



# Raising BACnet® to the Next Level

Connecting BACnet Devices  
to an IP Infrastructure

**George Thomas**  
**Contemporary Controls**

## Introduction

Few people understood what the Internet Protocol (IP) was before the Internet became wildly popular. IP is the heart of the Internet, and for Building Automation Systems (BAS), IP is becoming increasingly important. That was not the case in the last decade of BACnet development in which several data link technologies were included — including Ethernet. But Ethernet is not IP, although it works well with IP networks. The BACnet community recognized the need for a convenient method of attaching to IP networks in a meaningful way with the release of BACnet/IP, but many legacy BACnet devices exist and non-IP BACnet devices continue to be produced everyday. This paper reveals how all BACnet devices can effectively share a common IP network — thereby enhancing the power and convenience of BACnet.

## Why the Internet Protocol?

Why are BACnet Plugfest participants encouraged to attach to an IP network when testing for interoperability? Why at trade shows are IP networks used for interoperability demonstrations? It is because connecting to an Ethernet backbone running the IP protocol is convenient. Attempting to do the same with a BACnet MS/TP bus network is not as convenient. IP is important for reasons other than convenience. Building automation systems and information technology (IT) are

quickly converging with both areas sharing a common IP network. This IP network is the quickest way to gain access to the Internet which is the world's wide-area-network (WAN). All modern communication networks are IP-based even if communication is restricted to Local-Area-Networks (LANs). Modern buildings are designed and built with structured wiring in mind—with integrated telephone and data wiring that can operate at Gigabit Ethernet speeds. Why run proprietary fieldbus networks when structured cabling is already in place? Even non-BACnet building automation systems are connecting to IP — including access control systems, security systems, life-safety systems, and lighting systems. LON-based systems are using the IP networks as a tunnel, taking advantage of “free” wiring. When we think of IP networks we think of Ethernet with speeds of 10, 100 or 1000 Mbps running over CAT 5, CAT 5e or CAT 6 twisted-pair cabling. These same speeds can be achieved over multimode or single-mode fiber optic cabling as well. Granted, the higher speed connections are wired, but there are plenty of wireless technologies

that attach to IP networks. It is clear that the backbone of choice is IP.

## BACnet and Its Flavors

Building Automation and Control Network (BACnet) protocol was introduced in the mid-90s using four of the seven layers of the Open Systems Interconnection (OSI) model as shown in Figure 1. At the lowest level of the model is the physical layer which is concerned with sending symbols representing binary data across a medium. The highest level is the application layer which defines the *meaning* of the data as it is sent between stations. This is where BACnet objects and properties are defined. After surveying what BAS vendors were providing at the time, the BACnet committee of the American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE) decided to support five data links—Ethernet, ARCNET, Master-slave/Token-Passing (MS/TP), Point-to-Point protocol (PTP), and LonTalk. A data link defines how stations are addressed and how data in the form of frames are sent between stations within a Local-

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

Figure 1. The BACnet four-layer model supports several data links including Ethernet.

Area-Network (LAN). A set of similar stations within one data link constitute a network. Stations with incompatible data links cannot communicate to one another at this level. Since interoperability between the various data links was a goal of the BACnet SPC 135 committee, the BACnet Network Layer was introduced, completing the four-layer model.

### **BACnet/Ethernet**

IEEE 802.3, now an ISO standard, refers to part 3 of the Institute of Electrical and Electronics Engineers' 802 standard entitled *Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*. However, we typically call this 1500 page standard Ethernet. Ethernet, along with a Logical Link Control (LLC) as defined in ISO 8802-2, forms a data link that can operate at speeds of 10 Mbps, 100 Mbps and 1 Gbps. Ethernet's physical layer includes several copper and fiber options such as 10BASE2, 10BASE5, 10BASE-FL, 100BASE-TX, 100BASE-FX, and 1000BASE-T. Any of these options can be combined in one piece of equipment and each is compliant with BACnet/Ethernet. Ethernet provides for greater speed, star topology, and transformer-isolated transceivers. However, BACnet/Ethernet is not the same as BACnet/IP Ethernet. With BACnet/Ethernet, LAN addressing is accomplished using the Ethernet's media access control (MAC) address. The MAC address is the 48-

bit worldwide unique value given to every Ethernet controller chip and not the 32-bit IPv4 address we would expect with an IP/Ethernet device. Of all the BACnet data links, Ethernet provides the greatest speed.

### **BACnet/ARCNET**

Like Ethernet, ARCNET can be classified as having both a data link and physical layer. ARCNET's data link and physical layer options, which include support for coaxial, twisted-pair and fiber optic cabling, are described in the ARCNET Trade Association's ATA 878.1-1999 standard. Data rates range from 156 kbps to 10 Mbps. Unlike Ethernet, ARCNET uses a deterministic token-passing protocol, thereby providing improved real-time performance. The ARCNET controller chip is treated as a communications coprocessor, relieving the main processor from handling token-processing duties. One of the ARCNET physical layers is the inexpensive EIA-485 standard which will support 32 stations in a bus configuration. Bus topology is less expensive than star topology since no hub is required. However, troubleshooting a bus problem is more difficult than troubleshooting a star problem.

### **BACnet MS/TP**

Master-slave/token-passing remains a popular BACnet data link with baud rates from 9.6 kbaud to 76.8 kbaud. It provides its own logical

link control to BACnet's network layer. Like ARCNET, MS/TP uses a token-passing protocol, but it is implemented in software using a serial port on a microcontroller. MS/TP relies upon a very common physical layer called 2-wire EIA-485. EIA-485 transceivers are relatively inexpensive and typically found in low-cost controllers. They can drive long lines and can operate at the required upper limit data rate of 78.6 kbaud. Two versions of EIA-485 transceivers are found in the BAS industry — isolated and non-isolated. With isolated transceivers, there is no galvanic connection between signal ground on the transceiver and circuit common of the BACnet device. The network connection requires three wires and not two since the signal common must be carried between isolated devices. With a non-isolated transceiver, only two wires are carried because there is only one common (circuit common of the BACnet device is the same as the transceiver common). With non-isolated devices, more care is required when interconnecting devices since the ground potential must be the same at each device in the network.

### **BACnet/PTP**

The Point-to-Point protocol is mainly used to tie modems into BACnet networks. A serial port on a micro-controller is used for communication and a simple EIA-232 interface is used between the serial port and modem.

### BACnet/LonTalk

This implementation is seldom found and will not be discussed.

### BACnet/IP

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)** which is described in Annex J of the BACnet standard. The body of the BACnet standard makes exclusive use of MAC addresses for all data links, including Ethernet. 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.

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 BACnet 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. A directed message is exchanged between two IP addresses and no others. A broadcast message originates from

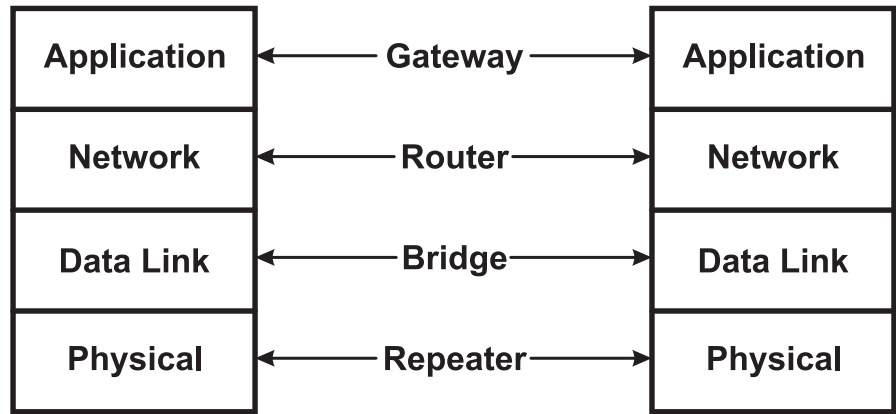


Figure 2. The role of infrastructure equipment depends upon the communications level.

one IP address and is sent to all other IP addresses on the subnet.

### Infrastructure Equipment

In order to understand how infrastructures are built, you need to understand the role of infrastructure equipment. Figure 2 shows the four-layer communications reference model that BACnet uses — with infrastructure equipment associated at each level.

### Repeaters

As mentioned before, the physical layer is concerned with the transmission and reception of symbols representing binary data sent across the medium. A repeater is used to simply link together two cable segments to make a longer run. A good example is a 2-port EIA-485 repeater used to extend MS/TP or ARCNET cable lengths. An example of a multi-port repeater is an Ethernet repeating hub. A media converter is used to change one medium to another such as from copper cabling to fiber optic

cabling. All these devices operate on the symbols sent over the wires. They provide low latency but do not understand protocols or even the data link under which they operate. These are very simple devices. In the case of Ethernet repeating hubs and Ethernet media converters, they reside within a single Ethernet collision domain which limits the maximum network diameter.

Ethernet operates on the CSMA/CD principle. A station that wants to initiate a transmission first waits to hear if the channel is clear. If it appears to be clear, it initiates the transmission while continuing to observe if the transmission was successful as evinced by a lack of a collision from another transmitting station. If a collision is detected, all parties that initiated a transmission will back-off for a random time and then try again. In order for this collision detection mechanism to function, all stations must reside within one collision domain — defined as twice the time for a transmission to be sent between the two most distant nodes.

This time constraint defines the collision domain which in turn limits the geographic size of the network. This limit is called the **maximum network diameter**. This is a potential issue when cascading repeating hubs or using fiber optics and, therefore, Ethernet repeating hubs are seldom used except at BACnet Plugfests.

Because a single Ethernet collision domain is shared by all stations, it is possible to view all traffic at any point in the network. This is very useful when troubleshooting protocols since a network analyzer can be attached anywhere within the network. This is called shared Ethernet. Besides geographic limitations, shared Ethernet restricts operation to a single data rate and half-duplex. Although bi-directional transmissions are allowed, they are not allowed at the same time.

## Bridges

One step up the reference model is the data link layer which is the home for bridges. Bridges link two or more of the same data links together with the best example being an Ethernet switch. An Ethernet switching hub is fundamentally different from an Ethernet repeating hub. A switching hub operates upon the frames sent from Ethernet stations or from other Ethernet switches.

In the normal mode of operation, a complete frame is received on one port of the switch before it is sent out to all other ports on the switch.

This is called **store and forwarding**. No forwarding occurs at the port where the frame was received. Therefore, a switch has much more latency than a repeater because it must wait until the complete frame is received. Although an Ethernet repeating hub is part of the Ethernet collision domain, an Ethernet switch terminates an individual collision domain at each of its ports. Therefore, cascading switches does not limit the physical Ethernet network like repeating hubs. Much greater distances can be achieved with switches than with repeating hubs. A switch can also operate in full-duplex mode — assuming its link partner is full-duplex compatible. Full-duplex can effectively double the throughput. With switches, there is potentially no restriction on data rates. Different ports on the switch can operate at different data rates.

There is another advantage to switches. A switch learns the location of Ethernet stations by noting in its database the MAC address of each station initiating a transmission and noting at which port the transmission was received. This process is called **learning**. This MAC address/port number combination remains in memory so that the switch will know to which port it should direct transmissions destined to a particular MAC address. When a switch receives a message with a destination MAC address recorded in its database, it will forward the message only from the port with the associated MAC address. This reduces traffic on the

network by restricting transmissions to only those ports party to the transmission. This process is very efficient as long as all transmissions are unicast or directed messages — where the transmission is from one station and directed to another. With broadcast transmissions, all stations must hear the transmission so the transmission is flooded to all ports on the switch. In this situation the switch functions much like a repeating hub. To allow for topology changes, the database is periodically cleared and the location of MAC addresses is re-learned. This process is called **aging**.

Switches are commonly used in Ethernet networks since their benefits far outweigh their shortcomings. Their greatest inconvenience is when attempting to troubleshoot network protocols — since network traffic does not appear on all ports of a switch.

## Routers

At the network level there are routers that link networks together to form an internetwork. Instead of individual frames, routers operate upon **packets**. The most famous internetwork is the Internet and the most famous network layer protocol is the Internet Protocol. The Internet is a public network, but it is not necessary to have access to the Internet in order to construct an IP infrastructure. Using the same Internet Protocol and the same IP infrastructure

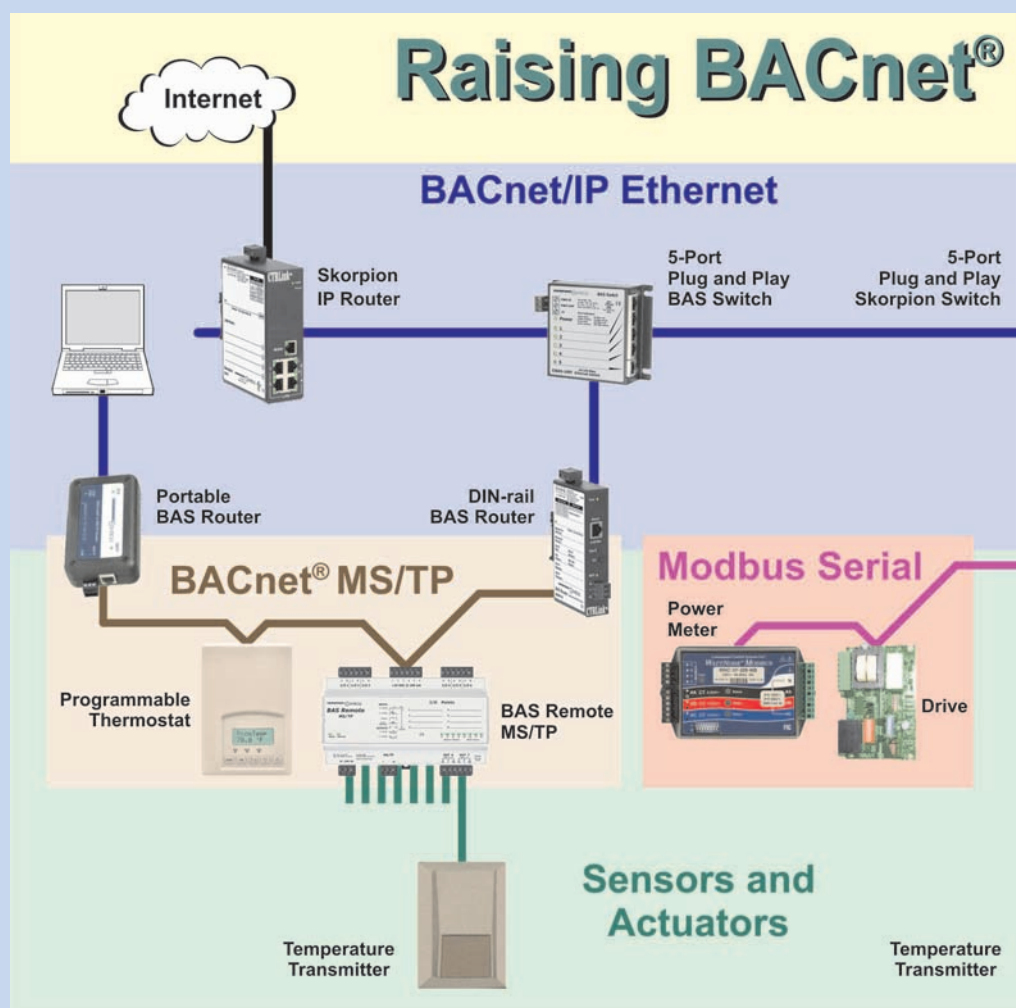
*Continued on page 6*

## Contemporary Controls' Approach to the Challenge of Connecting BAS Equipment to an IP Infrastructure

Although it is easy to delegate infrastructure equipment decisions to the information technology (IT) department, IT personnel are frequently unfamiliar with building automation equipment requirements. Besides, not all equipment is IP-compliant. For example, most commercial IT infrastructure equipment is mains-powered while BAS equipment is 24 VAC/VDC powered using Class 2 wiring methods. The sharing of a single control transformer in a control panel requires all powered devices to have half-wave power supplies. BAS equipment is usually mounted directly to a sub-panel or DIN-rail mounted in a control panel, while commercial IT equipment is either table-top mounted or rack-mounted in wiring closets. Locating BAS equipment in wiring closets is not convenient or practical. Contemporary Controls' products address the required IT standards, but are designed with building automation needs in mind. The result is a neat, professional-looking installation, worthy of the effort — while complying with the performance and regulatory requirements of the job. What follows are some example products.

### Portable BAS Router

Convenient for commissioning and troubleshooting, the Portable BAS

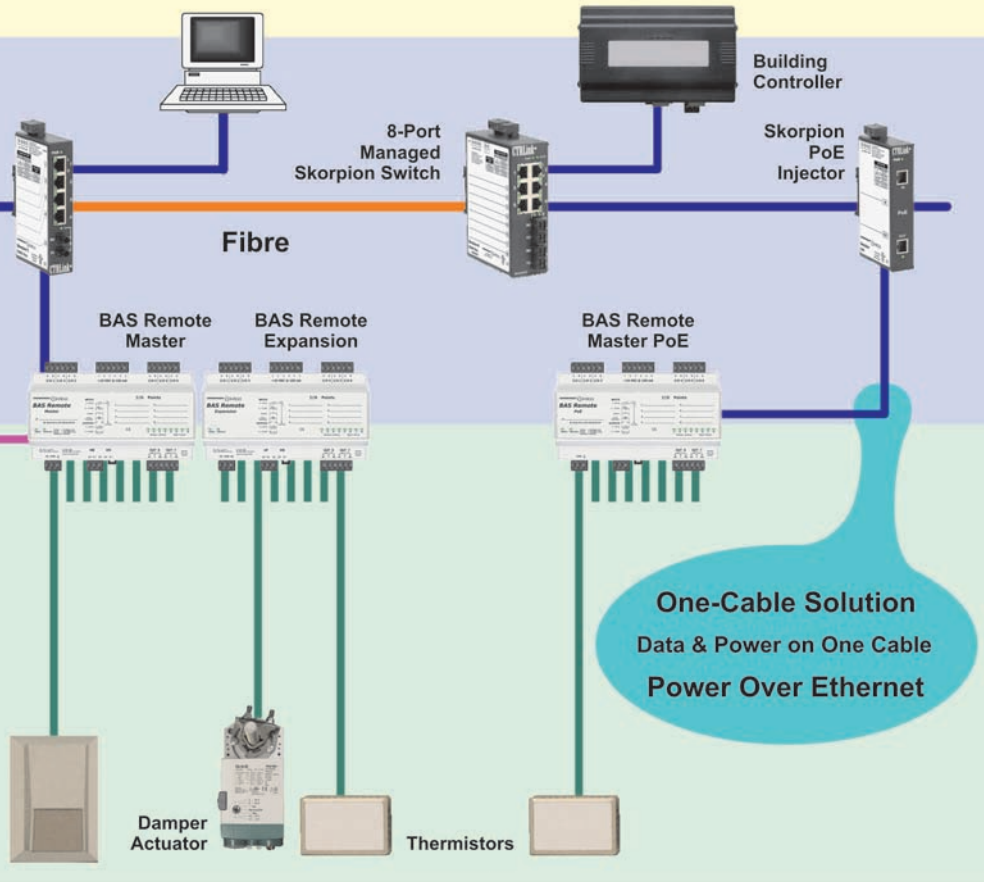


Router provides connectivity between a BACnet/IP Ethernet client residing on a laptop to BACnet MS/TP devices located in the field. Power for the router is derived from the laptop's USB port, but all communication is via the laptop's Ethernet port. An optically-isolated MS/TP port is capable of handling baud rates up to 76.8 kbaud. Configuration is via a web page. Modern commissioning tools are Ethernet-based, so a portable Ethernet device that allows attachment to a MS/TP network is an indispensable device to keep in the tool box.

### DIN-rail BAS Router

For permanent installations, the DIN-rail BAS Router provides a low-cost method of connecting isolated islands of BACnet MS/TP devices to a BACnet/IP Ethernet network. The half-wave rectified low-voltage power supply allows for the sharing of power with other 24 VAC/VDC control devices. The MS/TP port is optically-isolated and is capable of handling baud rates up to 76.8 kbaud. Built-in End-of-Line (EOL) termination and bias can be disabled for mid-span MS/TP installations. The BAS Router supports BACnet/IP Broadcast Management Device (BBMD) and Foreign Device (FD) registration —

# to the Next Level



troubleshooting. Unlike office-grade Ethernet equipment not adaptable to control panels, the BAS Switch makes an Ethernet installation neat, professional, and dependable.

## 5-Port Plug-and-Play Skorpion Switch

For control panels where DIN-rail space is at a premium, the Skorpion series of plug-and-play Ethernet switches with widths as little as one inch (26 mm) is the answer. Housed in a rugged metal enclosure with a metal DIN-rail clip, the Skorpion series includes models with 5, 8 and 16 ports. Some models provide one or two-ports of either single-mode or multimode fiber optics with either SC or ST connectors. No configuration is necessary. All copper ports automatically configure their data rate and duplex using the Auto-negotiation protocol. Depending on the capability of the link partner, communication is established at either 10 Mbps or 100 Mbps and at either half- or full-duplex. Each port will adapt to either a straight-through or crossover cable by using the Auto-MDIX protocol. Fiber ports are fixed at 100 Mbps full-duplex for the highest performance. Multimode cable lengths cannot exceed 2 km and single-mode lengths cannot exceed 15 km without a special order. Fiber optics is ideal for inter-building cabling in a campus environment.

The half-wave rectified low-voltage power supply allows for the sharing of power with other 24 VAC/VDC control devices. LED indicators of

thereby allowing the linking of BACnet devices over a sub-netted IP network. Configuration is via a web page.

## 5-Port Plug-and-Play BAS Switch

The BAS Switch is ideal for low-cost 10/100 Mbps Ethernet switching applications where equipment is mounted in shallow-depth control cabinets. No configuration is necessary. Each port automatically configures its data rate and duplex using the Auto-negotiation protocol. Depending on the capability of the link partner, communication is established at

either 10 Mbps or 100 Mbps and at either half- or full-duplex. Each port will adapt to either a straight-through or crossover cable by using the Auto-MDIX protocol. There is no need to stock crossover cables for switch-to-switch cabling. The BAS Switch is housed in a rugged metal enclosure and can be either panel or DIN-rail mounted. A writable label on the unit allows for documenting the location of field devices connected to each port. The half-wave rectified low-voltage power supply allows for the sharing of power with other 24 VAC/VDC control devices. LED port indicators of data rate and activity are prominently located to assist in

data rate and activity assist in troubleshooting. For control panels of nominal depth, the Skorpion series offers the widest range of Ethernet connectivity solutions.

### 8-Port Plug-and-Play Managed Skorpion Switch

The next big step-up from a plug-and-play switch is a fully-managed switch. The industry considers a managed switch as one that complies with the Simple Network Management Protocol (SNMP) and retains a Management Information Base (MIB) that provides detailed analysis of port status. The SNMP switch functions as an agent for a manager functioning as a client on the network. A trap can be set by the agent and reported to the client when an exception occurs. Although this functionality is seldom used in a BAS environment, the installation of managed switches may be mandated by IT departments. The Managed Skorpion series is a cost-effective solution in meeting the needs of IT department requirements.

Because of the sophisticated Ethernet controller chips used in managed switches, several useful features are available that have nothing to do with the SNMP protocol.

**Virtual Local Area Network (VLAN)** — VLANs allow for the separating of network traffic while sharing the same network infrastructure. This is ideal for BAS where all BACnet traffic is relegated to an assigned VLAN while other IT

traffic is restricted to other VLANs. This eliminates the need to pull separate network cabling for the BAS system because the BAS traffic can be carried by the building's structured wiring system.

**Cable Redundancy** — Protocols such as Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) allow for Ethernet networks to be cabled in either a ring or mesh topology. Proprietary ring protocols such as Contemporary Controls' RapidRing allow for fast recovery in a ring topology. Cabling redundancy adds another layer of robustness to an Ethernet-based BAS system.

**Quality of Service (QoS)** — The priority of messages can be assigned when switches support QoS, allowing more important messages to be sent ahead of those with a lesser priority. A priority field within a VLAN tag is appended to messages sent between switches. By reading the priority field, the switch understands what messages take precedence. Each port on a managed switch can be configured for a particular level of priority so that the simple connection of a cable to a port sets the level instead of VLAN tags.

### Skorpion IP/Ethernet Router

In order to interconnect two IP networks, an IP router is required. The Skorpion IP/Ethernet router combines the functionality of an Ethernet switch and that of an IP

router. On the LAN side of the router is a four-port 10/100 Mbps unmanaged Ethernet switch that supports both Auto-negotiation and Auto-MDIX. On the WAN side is a single 10/100 Mbps Ethernet port. Not only does the Skorpion IP/Ethernet Router transfer packets between the LAN and WAN sides of two networks, it provides a stateful firewall to protect the LAN side from unauthorized intrusions. The router is configured through its web page — where a host of features allow secure access to Wide Area Networks (WANs) such as the Internet.

**PPPoE Protocol** — External Ethernet to DSL modems that support the PPPoE protocol are directly supported — allowing easy access to the Internet through an Internet Service Provider (ISP).

**Dynamic Host Configuration Protocol (DHCP)** — On the LAN side, a DHCP server can provide private IP addresses to attached stations. Address assignments can also be fixed with a one-to-one mapping of MAC Ethernet addresses to IP addresses. On the WAN side, a DHCP client can request a public IP address or the IP address can be pre-defined.

**Network Address Translation (NAT)** — A one-to-one mapping of LAN-side client IP-addresses can be made to WAN IP-addresses — allowing stations on a private network access to the Internet.



### **Port Address Translation (PAT)**

— If public IP-addresses are limited, then PAT can be used. With PAT, one public IP-address is shared by a number of private IP-address on the LAN side by using individual port number assignments.

### **BAS Remote**

The BAS Remote is a utility device that can provide additional input/output capability, routing and gateway functionality in a Euro-style DIN-rail mounted enclosure. There are several models.

### **BAS Remote Master**

The BAS Remote Master is BACnet/IP compliant device conforming to the Application Specific Controller (B-ASC) profile. It is a remote I/O device that allows sensors and actuators to be accessed from an IP network. It also functions as a Modbus serial router to a Modbus TCP device. Finally, it is a gateway between Modbus serial and BACnet/IP.

A 10/100 Mbps auto-negotiating Ethernet port connects to the IP infrastructure. Its IP address can be static or dynamically assigned through a DHCP server. Six points of universal input/output points can be configured through a web server. Points can be configured for contact closure inputs, pulse inputs, 0–10 VDC or 0–20 mA analog inputs, or 0–10 VDC or 0–20 mA analog outputs. There are two contact closure outputs. An EIA-485 2-wire interface provides access to Modbus serial devices. Modbus registers

from attached devices or from the BAS Remote's internal I/O can be mapped to BACnet objects or simply presented as Modbus TCP. The BAS Remote is ideal for accessing non-BACnet compliant devices from an IP infrastructure when no convenient fieldbus wiring exists. A half-wave 24 VAC/VDC power supply allows for the sharing of power with other half-wave devices. The internal 24 VDC power supply of the BAS Remote is made available for powering 4–20 mA transmitters and other pilot devices.

### **BAS Remote Expansion**

Up to three BAS Remote Expansion modules can be connected to a single BAS Remote Master using a proprietary serial port—increasing the universal input/output count to 24 points and the relay output count to 8. A convenient 24 VDC power connection is provided for powering transmitters. Like the BAS Remote Master, the expansion modules are powered from a 24 VAC/VDC supply.

### **BAS Remote MS/TP**

The BAS Remote MS/TP is BACnet MS/TP compliant device conforming to the Application Specific Controller (B-ASC) profile. It has the same universal input/output relay output capability as the BAS Remote Master but only connects to the MS/TP network. Powering the device and the presence of a 24 VDC convenience connection is the same as the BAS Remote Master.

### **One-Cable Solution**

By using Ethernet, you can take advantage of some of the recent advances in Ethernet technology. One advance is Power over Ethernet (PoE) in which a single cable provides both power and data to attached devices. This would be ideal for attaching field devices to a network where power is not present or the power levels are not conducive for easy attachment.

### **BAS Remote PoE**

A BAS Remote Master is configured for powering over Ethernet. The BAS Remote PoE has the same features as the BAS Remote Master without the need to provide 24 VAC/VDC power. Field devices can then be powered using the BAS Remote's 24 VDC convenience connection. This is a slick way of providing power in the field when none exists.

### **Skorpion PoE Injector**

PoE power can be derived from a PoE switch or from a PoE injector. The Skorpion PoE Injector is classified as a mid-span device with two RJ-45 Ethernet ports. The first port connects to the Ethernet network and the second provides both power and data to an attached device such as the BAS Remote PoE.

Ethernet operation is transparent and wiring cost is lowered by running only an Ethernet cable to the attached device. Power for the injector is derived from a 24 VAC/VDC source.

equipment, an intranet can be created to achieve the highest level of security with the convenience of using a structured wiring system.

An *intranet* is a private network that uses the Internet Protocol. Best practice calls for assigning private IP addresses to all devices to ensure no conflict with public addresses. Private addresses are restricted to the LAN side of the router while public addresses are on the WAN side. If there is no intention to connect to the Internet, then there is no need to supply a router for this purpose. But if the intranet is so large or complex that sub-netting the networks is desired, IP routers are still needed.

Think of an IP router as one device with two halves. The names of the two halves vary but typical terms are LAN side – WAN side, Private Side – Public Side, Trusted Side – Not Trusted Side, and simply LAN1 – LAN2. The LAN – WAN terminology may be easier to understand when talking about IP routers connected to the Internet, while the LAN1 – LAN2 references are best for sub-netting a larger network.

IP routers can be much more complex than an Ethernet switch, but they serve a much different purpose. IP routers block broadcasts from propagating from one side to the other. They restrict blocks of IP addresses to one side or the other. They can provide a firewall function by allowing only those messages through the router that are intended. Unintended

messages, or messages constructed in an unexpected manner, are dropped with no indication given to the sender.

A BACnet router is not necessarily an IP router. A BACnet router understands the BACnet Network Layer protocol and not the Internet Protocol unless it is supporting BACnet/IP. A BACnet router attaches two or more BACnet data links together to form one BACnet internetwork. The physical layers could be quite different on each side of a BACnet router because of the different data links BACnet supports. With an IP router, Ethernet is typically present on each side of the router.

## Gateways

The terms gateway and router are sometimes intermixed. In the strict sense, gateways operate on messages sent between two different application layers. Since the application layers are incompatible, custom software must be developed in the gateway so that meaningful data can be exchanged between the two devices. The best example is the BACnet application layer and the Modbus application layer. Because there is no application layer commonality, a gateway must provide an interface. Converting Modbus serial to Modbus TCP is different. The application layers are compatible, so it would appear a router is in order. However, the term gateway could be loosely applied to this situation as well.

## An Infrastructure Example

In the side bar article, a typical building automation system is to share the same IP infrastructure as other information technology equipment. Perhaps the specification calls for existing structured wiring to be used to reduce installation expense while allowing the complete system to be monitored from any point on the IP network. For remote access, the Internet is to be used.

At the top is a single BACnet/IP compliant building controller (BC), having no point I/O of its own, is attached to Ethernet and supervises the complete system. It can be called a building controller, application engine, or IP network controller. A BACnet/IP operator workstation (OWS) provides an overview of the system. A laptop computer functions as a commission tool for a BACnet MS/TP device.

At the bottom are found individual sensors and actuators that are not part of any network — although sometimes proprietary sensor buses are used. However, for sake of discussion we will say that sensors and actuators connect on a one-to-one basis to Direct Digital Controllers (DDC) or Remote Input/Output (RIO) devices. A DDC is an intelligent device that can execute a control algorithm, while an RIO is an intelligent device that can concentrate input/output points and forward the data to a DDC over a serial bus or network. RIO devices do not implement control. The DDCs and RIOs in this

example connect to either an MS/TP, Modbus serial, or BACnet/IP network.

This BAS example identifies equipment residing in several domains.

- \* *Sensors and Actuators*
- \* *Modbus Serial*
- \* *BACnet MS/TP*
- \* *BACnet/IP Ethernet*
- \* *Internet*

### *Sensors and Actuators*

Sensors are used to measure parameters within the process, while actuators manipulate the process. These active or passive, analog or binary, input/output devices reside at the lowest level of the control hierarchy. Analog input devices are used to measure temperature, humidity, air quality, or velocity. An analog output device can be a motor speed control, a value positioner, or a damper positioner. Passive analog sensors, such as thermistors that measure temperature, require low-level excitation from the receiving device to accomplish the measurement. Calibration curves are built into the receiving equipment. More accurate measurements call for an analog transmitter capable of outputting either a 0–10 V or 0–20 mA signal to a receiving device. Binary input devices can be passive pushbuttons, limit switches, or level switches.

The receiving equipment provides the sensing current that

“measures” the state of the binary input. Binary output devices could be motor starters, interposing relays, pilot lights, and solenoid valves. The driving device must have sufficient capability to power the actuator. For analog output devices, either a 0–10 V or 0–20 mA command signal is usually required.

### *Modbus Serial*

Besides BACnet and LON, Modbus-compatible equipment is frequently used for building automation—especially for energy measurement or for motor drives. The Modbus physical layer is typically 2-wire EIA-485. While a Modbus TCP device would allow for a direct connection to an IP/Ethernet network, Modbus serial devices (because of the incompatible application layers) will require either a gateway to BACnet/IP or a Modbus Serial to Modbus TCP router. Either way, Modbus serial devices can be viewed from an IP network.

### *BACnet MS/TP*

The popularity of MS/TP ensures that there will be plenty of devices that require attachment to an IP network. Unitary controllers and programmable thermostats based over an EIA-485 physical layer are typically found at this level. Attachment to an IP infrastructure is accomplished using a BACnet MS/TP to BACnet/IP router. This routing capability can be found in either a building controller that supports routing or in a stand-alone router.

### *BACnet/IP Ethernet*

BACnet/IP devices can directly attach to the building’s IP infrastructure. The most convenient method is to use Ethernet. In this example there is one building controller and one workstation attached to all other devices through an Ethernet copper connection. That does not preclude the use of fiber optics as shown in the example. BACnet MS/TP devices are connected to routers which are attached to switches. Ethernet switches are not protocol-aware and only facilitate connections to the IP infrastructure. They do not block broadcasts and the complete IP network can be treated as a single BACnet internetwork.

### *Internet*

In order to gain remote access to or from the Internet, an IP Router is needed. For security, the IP router also functions as a stateful firewall. On the LAN side of the router is the BAS which is treated as an intranet. On the WAN side is the Internet.

**Contemporary Control  
Systems, Inc**

2431 Curtiss Street  
Downers Grove, IL 60515  
USA

[info@ccontrols.com](mailto:info@ccontrols.com)  
[www.ccontrols.com](http://www.ccontrols.com)

**Contemporary Controls Ltd**

Sovereign Court Two  
University of Warwick  
Science Park  
Sir William Lyons Road  
Coventry CV4 7EZ  
United Kingdom

[info@ccontrols.co.uk](mailto:info@ccontrols.co.uk)  
[www.ccontrols.co.uk](http://www.ccontrols.co.uk)

**Contemporary Controls  
(Suzhou) Co. Ltd**

11 Huoju Road  
Science & Technology Park  
New District, Suzhou  
PR China 215009

[info@ccontrols.com.cn](mailto:info@ccontrols.com.cn)  
[www.ccontrols.com.cn](http://www.ccontrols.com.cn)

**Contemporary Controls GmbH**

Fuggerstraße 1 B  
04158 Leipzig  
Germany

[info@ccontrols.de](mailto:info@ccontrols.de)  
[www.ccontrols.eu](http://www.ccontrols.eu)