Using the BACnet® Firewall Router

By David G. Holmberg, Ph.D.; Joel Bender; and **Mike Galler**

If you pay attention to the news, then you know that network security is an important issue. It seems that every day brings a new account of compromised networks and compromised personal information; new viruses, worms, trojans, phishing attacks, and the like. We hear reports on identity theft, criminal use of botnets (networks of hijacked computers), and foreign countries' concerted efforts to break into defense networks. Clearly, attackers, motives, and methods vary, but the dangers are real.

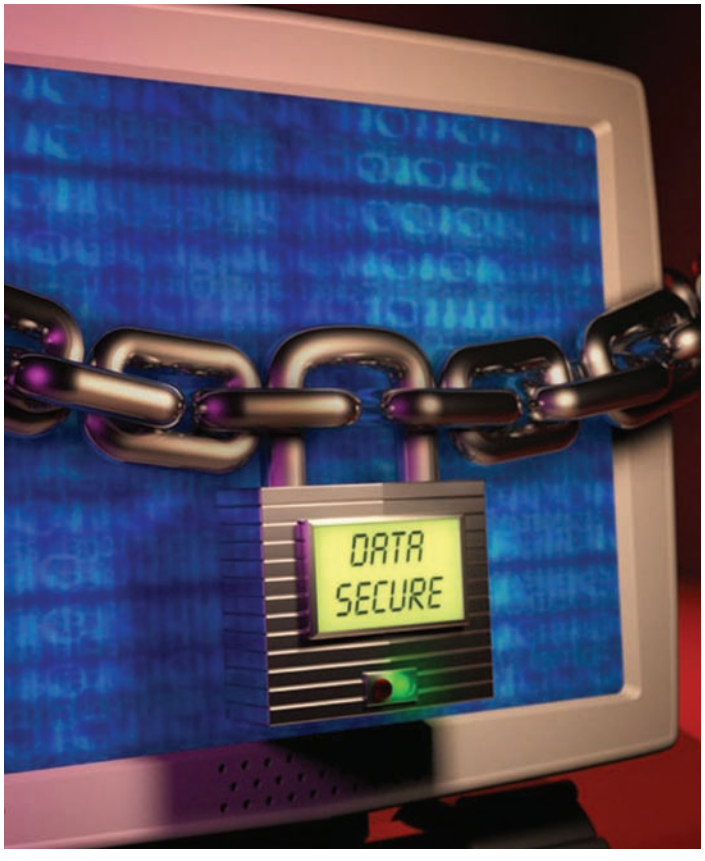
What are the security concerns of the facility HVAC network? Are they the same as an IT network? A decade ago, most HVAC equipment came from a single vendor and sat on an isolated network and used a proprietary communications protocol. Even today, most controller-level devices run operating systems (OS) that are hardened (or at least smaller and less vulnerable), and don't have large hard-disk drives or common applications (such as e-mail) that either make them attractive to hackers or vulnerable to common attacks. Smaller controllers are even less attractive and vulnerable. So, what is different today?

First, although BACnet has brought facility managers a robust standard that brings freedom from vendor lock-in, hope for multivendor interoperation, and the benefits of standard tools, it has also made it easier for an outsider to discover network resources (using standard tools), and communicate with devices on the network (with an open protocol). No more hiding behind the "security by obscurity" defense.

Second, facility networks today see a trend toward more connection to a general purpose facility IT LAN (local area network) or campus WAN (wide area network). But, didn't we just establish that common IT security threats are not really an issue on facility networks? Are we worried that some hacker is going to twiddle with chiller setpoints or turn out the lights? If you see the hacker as some remote individual poking around the net late at night with no clue about your

About the Authors

David G. Holmberg, Ph.D., and **Mike Galler** are mechanical engineers in the Building and Fire Research Laboratory, Building Environment Division at the National Institute of Standards and Technology (NIST), Gaithersburg, Md. Holmberg serves on the Network Security and Utility Interaction Working Groups of ASHRAE Standing Standards Project Committee 135 (BACnet). **Joel Bender** is a programmer analyst at Cornell University Utilities Department, Ithaca, N.Y.



… there are real people with knowledge of your location, and some might be poking around where they don't belong—students nosing around, disgruntled employees, vendors going places they should not. Just as you want to keep the door to the mechanical room locked, you'd like to keep the network closed as well.

facility, the answer is probably no. On the other hand, there are real people with knowledge of your location, and some might be poking around where they don't belong—students nosing around, disgruntled employees, vendors going places they should not. Just as you want to keep the door to the mechanical room locked, you'd like to keep the network closed as well. That's where the connection to the IT network becomes an issue. If the operator workstation (OWS) has Internet access, runs a common OS and common applications with vulnerabilities, then it is possible that someone could break into that machine and have easy access to your facility network. Plus, how many modem connections do you have to the facility network where easy network access might be obtained?

This leads to a third big issue about security—in many places the IT department cares more about the connection(s) of the HVAC facility network to the IT LAN than the facility manager does. It's the IT department that has the real network security issues to deal with, and they don't want the facility network to compromise the IT network. So, the facility manager is in the position of following IT department rules. And, it is here that we can see that HVAC device misconfiguration and security holes can become IT security issues. If the high level controllers in a building are BACnet/IP and sitting on the IT LAN (which is becoming more common), then those devices become just another device for the IT department to be concerned about.

Is the OS secure? Are applications patched? What happens when a controller is misconfigured and flooding the network with useless messages? What happens if someone can get to the modem on an HVAC controller and bypass the corporate firewall?

The IT department cares. How can the building controls community do better at setting up networks and maintaining the facility network such that harmony prevails with the IT department and security is maintained?

One step is to build some security into the products and protocols and networking architecture of the facility net. As far as products are concerned, vendors have implemented varying degrees of product security per customer demands—passwords for configuration access, hardened operating systems, perhaps message encryption for sensitive applications. For protocol security, BACnet has recently issued a draft for the new BACnet network security[1] specification, which will replace the existing Clause 24 of the BACnet standard. This update to the standard goes far beyond the existing Clause 24 and provides

for device authentication, message integrity and data hiding. A more complete introduction was given in last year's BACnet supplement.[2] The new BACnet network security specification uses standard methods to provide protocol security. But what about secure network design?

One aspect of an overall security plan that can be implemented today is a simple BACnet-specific firewall to sit at the connection of a BACnet facility network to the IT network. It might even have some extra tools to make facility network administration easier. That's the BACnet Firewall Router.

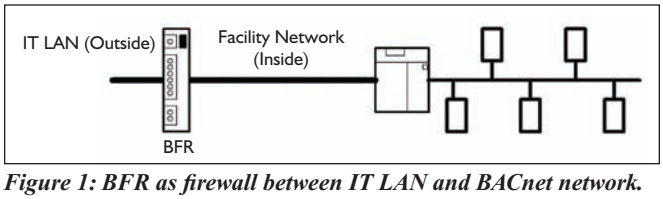


Figure 1: BFR as firewall between IT LAN and BACnet network.

A BACnet Firewall

The BACnet Firewall Router (BFR) is a BACnet router with security firewall functionality. As a firewall it allows network and address filtering plus network and application layer service filtering of BACnet communications according to a security policy. The BFR also has the ability to function as a BACnet Broadcast Management Device (BBMD) and provide network address translation (NAT). The BFR is a piece of software that runs under Linux on a PC with two network cards (one facing the external network and one facing the internal protected network). The BFR is presently under development as a Sourceforge project (http://sourceforge.net/projects/bfr/). Sourceforge is a Web site that hosts many open-source software development efforts. Source code, user manuals, and other details are available for free at Sourceforge.

The BFR has been developed as a tool with multiple security functions to provide another layer of security, and it has the potential to serve as a platform for future security products. Unlike firewalls and routers that are commercially available, the BFR is designed specifically for controlling BACnet traffic. It likely will serve as a router between the IT LAN and a BACnet network segment (*Figure 1*).

The rest of this article looks at some specific applications of the BFR that will help to better secure and administer a BACnet facility network.

Traffic Cop

Perhaps the most useful feature of the BFR is the ability to control what messages can pass from one side to the other. For example, if the operator workstation is the only device on the IT backbone that needs to talk to any device on a BACnet subnet, then the BFR can be configured to only allow traffic to and from that device to pass the BFR. Messages from any device specifically can be allowed or disallowed (dropped). The disallow feature may be useful for blocking nuisance traffic from a device on the facility network from reaching the IT LAN.

Consider the case of a campus environment with a campus WAN (*Figure 2*), and a vendor coming on to Site A to install some new controllers on the facility LAN in the Administration Building. As shown in *Figure 2*, the facility LAN is a BACnet Ethernet network that connects to the building LAN via an Ethernet to IP router that also serves as a BBMD.

Now suppose that the vendor configures the controllers to issue change of value (COV) notification messages (these are broadcast messages, typically to report some sensor value) but fails to properly configure the threshold values, leaving the devices in a state where any meaningless change in value is reported with a broadcast BACnet COVNotification message with (for example) a once per second update rate. The router dutifully passes on this broadcast message to the building LAN and also, as BBMD, passes the message to all remote BACnet/IP networks in its broadcast distribution table. This table might likely have the IP addresses of every BBMD in every building on campus in Site A as well as other sites on the campus WAN. The end result is that the several messages per second from the misconfigured devices on the facility LAN are resulting in tens or hundreds of messages per second on the campus WAN. Therefore, the IT department might not be happy. What's the solution?

Replacing the router/BBMD with a BFR provides a means to stop the flood of nuisance messages and give time to diagnose the problem and configure the COV notification threshold levels properly. Besides that, the BFR is not only a stopgap measure, but also a guard at the door, preconfigured to allow only certain devices on the inside to talk to certain devices on the outside (or vice versa) with certain messages. This has the dual benefit of protecting the facility controllers from IT network threats while also protecting the IT network from misconfigured controllers.

Also, since the BFR can drop all non-BACnet traffic, anyone who manages to find a backdoor into the facility network can no longer use that to get on to the IT network. So, the BFR can police traffic going both ways.

NAT for Network Security and Configuration Problems

Perhaps the second most useful feature of the BFR is that it can do network address translation (NAT), a process of modifying the source and/or destination address of a packet as it passes through a router. It is widely used with IP protocols with home and small-office Internet connections, where all of the devices in the home can share the IP address provided by the internet service provider (ISP).

For a small office network, all of the devices consider themselves to be on the same LAN and share a router to the rest of

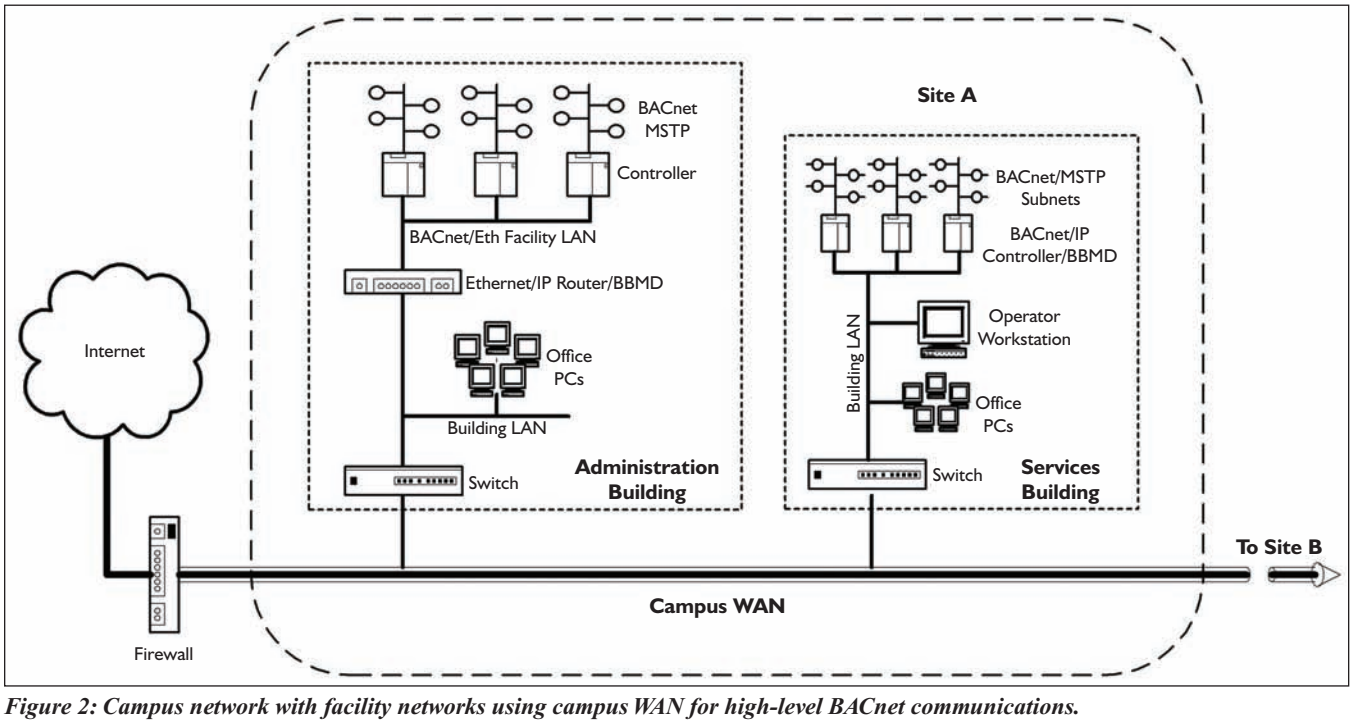


Figure 2: Campus network with facility networks using campus WAN for high-level BACnet communications.

the Internet. They typically use "private" IP addresses, rather than going through the process of asking the Internet Assigned Numbers Authority for an address range. They use local IP protocols to communicate among themselves just as they would if they were on any public network.

When a machine requests a connection to an address outside of the office, say for a browser requesting a Web page, the router translates the office machine's private address into the public one assigned by the ISP. Then when the response comes back from the website, the router maps the destination back to the office machine and forwards the packet along.

BACnet routers are similar to Internet routers—they present the source and destination information untouched. If a BACnet router had a public address, it would be easy to expose the addresses of internal devices using the widely available broadcast services Who-Is and I-Am.

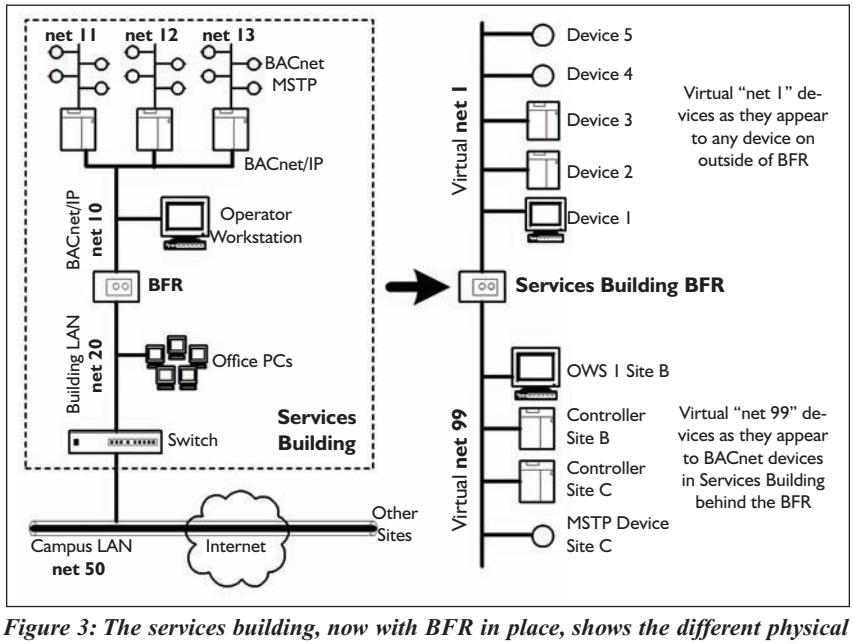


Figure 3: The services building, now with BFR in place, shows the different physical networks (left) and the translated "virtual" networks (right).

The BFR can provide NAT-functionality by mapping all of the devices in an intranet into a "virtual" BACnet network. For example, consider a BFR with two network cards, one connected to an "outside" network provided by an ISP and the other connected to an "inside" network within a facility (*Figure 1*). Also consider that the "inside" intranet consists of multiple BACnet networks such as for the different MSTP networks in the services building of *Figure 2*. The services building of *Figure 2* is shown again in *Figure 3,* with a BFR in place, and the "inside" network is the BACnet side.

The BFR can be configured to "masquerade" or translate all of the devices on the inside network to appear as a single network to the outside (network 1 in *Figure 3*) and all of the

outside devices to appear to the inside as a single network (network 99 in *Figure 3*). As with typical routers, devices on the outside cannot communicate directly with the devices on the inside without going through the BFR, which puts the BFR in the position to filter messages.

When a BACnet device on the "outside" sends a packet to the BFR, its address is translated into a virtual address (network 99 in the example) when it is forwarded to the internal network. Internal devices see this as a normal address. When they reply, the packet goes back to the BFR as it would with any other router. The BFR sees the destination address and translates it back into the "outside" address of the destination and forwards the packet along.

Unlike most devices that implement NAT such as cable routers, the BFR translates both the source and destination addresses. So the source address of our reply is mapped into a virtual address on network 1 when sent back to the client. By restricting what devices are allowed to be mapped, the BACnet network administrator can provide BACnet services to the "outside" without exposing the entire internal network. This is similar to the safety that a cable router provides the small office, outside devices cannot attack a device on the inside network.

In addition to the security aspect, the BFR NAT functionality can address a common network configuration problem that can occur when two previously separate BACnet networks are joined into a BACnet internetwork. BACnet requires unique network numbers, but installers may leave default network numbers such that different network segments have the same network numbers. This is not a problem until data sharing between networks is desired. Using the BFR as a router to a given network segment and virtualizing the network number allows one to get around this problem. Thus, multiple BACnet intranets can be connected together without requiring local network administrators to be concerned about using a BACnet network number that may be in use by some other intranet—local topology changes are insulated behind the BFR.

However, the NAT capability of the BFR is not a panacea. Inside devices can be configured with BACnet intranet addresses and expose them to the outside via such object properties as the Device_Address_Binding list. However, with the use of filters, these addresses cannot be used by an outside device to attack an inside one.

Testing and Future developments

The National Institute of Standards and Technology (NIST) and Cornell University have worked together on the development and testing of the BFR. The current version of the BFR has been tested for correct filter functionality and for compliance with BACnet testing standard ANSI/ASHRAE Standard 135.1, *Method of Test for Conformance to BACnet,* for router and BBMD operation.

The current version of the BFR provides full BBMD and BACnet router functionality, except that it will not function as a half-router (routing to a remote network over a temporary point-to-point phone connection).

The BFR is an ideal candidate to serve as a secure router that implements the new BACnet network security specification. A secure router would allow traffic over the IT backbone to be signed and/or encrypted. BACnet security also provides a means for authentication of devices and authorization of users that would prevent spoofing (forging) device addresses and allow for filtering according to authorization policy. It is the hope of the authors that the BFR will see continued development and have the network security functionality added to the code base in the coming year.

The BFR is available at http://sourceforge.net/projects/bfr/. Please let us know (via the Sourceforge admin link) how you use it.

References

1. Proposed Addendum *g* to *Standard 135-2004, BACnet®—A Data Communication Protocol for Building Automation and Control Networks* (BACnet Network Security draft specification) is available at www.bacnet.org/Addenda/Add-2004-135g-PR1.pdf.

2. Holmberg, D. G. 2005. "Secure messaging in BACnet." *ASHRAE Journal* 47(11):B23–B26.