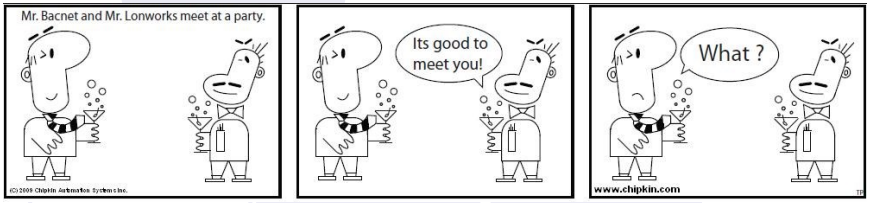
CHIPKIN

BACnet for Field Technicians

Chipkin Automation Systems presents a short guide filled with practical information

Updated Rev 2.0 - Feb 2024

By Peter Chipkin



Need Answers ?

- Why can't I discover devices on another subnet?
- Why can't a new device be discovered on a MSTP network?
- What cable should we use for MSTP?

BACnet is a registered trademark of ASHRAE

LonWorks is a registered trademark of Echelon Corporation

Revision 2.0

Mailing Addr: 3381 Cambie St, # 211, Vancouver, BC , Canada, V5Z 4R3

Thanks to Tim Plumridge our cartoonist.

CHIPKIN

Table of Contents

BACnet Introduction

Introduction

BACnet is a building automation and control networking protocol. It was developed by ASHRAE. BACnet was designed specifically to meet the communication needs of building automation and control systems. Typical applications include: heating, ventilating, air-conditioning control, lighting control, access control, and fire detection systems.

History and Background

Who cares. It works. It's open and it's growing.

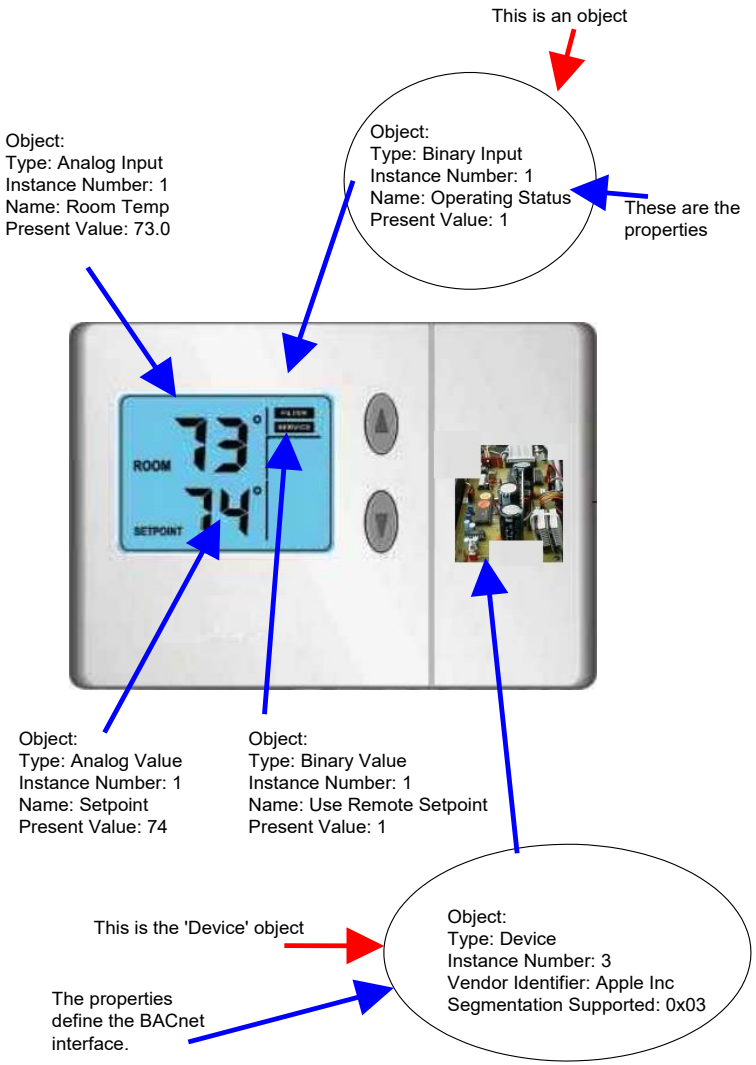
Flavors Of BACnet

Clarification

Native BACnet – What does that mean? In the Building Automation world, the term 'Native' means that a device supports that functionality / protocol without the addition of a gateway or other modules.

Flavor	Application	Affects you ?
IP	• Uses the IP protocol • Device to device • Device to HMI • Some field devices.	On the up
Ethernet 802.3	• Raw Ethernet Packets	Being displaced by IP
Point to Point	• Modems and phone lines	Rare. Expect to disappear
MS/TP	• Field Devices	Millions of installed devices
ARCnet	• Device to device	Rare. Expect to disappear
Secure Connect	• Hub and spoke	New and rising

BACnet Objects and Properties



BACnet Objects and Properties cont'd

Data inside a BACnet device is organized as a series of objects. Each object has a type and a set of properties. There is always at least one object in a device – it is used to represent the device itself. The other objects represent the device's data.

In practical terms, think of a simple thermostat. Our example is a simple device that has a temperature sensor. It allows the set point to be changed locally or remotely, has a local remote selection, and reports if there is an internal fault by reporting its status as normal/abnormal.

Useful Tip

The **device object** is the first object read after a device is discovered because it has lots of interesting information for the client. For example, the device object has properties that report whether the device supports COV, whether more than one property can be read in a single message, etc.

Useful Tip

Unique Numbers are required for BACnet Device Object Instance Numbers across the entire BACnet intra-network. Duplicates can exist if the devices are on completely separated networks (i.e. different subnets where the network mask for broadcasts do not encompass the subnets). See 'Extra' in 'Working Example: Routers and BBMD' section for example.

Heads Up

Some vendor systems and controllers require each object within a device to have a **unique name** because they use the name as an internal index key. This is called "Who-Has" by Object Name.

CHIPKIN

BACnet Objects and Properties cont'd

Commonly used properties - Almost all objects you encounter will have these (and more) properties.

Object Type:
Popular Object Types: Analog Input (AI), Analog Output (AO), Binary Input (BI), Binary Output (BO).

Instance Number:
A number that must be not be repeated for any other object of the same type. The instance number and the object type must be unique for every object in a device.

Name:
Speaks for itself.

Present Value:
The current value of the object. BACnet has ways of telling you if the present value is valid – it uses a property called 'Reliability'.

Example of the properties and their values for a BACnet data object.

object-identifier:	*analog-input [180]*
object-name:	*One_sec_Ph_A-NVolt*
object-type:	*analog-input*
present-value:	*100.000000*
status-flags:	*In-Alarm=[false], Fault=[true], Overriden=[false], Out-Of-Service=[false]*
event-state:	*normal*
reliability:	*unreliable-other*
out-of-service:	*False*
units:	*Volts*
description:	*Zero length/empty string*

BACnet Objects and Properties cont'd

Multistate Object Type

One of the more versatile object types that you can use falls under Multistate. It allows you to define as many states as you desire to describe the object. However, due to this versatility, people commonly make mistakes when implementing a multistate object on a BACnet device. Here, we describe one of the most common problems that occur when using multistate objects.

Multistate objects have user-defined states in the form of enumerations. As code, they are in the form of an array, where each array index is linked to one of the states (states are CharacterString). As an example, you may have a BACnet lighting device with states 1=Off, 2=On, and 3=Blinking. Right away, you may notice that our enumeration starts at 1, but the array starts at 0. This is a common pitfall for people because they assume that the first state will be in the first slot of the array - index 0. For multistate objects, the 0th index is reserved for the size of the enumeration (or the number of states). By setting the device's state to 0, for example, you will be setting the state into an invalid/incorrect state. The consequence of doing so may vary. For some devices, nothing significant may happen. For other devices, it might randomly assume an unexpected state that could be dangerous for the device and/or its environment.

BACnet Supports Discovery

In Modbus, you need a data sheet to know what data is inside a field device. In BACnet, you don't. You can go online, discover the devices on a network and then interrogate the devices so they report what data objects they contain, what properties each object supports, and what the current state of each property is.

The ability to discover is an almost universal truth in BACnet, but there is an obscure technicality that may limit what you can learn about the object properties – devices that support Read-Property-Multiple and don't support segmentation may not be able to fill the response into a single message and thus doesn't respond with useful information. See Segmentation in BACnet for more details.

We should also mention that most 'Discoverers' (or clients as we like to call them) cannot discover the names of vendor-created proprietary properties, object types, or enumerations.

What are vendor-created proprietary properties?

Vendor-created proprietary properties are special manually-created properties that are not associated with the ones documented by BACnet specification. These properties are often given a property ID greater than 512 where all values below 512 are the pre-determined properties provided by BACnet.

Why can't vendor-created proprietary properties be discovered?

While vendor-created properties allow for customizability of the device, one downside to this is that BACnet is only able to provide the value of the property. As the ID is out of the range of values BACnet can interpret, it will not be able to provide any interpretation of that value and so vendors are in charge of knowing and documenting the details about the property themselves.

BACnet Supports Discovery cont'd

There are two important practical implications of discovery:

1. If your client software is half decent, you do not have to type object/ properties into the configuration screens. You simply discover and then drag and drop. Unfortunately, more than half the BACnet software out there is not half decent.

2. You would think you can get away without data sheets, but again, you are then dependent on how decent a job the device vendor did in naming and describing their points. Bad naming, missing object descriptions, and unimplemented properties like max and min values make your job harder and force you to use vendor docs.

Useful Tip

To discover devices on a **foreign subnet,** you can configure the router to forward UDP broadcasts or you can use BBMDs.

BACNET BBMD Connects Networks

The BACnet discovery uses two services called 'Who-Is' and 'I-Am'. The 'Who-Is' service signal is used to find/discover devices from a network using broadcasting. The 'I-Am' service is a broadcast in response to the 'Who-Is' service. It notifies the original sender of their existence.

Heads Up

Routers join IP networks together so messages from one network can be sent to another. Most routers do not forward UDP broadcast messages and this means discovery **can't discover devices on another network.**

To solve the problem above, BACnet provides a technology called BBMD - BACnet/IP Broadcast Management Device.

In overview, the technology is simple. You install a BBMD (might be a physical device or just a software application on a computer) on each network. You can configure the BBMDs by specifying the IP Address and mask of the other BBMD. This makes both BBMD configs identical. When the one BBMD receives a broadcast, it forwards the messages to the other BBMD which it re-broadcasts on the other network. They are configured by Broadcast Distribution Table (BDT) files and these may be modified on the fly using selected BACnet services.

The technology also provides for foreign device registration. This allows a device on one network to communicate with a device on another network by using the BBMD to forward and route the messages.

A detailed example of this topic can be found in the 'Worked Example: Routers and BBMD' section.

Segmentation in BACnet

Segmentation

BACnet messages that don't fit in a single packet use segmentation. Why would one message need more than one packet? Well, IP packets have a maximum length of ~1500 bytes. So if you are sending a BACnet IP message that is longer than 1500 bytes, then you need to send more than one Ethernet packet.

Example: Ask your fishing buddy if he wants another beer. The reply is short and fits in a single response packet: Yes. Now, ask him to tell you about the one that got away. He will need multiple sentences to tell you the long story. Your buddy needs you to support segmentation, otherwise you will only hear the first sentence of his story (lucky you).

Be Aware

1500 is not a hard-coded Maximum Transmission Unit (MTU) length in all Ethernet applications. Often, the size is set smaller.

Most serial protocols like MS/TP choose a small number for the MTU because an error requires retransmission and the transmission of data is slow. Thus, it is better to catch an error in a smaller packet.

How does Segmentation affect you as a user?

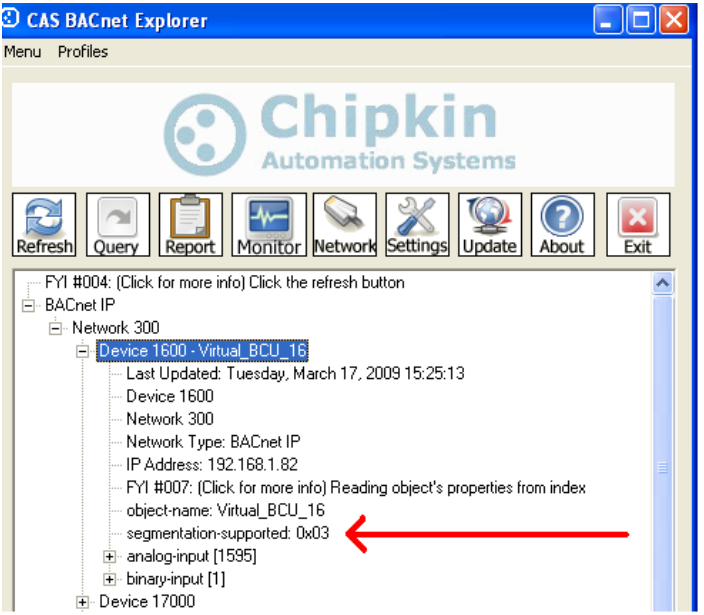
If a device has a large number of objects and a message is sent to read the object list, then it is possible that the response won't fit in a single packet. If both the device and the requestor support segmentation, then there is no problem. If either side doesn't support segmentation, then 1) You are out of luck or 2) The requestor must use a different method to read the object list - for example, reading each object using its index until it reaches an index number with no object.

The CAS BACnet explorer works like that - first, it tries the most efficient method and then it slowly downgrades itself to try and ensure the response will fit in a single packet. Not all software works in this intelligent manner.

Segmentation in BACnet cont'd

How do you know if a device supports segmentation?

You can read the vendor's PICS (Protocol Implementation and Conformance Statement) or you can look at the device object's properties.



segmented-both (0),
segmented-transmit (1),
segmented-receive (2),
no-segmentation (3)

How can you work around the segmentation issue?

Ensure you use read-property for a single property - avoid read-property for all properties. If you have to use read-property-multiple, then limit the list of properties to be read and avoid reading all of them using this service. This might not be possible if you can't configure which services get used by your system.

BACnet Services

Think of a service as a task / action. Reading and writing data uses some of the BACnet services known collectively as Data Access Service.

Building Automation Systems (BAS) / Building Management Systems (BMS) interact with BACnet devices and objects using these services. For the most part the actual service used is hidden from the engineer building / using the BAS.

When would you take an interest in what services are supported? From our point of view (as users of BACnet), we care about the services that a BACnet device supports because we want to know the capabilities that the device has. This tells us what functionalities we can use.

Example: BACnet provides a wide range of services. However, these services may not necessarily be a service that a BACnet device can handle. Take a field device as an example. Many field devices disallow the creation of new objects. However, BACnet provides a service called 'CreateObject'. An application may implement a functionality that can call this 'CreateObject' service. The problem comes in when the application tries to execute a service that is not provided by the device itself. Thus, the device may throw an error. This is an example of how the device's services provided can directly reflect the capabilities of the device.

This is the point where the services supported by the BAS and the field devices becomes interesting to you. The place to look to see what services a device supports is in the vendor PIC statement. There are three mandatory services - Read Property Service, Who-Is Service, and I-Am Service.

Unfortunately, because the actual services used by a BAS are hidden beneath the GUI, it's not always easy to know if you can exploit the capability of a field device.

BACnet Services cont'd

Useful Tip

ReadPropertyMultiple - Reads one or more properties from one or more objects BUT there is a catch. If segmentation isn't supported, then the reply must fit in a single transmission unit (typical effective for Ethernet is < 1500 bytes and for MS/TP < 480 bytes.) This is a fundamental weakness in BACnet since you can't know in advance how big the response will be. A number of (cleverer) clients will use ReadProperty to read each item when a ReadPropertyMultiple fails.

Below, is a small subset of services supported. The list below is not exhaustive and there are many more services supported than these.

Service	Notes
AddListElement Service	Rarely supported
RemoveListElement Service	Rarely supported
CreateObject Service	Rarely supported
DeleteObject Service	Rarely supported
ReadProperty Service	Always Supported
ReadPropertyConditional Service	Rarely supported - Returns a list of objects/properties that meet the specified selection criteria. E.g. all Analog Inputs.
ReadPropertyMultiple Service	Often supported
ReadRange Service	Rarely supported
WriteProperty Service	Almost always supported
WritePropertyMultiple Service	Less often supported than ReadPropertyMultiple

BIBBs

The implementation of BACnet is under-the-hood. It is invisible to most of us users. We don't know what services are supported nor do we know when each service is used. If we don't know that, then how can we tell, for example, whether a controller and field device such as a thermostat can interact?

The question is: How do you match requirements of a project to the capabilities of the devices being installed? The Answer - in BACnet - is BIBBs.

A BIBB is a BACnet Interoperability Building Block.

Continuing with our example: Say your controller needs to read the set point on a thermostat to perform its control. Then, the controller needs to support a BIBB called DS-RP-A. This isn't enough. The thermostat must be able to respond so it needs to support a BIBB called DS-RP-B. DS stands for Data Sharing. RP stands for Read Property. The A and the B stand for Client (A) and Server (B).

The outdoor temperature on a HVAC controller could come from two places - a local sensor connected to the unit or a remote value sent via BACnet. In this case, you would want to match the BAS controller and HVAC controller with BIBBs DS-WP-A and DS-WP-B (DataSharing-WriteProperty-A or B for Client and Server).

Thus, if you buy a great controller that supports Conditional and Range Reads, you would want to buy field devices that support these services. DS-RPC-A/B for DataSharing-ReadPropertyConditional-Client/Server.

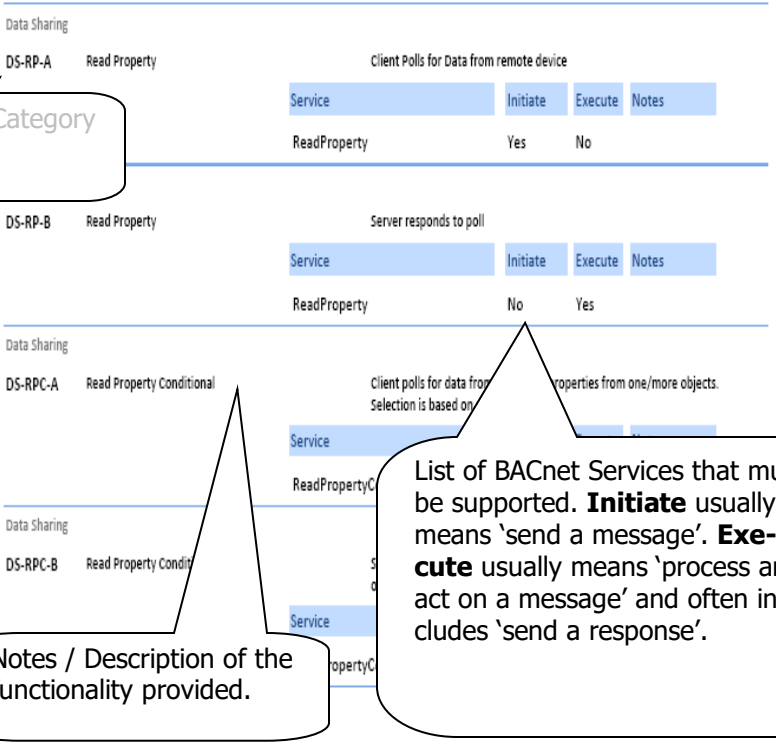
Abbreviation	BIBB Category
DS	Data Sharing
AE	Alarm and Event Management
DM	Device Management DM and NM are part of the same category.
NM	Network Management
T	Trend
SCHED	Schedule

BIBBs cont'd

Useful Tip

Device "A" and Device "B". All the BIBBs end in '-A' or '-B'. BACnet refers to the "A" device and the "B" device. The "A" device in this context is a device acting as a client (initiate). The "B" device means a device acting as a server. In BACnet devices can be both clients and servers since almost all devices can read data from each other.

Extract – The full BIBBs table is available at https://store.chipkin.com/articles/bacnet-bibbs-table-bacnet-interoperability-building-blocks



BIBB Category
BIBB

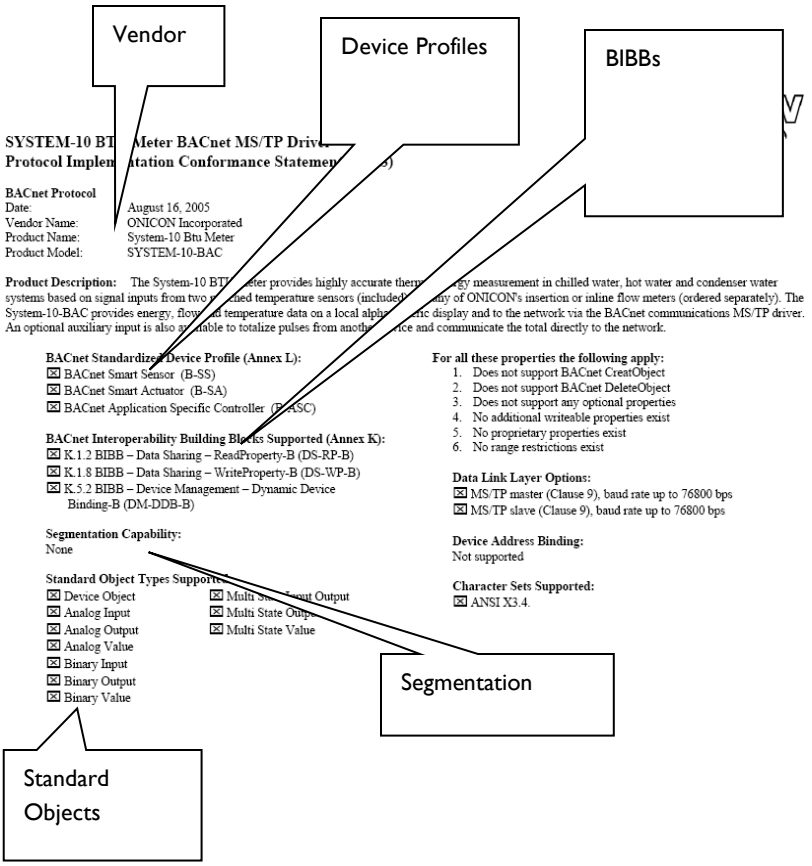
Notes / Description of the functionality provided.

List of BACnet Services that must be supported. **Initiate** usually means 'send a message'. **Execute** usually means 'process and act on a message' and often includes 'send a response'.

PIC Statements

The BACnet specification defines theoretical capabilities. The PICS tells you what capabilities have been implemented.

Every BACnet capable device (controllers, software and field devices) has a PICS. The PICS is very useful to you as a field tech, engineer or designer.



Services vs. BIBBs

Although closely-related, BACnet services and BIBBs are different. BIBBs can be seen as an abstraction for BACnet services. In other words, BACnet services are the actual services that run under-the-hood to complete the request/ requirements of a BIBB. Oftentimes, BIBBs and services have a one-to-one relationship, where there is only one underlying service that runs when a BIBB is used. Some BIBBs, however, will call upon multiple services in some way to realize the service. For example, the DS-COVP-B uses 3 BACnet services: SubscribeCOVProperty, ConfirmedCOVNotification, and UnconfirmedCOVNotification

Note

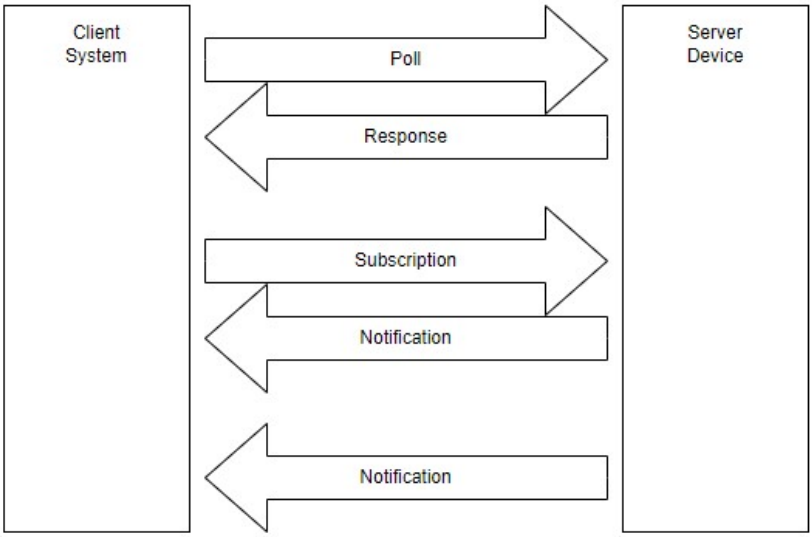
A common occurrence is that someone will often refer to some service, when they are actually referring to a BIBB. Be sure to understand whether the "service" that you are referring to is a BACnet service or actually a BIBB.

BACnet Change of Value (COV)

Introduction

Most field devices are passive servers. They wait passively for a system to poll them for data and only then do the devices respond. A consequence of this is that the data client only knows the value of an object property when it polls for the value. If the duration of an event (change of value) is shorter than the interval between polls, then the data client will not know that the event occurred.

BACnet provides a solution for this by defining services to report events. These services allow a device to be transformed from a passive server to an active server since it is now capable of sending messages reporting the value of an object property based on some event rules. BACnet COV is a subset of the 'Alarm and Event Services'.



BACnet Change of Value (COV) cont'd

This article discusses how the technology operates and then provides a discussion on some weaknesses in the COV system.

Simple Definition of COV

Data clients subscribe to an object for COV reporting. The device monitors the value of the object property, the subscription list and the change criteria. When the change criteria are met, the devices sends a notification of the new value to the subscribers.

Useful Tip

Not all devices / objects support COV

The BACnet COV system is not a mandatory part of the protocol. Each vendor decides if they want to support it. In addition, each vendor gets to decide which properties of which objects support COV.

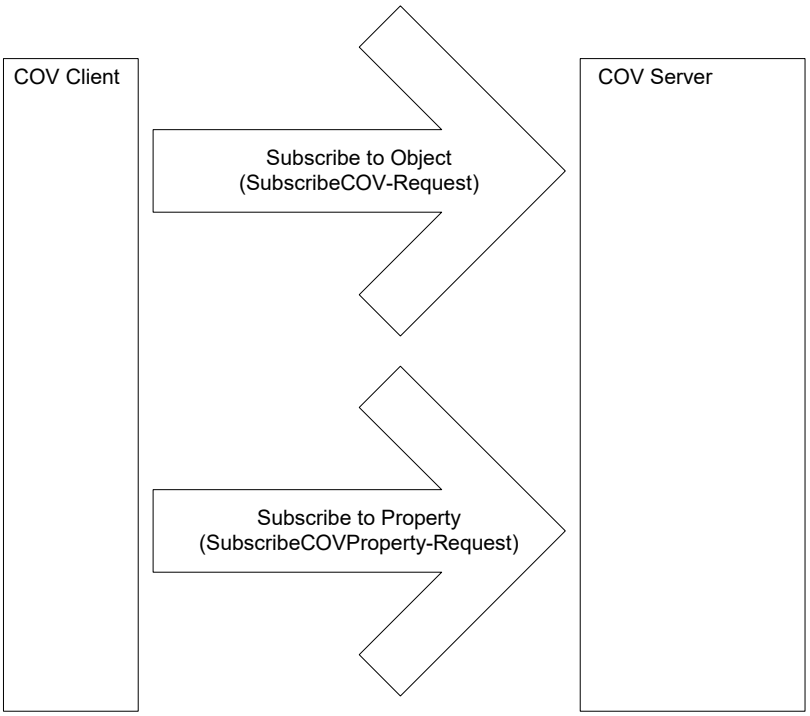
The device object property "Services Supported" indicates whether there is support for COV. Beyond that, you can look for the presence of certain properties such as 'COV Increment' to tell if an object supports COV. You can also refer to the vendor documentation or PICS documentation.

How COV Works

The system is a little more complex than these notes describe. For example, subscriptions have durations and there is more than one way the notification can be sent.

Subscribe

A data client sends messages to the device to subscribe to COV notifications. The server must accept the subscription and send a subscription acknowledgement and value or an error to represent a success or failure respectively.



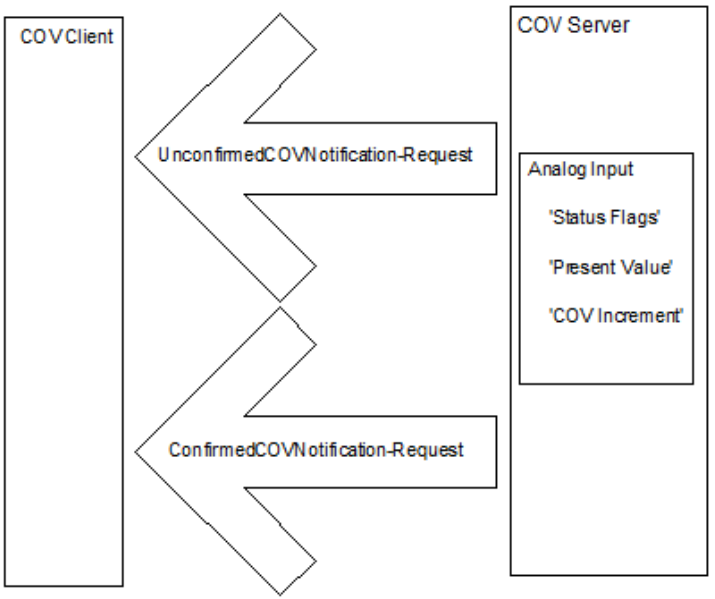
Monitor

COV Server device monitors the property values of subscribed objects and the COV change criteria.

How COV Works cont'd

Notify

When a change has occurred that meets the COV change criteria, the server sends notifications to the subscribers.



Process Notification

The data client must process the notification and update the display, log, etc.

Unsubscribe / Renew Subscription

If the data client no longer needs the subscription, it unsubscribes. If it needs the subscription maintained, then the client should periodically re-subscribe.

Key Elements of the COV Technology

COV Server :
A BACnet device that supports COV, accepts subscriptions, and sends COV notifications messages to a COV Client.

COV Client :
A BACnet device, typically a SCADA or logging application, which can subscribe for COV notification and process the notification messages.

Subscription :
Establishes a relationship between a COV Server and a COV Client.
Subscriptions have the following attributes:

Subscription to an Object or to a Property
BACnet provides two services for subscription. One subscribes to an object and the other subscribes to a property of an object.

Identification of the Subscriber
The server needs to know where to send the notifications.

Object Identifier
E.g. Analog Input 1
If the server subscribes to a property, then the property must be identified too.

Lifetime
Is indefinite or a specific number of seconds. Values can be large.

Notification Type
Notification can be sent with/without requiring confirmation from the data client.

COV Increment
This parameter is only used in subscriptions to object properties. If not specified in the subscription, the object uses its own increment.

Notification :
A message which reports the current value of the changed property as well as the current state of the object's Status Flag property if it exists. The notification also contains the number of seconds remaining to the subscription. Confirmed notifications require a response from the COV client. A client can configure the confirmation of the notifications.

COV Change Criteria

Useful Tip

The device needs to send a notification about a change to you. How does it decide when to do this ? You have some control - specify the COV Increment when you subscribe. You should also consider the object and property type because there are different rules for when they send notifications.

The change criteria are based on the type of subscription.

Subscribe to the object:

Either of these changes trigger notification.

1) If the status flags change at all
2) If the Present Value changes
    - Binary, Life Safety and Multistate Objects : any change to Present Value
    - - Analog, Loop and Pulse Objects: change by COV_Increment

Subscribe to a property :

Either of these changes trigger notification.

1) If the status flags change at all (if the object has status flags)
2) If the Property Value changes
    - Property is of type REAL: change by COV_Increment (which may be defined in the subscription or may be the native increment defined in the device).
    - Property is of some other type: any change to Present Value

COV Issues and Limitations

General Discussion

There are some intrinsic problems with event or change reporting systems.

In our experience, it is fairly common to learn that a well-configured system failed to deliver critical information only after a significant failure. We learned the hard way that we polled for data too slowly, the logger was offline when the notification was sent or that the logger was swamped with data because of the overload of incoming feed. With this in mind, we draw your attention to some of the issues you should consider.

The Deluge of Changes Problem

These event reporting systems are commonly implemented to reduce the bandwidth requirements for monitoring remote devices or to ensure that the data client sees changes whose durations are less than their minimum polling interval. When a client reduces the frequency of its polls for data or reduces which objects it polls, this reduces the bandwidth requirements of the system. To compensate for the lower frequency of updates, a COV service may be employed.

If COV services are employed to 'guarantee the delivery of critical data', great care should be taken in assessing the so-called 'guarantee'. The guarantee is often based on the assumption that changes are infrequent and small in scope, but this isn't always the case. Often a single change can spawn a number of changes and those changes can spawn more changes in a system similar to a nuclear reaction. The more changes that occur, the more notifications that must be sent. If all the changes occur in a short interval, then it easy to foresee a situation where a network or data client can be deluged with notifications. Now we have to assume there is enough bandwidth to handle sending them all and that each client can handle all the incoming messages quickly. If the notifications require confirmation, then the speed of the client in processing the messages is material. If there is no notification required, then it is conceivable in a poor BACnet implementation that the client could drop messages when its buffer is full.

It is very difficult to test these conditions because the test requires monitoring large data sets and the test setup requires a knowledge of how changes can spawn other changes within a device and / or a system. A consequence of these difficulties is that the performance of COV services can be unpredictable.

COV Issues and Limitations cont'd

The Offline Subscriber Problem

A subscriber may be offline when a notification is sent. If the subscription requires a confirmed notification, then this could present a temporary but significant loss of bandwidth while the COV server waits the timeout period before sending the next notification. If no confirmation was required, then there is no way of knowing that the subscriber was offline and even if it wanted to, the COV server device cannot signal this in any way.

The COV system does not require vendors to manage notifications sent to offline subscribers. Thus, the COV server does not have to queue them and resend them. Therefore, it is possible for a COV client to lose its data synchronization with the Server. The only way around this is to use occasional polling. However, if the data client was a logging system, then the damage is already done and the log records will not be made.

COV Issues and Limitations cont'd

Subscriptions May be Lost on Reset

The BACnet spec does not require vendors to maintain the subscriptions if the device resets. Thus, a reset may result in the loss of all subscriptions. Now, the system is dependent on the frequency of the re-subscription by the data client. That frequency is a client choice too and some systems don't send periodic re-subscriptions.

Single/Multiple Subscriptions

A single data client can potentially subscribe more than once to the same data object. This is possible because in identifying itself in the subscription, the client provides two elements of information - identifier and handle. The identifier tells the server where to send responses. The handle is a number allocated by the client for some internal purpose. Changing the handle is enough to make a subscription unique and hence it is possible to have multiple subscriptions to the same object from the same client.

Subscribing to Arrays

The spec only allows subscriptions to particular elements of an array. To subscribe to the whole array, you would need to subscribe to each and every element in the array.

Variable Number of Subscriptions

Each vendor chooses how many subscriptions to an object / property are supported. The spec requires that at least one must be supported. You should assume the list is finite and fairly short.

It's conceivable that subscription space could be wasted by temporary subscriptions from test equipment of software, thus denying room for important subscriptions.

It is important to understand how your COV client application handles and reports failed subscriptions as these events can be as important as the event they are attempting to monitor.

COV Issues and Limitations cont'd

Unconfirmed Notifications can be Sent Without Subscription

The spec allows a device to send unconfirmed notifications for any property of any object to any other device on the network. Thus, a device can broadcast changes of a object property that has a wide area of interest (such as an outside air temperature) to every device the network. The vendor chooses if they wish to implement this, and can choose which objects and/or properties to send and the frequency of the notification.

Notifications can be Sent Without a Change of Value

The criteria for triggering notification messages requires notifications to be sent if the Status Flags associated with the object change even if the value hasn't changed. This is potentially, important information but a number of data client systems ignore this element of the notification data.

Warning!

There are some risks to using COV. Read the notes on these pages to learn about them. We strongly recommend that you test the system to avoid being burned by assumptions.

If data is critical, then poll for it as well as using COV.

MS/TP— An Introduction

This flavor of BACnet is most commonly used to connect field devices to controllers / routers / control applications.

MS/TP

M = Master
S = Slave
TP = Token Passing

The physical layer uses RS485 which allows up to 128 devices to be installed on a single network with a max physical length of 4000ft (~1219.2m) and speeds up to 115k baud. Using repeaters allows the length to be increased. Compare it to Ethernet, where the spec allows a max of 100 meters (330ft) on a single, unrepeated segment.

Common baud rates are 9600, 38400 and 76800. All devices must operate at the same baud rate. More and more devices can auto sense the baud rate and configure themselves correctly.

Warning !

A number of microprocessor UARTS cannot accurately produce 76800 baud signals. Devices using these microprocessors might list 76800 as supported. If you are having issues, you might want to downgrade your network's baud rate.

We divide the messages on a MS/TP network into two categories

- Overhead (token, poll for master…)
- Application. These carry payloads that we have an interest in.

Only a device with the token can initiate an application layer message. It can send the message to any device on the network. Some messages demand an instantaneous reply, some don't. The receiving device doesn't need the token to respond. There is a limit to how many application layer messages a device can send before it must pass the token on. (The limit is implied by the max number of frames that can be sent before the token is passed.)

MS/TP— An Introduction cont'd

The benefits of token passing networks are the following:

1. They are self healing. (Self-healing refers to being able to reconnect into the network of devices automatically, see MS/TP Discovery section for more details)
2. They can discover new devices.
3. They ensure each device gets its chance.
4. They avoid collisions, making network performance (somewhat) deterministic.

A disadvantage of the token system is that any one device gets a limited use of the bandwidth. Thus, a device may need to keep an internal queue of application layer messages it wants to send while waiting to use the token. We have encountered some vendor systems which fill their queue and drop subsequent messages without notifying the user of the problem. Limited access combined with the overhead makes it easy to use up all the bandwidth on the network if there are many devices with many objects and many properties of interest.

BACnet MS/TP Installation and RS485

Here is our simplified advice :

RS485 is a 3 conductor network.
The three conductors are the Tx, Rx, and the Ground Terminal. The Tx and Rx are responsible for transmitting and receiving data respectively. The Ground acts as a common reference signal. You take a huge risk by not installing the 3rd conductor. You risk blowing RS485 ports, you risk unstable operation (works sometimes and doesn't work other times) and as a result, you risk re-installation. The more power sources used to power devices, the greater the physical separation of devices, and the less well-grounded devices and power sources are, the greater the risk.

What's the use of the 3rd conductor?

The RS485 transmits data through using the potential difference between two wires. When devices have the same ground, they are more or less guaranteed to transmit, receive, understand and interpret the same certain range of voltages. When devices do not have a common ground (i.e. devices are not in the same building, not powered by the same source, …), they may struggle to understand and interpret received signals. By having that third conductor, we can use it as a common reference for the two devices so that communication can occur dependably.

Remember this statement: The so-called Ground Terminal on an RS485 interface is not a connection to ground. It is a common reference signal. The voltage level on the Tx/Rx conductors are measured relative to this voltage level.

You can (if you must) use a shield drain wire as the 3rd conductor (ground reference conductor)

Controversial

Some people argue that the 3rd conductor is not necessary. We argue it is. Read more about this debate here:
https://store.chipkin.com/articles/rs485-rs485-cables-why-you-need-3-wires-for-2-two-wire-rs485

BACnet MS/TP Installation and RS485 cont'd

Ground Reference
Always connect the ground reference conductor first if you are connecting a device that is powered up or if you are connecting your laptop to an operating network.

OR

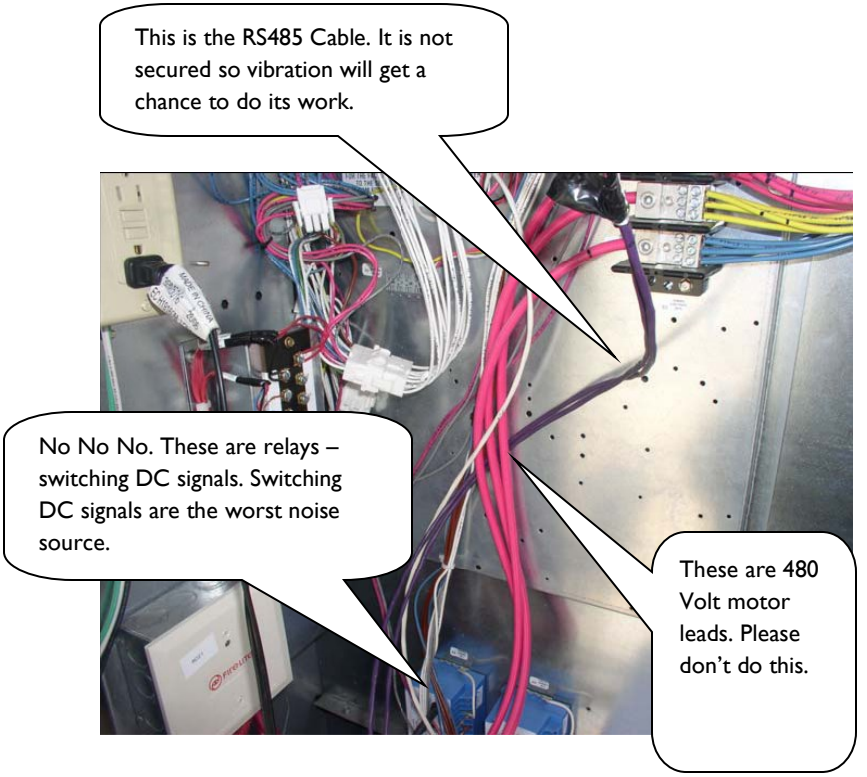
Always choose devices that have optical isolation - this will almost always protect the RS485 transmitter / receivers.

Cable Shield
You can get away without the shield. The twisted pair used for Tx and Rx is more effective at noise cancellation than the shield.

MS/TP— Where to Run Your Cables

Cable Runs

Take care of where you run your cables. It seems obvious not to wind your cable around other cables or sources of electricity / magnetism. People are often surprised to find that the worst source of induced noise are switching DC loads. Another big culprit are Variable Frequency Drives (VFD).



BACnet MS/TP Cable Selection

Cable selection does make a difference.

All cables have impedance (resistance). Some cables are designed so that the impedance is relatively independent of distance. You want one of these cables. A clue to knowing if you selected one is to look at the cable's Nominal Impedance. If they quote a number such a 100 Ohms, you have a good cable. If they quote an impedance per meter/foot, you have chosen the wrong kind. Wrong in the sense that determining the value of terminating resistors now requires measurements and calculations. Choose low capacitance cables.

Can you use Cat5 cable? Yes. Use one pair for Tx, Rx and a conductor from another pair for the ground reference signal.

We recommend these two cables.

Belden 3106A

Multi-Conductor - EIA Industrial RS-485 PLTC/CM
22 AWG stranded (7x30) tinned copper conductors, Datalene® insulation, twisted pairs, overall Beldfoil® shield (100% coverage) plus a tinned copper braid (90% coverage), drain wire, UV resistant PVC jacket.

Belden 3107A

Multi-Conductor - EIA Industrial RS-485 PLTC/CM
22 AWG stranded (7x30) tinned copper conductors, Datalene® insulation, twisted pairs, overall Beldfoil® shield (100% coverage) plus a tinned copper braid (90% coverage), drain wire, UV resistant PVC jacket.

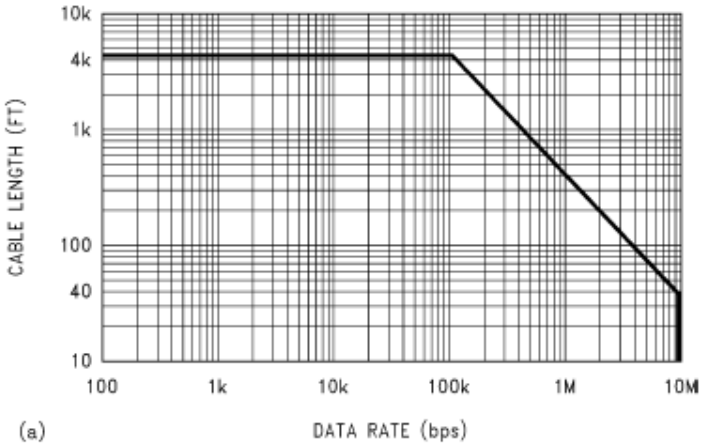
BACnet MS/TP Cable Lengths

Cable Lengths and Baud Rates

Practically speaking, you can go up to 4000 feet at baud rates up to 76800 baud. Above that, you need to do a little math and reduce the length. For example, at 115k baud, your cable should not be much longer than 2500 feet.

However, the higher the baud rate, the more sensitive the cable is to the quality of installation - issues like how much a twisted pair is unwound at each termination starts to become very, very important.

Our advise: For longer networks with lots of devices, choose 38k400 baud over 76k800 baud and optimize using COV. Separate networks and set the Max Master to a lower number.

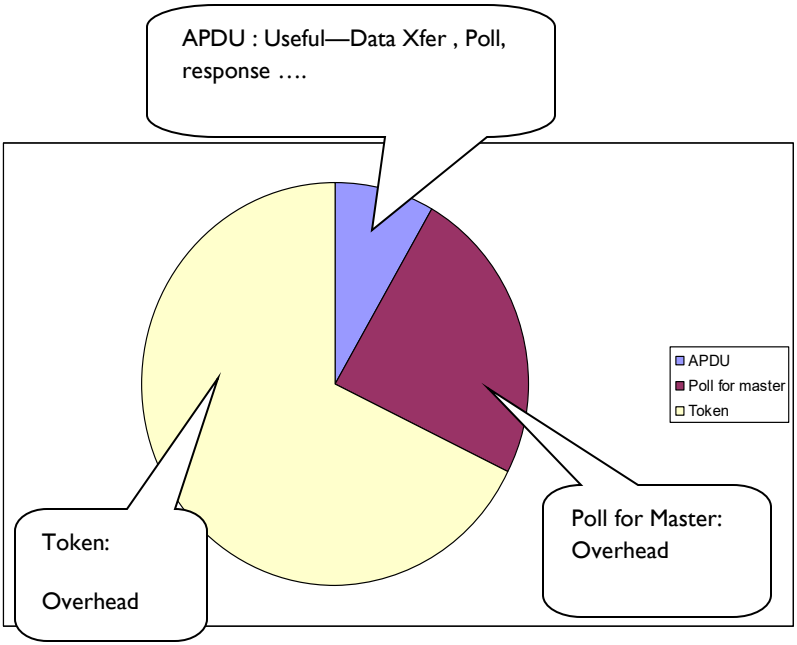


Source: ***Ten Ways to Bulletproof RS-485 Interfaces*** *National Semiconductor Application Note 1057 John Goldie October 1996*

BACnet MS/TP Bandwidth Issues

There are non-electrical considerations to determine how many devices you put on an MS/TP network.

The chart below illustrates (from one installation) how little of the bandwidth is used to transfer data. The APDU's are application layer messages that poll and respond with property values - they do work for us as data consumers. The rest is used to maintain the network - passing the token around and looking for new devices.



It's not possible to provide a calculator to work out how many devices to install on a single network but the following list provides some help in assessing bandwidth considerations.

BACnet MS/TP Bandwidth Issues cont'd

How many of the devices will be BACnet slaves.

Token passing and looking for new devices on the MS/TP trunk consumes a fair amount of bandwidth.

A BACnet slave can be read/written, but never gets the token. So it can't initiate any messages because it never gets the token. The more slaves, the fewer token passes. Typically, you are not able to put a device in slave mode. Most vendors implement their devices as masters (i.e. token passing devices).

How many Objects in each device are you interested in monitoring?

The more you read and the greater the frequency, the more bandwidth that will be consumed.

It takes approx. 30 bytes to poll for a single property. It takes about 40 bytes to reply. A token is 8 bytes as is a poll for master. Assume that 50% of your bandwidth will be used by overhead (token, poll for master). Divide the baud rate by 10 to get bytes per seconds. Using a number like 30+40=70 as a best case and 100 as a worst case (obviously reading descriptions will take more), multiply that by the number of objects and properties you are going to poll on a regular basis.

Baud	38400
Bytes Per Sec	3840
Overhead	50%
Bytes per Sec for Payload	1920
Typical poll and response for a single property	70
Number of properties that can be polled per sec	27.43
Typical number of properties that must be polled per object	4
Number of objects per sec	6.86

BACnet MS/TP Bandwidth Issues cont'd

How many properties from each of these objects?

What is the baud rate?

What is Max Master set to?

> Every few cycles, each token passing device (master) on the network must look to see if there are new devices. Max Master determines the biggest address that must be searched for. Each search involves sending a message and waiting for a response or a timeout (if the devices aren't there). Timeouts cost time. The higher the number of Max Master (default is 127), the more potential devices must be searched for. If you use Max Master to improve bandwidth, then you must adjust it in each device.

Warning !

Every device can have Max Master set to a different value.

Max Master is your friend when saving some bandwidth, but your enemy when it limits the discovery of new devices. No device with a MAC address greater than Max Master will be discovered.

Do the devices support the "Read/Write Property Multiple" services or must each property be read in a separate message?

> Find the answer to this question by reading the BIBB statement for each device. You could also explore the device object of the device, find the property called BACnetServicesSupported and then look at the 14th item in the array to see if Read Property Multiple is supported and the 16th for Write Property Multiple. However, we have found that a large number of devices don't display this information.
>
> Obviously, if you can read a chunk of properties in one message, you will be better off than if you can only read a single one.

BACnet MS/TP Bandwidth Issues cont'd

Can you use BACnet's COV mechanism?

> COV stands for Change of Value. When a device supports COV, another device / application can subscribe to receive notifications when an object property changes. This means the data client doesn't have to poll for data continuously, but can wait passively to be notified of the change. This reduces the number of messages on a network dramatically.

Some devices are slower than others.

> BACnet allows up to 15 milliseconds (ms) for a device to use the token. Since most messages on a MS/TP network are token passes, a device that uses the token in 5 ms will consume much less bandwidth than one that takes 15 ms. (A number of vendors relax this requirement to allow for other vendors implementations. The more relaxed, the more bandwidth that is consumed for doing nothing.)

How do you put more than 32 devices on a single RS485 trunk?

The simple answer is use a repeater, but in practice, one isn't always necessary.

Useful Tip

Use a RS485 repeater to put more than 32 devices on a trunk. The repeater doesn't need to know its repeating BACnet messages.

Each device has its own potential difference and capacitance. When you attach a new device onto a network, these properties mentioned above will have a cost on the network (signal clarity). Thus, we must limit the number of devices on the MS/TP trunk. The RS485 standard is based on 32 devices. Since the standard was developed, most RS485 chips present less than the full unit load originally specified. Today, you can get half and quarter load devices, which have half or a quarter of the potential difference and capacitance of normal devices. Thus, to see how many devices you can install, you simply get the data sheets and add the loads. Look for "UL" on the data sheet. It stands for Unit Load.

What Can Go Wrong with RS485

What can go wrong with RS485

Let's say you adopted all the best practices for installation of the network but you get intermittent or unacceptable performance because of packet loss, noise, collisions, etc. Then you should consider hiring an expert to resolve your problems because now you are in the 'Art' part of RS485. These are some of the things they will look at.

Reflections.

Without a scope and expertise, you won't know this is a factor. It's easy and cheap to eliminate. Look at the cable spec. Find the nominal impedance. Buy two resistors of the same value. At each end of the trunk, install the resistors between the Tx and Rx terminals. If you don't have obvious ends of the trunk (because you created a star) then we recommend re-cabling to form a linear trunk or we wish you luck.

Some devices have terminating resistors built into them. If the vendor did a poor job, the default is to have the resistor active and they must be disabled unless they are the terminating devices on the network. Read vendor docs.

Biasing , Idle State Biasing, Fail Safe Biasing, Anti Aliasing

There are a whole string of terms used as synonyms to describe this phenomenon.

To use two wires (as opposed to full duplex 4 wire) for RS485, each devices transmitter and receiver must be set to an idle state to release the line for others use. Releasing the line means allowing it to 'float'. It must not be allowed to float at just any voltage level, so devices have pull up/down resistors to pull the line to an allowable 'floating' voltage. (the floating state is also known as the tri-state.) The load presented by other devices on the network affects the floating so the resistor values may need to be changed depending on the number of devices installed and the values of the pull up/down resistors they are using. (You can imagine how tricky its going to be to resolve this).

What Can Go Wrong with RS485 cont'd

If a device floats out of the specified range, then to other devices, it will look like the floating devices isn't floating at all. The other devices will think that it is transmitting or receiving and thus blocking the line.

The simplest way of knowing if this is a factor - Does the device work properly when it is the only device on the network? When you install it in the full network, other devices or this device stops working properly. This device and/or the pull up/down resistors of other devices are candidates for investigation.

A number of vendors have a range of pull up/down resistors installed and allow you to change the selection using software or jumpers.

Line Drive On / Off

To use two wires for RS485, each device's transmitter and receiver must be set to an idle state to release the line for others' use. When a device wants to send a message, it must grab the line. When it has finished sending, it must release the line. You can see that there are potential problems here. What happens if one device waits too long after sending its last bit before releasing the line - its possible that the other devices will miss some bits of data.

Useful Tip

Other than the addition of terminating resistors to cancel reflections, you probably need an expert to help resolve these difficulties. That is why its best to adopt good installation practices.

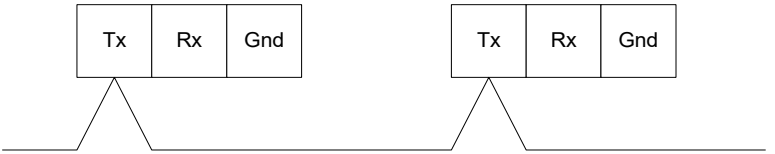
MS/TP Trunk Topology

Take care of your Trunk Topology

Take care with the topology. The best topology is a single trunk that in-outs on the terminal blocks of each device it connects to. What do we mean by best? We mean the choice which is least likely to cause problems.

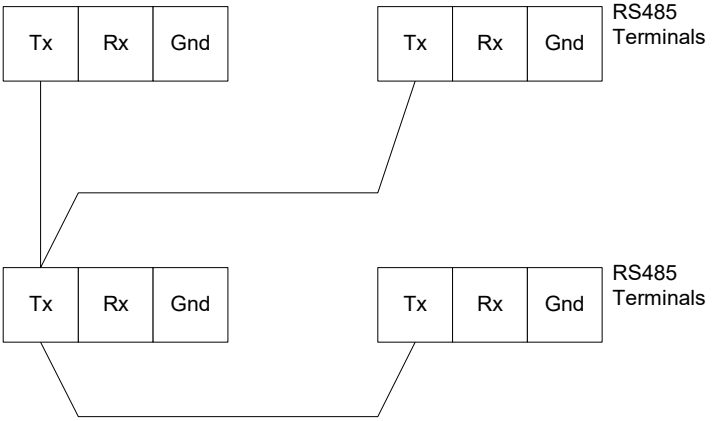
Best Topology

Simple Multidrop, unwind the twists as little as possible. (Showing TX conductor for reference only)



Worse

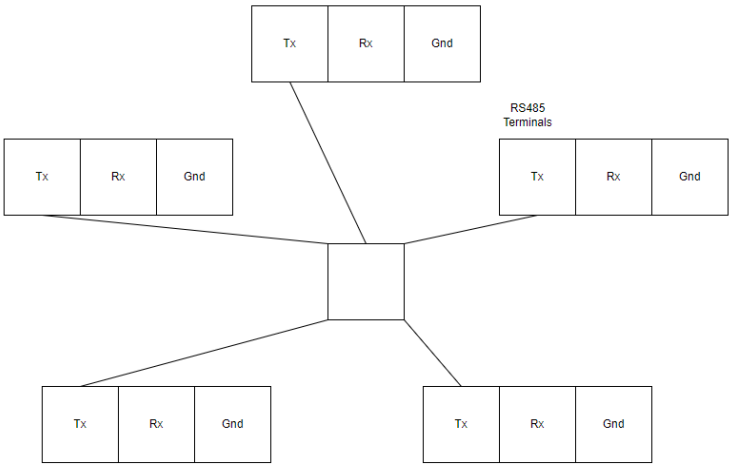
Making the connections to the RS485 terminal. If you do not make a simple multidrop system, then the electrical signals can take all kinds of complicated paths, causing reflections and harmonics. (Showing TX conductor for reference only)



MS/TP Trunk Topology cont'd

Worst

Avoid star configurations. They are so much harder to debug when it gets tricky. (Showing TX conductor for reference only)



MS/TP Discovery

BACnet MS/TP is a token passing protocol. Only nodes with the token are allowed to initiate service requests such as requests for data. A device that receives a request that requires a response may respond without having the token.

Based on this behavior, it is easy to understand the difference between a MS/TP master and slave. A slave is a device that can only send responses. A master is an initiator of a service request.

Only allowing masters to initiate a message exchange when they have the token provides a mechanism whereby there can be multiple masters on a network and contention or collision can be avoided. Ethernet uses a different system - it allows collisions but provides a recovery mechanism. Imposing rules on the token passing such as specifying how much a master can do while it has the token provides a mechanism to balance the performance of various devices on a single network.

Back to the question of how new devices are added to the network. If you add a new slave device, then you will need to program at least one master on the network to exchange data with that slave.

If you add a master, it needs to receive the token before it can act like a master. Thus, the other devices on the network must discover the new device first. Every master on the network has the job of periodically polling for new masters.

Each master knows who the next master on a network is because that is who it will pass the token to. So, each master must poll for new masters that could exist in the address range between its own address and the next master's address. Thus a master addressed as 1 must look for masters in the range 2 to 10 if the next known master is 11. Master number 11 must look for new masters starting at 12 etc. The master with the highest number must try to search starting from one above its number all the way to 127, before looping back to 0 to continue searching. When a device receives a poll asking if it is a master (Called a 'Poll for Master' message), it replies immediately. In the above example, if master number 1 can't find a master number 2, it should try number 3.

When should it try? That's is left up to the implementer of the BACnet protocol on that device. The spec only demands a minimum of 1 Poll for Master every 50 times a master receives or uses the token. The new master must respond within 20 milliseconds.

MS/TP Discovery cont'd

You can see that if every master polls for a large number of new masters and they do this often, then lots of bandwidth is lost. For this reason, BACnet MS/TP has a parameter called Max Master. Each master has its own setting for this variable. Typically, it is set at 127. For understanding's sake, imagine that master number 50 is the highest master on the network, and its Max Master is set to 64. Then it will never discover a new master whose address is larger than its max master, i.e. it will never discover masters with address 65 to 127. This is a common reason why a new device on a network is not discovered.

What if the next master goes offline?

A master periodically polls for any masters between itself and the supposed next master. If none are found, it would pass the token to the next master. However, if the token passing is unsuccessful (for reasons that include the next master being offline), then the master will simply retry. It does so a total 3 times. If it still fails, then we move onto the next phase, where the master will poll to find the next possible master. In other words, it will start polling for masters starting from it's own number up until it reaches another master. When found, it'll set the next master to it.

How often should a master search? For more information, check: https://store.chipkin.com/articles/bacnetmstp-how-often-should-a-bacnet-mstp-device-search-for-a-new-master/

MS/TP Discovery cont'd

Passive Slaves
The BACnet Master Slave Token Passing (MS/TP) Local Area Network (LAN) works on a token passing principle. A master node has to gain access to a token to be able to use the transport medium. Only master nodes are allowed to send and receive tokens on the MS/TP network. Passive slave nodes, on the other hand, may only transmit data frames on the network in response to a request from a master node. Passing the token represents overhead in the sense that the messages used for managing the token do not carry data that is useful to automation or monitoring.

On the BACnet MS/TP network, frame types are used as a mechanism to provide passive slave nodes a means to return replies.

Tip—Mac Addresses

MAC Addr	MS/TP Device Type
0-127	Masters and Slaves. (Shared address range)
128-254	Slaves Only
255	Reserved as the broadcast address. Do not assign this address.

MS/TP Slaves vs. Masters

Slaves cannot discover new devices and receive the token.
A slave node shall neither transmit nor receive segmented messages.
Slaves can be discovered.
Slaves conserve bandwidth.
Masters burn bandwidth.

Slaves do not consume as much bandwidth as masters but are much harder to configured. Some vendors will choose to only allow devices to be masters and won't make devices support slave configurations. Depending on your project needs, you may have a preference for all masters or a mixture of masters and slaves. The charts below describe how big the burden of maintaining a master is.

Based on traffic on a simple network with a single master and a single field device, we configured the field device as a Master in test 1. In test 2 we configured the field device as a slave.

The frames and frame types that will be ignored by a passive slave node are as follows:

- Frames with a destination address not equal to this station address (TS).
- Frame with destination address equal to 255 (broadcast address) and frame type equal to BACnet_Data_Expecting_Reply, Test_Request or a proprietary type known to the node that expects a reply (such frames may not be broadcasted).
- Frame types Token, Poll_For_Master, Reply_To_Poll_For_Master, Reply_Postponed or a standard or proprietary frame type not known to this station.

The frames and frame types accepted by a passive slave node are as follows:

- Frames with destination address equal to this station address (TS) and with frame type Receive_data_no_reply, Test_Response or proprietary type known to the node that does not expect a reply.
- Frames with destination address equal to this station address (TS) and with frame type Receive_Data_Expecting_Reply, Test_Request or proprietary type known to this station that expects a reply.

  The passive slave node needs to respond, to a frame expecting a reply, within a specified time frame (Not exceed T_{reply_delay}) from when receiving the last octet of the requesting frame. If this time period has expired the slave will not respond to the frame and will return to its Idle mode.

MS/TP Slaves vs. Masters cont'd

Chart 1 : Typical ratio of payload (APDU) to overhead (Token) when using **Masters**.

APDU = 5% (Useful)
Token = 95% (Overhead)

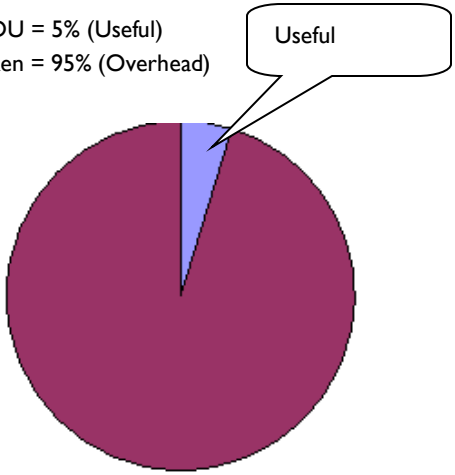
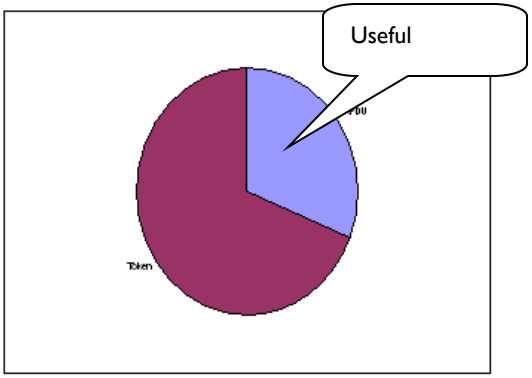


Chart 2 : Typical ratio of payload (APDU) to overhead (Token) when using a **Slave** device.

APDU = 31% (Useful)
Token = 69% (Overhead)



Changing the Present Value

All devices on a BACnet network are effectively peers. This means that any device (we take device here to mean any BACnet capable entity - device or software application) can write to the writable properties of another device's objects. This can result in conflicting commands.

BACnet has a mechanism to resolve the conflict. It differentiates between writable and commandable properties and the conflict resolution only applies to commandable properties. For writable (and non-commandable) properties, the last write wins and overwrites any previous writes - there is no conflict resolution.

Which properties are commandable and how does the command resolution work?

Useful Tip

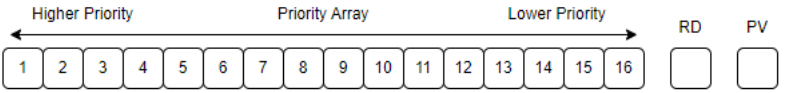
Its possible that when you change the set point, it will have no effect. The reason is that you may not have sent the new set point with a high enough priority so it's using the set point someone else sent instead.

Note that the lower the number, the higher the priority. For example, 1 has the highest priority and 16 has the lowest priority.

- The Present Value of AO, BO, MO objects are always commandable.
- The Present Value of AV, BV, MV objects are commandable if the vendor implemented them that way. It's a vendor choice. You can tell what choice they made by looking for the Priority_Array and Relinquish_Default properties on the object. That's a clue but not a guarantee (we have found). Last resort is their documentation. (good luck)
- A vendor may choose to make any vendor (proprietary) object commandable. If an object is commandable, it is required to have appropriately named Priority_Array and Relinquish_Default properties.

Relinquish Default—Worked Example

The Relinquish Default (RD) Value is set by the device. The Vendor may choose to make it a writable property, in which case it can be changed remotely. Even though the present value (PV) is commanded, the device stores the commanded value in the priority array and uses the highest priority array slot to set the Present Value.



In our example, the device boots and the Priority Array slots are all Null (Unused) and this vendor has set the Relinquish Default to 50. Since all the slots are null, the device sets the Present Value to the Relinquish Default Value. The Present Value changes to 50.

Now, a command is sent to set this object's Present Value to 45 at Priority 5. The device sets slot 5 in the Priority Array to 45. It then starts at the highest priority (1) and looks for the 1st non Null slot. It finds slot 5 filled with 45 and sets the Present Value to 45.

Relinquish Default—Worked Example

Now, a new command is sent to set this object's Present Value to 70 at Priority 8. The device sets slot 8 in the Priority Array to 70 . It then starts at the highest priority (1) and looks for the 1st non Null slot. It finds slot 5 filled with 45. Thus, there is no change to the Present Value of 45.

Now, a command is sent to relinquish the command at Priority 5. One would hope that the device that sent the original command would send the relinquish command but that is up to you and how you configured your system. When the relinquish command is received, the device sets the corresponding slot in the Priority Array to Null. The device then starts at the highest priority (1) and looks for the 1st non Null slot. The device finds slot 8 filled with 70. It changes the Present Value to 70.

The most recent command at a specific priority wins. Here, a command is sent to set the Present Value to 80 at priority 8. The device overrides slot 8 in the array with the new value. In this case, it is also the highest priority slot that is used so the device updates the Present Value to 80.

Relinquish Default—Worked Example

Finally, a command is sent to relinquish the command at priority 8. Slot 8 is set to Null. When the device looks through the priority array, it finds it all empty and thus uses the Relinquish Default value to set the Present Value to 50.

This mechanism can be complicated if the object has minimum on/off times. Additionally, slots 13-16 are most commonly used.

Heads Up

Commandable properties with a priority array gives BACnet devices a mechanism to sort values by priority. However, if multiple devices write to the same priority, you will have the same issue, where the last write wins and overwrites any previous writes.

Why does the Present Value keep changing back to some specific state?

Recall that if a property is commandable, then there exists a priority array that devices can write to. A potential reason why you may be experiencing this issue is because another device is periodically writing a present value at a higher priority than the one prior to the change. As an example, suppose the Relinquish Default is 50. You may choose to write 25 into slot 8. The present value will change to 25. Now, imagine some device that will periodically set slot 3 to 5. Because the 3rd slot has the most priority at the moment, from your perspective, the present value will suddenly become 5. No matter what value you set in slot 8, the 3rd slot will take priority and keep the present value at 5. A fix could be to write a value into a slot that takes precedence over the 3rd slot. Better yet, find the device that is periodically changing the value and disable the action. It is also possible to restrict the devices that can write to the priority array.

Troubleshooting BACnet IP / Ethernet

Required tools:

Hub or Supervised Switch
Wireshark – Free Download
http://www.wireshark.org/download.html

Warning !

You might not capture the traffic if you don't use a hub. Read the article on hub and switches to understand why. https://store.chipkin.com/articles/hubs-vs-switches-using-wireshark-to-sniff-network-packets

Useful Tip

You can select the packets you capture to reduce log file size by defining a capture filter before you start the capture. We suggest you avoid this. If you are short of space, you can select which packets you save.

Useful Tip

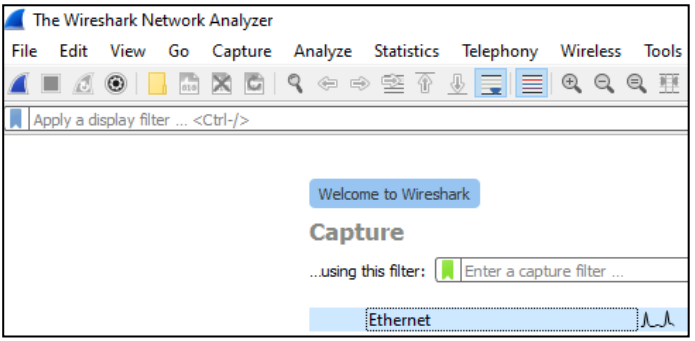
You can select which packets you view from the total log by defining a display filter. You can select which packets to save in the log files.

Useful Tip

You can search for particular packets.

How to Capture with Wireshark

Step 1: Capture – Main Menu



Step 2: Interfaces - On Capture Menu

a. You will notice a list of network adapters. Pick the one connected to the network of interest. It's probably not the wireless adapter. They will like have a graph that is drawn next to the name to indicate its activity. An example can be seen to the right of Ethernet.
b. Press the network adapter you would like to monitor.

How to Capture with Wireshark cont'd

Step 3: A list of packets accumulates on the screen

	Time	Source	Destination	Protocol	Length	Info
878	228.498234	192.168.68.109	255.255.255.255	BACnet…	54	Unconfirme
881	228.558126	192.168.68.105	255.255.255.255	BACnet…	67	Unconfirme
882	228.647894	192.168.68.109	255.255.255.255	BACnet…	67	Unconfirme
887	230.638135	192.168.68.109	255.255.255.255	BACnet…	54	Unconfirme
889	230.702242	192.168.68.105	255.255.255.255	BACnet…	67	Unconfirme
890	230.786136	192.168.68.109	255.255.255.255	BACnet…	67	Unconfirme
915	232.742455	192.168.68.109	255.255.255.255	BACnet…	54	Unconfirme
916	232.856194	192.168.68.105	255.255.255.255	BACnet…	67	Unconfirme
917	232.888983	192.168.68.109	255.255.255.255	BACnet…	67	Unconfirme
981	240.209024	192.168.68.109	255.255.255.255	BACnet…	54	Unconfirme
982	240.356739	192.168.68.109	255.255.255.255	BACnet…	67	Unconfirme
983	240.380027	192.168.68.105	255.255.255.255	BACnet…	67	Unconfirme

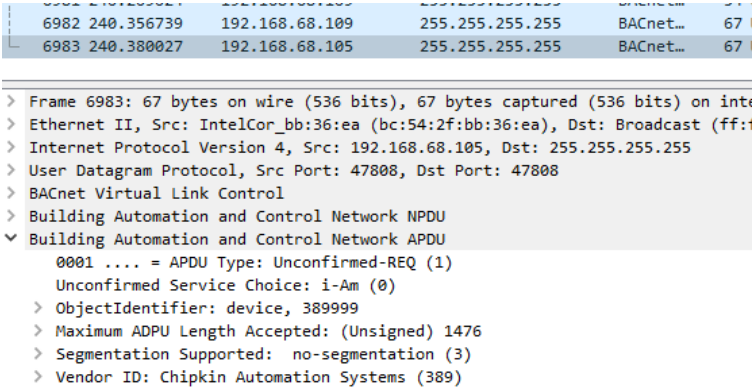
Step 4: Apply a Display Filter. More on display filters later. For now, simply type BACnet into the filter field and press enter.

bacnet

No.	Time	Source	Destination	Protocol	Length	Info
6878	228.498234	192.168.68.109	255.255.255.255	BACnet…	54	Unconfirmed-REQ who-Is
6881	228.558126	192.168.68.105	255.255.255.255	BACnet…	67	Unconfirmed-REQ i-Am device,3899
6882	228.647894	192.168.68.109	255.255.255.255	BACnet…	67	Unconfirmed-REQ i-Am device,3890
6887	230.638135	192.168.68.109	255.255.255.255	BACnet…	54	Unconfirmed-REQ who-Is
6889	230.702242	192.168.68.105	255.255.255.255	BACnet…	67	Unconfirmed-REQ i-Am device,3899
6890	230.786136	192.168.68.109	255.255.255.255	BACnet…	67	Unconfirmed-REQ i-Am device,3890
6915	232.742455	192.168.68.109	255.255.255.255	BACnet…	54	Unconfirmed-REQ who-Is
6916	232.856194	192.168.68.105	255.255.255.255	BACnet…	67	Unconfirmed-REQ i-Am device,3899
6917	232.888983	192.168.68.109	255.255.255.255	BACnet…	67	Unconfirmed-REQ i-Am device,3890
6981	240.209024	192.168.68.109	255.255.255.255	BACnet…	54	Unconfirmed-REQ who-Is
6982	240.356739	192.168.68.109	255.255.255.255	BACnet…	67	Unconfirmed-REQ i-Am device,3890
6983	240.380027	192.168.68.105	255.255.255.255	BACnet…	67	Unconfirmed-REQ i-Am device,3899

How to Capture with Wireshark cont'd

Step 5: Find the packet you are interested in. Click on it to select it. A breakout of the selected packet's data is shown below the packet list.



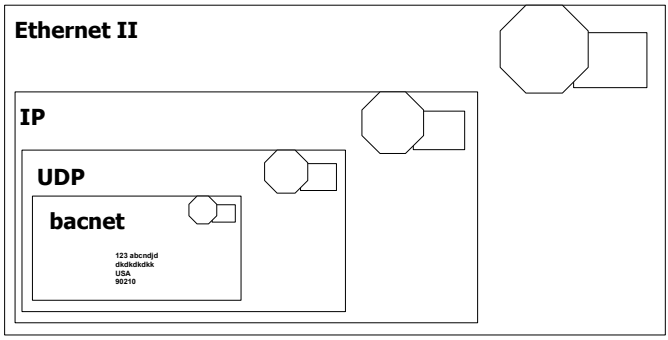
Step 6: You can break out the level of detail by expanding the sections of the packet.

Think of a BACnet packet as a letter you send to a BACnet device. When you take it to the BACnet post office, the clerk says he does not understand the address. He passes it to the UDP clerk. The UDP clerk takes your letter and puts it in a bigger envelope. He addresses the envelope with a UDP address. He passes it to the IP post office clerk. The IP clerk takes your letter and puts it in a bigger envelope. He addresses the envelope with an IP address. He passes it to the Ethernet post office clerk. (cont'd)

How to Capture with Wireshark cont'd

Step 6: cont'd

The Ethernet clerk takes your letter and puts it in a bigger envelope. He addresses the envelope with a hardware address and sends it to that computer. When it arrives, the process is reversed until finally the contents are passed to the BACnet application.

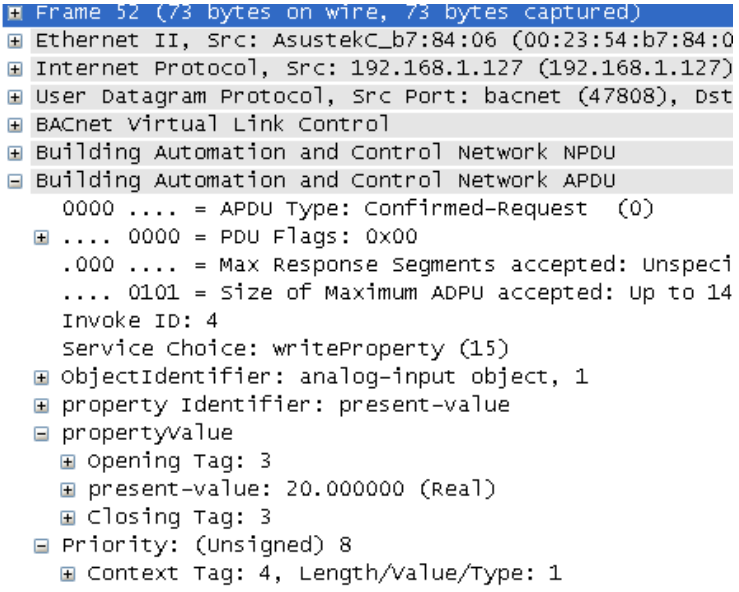


Ethernet packets contain packets from other higher level protocols nested inside each other. You can drill down to see the detail you want.

In the example below, you can see the BACnet packet nested inside a UDP (User Datagram Protocol), which is nested inside an IP protocol packet, which is in turn nested inside an Ethernet packet. Drilling down into the BACnet packet, you can see that the concept is carried even further.

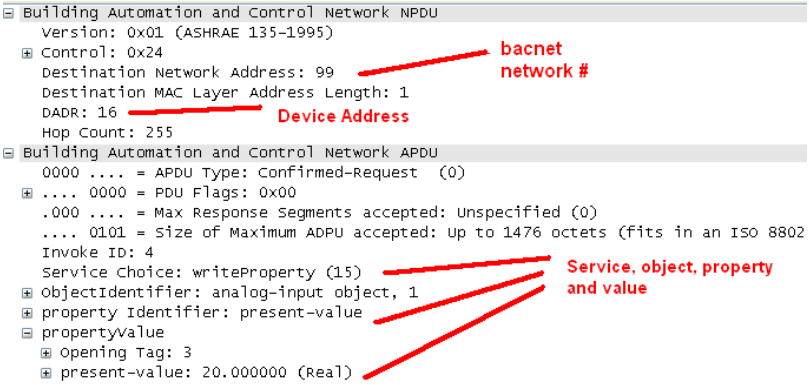
How to Capture with Wireshark cont'd

The BACnet service shown below is a write to analog input #1. It is wrapped up with some information about the device – both the device number and network number is contained inside the NPDU.



How to Capture with Wireshark cont'd

Step 7: Drill down to see the BACnet info

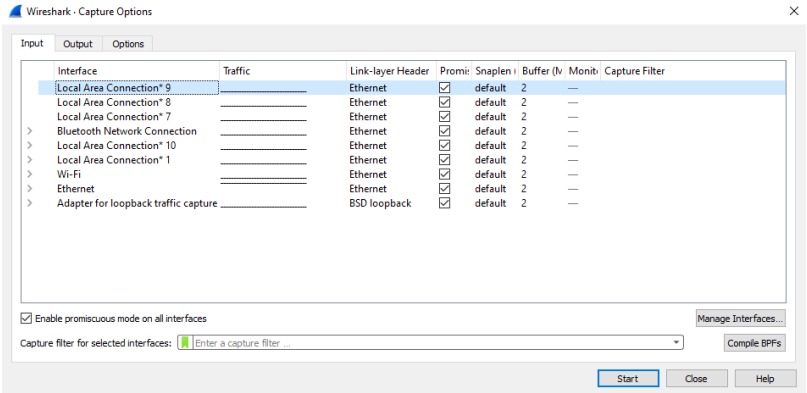


How to Filter with Wireshark

Before you start a capture, you can specify a capture filter. The effect of the filter is to prevent all packets from being captured. Doing this can save space when you save the log and it might make it easier to find the packets you are interested in. However, there is some risk that you might unintentionally filter out the packets of interest.

For example, a BACnet device might not operate correctly because it is being hammered with packets from another protocol being sent incorrectly to the BACnet device. Our advise is to capture as much as possible and then filter what is displayed.

To capture, you can go to Capture > Options and then type a filter into "Capture filter for selected interfaces". Alternatively, you can stay on the main screen and there will be a text box for you to enter a capture filter (Refer to Step 1's image, to the right of the green bookmark symbol).



How to Filter with Wireshark cont'd

Here are some sample filters:
Examples

Capture only traffic to or from IP address 172.18.5.4:

host 172.18.5.4

Capture only traffic to or from IP address 172.18.5.4 but exclude all FieldServer RUINET messages

host 192.168.1.81 and port not 1024

Capture traffic to or from a range of IP addresses (192.168.0.0 - 192.168.0.255):

net 192.168.0.0/24

or

net 192.168.0.0 mask 255.255.255.0

Capture traffic from a range of IP addresses (192.168.0.0 - 192.168.0.255):

src net 192.168.0.0/24

or

src net 192.168.0.0 mask 255.255.255.0

How to Filter with Wireshark cont'd

Capture traffic to a range of IP addresses (192.168.0.0 - 192.168.0.255):

dst net 192.168.0.0/24

or

dst net 192.168.0.0 mask 255.255.255.0

Capture only BACnet traffic: Assumes every device is compliant and is using the standard port.

port 47808

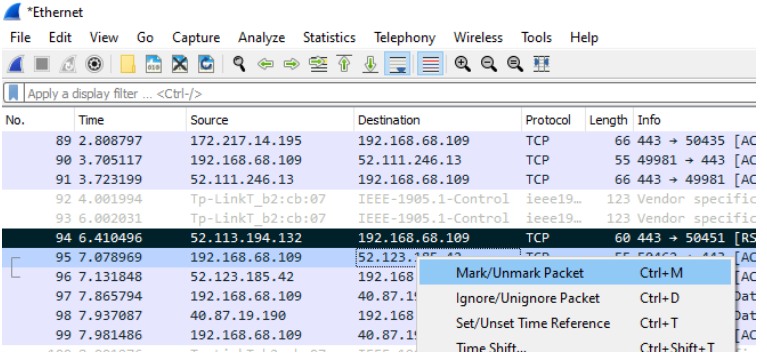
Finding Packets in Wireshark

Useful Tip

It's easy to sort packets by source or destination IP. Click the column headings.

Useful Tip

You can mark packets you find interesting. Later, you can save, display or print the marked packets. To do this, select the packet, go to Edit > Mark/Unmark Packet. Alternatively, you can also right click the packet and press "Mark/Unmark Packet".



*Dark (turquoise) highlight represents a marked packet.

Finding Packets in Wireshark cont'd

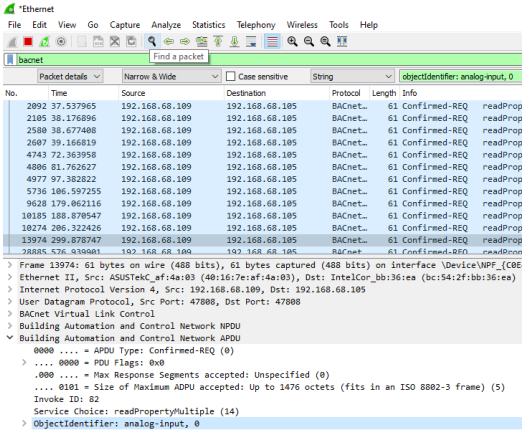
Searching :

The problem is that you can only specify one text string and hence you can only specify one search criteria. For example, in the search below, all packets that contain the string = 'analog object (1)' will be found irrespective of the device, IP address, etc.

Some Useful Search Strings

writeProperty

objectIdentifier: analog-input, 1
objectIdentifier: analog-output, 11
objectIdentifier: binary-input, 10041
objectIdentifier: binary-output, 45
(Be sure to change the dropdown from "Packet list" to "Packet details".)



Find Packets using Display Filters

Wireshark - Display Filtering

Useful Tip

Any capture filter can be used as a display filter.

Looking for failures:
Try the following search strings:

bacapp.type == 5 || bacapp.type == 6 || bacapp.type == 7

|| Means OR

&& means AND

(Type5 are errors, Type6 are Reject messages and Type 7 are abort messages.)

Looking for messages which specify particular objects types:

Try these search strings. 0=AI, 1=AO, 2=AV, 3=BI, 4=BO, 5=BV, 6=Calendar Object, 7=Command Object, 8=Device Object, 9=Event Enrollment, 10=File, 11=Group, 12=Loop, 13=MI, 14=MO,17=Schedule,19=MV, 20=Trend Log

bacapp.objectType == 0

Find Packets using Display Filters cont'd

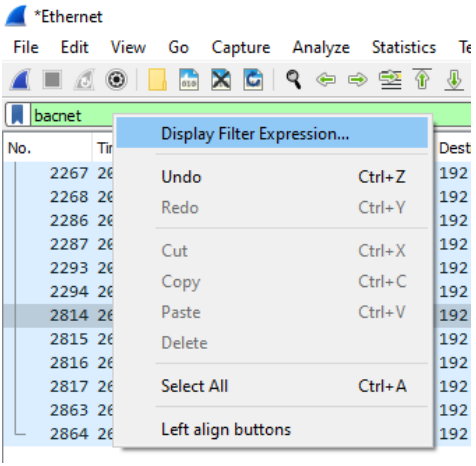
Looking for a particular object: In this example, all messages which reference AI(1) are listed:

bacapp.instance_number == 1 && bacapp.objectType == 0

Looking for messages to/from particular devices:

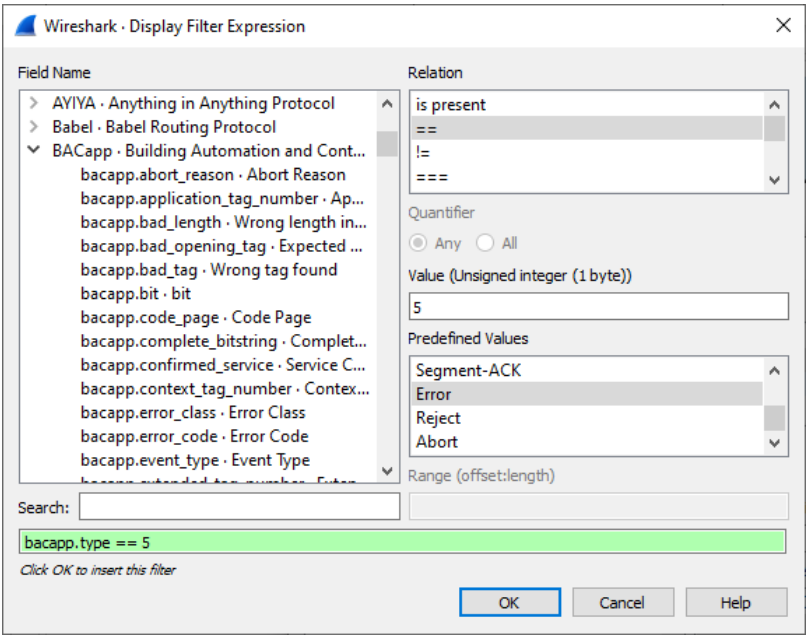
ip.addr == 192.168.1.90 (Sent to/Sent From)
ip.dst_host == "192.168.1.90"
ip.src_host == "192.168.1.90"

You can use the expression builder to build filter expressions.

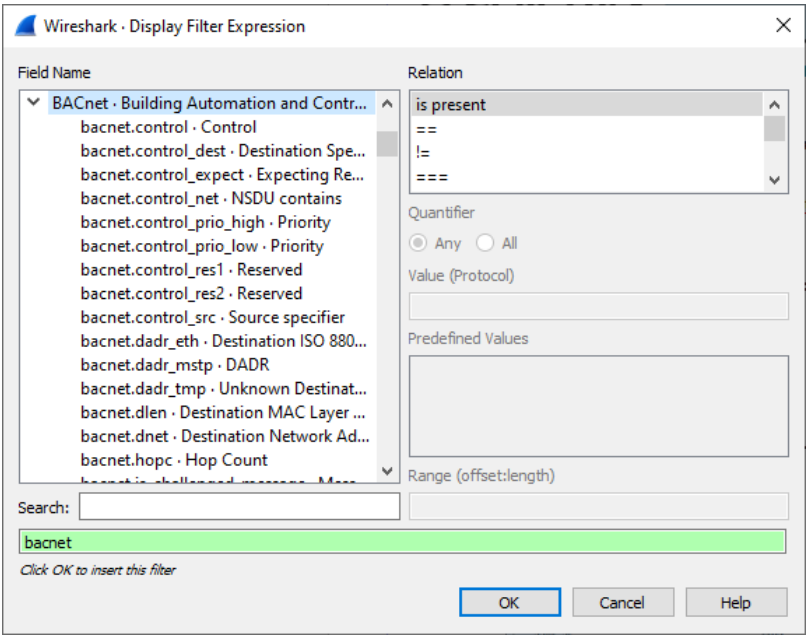


Find Packets using Display Filters cont'd

From the drop down list of protocols there are two specifically related to BACnet. They are shown below.



Find Packets using Display Filters cont'd



Troubleshooting BACnet MS/TP

Trouble Shooting BACnet MS/TP

One badly-behaved device on a MS/TP trunk can cause a collapse in performance.

To understand why, consider this one example of what can go wrong. RS485 is a shared trunk. When two devices transmit at the same time, this causes a collision. In simple terms, think of the messages interfering with each other and corrupting each other so that neither message is recognizable. To prevent this from happening while allowing for multiple masters on a network, BACnet has chosen a token-based system. Only devices with the token can initiate a message transaction. To keep things running smoothly, BACnet has some demanding timing requirements. For example, a device passes the token on. The receiving device has 15 ms to use the token. Let's say it responds in 18 ms. During that interval, the original device doesn't see the token being used so it send the token again. As it sends it, the 2nd device uses the token (3 ms late). Now, the messages from the 1st and 2nd device clash. The 2nd device thinks it has the token and starts to use it. The 1st device thinks the token got lost and starts to poll for a new master. Messages clash, causing contention and eventually both devices recover to a valid state using the protocol rules. These rules require waiting various timeout periods. All the waiting, collisions, and recovery waste time and bandwidth. If this happens often (as it will because one device doesn't meet the spec), then you can lose significant bandwidth.

Troubleshooting BACnet MS/TP cont'd

Strategy

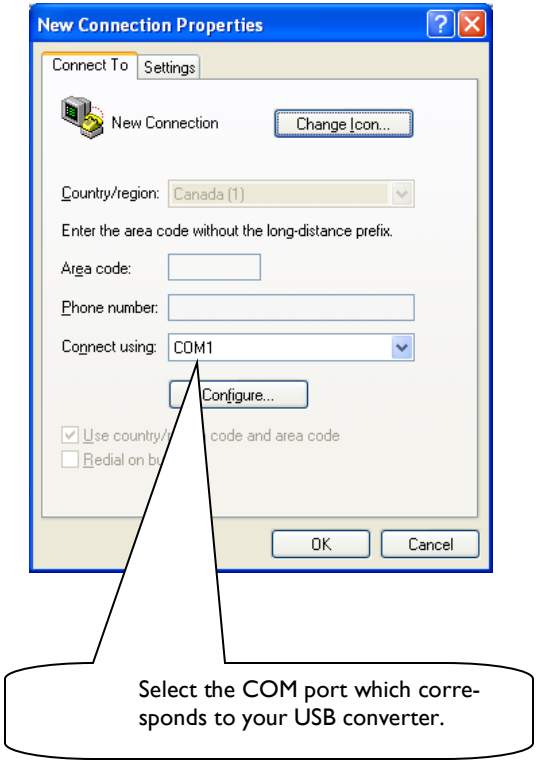
Capture Traffic using USB-485 converter
- Use a tool like BACspy
- Or
- Use Hyperterminal

Analyze Traffic
- Use a tool like BACspy online or Offline
- Or
- Perform a manual analysis

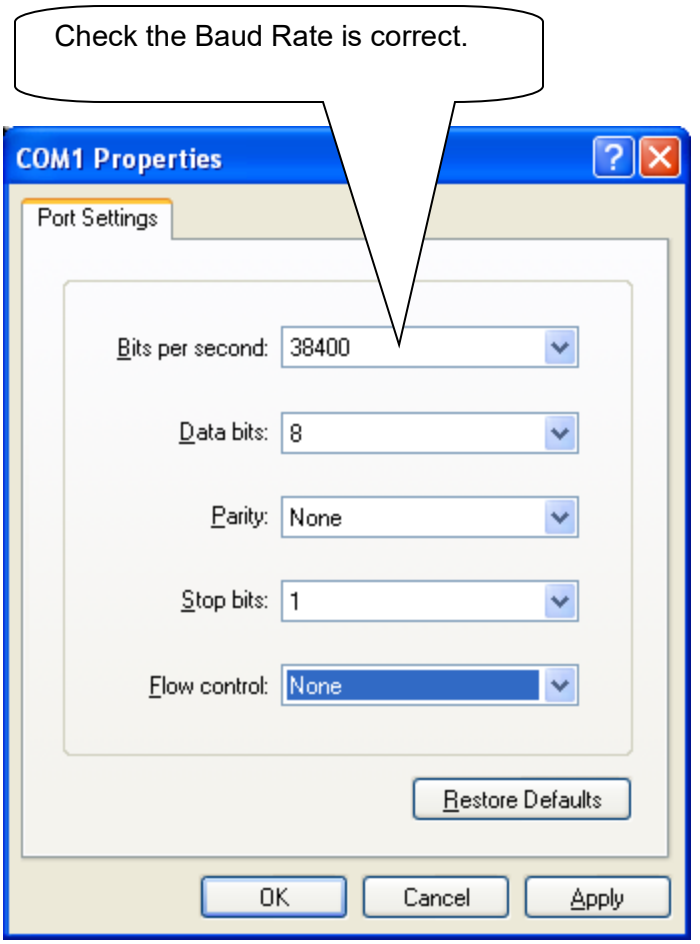
Troubleshooting BACnet MSTP cont'd

Step 1: Configure HyperTerminal

Select the COM port which corresponds to your USB converter.
Set the Baud Rate correctly.
Set the other parameters as shown.



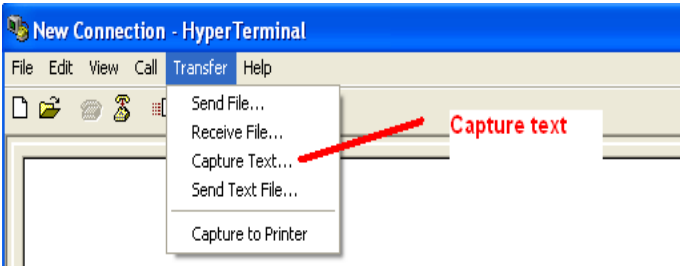
Troubleshooting BACnet MSTP cont'd



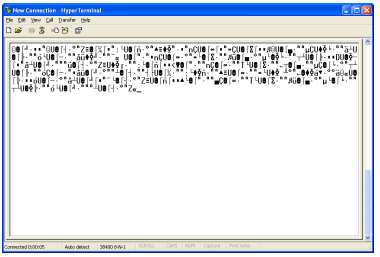
Troubleshooting BACnet MSTP cont'd

Step 2: Capture to File

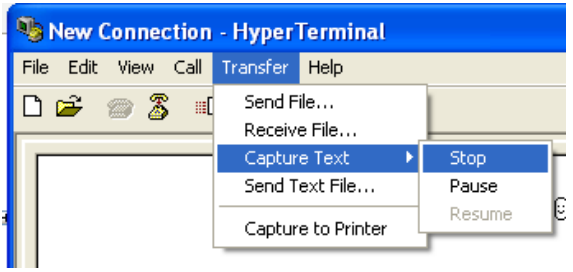
Use this menu to start and stop the capture.



As the messages are captured you will see these non-human readable characters fill the screen.



Use this menu to start and stop the capture.

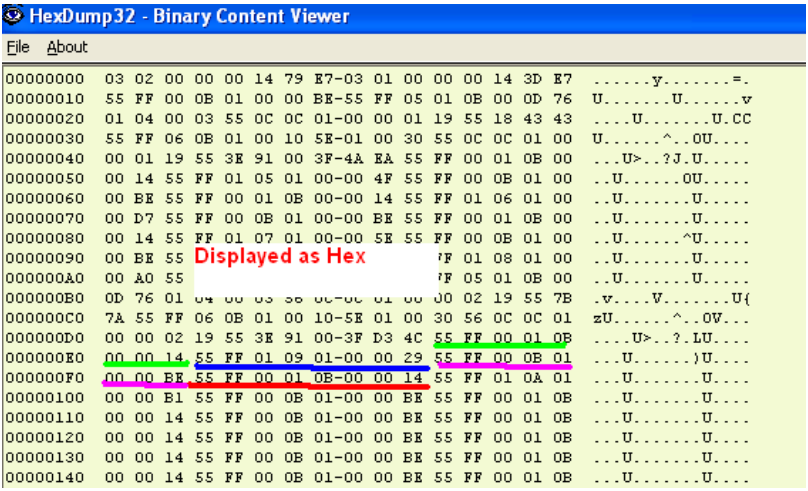


Troubleshooting BACnet MSTP cont'd

Step 3: Inspect the captured data before you leave site to see if it usable.

You need a viewer capable of displaying the hex bytes. Here is a free download and hex viewer. Open the log file.

To ensure you captured useful data look for messages that begin 55 FF. All BACnet MSTP messages begin with the same codes. If you don't see any then this may mean you captured at the wrong baud rate or some other setting is wrong. It is also possible that there is no BACnet communication.

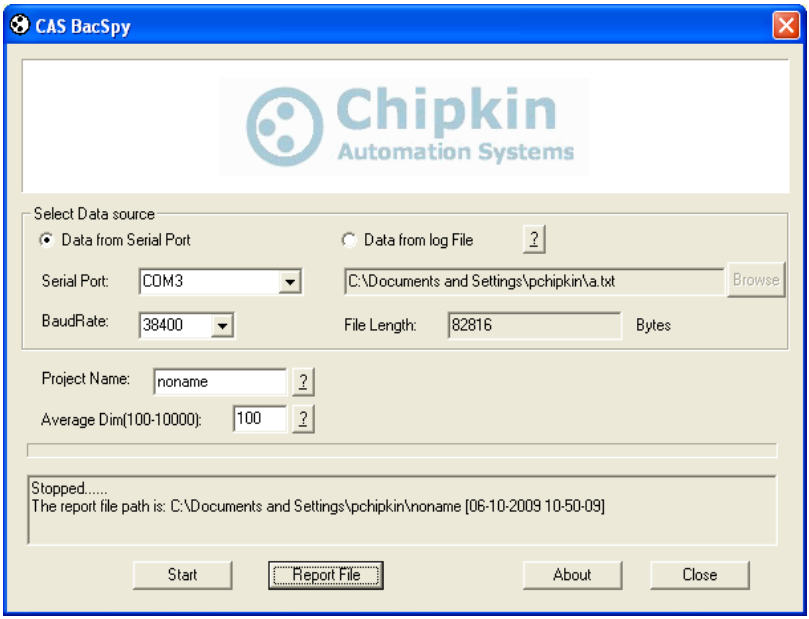


http://hexdump32.salty-brine-software.qarchive.org/_download2.html

Troubleshooting BACnet MSTP cont'd

Step 4: You can use CAS BACspy

BACspy automates this process of capture and analysis.

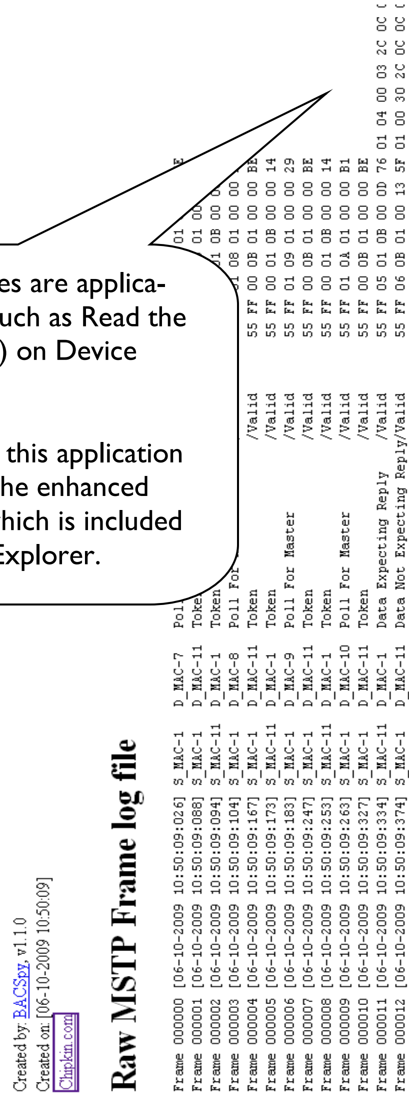


BACspy can also be used to analyze data captured using HyperTerminal

Troubleshooting BACnet MSTP cont'd

These longer messages are application layer messages such as Read the present value of AI(2) on Device 37001.

To see a breakout of this application layer data you need the enhanced version of BACspy which is included in the CAS BACnet Explorer.



Hubs vs. Switches

Hubs vs Switches - Using WireShark to sniff network packets

Simple definitions

A hub works in the physical layer to connect computers together in a network. It allows computers to send a message that is broadcasted to all devices. A switch, on the other hand, works in the data link layer to connect devices together in a network. They allow computers to restrict whom receives a message.

Gotcha #1 : Use a hub, not a switch

Why: Switches don't copy all messages to all ports. They try and optimize traffic so when they learn which port a device is connected to, they send all the messages intended for that device to that port and stop copying to all ports. (The jargon they use for this function is 'learning mode')

How do you know it's a hub: Just because it calls itself a hub doesn't mean it is one.

- If it says full-duplex in the product description, it's probably not a hub.
- A switch that allows you to turn off the learning mode is effectively a hub.
- A switch with a monitored port copies all messages to the monitored port and thus you can use that port as if it were a hub.
- If it says 'switch' and you cant turn off learning mode and it doesn't have a monitor port, then it is not a hub.
- A router is never a hub.

Hubs vs. Switches cont'd

Gotcha #2 : Mixing 10 and 100 mbits/sec can cause problems.

Not all hubs copy 10mbit messages to 100mbit ports and vice versa. Use a 10mbit/sec hub if you are on a mixed network – almost all other faster devices are speed sensing and will downgrade themselves to 10mbits/sec and thus you will see all the packets. This is not true of some building automation engines where the speed of the port is configured.

You can work around this problem by connecting higher speed devices to a self-sending switch/hub and then connecting that switch/hub to the 10mbit hub.

Recommended Hubs

10Mbit/sec Networks - DX-EHB4 - 4 Port 10 Mbps HUB

Netgear - DS104 Dual Speed HUB

10Mbit/sec Networks – D-LINK DE-805TP

Resistors

Beer and Vodka Can Help You Select a Terminating Resistor

Try this mnemonic if you are trying to remember the resistor color codes:

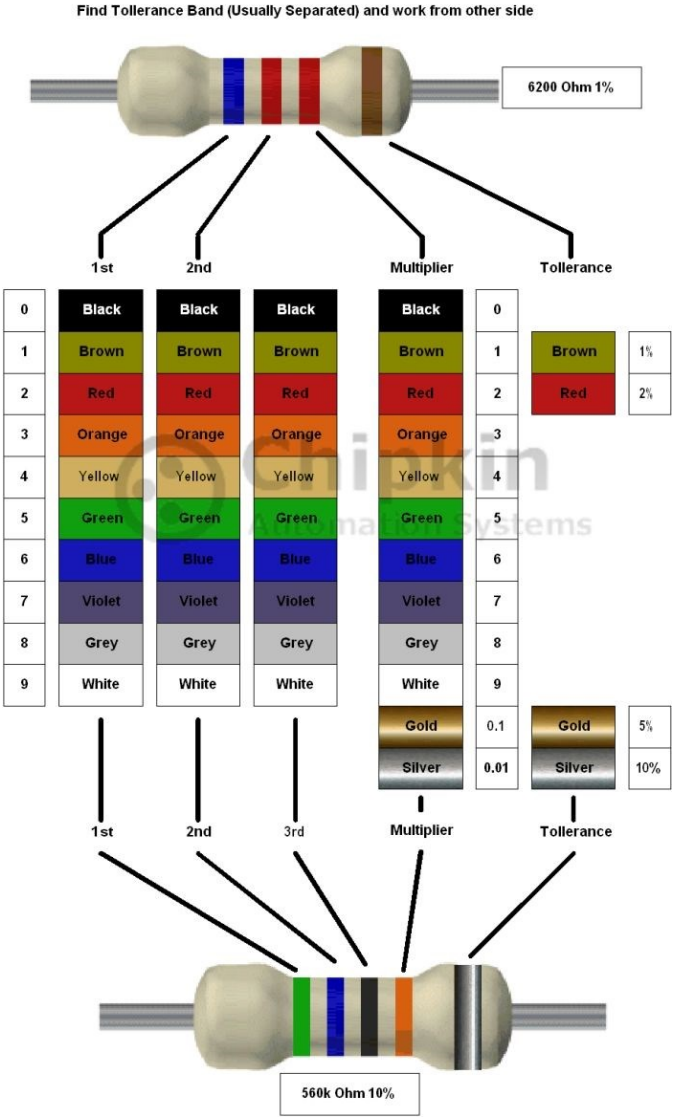
Note: If you're missing a tolerance band that implies that the tolerance is 20%.

Which end do you start reading the color bands?

There are usually two ways:

1) If one of the bands at the end of the sequence is further apart, then that is the tolerance band - start from the opposite end.
2) If all the bands are closer to one side of the resistor, then start from that end - the tolerance band is the last one you read.

Resistors cont'd



Terminating and Biasing Resistors

What should you carry with you to site? (for communication networks purposes)

For Terminations	
Value	**Tolerance**
75 Ohm	5%
100 Ohm	5%
120 Ohm	5%

For Biasing
Value
10k Ohm
4k7 Ohm
2k4 Ohm
1k Ohm
560 Ohm
30 Ohm

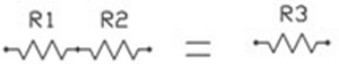
How to buy resistors

Buy a series - E12 or E24 (they come in packs and provide a comprehensive range of resistors).

Terminating and Biasing Resistors cont'd

How to make a resistance value even if you don't have the correct resistor in your toolbox.

Series

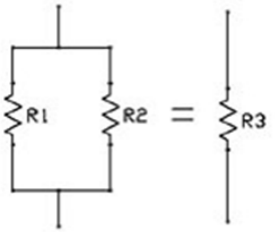


$$R_3 = R_1 + R_2$$

- R1 and R2 connected in series could be replaced with one resistor of resistance R3.
- Using 2 or more resistors instead of one allows you to achieve custom resistances.
  Less resistors are required when used in series to achieve greater resistance than when used in parallel.

Parallel

- R1 and R2 connected in parallel act as one resistor with a custom resistance of R3.
- This method allows you to get custom resistances using the formula.
- R3 will always be smaller than R1 and R2, so more resistors are required to achieve higher custom resistances.

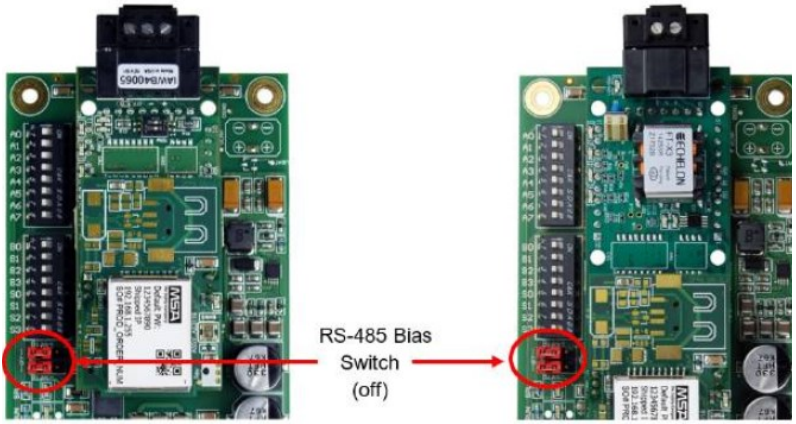


$$\frac{1}{R_3} = \frac{1}{R_1} + \frac{1}{R_2}$$

Enable Biasing on FieldServer Classic Products

The ProtoNode and FieldServer Classic bias resistors are used to keep the RS-485 bus to a known state to prevent false bits of data from being detected when there is no transmission on the line (bus is idling). The bias resistors typically pull one line high and the other low—i.e. far away from the decision point of the logic.

In the RS-485 carrier, the bias resistor is 510 ohms, which is in line with the BACnet spec. It should only be enabled at one point on the bus (on the ProtoNode/Classic field port where there are very weak bias resistors of 100k). Since there are no jumpers, many ProtoNode/Classic bias resistors can be put on the network without running into the bias resistor limit, which is < 500 ohms.

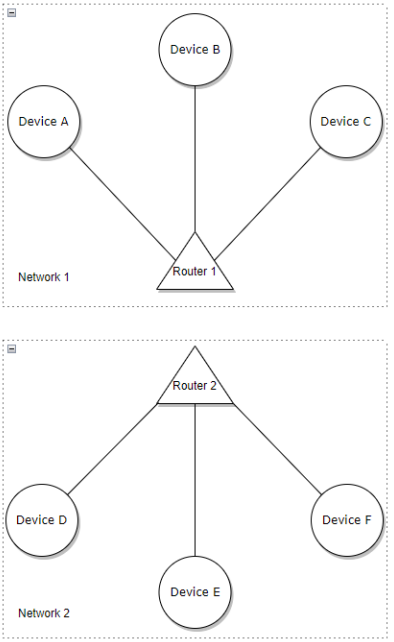


Enable Biasing on FieldServer Classic Products cont'd

Enabling biasing on FieldServer 2010-F series

Working Example: Routers and BBMD

To explain the relationship of routers, subnets and networks, we can look at a simple example.



In the diagram to the right, we have two routers: Router 1 and Router 2. Each router has their own network of 3 devices. As a whole, Router 1 and 2, along with their devices, may collectively be a part of one larger network. In that case, Router 1 and all its devices are considered a subnet (subnetwork), and Router 2 and all its devices are considered another subnet. Note that the distinction between subnet and network are not clear-cut, but relative. A network may have several subnets. That same network may be a subnet for a larger network.

Devices in the network are able to directly communicate to each other through the router. Thus, Device A can contact Device C directly. Devices that want to communicate to devices on other networks will require the routers to direct the messages through a specific delivery method. That is not important for our discussion.

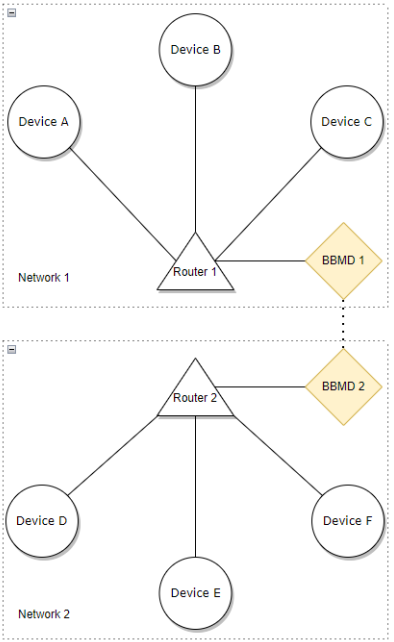
The problem we want to bring up is that broadcasts can only be sent within a network. If Device A wants to discover the devices on a network through a 'Who-Is' service, a broadcast must be sent by Router 1 to all devices in its network. The only devices that will be able to receive the broadcast will be Device A, B, and C. Naturally, those devices will send an 'I-Am' response back. Notice that Device A is not able to discover Device D, E, and F. To allow it to discover the other devices, we can use a BBMD.

Working Example: Routers and BBMD

On this page, we have revised the example to include a BBMD.

We have now added BBMD 1 and 2 to network 1 and 2 respectively. With the BBMDs configured to each other, they will allow Device A to be able to discover Device A - F. Here's how:

When Device A wants to discover the devices on a network through a 'Who-Is' service, a broadcast is sent by Router 1. As normal, Devices A - C will respond with 'I-Am'. BBMD 1 is responsible for translating the broadcast into a directed message. It gets sent by Router 1 to Router 2, where it will be translated back into a broadcast by BBMD 2. Thus, the broadcast will reach Device D - F, where they will return a 'I-Am' response. (Note that the broadcast back will be handled similarly).



Extra: Device Object Instance Numbers
The BACnet devices (Device D, E, and F) in Router 2 may have the same Device Object Instance Numbers as the devices in Router 1 (Device A, B, and C respectively) if there is no BBMD in either network. This is allowed as the devices in Router 1 will never be able to discover devices in Router 2. Even with a BBMD, as long as it isn't configured to each other, the duplicate Device Object Instance Numbers will be fine. The moment those BBMDs are configured to each other, this means that the devices can discover each other and so all their Device Object Instance Numbers must be unique to avoid conflicts.

CAS BACnet Software

BACspy

MSTP performance and troubleshooting tool. Reports used MAC addresses, who talks to who, who breaks rules, etc.

BACsql

Provides a MySQL or SQLite interface to a BACnet network.

BACwatchdog

Monitor who reads or writes to a device, object or property.

BACnet Explorer

Discover, browse, monitor, document BACnet networks.

Virtual Thermostat / Lighting Controllers

Windows temperature and lighting controllers that talk BACnet.

MSTP / IP / Eth Stack (Protocol Library)

Support for C++ and C#. Tested on Windows and Linux.

Glossary

Bandwidth

Maximum rate of data transfer over a path on a network. It refers to how much data can flow through a path per second. Bigger bandwidth means more data flow and thus faster network speeds. An analogy to think about: the amount of water that flows through a pipe per second.

Baud

Pulses per second (or the number of symbol changes per second). Used to describe the speed of data transmission.

Client

Computer hardware/software that requests some service from a server. In our case, it is usually the software applications that monitor and access BACnet devices.

Controller

The definition of controller changes when describing different protocols. In our case, a controller is synonymous for a device. Controllers can act as either a client or a server.

Data Sheet

1-2 pages of basic information about a product. Refer to a product's manual for troubleshooting rather than a data sheet.

Glossary

Data Synchronization

Refers to the consistency of data between devices. When a client loses data synchronization with a server, for example, it implies the client's data is different from the server's data.

Flavors of BACnet

Flavors of BACnet refers to the data link layer protocols used alongside BACnet to facilitate communication between devices.

Frame

Container for data packet. Contains information for data transfer on LAN.

Gateway

Hardware/software that is used to support the communication between devices using different protocols, however, it must support the conversion between the two protocols.

IP Address

Unique ID given to a device to allow communication over a network using IP. A device usually has a public IP address for the Internet and a private IP address locally.

IP Network

Group of devices connected based on a common public IP address.

Glossary

Master

Refers to a device in MS/TP protocol that sends requests. It must have a token to allow it to provide requests to slave devices.

MS/TP Trunk

A network topology where multiple devices are connected through a single conduit. Has the same structure as a simple multidrop.

Noise

Unwanted interferences with electrical signal. Refers to disturbances that will affect the transmission of data. Some examples could include electromagnetic interference, power supply noise, etc.

Optical Isolation

The transfer of electricity between two isolated circuits using light. It only allows the light to transmit electricity in one direction.

Overhead

Refers to the loss of resources (time, memory, bandwidth, etc) due to any excess computation that does not yield direct results. For example, token passing in MS/TP helps regulate the transmission of data, but does not transmit useful information between the devices.

Glossary

Pull Up/Down Resistor

Pulls the voltage to a known state so other devices can determine the state of the wire.

Re-installation

Act of re-installing wires into some infrastructure.

Repeater

Device that strengthens and retransmits signals. It is used to extend the distance signals can travel, thus allowing more devices to connect to an MS/TP trunk.

Server

Provides service to client based on a request. Usually refers to the applications in the BACnet devices that contain raw data of some form.

Slave

Refers to a device in MS/TP protocol that listens to requests from master devices. They are in charge of sending back responses to those requests.

Terminating Resistor

Resistor that is placed at the end of a cable to prevent the reflection of signals.

Glossary

Twisted Pair

2 conductors that are twisted together as a means of reducing noise.

Frequently Asked Questions (FAQ)

General

Q: What are the ports that BACnet uses?

While, it is technically possible to use any UDP port, the default is 47808 (0xBAC0 in hex). Other commonly used ports are 47809 - 47817 (0xBAC1 - 0xBAC9 in hex).

(See what they did there? All the hex have BAC in them!)

Q: Why would someone use the non default port for BACnet IP?

There may be a situation where you want to have multiple vendors on the same network and using the same infrastructure without any communication between the vendors. By using different ports per vendor, you can ensure that communication exists only between the same vendors.

Q: How does a BACnet client discover another BACnet device?

It uses the Who-Is and I-Am services to discover other devices. The client will send a Who-Is broadcast and receive I-Am broadcasts back from each of the devices. This is how a device is discovered. The Who-Is broadcast can also limit the search to a specific range of device instances. You may also use a Who-Has broadcast to search via object name.

Remember that discovery does not work across subnetworks unless BBMDs are installed.

Frequently Asked Questions (FAQ)

Q: What is a vendor property with a ID of greater than 512?

All the properties are enumerated with an ID. This means that we are able to identify the property based on that ID. While BACnet has an enriched list of properties, there may be specific properties that vendors may want that don't align with the properties provided. Thus, vendors are allowed to create those niche properties with IDs set greater than 512. This also means that all documentation relies on the vendor, not BACnet.

Q: What should I bring to site to diagnose a issue with BACnet?

MSTP: RS485 convertors, 47k resistors, 47 ohm resistors (other diagnostic page), wire clippers, wire, logic analyzer, logging software like Realterm or Rutty software tools. Read more at:
https://store.chipkin.com/articles/serial-com-connections-putty-or-realterm-hyperterminal-alternative
https://store.chipkin.com/articles/rs232-how-can-i-do-serial-port-sniffing-snooping-through-rs232

BACnet IP: Hub OR switch with a supervisory port, Wireshark.

QuickServers have an internal method of capturing and reporting Ethernet Traffic. The log file is a PCAP file which is suitable for opening with Wireshark. Inside this log, you can search for tcp.port = 47808 or simply type the word "bacnet" (lower case) into the filter to capture the BACnet/IP traffic and MS/TP traffic. From the user interface, one can select a 'Diagnostic', initiate the process, then download the diagnostic files. Among these files, you will find a ".pcap" file. To open the file, start Wireshark and open the file.

Frequently Asked Questions (FAQ)

MS/TP

Q: How many MS/TP devices should I have on a network?

We suggest having 32 devices or less on the same network. That is a good range of devices for a smooth and relatively problem-free network. When the number of devices on the network reaches 64, more problems may arise. For example, the devices may start communicating over each other, discovery of new devices will take extremely long, and misbehaving devices may disrupt the network for all devices. 64 devices is possible if all the devices are from the same manufacturer.

Q: How do I know what I should set the MS/TP address to?

You want to use a MAC Address that is not being used. There are a couple ways of figuring this out - you can either monitor the network and see what MAC addresses are not being used or check the devices' configurations to see what MAC addresses are being used. Then, you can freely choose any of the MAC addresses that you have found to be free.

Q: What happens if two devices have the same MAC address on the network?

They will try to talk over each other, sending messages at the same time. Those messages will overlap to make an indistinguishable mess of signals. This is reported as EatAnOctet to the devices and all the devices will stop communicating. This often arises when a new device is added with a MAC address that was incorrectly assumed to be free or when you configure a device on a network to a MAC address that is being used. Always add devices one at a time.

Frequently Asked Questions (FAQ)

Q: I used a MAC address above 127 and I can't discover it on the network.

All devices have a Max Master of 127 by default. Max Master is the highest MAC Address a device will poll to discover new devices. Thus, it is likely that your device is not being discovered because the device with the highest MAC address on the network has a Max Master of 127 or lower. It is suggested that you use a MAC Address number below 127 as, by convention, values greater than 127 are usually reserved for slave devices. If you must use MAC addresses above 127, then make sure all the devices' Max Masters are set to a high value.

Q: My device MAC address is less than 127 but it isn't being discovered.

One cause could be that the device with the highest MAC Address prior to adding your device has a Max Master setting that is less than your device's MAC address. For example, if the previous device has a Max Master of 35 and your device's MAC address is 40, then the device won't be discovered. An easy fix is to increase the Max Master on the other devices. In general, it is highly discouraged to change the Max Master at all because others who try to add a device on the network will run into similar problems.

Q: I created a network of MSTP devices between two buildings and it doesn't work.

Recall that the ground level voltage between the buildings may be different, which means the RS485 cannot read the bits inside the wire. It is recommended to have two wires for data, a GND, and a shield that is connected to ground at one end to prevent any noise from disrupting data transfer. Refer to this article for more information: https://store.chipkin.com/articles/rs485-rs485-cables-why-you-need-3-wires-for-2-two-wire-rs485.

Frequently Asked Questions (FAQ)

Q: My MS/TP network works in the lab but when I install it on site, it stops working. Why?

There are a lot of possible problems. One could be like the situation described in the previous question. In that case, a GND wire is suggested. Another situation may be that there is a lot of electrical noise in the environment that is caused by hardware such as a Variable Speed Drive or Compressor. Attach a shield that is connected to ground at one end to prevent noise. Refer to these articles for more detail: https://store.chipkin.com/articles/bacnet-mstp-installation-rs485-and-cables

Q: How do I add a new device to the MS/TP network?

Set an appropriate MAC address to the device that is not used by other devices. This MAC address should be less than 127.

Find the baud rate that the other devices on the network are using. Set the baud rate of the device to that.

Wire the device to the network.

Aside: Use a trunk topology. The trunk topology allows devices to have a lower capacitance on the network, while keeping the speed of the communication consistent. The star topology, for example, makes it so that the device in the centre can communicate with all other devices faster than those devices can communicate with each other, causing inconsistent speeds. Read “MS/TP Trunk Topology” in this manual for more details.

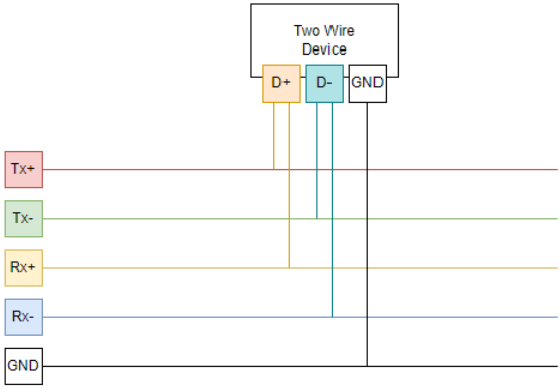
Wait for it to be added to the network (< 5 mins).

Confirm that it was added to the network by using the CAS BACnet Explorer to discover it.

Frequently Asked Questions (FAQ)

Q: I have a 4 wire MS/TP network and I have a 2 wire MS/TP device. How do I connect the 2 wire device to the network?

The D+ should be connected to Tx+ and Rx+. The D- should be connected to Tx- and Rx-. The GND will connect to each other. Refer to this diagram.



Q: How do I discover a MS/TP device using my laptop?

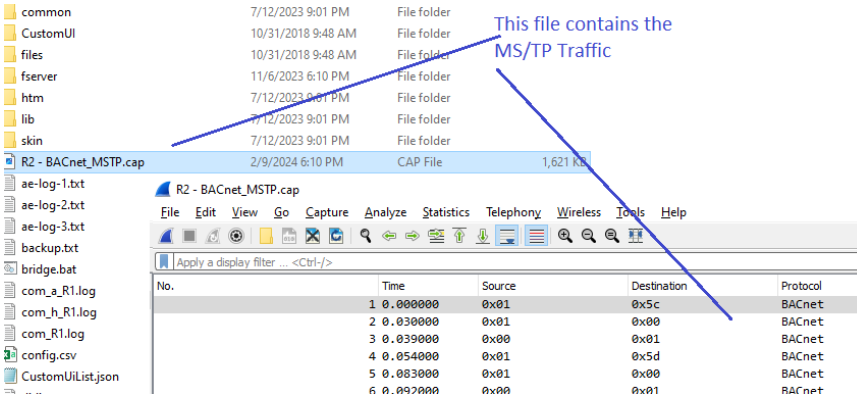
We recommend using a BACnet MS/TP to BACnet IP router. They are available for purchase in our store. If you cannot use the router, then you can use a USB to RS485 converter and a tool that supports BACnet MS/TP like the CAS BACnet Explorer. Note that there may be some issues with non-real-time operating systems (OS) like Windows or Linux. As MSTP devices send messages back and forth, the non-real-time OS may not be able to receive and respond to messages as fast as the MS/TP devices can. Thus, the laptop may talk out of turn and cause problems on the network. Nowadays, this is less of a problem.

Frequently Asked Questions (FAQ)

Q: How do I take a log of the communication on a MS/TP network?

You will need a USB to RS485 converter. Then, follow these steps: https://steve.kargs.net/bacnet/bacnet-mstp-wireshark-live-capture/

QuickServers have an internal method of capturing and reporting MS/TP Traffic. From the user interface, one can select a 'Diagnostic', initiate the process, then download the diagnostic files. Among these files, you will find a ".cap" file. To open the file, start Wireshark and open the file.



BBMD

Read these articles:

https://store.chipkin.com/articles/cas-bacnet-bbmd-solves-the-bacnet-broadcasting-problem

Chipkin - CAS BBMD - BACnet Broadcasts solved - Press Release2_13-16-14-48.pdf

Frequently Asked Questions (FAQ)

Q: I have a large MS/TP network with a lot of devices. My devices are slow to respond. Why?

There is a lot of frame overhead that is created when using a MS/TP network. Overhead refers to the costs used on managing the network rather than the communication of messages. This includes the management of the token, polling, etc. More details can be found in the "BACnet MS/TP Bandwidth Issues" section of the manual.

Q: What is a MS/TP repeater? What problems do they solve? Where can I buy one?

MSTP repeaters are used to fix degradation of voltages over a long distance of wire. Because wires have resistance, voltage levels may drop below the interpretable amount over long distances such as between buildings. We can use the repeater to increase the voltage levels and propagate the signal further. Unless you have 1000 - 2000 ft of wire, this is rarely needed. You can buy a RS485 repeater, which is essentially a MS/TP repeater.

Q: What is line drive on and line drive off? Why is this important to know?

This is a topic that you should not need to know in detail, however, it is described in the "What can go wrong with RS485" section of the manual.

Frequently Asked Questions (FAQ)

Q: What is a bias resistor? Why would I use one? What value should I use? Where do I install it?

Wires can become capacitors and keep at a certain voltage after it's done transferring data. By using a bias resistor, it can drain the voltage so that it won't interfere with any other signals sent through the wire. You should install one at one end of a network/repeated trunk. However, this is very rare and more apparent with big wires. More details can be seen here:
https://store.chipkin.com/articles/rs485-rs485-cables-why-you-need-3-wires-for-2-two-wire-rs485

Q: What are some of the MS/TP network settings, and what do they do?

Max_master: The highest address a device will poll to discover a master. The default is 127.

Max_info_frames: How many frames a device can send out before it is required to pass the token to the next master. You may set it higher if you have devices that need to respond to a lot of important messages.

Poll Station: Devices do not poll for master all at once, but rather a few at a time. The Poll Station contains the last node it visited to poll for a master. A device may or may not be occupying this node.

This Station: Current station, refers to the devices' own MAC Address.

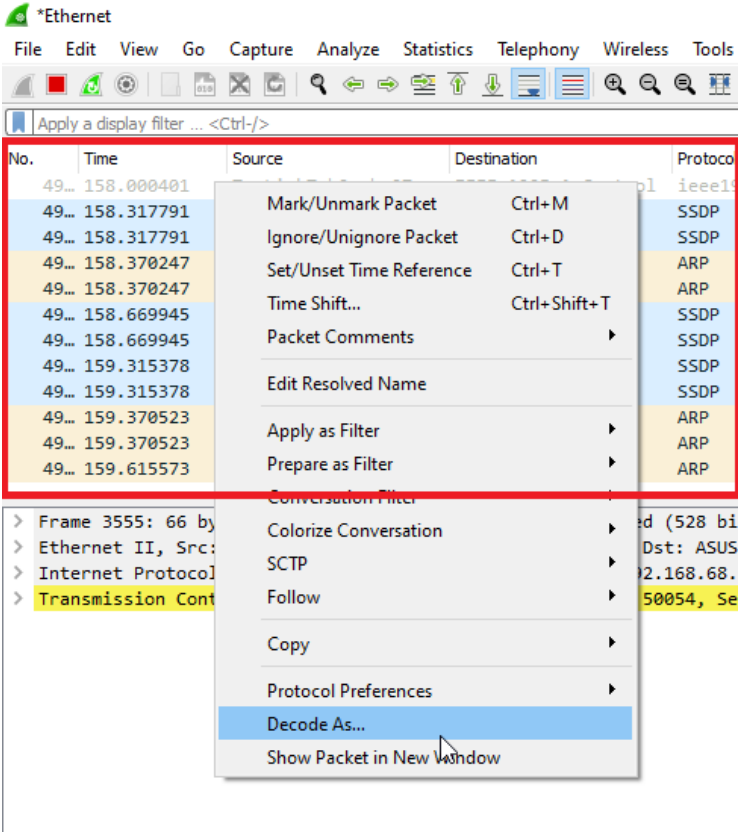
Next Station: The next station it will pass the token to. Essentially, it is the next known master. If there is none, it will simply be its own MAC Address.

Frequently Asked Questions (FAQ)

Wireshark

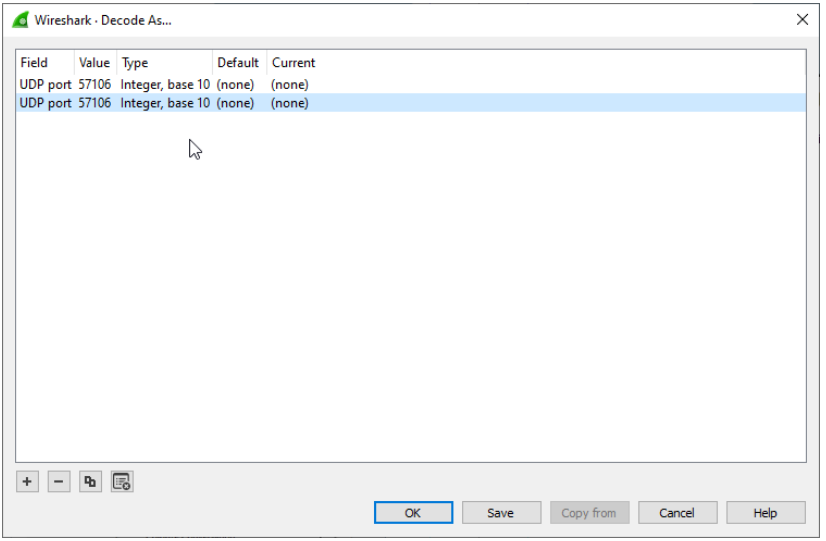
Q: How do I view a BACnet packet that is not on the standard BACnet port 47808?

You can view a BACnet packet by opening Wireshark, choosing a network of interest, and right-clicking anywhere in the red box shown in the image below and press "Decode As".



Frequently Asked Questions (FAQ)

Press the plus sign in the bottom left corner of the pop-up window. There should be a new row that appears. (This is the row highlighted blue in the image.)



Next, change the "Value" to the port desired and the "Current" into BVLC and press OK.

Field	Value	Type	Default	Current
UDP port	57106	Integer, base 10	(none)	(none)
UDP port	47809	Integer, base 10	(none)	BVLC

Frequently Asked Questions (FAQ)

BBMD

Q: I have a network with two different subnets on the same network. They can't discover each other, why?

BACnet uses UDP to broadcast discovery messages. However, these broadcasts are only within subnets as routers are unable to forward broadcast messages. To allow discovery between subnets, you would need a BBMD on each subnet, configured with each other's IP addresses and subnet mask.

Q: Do I need a BBMD for each subnetwork?

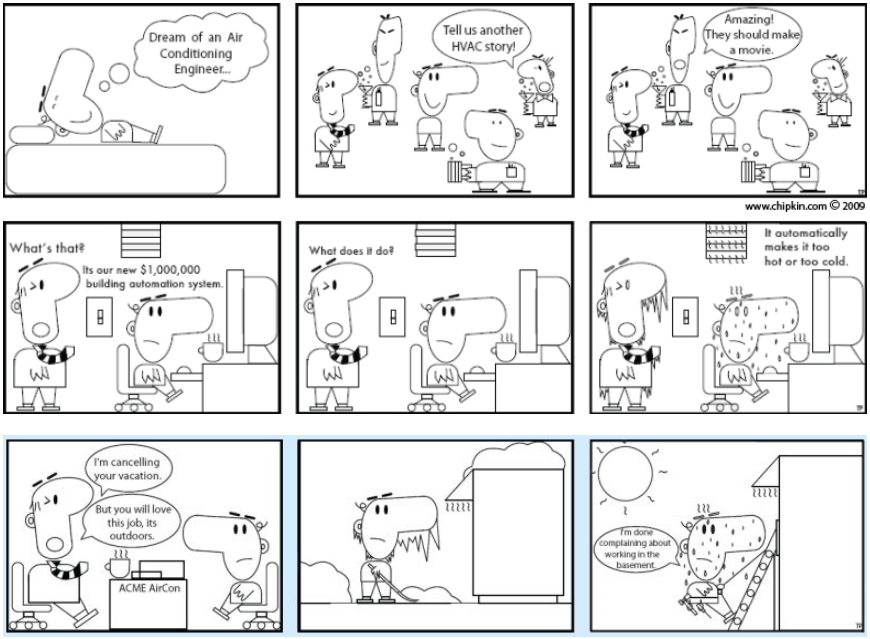
Yes and no. If a device supports Foreign Device Registration (mandatory after revision 17), it can register itself with a central BBMD to avoid needing a BBMD for that device in particular on the subnet. Other devices on that subnet will need a BBMD though. If FDR is not supported, then a BBMD must be used for discovery. If your BACnet client can manually configure a BACnet device, then you can bypass the discovery. Since BBMD is mainly used for discovery, a BBMD won't be necessary in that case.

Q: Are BBMDs software or hardware?

All the gateways sold by Chipkin support BBMD. They can be BBMDs and also do protocol conversion simultaneously. E.g. You are doing Modbus to BACnet—that gateway can also be configured to implement a BBMD.

There is also a software version of a BBMD. This is an application that runs on a Windows or Linux (tested on Ubuntu). No additional hardware is required.

CHIPKIN



Chipkin Automation Systems

3381 Cambie St, #211
Vancouver, BC
Canada,
V5Z 4R3

Phone: 866-383-1657
E-mail: bacnet@chipkin.com

www.chipkin.com