Commissioning and Troubleshooting BACnet Networks Securely Using VPNs

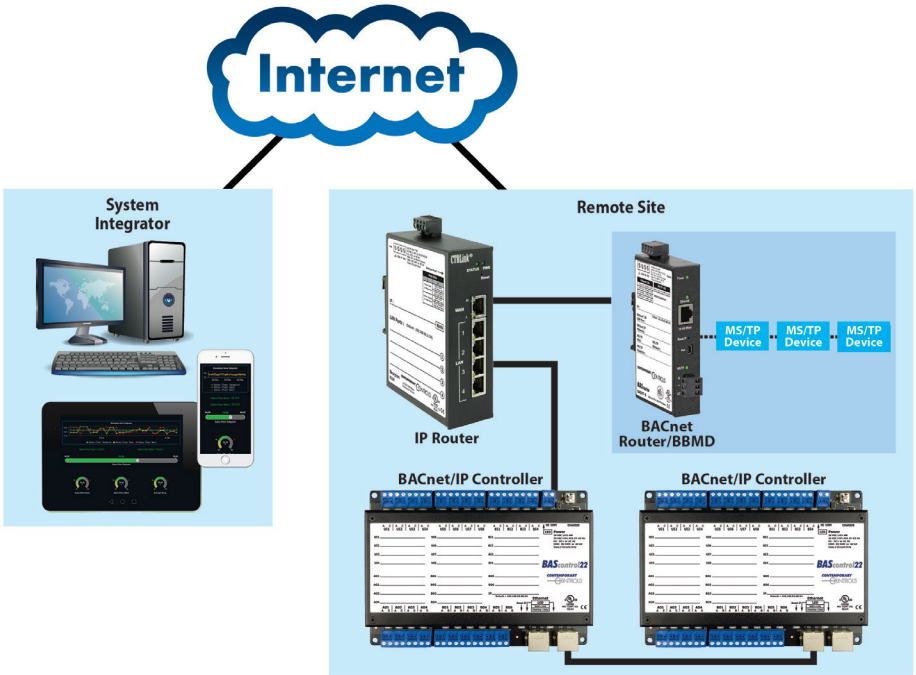
CONTEMPORARY CONTROLS®

There has always been a need to access systems remotely and securely, either for initial commissioning or for troubleshooting later over its lifetime.

The advent of internet has made it possible to access Building Automation Systems from anywhere in the world. The days of an HVAC system being in a silo are long gone. There may be a requirement to just gather the building performance optimization, or to data further for energy change the parameters remotely for optimal operation. While this connection to the internet provides ease of access, it also raises some security concerns regarding unauthorized access and misuse. Fortunately, the world of Building Automation is dominated by the BACnet protocol and its IP version, BACnet/IP, lends itself well to all the enhancements and techniques deployed in the Information Technology (IT) world. This includes the use of IP routing, Firewalls and Virtual Private Networks (VPNs). BACnet Secure Connect (BACnet/SC) communication layer is another example of including the security aspects from the IP protocol, that powers millions of safe credit card transactions every day, into BACnet. The adoption of BACnet/ SC will take time and not everyone will replace their working "non BACnet/SC legacy devices", so there is a need to maintain safe and secure access for these legacy devices. Common techniques for remote access involve the use of Port Forwarding through a firewall and the use of VPNs. But the security provided and their ease of setup for BACnet systems varies.

Remote Access to BACnet Systems via Port Forwarding

One current method of accessing devices at remote locations involves setting up Port Forwarding entries in the internet facing firewall/ IP router. For BACnet/IP, this involves setting up a port forward entry to a BACnet/ IP device, usually a BACnet router, behind the firewall. BACnet communication occurs over UDP ports 0xBAC0 to 0xBACF that are configured by the user. There are many port and IP scanning programs available on the internet for free that can be misused. With the popularity of BACnet, malicious scanning software now also scan for the

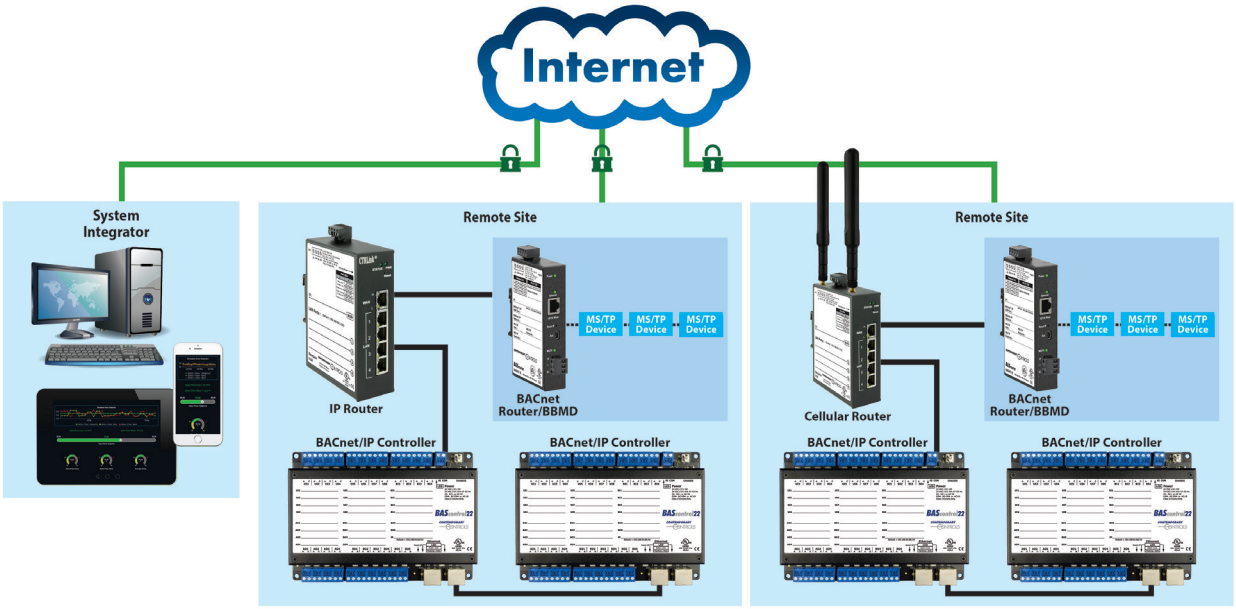


Remote Access to BACnet Systems using Port Forwarding

UDP ports used by BACnet and can provide information regarding Building Automation Systems to bad actors. The use of an Allowlist in an IP router with the list of originating IP addresses allowed to access the system should be used at a minimum. This is not a foolproof method with IP spoofing, and the traffic over the internet is still unencrypted.

Remote Access via Virtual Private Networks

VPNs provide a secure method for accessing BACnet systems for commissioning and troubleshooting. VPNs use the same Transport Layer Security (TLS) standard that is the basis for the new BACnet/SC communication layer. It incorporates the use of security certificates and keys that provide authentication to prevent unauthorized access, data integration to prevent against data tampering, and encryption to safeguard data as it traverses over the open internet. A VPN server and a VPN client form a secure communication channel, or VPN tunnel, that can provide remote access to all kinds of data over the single IP port used for VPN connection. The IP protocol port numbers go up to 65535, can be TCP or UDP, and provide more security for remote communication than the well-known BACnet UDP ports. A client can only succeed in creating a remote connection it © Contemporary Controls if has the client certificate and security key that must be explicitly provided to it.



Secure Remote Access to BACnet Systems using VPN

Routing Mode vs Bridge Mode VPNs for BACnet Access

There are two popular methods for VPN – Routing Mode and Bridge Mode that can be used to securely access BACnet systems. With routing mode, the remote site IP address and the VPN address for the client are on separate subnets. This is the same as accessing a BACnet system across an IP router with different subnets where Broadcast messages are blocked. A BACnet Broadcast Management The user has the same application experience as if they were present at the remote site.

VPNs can be setup between two sites or multiple sites. It can be set up by the IT department for large sites or can be set up by system integrators using IP routers. Furthermore, remote sites benefit from the options of wired or wireless IP routers. Cellular IP routers can be used for locations where wired internet connectivity is not possible or for buildings where the commissioning can be done before the wired Cybersecurity is no longer an option.

Every building automation system needs to be designed with security for both the BAS, and the enterprise, considered as a part of the design. Remote access and digitalization technologies provide significant operational benefits and cost savings to both the building owner and their support contractor. But, along with that comes the associated risks. This article has presented multiple ways to mitigate those risks. In the short term, a Bridge VPN provides the best protection with minimum complexity. Longer term, BACnet/ SC will become a part of every BACnet product offering.

Remote Access Method	Data Encrypted	BBMD needed
Port Forwarding	No	Yes
Routed VPN	Yes	Yes
Bridge VPN	Yes	No
BACnet/SC	Yes	No

Security and ease of Setup for BACnet Access

Cybersecurity is no longer an option. Every building automation system needs to be designed with security for both the BAS, and the enterprise, considered as a part of the design. Remote access and digitalization technologies provide significant operational benefits and cost savings to both the building owner and their support contractor. But, along with that comes the associated risks.
This paper has presented multiple ways to mitigate those risks. In the short term, a Bridge VPN provides the best protection with minimum complexity. Longer term BACnet/SC will become a part of every BACnet product offering.

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