



SharkFest'20 Virtual



BACnet & Wireshark for beginners

by looking at packets!

Werner Fischer

Manager Infrastructure | avodaq AG



#whoami



- Speaker on all EU SharkFests, Asia and today virtual
- Protocol geek for more than two decades right now
- Learning always new things – also on every SharkFest
- Comparing Bits and Bytes
- Your presenter for the next hour



Agenda



- General
- Data Link Layer
- Objects and Services
- BACnet and Wireshark
- Protocol Basics
- BACnet MS/TP
- Internetworking
- Wrap-up



→ Czech cartoon hero Little Mole guides with you during this presentation – each clipart © by Zdenek Miler



BACnet - General





BACnet



- “Building Automation and Control Networks”
- What is it?
 - BACnet is a registered trademark of ASHRAE
 - Protocol specification
- Data and communication of all devices specified in ISO-Standard 16-484-5
- ASHRAE
 - (American Society of Heating, Refrigeration and Air-Conditioning Engineering)





BACnet



- 0xBAC0 – 0xBAC9
- 1011 1010 1100 0000 - 1011 1010 1100 1001
- 47808 - 47817





BACnet – used for what?



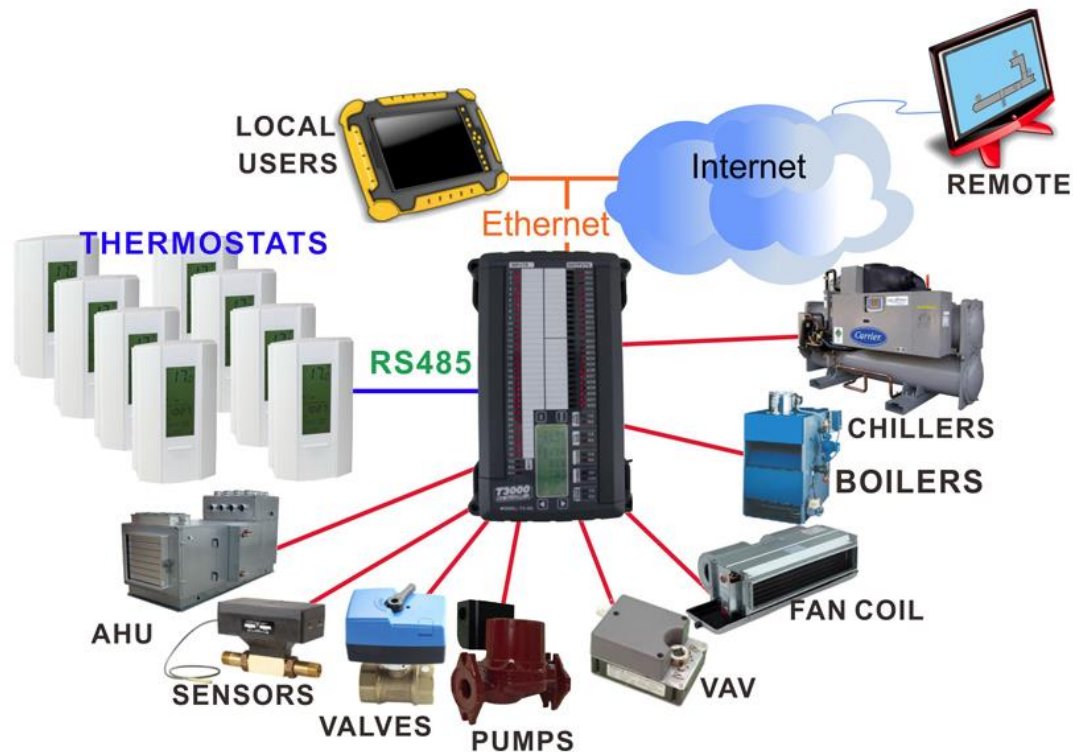
- BACnet today provides all the capabilities to interconnect BACnet devices within a BA system
- Control of
 - Ventilating
 - air-conditioning
 - Lighting
 - Heating
 - Access
 - fire detection systems
 - and many more things



© Zdeněk Miller
Agentur: WDR mediagroup licensing GmbH



BACnet – used for what?





Terms and Abbreviations



- APDU
- BBMD
- BDT
- BVLC
- BVLL
- COV
- DADR
- DLEN
- DNET
- FDT
- LPCI
- LPDU

- LSAP
- LSDU
- MAC
- NPCI
- NPDU
- NSAP
- NSDU
- PFM
- SA
- SADR
- SNET

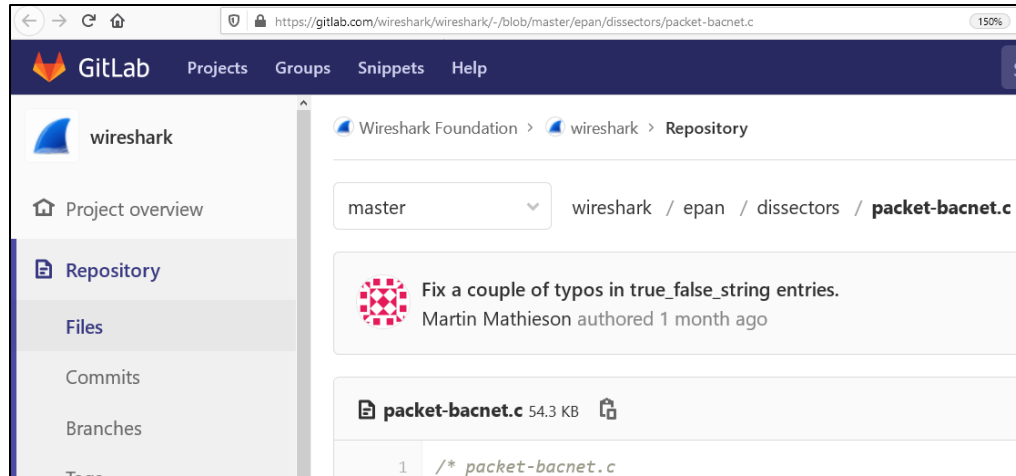




BACnet Protocol – search the source code



- Learn more about the protocol itself
- → How we can do it together?





BACnet – Data Link Layer



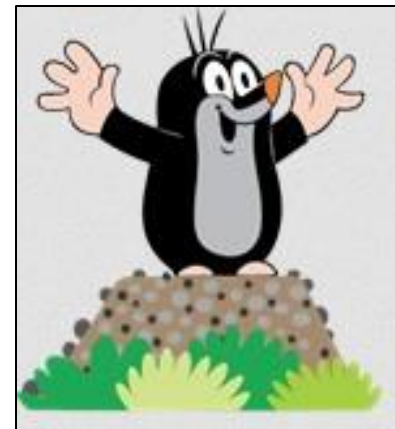
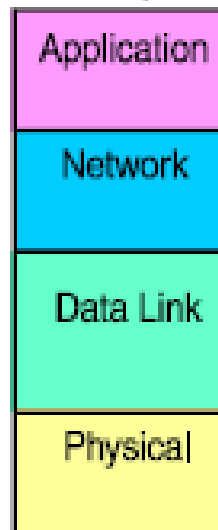
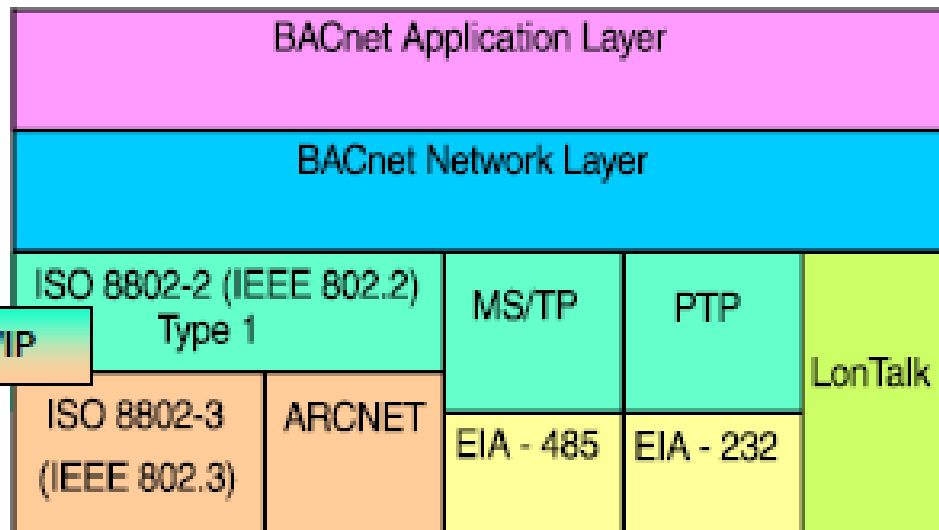


BACnet is using different media – Data Link protocols



BACnet Layers

Equivalent
OSI Layers





BACnet Protocol – different DL protocols



GitLab

Projects

Groups

Snippets

Help



wireshark

<https://gitlab.com/wireshark/wireshark/-/issues/4168>

ARCNET

<https://gitlab.com/wireshark/wireshark/-/issues/15530>

IPv4

<https://gitlab.com/wireshark/wireshark/-/issues/16008>

MS/TP

<https://gitlab.com/wireshark/wireshark/-/issues/12422>

802.3



BACnet Protocol – ARCNET



- <https://gitlab.com/wireshark/wireshark/-/blob/master/epan/dissectors/packet-llc.c>
- → Reading the comments inside the code

```
900      /*  
901         * BACNET-over-ARCNET is really BACNET-over-802.2 LLC-over-ARCNET,  
902         * apparently.  
903         */
```





BACnet and Wireshark





BACnet Protocol



- Learn more about the protocol itself
- → How we can do it together?
- Let's setup a small BACnet lab
- → Wireshark, BACnet Server and a BACnet Explorer (YABE)

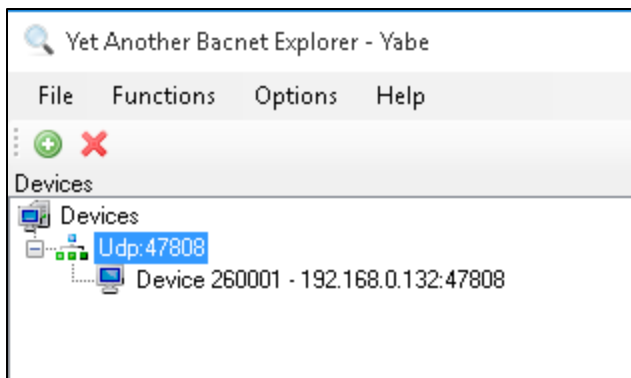
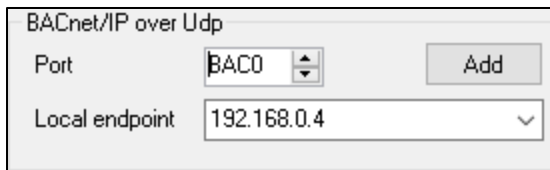
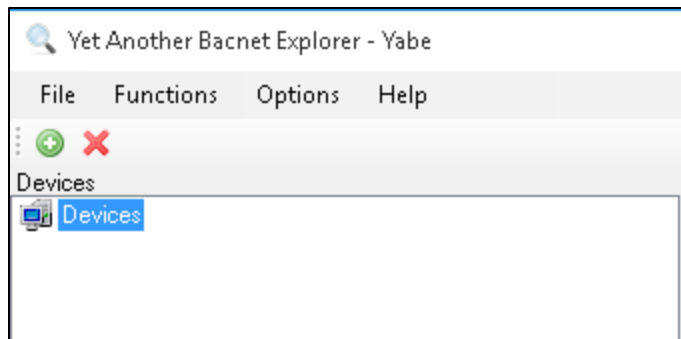




BACnet first steps



- Some software tools needed





BACnet & Wireshark & Colors



Wireshark · Coloring Rules BACNET

Name	Filter
<input checked="" type="checkbox"/> BACnet_APDU_Complex-ACK	bacapp.type == 3
<input checked="" type="checkbox"/> BACnet_NPDU_I-Am-Router-to-Network	bacnet.mesgtyp == 0x01
<input checked="" type="checkbox"/> BACnet_NPDU_Who-IS-Router-to-Network	bacnet.mesgtyp == 0x00
<input checked="" type="checkbox"/> BACnet_APDU_who-Has	bacapp.unconfirmed_service == 7
<input checked="" type="checkbox"/> BACnet_APDU_who-Is	bacapp.unconfirmed_service == 8
<input checked="" type="checkbox"/> BACnet_APDU_I-Am packets...	bacapp.unconfirmed_service == 0
<input checked="" type="checkbox"/> BACnet_BVLC_Broadcast-to-Network	bvlc.function == 0x09
<input checked="" type="checkbox"/> Local BACnet broadcast	eth.dst == ff:ff:ff:ff:ff:ff && !bacnet.dnet && bacnet
<input checked="" type="checkbox"/> BACnet_APDU_NACK	bacapp.NAK == 1
<input checked="" type="checkbox"/> BACnet_APDU_Abort	bacapp.abort_reason
<input checked="" type="checkbox"/> V2 tunneled	bacnet.mesgtyp == 0x81
<input checked="" type="checkbox"/> BACnet_APDU_Error	bacapp.type == 5
<input checked="" type="checkbox"/> MSTP_Token	mstp.frame_type == 0
<input checked="" type="checkbox"/> MSTP_Poll-For-MAster	mstp.frame_type == 1





Wireshark · Preferences

The screenshot shows the Wireshark 'Columns' pane on the left, which is used to configure the columns displayed in the packet list. The 'Columns' pane has a tree view on the left with 'Appearance' expanded, and 'Columns' selected. The main pane shows a list of columns with checkboxes for 'Displayed' and 'Type'. The main packet list on the right shows the columns as they appear in the interface.

Displayed	Title	Type	Fields
<input checked="" type="checkbox"/>	Source	Source address	
<input checked="" type="checkbox"/>	Destination	Destination address	
<input checked="" type="checkbox"/>	Protocol	Protocol	
<input checked="" type="checkbox"/>	Length	Packet length (bytes)	
<input type="checkbox"/>	Destination Network Address	Custom	bacnet.dnet
<input type="checkbox"/>	Priority	Custom	bacnet.control_prio
<input type="checkbox"/>	Priority	Custom	bacnet.control_prio
<input type="checkbox"/>	Frame Type	Custom	mstp.frame_type
<input type="checkbox"/>	Abort Reason	Custom	bacapp.abort_reason
<input type="checkbox"/>	Error Code	Custom	bacapp.error_code
<input type="checkbox"/>	Reject Reason	Custom	bacapp.reject_reason
<input type="checkbox"/>	Destination Network Address	Custom	bacnet.dnet
<input checked="" type="checkbox"/>	Destination MAC Layer Address Length	Custom	bacnet.dlen
<input checked="" type="checkbox"/>	Destination ISO 8802-3 MAC Address	Custom	bacnet.dadr_eth
<input checked="" type="checkbox"/>	Hop Count	Custom	bacnet.hopc
<input checked="" type="checkbox"/>	ProcessIdentifier	Custom	bacapp.processId
<input checked="" type="checkbox"/>	Source Network Address	Custom	bacnet.snet
<input checked="" type="checkbox"/>	Source MAC Layer Address Length	Custom	bacnet.slen
<input checked="" type="checkbox"/>	SADR	Custom	bacnet.sadr_mstp
<input checked="" type="checkbox"/>	Info	Information	

The screenshot shows the Wireshark column menu. The columns are listed with checkboxes. The 'Length' column is highlighted in blue, indicating it is selected. The 'Info' column is also highlighted in blue, indicating it is selected. The 'Remove this Column' option is at the bottom of the menu.

Protocol	Length	Destination
5 BACnet-APDU	67	
5 BACnet-APDU	67	
5 BACnet-APDU	54	
BACnet-APDU	77	
5 BACnet-APDU	67	
BACnet-APDU	77	
BACnet-APDU	77	
BACnet-APDU	77	

Column Menu:

- ☐ No.
- ☒ Time
- ☐ Delta Time
- ☐ Source
- ☐ Destination
- ☐ Protocol
- ☒ Length
- ☐ Destination Network Address
- ☐ Priority
- ☐ Priority
- ☐ Frame Type
- ☐ Abort Reason
- ☐ Error Code
- ☐ Reject Reason
- ☐ Destination Network Address
- ☒ Destination MAC Layer Address Length
- ☐ Destination ISO 8802-3 MAC Address
- ☐ Hop Count
- ☐ ProcessIdentifier
- ☐ Source Network Address
- ☐ Source MAC Layer Address Length
- ☐ SADR
- ☒ Info
- ☐ Remove this Column



BACnet useful filters



- BACnet Abort
 - `bacapp.abort_reason`
- Reply for PFM
 - `mstp.frame_type == 2`
- all BACnet packets
 - `bvlc || bacnet || bacapp`



BACnet & Wireshark statistics



Wireshark · Packets sorted by Service · Adapter for loopback traffic capture (udp port 47808 or ip6 multicast)



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
▼ BACnet Packets by Service	21				0.0000	100%	0.0600	649.427
> who-Is (Unconfirmed Service Request)	3				0.0000	14.29%	0.0100	634.706
> utcTimeSynchronization (Unconfirmed Service Request)	1				0.0000	4.76%	0.0100	651.196
> readProperty (Confirmed Service Request)	3				0.0000	14.29%	0.0300	649.427
> readProperty (ComplexAck)	2				0.0000	9.52%	0.0200	649.429
> i-Am (Unconfirmed Service Request)	11				0.0000	52.38%	0.0100	107.193
> ERROR: readProperty	1				0.0000	4.76%	0.0100	649.427





BACnet & Random packet generator (Randpkt)



```
C:\Program Files\Wireshark>randpkt.exe
```

```
Usage: randpkt [-b maxbytes] [-c count] [-t type] [-r] filename
```

```
Default max bytes (per packet) is 5000
```

```
Default count is 1000.
```

```
-r: random packet type selection
```

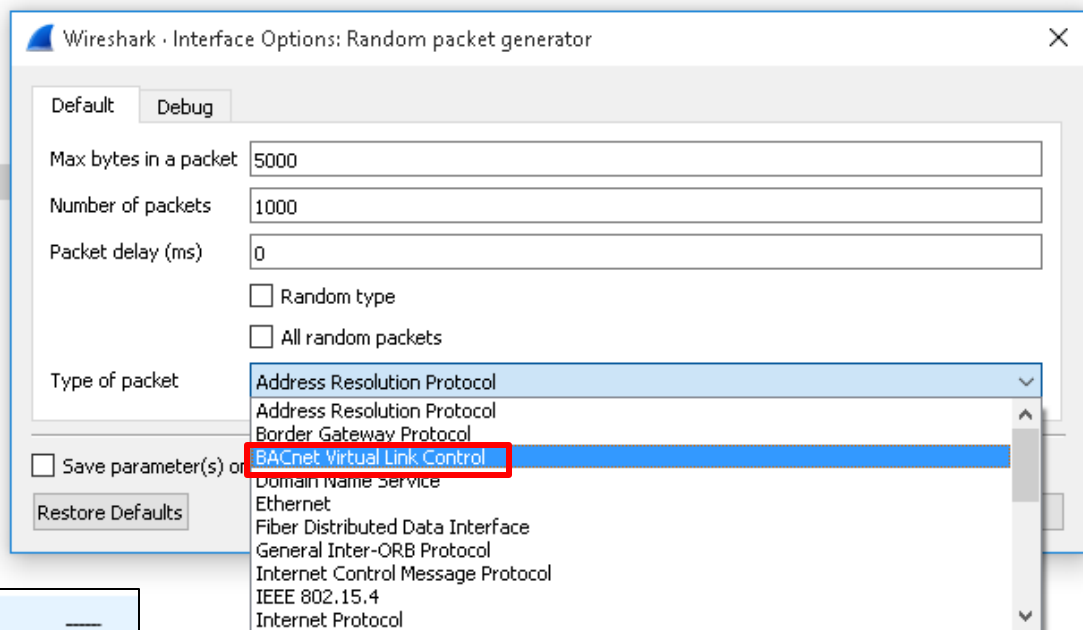
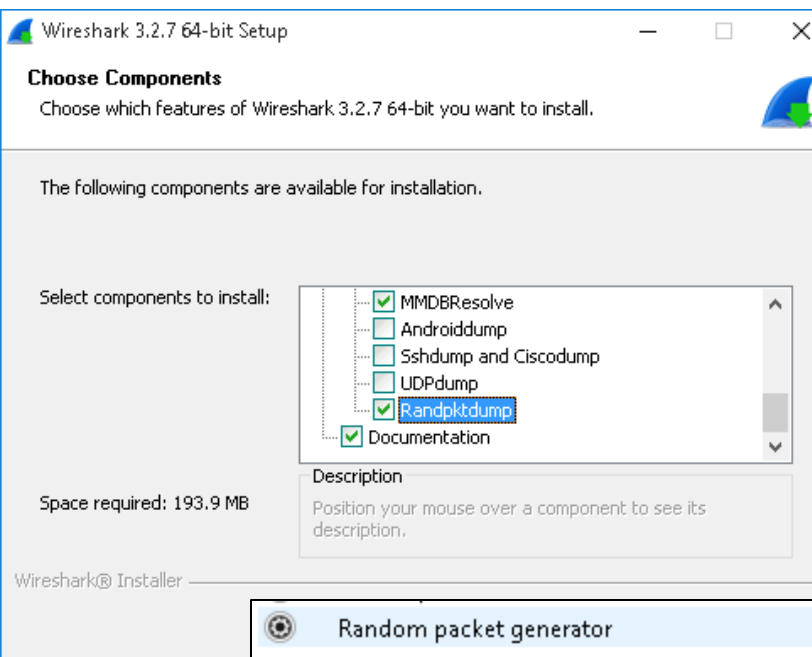


Types:

arp	Address Resolution Protocol
bgp	Border Gateway Protocol
bvlc	BACnet Virtual Link Control
dns	Domain Name Service

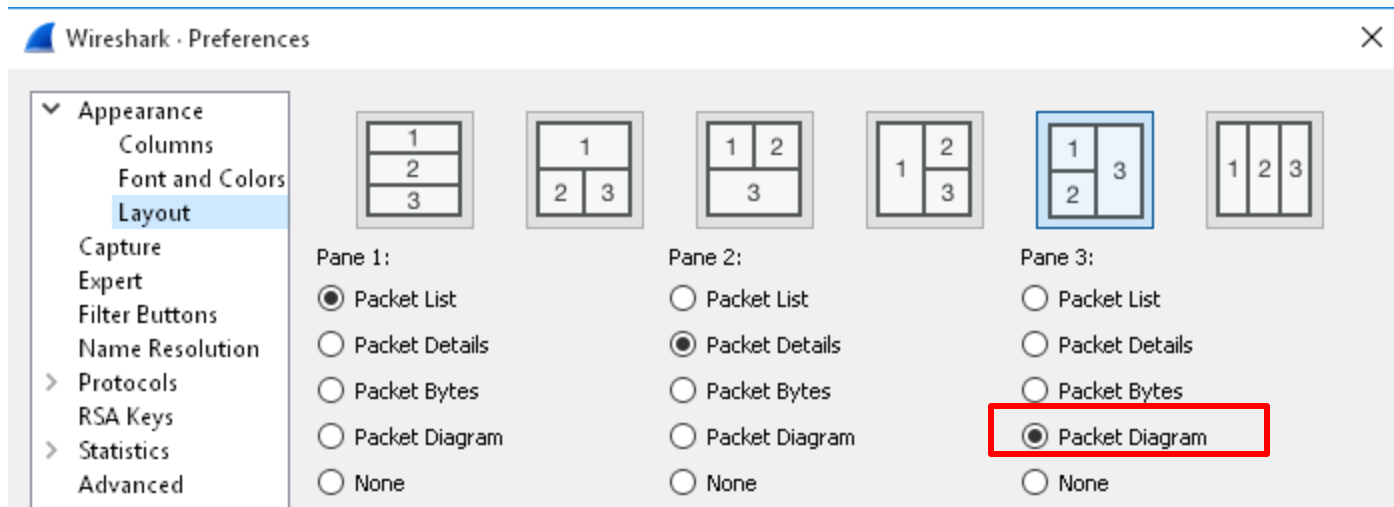


BACnet & Random packet generator (RandpktDump)





BACnet & Packet diagram

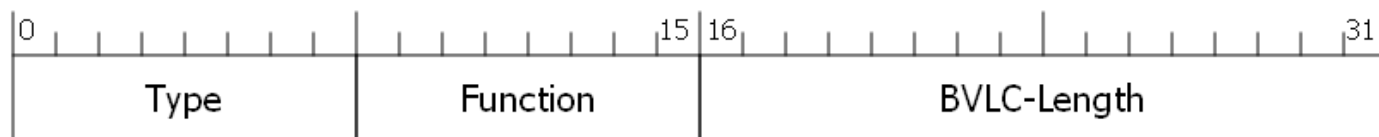




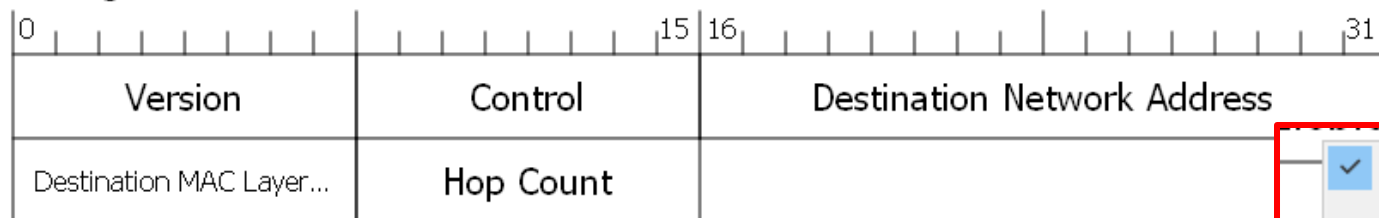
BACnet & Packet diagram



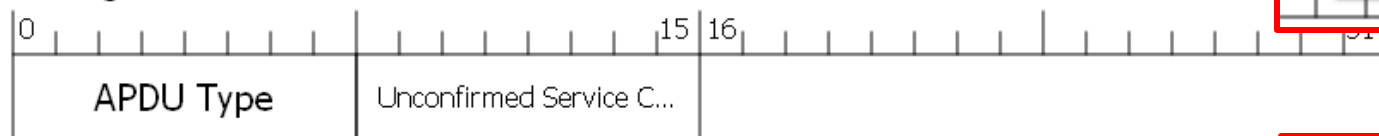
BACnet Virtual Link Control



Building Automation and Control Network NPDU



Building Automation and Control Network APDU



DEVELOPMENT VERSION
WIRESHARK

- ☒ Show Field Values
- Save Diagram As...
- Copy as Raster Image

Packets: 9 · Displayed: 9 (100.0%)

Profile: BACNET (diagram)



BACnet protocol



```
0000 11111111 11111111 11111111 11111111 11111111 11111111
0008 11001001 00000000 00010000 10100101 00001000 00000000
0010 00000000 00100101 01100000 00011100 00000000 00000000
0018 10111010 01000100 11000000 10101000 00000000 00011000
0020 00000000 11111111 10111010 11000000 10111010 11000000
0028 00000000 00000000 10000001 00001011 00000000 00001000
0030 00000001 00010000 01101011 01101011 01101011 01101011
0038 01101011 01101011 01101011 01101011
```





BACnet protocol basics - Devices



- The BACnet standard defines a service that allows devices to advertise themselves in the network
- The service is called "I-Am"
- "I-Am" messages contain information that univocally identify BACnet devices
 - the BACnet MAC address and
 - the device ID





BACnet protocol basics



- Very basic service is Who-Is request



- Followed by I-am replies:





BACnet protocol basics – who-Is



- ▼ Building Automation and Control Network NPDU
 - Version: 0x01 (ASHRAE 135-1995)
 - Control: 0x20, Destination Specifier
 - Destination Network Address: 65535
 - Destination MAC Layer Address Length: 0 indicates Broadcast on Destination Network
 - Hop Count: 255
- ▼ Building Automation and Control Network APDU
 - 0001 = APDU Type: Unconfirmed-REQ (1)
 - Unconfirmed Service Choice: who-Is (8)

- ▼ Building Automation and Control Network APDU
 - 0001 = APDU Type: Unconfirmed-REQ (1)
 - Unconfirmed Service Choice: who-Is (8)
 - ▼ Device Instance Range Low Limit: 2500
 - Context Tag: 0, Length/Value/Type: 2
 - ▼ Device Instance Range High Limit: 2510
 - Context Tag: 1, Length/Value/Type: 2





BACnet protocol basics

– i-Am



```
▼ Building Automation and Control Network APDU
  0001 .... = APDU Type: Unconfirmed-REQ (1)
  Unconfirmed Service Choice: i-Am (0)
  ▼ ObjectIdentifier: device, 260001
    ▼ Application Tag: BACnetObjectIdentifier, Length/Value/Type: 4
      .... 0... = Tag Class: Application Tag
      1100 .... = Application Tag Number: BACnetObjectIdentifier (12)
      Length Value Type: 4
      0000 0010 00.. .... .... .... = Object Type: device (8)
      .... .... ..00 0011 1111 0111 1010 0001 = Instance Number: 260001
```





BACnet - Objects and Services





BACnet objects



- The BACnet protocol makes the information available as objects
- Each object contains several properties
- Object describe its current state, allow it to be controlled, and can indicate alarm states
- There is always at least one object in a device – it is used to represent the device itself

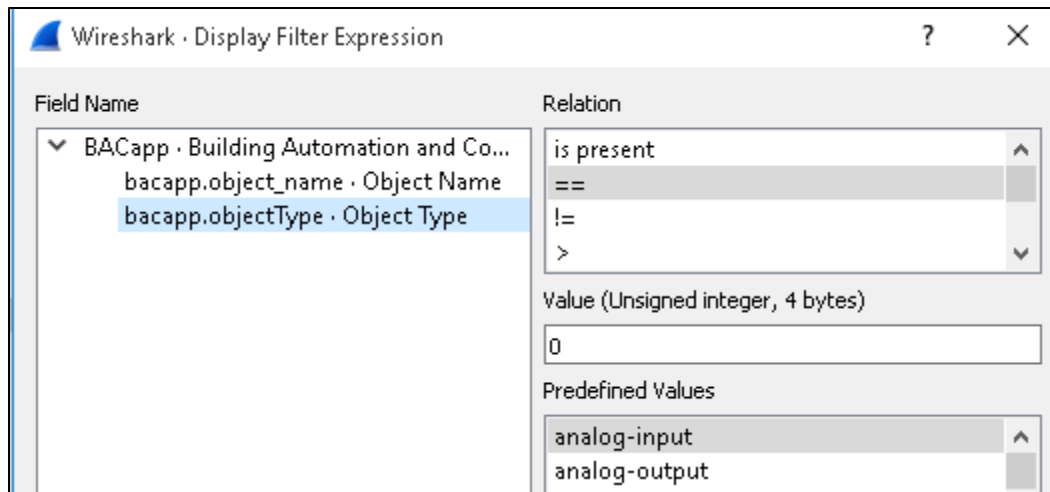




BACnet object types



- Analog Input
- Analog Output
- Binary Input
- Binary Output
- Device
- Program
- Trend Log Multiple
- ...and many more



GitLab

Projects

Groups

Snippets

Help



wireshark

<https://bugs.wireshark.org/bugzilla/attachment.cgi?id=14582>



BACnet services



- To exchange information, BACnet devices use services
- BACnet services are functions for obtaining and defining information in devices:
 - Alarm & Event Services
 - Change of Value (COV) reporting
 - Subscribe COV
 - Atomic Write File
 - Create Object
 - Delete Object
 - ...






BACnet services



- Services = Capabilities
- Some are confirmed, some are not confirmed

 Wireshark · Display Filter Expression

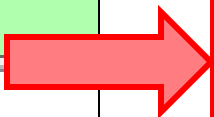
Field Name

▼ BACapp · Building Automation and Control Network AP...
bacapp.type · APDU Type

Predefined Values

Confirmed-REQ
Unconfirmed-REQ
Simple-ACK
Complex-ACK
Segment-ACK
Error
Reject
Abort

bacapp.type > 4	
No.	Time



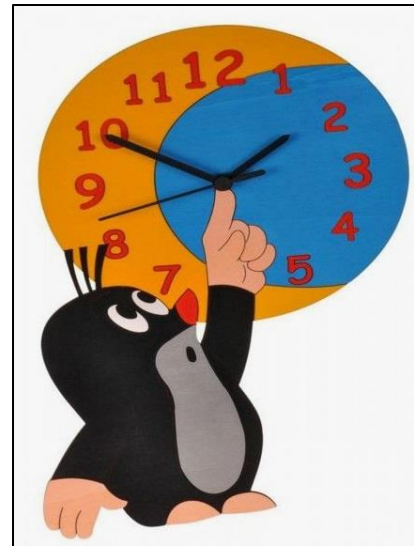


BACnet and time



- Time Synchronization
- UTC Time Synchronization

```
▼ Building Automation and Control Network APDU
  0001 .... = APDU Type: Unconfirmed-REQ (1)
  Unconfirmed Service Choice: utcTimeSynchronization (9)
  ▼ UTC-Time:
    ▼ Date: October 31, 2019, (Day of Week = Thursday)
      ▼ Application Tag: Date, Length/Value/Type: 4
        .... 0... = Tag Class: Application Tag
        1010 .... = Application Tag Number: Date (10)
        Length Value Type: 4
    ▼ Time: 5:54:51.51 P.M. = 17:54:51.51
      ▼ Application Tag: Time, Length/Value/Type: 4
        .... 0... = Tag Class: Application Tag
        1011 .... = Application Tag Number: Time (11)
        Length Value Type: 4
```





BACnet segmentation



- BACnet messages that don't fit in a single packet use segmentation
- Segmented messaging in BACnet is optional, which means that client devices must support methods to read data when a device APDU is small

```
▼ Building Automation and Control Network APDU
  0001 .... = APDU Type: Unconfirmed-REQ (1)
  Unconfirmed Service Choice: i-Am (0)
  > ObjectIdentifier: device, 110
  > Maximum ADPU Length Accepted: (Unsigned) 1476
  > Segmentation Supported: segmented-both
  > Vendor ID: Fr. Sauter AG (80)
```



BACnet max. APDU



bacapp.max_adpu_size · Size of Maximum ADPU accepted
bacapp.more_segments · More Segments
bacapp.NAK · NAK
bacapp.named_tag · Named Tag
bacapp.notify_type · Notify Type
bacapp.object_name · Object Name
bacapp.objectType · Object Type
bacapp.pduflags · PDU Flags
bacapp.Port · Port
bacapp.present_value.bit_string · Present Value (bit string)
bacapp.present_value.boolean · Present Value (bool)
bacapp.present_value.char_string · Present Value (char st...
bacapp.present_value.enum_index · Present Value (enu...

Up to MinimumMessageSize (50 octets)
Up to 128 octets
Up to 206 octets (fits in a LonTalk frame)
Up to 480 octets (fits in an ARCNET frame)
Up to 1024 octets
Up to 1476 octets (fits in an ISO 8802-3 frame)
reserved by ASHRAE
reserved by ASHRAE
reserved by ASHRAE
reserved by ASHRAE
reserved by ASHRAE
reserved by ASHRAE



BACnet MS/TP





BACnet MS/TP



- M (Master) S (Slave) TP (Token Passing)
- 0-127 addresses are for master devices
- 128-254 addresses are reserved for slave devices
- Only master devices can initiate requests and are part of the token passing
- Slave devices cannot initiate requests for data, they only reply to messages from other master devices and are not part of the token passing





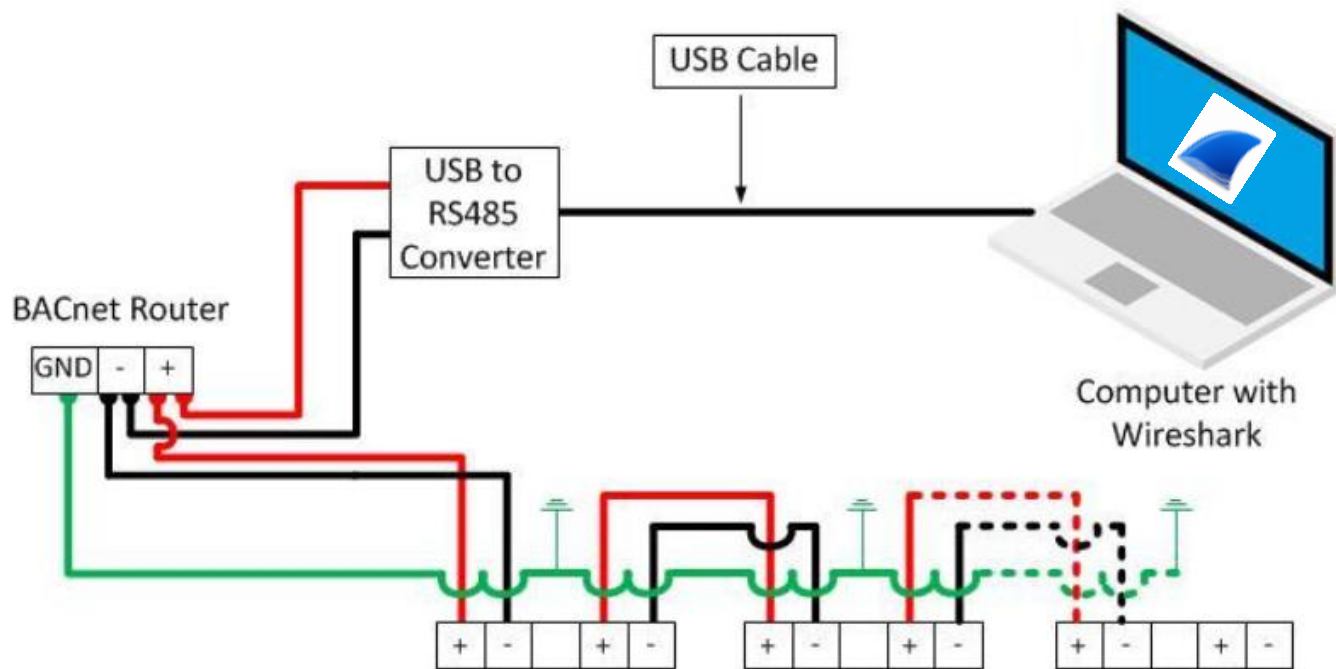
BACnet MS/TP PFM



- Address 255 used as broadcast
- It is better to cluster all the devices at adjacent addresses to minimize unwanted Poll From Master (PFM)
- Slaves conserve bandwidth, Masters burn bandwidth



How-to capture RS-485





RS-485 as extcap



Capture

...using this filter: All interfaces shown ▼

- ONBOARD
- BACnet MS/TP on COM3**
- USBPcap1
- USBPcap2

Learn

Wireshark · Interface Options: BACnet MS/TP on COM3

Baud Rate: 76800

- 9600
- 19200
- 38400
- 57600
- 76800**
- 115200

☐ Save parameters on capture start



About Wireshark

Wireshark Authors Folders

Filter by path

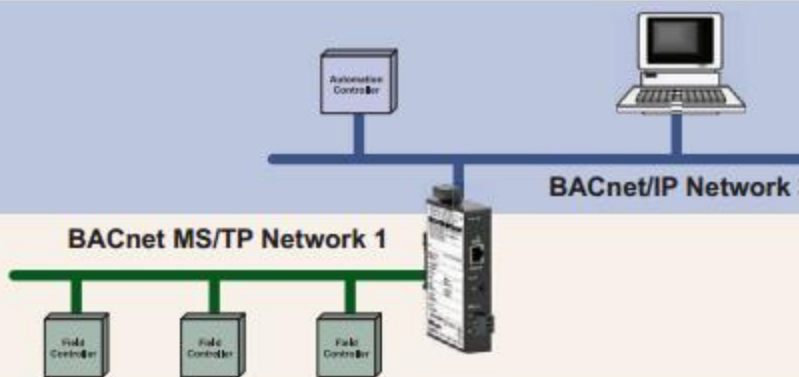
Extcap path: C:\Program Files\Wireshark\extcap

Name: mstpcap.exe

<https://sourceforge.net/projects/bacnet/files/bacnet-tools/bacnet-tools-0.8.6/bacnet-tools-0.8.6.zip>



BACnet internetworking





BACnet network



- “A set of two or more networks interconnected by routers. In a BACnet internetwork, there exists exactly one message path between any two nodes.”

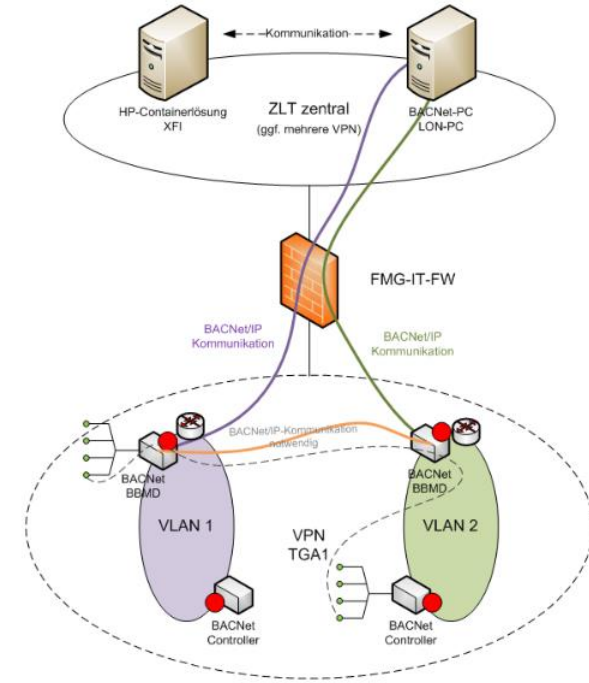




BACnet network with more than one subnet



- To discover devices on a foreign subnet you can configure the router to forward broadcasts or you can use **BBMD** (BACnet Broadcast Management Device)

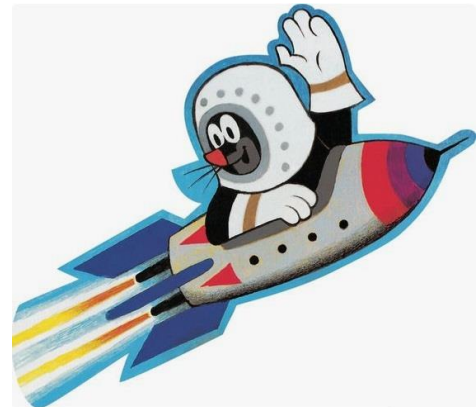




BBMD

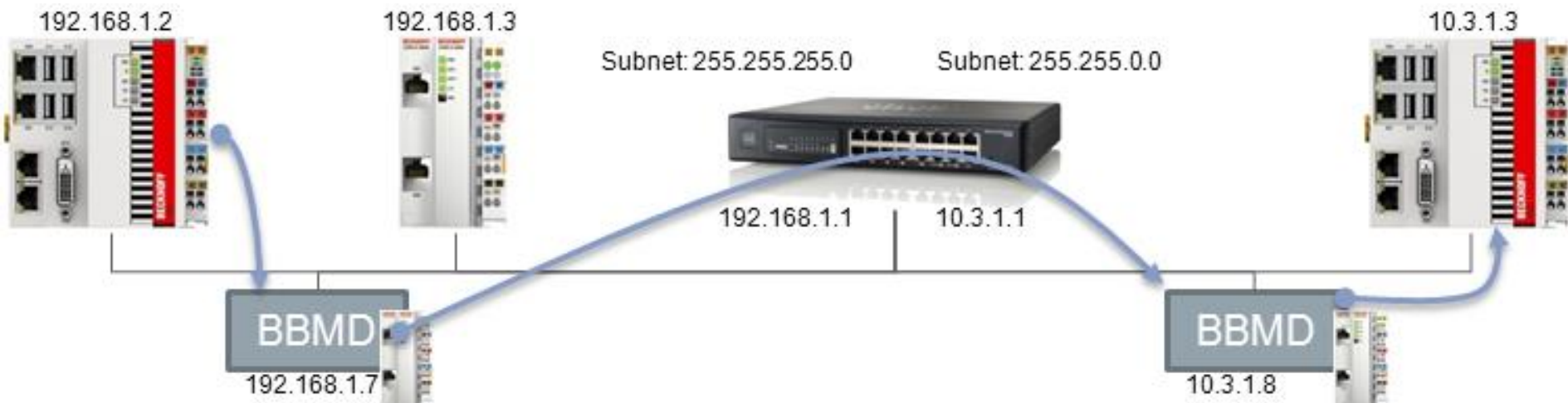


- BBMD - BACnet/IP Broadcast Management Device
- Different networks
 - One-Hop and Two-Hop





BBMD - two hop





BBMD function



Adapter | Settings | **BBMD** | Diagnosis

BACnet Broadcast Management Device Settings

Enable BBMD ☒ Enable

BD Table Size

Foreign device registration ☒ Allow

FD Table Size

Registration as Foreign Device

Remote Registration ☐ Enable

Remote BBMD IP

UDP Port

Time to Live (sec)

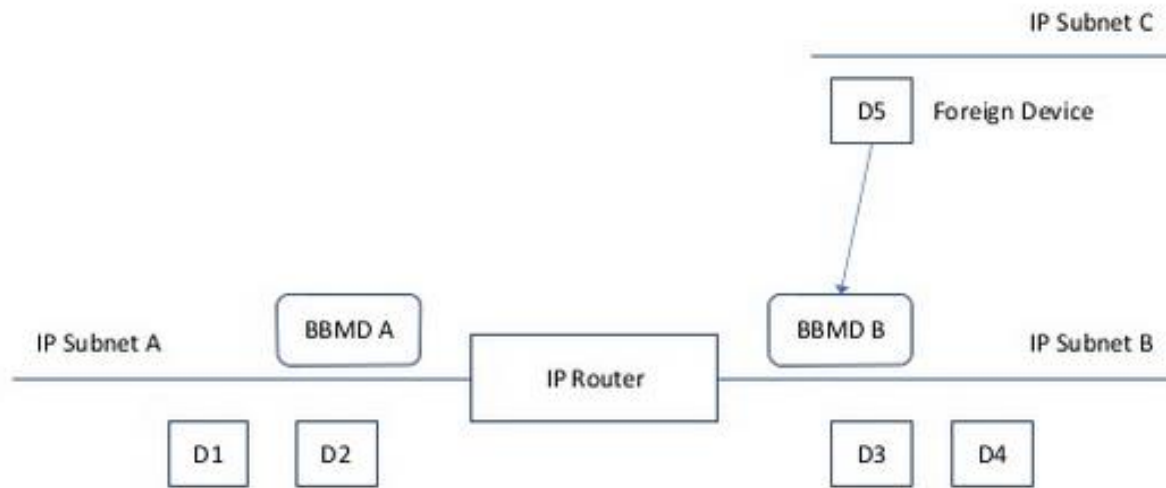
BBMD Table Configuration

Initial BDT | **Online BDT** | Online FDT

Entry Nr	Distribution Entry
<input checked="" type="checkbox"/> Entry_0	(10.3.1.8;255.255.255.255;47808)
<input type="checkbox"/> + ipAddr	10.3.1.8
<input type="checkbox"/> + mask	255.255.255.255
<input type="checkbox"/> udpPort	47808

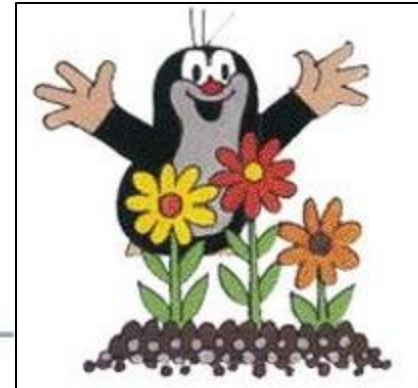
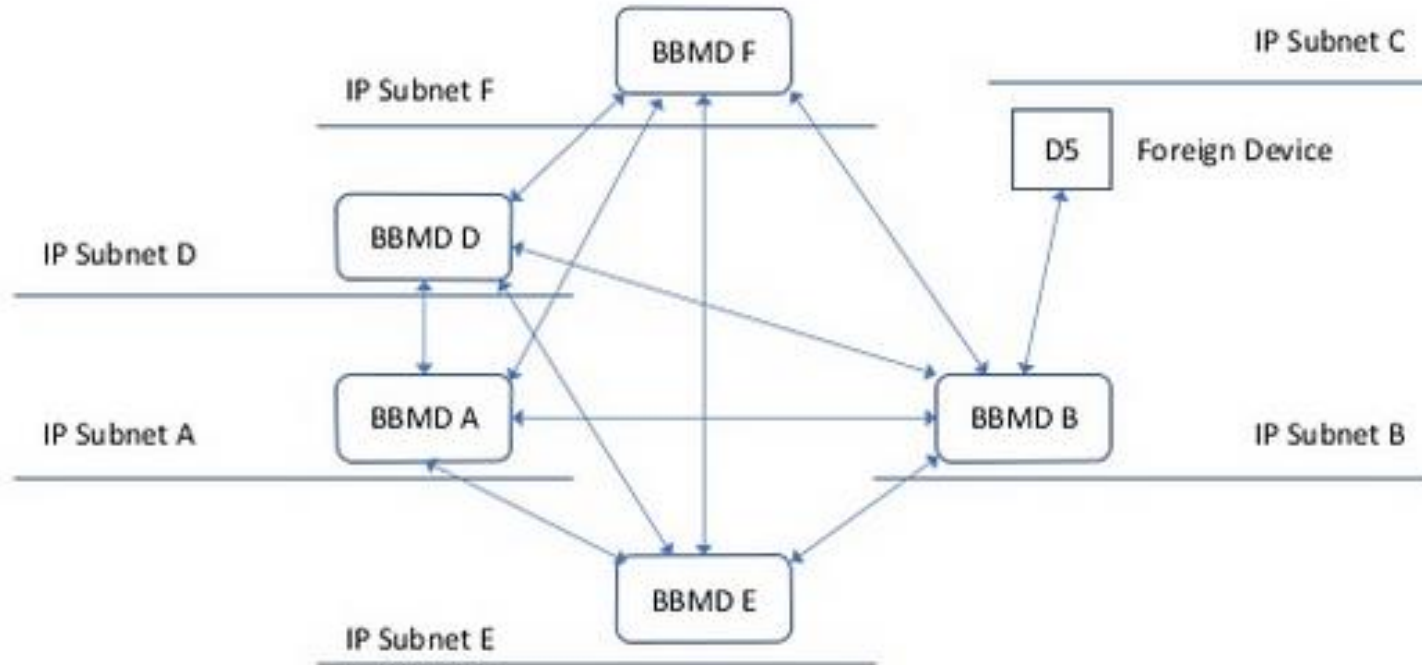


BBMD / Foreign Device Registration



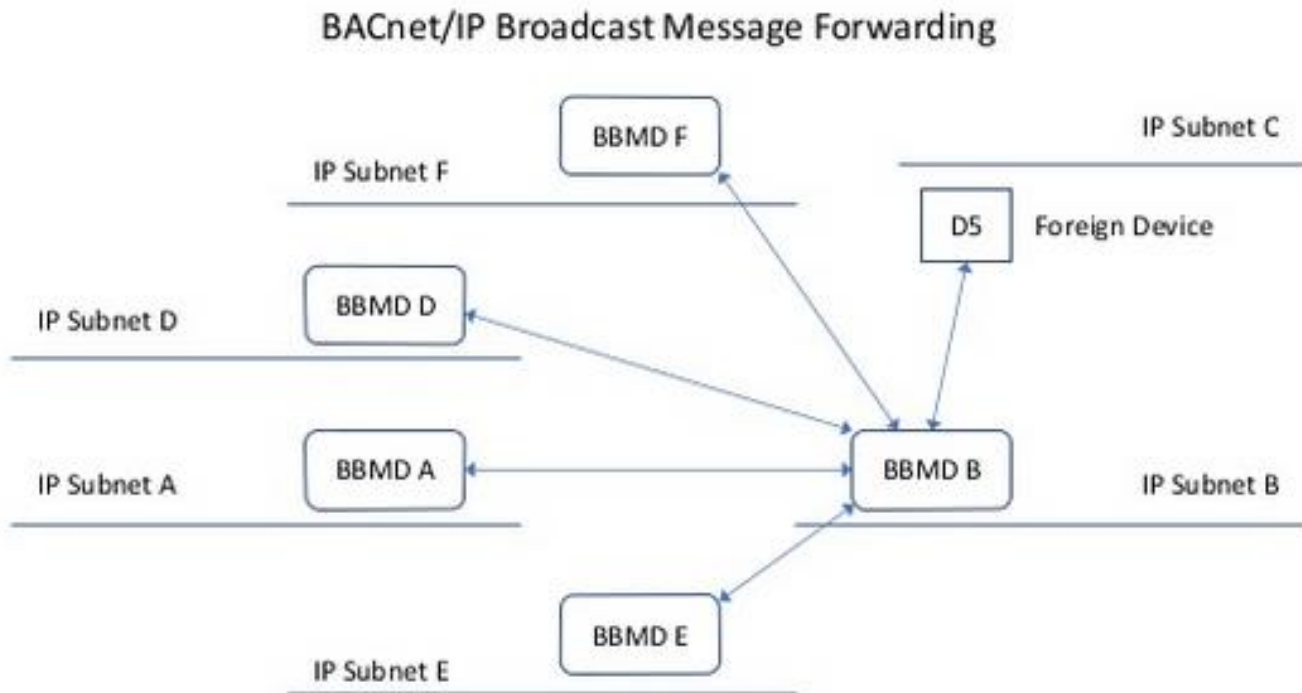


BBMD / Big network



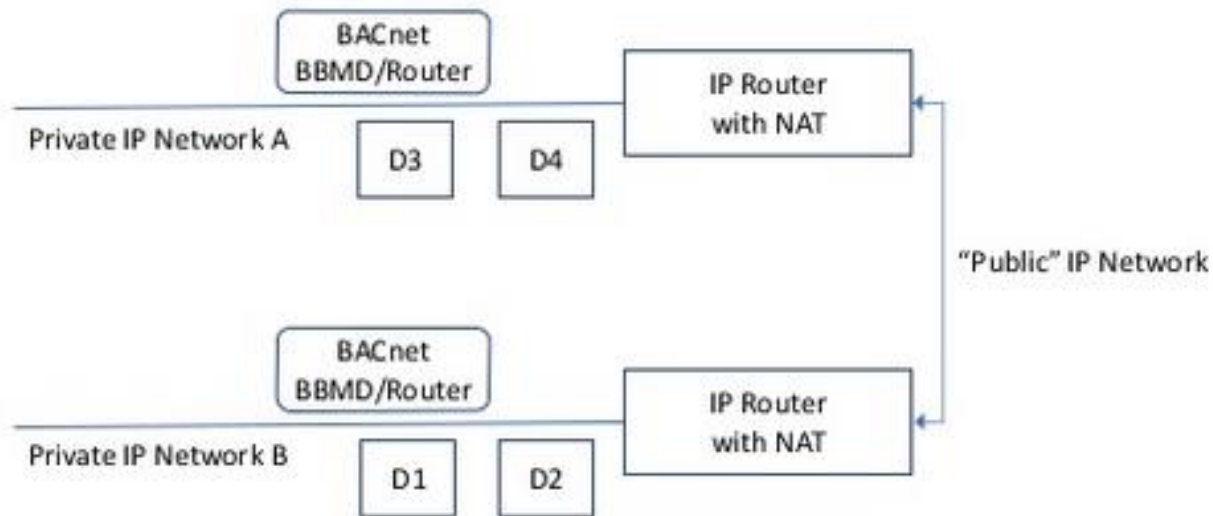


BBMD / Big network





BBMD / Big network





BACnet Secure





BACnet Secure Connect - BACnet/SC



- Secure Version of BACnet/IP
- No security mechanism in BACnet/IP
- Websockets and TLS 1.2
- No UDP Broadcasts and BBMD



BACnet IPv6





BACnet IPv6



IPv6-start-Browser.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000000	fe80::cc21:9026:4024:4a6b	ff0e::bac0	BVLC	72	BACnet Virtual Link Control
2	0.000281	0.000281000	fe80::cc21:9026:4024:4a6b	ff0e::bac0	BACnet-APDU	77	Unconfirmed-REQ who-Is
3	1.004198	1.003917000	fe80::cc21:9026:4024:4a6b	ff0e::bac0	BACnet-APDU	77	Unconfirmed-REQ who-Is
4	2.019785	1.015587000	fe80::cc21:9026:4024:4a6b	ff0e::bac0	BACnet-APDU	77	Unconfirmed-REQ who-Is

- Hard to find samle captures ☹️
- ff0x::bac0
- BACnet Virtual MAC Layer (VMAC)



BACnet BVLC



Field Name	Relation
▼ BVLC · BACnet Virtual Link Control	is present
bvlc.function · Function	==
bvlc.function_ipv6 · Function	!=



Predefined Values

BVLC-Result
Write-Broadcast-Distribution-Table
Read-Broadcast-Distribution-Table
Read-Broadcast-Distribution-Table-Ack
Forwarded-NPDU
Register-Foreign-Device
Read-Foreign-Device-Table
Read-Foreign-Device-Table-Ack
Delete-Foreign-Device-Table-Entry
Distribute-Broadcast-To-Network
Original-Unicast-NPDU
Original-Broadcast-NPDU
Secured-BVLL

IPv4

Predefined Values

BVLC-Result
Original-Unicast-NPDU
Original-Broadcast-NPDU
Address-Resolution
Forwarded-Address-Resolution
Address-Resolution-ACK
Virtual-Address-Resolution
Virtual-Address-Resolution-ACK
Forwarded-NPDU
Register-Foreign-Device
Delete-Foreign-Device-Table-Entry
Secure-BVLL
Distribute-Broadcast-To-Network

IPv6



BACnet BVLC



BVLC Message	Function
Address-Resolution	This message is used to lookup the B/IPv6 address of known VMAC address. This message is sent via multicast
Forwarded-Address-Resolution	This message is used by BBMDs to forward an Address-Resolution message to nodes in its broadcast distribution and foreign device tables. This message is sent via unicast
Address-Resolution-Ack	This message is sent in response to an Address-Resolution message. This message is sent via unicast and is directed to the node which originally sent the Address-Resolution message
Virtual-Address-Resolution	This message is used by B/IPv6 nodes to lookup the virtual address of known B/IPv6 addresses. This message is sent via unicast.
Virtual-Address-Resolution-Ack	This message is sent in response a Virtual-Address-Resolution message. This message is sent via unicast to the node which originally sent the Virtual-Address-Resolution message.



BACnet VMAC



```
> Frame 1: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
> Ethernet II, Src: IntelCor_99:be:57 (ac:7b:a1:99:be:57), Dst: IPv6mcast_ba:c0 (33:33:00:00:ba:c0)
> Internet Protocol Version 6, Src: fe80::cc21:9026:4024:4a6b, Dst: ff0e::bac0
> User Datagram Protocol, Src Port: 58890, Dst Port: 47808
✓ BACnet Virtual Link Control
  Type: BACnet/IPV6 (Annex U) (0x82)
  Function: Address-Resolution (0x03)
  BVLC-Length: 10 of 10 bytes BACnet packet length
  BVLC-Virtual-Source: 4302978 (0x41a882)
  BVLC-Virtual-Destination: 4302978 (0x41a882)
```

- virtual MACs using new IPv6 BACnet Virtual Link Layer (BVLL)



BACnet wrap-up



- Take away:
 - With Wireshark I learned more about BACnet, new Wireshark features itself and real captures helps a lot.

