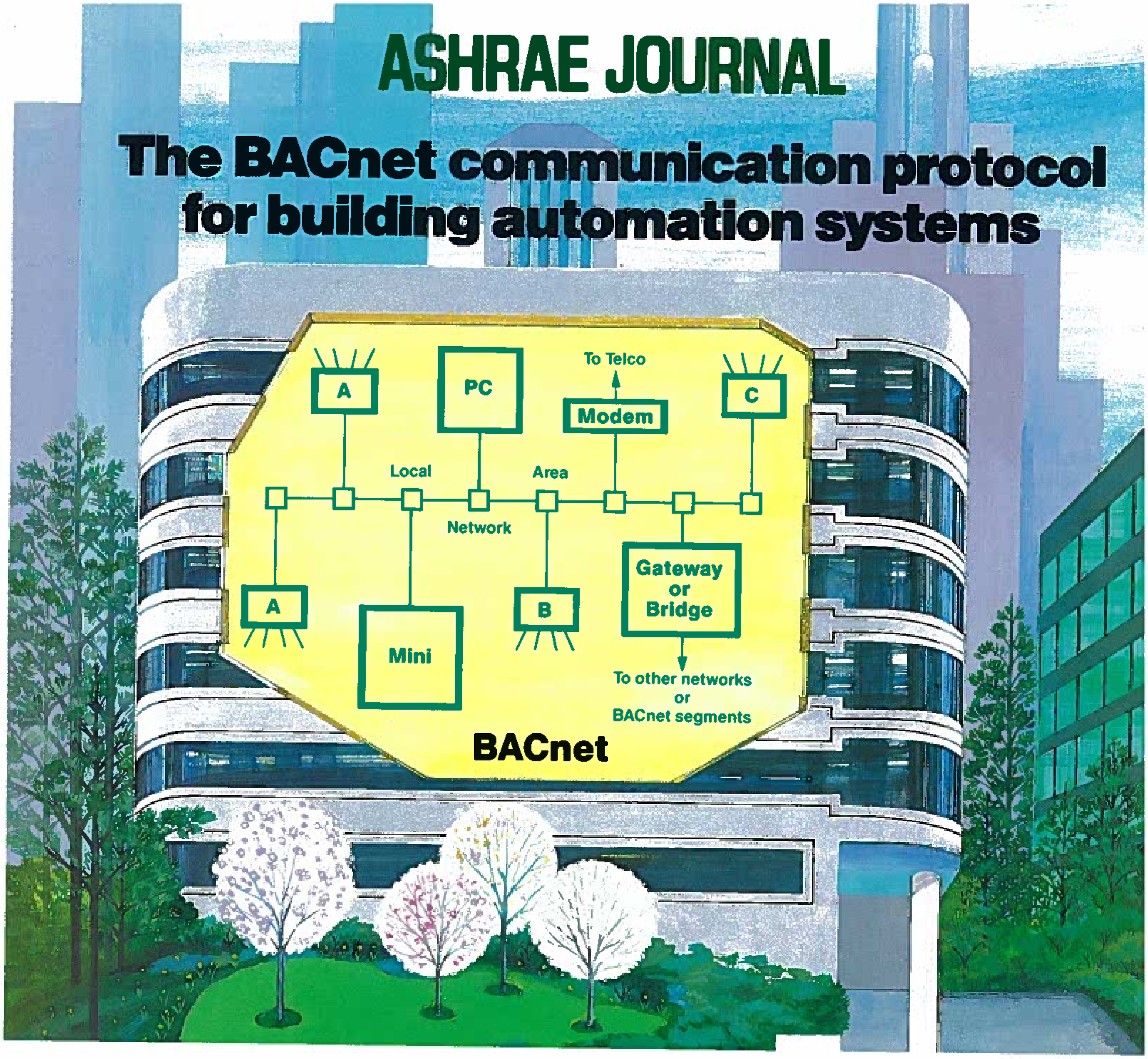
ASHRAE JOURNAL

# The BACnet communication protocol for building automation systems




*This article describes BACnet as it exists now and also the tasks remaining to finalize it*

**By Steven T. Bushby** and **H. Michael Newman**
*Associate Member ASHRAE* *Member ASHRAE*

The building community in the United States and in several other countries has been carefully watching the efforts by ASHRAE to develop a communication protocol for building energy management and control systems (EMCS). In January, 1987, the ASHRAE Standards Committee formed a Standards Project Committee (SPC-135P) to deliberate the creation of a communication protocol that will become an industry standard. The name chosen for this protocol is "BACnet—A Data Communication Protocol for Building Automation and Control Networks."

A communication protocol is a set of rules governing the exchange of data between two computers. In the broadest sense, a protocol encompasses both hardware and software specifications including: the physical medium; rules for controlling access to the medium; mechanisms for addressing and routing messages; procedures for error recovery; the specific formats for the data being exchanged; and the contents of the messages.

The basic approach and guiding philosophy adopted by SPC-135P was described two years ago in an ASHRAE *Journal* article (Bushby, Newman 1989). This article presents an overview of BACnet as it is today and describes the tasks remaining to be completed.

BACnet is a communication protocol designed specifically to meet the needs and constraints of building automation systems. BACnet provides a way to convey data including, but not limited to: hardware binary input and output values; hardware analog input and output values; software binary and analog values; schedule information; alarm and event information; files; and control logic.

All of these data can already be conveyed by current state-of-the-art building control systems. What makes BACnet different is that it will enable the exchange of this information between devices made by different manufacturers and it can be used for building systems other than EMCS. Thus BACnet may become a key to truly integrated building systems.

BACnet will allow designers several options regarding the type of communication wiring used and the amount of message "traffic" that a network will be able to carry. This means that, if the building is small and has limited communication requirements, it will not be necessary to invest in the technology needed for a large, fully integrated building or campus of buildings to take advantage of BACnet technology.

The key to understanding how BACnet works is to think of it as two separate but closely related parts: a model of the information contained in a building automation device; and a group of functions or "services" used to exchange that information.

### Modeling building automation devices

The internal design and configuration of a building automation device will continue to be proprietary in nature and different for each vendor. BACnet overcomes this obstacle by defining a collection of abstract data structures called "objects," the properties of which represent the various aspects of the hardware, software and operation of the device (see *Figure 1*).

These objects provide a means of identifying and accessing information without requiring knowledge of the details of a device's internal design. The communication software in the device can interpret requests for information about these abstract objects and, in effect, translate that request to obtain the information from the real data structures inside the device. These objects collectively provide a "network-visible" representation of the building automation device.

The current draft of BACnet (ASHRAE 1990) defines 20 different types of objects, as shown in *Table 1*. A building automation device may have zero, one, or many objects of each object type. An object is accessed by means of a property called "Object Identifier" that uniquely identifies each object within a single device. The Object Identifier can be thought of as the "name" of the object.

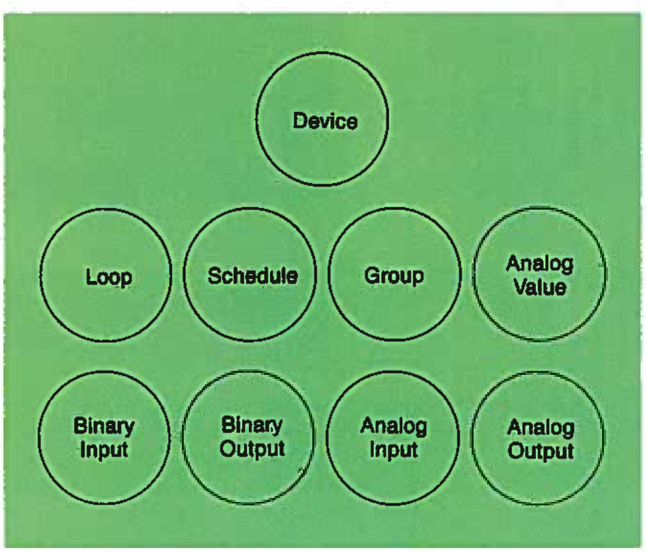



**Figure 1.** Sample objects that may comprise a typical BACnet device.

**About the authors**

Steven T. Bushby is an engineer in the Mechanical Systems and Controls Group, Building Environment Division, Center for Building Technology, National Institute of Standards and Technology. He received a bachelor's degree from Northwestern University and a master's degree from Colorado State University, both in chemical engineering. Bushby is a member of ASHRAE Technical Committee 1.4 (Control Theory and Applications) and serves as secretary of Standards Project Committee 135P.

H. Michael Newman is the manager of the Facilities Engineering Computer Section at Cornell University. He received his bachelor's and master's degrees in engineering physics from Cornell University and did post-graduate work in astrophysics in the NASA Center for Radiophysics and Space Research. Newman served on the ASHRAE Research and Technical Committee and is currently chairman of Standards Project Committee 135P.

The list of object types in *Table 1* provides a fairly comprehensive picture of the kinds of information found in modern building automation devices and will probably be very close to the final list of object types included in the standard. For each object type, a set of properties is defined and each property is described in detail. For example, *Table 2* shows the properties that are defined for Binary Input objects.

The roles of many object types in *Table 1* are readily apparent from their names. Others that are less obvious are described as follows:

- Calendar represents a list of dates that have special meaning when scheduling the operation of mechanical equipment. A list of holidays would be one example.
- Device contains general information about a particular device, such as vendor name, model name, location, object types supported, etc.
- Device Table provides a shorthand way to reference a list of devices. For example, it may be used to list several alarm terminals or printers that must be notified when an alarm or other event occurs.

**Table 1. BACnet Standard Object Types**

| | |
|---|---|
| Analog Input | Directory |
| Analog Output | Event Enrollment |
| Analog Value | File |
| Binary Input | Group |
| Binary Output | Loop |
| Binary Value | Mail Box |
| Calendar | Multi-State Input |
| Command | Multi-State Output |
| Device | Program |
| Device Table | Schedule |

**Table 2. Properties of Binary Input Objects**

| | |
|---|---|
| Object Identifier | Polarity |
| Object Type | Inactive Text |
| Present Value | Active Text |
| Description | Change-of-State Time |
| Status Flags | Elapsed Active Time |
| Reliability | Change-of-State Count |
| Override | Time of Reset |
| Out-of-Service | |

• Directory provides information about how to access other objects, much like a telephone directory provides information about how to call someone on the phone.

• Group provides a shorthand way to read a number of values in one request. For example, it might be used to simultaneously update several fields on an operator graphic display.

• Loop can be used to represent any feedback control loop, which is some combination of proportional, integral or derivative control.

• Event Enrollment provides a way to define alarms or other types of events and to indicate who should be notified when they occur.

### BACnet services

Objects provide an abstract representation of the "network-visible" portion of a building automation device. The "application services" provide "commands" for accessing and manipulating this information as well as providing some additional functions. The current draft of the standard defines 25 application services that are divided into five categories. *Table 3* lists all of the services and shows how they are grouped.

The Alarm and Event Services provide a way to request a status summary for alarms or events, notify devices that alarms or events have occurred, and acknowledge that an operator has seen an alarm notification. The File Access Services provide the means to read and write files, including the ability to upload and download control programs and databases. Object Access Services provide a means to read the properties of objects, write to properties of objects and, in some cases, to create or delete an object. The Remote Device Management Services provide tools for troubleshooting and maintaining devices.

Because the hardware and configuration details of building automation devices will continue to be proprietary and vendor-specific, there is a need to provide operators with tools that are vendor-specific for configuring these devices. This is the role of virtual terminal (VT) services, which provide a mechanism for bi-directional exchange of character-oriented data. This allows an operator console to interact with a BACnet device as if it were a directly-connected dumb terminal.

The protocol service merely conveys the character streams between the two devices. The meaning of the character streams is not defined in the standard and must be interpreted in a proprietary manner.

VT services can also be used as a security mechanism. If portions of the object database should not be changed by other devices on the network, these properties may be read-only. VT services provide a way to change these properties with vendor-specific security control.

### Conformance issues

The goal of BACnet is to enable building automation and control devices from different manufacturers to communicate. Experience with other communication protocols shows that, for this goal to be achieved, there must be clear specifications about what it means to conform to BACnet and a conformance testing procedure that can be conducted by an independent, unbiased party. Experience also shows that the way conformance is defined will have important implications on how specifications for procurement of building automation systems will be written.

BACnet defines a comprehensive set of object types and application services, in the sense that communication requirements among all control levels in a distributed, hierarchical control system are addressed. There is considerable variation in the sophistication of the devices found in the various levels of such a system. Thus, there is the reality that all devices do not need to support the full functionality of BACnet to perform their tasks. BACnet accounts for this by classifying levels of conformance. The guiding philosophy is that conformance requirements should be driven by the device's functionality.

There are two conflicting goals that make defining the conformance classifications difficult. One goal is to maximize the chances for interoperability. This can be achieved by simply eliminating the choices and requiring all of BACnet to be supported. This has a benefit of making it easy for users and consultants to draft system specifications. It also places unreasonable requirements on many control devices and would make them prohibitively expensive.

The second goal is to give manufacturers flexibility to select the portions of BACnet that are appropriate for the device's intended application. This solves the problem of artificially restrictive conformance requirements, but virtually guarantees that devices made by different manufacturers will not be fully compatible.

Many different building automation devices would appear in the market, each supporting a slightly different combination of BACnet services. Because different choices were made when the devices were designed, they would not be completely compatible. A terrible side-effect of this might be a tendency to specify that *all* of BACnet be supported to get around this problem, thus making over-designed and needlessly expensive systems commonplace. The task before SPC-135P is to find the best balance between these conflicting goals.

One proposal being considered defines three hierarchical classes of conformance. Each class specifies a *minimum* set of services (and object types) that must be supported to claim membership in that particular conformance class. A device with capabilities that exceed those in a particular class, but not enough to claim conformance to the next higher class, can indicate this through the use of a protocol implementation conformance statement (PICS) that lists the device's additional capabilities.

Class 0 devices are the least sophisticated and might, for example, be characteristic of a smart sensor. Class 1 devices, which include the Class 0 requirements, represent an intermediate level of sophistication. A unitary controller might be designed as a Class 1 BACnet device.

Class 2 defines the most sophisticated BACnet devices. For membership in this class, all services defined in the standard must be supported. Real devices in this class would be operator interface devices and sophisticated supervisory controllers or field panels.

It is important to note that the conformance classes define the communication capabilities of a device, *not* the device's function. This approach represents a bias towards maximizing interoperability and making specification easier.

An alternative to the hierarchical class approach has been proposed that relies on the concept of "functional groups." The idea is that the communication functions provided by the protocol would be divided into logical groupings that relate to particular functions. Examples might be Alarm and Event Processing, Scheduling, and File Handling. Altogether, 18 functional groups have been proposed.

With this approach, a manufacturer would be free to select any combination of these functional groups. This approach represents a bias towards the maximum flexibility-in-design end of the spectrum.

It is not yet clear how conformance classification will be resolved in the final standard. It is clear that there will be several classifications. Most likely, the final standard will have more flexibility than a three-tiered hierarchy and less flexibility than a selection from among 18 functional groups.

The National Institute of Standards and Technology (NIST) has proposed a test architecture and a methodology for developing the test procedures for determining conformance to BACnet (Bushby 1990a, 1990b). Work is currently underway at NIST to develop a testbed implementation based on the most recent working draft of the standard. Prototype BACnet implementations provided by control system manufacturers will be tested at NIST to evaluate and refine the conformance testing process. It is expected that this work will form the basis for an industry certification program for compliance to the BACnet standard. It is not yet clear how such a certification program will be administered.

### Interconnecting BACnet devices

From the start, SPC-135P has taken a "top down" approach to developing BACnet. The emphasis has been on how to represent the internal operation of a building automation device in a common, network-visible way and how to interact with this standard interface by means of a common set of protocol services. As a result, the concept of BACnet objects and services was developed and their refinement is nearly complete. The committee's final hurdle is how to convey the various service requests and responses from one device to another, the data communication problem usually referred to as "networking."

Why was networking left until last? Simply because the committee first needed to solve the problem of what dialog should take place between two BACnet devices; it made no sense to worry about the interconnection if there was no agreement on what the machines would say to each other. With so many viable network-

**Table 3. Application Services**

**Alarm and Event Services**
- Acknowledge Alarm Service
- Confirmed Event Notification Service
- Get Alarm Summary Service
- Get Enrollment Summary Service
- Unconfirmed Event Notification Service

**File Access Services**
- Atomic Read File Service
- Atomic Write File Service

**Object Access Services**
- Add List Element Service
- Create Object Service
- Delete Object Service
- Read Property Service
- Read Property Conditional Service
- Read Property Multiple Service
- Remove List Element Service
- Write Multiple Property Service
- Write Property Service

**Remote Device Management Services**
- Block Transfer Service
- Reinitialize Device Service
- Confirmed Text Message Service
- Unconfirmed Test Message Service
- Time Synchronization Service
- Who-is and I-am Services

**Virtual Terminal Services**
- VT-Open Service
- VT-Close Service
- VT-Data Service

ing technologies already commercially available from the computer industry, it would be senseless for ASHRAE to try to develop its own industry-specific data communication methodology.

As a result of this strategy, SPC-135P selected three distinct networking methods that best meet the many needs of building automation and control systems. Two of the three, Arcnet and Ethernet, have been developed entirely outside of ASHRAE. The third, Master-Slave/Token-Passing (MS/TP), is being defined by the committee, but relies on a standard physical layer, EIA-485. These technologies (which differ in speed, throughput and cost) are all forms of local area networks (LANs) and will be described in more detail below.

The ability to use different networking technologies is one tangible benefit of adhering to the open systems interconnection (OSI) model (ISO 1984) of a layered communication architecture (Bushby, Newman 1989). The concept is to divide the various communication requirements into groups of related requirements that can then be developed and refined independently of each other. In the OSI model, these groups are referred to as "layers."

However, for this idea to work, it is necessary to unambiguously define the interfaces between the layers. One such layer interface has been defined by the IEEE and is also an international standard, ISO 8802-2 (ISO 1989). Called Logical Link Control (LLC), it provides a standardized interface between higher level services (such as those provided by BACnet's application layer) and underlying medium access control services and physical media.

Medium access control (MAC) refers to the mechanism by which a particular device gains access to the physical transmission medium. Standards exist for master-slave networks, contention resolution networks and various types of token-passing networks. Moreover, many MAC technologies can be used with more than one type of cabling system.

With a common interface such as LLC, BACnet can be readily adapted to the best medium for the application at hand. *Figure 2* shows the lower layer protocols adopted by SPC-135P.

<table>
<tr><td>LLC</td><td colspan="4">ISO 8802-2 Connectionless or Acknowledged Connectionless</td></tr>
<tr><td>MAC</td><td colspan="2">Master-Slave/Token-Passing</td><td rowspan="2">ARCNET</td><td rowspan="2">ISO 8802-3</td></tr>
<tr><td>PHY</td><td>EIA-485</td><td>EIA-232</td></tr>
</table>

**Figure 2. Protocols for the lower layers of the BACnet architecture.**

How did the committee decide on the three recommended networking technologies? Basically, the committee analyzed all major LAN technologies and rated each in the following areas: speed; availability of chips or boards that implement the LAN; familiarity with the LAN on the part of manufacturers in the building automation industry; degree of compatibility with existing hardware; and cost. The committee also tried to identify any other distinguishing features of each LAN that could then be rated pro or con in the analysis. The result is three alternative, but complementary technologies, each of which has certain unique strengths in one or more of the areas cited above.

The first alternative, Ethernet (or more specifically, the ISO 8802-3 standardized version of it) is a data link and physical layer specification developed jointly in the early 1980s by Digital Equipment Corporation, Intel and Xerox. It offers high speed (10 Mbps) and is extremely widespread, with more than 2 million nodes in existence. Not only has the cost of the chip sets been dropping radically, but a new version of the specification has recently been approved that allows for operation on unshielded, twisted pair as well as the traditional thick and thin wire coaxial cable.

Ethernet uses the carrier sense multiple access with collision detection (CSMA/CD) form of network access method. This is a contention method, meaning that any station can try to transmit on the network at will (all stations are peers). Each station waits for silence before transmitting and then also listens to its own transmission as it is being sent, comparing each bit with what it is supposed be. Any differences are taken to be the result of a "collision" with a transmission from another station. Both stations then cease transmission immediately and wait a random time interval before trying again.

As a result of using CSMA/CD, Ethernet makes very efficient use of the transmission medium, at least most of the time. There is no communication overhead such as is associated with token-passing (see below) where the token has to be passed even if no station has any data to send. However, it is not deterministic in that it is not possible to predict with absolute certainty how long a station might have to wait before being able to transmit successfully. Nonetheless, properly engineered Ethernet installations will provide the highest speed performance and data throughput of any of the BACnet networking technologies for those applications requiring it.

The second alternative, Arcnet, is a *de facto* standard, originally developed by the Datapoint Corporation, that has about a decade of practical field experience behind it. It is a lower-cost alternative than Ethernet but, nonetheless, operates at the respectable speed of 2.5 Mbps. Arcnet claims to be the oldest commercially available LAN, with nearly 3 million nodes installed worldwide.

Unlike Ethernet, Arcnet uses a token-passing network access method; permission to transmit is conveyed sequentially from one network participant to the next. Arcnet is thus deterministic and token passing times of only several milliseconds are to be expected, and can readily be verified after installation. Like Ethernet, Arcnet can be used on both twisted pairs and coax. Apart from the fact that several vendors in our industry are currently marketing Arcnet-based products, there is an additional sweetener: a 20 Mbps version is on the drawing boards and may be available before long.

BACnet's third networking possibility is based on the use of the EIA-485 (Electronic Industries Association) physical layer standard. EIA-485 (formerly called RS-485) prescribes the characteristics that must be met by up to 32 digital transceivers communicating in a multipoint configuration (meaning that the transceivers are all connected to the same physical medium). While the transceiver design parameters allow speeds up to 10 Mbps, the use of twisted pair wire and low cost asynchronous receiver-transmitter chips has resulted in EIA-485 finding use predominantly at low speed, usually less than 19.2 Kbps. Nonetheless, it is used by almost all vendors, particularly for their unitary, application-specific controllers.

But EIA-485 is *not* a data link standard; it does not address the problem of network access. For this reason, SPC-135P has decided to define an appropriate master-slave and/or token-passing protocol (MS/TP), similar to one or more of the many proprietary schemes already in use, that can be used with this very common type of hardware. (A master-slave access method is one in which one station, the master, controls all activity on the medium by passing transmission authority to each subordinate station, the slaves, one after the other.) MS/TP should prove to be the lowest cost type of LAN and might only require firmware changes to be used with equipment of current design.

### What remains to be done?

The selection of physical and data link technologies may, as a by-product, help to solve one other remaining problem facing

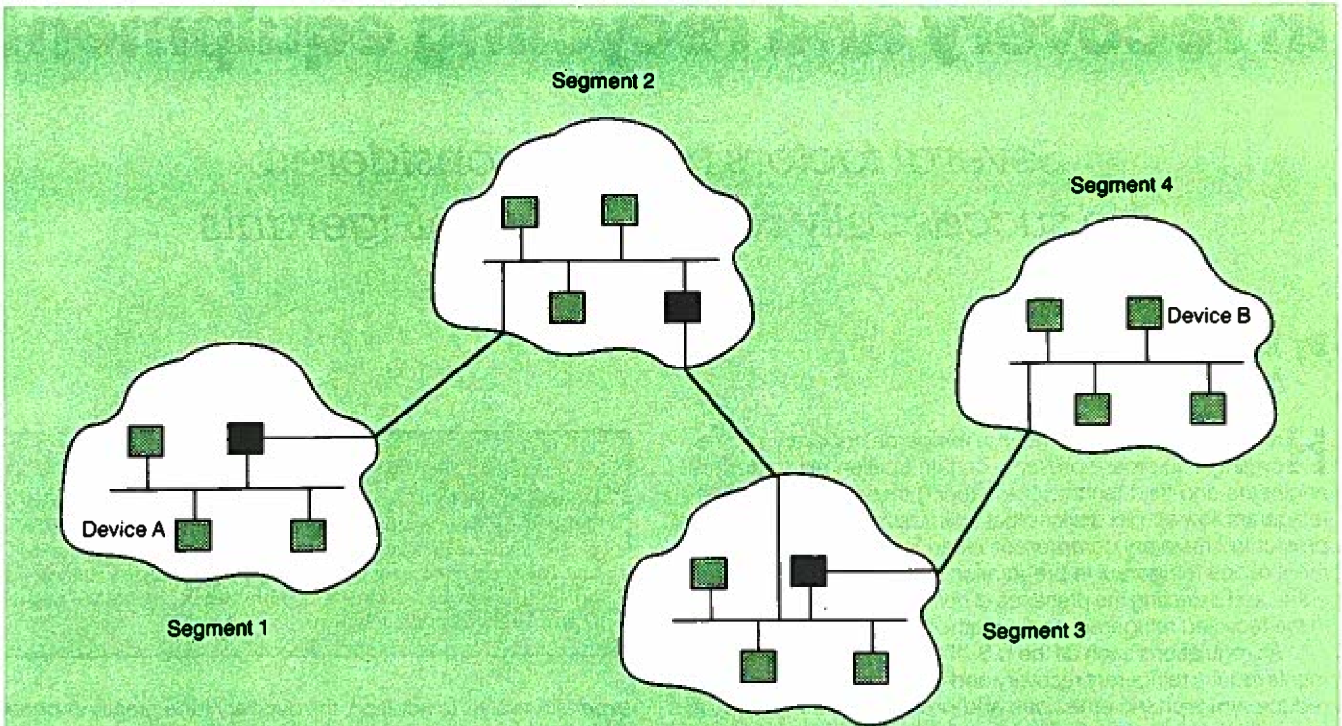



**Figure 3.** BACnet intersegment relaying. To pass a message from Device A to Device B, one device per segment (shown in black) must be able to communicate on two media and understand how to shuttle messages back and forth.

the committee: How to relay messages from one local area network segment to another. (See *Figure 3*.) This problem arises because there is no requirement that all BACnet devices be physically connected to the same medium or use the same LAN technology. Thus a device's address might not be unique across the entire network.

Indeed, BACnet makes no assumptions whatsoever about the physical arrangement of devices in an actual installation. Thus, it avoids the trap of binding the protocol to any particular network topology or hierarchy. Instead, the protocol concentrates only on devices' communication requirements.

Two competing approaches exist. One is to define a network layer protocol that adds information to each message such that certain devices in the network (often called routers) are able to direct messages to their final destinations, possibly through several intermediate devices. A BACnet router may not have to be as sophisticated as its wide area network counterpart. Much of the complexity of routing software relates to the problem of selecting a path from source to destination based on the possibility of multiple paths. A working hypothesis of BACnet is that only one such path between devices is allowed, thus greatly simplifying the problem. Routers of some type may be the only solution where several different kinds of LAN segments are present.

The other approach, which works if all LAN segments are the same type, is to use MAC-layer bridges (devices readily available) at least for Ethernet. In this type of network, each BACnet device's address is unique, not just on the local segment, but across the entire network. The bridge may be smart, passing only selected traffic between devices on opposite sides of it, or it may be dumb, passing all traffic that it hears bi-directionally. Whether the final solution will be routers, bridges or a combination of the two remains to be decided.

### When will BACnet be finished?

Current plans call for a Public Review Draft of BACnet to be ready by Spring of this year. If the comments received do not reveal the need for substantive changes, the final version could be published as an ASHRAE standard sometime later in 1991. However, if changes are required, additional public reviews might be necessary, delaying final publication by an uncertain amount.

The overwhelming desire of SPC-135P is to ensure that BACnet, once finalized, meets the considerable expectations of building automation and control system users, designers and manufacturers for a well-conceived, thoroughly proven, highly reliable data communication protocol. ■

### References

ASHRAE. 1990. "BACnet—A Data Communication Protocol for Building Automation and Control Networks, working draft 4." SPC-135P—015.

Bushby, S.T., Newman, H.M. 1989. "Standardizing EMCS communication protocols." ASHRAE *Journal*. Vol. 31, No. 1, pp. 33-36.

Bushby, S.T. 1990a. "Testing conformance to energy management and control system communication protocols—Part 1: Test architecture." ASHRAE *Transactions*. Vol. 96, Pt. 1, Paper No. AT-90-14-3.

Bushby, S.T. 1990b. "Testing conformance to energy management and control system communication protocols—Part 2: Test suite generation." ASHRAE *Transactions*. Vol. 96, Pt. 1, Paper No. AT 90-14-4.

ISO. 1984. *International Standard 7498*, "Information processing systems—Open systems interconnection—Basic reference model." New York, New York: ANSI.

ISO. 1989. *International Standard 8802-2*, "Information processing systems-Local area networks—Part 2: Logical link control." New York, New York: ANSI.