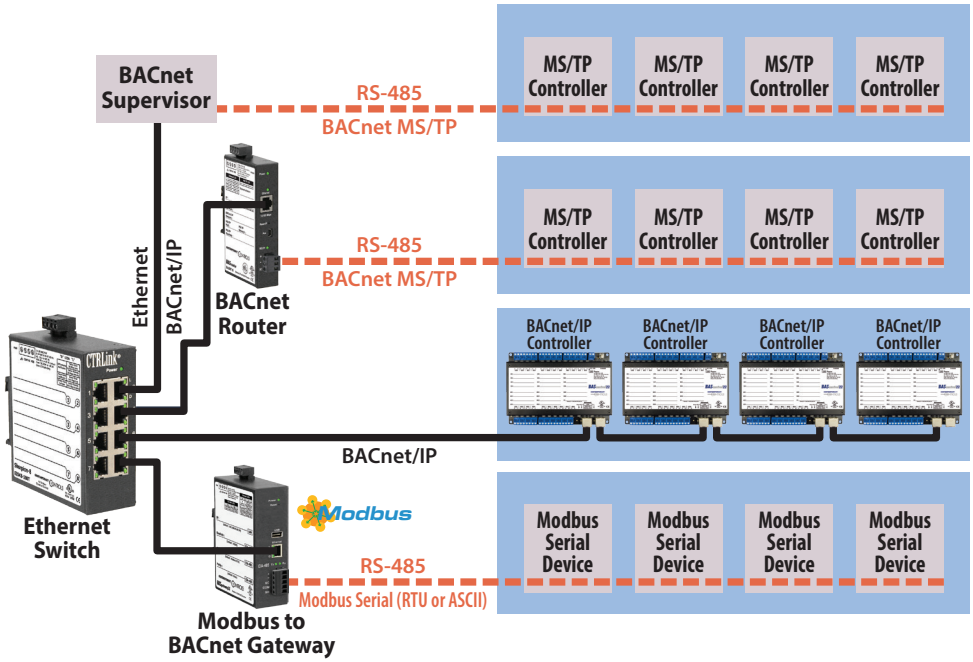
Deploying and Maintaining BACnet Systems in Today's Networks

CONTEMPORARY CONTROLS®

HVAC has made long strides from the days of pneumatic controls to Direct Digital Controls (DDC). DDC systems allow for more precise control of the equipment and processes, leading to greater efficiency. These DDC systems can be networked together over a communication protocol evolving into a Building Automation System (BAS). The Building Automation Systems of today utilize various protocols, such as Modbus, LonWorks, and KNX, but BACnet is the most popular protocol utilized in HVAC/R control systems. There are multiple vendors that support this open protocol which provides a robust ecosystem of devices to choose from. Gateways are available to integrate other protocols to BACnet. BACnet supports communication over multiple transport layers, such as RS-485 interface with BACnet MS/TP, an Ethernet interface with BACnet/IP and BACnet over Ethernet, and more recently BACnet/SC. This article will explore some of the best practices to keep in mind while deploying BACnet. There are considerations which include choosing between MS/TP and Ethernet, size of networks, number of devices, integration with existing IT infrastructure, future expansion capability, and cost. A one-size-fits-all approach cannot be utilized anymore with these networked systems, and the contractor, systems integrator and building owner must all work in tandem to choose the best option based on their requirements.

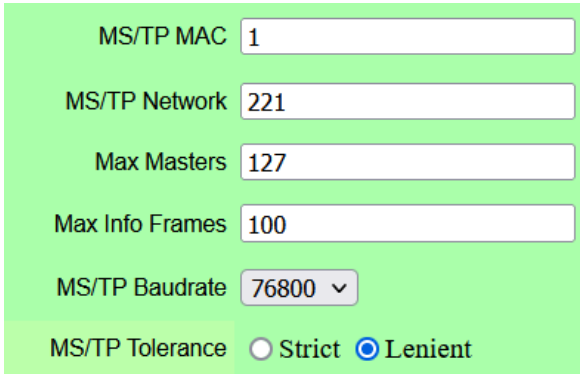
BACnet MS/TP Networks

Over a decade ago, MS/TP networks dominated building automation, and IP networks were rare. MS/TP provided longer cable distances, devices could be daisy chained over a bus, and MS/TP cables were cheaper than Ethernet cables. This allowed the MS/TP devices to be kept separate from the IP network traffic, but they could be easily integrated into a BACnet Supervisory Controller directly or by using a BACnet router. MS/TP networks specify a maximum load of 32 devices on the bus. However, with half or quarter load RS-485 transceivers, more devices can operate over the same segment. BACnet MS/TP can support up to 128 MS/TP master devices that participate in the token passing using MAC addresses from 0 to 127. The more the number



Flexible Architecture with BACnet/IP and BACnet-MS/TP

of devices in the segment, the longer it will take for the token passing to occur on the bus leading to slower communication. In practice, 32-64 devices in a MS/TP segment are suggested for optimal communication. Using BACnet routers offers a low-cost option for segmenting MS/TP networks.

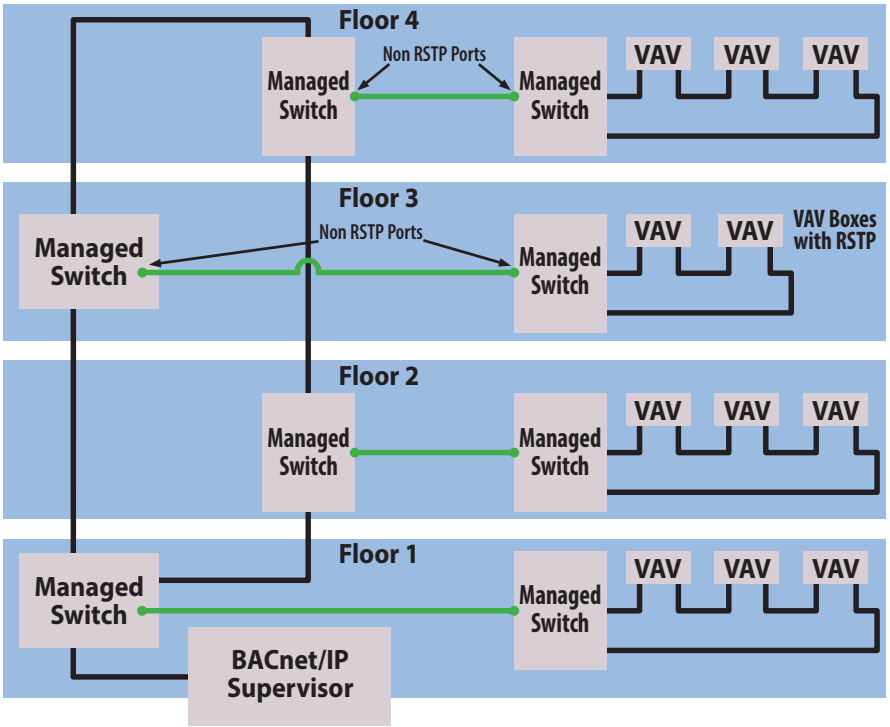


Tune MS/TP Settings for faster communication

Specifying the MS/TP device MAC addresses in a consecutive range also eliminates polling for non-existing MS/TP master devices. The MS/TP devices provide a setting called Max Masters to indicate the highest MAC address on the bus. The default value of 127 should be changed to the actual highest MS/TP MAC for fastest communication. But if some additional MS/TP devices are planned to be added later to the segment, the Max Masters should be incremented to allow for that expansion. A common issue while adding MS/TP devices is having a Max Masters value lower than the MS/TP MAC of the new device thereby preventing it from receiving the MS/TP token and participating in communication. Today, MS/TP networks remain popular, providing communication to field devices with supervision from high performance BACnet/IP headends. Multiple BACnet routers can be used to integrate the MS/TP segments back to IP networks. Usually the MS/TP devices utilize less powerful CPUs, and BACnet routers can also provide additional features to separate the MS/TP segment from extra BACnet traffic. For example, blocking broadcast I-AM messages if there are only MS/TP end devices on the MS/TP segment saves valuable CPU resources, especially in a large network. Having a smaller MS/TP segment helps isolate a problem to that specific segment because one bad MS/TP device can impact the performance of all devices on that segment.

BACnet/IP in IT Infrastructure

Today, BACnet networks share IP infrastructure with business networks, high-speed cameras, and IP routers. The result is an immense amount of IP traffic, unrelated to BACnet, impacting the throughput of BACnet networks. The best way to handle the congestion is to restrict communication to only those devices that must be part of the BACnet communication. The use of IP protocol with BACnet/IP lends well to the use of IT best practices to manage the traffic and provide security for BACnet networks. One technique available in TCP/IP routers to restrict the communication is the use of Allowlist to only accept traffic from specific BACnet devices. The Allowlist feature can restrict BACnet/IP traffic to only the BACnet headends and supervisors specified in the Allowlist, thereby providing additional security, and eliminating the devices' need to respond to unrelated messages. Additional options include segmenting networks either by restricting



Redundant topology with Managed Ethernet Switches and VAVs using RSTP

the number of devices in an IP subnet domain with the use of IP routers or separating them logically with the use of Virtual Local Area Networks (VLANs). This again leads to a choice between using low-cost, unmanaged Ethernet switches to connect the Ethernet segments with plug-and-play operation or using managed Ethernet switches that provide features such as VLAN, fault detection, SNMP for traffic count, and redundancy with Rapid Spanning Tree protocol (RSTP).

Managed Ethernet Switches – Redundancy and VLANs

RSTP is an IEEE protocol that has been used to provide cable redundancy in Ethernet networks. Quite a few IP controllers and rooftop units (RTUs)and air handling units (AHUs) have two Ethernet ports to daisy-chain devices for easy wiring. An issue with daisy-chaining devices that impacts both MS/TP and IP devices is that a cable break renders the devices after the break unreachable. By using RSTP, the IP devices can be wired in a ring topology where the protocol keeps one Ethernet port in blocking state to prevent a communication loop. If a cable break occurs, the backup port is enabled allowing the communication to continue. The maximum number of devices in an RSTP ring is 40. This warrants the use of Managed Ethernet switches for all devices to support, with the RSTP protocol enabled. A common issue seen is mixing unmanaged Ethernet switches to save cost by justifying that the cable break at the segment will not occur, thereby jeopardizing the whole setup. Another issue is having two RSTP rings conform to the size of 40 devices going back to the same managed switch backbone. A break in these two rings will lead to the violation and exceed the 40-device limit in the RSTP segment. It is advisable to use a separate backbone of Managed Ethernet switches with RSTP and then have another managed switch that provides an RSTP segment for the AHUs/RTUs. The RSTP protocol on the Ethernet ports connecting this managed switch for AHUs to the main RSTP backbone Ethernet switch should be disabled. To prevent communication loss due to a power failure, some dual Ethernet port devices utilize an internal relay to bridge the two Ethernet ports together, effectively incrementing the Ethernet segment length. The stipulation for maximum Ethernet segment length of 100 m still applies, and care must be taken not to exceed this distance when the device loses power.

Managed Ethernet switches also provide the VLAN feature to keep groups of devices in logical partitions even though the same physical Ethernet cable carries the traffic. This can be useful to keep the high traffic IP cameras separate from the BMS system. A 10-year-old BMS system may not be able to keep up with the high multicast traffic from the cameras, while new BACnet/IP controllers with powerful CPUs will work fine in the same network. Using managed switches with VLANs provides a secure and easy way to prolong the life of the BMS systems.

Network Sizing and limiting Traffic using IP Routers

Segmenting using IP routers also provides a convenient way to manage and later expand IP networks. It may seem easy to have a flat network for all the devices, but then all the devices are inundated with the extra broadcast and multicast traffic on this single subnet. The IP routers keep the broadcast and multicast traffic constrained to their own IP subnets. A few years ago, a single bad Ethernet card was blamed for bringing

down an airline system at an airport. This is analogous to having a big warehouse with an open office where all departments and personnel are trying to communicate over one another versus subdividing that office space into different sections and rooms. BACnet communication relies on the use of broadcast messages for device discovery, but a BACnet/IP Broadcast Management Device (BBMD) can easily be used to facilitate BACnet communication across subnets. Almost all the BACnet/IP to MS/TP routers provide BBMD functionality, though the support of the number of BBMDs/subnets may vary. Vendors may have different models to support different network sizes. A gas station with a few devices needs to be designed differently than a high-rise office building. Care must be taken not to create a BACnet loop by improper duplicate BBMD entries.

IP routers also facilitate the integration of BACnet devices in the existing IT infrastructure. The IT personnel only need to assign one IP address for the WAN port of the IP router, and all the BACnet devices can form their own networks on the LAN subnet with an independent IP address scheme. Compare this to getting IP addresses for each device that must be integrated. The IT department may still need to know some information regarding the devices being added to the BMS system but will surely appreciate the option of not handing out additional IP addresses. We explored how to separate BACnet devices from extra traffic within business networks, but the reverse is also true. The IP routers also prevent the BACnet traffic from reaching the business system network. Additional IP router features, such as VPN, provide remote access for diagnostics and troubleshooting.

The BMS systems are installed for comfort, occupant safety, as well as energy savings. Many times, a BMS system must be changed when the building owner wants to change maintenance contractors, but the owner later finds out that he only has the login credentials for viewing the display graphics and doesn't have the administrative credentials to make additional changes. Having access to the administrative credentials for the BMS system is a must for building owners. The advent of security in BACnet with BACnet/SC and the push towards IP networks in general for BACnet will warrant a closer collaboration between HVAC and IT departments, and it is imperative that basic knowledge regarding IP networks be part of companies' training plans for their personnel.

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