Internetworking with BACnet

A first look at networking in BACnet

By Bill Swan, Alerton Technologies, Inc.

The Building Automation and Control Network ("BACnet") is an open data communications protocol developed by ASHRAE and adopted by ANSI (ANSI/ASHRAE 135-1995). It is designed to handle a number of building automation system (BAS) applications such as hvac, lighting, and fire. It is also designed to be cost-effective meeting requirements ranging from those of small to very large buildings and the largest campus-wide or regional applications.

Such a broad spectrum of applications has varied and conflicting requirements for the local-area networks (LANs) which interconnect the various components of a BAS, from the operator and maintenance stations down to the unitary controllers. In some instances cost must be kept very low. In others high volumes of data need to be transferred quickly.

To meet these requirements the BACnet committee incorporated several LANs into the BACnet standard. They chose existing LAN technologies whenever possible. In cases where LANs fitting the established criteria could not be found, the committee developed its own LANs. These LANs, listed in Table 1, cover a wide range from low cost to high performance.

BACnet LAN	**Standard**	**Data Rate**	**Packet[1] size**	**Cost**
Ethernet	ISO/IEC 8802-3	10 to 100 Mbps	1515 bytes	High
ARCNET	ATA/ANSI 878.1	0.156 to 10 Mbps	501	Medium
MS/TP	ANSI/ASHRAE 135-1995	9.6 to 78.4 kbps	501	Low
LonTalk[2]	n/a	4.8 to 1250 kbps	228	Varied

Table 1: BACnet LANs

Ethernet is a high-speed LAN which has been widely used for many years. By virtue of its popularity the expense of its interface has been dropping, though it still remains high compared to many other LANs. It offers a number of media alternatives such as twisted-pair, coax and fiber-optic cabling. Off-the-shelf interfaces for personal computer workstations are readily available and inexpensive, though the need for hubs and repeaters can increase the cost of the system.

ARCNET is popular with the process control industry. It is a lower-cost LAN than Ethernet, but requires dedicated communication integrated circuits (ICs) which keep its cost higher than some BACnet LANs. (It was on the basis of cost that ARCNET was chosen over otherwise competitive international LANs.) The ARCNET specification defines suitable media as including, but not limited to, coaxial, twisted pair (shielded and unshielded) and fiber optic cables.

The MS/TP (Master-Slave/Token-Passing) LAN was designed to make it possible for BAS manufacturers to build BACnet devices with the low cost necessary for BACnet's success in competing with proprietary LANs. By virtue of its simple interface and its communication rates MS/TP can be implemented on many standard microcontrollers without the added cost of dedicated communications ICs. The MS/TP LAN uses EIA-485 signaling over twisted-pair wiring.

MS/TP devices come in two varieties: Slaves and Masters. Slave devices are especially suited for the lowest-cost implementations but they lack the capability to initiate requests; they can only reply to messages from other devices. Master devices are able to initiate requests, but they must also be able to negotiate for a time slot in which

to make their requests. This adds some processing and memory requirements to the Master device which can result in higher cost than the Slave.

LonTalk was originally developed as a proprietary LAN; LonTalk devices used a special communications device which incorporated three microprocessors to handle the overhead. Recently it has been released as an open protocol. Although LonTalk was developed for the LonWorks protocol it provides a means for what it terms "foreign frame transmission."[3] The BACnet standard makes use of this capability of LonTalk for transporting its "foreign" frames.[4] LonTalk offers the greatest number of options in signaling media including RF, infrared, twisted pair, coax and fiber-optic cable.

INTERNETWORKING

It is frequently necessary to have multiple networks in a single BAS installation. There may be too many devices to be connected to a single LAN, or the requirements of the installation might dictate the use of different types of LANs for different functions.

When two or more networks are set up to communicate with each other the result is called an "internetwork." (The Internet is the best-known internetwork; it is composed of many smaller networks worldwide.) Internetworks may be comprised of similar networks linked together or, as in BACnet, they may contain different networks with different characteristics.

Internetworking in a building automation system allows the control engineer to keep the system's cost down by a couple of stratagems.

First, the small devices such as unitary controllers which make up the major portion of a BAS make a major contribution to the system's total cost by their sheer numbers. Since their communications requirements are small they typically connect to a LAN designed to have an inexpensive interface. Because such LANs have lower throughput, there is an effective upper limit to the number of devices which may be connected to any one such LAN. A larger building or campus may have several such LANs.

Second, a BAS may have devices such as operator workstations or file servers which need to transfer larger volumes of data than can be handled by the low-cost LAN. There are few such devices in any particular BAS and the cost of a high-performance LAN interface is small compared to the price of the device. By using both kinds of LANs, and selecting each for the characteristics which best match the building's requirements, the lowest-cost system can be achieved without incurring performance penalties.

This concept of mixing network varieties is not new. Many existing proprietary building automation systems are in fact internetworks comprising different types of LANs. BACnet, though, provides the control engineer with the flexibility of selecting the types of LANs to be used in a particular BAS for the lowest system cost.

The BAS designed for the very large Phillip Burton Federal Building in San Francisco demonstrates the effective use of these strategies. Low cost MS/TP LANs are used to communicate with the unitary controllers; each MS/TP LAN controls one or two floors. A high-performance Ethernet network is used as the "backbone," providing the communications between the operator workstations, the file and printer servers, and the MS/TP networks, as shown in Figure 1.

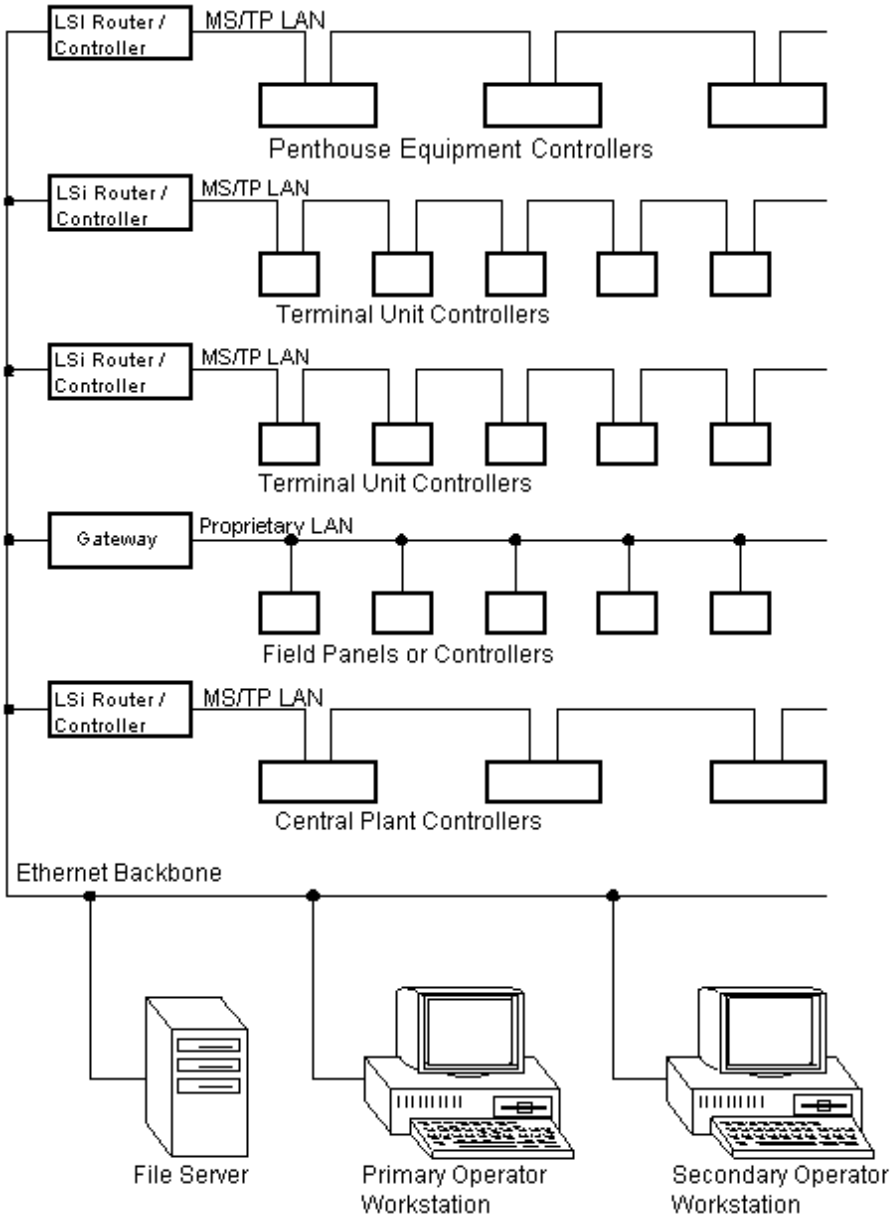

Figure 1: A large BAS internetwork

Such implementations need not exclude proprietary systems. As an additional demonstration of interoperability, a proprietary network will be installed in the Phillip Burton Building to control the HVAC on three floors. It will connect to the Ethernet backbone through a "gateway," a device which provides some BACnet access to the proprietary network's operations.

SEGMENTS, REPEATERS and BRIDGES

Each device on a LAN is connected to a signaling medium, typically a coax, twisted pair or fiber optic cable. There are physical (mostly electrical) limitations to the number of devices which may connect to a single cable, as well as a limit to the length of a single run of cable, called a "segment." The standards for the various networks define the means for extending the physical length of a network through devices called "repeaters" and "bridges."

When a repeater receives a signal from a network segment, it retransmits that signal on all the other segments to which it is connected. It may amplify and perform noise reduction on the signal, and it may even translate the signal to a different medium, such as from coax to fiber optic cable, but it is otherwise quite invisible to the internetwork.

Bridges are similar in function to repeaters but may also selectively pass or block a message packet depending upon the destination address within the network.

Figure 2 illustrates the operation of repeaters and bridges. It shows a single network with four segments connected by a repeater and a bridge. A message packet sent by the device with address 1 to device address 5 would also be seen (but ignored) by devices with addresses 3 and 20. If the bridge were programmed to not pass (in this direction) packets with destination addresses less than 100, the device with address 100 would not see the packet.

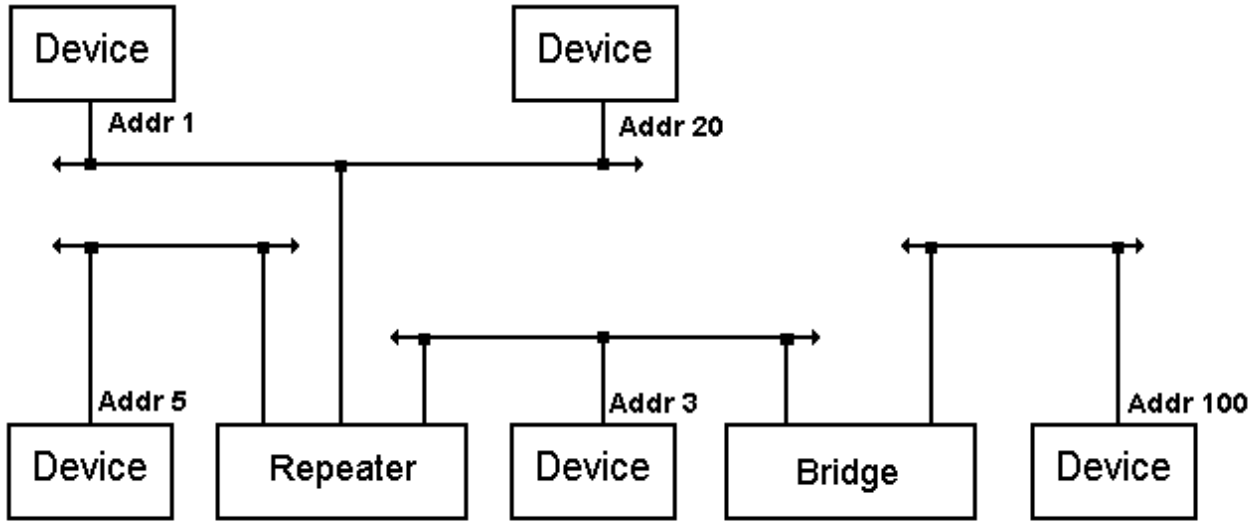

Figure 2: A local-area network connected by bridges and repeaters.

The cost of repeaters and bridges may be an additional factor in selecting and designing the layout for a LAN to be used in a BAS.

MAC and NETWORK ADDRESSES

The example of Figure 2 illustrated a message transfer within a single network. Message transfer in a BACnet internetwork is somewhat more complex and relies on each device's connection to a network having a unique address within the entire internetwork. This address is comprised of a pair of numbers.

The first number is referred to as the MAC (Medium Access Control) address, which must be unique on the network to which it is connected. The same MAC address may be used on a device on another network within the internetwork, in the same way house numbers can be the same for houses on different streets.

The device addresses shown in Figure 2 are MAC addresses. Typically one MAC address is reserved for use as a "broadcast" address. Each device on the network receives messages sent to the broadcast address as well as to its own MAC address. The MAC address is physically programmed into the device in some fashion, either by the manufacturer or the system provider.

The second part of every device's address is the number assigned by the system provider to the network to which the connection is made. This number is required to be unique throughout a BACnet internetwork. It is this number that will differentiate between devices with the same MAC number on different networks, to ensure that message packets traversing the internetwork arrive at the correct device.

ROUTERS

"Routers" are the devices which interconnect the component networks in an internetwork. Unlike most devices which contain a single network interface, routers connect to two or more LANs for the purpose of passing on messages coming from a device on one network and destined for a device on another.

Routers pass the messages only onto LANs which need to be crossed to get the message to its final destination. This ability to selectively forward the message is critical; without it the entire internetwork would soon be overloaded as each LAN's local traffic would be unnecessarily broadcast on every other LAN.

Routers act much like a mail-sorting facility. Each packet received by a router carries a destination address; the router examines the network number portion of the address and determines through which of its network connections, or "ports," the packet should be forwarded to reach the destination device.

If the destination address is a device on the LAN connected to that port the message is sent directly to that device. If the destination device does not reside on a LAN to which the router is connected, the message packet must be forwarded to another router which can deliver the packet to the destination device.

To keep network traffic down it is necessary for the router to determine which neighboring router can move the packet towards its destination. It must know which LAN that router is on (through which port it must send the packet) and what that router's MAC address is on that LAN.

This is accomplished by the use of "routing tables" in each router. Routing tables contain a list of network numbers in the internetwork with information on how to reach that network, including whether or not the network is directly connected to one of this router's ports. If it is the port is given; if not, the port through which the next router in that direction can be reached is listed along with that router's MAC address.

Routers are the only BACnet devices which know, or even need to know, the numbers of the networks to which they are attached. This simplifies the job of configuring a BACnet internetwork.

Figure 3 illustrates the use of routing tables in message forwarding. Router 1 receives the message destined for network 4, MAC address 8. It looks up network 4 in its table and finds it must forward the message to network 3, MAC address 5, which is Router 2. Router 2, upon receiving the packet looks in its table and finds that network 4 is directly connected, so it sends the packet to MAC address 8 on that network. Note that the device on network 3 with MAC address 8 does not receive the packet.

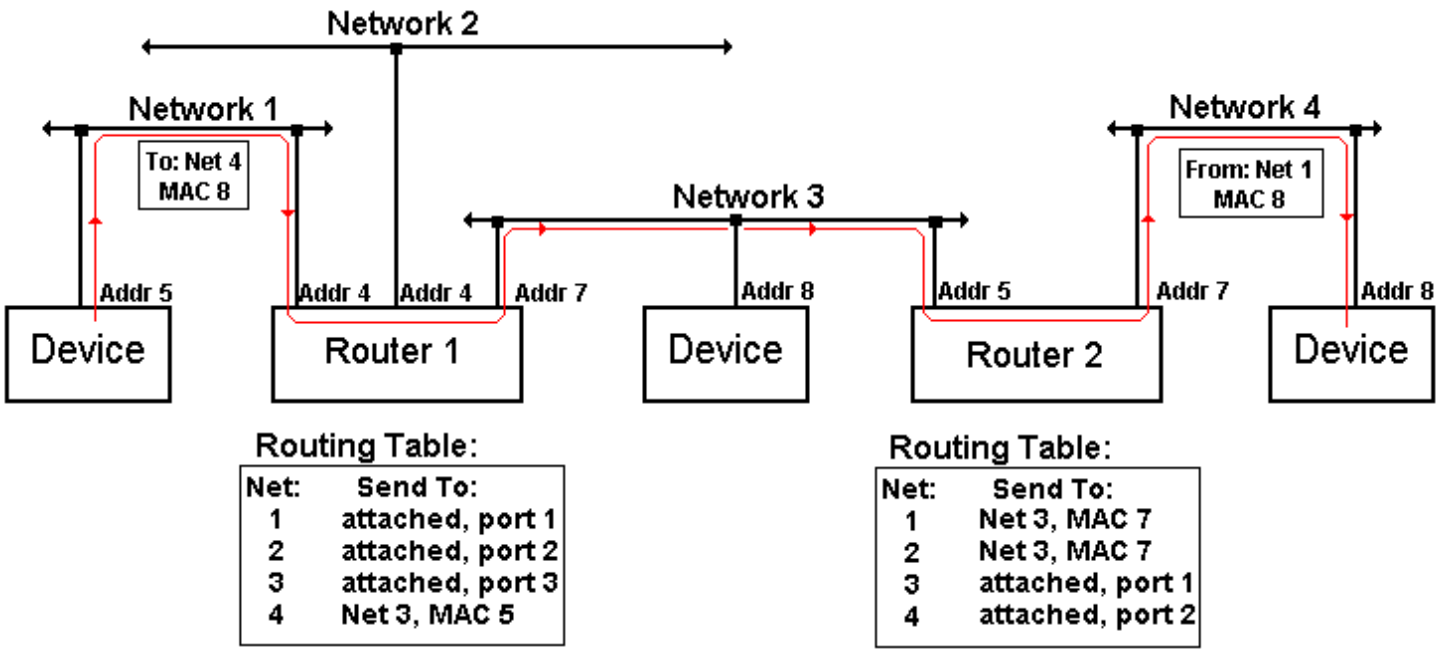

Figure 3: Message forwarding by routers.

Routers come in two varieties: "configured" and "learning." A configured router has its entire routing table set up in advance, typically with a commissioning tool. This can be a major task in setting up a large internetwork and an even larger task maintaining it, because every change in the internetwork configuration requires that many, if not

all, the routers must be reprogrammed before the internetwork can operate correctly. BACnet specifies that all routers shall be "learning" routers.

A learning router needs to be configured with only the network numbers and ports for the networks to which it is connected. The BACnet standard specifies "network messages" by which the routers can exchange information and automatically fill in the rest of their routing tables, even adjusting the tables as networks are added or removed from the internetwork.

It is important to note that the BACnet standard places a restriction on the topology of a BACnet internetwork: only one path may exist between any two devices on a BACnet internetwork. This greatly simplifies the task of the routers; they don't have to perform tests to determine the optimum routing of messages to other networks - a subject of ongoing debate for the Internet itself.

BACnet routers are not restricted to performing routing operations; it can be an efficient use of hardware to have the router device also perform higher-level BAS functions. One such application is a global controller device which monitors BAS devices on attached LANs to provide data-gathering and system coordination. In addition to its own communications with these devices it can also pass on messages from the backbone LAN over which it communicates with the file servers and workstations.

REMOTE DEVICE ADDRESS DETERMINATION

Devices which are about to send a packet on their local LAN need to know to which MAC address the packet should be sent. There are a couple means by which this can be automatically determined.

If the message packet is being sent as a response to a query from another device, the packet is simply returned to the MAC address from which it came. If the query was from another device on the same LAN, that MAC address is the final destination address.

If the query came from a device on another network, the MAC address belongs to the router which forwarded the request to this LAN, and which can return the reply to the sender. The router's MAC address, coupled with the full network address of the sender (which is present if the message came from another network), is sufficient information for the packet to be delivered to the proper remote device.

To send a query to a device on another network a BACnet device should know where the remote device is, as well as the MAC address on the local network of the router able to pass the message to, or in the direction of, the other network. This information could be manually programmed into the device, but normally devices able to initiate such queries will support the Who-Has and Who-Is Services.[5]

These services provide the means for locating a remote device by broadcasting a request for its identity; the reply from the device carries all the information necessary to send a packet to it. The request needs only the unique (internetwork-wide) identifying Device Number[6] of the remote device, or its Device Name. The Device Numbers or Names, of course, need to be entered into the requesting device as part of its configuration, but they eliminate the need to enter a sizable amount of routing informating.

The task of setting up a large (campus) BACnet internetwork can be simplified if a uniform numbering or naming system is established at the outset for the BACnet devices and networks. As an example of such a numeric encoding, one could assign digits of the Device Number to encode the device type, building, floor and room number. In this system, Device Number 1203412 might represent a unitary controller ("1") in building 203, floor 4, room 12. Device Numbers can be anywhere in the range of 0 through 4,194,303, which gives some flexibility to numbering systems. Network numbers should be assigned in similar systematic fashion to avoid accidentally duplicating numbers and to aid system maintenance.

MODEM CONNECTIONS AND HALF-ROUTERS

Not all communications between devices occur over LANs. The typical case-in-point is the dial-up modem connection used either for supervisory operations or for linking remote sites.

The BACnet standard supports this capability with its Point-To-Point (PTP) protocol which provides the means by which two devices may communicate directly with each other, without the overhead usually associated with LAN connections. This protocol provides a means for the two devices to establish a connection, exchange message packets (full duplex - in both directions simultaneously, for maximum efficiency), and to terminate the connection if desired.

The BACnet standard explicitly excludes any definition of the physical media over which the PTP protocol is used, but it readily supports EIA-232 or dial-up modem connections. With the latter in mind it also supports the implementation of password protection for the connection. The PTP protocol was also designed for the slower communication rates (9.6 to 56 kbps) typical of the EIA-232 or modem connections.

The PTP protocol is explicitly intended to be used for passing message packets from one network to another, just as a router does. Since each of the two communicating devices thus looks like a router to the network(s) to which it is connected, each of the devices is called a "half-router."

A PTP connection between two half-routers is shown in Figure 4. Router 1 is a full router with half-router (PTP) capability; it connects to two networks as well as a PTP port. Router 2 is simply a half-router; it has only one network connection.

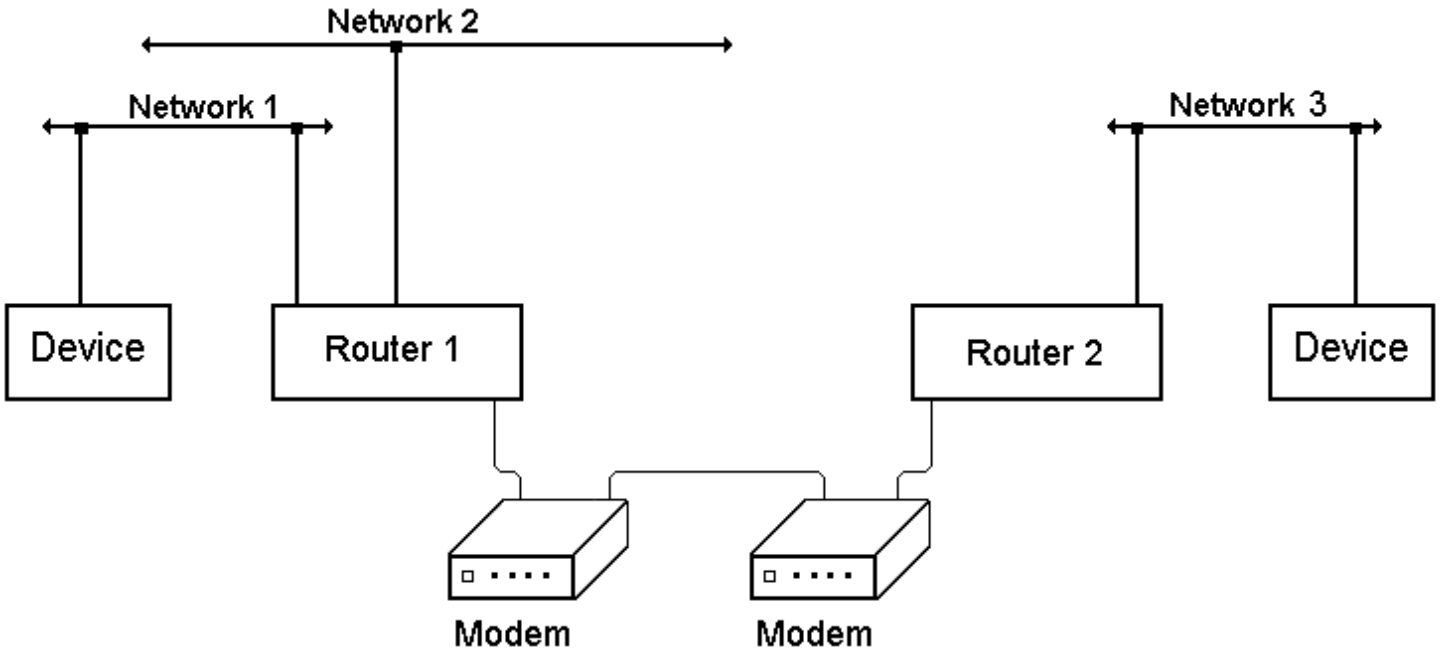

Figure 4. A PTP connection between two half-routers using modems.

Because the PTP connection is likely to be made over a toll connection such as the telephone network it will normally not be continuously active. The BACnet standard defines messages by which the half-router can report the status of its PTP connection to the routers on its "local" networks (those on the same side of the PTP connection as the half-router). It also defines messages by which the half-router can be instructed to establish or terminate the connection.

A PTP connection is established when a BACnet device needs to communicate with a device on a network on the other side of the connection. The initiating device sends out a request for information on how to reach that network; the half-router responds with a message stating that the network is the other side of a PTP connection. The initiating device then instructs the half-router to make the connection.

When the connection is made the half-router broadcasts that fact. It then transfers message packets it receives destined for networks on the other side of the PTP connection. The connection terminates on the occurrence of one of three conditions: the connection is explicitly terminated, the connection times out, or if the protocol discovers that multiple connections to the remote network exist.

LARGE MESSAGES and SEGMENTING

Some BACnet messages can exceed the packet size limits of any of its networks. The BACnet standard makes it possible to send an oversize message by "segmenting," breaking the message into chunks, or "segments," for transmission and then re-assembling it from the segments as they are received.

Segmenting is an optional feature for BACnet devices. It will usually be implemented in more complex devices such as field panels or workstations but might not be in the smaller unitary controllers which are less likely to need to send or receive large messages.

When a message segment is received, the receiver checks that the segment is intact before accepting it and sending an acknowledgement to the transmitter. The receiver can alternatively request that the sequence of segments be retransmitted, starting with the bad segment. This avoids the necessity of retransmitting the preceding good segments when a bad one is detected, thus reducing the amount of traffic on the internetwork when errors do occur.

To gain some performance in transferring segments, BACnet allows several segments to be sent and received before the reply is returned. The maximum number of segments which can be sent before a reply is received is called the "window size."

The degree of performance gain is somewhat dependent upon the "quality" of the networks. If the networks were perfect, if packets were never lost or delivered in the wrong sequence, the window size could be infinite. In the real world where packets are sometimes lost in transit[7], the window size needs to be lower. If internetwork transit times are small, window size can also be small.

Before a BACnet message is transmitted in segments the sending and receiving devices negotiate the mechanics of the transmission. They determine whether both sides support segmentation and what the window size will be (i.e., the smallest number supported by both devices). They also need to agree on the packet size; it will be the largest size that can be handled by both devices. If these negotiations fail an error message is generated because operator intervention will be required; some element of the BAS internetwork will need to be reconfigured.

It is very important to note that the BACnet standard presupposes a "normal" hierarchy of LANs. Any LAN or PTP connection forming a link between other LANs must be able to handle messages at least the size of the two others because the negotiating process does not account for message size in intervening networks.[8] (There exist proprietary means for resolving this problem.) An "inverted" architecture, such as a LonTalk LAN connecting an Ethernet and an ARCNET LAN, runs the risk of producing message packets which cannot be delivered.

SPECIFICATIONS and the PICS

The task of evaluating a device's networking capabilities has been simplified by the "Protocol Implementation Conformance Statement" (PICS) specified in the BACnet standard. The PICS, provided by the manufacturer of a BACnet device, identifies the manufacturer, describes the device and gives details of the implementation including the device's networking capability. Figure 5 gives an example of the portion of the PICS which describes the capabilities of a BACnet router.

Data Link Layer Option

ISO 8802-3, 10BASE5	ARCNET, coax star	MS/TP master: 9600, 19.2k 38.4k, 76.8k bps
ISO 8802-3, 10BASE2	ARCNET, coax bus	MS/TP slave
ISO 8802-3, 10BASET	ARCNET, twisted pair star	Point-To-Point, EIA 232, standard baud rates
ISO 8802-3, Fiber	ARCNET, twisted pair bus	Point-To-Point, modem, standard baud rates
	ARCNET, fiber star	LonTalk

Other

Character Sets Supported

Indicating support for multiple character sets does not imply that they can all be supported simultaneously.

ANSI X3.4 IBM/Microsoft DBCS JIS C 6226 ISO 10646 (ICS-4) ISO 10646 (UCS2)
ISO 8859-1

Special Functionality

Segmented Requests Supported	Yes	No	Window Size: 1
Segmented Responses Supported	Yes	No	Window Size: 1
Max APDU Length Accepted	1476 Octets		

Router

Describe the supported routing capabilities:
Router is auto-configuring; half-router is provided for Point-To-Point sessions.
Application layer functionality is provided for Global Controller capability.

Property Range Restrictions:

Figure 5. A router's networking PICS

SUMMARY

With any but the most limited internetwork there are issues to be considered in designing the network configuration to best fit the constraints of cost and performance. In the past many of these issues were resolved in predetermined ways by the manufacturers of proprietary BAS networks. Any resultant network inefficiencies may not have been apparent to the user.

With its open protocol and multiple manufacturers of interoperable equipment BACnet provides the possibility for a more completely optimized internetwork incorporating the various aspects of building automation systems.

---

1 The reader of the BACnet standard will encounter an almost bewildering array of acronyms for the message packet. The "packet" to which this refers is the NPDU (Network Protocol Data Unit), which consists of the actual message being sent plus a header containing the information necessary to deliver the packet over the internetwork. This portion of the actual transmitted packet appears the same on all LANs; the rest varies from LAN to LAN.

2 LonTalk® is a registered trademark of Echelon Corp.

3 *The LonTalk Protocol Specification, Version 3.0*, page 70.

4 A common misperception is that LonTalk devices are automatically compatible with BACnet. This is only true if the device on the LonTalk LAN communicates using BACnet messages.

5 See "The Language of BACnet", Engineered Systems, July 1996.

6 ibid.

7 Non-segmented messages can also be lost. The BACnet protocol provides means for automatically detecting a failure in transmission and

for re-transmitting the lost message.

8 A PTP connection has a maximum packet size of 501 bytes.