

# the **EXTENSION**

A Technical Supplement to Control Network

© 2008 Contemporary Control Systems, Inc.

## Introduction to BACnet® Routers

By George Thomas, Contemporary Controls

### Introduction

An interesting attribute of the Building Automation and Control Network (BACnet) is that Ethernet is supported along with several data links, and communication between the various data links is possible through the use of routers. Each data link is treated as a separate network and the collection of data links is considered a single BACnet internetwork. BACnet routers facilitate the connections — but when BACnet/IP is used as one of the data links, adjustments must be made to how BACnet routers are used in an IP network.

### BACnet's Four-layer Communication Model

Within the first few pages of the 600-page BACnet standard (ANSI/ASHRAE Standard 135-2004), the BACnet communications model is introduced as it compares to the Open Systems Interconnection — Basic Reference Model with its seven-layers. BACnet uses a collapsed architecture with only four layers. One of those four layers is the network layer (layer 3) and there is where routers live. Although many industrial automation communication architectures use the more simplified three-layer model, the BACnet community incorporated a network layer from the very beginning — even before the popularity of the Internet Protocol (IP).

in the form of “1s and 0s”. A good example of a repeater would be an EIA-485 repeater that extends two MS/TP segments. The data link layer is responsible for organizing the transmission of data in the form of frames from one station to another. Stations require addresses so that access to a shared medium is controlled. This is called **Media Access Control (MAC)** with each station being assigned a unique MAC address. A collection of MAC-level devices — each with a unique MAC address — comprise a local area network (LAN) or simply a network. Devices that connect the same data link technologies together and provide some MAC filtering are called bridges. Bridges maintain the integrity of the single MAC domain requirement and do not duplicate MAC addresses. A good example of a bridge is an Ethernet switch.

Assume you have two isolated Ethernet segments that you want to connect together. You can use an Ethernet hub which functions as a repeater or you can use an Ethernet switch that functions like a bridge. In both instances the integrity of the single MAC domain is maintained. Now suppose we want to connect an Ethernet segment to an ARCNET segment. The MAC domains are different and incompatible so both MAC domains must be treated as separate networks. BACnet

defines an **internetwork** as a collection of two or more networks interconnected by **routers**.

### Device Instance and Network Addressing

One requirement of BACnet is that a BACnet device address, called a **device instance**, must be unique within a BACnet internetwork. This means that regardless of the network location of the BACnet device, its

address must be unique. With a 22-bit address field allowing over 4 million possible addresses, this requirement should not be too hard to achieve. The BACnet application layer does not understand the concept of networks and therefore it is not necessary to assign a network number to a BACnet device. Only BACnet routers and the BACnet network layer need to know the 16-bit BACnet network numbers. With 65,534 possible network addresses plus one for broadcasts, there are

BACnet Layers

BACnet Application Layer				
BACnet Network Layer				
ISO 8802-2 (IEEE 8802.3) Type 1		MS/TP	PTP	LonTalk
ISO 8802-3 (IEEE 802.3)	ARCNET	EIA-485	EIA-232	

Equivalent OSI Layers

Application
Network
Data Link
Physical

Figure 1. BACnet supports several data links including Ethernet.

In Figure 1 you will find the BACnet communications model. Notice that BACnet supports several data links including Ethernet. The standard allows for the mixing of data links — which consequently requires the use of BACnet routers. Above the data links is the network layer, but this network layer is not the Internet Protocol. IP will be addressed later. BACnet devices attach to segments and segments are interconnected through the use of repeaters. Repeaters operate at the physical layer since they manipulate the symbols sent over the medium

plenty of possibilities. There is no address assignment for a BACnet internetwork. Although BACnet devices are uniquely defined, you still need to find them if they are located on a particular network. BACnet routers and devices generally work together to discover the location and MAC address of target devices through a procedure known as *dynamic device binding*.

## The BACnet Network Layer

According to the BACnet standard, the purpose of the BACnet network layer is to provide the means by which messages can be relayed from one BACnet network to another — regardless of the BACnet data link technology in use on that network. Devices that interconnect two networks together are called routers and their activities are called routing. When we are talking about routers, we are talking about layer-3 (network) functionality. Messages that are sent at the data link and physical layer are usually called frames — although BACnet uses the term **MAC Layer Protocol Data Unit (MPDU)**. At the network layer, BACnet sends out **Network Protocol Data Units (NPDUs)** which are shown in Figure 2.



Figure 2. An NPDU is comprised of a header and APDU payload.

Encapsulated into the NPDU is an **Application Protocol Data Unit (APDU)** which represents the BACnet payload. It consists of a header and service-related data. The NPDU has a header as well — and it is called the **Network Protocol Control Information (NPCI)**. The length of the NPDU depends upon the type of message and its destination. If the message is being sent from one BACnet device to another on a local bus involving no routers, the NPCI collapses to only two bytes. However, if a message is being sent to a remote device (a device on another network), the NPCI expands since the network layer must specify the destination network in the NPCI. When a router relays this same remote message to its attached destination data link, the source network is substituted for the destination network in the NPCI. The longest messages involve router-to-router communication where both source and destination network addresses are specified in the NPCI.

Usually one of the requirements of the network layer is to be able to route messages from one network to another over different paths. However, BACnet is explicit about this requirement; it does not allow it. There can be only one path between devices on the BACnet internetwork. Another requirement is message segmentation and reassembly. The maximum message lengths for the various data links differ — so it is possible a message will need to be broken into two or more packets, sent sequentially then reassembled at the other side. BACnet skirts this problem at the network layer by insisting that no segmentation occur at this level. It must be done at the application layer.

## Segmentation

Each data link has a **Maximum Transmission Unit (MTU)** specification that cannot be exceeded. A message larger than the MTU figure requires the message be broken into segments — each smaller or equal to the MTU of the receiving device. The receiving device is then obligated to put the segments back together in correct order for the message to be understood. This is called segmentation although the term fragmentation is often used. Unlike the IP protocol, the order of the segments is guaranteed since BACnet allows only one path between any two BACnet devices. The BACnet specification stipulates an MTU value of 501 bytes for ARCNET, MS/TP and Point-to-Point (see Figure 3). Ethernet has the largest MTU with 1497 bytes, while LonTalk has the smallest with 228 bytes. If an Ethernet device communicates with another Ethernet device, there should be no problem since each device is capable of receiving and transmitting the same size message. This assumes that the receiving device has allowed sufficient buffer space to receive the largest packets. However, there could be problems with a transfer from Ethernet to another data link — resulting in an error message. The source device could try again by segmenting the message which assumes the destination device supports segmentation. Note that with BACnet, segmentation occurs at the application layer and not the network layer.

Data Link Technology	Maximum NPDU Length (bytes)
IEEE 802.3 Ethernet	1497
ARCNET	501
MS/TP	501
Point-to-Point	501
LonTalk	228
BACnet/IP	1497

Figure 3. Maximum Transmission Units vary with the data link.

## Router Operation

Routers do not need to be stand-alone devices. Router functionality can be built into building controllers or other control equipment — and it frequently is. BACnet routers automatically build and maintain their routing tables based on network-layer communications with other routers. By definition, a router connects networks — with each connection called a port. Each port has a MAC address that is maintained in the router's routing table. Also included in the routing table are the network numbers of the two attached networks — as well as any remote network number that can be reached via each port. When a router first comes up, it broadcasts an **I-Am-Router-To-Network** message out each port identifying what network numbers are reachable from its other port(s). This allows other routers to update their routing tables. When a router receives a message it first checks the NPCI to see if a destination network number is specified. It then looks up the MAC address of the router that provides the path to this network number. If this search is successful, the message is forwarded. If not, a **Who-Is-**

**Router-To-Network** message is sent by the router to learn the route. If that is not successful, a **Reject-Message-To-Network** message is returned to the originator. Routed messages travel from router to router as directed messages until the routed message reaches its final destination network. If the originating message was a broadcast, the router will substitute the appropriate broadcast command for the attached data link and send it accordingly.

### The Impact of BACnet/IP upon BACnet Routers

As the popularity of TCP/IP exploded, the BACnet community needed a strategy for using the BACnet protocol in an IP world without a major re-write of the standard. The result was **BACnet®/IP (B/IP)** and it is described in Annex J of the 135-1995 through 135-2004 standards. The body of the BACnet standard makes exclusive use of MAC addresses for all data links. (This holds true for Ethernet as well.) But in the BACnet/IP world, IP addresses are needed. For BACnet/IP, Annex J defines an equivalent MAC address comprising of a four-byte IP address followed by a two-byte UDP port number. The BACnet community registered a range of 16 UDP port numbers as hexadecimal BAC0 through BACF. This port number must accompany both directed and broadcast messages sent by BACnet/IP devices. If, for some reason, two independent BACnet/IP networks are to share the same IP subnet, it is possible to change the UDP port number to another of the reserved ports in the range. BACnet/IP devices that share the same UDP port number are considered part of the same BACnet network — even if it is sub-netted. A second BACnet/IP network with a different UDP port number is deemed another BACnet network, just as an Ethernet 8802-3 or ARCNET or MS/TP segment would be. It should be noted that BACnet does not use TCP transmissions — instead relying upon connectionless UDP messages.

BACnet/IP incorporates the same four-layer ISO model as shown in Figure 1. Routers operate at the network layer. Since routers were already defined in “The Network Layer” (clause 6 of the standard), Annex J makes reference to this clause. Annex J introduces the concept of the **BACnet Virtual Link Layer (BVLL)** which provides an interface between clause 6 equipment and another communications subsystem. BVLL messages can be either directed or broadcast messages. A directed message is exchanged between two IP addresses and no others. A broadcast message originates from one IP address and is sent to all other IP addresses on the subnet.

In the general case, a BACnet network consists of one or more IP subnets containing BACnet/IP devices using the same UDP port number. It is possible the BACnet network has only a single subnet. This is the simplest case since both directed and broadcast messages are sent along the subnet with no restrictions. Refer to Figure 4.

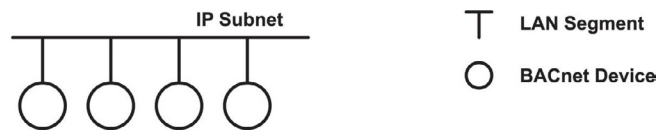


Figure 4. BACnet/IP traffic is unrestricted with one subnet.

However, if more than one subnet comprises the BACnet/IP network, there is an issue. Referring to Figure 5, an IP router is required to connect the IP subnet to the Internet or to an internetwork. IP routers perform differently than BACnet routers. Broadcast messages could be (and usually are) blocked by these IP routers if the IP routers do not support what is called a **directed broadcast**. For a directed broadcast to pass through the IP router, the IP router must support a feature called **bridging** in which the IP router treats these directed broadcasts more like a switch than a router. If this type of IP router cannot be found, then a way of managing broadcasts in a sub-netted BACnet/IP network must be devised.

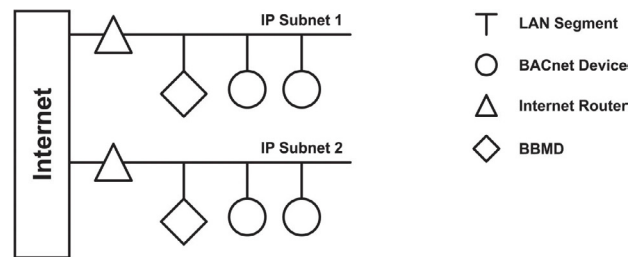


Figure 5. IP routers usually block broadcast messages.

### Directed and Broadcast Messages

The BACnet standard describes a **directed message** is a message sent from one device to another device within the BACnet internetwork. When it comes to **broadcast messages**, the standard defines three types. A **local broadcast** is a message sent from one device to all other devices on the same network. A **remote broadcast** is a message sent from one device on one network to all devices on another network. A **global broadcast** is a message sent from one device on one network to all devices on the internetwork. A BACnet/IP network with a shared UDP port number must function just like any other BACnet network in regard to directed and broadcast messages. If all devices are located within the same subnet, there is no problem sending or receiving either directed or broadcast messages since all parties to these messages face no communications restrictions.

Infrastructure devices such as hubs, repeaters, and switches do not interfere with the sending and receiving of directed or broadcast messages. But if a local broadcast message is sent to all subnets within the BACnet/IP network, there could be trouble if the IP routers do not support bridging.

## BACnet/IP Broadcast Management Device (BBMD)

With a BACnet/IP network comprised of two or more IP subnets, a local broadcast may not be able to span multiple subnets — if so, a device called a BBMD must be used. A BBMD located on an IP subnet monitors the origination of a broadcast message on that subnet and, in turn, constructs a different broadcast message **disguised** as a **directed message** in order to pass through an IP router. This disguised message is directed to other BBMDs (located on the various subnets) that receive the directed message and retransmit the broadcast on their attached subnets. Since the BBMD messages are directed messages, **individual messages** must be sent to **each** BBMD. Each BBMD device maintains a **Broadcast Distribution Table (BDT)**, the content of which is usually the same for all BBMDs within the network. BBMDs must know the IP address of all other BBMDs in the network. Note in Figure 5 that there is one BBMD on each subnet.

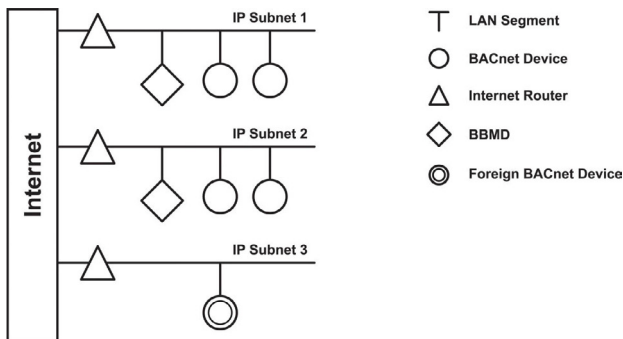


Figure 6. A foreign device can reside on a subnet without a BBMD.

It is possible to communicate to a device on a subnet that does not have a BBMD as in Figure 6. This type of device is called a **foreign device** since it resides on a different IP subnet from devices attempting to communicate with it. Usually in BACnet lingo, a foreign device is on a different network — but with BACnet/IP, a foreign device is on a different subnet. If the foreign device registers with the BBMDs, it can be party to communication with all other devices on the network. The BBMD must then maintain a **Foreign Device Table (FDT)**.

The final example is shown in Figure 7. In this case a non-BACnet/IP data link is attached via a BACnet router — creating two networks but one BACnet internetwork. This example demonstrates the flexibility of BACnet in that legacy data links or lower-cost data links can be supported along with more modern IP networks. There is nothing to preclude the embedding of a BBMD within the BACnet router — thereby eliminating one device on the subnet.

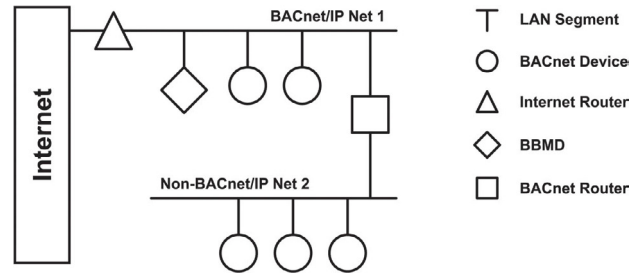


Figure 7. The addition of a non-BACnet/IP data link results in two networks.

## Summary

By providing network layer functionality into the BACnet stack, support for various data links was achieved through the use of BACnet routers. Annex J of the BACnet standard identifies the methods for attaching BACnet/IP networks to non-BACnet/IP networks while achieving interoperability. Although BACnet/IP provides some challenges, these challenges can be met by fully understanding the network architecture.

## Reference

**ANSI/ASHRAE 135-2004 BACnet — A Data Communication Protocol for Building Automation and Control Networks**, 2004, American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

## Acknowledgement

The author would like to thank David Fisher of PolarSoft for his assistance on this paper.

**CONTEMPORARY CONTROLS®**

www.ccontrols.com

Past issues of the copyrighted Extension are available. Please visit our web site [www.ccontrols.com](http://www.ccontrols.com). Select Support and click on Extension Archive.