Using VPN Bridges with BACnet for Easy Remote Access and Commissioning

CONTEMPORARY CONTROLS®

Remote Access to devices is an increasingly common requirement for Building Management Systems (BMS). Remote Access is used for commissioning, making changes to the operating parameters, monitoring or running diagnostics. Keeping buildings running more efficiently results in considerable savings and has given rise to Energy Management as its own trade. With the increased demand for remote access, it is necessary to implement secure solutions. VPN Bridges with BACnet provide secure remote access and commissioning.

According to a latest market research study conducted by BSRIA, BACnet has a global market share over 60%. BACnet/IP is based on the popular IP protocol and allows a distributed architecture via the use of the Internet. BACnet/IP devices inside a building are on their own subnet and are accessible to each other. A BACnet/IP to BACnet/MSTP router can easily connect the MS/TP devices up to the IP subnet. A PC or a controller running a head-end software can send a Who-Is message and get a response from all the devices in a building. The Who-Is message is a broadcast message and traverses on the same subnet to all devices, which subsequently respond with an I-Am message. Once the discovery process is completed, normal communication can occur using directed messages. Accessing a BMS system remotely involves the use of different subnets and these subnets are connected via IP routers. The broadcast messages that easily traverse on a single subnet are blocked by the IP routers, restricting the BACnet device discovery process to the subnet of the device that sent the Who-Is message.

BACnet Communication Across Subnets using BBMD and FDR

BACnet solves this issue of blocked broadcast messages across subnets by utilizing a BACnet/IP Broadcast Management Device (BBMD). For BACnet/IP communication to occur over two subnets, a BBMD device must exist on each subnet. Each BBMD device is configured with the IP address of its partner BBMD device. This is called the BBMD's Broadcast Distribution Table (BDT). On receiving a broadcast message, the BBMD device sends a unicast or directed message to its partner BBMD device with the original broadcast message as its payload. The partner BBMD device receives the message, decodes it and then sends a broadcast message on its own local subnet. The local BACnet devices respond and this is again sent back by the BBMD device to its partner BBMD device on the first subnet via a directed message. The original BBMD device follows the same process and distributes the remote subnet response via a broadcast message on the local subnet. This completes the discovery process.

BACnet also supports the concept of Foreign Device Registration (FDR). If a workstation or controller needs to access BACnet devices on a remote subnet and there are no other BACnet devices on its subnet, it does not need to support the full BBMD functionality. The device supporting FDR functionality registers with a BBMD device on the remote subnet and can send directed messages to the remote BBMD device and the remote BBMD device will send directed responses to the FDR device along with the other BBMD devices in its BDT table. At least one BBMD device is required on one of the subnets where the FDR devices can register.

In the setup shown in Figure 1, the BACnet router provides the BBMD functionality and can also support Foreign Device Registration. The PC running the application and all the BACnet/IP Controller on the 192.168.1.0/24 subnet support Foreign Device Registration and register with the BBMD device. The controllers on the 192.168.2.0/24 are on the same subnet and do not need to register with the BBMD device. Optionally, a BBMD device on 192.168.1.0/24 subnet can be used eliminating the need to setup FDR entries on the PC and the BACnet/IP controllers.

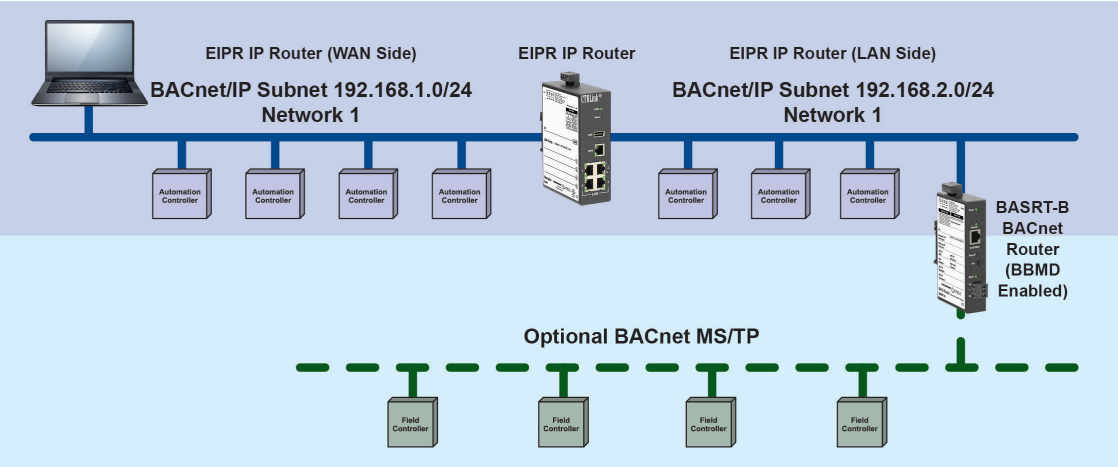

Figure 1: BBMD Functionality with IP Firewall Disabled

BACnet Communication Across Sites using Internet

Setting up BBMD entries and FDR can sometimes become challenging and cumbersome. Most IP routers or firewalls connected to the internet block the incoming traffic. Special rules must be setup to allow any traffic to pass the firewall and this involves setting up Port Forwarding for the BACnet UDP port in use (by default 47808 or 0xBAC0). The IP router receives the BACnet traffic intended for the specified BACnet UDP port and forwards it to the device specified in the Port Forwarding entry. For a remote BBMD or FDR device, it will have to use the address of the Firewall device instead of the real BBMD device behind the firewall. Furthermore, the BBMD device has an additional setting where the Firewall address must be setup as its Public IP address. Complicating things further, this setup only allows access to the BBMD device. If additional BACnet/IP devices exist on behind the firewall, an additional UDP port is required. The BACnet/IP devices besides the BBMD device use this second UDP port and the BBMD device also needs to support the BACnet/IP routing from one UDP port to another.

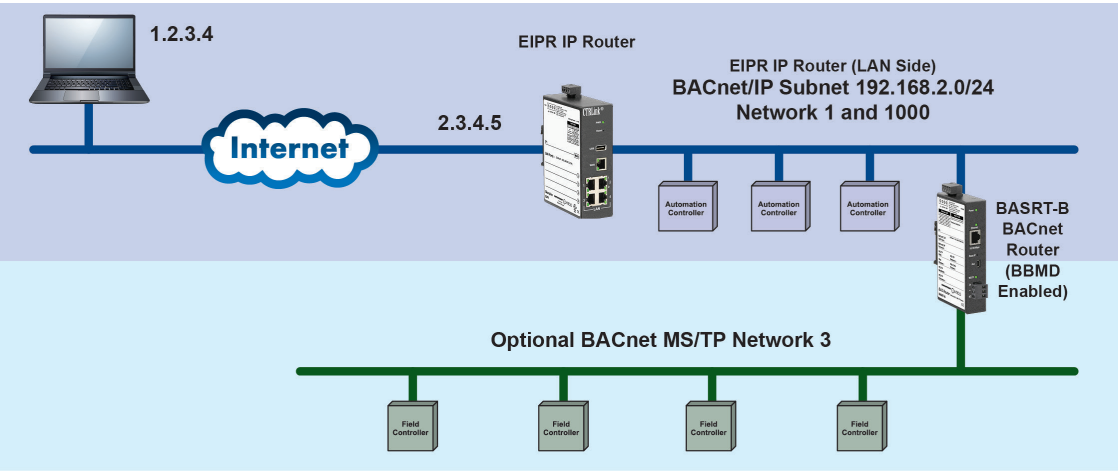

Figure 2: Remote Access to BACnet Network

In the setup shown in Figure 2, a BACnet Network on subnet 192.168.2.0/24 exists with controllers and a BACnet/IP router utilizing the default BACnet UDP port of 47808. If a PC application needs to access this from a remote location, BBMD and FDR are enabled on the BACnet router and a port forwarding entry is added to the IP router. Since UDP port 47808 is already being used on the local subnet, another UDP port, 47809, must be used for this port forwarding entry and a second network number is also setup. The BACnet router is configured to have a

secondary port of 47809 and specified to use this UDP port for BBMD. Although this is all on the same subnet of 192.168.2.0/24, BACnet treats them differently because of varying UDP port and network numbers. After a successful FDR by the PC application with the BACnet router, the discovery process occurs using port 47809, which the BBMD BACnet router forwards to the local subnet on port 47808, getting responses on the same default port and routing the responses back to the PC on port 47809. The BBMD device has the IP address of 2.3.4.5 setup as the Public IP address and the PC also has to direct all the communication to this IP address of 2.3.4.5 instead of the actual subnet of 192.168.2.0/24.

BACnet Communication Across VPN Bridges

Setting up Port Forwarding in the firewall, configuring Public IP address on the BBMD device and setting up the BACnet/IP devices for the correct UDP ports can be confusing. What if you could access the BACnet system remotely and securely as if the PC running your software was part of the local subnet? IP routers can provide a feature called Virtual Private Networks (VPNs) allowing you to connect two separate networks securely over the internet. There are multiple VPN options available but Virtual Private Networks (VPNs) can be setup for bridge mode for secure remote access and easy BACnet Broadcast Message traversal. Ethernet Bridges work on Layer 2 of the OSI layer and transparently pass messages, including broadcast messages. Once broadcast messages can be passed, there is no need for setting up BBMDs, FDRs or multiple BACnet UDP ports. There may be need to setup Port Forwarding if the VPN routers are behind a firewall but no additional setting is required. VPNs are also secure since they are based on the Transport Layer Security (TLS) protocol where the data is encrypted.

VPN bridges can be setup between two VPN routers. This can be used to connect two subnets in two separate buildings across the internet. BACnet/IP communication can occur without additional setup for BBMD or FDR. The IP addresses on the LAN subnets of the VPN routers are on the same subnet but are segmented to avoid any overlapping. This can be a permanent setup to connect two remote buildings securely. VPN bridges can also be setup where one IP router runs as the server and a PC can run as the VPN client. Once the VPN connection is established, the VPN router assigns the PC an IP addresses belonging to its LAN subnet. This is the same subnet where all the other BACnet/IP devices exists. The VPN client PC then communicates over the VPN bridge interface and all the communication occurs transparently. This setup can be used for remote diagnostics when a need arises for troubleshooting. The VPN bridge can also provide an option where different PCs can connect simultaneously or one at a time. This can be useful in a scenario where a technician performs a maintenance task and then an engineer can verify it, each logging to the device remotely without having to drive to the actual site.

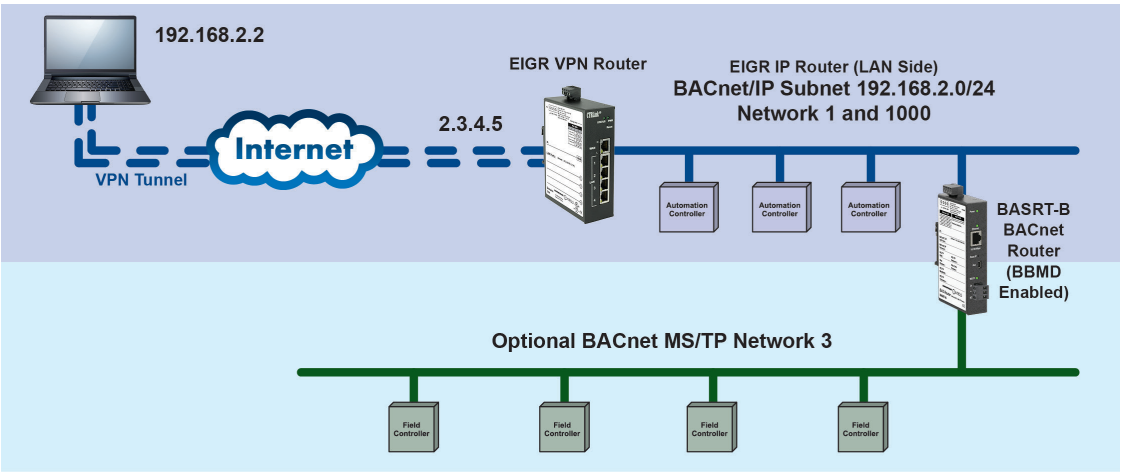

Figure3: Remote Access to BACnet Network using VPN Bridge

In the setup shown in Figure 3, a VPN router supporting bridging is used. The PC running the VPN client software connects to the VPN router establishing a secure VPN tunnel between the PC and the router. The PC is assigned

an additional virtual interface with an IP address belonging to the 192.168.2.0/24 subnet, which is the same subnet as the existing BACnet network. Since all communication now occurs over the same subnet and VPN bridges pass all traffic through them, it greatly simplifies the setup by eliminating the use of BBMD.

The cost of IP infrastructure devices like IP routers that provide VPN capabilities has come down significantly and is not a limiting factor anymore. All the advances in the IT field lend itself well to protocols based on IP, like BACnet/IP. VPN bridges can be used to speed up commissioning and save on equipment cost. A PC running a workstation or specific BACnet application can be setup to connect to different sites as required to perform maintenance, thereby getting rid of the need to setup dedicated equipment. VPNs have the added advantage of encrypted communication and easily restricting remote access to authorized personnel. With the increasing demand for remote access, using VPN bridges with BACnet provide the secure solution.

ASHRAE BACnet™ Secure Connect

United States
Contemporary Control Systems, Inc.
Tel: +1 630 963 7070
Fax:+1 630 963 0109
info@ccontrols.com

China
Contemporary Controls (Suzhou) Co. Ltd
Tel: +86 512 68095866
Fax: +86 512 68093760
info@ccontrols.com.cn

United Kingdom
Contemporary Controls Ltd
Tel: +44 (0)24 7641 3786
Fax:+44 (0)24 7641 3923
ccl.info@ccontrols.com

Germany
Contemporary Controls GmbH
Tel: +49 341 520359 0
Fax: +49 341 520359 16
ccg.info@ccontrols.com

www.ccontrols.com