BACnet Secure Connect

Switching to BACnet/SC

Creating a comprehensive infrastructure of BACnet/SC-compatible devices is one way for property operators to take advantage of BACnet Secure Connect (BACnet/SC) in building automation. However, when you consider that around 25 million end devices currently transfer their data via BACnet, it soon becomes clear that a complete switchover would involve significant effort and expense.

Those hoping to update their existing devices instead (an update that is still inconceivable) should consider that existing hardware may not be equipped for the computing power required by BACnet/SC.

It is therefore useful to plan for a transition, combining existing BACnet/IPv4 infrastructure (Internet Protocol version 4) with BACnet/SC-compatible hardware. When integrated into traditional infrastructure, this combination not only serves as a bridge between BACnet and BACnet/SC, it also allows users to physically encapsulate data exchange via BACnet/IP. This allows for secure, encrypted data communication in building automation.

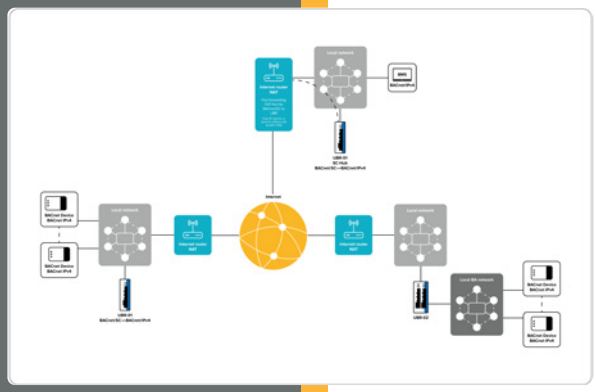
The following three graphics show the common network topologies for building automation with BACnet and aims to provide suggestions on how to successfully switch over to BACnet/SC.

In principle, the topology of traditional networks must be changed to make them fit for BACnet/SC. In doing so, each network receives a central point in its configuration. This is called the hub. This hub

- controls data traffic between any required number of end devices; and
- analyses data traffic to verify how many end devices information should be sent to.

The Universal BACnet Router (UBR) from MBS can take on this role. Located in the local management system network, the device has been used for implementing ISO 8802-2 BACnet network topologies (also known as BACnet/Ethernet), BACnet/IP and MS/TP (serial BACnet networks based on RS485) for quite some time. In the meantime, it also supports the current BACnet Revision 22 and can therefore be used to build the innovative BACnet/SC security structure. The UBR-01 contains one network card, the UBR-02 contains two. Which device can be used depends on the specific circumstances.

Connect across systems over the Internet with BACnet/SC



Starting point

A hub with locations across the world that are connected to one another via the Internet. Currently, data exchange in building automation via BACnet/IPv4 would only be possible if all locations were connected via VPN. Application examples include a company with sites across the globe, authorities with affiliated schools and gymnasiums, or a supermarket chain with its various branches.

The hub contains the building control system, which accesses building automation systems. The interface to the World Wide Web comes in the form of an Internet router with a firewall.

The challenge

Data exchange via IPv4 is unencrypted. The DHCP (Dynamic Host Configuration Protocol) control protocol for automatic assignment of IP addresses (useful when managing large networks) is also not supported. Complex VPNs (Virtual Private Network) were previously set up to secure such building automation networks.

The solution

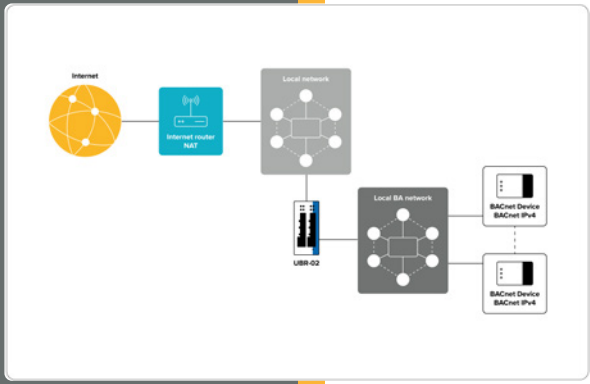
In this example, the Internet router transmits the data to the UBR-01, which then serves as a media converter to translate the BACnet/IP4 data protocol into BACnet/SC using its built-in network card. It also encrypts the data communication.

Connecting to the hub

The hub's Internet IP router has either a static IP address from the Internet or its dynamic address is resolvable via a dynamic DNS. Extensive data packages are forwarded to a UBR-01 via a defined port (port forwarding). The UBR-02 acts as an SC hub and BACnet router here to allow users to continue to use a building control system with BACnet/IPv4.

Connecting locations

Two versions are shown below the central control centre, outlining how, in this scenario, the building-related systems at the various separate locations can be connected to the control technology.



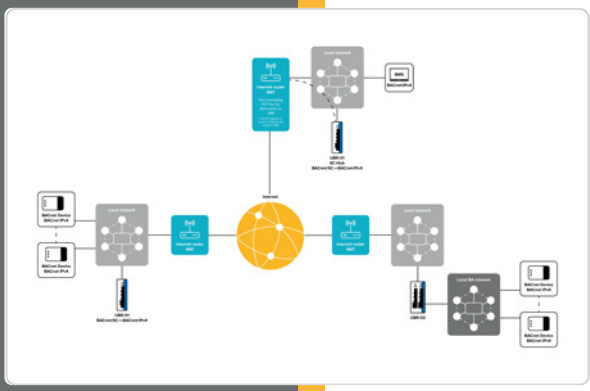
Description of the graphic on the right

On the right side, a router is used for transmitting data between local systems and the Internet, e.g. an IP-compatible DSL router. This does not have to be compatible with port forwarding. The local networks include both internal networks with BACnet/IPv4-compatible devices for building automation and other end devices, such as PCs in administration. Communication is not divided, meaning the other devices in the network can see the IPv4 traffic in BACnet and potentially influence it.

To make this location fit for BACnet/SC, a UBR-02 containing two network cards can be used. One of the network cards routes the data into the local network for building automation. The network's end devices are therefore separated from other devices in the rest of the local network and thus secured. The second network card connects the site network to the BACnet/SC hub in the control centre using the local Internet router. This allows for communication between the location and hub for encrypted data transmission.

Conclusion

The UBR-02 can ensure the most security for locations that only have a single Internet connection that is used by the whole building automation network.



Description of the graphic left side

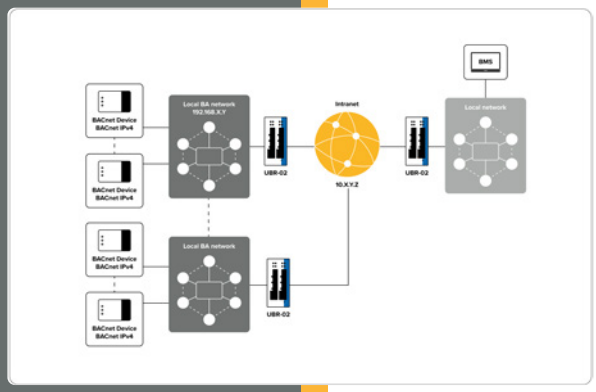
The scenario on the left side shows a similar local network at a company location. However, this scenario does not involve any other end devices other than BACnet/IPv4-compatible devices for building automation. For transmitting data between a local network and the Internet, an IP-compatible DSL router is also used (does not have to be compatible with port forwarding) as there is no need for static or dynamic IP addresses here.

In contrast to the scenario on the right side, however, the existing BACnet is translated into BACnet/SC and thus encrypted using a UBR-01 (with just one network card). The UBR-01 also uses the same network card to encrypt communication with the building control system via the DSL router.

Conclusion

This simplified set-up can be useful if the local network does not contain any other devices and the Internet connection is used solely for building automation.

BACnet/SC in a campus network (variant 1)



Starting point

A hub in a campus network with lots of participants that are interconnected via an intranet. Data exchange in building automation is currently carried out via BACnet/IPv4. Hospitals or university campuses are examples of this.

The hub is found in the building control system, which accesses the building-related systems in individual offices and building groups via an intranet. The local networks include both internal networks with BACnet/IPv4-compatible devices for building automation and other end devices, such as PCs in administration.

The challenge

These systems are virtual islands within local networks which exchange their data with BACnet/IPv4. The data packages are sent without encryption and can be viewed (and potentially changed) by all participants in the network.

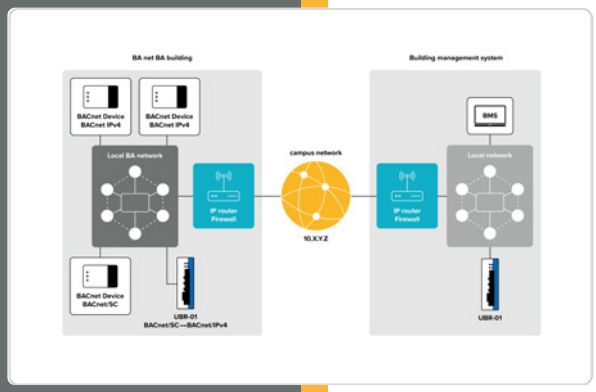
The solution

A UBR-02 can be used to physically secure building-related systems. Both of its network cards allow users to separate campus and building automation networks: one network card is used to exclusively route BACnet data between both networks. The second network card is used to enable campus communication with BACnet/SC. The data traffic can no longer be viewed by participants outside of building automation thanks to encryption.

Conclusion

The UBR-02 can ensure the most security in a local campus network.

BACnet/SC in a campus network (variant 2)



Starting point

A hub in a campus network with lots of participants that are interconnected via an intranet. Data exchange in building automation is currently carried out via BACnet/IPv4. Hospitals or university campuses are examples of this.

The hub is found in the building control system, which accesses the building-related systems in individual offices and building groups via an intranet. A local IP sub-network for general data traffic is shown on the right side. The local building automation network is shown on the left. Both sub-networks are connected to the network via an IP router.

The challenge

These building-related systems are virtual islands within local networks which exchange their data with BACnet/IPv4. The initial connection in BACnet is established using so-called BACnet Broadcast Management Devices (BBMD), which can be time-consuming to configure. The data packages are sent without encryption and can be viewed (and potentially changed) by all participants in the other sub-network.

The solution

A UBR-01 can be used in both sub-networks to physically secure building-related systems. Each of its network cards can be used to exclusively route BACnet/SC data into each sub-network. This ensures that data traffic on the intranet is encrypted. In addition, the individual devices no longer communicate individually via the intranet and instead communicate via the UBR-01.

Conclusion

The UBR-01 can provide the most security in a local campus network with sub-networks and makes configuring end devices much easier.

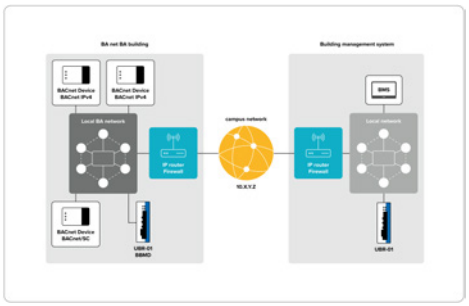
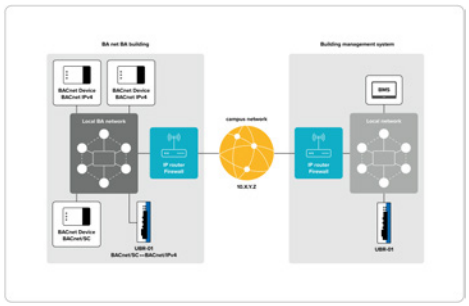
Our tip: MBS GmbH can support businesses in transitioning from BACnet/IPv4 to BACnet/SC:

- property inventory
- network analysis
- development of suggestions for solutions and their implementation
- delivery
- installation of BACnet/SC-compatible devices
- as complete service or individual service (e.g. including training).

Contact us – we're happy to help.

Before - After representation

BACnet/IPv4 - BBMD — BACnet/SC

	BACnet/IPv4 - BBMD	BACnet/SC
BACnet in the campus network		
Firewall options	Firewalls must allow for UDP (User Datagram Protocol) from each BACnet device in the network to every other BACnet device.	Firewalls can restrict BACnet traffic with TCP (Transmission Control Protocol) to the BACnet/SC router in the individual sub-networks.
IP configuration of individual BACnet devices	Each BACnet device must be configured to the local IP router/firewall so that it can reach all other BACnet devices (e.g. using a default route).	The BACnet devices must only communicate with other devices (including SC route in the local building automation network) directly. Internal IP routing across the entire campus network is not necessary.
Security in the campus network	The BACnet traffic in the campus network is unencrypted and unsecured via BACnet/IPv4.	The BACnet traffic in the campus network is encrypted and secured via BACnet/SC.
BBMD-configuration	required	not required

MBS GmbH | Römerstraße 15 | 47809 Krefeld | Tel. +49 21 51 72 94-0 | info@mbs-solutions.de

Imprint: **Managing Director:** Gerhard Memmen-Krüger, Nils-Gunnar Fritz
Register court: Krefeld HRB 33 7, USt.-IdNr.: DE 120 148 529, Headquarters: Krefeld
Responsible for contents according to § 6 MDStV: Gerhard Memmen-Krüger, Nils-Gunnar Fritz