Photo credit: Jason Koski (Cornell University Photography).

The initiative to develop a communication standard for building automation within ASHRAE began at Cornell University in Ithaca, N.Y.

BACnet® at Cornell

By H. Michael Newman, Fellow ASHRAE

The story of BACnet at Cornell University really begins with the story of BACnet itself. As you may know, the initiative to develop a communication standard for building automation within ASHRAE began here. This is how it happened.

It was the early 1980s and building controls manufacturers had discovered the power of microprocessors and computer networking. At Cornell, we had invested in a central, electromechanical control system that dated back to the mid-60s. The system was installed along with a district chilled water system that initially served a single new high-tech science building. In the mid-70s, as a direct result of the Arab oil embargo and the resulting cry for energy conservation, a small, diskless IBM System/7 minicomputer was interfaced to the electromechanical system. The minicomputer could measure electrical load and perform load shedding and time-of-day start/stop of a limited set of building equipment. This system was called our energy management and control system or EMCS. Not long after, a newer, more powerful minicomputer replaced the diskless machine. To place the new machine into perspective, it had a whopping 128 kilobytes of RAM and 5 megabytes of disk storage. In comparison, my current desktop PC has about 30,000 times more of both. The advantage of the new machine was that it could digitally communicate using “high-speed” 1,200 bits-per-second modems over dedicated copper wiring. This allowed us to read field sensor values with previously unattainable accuracy.

Meanwhile, our primary controls vendor wanted us to buy into the concept of direct digital control (DDC). When we asked them if we could use our existing minicomputer as a head-end to oversee

About the Author

H. Michael Newman is manager of the Utilities and Energy Management Department’s Computer Section at Cornell University in Ithaca, N.Y.

the DDC computers in the field, they insisted we purchase a new computer from them to provide such supervisory control. This made no sense to us. We already had a perfectly good computer that communicated with the original electromechanical system, as well as a growing number of field equipment multiplexers through the modem links, which was something their computer could not do. We told them that if we were going to buy their fancy new DDC controllers, we wanted to use our existing computer and write our own software to accomplish the interface; all we needed from them was the communication protocol—the set of rules that described how their DDC equipment communicated. After considerable back and forth, under cover of darkness, in a brown paper bag, the protocol specification arrived at the door. The controls vendor had never imagined that an owner actually would want to write his own communication driver to talk with their controllers and they were concerned about the dire consequences to our buildings if we messed up. However, we pushed on and soon the System/7 was happily talking with the new DDC computers.

At that point, the die had effectively been cast. Cornell had a multiprotocol computer that made use, simultaneously, of three separate communication languages.

Sixteen computers and 12 display screens provide the operators of Cornell's EMCS Operations Center flexible access to all campus systems.

The cost, however, was great. If you were fortunate enough to have the programming resources, you could "roll your own" as we had done. If not, you could buy a head-end computer from the manufacturer. Either way, you ended up with an ongoing maintenance situation because any change to the protocol necessitated programming work or the purchase of software updates for the vendor's computer. Expansion was highly constrained since equipment from a different vendor either required more programming or the purchase of a new computer. It was as if every TV channel required you to buy a TV just to watch that channel. An absurd situation!

With the realization that all the controls vendors were implementing basically the same type of networking, but all were doing it slightly differently, the frustration in the trenches became intolerable. Interoperability was all but impossible. A standard was desperately needed!

One day I was discussing this unfortunate situation with my director. He suggested that if anyone were working on the problem, it would be ASHRAE. At the time, I must confess, I had never heard of the society, having studied physics and astronomy in college. In January 1981, I dutifully headed off to my first ASHRAE meeting, in sunny Chicago, to see what ASHRAE was doing about this problem. To me, the lack of any network standardization had to be the biggest problem facing the building controls industry and surely was holding back the acceptance of this new and exciting DDC technology. I sought out the meeting of ASHRAE Technical Committee (TC) 1.4, Control Theory and Application. The topic was never mentioned. After the meeting I introduced myself to the chairman who, it turned out, worked for the company that had sold us our first DDC equipment. He explained that a communication standard was "impossible, because the controls vendors will never go along with it."

I joined TC 1.4 and began to work to persuade my new colleagues that a communication standard was not only possible, it was essential. It took six years, but in 1986 it was suggested that I write a title, purpose and scope that could be used by the standards committee as the basis for the formation of a new project committee to develop a protocol. With the sentiments of the previous TC 1.4 chairman still in the back of our minds, we decided to propose the creation of a guideline (a type of document that had been formalized within ASHRAE around this time), thinking this would allow us to approach full-fledged standardization more gradually, and possibly not incur as much opposition from the controls companies, at least in the early stages. Fortunately, the standards committee at the time would have none of it. They believed the ASHRAE protocol should be a bona fide standard right from the start, so the Standard Project Committee 135P was born, and I was asked to chair it.

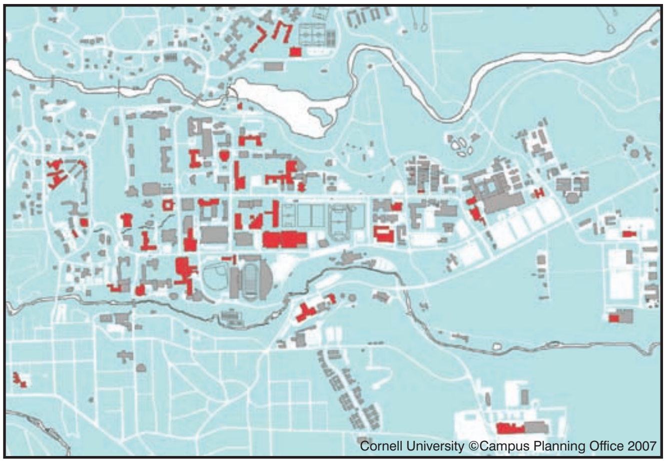
The SPC members, made up of mechanical and computer engineers, manufacturers, consultants, U.S. and Canadian government employees, and others, decided that a catchier name was needed. After discarding such memorable suggestions as ASHnet and ASHtalk, the members of the committee decided on BACnet as the name for ASHRAE's new protocol.

Eight-and-a-half years of effort later, in 1995, BACnet was published as ANSI/ASHRAE Standard 135, *A Data Communication Protocol for Building Automation and Control Networks*, and the problem of interoperable communication for building automation systems was, at least in principle, solved.

Cornell's Adoption of BACnet

Cornell University's Ithaca campus is comprised of more than 300 buildings, with about 100 that exceed 50,000 ft^2 (4646.5 m^2) in area. Almost all of the latter have digital controls and, at last count, 54 buildings had at least some BACnet equipment (*Figure 1*).

The adoption of BACnet at Cornell was not a given. True, I had been involved with its development from the start, but I also had been careful to try to let BACnet speak for itself. The first real opportunity for this came when the controls for our new nano-



Cornell University ©Campus Planning Office 2007

Figure 1: Currently, 54 buildings (identified in red) on Cornell University's Ithaca, N.Y., campus make use of BACnet devices.

Abbreviations

ACL	Access Control List
ARCNET	Attached Resource Computer Network
BBMD	BACnet Broadcast Management Device
BDT	Broadcast Distribution Table
COV	Change-of-Value
DDC	Direct Digital Control
EMCS	Energy Management and Control System
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
MS/TP	BACnet's Master-Slave/Token-Passing Protocol
NAT	Network Address Translation
PICS	Protocol Implementation Conformance Statement
RAM	Random Access Memory
USTAG	United States Technical Advisory Group
VLAN	Virtual LAN
VPN	Virtual Private Network

technology laboratory were to be bid in 2001. Duffield Hall is a massive, complex building with labs, cleanrooms, fume hoods, classrooms, offices and a large atrium. Were controls, based on BACnet communications and the newly emerging BACnet suppliers and contractors, up to a job of this complexity when matched against the traditional controls companies? The answer turned out to be a resounding "yes." Of the three bids received, two were based on BACnet while the third was a proprietary solution. Happily, the two BACnet bids came in significantly lower than the proprietary one and, with just a bit of trepidation, the job was awarded to an untested BACnet supplier. This was the start.

Fortunately, the job went relatively smoothly and our facilities designers began to take BACnet seriously. Our HVAC&R controls shop, always willing to take on new challenges, began training in the use of our new controls and started using BACnet products in small retrofit situations.

At this point, our single EMCS minicomputer had given way to a cluster of DEC MicroVAXes, and the number of supported protocols had grown to eight. It was time to implement one more—hopefully the last—BACnet!

Reducing the Chaos

It became immediately clear that to avoid total chaos, we would need to develop some Cornell-specific standards in the areas of naming, addressing, broadcast distribution and security. The result has been a new section in our Design and Construction Standards, 15956, Building Automation and Control System Communications and Interoperability (http://cds.pdc.cornell.edu/default.cfm). In the remainder of this article, I describe some of the steps we have taken to ensure BACnet is a success on our campus as more systems come online.

Object Naming

The method we use for naming our BACnet objects is based on the concept of Facility/System.Point. The *facility* is typically a building and may be followed by a subfacility such as the system's physical location in the building. The *system* describes the type of equipment and may be followed by a subsystem. The *point* is the specific input, output or value that is being described. An example of this might be DuffieldHall/AHU-1.CW.STEMP, where the facility is DuffieldHall; the system is AHU-1 (Air Handler Unit 1); the subsystem is CW (chilled water); and the point is STEMP (the supply temperature). The trick is coming up with a standard list of facilities, subfacilities, systems, subsystems and points. It is important to know what constraints are imposed on object naming by the DDC equipment being used. BACnet does not specify how long an Object_Name can be, though the property must be able to hold at least one printable character—not too stringent a requirement. This information is provided in a vendor's Protocol Implementation Conformance Statement (PICS). Naming is an important area of ongoing work for us and one that could benefit from the efforts of a guideline or standards committee. Any volunteers?

Addressing: Network Numbering

Although a BACnet internetwork, i.e., a collection of BACnet networks, possibly using different technologies such as BACnet/IP (BACnet using the Internet protocol), BACnet over Ethernet or ARCNET or BACnet MS/TP, can still function with a collection of inconsistent object names, the same is not true of network numbers and device instance numbers. These must be planned carefully or you will have a disaster on your hands. This is the biggest challenge facing owners or system integrators, those that must deal with equipment from more than a single supplier.

Consider this: almost every contractor, left alone, assigns 1 as the number of their first network and 1 as the number of their first controller. Without coordination, problems arise almost immediately.

BACnet provides for up to 65,535 network numbers so there is some room for maneuvering in most cases. For example, if you only had three buildings, and they were numbered Building 1, Building 2 and Building 3, you could assign the numbers 100 – 199 to the first building, 200 – 299 to the second building and 300 – 399 to the third. This makes it easy to keep track of the numbers since the first digit of the network number corresponds to the building number.

At Cornell we use a scheme based on a facility code assigned to each building by our facilities inventory group:

0000–0999	Open
1000–1999	Statutory facilities
2000–2999	Endowed facilities
3000–3999	Housing and dining facilities
4000–4999	Off-campus facilities
5000–5999	Utilities

Using the facility code as a basis, we numbered our networks FFFFN, where FFFF is the four-digit facility code and N is the number of the network in the building, 0 – 9. As an example, Duffield Hall has a facility code of 2000, so the networks in Duffield are given the BACnet network numbers of 20000 to 20009. The downside is that on rare occasions a building may have more than the 10 networks that this scheme accommodates. In that case, we have used facility codes from the Open category to fill in. The beauty of this numbering method is that troubleshooting is dramatically simplified. When a technician needs to monitor network traffic, the origin and destination of messages on the wire are instantly apparent. Soon, you begin learning the facility codes by heart.

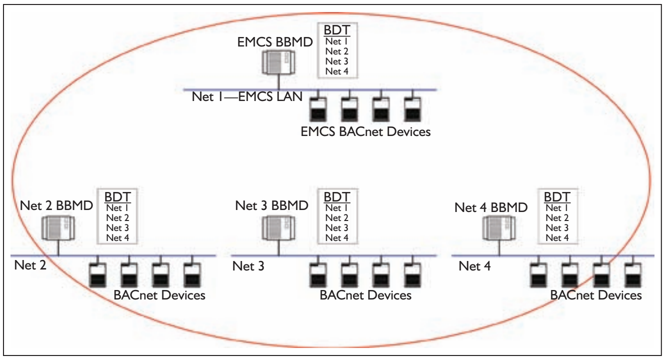


Figure 2: BACnet prescribes that all BDTs should be the same. In this case, all devices, on all networks, receive global broadcasts.

Addressing: Device Instance Numbering

BACnet requires that device instance numbers be unique within a BACnet internetwork so that each device has a unique identifier. Instance numbers are defined in the standard as 22 bits long, in decimal instance numbers range from 0 to 4194303. Given this situation, we decided to build upon our network numbering scheme by adding two digits to our network numbers to form device instance numbers: FFFFNDD, where FFFF and N are as described above and DD ranges from 00 to 99. Given our numbering, each individual BACnet network can have up to 100 devices on it.

The only problem is that our scheme falls apart for facilities with codes above 4194. Fortunately, in practice, all but one of our BACnet buildings on the Ithaca campus fall in the facility code range of 1000 to 3999 so our method basically works. In the case of the off-campus building with facility code 4706, we just assigned a network number of 0706 from the Open range.

The point is that some rational method of assigning and administering network and device instance numbers needs to be established early in the BACnet deployment process and rigorously adhered to otherwise, sooner or later, you will face a lengthy, costly and highly annoying cleanup effort.

Broadcast Management: Split Horizons

One of BACnet's many strengths is that it supports the idea of distributing messages to all devices with one transmission. These messages are called broadcast messages and can be configured for delivery to all devices on a single network or all devices on all networks, so-called global broadcasts. Broadcasts are useful for dynamic binding (sending a global Who-Is message to determine the address of a particular device), sending a load shedding command (we have a load shedding program for potential emergencies involving chilled water and are developing one for steam) and sharing variables that may be needed by many different control processes (unexpected occupancy of a lecture hall or a common temperature or pressure value).

Broadcasting, especially globally, can be a problem for certain types of internetworks and is a particular problem for the Internet where broadcasts are explicitly blocked from moving from one Internet Protocol (IP) subnet to another. The reason for this is obvious. The Internet connects millions of computers all over the world and global broadcasts need to be delivered to each one of them. If broadcast traffic were allowed and commonly used, the load on the system could quickly become intolerable, potentially crippling the Internet. Not good!

BACnet solves this problem by defining a BACnet Broadcast Management Device (BBMD), one per IP subnet. A BBMD is simply a dedicated computer (or a program within an existing controller) that intercepts broadcasts and then sends them on as directed, unicast messages to peer BBMDs, which then rebroadcast them locally on their own subnet. The list of peers is contained in a Broadcast Distribution Table (BDT) and, to ensure consistency and ease of administration, the BDT is supposed to be identical in every BBMD. At least that was the thinking when we added the idea into the standard because we were envisioning that all the systems would be tightly integrated (*Figure 2*).

The reality is that most broadcasts are only relevant in a limited area, e.g., within a single building. At Cornell we have found it to be the exception rather than the rule that a dynamic binding request or common value needs to be truly globally broadcast. In other words, nobody in ABC Hall cares very much about what is happening in XYZ Hall—at least as far as the building automation systems are concerned!

To control the situation, we have decided to ignore the standard's requirement that all BDTs must be created equal. Each of our BDTs contains just the address of the local BBMD and the BBMD at our EMCS operations center (*Figure 3*). At the EMCS we can monitor all the broadcast traffic everywhere on campus—but the propagation is tightly controlled—and problems from misconfiguration of controllers are minimized. Such problems can arise if a controller is programmed to report alarms/events to a recipient that doesn't exist, to read a value from a non-existent address, or if it generates excessive Change-of-Value (COV) notifications because the COV increment for generating the notification has been set too small.

We call this approach split horizon because each BACnet network only sees its own network and that of the EMCS, the other networks are below the horizon. The split horizon approach has worked well in our situation. However, the technique is adaptable. You can configure your BDTs to span whatever group of facilities/networks makes sense for your application.

Security: ACLs, VLANs and VPNs

Computer security on college campuses is a big deal. Fortunately, the information technology (IT) industry has developed a variety of solutions that can be applied directly to networked building automation systems. The main threats are an intruder gaining access to a building automation network and penetrating an access control system; shutting off critical equipment, and creating a diversion that might permit a more direct physical attack; or generating enough spurious traffic to cause a denial of service attack, preventing normal traffic from traversing the network. In any of these cases, the first line of defense is to keep potential troublemakers from getting on the network in the first place.

In the case of local networks (e.g., Ethernet, ARCNET or MS/TP), dedicated media and physical security are the best means of deterrence. In the case of networks with connectivity to the outside world, such as Internet subnets, a carefully configured firewall is needed. Fortunately for us, our multiple IP subnets are interconnected by switches that can be provided with access control lists (ACLs) by our IT group. The ACLs can be fine-tuned as needed. For example, in the case of our BACnet/IP subnets, the ACLs allow only access from a couple of our office networks and from the EMCS subnet. Access from other subnets on campus, or from addresses outside of the university, are barred entirely. It also is possible to prevent access based on the kind of protocol. We could disallow anything other than BACnet messages, even from the trusted on-campus subnets.

So that we don't tie ourselves in knots (something that security measures can easily do), we have set up several virtual private network (VPN) portals (specialized computers that are attached to the secured network and the outside world) that require users to provide a user name and password for authentication and require their computers to encrypt all traffic to the VPN and to accept encrypted traffic in return. The VPNs provide a secure tunnel into the secure networks with the advantage that the VPNs can be accessed from anywhere.

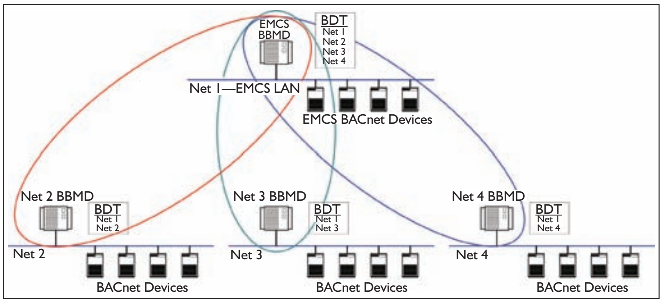


Figure 3: Cornell has implemented the "split horizon" concept illustrated here. In our case, the BDTs are configured to limit global broadcasts to the network on which they originate plus the network of our EMCS operations center. This eliminates routine building-to-building broadcast traffic. Only the EMCS is allowed to distribute, at its discretion, truly global broadcasts.

Smaller networks also can be protected by inexpensive commercial firewalls that provide network address translation (NAT) to devices on the inside. NAT protects devices by presenting them to the outside world with the address of the NAT firewall itself instead of the device's true IP address. Since the firewall can be set up with rules similar to the ACLs described previously, it can prevent outside intruders from ever getting to the devices inside its protective wall.

Another technique available to users of sophisticated switches is that devices on various physical networks can be made members of a virtual local area network (VLAN). These devices appear to be on a common IP subnet, even though they may be anywhere within the range of the communicating switches. The devices on a VLAN can be protected by ACLs just as if they were on the same physical network and one common switch. Almost all of Cornell's BACnet/IP equipment is now protected by VLAN/ACL technology.

Addendum *g* to BACnet-2004 (www.bacnet.org/Addenda/index.html), a complete rewrite of BACnet's security clause, will soon go out for a third public review. This new network security architecture provides device and user authentication and data hiding through encryption and the techniques can be applied to any of the BACnet network types, not just BACnet/IP networks. Even if an intruder could gain access to the network, the contents of the traffic are undecipherable, and the intruder's ability to communicate with the BACnet devices in any form are all but impossible.

Summary

At the time of this article, we have nearly 2,000 BACnet devices on the Cornell campus, ranging from small application-specific devices to full-scale building controllers. BACnet has allowed us to integrate disparate systems as never before. While most of the BACnet devices are dedicated to HVAC applications, we also have several lighting control and switchgear monitoring systems. In all, we have BACnet equipment from six different suppliers, all happily interoperating. Now, thanks to BACnet, we can quit worrying about getting devices to talk to each other and can get on with the real work: running our campus mechanical equipment as smartly and efficiently as possible.●