BACnet Secure Connect

Passer à BACnet/SC

Afin d'utiliser BACnet Secure Connect (BACnet/SC) dans l'automatisation des bâtiments (AB), un exploitant immobilier pourrait bien sûr mettre en place une infrastructure d'appareils compatibles avec BACnet/SC qui couvrirait toute la surface. Cependant, si l'on considère qu'environ 25 millions d'appareils terminaux transfèrent actuellement leurs données via BACnet, il devient vite évident que leur remplacement complet nécessiterait des efforts considérables.

Pour ceux qui espèrent peut-être sur une mise à jour (pas encore prévisible pour l'instant) de leurs appareils existants, ils devraient garder en tête que le matériel existant pourrait ne pas supporter la puissance de calcul requise par BACnet/SC.

Il est donc judicieux de planifier une transition : avec une combinaison de l'infrastructure BACnet/IPv4 existante (Internet Protocol Version 4) et du matériel compatible avec BACnet/SC. Intégrée à l'infrastructure traditionnelle, cette combinaison va au-delà d'une simple liaison entre BACnet et BACnet/SC, et permet, au contraire, d'isoler physiquement l'échange de données via BACnet/IP. De cette manière, une communication des données sécurisée et cryptée au sein de l'automatisation des bâtiments est garantie.

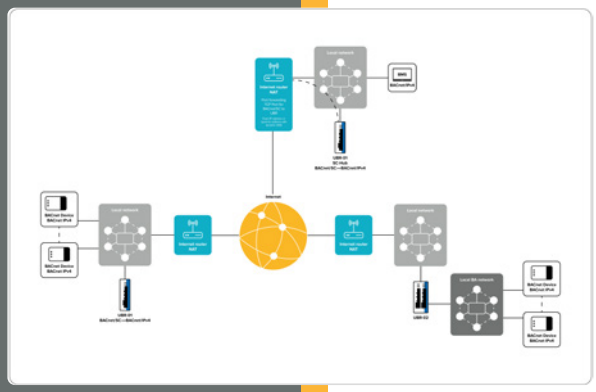
Les trois graphiques ci-après représentent des topologies de réseau courantes pour l'automatisation des bâtiments et sont destinés à fournir des suggestions sur la manière de réussir le passage à BACnet/SC.

Principes généraux: pour rendre un réseau conventionnel compatible avec BACnet/SC, sa topologie doit être modifiée. À cet effet, chaque réseau se voit attribuer un point central – le fameux « hub » – lors de la configuration. Ce centre

- gère le trafic de données entre un nombre quelconque d'appareils terminaux et
- prend en charge l'analyse du trafic de données afin de vérifier à combien d'appareils terminaux les informations doivent être transmises.

Le routeur universel BACnet (RUB) de MBS peut s'en charger. Intégré dans le réseau local de la gestion technique, l'appareil est utilisé depuis longtemps déjà pour la mise en œuvre des topologies de réseau BACnet ISO 8802-2 (également connue sous le nom de BACnet/Ethernet), BACnet/IP et MS/TP (réseaux BACnet série basés sur RS485). Il prend désormais également en charge la révision 22 actuelle de BACnet et convient par conséquent à la mise en place de la structure de sécurité innovante BACnet/SC. L'UBR-01 et l'UBR-02 contiennent respectivement une et deux cartes réseau. Le choix de l'appareil à utiliser dépend des circonstances spécifiques.

Relier toutes les installations par Internet avec BACnet/SC



La situation initiale

Une centrale avec des sites répartis dans le monde entier et reliés les uns aux autres via Internet. Actuellement, l'échange de données dans l'automatisation des bâtiments via BACnet/IPv4 ne serait possible que si tous les sites étaient connectés via un VPN. Parmi les exemples d'application, on trouve une entreprise avec des sites répartis dans le monde entier, un organisme public avec des écoles et des gymnases reliés, ou encore d'une chaîne de supermarchés avec ses filiales.

La centrale renferme la gestion technique du bâtiment (GTB), qui doit pouvoir accéder aux systèmes de technique du bâtiment. L'interface menant au World Wide Web consiste en un routeur Internet avec un pare-feu.

Le défi

L'échange de données via IPv4 n'est pas crypté. De plus, le protocole de commande DHCP (Dynamic Host Configuration Protocol) n'est pas supporté pour l'attribution automatique d'adresses IP, pourtant fort utile lors de la gestion de grands réseaux. Jusqu'à présent, la sécurisation de tels réseaux d'AB nécessitait la mise en place complexe de VPN (Virtual Private Network).

Que faire?

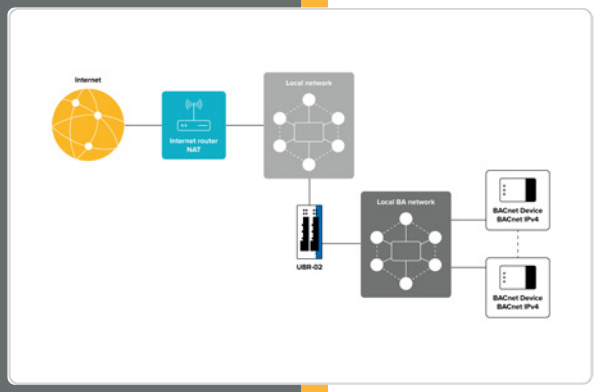
Dans cet exemple, le routeur Internet transmet les données à l'UBR-01 qui, avec sa carte réseau intégrée, agit comme un convertisseur de médias pour traduire le protocole de données BACnet/IPv4 en BACnet/SC. Deuxièmement, il crypte l'échange de données.

Connexion de la centrale

Pour accéder à Internet, soit le routeur Internet IP de la centrale dispose d'une adresse IP statique, soit son adresse dynamique peut être résolue via un DNS dynamique. Les paquets de données entrants sont transmis à un UBR-01 via un port défini (Port Forwarding). L'UBR-02 agit ici en tant que hub SC et en tant que routeur BACnet afin qu'une GTB avec BACnet/IPv4 puisse continuer à être utilisée.

Connexion des sites

En dessous de la gestion centrale, deux versions sont présentées sur la façon dont les systèmes de technique du bâtiment dans les sites répartis peuvent être reliés à la gestion technique dans ce scénario.



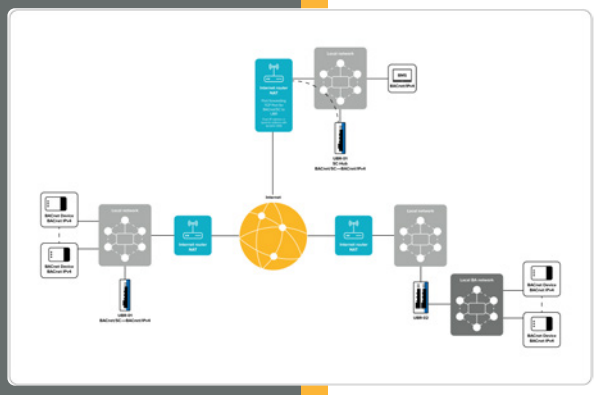
Description du graphique à droite

À droite, un routeur est mis en place pour la transmission de données entre le système local et Internet, par exemple un routeur DSL compatible IP. Il ne doit pas nécessairement supporter le Port Forwarding. Le réseau local comprend non seulement son propre réseau d'appareils compatibles avec BACnet/IPv4 pour l'automatisation des bâtiments, mais aussi d'autres appareils terminaux tels que des PC dans l'administration. La communication n'est pas séparée ; cela signifie que les autres appareils du réseau peuvent visualiser le trafic IPv4 dans BACnet, et exercer une influence dessus si nécessaire.

Un UBR-02 contenant deux cartes réseau peut être utilisé pour rendre ce site compatible avec BACnet/SC. Une des cartes réseau achemine les données vers le réseau local pour l'automatisation du bâtiment, dont les appareils terminaux sont ainsi séparés des autres appareils du reste du réseau et par conséquent sécurisés. La deuxième carte réseau relie le réseau du site à BACnet/au hub SC de la gestion centrale via le routeur Internet local. De cette manière, la transmission cryptée de données est également assurée dans la communication entre le site et la centrale.

Conclusion

Si un site ne dispose que d'un seul raccord à Internet et qu'il est également utilisé par le réseau de l'AB, l'UBR-02 offre la plus grande sécurité possible.



Description du graphique page de gauche

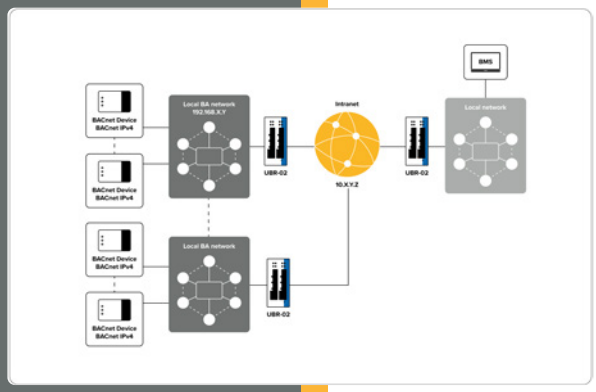
Le scénario de la page gauche présente un réseau local similaire sur le site d'une entreprise. Outre les appareils compatibles avec BACnet/IPv4 pour l'automatisation des bâtiments, il inclut toutefois aussi d'autres appareils terminaux. Un routeur DSL compatible IP est également utilisé pour la transmission de données entre le réseau local et Internet, qui n'a pas besoin d'être compatible avec le Port-Forwarding, car aucune adresse IP fixe ou attribuée de façon dynamique n'est requise ici.

Contrairement au scénario de la page droite, le BACnet existant est traduit en BACnet/SC et donc crypté avec un UBR-01 (avec une seule carte réseau). Toujours avec la même carte réseau, l'UBR-01 communique en outre avec la GTB de façon cryptée via le routeur DSL

Conclusion

Cette variante plus simple peut s'avérer très utile si le réseau local ne comprend aucun autre appareil et que la connexion à Internet est exclusivement utilisée pour l'automatisation des bâtiments.

BACnet/SC dans le réseau d’un campus (version 1)



La situation initiale

Une centrale sur le réseau d’un campus avec de très nombreux participants qui sont mis en réseau via l’intranet. Actuellement, l’échange de données dans l’automatisation des bâtiments est réalisé via BACnet/IPv4. Un exemple d’application pourrait être un complexe hospitalier ou un campus universitaire.

La centrale renferme la gestion technique du bâtiment (GTB), qui accède aux systèmes de technique du bâtiment dans les différentes unités et groupes de bâtiments via l’intranet. Le réseau local comprend non seulement son propre réseau d’appareils compatibles avec BACnet/IPv4 pour l’automatisation des bâtiments, mais aussi d’autres appareils terminaux tels que des PC dans l’administration.

Le défi

Ces systèmes sont des quasi-îlots issus de réseaux locaux qui échangent leurs données par BACnet/IPv4. Les paquets de données sont envoyés non cryptés et peuvent être consultés, et modifiés si nécessaire, par tous les participants du réseau.

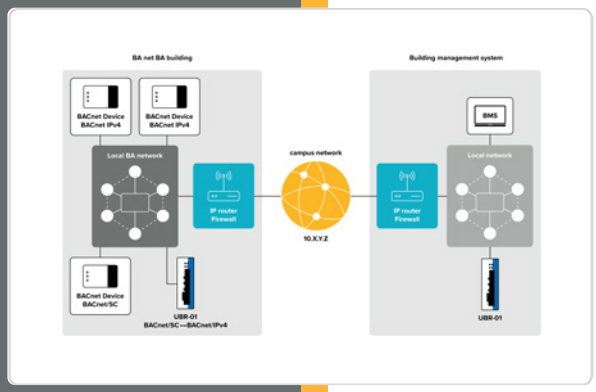
Que faire?

Pour sécuriser physiquement les systèmes de technique du bâtiment, on peut recourir à un UBR-02, dont les deux cartes réseau permettront de séparer le réseau du campus de celui de l’AB. Une carte réseau est utilisée pour acheminer uniquement les données BACnet entre les deux réseaux. La seconde se charge de la communication avec BACnet/SC au sein du campus. Grâce au cryptage, le trafic de données n‘est plus visible pour les participants en dehors de l‘automatisation du bâtiment.

Conclusion

Dans un réseau de campus local, l’UBR-02 offre la plus grande sécurité possible.

BACnet/SC dans le réseau d’un campus (version 2)



La situation initiale

Une centrale sur le réseau d’un campus avec de très nombreux participants qui sont mis en réseau via l’intranet. Actuellement, l’échange de données dans l’automatisation des bâtiments est réalisé via BACnet/IPv4. Un exemple d’application pourrait être un complexe hospitalier ou un campus universitaire.

La centrale renferme la gestion technique du bâtiment (GTB), qui accède aux systèmes de technique du bâtiment dans les différentes unités et groupes de bâtiments via l’intranet. Un sous-réseau IP local pour le trafic de données général est représenté à droite et le réseau AB local à gauche. Les deux sous-réseaux sont reliés au réseau via un routeur IP.

Le défi

Ces systèmes de technique du bâtiment sont des quasi-îlots issus de réseaux locaux qui échangent leurs données avec BACnet/IPv4. L’établissement de la connexion initiale dans BACnet est effectué à l’aide de « BACnet Broadcast Management Devices » (BBMD), ce qui exige une configuration complexe. Les paquets de données sont non seulement envoyés non cryptés, mais peuvent également être consultés, et modifiés si nécessaire, par tous les participants de l’autre sous-réseau.

Que faire?

Pour sécuriser physiquement les systèmes de technique du bâtiment, on peut recourir à un UBR-01 dans chacun des deux sous-réseaux. Ses cartes réseau sont utilisées pour router uniquement des données BACnet/SC dans chacun des sous-réseaux. De cette manière, le trafic de données dans l’intranet est crypté. De plus, les différents appareils ne communiquent plus de façon autonome via l’intranet, mais toujours via l’UBR-01.

Conclusion

Dans le réseau local d’un campus avec des sous-réseaux, l’UBR-01 offre non seulement la plus grande sécurité possible, mais simplifie aussi considérablement la configuration des appareils terminaux.

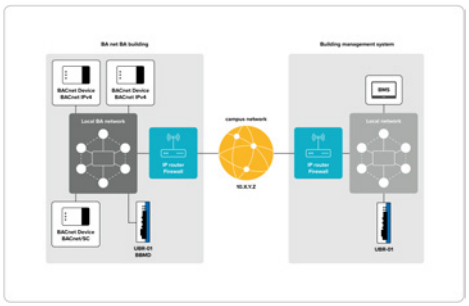
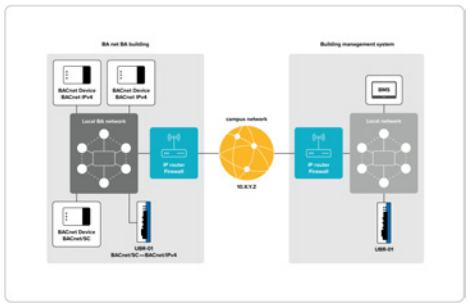
Notre conseil: MBS GmbH accompagne les entreprises dans la transition de BACnet/IPv4 vers BACnet/SC:

- en commençant par l’état des lieux d’un bien et
- l’analyse réseau en passant par
- l’élaboration de propositions pour la solution et la mise en œuvre
- jusqu’à la livraison et
- l’intégration des appareils compatibles BACnet/SC
- en tant que service complet ou service individuel (comme par exemple les formations également).

Posez-nous vos questions, nous serons ravis d’y répondre.

Représentation avant - Après

BACnet/IPv4 - BBMD — BACnet/SC

	BACnet/IPv4 - BBMD	BACnet/SC
BACnet dans le réseau d'un campus		
Options de pare-feu	Les pare-feux doivent autoriser l'UDP (User Datagram Protocol) de chaque appareil BACnet du réseau vers tous les autres appareils BACnet.	Les pare-feux peuvent limiter le trafic BACnet à l'aide de TCP (Transmission Control Protocol) vers les routeurs BACnet/SC dans chaque sous-réseau.
Configuration IP des différents appareils BACnet	Chaque appareil BACnet doit être configuré, par exemple avec une route par défaut sur le routeur IP/pare-feu local, afin qu'il puisse atteindre tous les autres appareils BACnet.	Les appareils BACnet doivent uniquement communiquer directement avec les autres appareils, y compris avec le routeur SC du réseau local d'AB. Un routage IP propre sur l'ensemble du réseau du campus n'est nécessaire.
Sécurité dans le réseau du campus	Le trafic BACnet dans le réseau du campus n'est ni crypté ni sécurisé via BACnet/IPv4.	Le trafic BACnet dans le réseau du campus est crypté et sécurisé via BACnet/SC.
Configuration BBMD	nécessaire	inutile

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