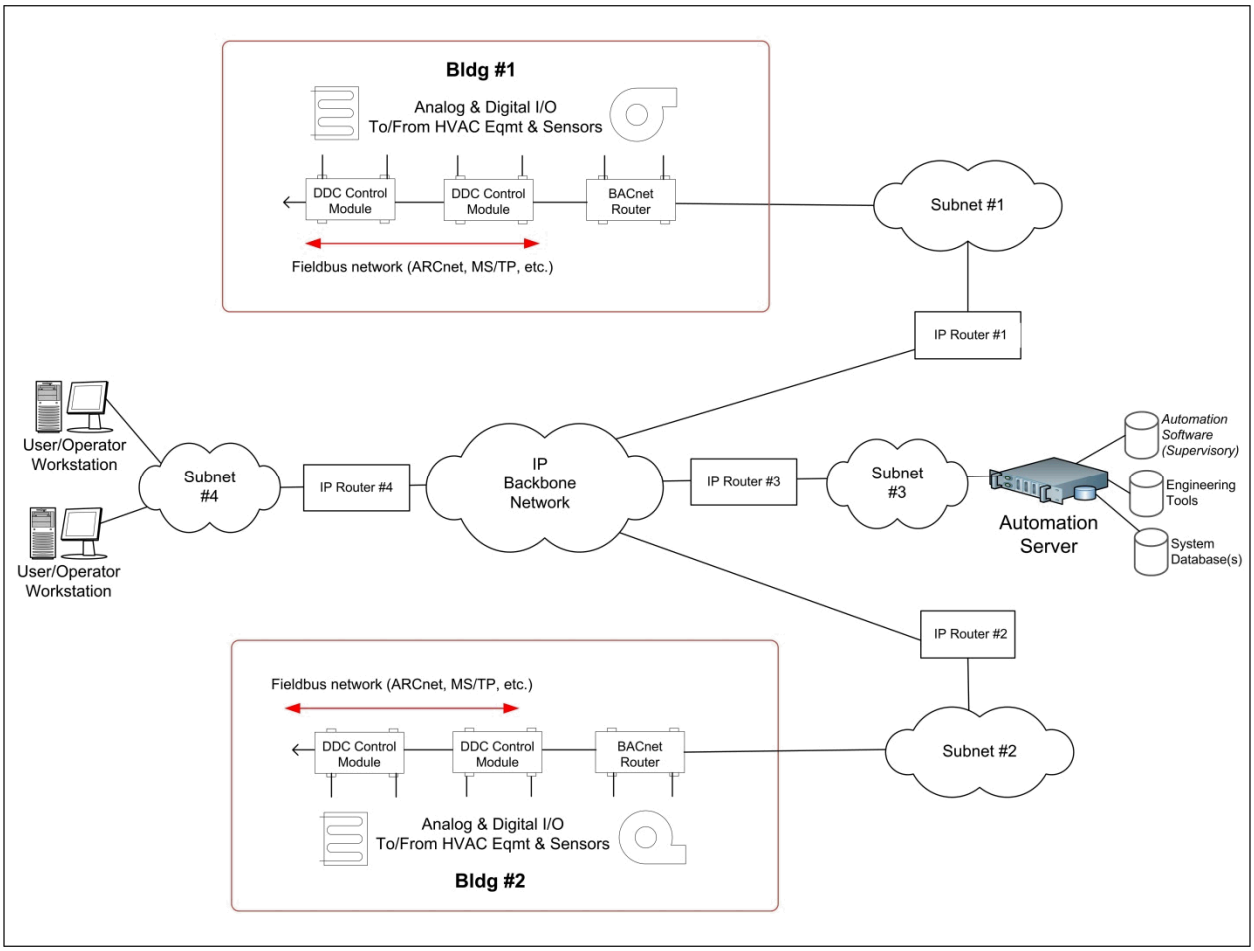

Figure-2: Example campus building automation system architecture using IP Subnets.

As described previously in the BACnet connectivity section, the IP backbone network can be a dedicated or hybrid infrastructure or utilize the existing campus network infrastructure with additional measures to isolate and protect it. In the example above, there is a BACnet network created in each of the buildings by interconnecting the BACnet controllers using one or more of the supported Layer-2 field bus network technologies supported by the BACnet standard (MS/TP, ARCNET, LonTalk, PTP, Ethernet.). Devices within each of the two BACnet networks can communicate with each other directly using their field bus network. However, when a BACnet device in Building #1 needs to send a broadcast that will be received by all BACnet devices in Build #2, the BBMD function in its local BACnet router will forward the BACnet data by encapsulating it as the payload inside a unicast IP packet that it sends directly to the IP address of the Build #2 BACnet router contained in its BBMD table. In this simple two subnet example, the BBMD table in each BACnet router would have the values shown in Table-1 provide below.

BACnet Network Number	BACnet Router Address
1	Router #1 IP Address
2	Router #2 IP Address

Table-1: BBMD table values for an example two subnet building automation system .

In contrast to this simple example, large campus implementations will typically have a large number of buildings with one or more BACnet networks implemented within them and that will also likely be located in different IP subnets. The BACnet Routers deployed across the campus

will have BBMD tables that contain the IP addresses of the other BACnet Routers to enable communication between them.
An aspect of effective BACnet network planning for large campus implementations is to understand what BACnet traffic must propagate across the campus backbone between subnets. The number and type of inter-building BACnet network points will vary by campus. For example, a centralized source for outside air temperature (OAT) and humidity (OAH) that is used by other controllers within the campus BACnet system will require that BBMD tables are properly configured in each BACnet router that has devices in its BACnet network that need to discover and query the BACnet device containing the these objects if that device resides in a BACnet network located on a different subnet within the campus.

EIGHTH CHALLENGE: Implement BACnet

At the start of a large multi-building DDC upgrade project performed at LLNL, a decision was made to use a centralized source for OAT and OAH to achieve consistent and accurate readings across the campus. LLNL owns and operates a campus Meteorological (Met) Tower that provides weather and environmental data to researchers as well other operational support programs. (See photo to the right.) Two of the Met Tower suite of sensors were used to provide the outside air temperature (OAT) and outside air humidity (OAH) point values that were then used in building control programs that implemented energy savings strategies based on economizer operation that used outside air directly to meet cooling demand under the right conditions. By using outside air directly for space cooling, less energy is used in chiller operation since the chilled water demand is reduced during economizer operation. Because of the interoperability, scalability, and communications features of the BACnet protocol, a multi-vendor solution based on BACnet that used existing infrastructure and scaled across the LLNL campus was possible.

The first step in the BACnet implementation was to install a BACnet gateway device in the Met Tower that could integrate with the existing high accuracy temperature and humidity sensors and convert the sampled analog values to BACnet objects available to the campus DDC system. Because of the vendor interoperability provided by the BACnet standard, the vendor of the BACnet gateway device used in the Met Tower was different from the vendor of the DDC controllers used in the buildings that were reading the OAT and OAH values. The Met Tower temperature and humidity sensor outputs were wired directly to the analog inputs of the BACnet device and then the device was configured to scale the sensor voltage ranges (0 VDC to +1 VDC in this case) to the temperature range of the OAT sensor (-40F to + 140F) and the humidity range of the OAH sensor (0% to 99%). The IP protocol parameters were then configured, including the device address, default gateway address, and the subnet mask. The BACnet parameters were then configured, including the BACnet Device ID, BACnet Object Names, BACnet Properties such as

Units, BACnet COV increment value, and the BBMD entry used for device registration with the BACnet network in the building on campus that is physically closest to the Met Tower. Once configured, the Met Tower BACnet device would continuously sample the temperature and humidity sensor analog voltage values, perform an analog-to-digital conversion, translate the digital values to decimal values based on the scaling range, and then package the decimal values into BACnet objects. The OAT and OAH BACnet objects could then be made available as network analog points and serve as inputs to the control logic running in the DDC controllers in the buildings where economizer operation was enabled.

Once the Met Tower was outfitted with a configured BACnet/IP gateway device and protected with a firewall appliance, the next step in the implementation process was to ensure it could communicate across with the BACnet controllers in the other buildings. One BACnet controller was designated to poll the Met Tower to retrieve the OAT and OAH values and make them available as COV subscriptions to the other controllers within the BACnet system. This approach was taken to prevent each building on site from querying the Met Tower directly and creating a potential bandwidth issue because of the low speed circuit used to communicate with the isolated MET tower location. BBMD table entries that included the IP address of the designated polling controller were then created for the BACnet gateway devices in each building that had economizer operation enabled and that were located in different subnets.

The final step in the implementation process was to configure the BACnet query string in the designated controller so that it could read the OAT and OAH analog point values in the Met Tower BACnet device. The vendor of the designated controller in this case uses a URL format to reference the Met Tower BACnet device and objects within that device. Shown below are the BACnet address strings used in the polling controller to query the Met Tower device and obtain the OAT and OAH readings:

```
bacnet://Met_Tower_Device_ID/ai:2/Present_Value    # For the temperature sensor
bacnet://Met_Tower_Device_ID/ai:3/Present_Value    # For the humidity sensor
```

The first part of the address identifies the protocol as BACnet. The second part of the address ("Met_Tower_Device_ID") is the BACnet Device ID assigned to the Met Tower BACnet device. (The actual assigned values are omitted in the example above.) The "ai" in the address strings above represent the standard BACnet object type for an *analog-input*, and the numbers that follow are the instance number of that object type. They refer to the physical analog input ports on the Met Tower BACnet device since the temperature sensor connects to physical port #2 and the humidity sensor connects to physical port #3. The last part of the address string represents the property of the object that is being read, which in this case is simply the present value of the ai:2 and ai:3 objects which correspond to the temperature and humidity readings from the connected sensors respectively. Note that more descriptive BACnet object names can be used in place of the "ai:2" and "ai3" such as Met-OAT and Met-OAH but for this example the type/instance format is described.

Once the Met Tower sensors connected to a BACnet gateway device that could create OAT and OAH objects and the BACnet controllers in the other buildings on the campus could receive those values, a scalable and multi-vendor interoperable implementation based on BACnet was achieved.

CONCLUSION

As explained in the first part of this two part article, understanding the BACnet protocol object model enables campus building automation designers to develop naming conventions for BACnet devices and their associated properties as well as develop numbering conventions for BACnet networks that can scale to large campus environments. The second part of this article has explored issues related to how the existing campus network infrastructure can be used to provide BACnet Network connectivity as well as methods for protecting BACnet traffic and controlling and directing broadcasts across the campus implementation.

BIBLIOGRAPHY

- ANSI/ASHRAE Standard 135-2012, *BACnet: A Data Communication Protocol for Building Automation and Control Networks*

Prepared by LLNL under Contract DE-AC52-07NA27344