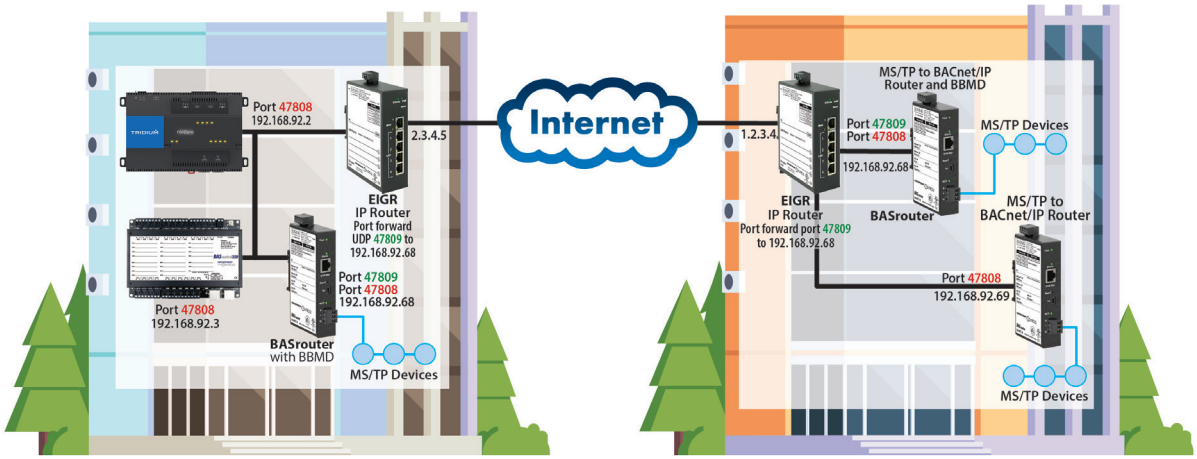
Secure Remote Access to BACnet Systems

CONTEMPORARY CONTROLS®

The Internet makes it possible for systems integrators to easily manage buildings from the comfort of their home or office. Initial commissioning, remote diagnostics and troubleshooting of the building provide additional savings over the building's lifetime. Remote access can be achieved using various methods – some are more secure than others. Fortunately, the Building Automation industry 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. Common techniques for remote access involve the use of Port Forwarding through a firewall, setting up BBMDs, and the use of VPNs. But the security provided and their ease of setup for BACnet systems varies. IP routing with Firewalls and VPNs adds to the security of BMS systems. The IP Protocol and TLS form the basis for the new BACnet Secure Connect allowing secure communication.

Remote Access with BACnet/IP

BACnet/IP uses broadcast messages to initially discover other devices. BACnet communication across subnets needs additional configuration since IP Routers do not route broadcast messages. BACnet resolves this issue by utilizing a BACnet/IP Broadcast Management Device (BBMD). The BBMD sends received BACnet broadcast messages as directed messages through the IP router to its partner BBMD devices. The receiving BBMD device retransmits it as a broadcast message to its local network. You can configure each BBMD with the IP addresses of all other BBMDs or have all BBMDs send their broadcast messages to one central BBMD, however, all client devices must utilize the central BBMD. These entries go into the BBMD's Broadcast Distribution Table (BDT). It is possible to have more than one BBMD device on a single subnet and care must be taken while configuring BDT entries. A duplicate entry in BBMD devices will result in broadcast loops.



Typical setup connecting 2 Buildings using Port Forwarding and BBMDs

Many BACnet/IP devices or applications also support a feature called Foreign Device Registration (FDR). FDR allows the BACnet/IP device or application to send its messages to a BBMD which then forwards broadcast messages to all other BBMDs and all other FDR devices. If a subnet has only FDR supported devices, then it does not need a local BBMD. These devices can register with a BBMD on another subnet.

BBMD and FDR allow BACnet devices and application PCs to communicate across subnets, i.e., the Internet. This setup is used to connect buildings or to gather data at a central location from multiple buildings.

Adding Security to BACnet/IP Communications

There are tools that can detect BACnet communication over the Internet by checking for the standard BACnet UDP Port 47808. It is good practice to change this port to a non-standard port if communicating over the Internet. The IP routers/firewalls also provide additional features that should be utilized. A list of IP addresses that can communicate through the firewall can be specified on the Internet facing firewall. Some BACnet routers also provide this Allowlist feature. BACnet/IP communication occurs over UDP and is unencrypted. Using VPNs can provide additional security by encrypting the traffic over the Internet and restricting communication to only authorized VPN endpoints. There is no need to use non-standard BACnet UDP Ports with VPNs. Setting up firewall rules or VPNs requires help from the IT department while the BMS professional can configure the non-standard BACnet UDP port on their own.

Security with BACnet/SC datalink

The open nature of BACnet/IP and broadcast traffic created some pushback from IT departments. BACnet Secure Connect (BACnet/SC) was released to address these concerns by incorporating the widely used IT security practices. BACnet/SC used connection-oriented TCP instead of UDP and TLS 1.3 for security with encrypted communications. Each device must be authorized to be on the network and assigned a certificate and key. The broadcast discovery protocol and BBMD have been eliminated. BACnet/SC uses a hub and node model. Devices/nodes primarily communicate via the BACnet/SC hub with standard provisions for node-to-node communication. The SC hub can be on the Internet, with nodes at different locations only originating an outbound connection that doesn't require firewall changes. If the hub is located behind the firewall, a port forwarding entry for access from the Internet is needed. But for a remote node or application to successfully connect to the hub, it must have already been provided the credentials (certificate and key) and approved to be part of this network. Temporary access can be granted by creating a certificate for a shorter time duration. The use of BACnet/SC provides security inherently. BACnet/IP and BACnet MS/TP devices can be integrated with BACnet/SC using BACnet routers that support all three datalinks, thus allowing current and future BACnet Systems to be securely interconnected.

BACnet/IP vs BACnet/SC Communications	
BACnet/IP	UDP Broadcast traffic No encryption Any device can join
Firewall Rules	VPN
BACnet/SC	TCP No broadcast traffic Encrypted communications Device authorization required

Benefits of BACnet/SC vs BACnet/IP. Non-standard Ports, Firewall Access Control Lists and VPNs provide additional security

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