
Jim Butler

Introducing BACnet Secure Connect

BY JIM BUTLER, MEMBER ASHRAE

Cybersecurity-conscious building owners should consider using the new BACnet/Secure Connect (BACnet/SC) as an alternative to BACnet/IP to augment cybersecurity measures that protect their building automation systems (BAS). This column gives an overview of the features of BACnet/SC and provides a summary of the differences between BACnet/SC and BACnet/IP.

Both BACnet/IP and BACnet/SC are both interoperable communication methods found in ANSI/ASHRAE Standard 135-2020, *BACnet, A Data Communication Protocol for Building Automation and Control Networks*. BACnet/SC was introduced in the 2020 edition of the standard.

While both methods define interoperable methods for the transmission of BACnet messages on IP networks, they are different in some important ways. At a very high level:

- BACnet/IP is widely used today because it is straightforward to implement in products, and the communication parameters of BACnet/IP devices are simple to configure in the field. However, BACnet/IP is considered to be "IT unfriendly" in some ways, and it does not have any built-in network security functionality.
- BACnet/SC has state-of-the-art communication security features inherited from modern data communication standards that are widely used in the IT world to improve cybersecurity. Implementation of BACnet/SC in a product requires significant computing resources (CPU and memory), which means that many installed BACnet/IP controllers will not be able to be upgraded to support BACnet/SC. Also, the deployment of BACnet/SC devices is more complicated than the deployment of devices that use other BACnet communication methods.

Networks of BACnet/SC devices can be connected to other BACnet networks (BACnet/IP, MS/TP, etc.) using BACnet routers. This gives building owners the flexibility to deploy the types of BACnet networks that are most appropriate for their facilities.

Let's look at the differences between BACnet/IP and BACnet/SC in more detail, starting with a brief review of BACnet/IP.

BACnet/IP

BACnet/IP, added to the BACnet Standard in 1999, is a relatively simple communication method for internet protocol (IP) networks that has been widely implemented in HVAC control devices as small as thermostats. The configuration of the IP communication parameters of BACnet/IP devices is straightforward, and no special network infrastructure is needed to use BACnet/IP.

Jim Butler is CTO of Cimetrics Inc. He is the convener of the BACnet committee's IT working group, and he served as the first manager of the BACnet Testing Laboratories.

In some buildings, BACnet/IP devices share network infrastructure with devices used for other applications. Since BACnet/IP does not have any built-in network security functionality, virtual private networks (VPNs) and virtual local area networks (VLANs) have been used to provide virtual separation of BACnet/IP devices from other IP-network-connected devices. And in some facilities, BACnet/IP devices are connected to dedicated IP networks that are physically separate from other networks.

The BACnet standard does not require BACnet/IP devices to use static IP addresses, but most manufacturers recommend this configuration for their devices. By contrast, dynamic IP addresses are heavily used in mainstream IT networks because they are easier to manage. This has become a source of friction between BAS personnel and IT personnel as increasing numbers of BACnet/IP devices are connected to networks managed by IT departments.

BACnet/SC

BACnet/SC, added as an addendum to the BACnet standard in 2019, is based on commonly used IT network protocols—WebSockets and Transport Layer Security (TLS) version 1.3 in particular. TLS and digital certificates are the basis for the cybersecurity features of BACnet/SC. Outside of BACnet, TLS is used for secure communication between web browsers and web servers (the technology used in https:// websites), so it is one of the most important protocols used in the internet.

An important BACnet/SC cybersecurity measure enabled by TLS is certificate-based device authentication. Every BACnet/SC device in a BACnet/SC network must have a digital certificate signed by a locally controlled certificate authority. When a BACnet/SC device attempts to connect to another BACnet/SC device (or hub), each device checks the other device's certificate, and the connection attempt will not succeed unless the certificates presented by both devices have been signed by the designated certificate authority for that BACnet/SC network. This allows network administrators to control which devices are permitted to join a BACnet/SC network.

BACnet/SC network traffic will be encrypted in most installations (also enabled by TLS). This is good for cybersecurity, but it will make it more difficult for technicians to use third-party network diagnostic tools to decode and analyze BACnet/SC network traffic.

TABLE 1 Comparison of BACnet/IP and BACnet/SC.

	BACNET/IP	BACNET/SC
TRANSPORT PROTOCOL	User Datagram Protocol (UDP)	Transmission Control Protocol (TCP)
IP ADDRESSES	Usually Static	Static or Dynamic
DOMAIN SYSTEM NAME (DNS)	Rarely Used	Often Used But Not Required
MESSAGE FORWARDING DEVICE	BBMD (Broadcasts Only)	BACnet/SC Hub (All Traffic)
USES DIGITAL CERTIFICATES	No	Yes (Required)
ENCRYPTED COMMUNICATION	No	Yes
DEVICE AUTHENTICATION	No	Certificate Based

Every BACnet/SC network will have one or two BACnet/SC hubs whose function is to forward both broadcast and unicast messages between BACnet/SC devices. Each BACnet/SC device is responsible for establishing a secure (TLS) connection to the primary BACnet/SC hub in its network or to the designated failover hub if the primary hub cannot be reached. BACnet/SC devices may also communicate directly with each other, but BACnet broadcast messages must be sent via a BACnet/SC hub.

In contrast to BACnet/IP, little advantage exists to using static IP addresses due to the connection-oriented nature of BACnet/SC communication. A BACnet/SC device may be assigned a static or a dynamic IP address, and the device need not be on the same IP subnetwork as either of the BACnet/SC hubs as long as the device can establish a connection to both hubs.

Defense in depth is a well-accepted cybersecurity strategy that involves the use of multiple defensive measures to protect against potential attacks. By using BACnet/SC in combination with carefully configured VLANs or VPNs, the likelihood of a successful network-based cyber attack should be significantly reduced. A future cybersecurity column will describe technologies currently under development that build upon BACnet/SC to further enhance the cybersecurity of BACnet-based building automation systems.

For Further Reading

Fisher, D., B. Isler, M. Osborne. 2019. "BACnet Secure Connect: A Secure Infrastructure for Building Automation." ASHRAE. ■