



This article was published in ASHRAE Journal, November 2010. Copyright 2010 American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc. Posted at www.ashrae.org. This article may not be copied and/or distributed electronically or in paper form without permission of ASHRAE. For more information about ASHRAE Journal, visit www.ashrae.org.

Broadcasting BACnet®

By **H. Michael Newman**, Fellow ASHRAE

Broadcasting is not evil. The concept of sending messages to all possible recipients on a network is a normal and extremely useful technique that is used by many different protocols, not just BACnet. Some of the most common network architectures, for example, the Internet Protocol (IP) on an Ethernet Local Area Network (LAN), would be incredibly hard to set up if it were not for the availability of broadcast messaging.

It is true that broadcasting, if not properly managed, can cause problems. But this is also true for many other network characteristics (address assignments, number of shared data points, point names, and so on). Still, broadcasting is often singled out as “problematic” even though, properly managed, it is not. This article will explain how broadcasting is used in BACnet and how to solve problems should they occur.

Some Networking Basics

Before we begin, a brief review of some fundamental network concepts may be helpful.

First, for computers to communicate they must know each other’s “address,” a numerical value assigned to each machine which must be unique on a given LAN. A message sent from *one machine to another* is called a “unicast” message. A message intended for *all* machines is called a “broadcast” message. A mes-

sage intended for a particular *group* of machines is called a “multicast” message. Each machine must be given its unicast address but knows, by virtue of its LAN type, what its broadcast address is. If a machine is also a member of a multicast group, that too must be configured into the device by some means or other. For the purpose of this article, we’ll focus on unicast and broadcast messages.

So how do LANs actually work? On a LAN, all devices are physically “within earshot” of each other, i.e., they all share a physical communication medium and can hear all the traffic on the network. At least that is the traditional notion. Today, with intelligent switches (that “learn” the addresses of the devices attached to them), a device may only hear traffic with its unicast address and broadcast messages. In any case, a device on a LAN can only *directly communicate with other devices on the same LAN*. For Device A to send

a message to Device B, it must know the LAN address of Device B.

But how does Device A find out the LAN address of Device B? There are only a few ways to do it. One is to have a local database that contains a list of all the devices and their addresses, a kind of “phone book.” Since most devices have a symbolic name, the table would really be like a phone book. Another way would be to send a message to the preprogrammed address of an address server, like calling directory assistance by dialing 411. It would be up to the address server to maintain the table of names and addresses. Both of these techniques require that the table be created by someone, somehow.

The last technique, and the one most commonly used, is to *broadcast* a request asking for the desired address. All the devices hear the request but only the one that is being requested answers, sending a unicast message to the requester with its own LAN address in the sender field. At that point, the two machines can converse at will. The beauty of this technique is that no address tables or databases need to be established and maintained.

But wait! I hear you saying “What do you mean my computer can only talk to

About the Author

H. Michael Newman is manager of the Building Automation and Control Systems Integration group in the Facilities Operations department at Cornell University in Ithaca, N.Y. He was chair of the BACnet Committee from 1987 until 2000 and is chair of the ASHRAE Standards Committee.


other devices on the same LAN? My computer is on an Ethernet LAN, and I can communicate with devices all over the world!” That may be true but to do so, it sends its messages destined for computers not on your LAN to a special computer that is connected to both your LAN and some other network. Also, your message has to contain some kind of address for the destination machine that the special computer can use to send your message. If the address is an IP address, then the “special computer” on your LAN is called an “IP Gateway.” Note that to communicate with the IP gateway, its IP address has to be known and added to your IP protocol information at configuration time. To find the LAN or “Medium Access Control” (MAC) address of the IP gateway, your computer uses the broadcast mechanism mentioned previously, which in the case of an IP device on an Ethernet network, is called the “Address Resolution Protocol” (ARP). This protocol is also known as RFC 826 (sidebar on *Creation of the Internet Protocol*).

Increasingly, for mobile computers such as laptops, another well-known broadcast method is used called the “Dynamic Host Configuration Protocol” (DHCP). In this case, the initiating device does not know its own IP address or IP gateway address. It broadcasts a message saying, essentially, send me my IP configuration details and, if there is a DHCP server that hears the request, a message is sent to the requesting device that allows it to configure itself.

BACnet Networks

Now, let’s talk about BACnet. At the BACnet committee’s early meetings in the late ’80s we had intentionally deferred the question of how BACnet messages would be conveyed. We focused, rather, on the content and format of the messages since we knew that networking technology was changing rapidly. The discussions on message transport continued up until the last moment. When BACnet was finally published in 1995, it included clauses on how to use four different LANs: Ethernet, ARCNET, LonTalk and Master-Slave/Token-Passing (MS/TP). The use of IP as a “virtual LAN” was not completely specified until Addendum *a*, which was also published in 1995, shortly after BACnet itself. The important thing to understand is that a BACnet “internetwork” is a collection of two or more of these LANs, which may consist of different LAN types, each of which is called a BACnet “network.”

Each LAN type has its own address format and protocol control information (PCI), the latter being items such as message length, error check digits, and so on. On Ethernet LANs, for instance, each device has a 48-bit unicast address that ranges from 0 to approximately 2.8×10^{14} . The address, made up of 48 1-bits, is the broadcast address for Ethernet. On an ARCNET LAN, a unicast address is an 8-bit number between 1 and 255. Address 0 is interpreted to be the broadcast address and messages



Creation of the Internet Protocol

The Internet was created in the late '70s and early '80s by a group of engineers and computer technicians who were working on projects for the government’s Defense Advanced Research Projects Agency. They needed to collaborate and, although they had computers, they had no established way of networking them.

So this early work to establish networking standards took the form of discussions by mail, telephone, fax and face-to-face meetings that led to varying degrees of consensus on how to solve the problems. This, in turn, led to someone taking on the task of writing up the various possible solutions in the form of specifications known as a “Request for Comment” or RFC. The RFCs were then circulated within the community and, eventually, became the law of the Internet land.

The Internet Protocol itself, for example, is also known as RFC 791 and was adopted in 1981. Other protocols mentioned in this article are also RFCs: the Address Resolution Protocol (ARP) is RFC 826; the Dynamic Host Configuration Protocol (DHCP) was originally RFC 1531 but has been superseded twice. The latest version is RFC 2131. All of these can be found on the web by entering “RFC” into any browser or at www.faqs.org.

But RFCs are not exclusively about 1’s and 0’s. Every so often one encounters a philosophical insight worth pondering. For example, the problem statement in RFC 826 contains this gem: “The world is a jungle in general, and the networking game contributes many animals.” No wonder networking can be confusing at times!

with 0 in the destination field must be processed by all machines on the LAN. LonTalk and MS/TP also use 8-bit addressing with the broadcast address being 0 and 255, respectively.

If a BACnet system consists of only a single network, life is simple. Device-to-device communication uses the unicast address and broadcasts use the broadcast address. But what if there is a need to interconnect multiple networks? How do

messages, whether unicast or broadcast, get from one to the other? Given that ARCNET and MS/TP networks only have 254 unicast addresses available, what if there is more than one device with a particular address? This is like a house with a street address of “100 Main Street,” of which there are many in the U.S. The answer, both for sending mail and for sending computer messages, is the same: add some additional piece of information that makes the address of the house or the computer unique. For the house, we can use a “zip code;” for the computer, we use a “network number.” The network number and MAC address pair uniquely specifies the address of a BACnet device.

So every BACnet network has a network number that must be unique within the internetwork. To get from Network 1 to Network 2, there needs to be a device that is connected to both. These devices are called “routers” and their functional details are defined in Clause 6, The Network Layer, of BACnet (Figure 1). Whereas the BACnet application layer protocol contains information about building automation and control functions (the subject of other discussions), the BACnet network layer protocol contains information about routing from one network to another.

The most significant elements of the network layer PCI are the source and destination network numbers, known as the “SNET” and “DNET,” respectively, and the source and destination device MAC addresses, known as the “SADR” and “DADR.” Clause 6 also defines the three types of BACnet broadcasts: “local,” “remote” and “global.” A local broadcast is received by all devices on the local network. A remote broadcast is received by all devices on a single remote network. A global broadcast is received by all devices on all networks comprising the BACnet internetwork.

BACnet Routing

To send a unicast message to a device on its own LAN, the sender simply omits the network layer address information and sends the message to the MAC address of the intended receiver. To send to a device “x” on a remote network “y,” the network layer DADR is set to “x,” the DNET is set to “y” and the message is sent to the router to network “y” on the sender’s LAN. To send a local broadcast, the sender just uses the LAN broadcast address. To send a remote broadcast, the sender sets the DNET to the network number of the desired remote LAN, omits the DADR and sends the message to the router to the remote network. To send a global broadcast, the DNET is set to all 1’s, the DADR is omitted and the message is broadcast on the local network.

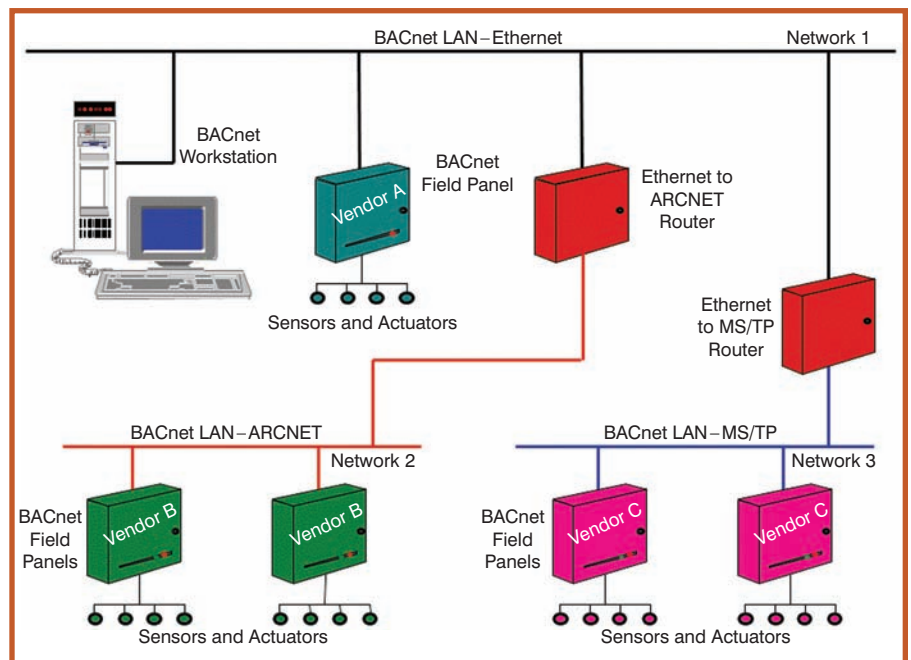


Figure 1: Different BACnet LANs are interconnected by routers that repackage BACnet messages and retransmit them unchanged.

How BACnet Uses Broadcasts

There are two main uses of broadcasts in BACnet: 1) transmission of “unconfirmed” application layer service requests; and 2) dynamic binding. Unconfirmed services are broadcast if they are intended for processing by multiple recipients. Such messages include routine change-of-value and event notifications, time synchronization messages, and Who-Is, I-Am, Who-Has, and I-Have. Unlike “confirmed” application layer service requests that are always sent to a single recipient and must always be explicitly acknowledged via a BACnet “ACK” message, unconfirmed messages are often sent to multiple recipients but are designed such that, if a response is desired, only a single recipient responds. Rather than sending a BACnet ACK, whose use is limited to confirmed services, the recipient responds by sending its own unconfirmed service request.

Here is an example drawn from a dynamic binding situation. Device A wants to communicate with Device B but does not know B’s address. A global unconfirmed “Who-Is” message containing the “Device Instance Number” (DIN) of B is sent and received by all BACnet devices in the system. Since DINs are required to be unique Internet-wide, only one device (hopefully) will respond to the message by sending an “I-Am” message indicating that it is Device B. From the MAC address and, possibly, network layer DNET and DADR parameters, Device A now has all the address information needed to communicate with Device B.

Network layer messages are also used for dynamic binding. The most common is the Who-Is-Router-To-Network message. As its name suggests, this message is used to find the address of the router to a specific DNET (or, if the DNET parameter is omitted, all routers to all networks). It is usually broadcast using

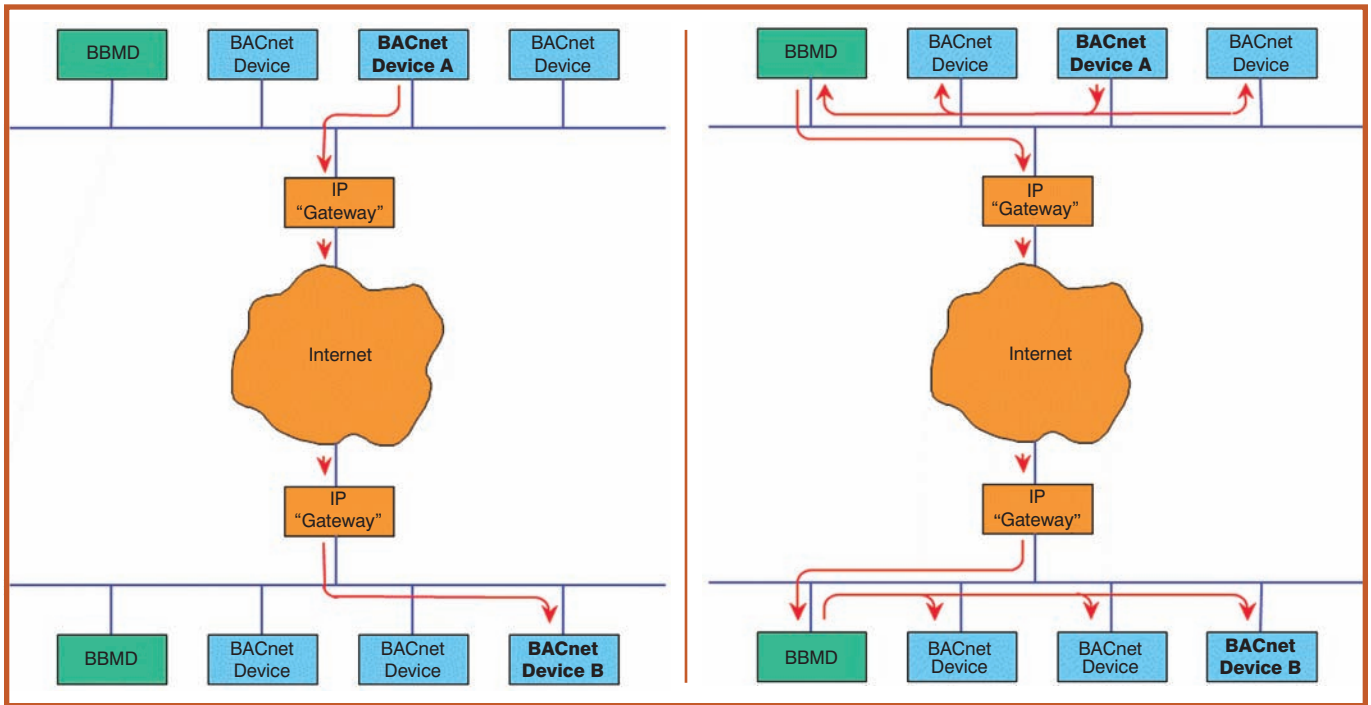


Figure 2 (left): Unicast messages, from Device A to Device B, are sent through the Internet using the IP address (and BACnet UDP port number) of the destination. The term gateway is in quotes because in BACnet terminology gateways translate to or from BACnet into some other protocol format. Using the BACnet terminology of today, IP gateways would properly be called IP routers. **Figure 3 (right):** BBMDs intercept Original-Broadcast-NPDUs and send them as Forwarded-NPDUs to the peer(s) in their Broadcast Distribution Tables. The remote BBMD sends the messages as Forwarded-NPDUs on its local network using the IP broadcast address appropriate for its IP subnet. The message appears twice on the source and destination networks—once as a broadcast and once as a BBMD-to-BBMD unicast.

the local LAN broadcast address but may be directed to a known router to learn the contents of its routing table.

Broadcasting in BACnet/IP (B/IP)

When it came time to take advantage of the wide-area routing capability of the Internet, we decided to implement the use of IP as if it were just a fifth kind of LAN so as to preserve all of the existing BACnet application and network layer mechanisms, including local, remote and global broadcasting. See BACnet Annex J. The combination of the 32-bit IP address and the 16-bit “User Datagram Protocol” (UDP) port number uniquely specify a device’s B/IP address, just like the MAC address of a true LAN. Since, in reality, there is still a true LAN involved (usually Ethernet) on which the IP traffic is carried, B/IP is referred to as a “BACnet Virtual Link Layer” (BVLL) and the functions needed by the BVLL to carry out unicast and broadcast messaging are called “BACnet Virtual Link Control” (BVLC) functions. While there are 11 BVLC message types in all, three are of particular importance here: Original-Unicast-NPDU; Original-Broadcast-NPDU; and Forwarded-NPDU. (NPDU stands for “Network Protocol Data Unit” and is just a fancy way to indicate the entire BACnet message that is being communicated by the LAN, in this case the virtual LAN.)

So how does B/IP work? For unicast messages, the data is just sent via UDP, using the BACnet port number, to the IP address of the recipient device as an Original-Unicast-NPDU using

the usual IP mechanisms (Figure 2). To determine whether the destination device is on the local subnet or on a remote one, i.e., whether the message may be sent to the destination device directly or must be sent to the IP gateway, the originating device uses a configuration parameter called the “subnet mask,” AND’s it with the source and destination IP addresses, and compares the results. If they match, the destination is local; if not it is remote. Any text on IP will explain this process in more detail (or, if you are a glutton for punishment, you could refer to RFC 791).

A challenge arises when a message is to be broadcast. Even though, for unicast messages, the entire Internet appears as one humongous LAN, it does not for broadcasts. Broadcasts are not allowed to pass through IP gateways since they could potentially reach every device on the Internet worldwide, causing untold congestion. The solution is to intercept the *broadcast* message and send it as a *unicast* message to a compatriot that then broadcasts it on the remote subnet. A broadcast interceptor of this sort is called a “BACnet Broadcast Management Device” (BBMD).

BBMD operation is actually quite simple. Each BBMD has a “Broadcast Distribution Table” (BDT) containing a list of its peers. When the BBMD sees an Original-Broadcast-NPDU, it sends it as a Forwarded-NPDU to its peers that then broadcast the message on their local subnet using the IP broadcast address for that subnet (Figure 3).

How to Solve Problems with BACnet Broadcasting

You might suspect that you have such problems if your BACnet network seems to be getting sluggish or devices seem to randomly go offline for awhile and then come back. These issues can be caused by excessive broadcast traffic sometimes rising to the level of a “broadcast storm” of hundreds of packets per second and, in every case I know of, *arise because of erroneous device configuration*.

Most of the problems I have seen manifest themselves on B/IP networks, so let’s focus on these. To find out why the excessive traffic is occurring, it is essential to find out what the nature of the broadcasts is and where they are coming from. For this, you need a tool called a “protocol analyzer” that lets you inspect and interpret the actual messages on the network. Several commercial ones are available, and you can also download an open source analyzer called Wireshark, which has very good BACnet filtering and decoding capabilities (www.bacnet.org/Developer#wireshark for details).¹

First, capture all the packets on the network for a few minutes. I generally turn off any capture filters because I don’t want to miss anything. Also note that if you connect to the network through a switch (as opposed to a hub), you will only see the broadcast traffic and any traffic specifically targeted to any devices also on the same switch port. Here are some broadcasts you might see:

1. UnconfirmedCOVNotification broadcasts. If you see a storm of these, it usually means that the Change-of-Value (COV) increment is set to 0 or other ridiculously low value for the quantity being measured. I have seen cases where the COV increment was so small that every scan of the quantity in question, e.g., an airflow of thousands of cfm that could easily change by tens of cfm between scans, produced an UnconfirmedCOVNotification. Since such scans often occur dozens of times per second, this can be a problem. Besides adjusting the COV increment, it may also be possible to use unicast messaging since there is nothing that requires unconfirmed messages to be broadcast.
2. Who-Is broadcasts. Who-Is messages should be rare. Devices are supposed to figure out how to communicate with their peers and store the address. But if a device can’t locate its peer, then it may continue to seek it out, hour after hour after hour. Usually this means that the sending device has an erroneous DIN for the peer or that the peer simply isn’t there. This can easily happen if a program is cut-and-pasted from one controller to another and the programmer has not updated network variable references. Find the references in the device’s program and fix them.
3. Who-Is-Router-to-Network broadcasts. These can occur for similar reasons to those cited in the previous item: the network number reference is invalid, or there is no router to the requested network. Again, cut-and-paste errors are frequently the cause.
4. Forwarded-NPDU broadcasts from more than one address. This means that more than one device is acting as a BBMD since forwarded NPDUs are only broadcast by BBMDs. Originally, only one BBMD was allowed per IP subnet and although this constraint was relaxed in Addendum o to BACnet-2008, most IP subnets still only have one. The problem can occur when a particular manufacturer’s system decides “to be helpful” and *automatically* instructs one or more of its devices to be a BBMD without the authorization of a human. This can create complete havoc since now broadcasts can have multiple paths between subnets, and loops can be set up whereby a broadcast on one subnet appears on another, is forwarded back to the original subnet by the rogue BBMD, *ad infinitum*. The most serious broadcast problem I personally have ever experienced was due to this cause. Track down the offending device(s) and turn off their BBMD functionality or fix their BDTs.

Communication is the key

Greystone is pleased to announce the release of our new line of CO₂ Detectors, Model CDD2 featuring BACnet® Communication

Features include:

- BACnet® Communication
- CO₂/Humidity/Temperature
- 5 Year Calibration Interval (CO₂)
- Optional on-board Relay
- Optional LCD Display
- Optional Setpoint Adjustment
- Optional Manual Override
- Decorative Enclosure

For more information on the CDD2 or other Greystone products, please contact us using the information provided below.



Here’s a sneak peak of our new wall mount enclosure design which will be available for our complete line of CO₂ sensors in early 2011



GREYSTONE
ACCURACY BY DESIGN
Greystone Energy Systems Inc.
150 English Drive, Moncton, NB
Canada E1E 4G7
(506) 853-3057 Fax: (506) 853-6014
North America: 1-800-561-5611
e-mail: mail@greystoneenergy.com
web site: www.greystoneenergy.com



Greystone Energy Systems Inc. is one of North America’s largest ISO registered manufacturers of HVAC sensors and transducers for Building Automation Management Systems. We have conscientiously established a worldwide reputation as an industry leader by maintaining leading-edge design technology, prompt technical support, and a commitment to on-time deliveries. We take pride in our Quality Management System which is ISO 9001 certified, assuring our customers of consistent product reliability.

Conclusion

The use of broadcast messaging is an important and time-honored technique, not just in BACnet but in many other common network technologies, but, like any powerful capability, must be carefully configured and managed.

References

1. Karg, S. 2008. “Analyzing BACnet.” *BACnet Today* supplement to *ASHRAE Journal* 50(11): B24–29.●