The following article was published in ASHRAE Journal, November 2008. ©Copyright 2008 American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc. It is presented for educational purposes only. This article may not be copied and/or distributed electronically or in paper form without permission of ASHRAE.

dacnet-	stack-services.	cap - Wireshark				<u>_0×</u>					
File Edit View Go Capture Analyze Statistics Tools Help											
≝ ≝ ≝ ≝ ⊨ 급 % ≇ ≞ ♀ ⇔ ⊚ 7 ½ ■ ⊑ ♀ ♀ 0 7 ½ ■ □ ■ ♀ ♀ 0 7 ½ ■ □ □ ♀ ♀ 0 7 ½ ■ □ □ ♀ ♀ 0 7 ½ ■ □ □ ○ ○ ○ □ ₩ ⊠											
Elber: [bacnet bvlc Expression Gear Apply											
No. +	Time	Source	Destination	Protocol	Info	_					
51	0.004818	192.168.0.5	192.168.0.255	BACNET-APDU	Unconfirmed-Request : 1-Am						
52	0.000199	192.168.0.13	192.168.0.5	BACnet-APDU	Confirmed-Request [invoke:1]: readProperty						
53	0.024796	192.168.0.5	192.168.0.13	BACnet-APDU	ComplexACK [invoke:1]: readProperty						
54	36.195587	192.168.0.13	192.168.0.255	BACnet-APDU	Unconfirmed-Request : unconfirmedCOVNotification						
35	0.030263	AlertonT_00:15:d5	Broadcast	BACNET-APDU	Unconfirmed-Request : unconfirmedCOVNotification						
50	78.891852	192.108.0.13	192.168.0.255	BACRET-APDU	Unconfirmed-Request : who-is						
50	0.040168	Alector 00:15:d5	Broadcast	BACRAT-APDU	Unconfirmed_Request : 1-Am						
59	0.004831	192 168 0 5	192 168 0 255	BACNET-APDU	Unconfirmed_Request : i_Am						
60	0.005001	192,168,0,13	192.168.0.5	BACnet-APDU	Confirmed_Request [invoke:1]: writeProperty						
61	0.024973	192.168.0.5	192.168.0.13	BACnet-APDU	Error [invoke:1]: writeProperty						
62	72.850640	192.168.0.13	192.168.0.255	BACnet-APDU	Unconfirmed-Request : who-Is						
63	0.038858	AlertonT_00:15:d5	Broadcast	BACnet-APDU	Unconfirmed-Request : who-Is						
64	0.039985	AlertonT_00:15:d5	Broadcast	BACnet-APDU	Unconfirmed-Request : 1-Am						
65	0.005020	192.168.0.5	192.168.0.255	BACnet-APDU	Unconfirmed-Request : i-Am						
66	0.023194	192.168.0.13	192.168.0.5	BACnet-APDU	Confirmed-Request [invoke:1]: deviceCommunicationControl						
6/	0.021/66	192.168.0.5	192.168.0.13	BACNET-APDU	SimpleACK [invoke:1]: deviceCommunicationControl						
08	13.9/51/0	192.108.0.13	192.108.0.255	BACHET-APDU	Unconfirmed-Request : who-is	<u> </u>					
<pre>B Frame 66 (70 bytes on wire, 70 bytes captured) E Ethernet II, Src: Asustekc_b0:3c:15 (00:0c:6e:b0:3c:15), Dst: AlertonT_00:15:d5 (00:60:2d:00:15:d5) Internet Protocol, Src: 192.168.0.13 (192.168.0.13), Dst: 192.168.0.5) User Datagram Protocol, Src Port: bacnet (47808), Dst Port: bacnet (47808) B Bachet Virtual Link Control B Building Automation and Control Network NPDU B Building Automation and Control Network APDU 0000 = APDU Type: Confirmed-Request (0) M 0001 = PDU Flags: 0x00 0011 = Size of Maximum ADPU accepted: Up to 480 octets (fits in an ARCNET frame) (3) Invoke ID: 1 Service Choice: deviceCommunicationControl (17)</pre>											
Henable-disable: enable Password: 'filister' 0010 00 38 00 00 40 11 b9 52 c0 a8 00 0d c0 a8 .8.€.€. R 0020 00 05 ba c0 ba c0 00 24 bd 2b 81 0a 00 1c 01 24\$											
0040 6c 69 73 74 65 72											

Figure 1: Wireshark displays a variety of BACnet services from various sources, and is useful for troubleshooting, developing, or learning about the BACnet protocol.



By Steve Karg, Member ASHRAE

Writeshark* (*Figure 1*) is a general purpose network protocol analyzer software application that is cross-platform (runs on various computer operating systems including Linux, Windows, and Mac OS X) and open source (released under the GNU General Public License). Wireshark can be downloaded

for free from www.wireshark.org.

It was created by Gerald Combs and first released to the public in 1998 under the name Ethereal. A typical open source application, Wireshark is the result of thousands of contributions by hundreds of people. Its ability to analyze BACnet and many other protocol packets stems from the efforts of many people contributing enhancements and bug fixes over the years. The Wireshark Web site includes additional documentation and tutorials, a bug tracking tool to aid in product improvement, technical support and training services, and developer information that enables developers to easily contribute to the project.

My first use of Wireshark (at that time

About the Author

Steve Karg is a senior engineer at Watt Stopper/ Legrand in Birmingham, Ala. He has been an active member of ASHRAE SSPC 135 (BACnet) since 2001, and convenes their Lighting Applications working group. He wrote the open source BACnet Stack at SourceForge.net[®], and continues to help maintain the BACnet decoder in Wireshark.

^{*}Wireshark is a registered trademark of Gerald Combs.

the software was known as Ethereal) to handle BACnet decoding happened in 2005 when a customer site hundreds of miles from me was experiencing problems with a controller that stopped responding after connecting it to the BACnet network at the site. The problem occurred intermittently, but usually after several weeks of BACnet network activity. I placed a laptop PC at the site, connected the BACnet network to the laptop PC using an Ethernet hub, and set Ethereal in packet record mode. A couple of weeks later, the maintenance supervisor called me and said that the controller had stopped responding. He stopped the Ethereal packet recording operation, saved the data, and sent me the 400 MB file on a CD-ROM.

My first look at the BACnet data from the customer site using Ethereal left me desiring more detailed information. The BACnet decoding only showed BACnet Confirmed or Unconfirmed APDU messages and raw data, without naming the BACnet service or showing data names or values in the services. Understanding the nature of this open source application, I immediately set to work downloading the Ethereal protocol analyzer source code and the required libraries, reading the developer documentation, and compiling.

In only a few days, I had modified the Ethereal code to display the specific BACnet services, and submitted a patch to the Ethereal developers. The following day another BACnet patch arrived from a developer in Berlin who had reworked an earlier patch submission, which had added the majority of BACnet application decoding. The large capture from the customer site revealed that my controller was receiving bursts of 30 to 50 WriteProperty requests about every 10 seconds. I configured a similar test in my office to simulate the customer site. My controller stopped responding in a few hours, and I was able to debug my application code and correct the firmware.

Additional patches to Ethereal by me and others enhanced the property decoding and fixed a number of subtleties over the following weeks. The BACnet decoding in Wireshark continues to improve and evolve along with the BACnet standard, and today is very good.

Wireshark can monitor and decode most BACnet packets that are received primarily from an Ethernet interface. It can also receive packets from an ARCNET interface. The software is not yet able to directly capture or decode packets from a BACnet PTP (serial) or a BACnet MS/TP (EIA-485) interface. However, BACnet MS/TP can be supported by adding an external interface (*Figure 2*), which sends Ethernet SNAP protocol packets. Wireshark does not yet support BACnet Segmentation. These features will probably be added someday because someone will eventually be motivated to add the missing functionality to this highly regarded open source tool.

Wireshark can import and export packet files in a variety of network analyzer formats. The libpcap file format is the software's default file format.

Using Wireshark for Live Captures

To monitor or record BACnet traffic, you must be able to "see" the network traffic from the computer running the protocol

ame!	trics_mstp.pcap -	Wireshark				<u>. 0 ×</u>
Ele B	ar Yen go Si	spture Analyze Statistics Ico	e Reb			
			144037		. Q, Q, 🖸 👹 🕅 🧏 🐝 📓	
Elter:			* Express	ion Gear Ap	ply	
No. +	Tine	Source	Destination	Protocol	Info	-
0 6	46 0.025782	00:00:00_00:00:01	00:00:00_00:00:63	BACNET	BAChet MS/TP Token	
6	48 0.020996	00:00:00_00:00:03	00:00:00_00:00:00:03	BACnet BACnet-A	BACNET MS/TP Token A Confirmed-Request [invoke:126]: readProp	erty
6	49 0.219978	00:00:00_00:00:63	00:00:00_00:00:01	BACnet-	A ComplexACK [invoke:126]: readProperty	
6	51 0.025002	00:00:00_00:00:01	00:00:00_00:00:63	BAChet	BAChet MS/TP Token	
6	52 0.007997	00:00:00_00:00:63	00:00:00_00:00:01	BACnet	BACNET MS/TP Token	
6	53 0.006997 54 0.025000	00:00:00_00:00:00	00:00:00_00:00:4c	BACnet	BACNET MS/TP Poil For Master Bacnet MS/TP Token	
6	55 0.007998	00:00:00_00:00:63	00:00:00_00:00:01	BACnet	BACNET MS/TP Token	
6	56 0.007000	00:00:00_00:00:01	00:00:00_00:00:4d	BACnet	BACNET MS/TP Poll For Master	2
4						<u> </u>
E Fra	me 648 (55 b)	ytes on wire, 55 bytes	captured)			
+ IEE	E 802.3 Ether	rnet				
= LOG	ICAI-LINK CO	ntrol				
	sar: shar (u	(dua)				
	CAP: SNAP (0)	(1008) (223)				
	R Rit: Comman	nd				
E C	ontrol field	: U. func=UI (0x03)				
0	roanization (code: Cimetrics (0x00)	090)			
P	10: U+4 MS/TR	P (0x0001)				
B BAC	net MS/TP, Si	rc (1), Dst (99), BACr	et Data Expecting Rep	ly		
D	elta Time: 5					
8	-bit value: 1	128				
F	rame Type: BA	ACnet Data Expecting A	eply (5)			
D	estination A	ddress: 99				
5	ource Address	5;1				
L	ength: 5632					
H	eader CRC: 0:	xa4				
D	ata CRC: 0x18	bSf				
E Bui	Iding Automat	tion and Control Netwo	rk NPDU			
V	ersion: 0x01	(ASHRAE 135-1995)				
. € 0	ontrol: 0x0c	ennen an se				
S	ource Network	k Address: 1				
S	ource MAC Lay	yer Address Length: 6				
S	ADR: 38:98:11	f:07:ba:c0 (a8:98:1f:0	(7:ba:c0)			
BUI	Iding Automat	tion and control Netwo	PK APDU			
	000 = A	PUU Type: Confirmed-ke	quest (u)			
	0010 = P	UU Flags: UXU2	contade unconclified	(0)		
	0101 - 5	the of Maximum ADDII and	coepced. Units 1476 or	tote (fite	in an 160 8902-2 frame) (5)	
T	nyoke to: 12	6	celetar of to Ture of	rees fries.		
	ervice choice	e: readproperty (12)				
	biectIdentif	ier: device object, 22				
EP	roperty Ident	tifier: object-list ()	6)			
	00 00 00 00	00 00 00 00 00 00	01 00 29 33 33			_
0010	03 00 10 90	00 01 05 00 80 05 63	01 00 16 a4 01			
0020	OC 00 01 06	a8 98 1f 07 ba c0 02	05 7e 0c 0c 02			
0030	00 00 16 19	40 37 10	•••			
O PED /	r cinatrics nich 2 h	uter	Parketo 1915 Nimbu	at 1915 Madada	0 Devilie: Defait	
C multi	errenenies (per), 20	Pres .	Papers: 1115 Dobley	on 1315 Lighter	a lainte nei ang	

Figure 2: Wireshark and a BACnet MS/TP capture from an external interface, which sends Ethernet SNAP protocol packets.

analyzer. This usually requires connecting the computer and BACnet devices to an Ethernet hub, as unicast traffic between devices may not be seen on all ports of an Ethernet switch (bridge). Ethernet switches may be used if they have the ability to span, monitor, or mirror all port traffic and send it to a single port. The computer network interface must also support promiscuous mode, where the interface supplies the protocol analyzer with all the network packets it sees.

Selecting the network interface to monitor or capture is accomplished through the Capture menu options, under Interfaces or Options. The Capture Options dialog (*Figure 3*) offers the selection of a capture interface, optional display of packets in real time or automatic scrolling, MAC, network, or transport name resolution, and the ability to save a file or multiple files while capturing. The Options dialog also provides the ability to limit the capture by providing "Stop Capture" options after a number of packets, megabytes, or minutes.

Wireshark supports capture and display filtering, and the syntax for a capture filter and a display filter is different. A capture filter limits the packets captured to a couple of specific header fields. The capture filter expressions can include a specific protocol (ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp, udp), a direction (src, dest, src and dest, src or dest), and logical operations (nor, and, or). These filter expressions can be used on a BACnet/ IP network to filter out any non-BACnet/ IP traffic. A common capture filter to only capture standard BACnet/IP packets would be "udp port 47808".

Before we start our capture, we should consider our Display Options. Wireshark can display the packets in real-time and can automatically scroll the packets while they are being received, which is fun to watch, but not as useful when trying to see specific packets. The latest builds of the software enables automatic scrolling during a capture by selecting the last packet on the display. The software also permits hiding of the Capture Info dialog box that summarizes the count and type of packets captured.

Another option to consider is Capture File(s). Although Wireshark can save a capture or portions of a capture after it is displayed, sometimes it is necessary to capture over a longer period of time.

Wireshark has the ability to capture to a file or even multiple files. The software automatically appends unique identifiers to files when multiple files are used. The file or files can be limited to size, time or number of files, or can save indefinitely, only limited to the amount of disk space available. When I am capturing for days, weeks, or months, I normally disable the Display Option for "Update list of packets in real time" to limit the amount of display memory used.

Selecting "Start" from Capture Options begins the capture. Selecting "Stop" from the "Capture" menu stops the capture. The capture can be saved to a file or discarded.

Display Filtering

A common BACnet configuration issue that I have seen during the commissioning of a BACnet network is due to some device or workstation writing to a Present_Value property of an object at a higher priority than it should. This usually makes an output point unresponsive to other network applications. Finding the writer of the high priority usually involves some forethought at the end-device, or just some monitoring with Wireshark. Sifting through many hours or days of data packets is made easier by using the display filtering that is built into the software.

The display filter (*Figure 4*) allows for protocol specific filtering, during the live capture, after the capture has been stopped, or after opening a capture file in the display. It can be built using the Wireshark Filter Expression wizard, by typing specific values into the filter box, or by using the context menu. Each protocol decoder has its own expression words. The BACnet decoders are currently defined as BVLC (BACnet Virtual Link



Figure 3: Wireshark Capture Options dialog box allows control of the capture display, name resolution, capture files, capture interface, capture filter, and the ability to stop after so many packets, bytes, or time.

Control or BACnet/IP specific decoding), BACnet (BACnet NPDU or network layer decoding), and BACapp (BACnet APDU or application layer decoding). A common display filter to view all BACnet messages containing an NPDU would be "bacnet." A display filter to view only BACnet WriteProperty service packets would be "bacapp.confirmed_service == 15," where 15 is the service choice for the WriteProperty service of a BACnet APDU Confirmed Request.

Many, but not all, of the decoded variables are available for use in a display filter. The name of the variable can be found by first selecting the line of the variable decoding, and seeing the text, such as "bacapp.confirmed_service," shown in parenthesis in the lower left corner status box of the Wireshark window. Display filters (*Table 1*) can be applied to a data capture by using the "Apply as Filter" context menu in Wireshark. The context menu can be activated by selecting a particular packet or data element of a packet, and using the context button on the mouse (e.g., the right button on a Windows mouse).

The packets displayed using a display filter can also be saved as a separate file using "Save-As" from the "File" menu. This is useful when working with large capture files.

Some BACnet installations use BACnet/IP with a UDP port other than 47808 (0xBAC0). The Wireshark context menu allows for decoding BACnet messages on other UDP ports using the "Decode As..." option (*Figure 5*) and selecting BVLC.

The default Wireshark time display format is seconds since the beginning of the capture. Other useful formats include seconds since the previous packet, and time of day. Being able to change the reference or start time for the time display is useful when checking for bandwidth issues. I monitored a college campus Ethernet network port using a hub connected to a BACnet router, which also connected to a 156K ARCNET segment. I found, using the software, that the campus network was producing thousands of BACnet UnconfirmedCOV (change of value) broadcast packets per minute, and this was saturating the 156K ARCNET segment and causing slow response and retransmits from the devices on the ARC-NET segment. Adjusting the offending objects COV_Increment property around the campus eliminated the issue.

Developing BACnet Products

Wireshark is well known for being used in software and communications protocol development, and its use during BACnet software development is no exception. Timing information, the raw bytes on the wire, and the decoded meaning of the bytes on the wire provide immediate feedback to a BACnet developer. The Wireshark source code may also provide deeper insight into how particular packets or properties may be formed and decoded.

Wireshark, accompanied by a BACnet testing tool, is a common setup for testing and validating a BACnet device. The software can provide the evidence (a capture) from a testing session, which can be used by the BACnet developer to find and fix a problem discovered during testing.

Wireshark From the Command Line

Wireshark can also be used from the command line (Command Prompt under Windows; shell or console under Linux

Ele Edit View Go Capture Analyze Statistics Tools Help Elter: bacapp.confirmed_service == 15 ▼ Expression... Clear Apply No. - Time Source Destination Protocol Info 55 0.03026 AlertonT_00:15:d5 Broadcast BACnet-A Unconfirmed-Request : unconfirmedCOVNotification 56 78.89185 192.168.0.13 192.168.0.255 BACnet-A Unconfirmed-Request AlertonT_00:15:d5 AlertonT_00:15:d5 BACnet-A Unconfirmed-Request : who-BACnet-A Unconfirmed-Request : i-Am 57 0.061611 Broadcast who-Is 58 0.040168 Broadcast BACnet-A Unconfirmed-Request 59 0.004831 192,168.0.5 192,168,0,255 1-Am 61 0.024973 62 72.850640 192.168.0. 192,168,0,13 BACnet-A Error [invoke:1]: writePro 192.168.0.13 firmed-Request 192,168,0,255 BACnet-A Lincon Broadcast 63 0.038858 64 0.039985 AlertonT_00:15:d5 AlertonT_00:15:d5 BACnet-A Unconfirmed-Request : i-Am Broadcast BACnet-A Unconfirmed-Request : i-Am BACnet-A Confirmed-Request [invoke:1]: deviceCommunicationControl BACnet-A SimpleACK [invoke:1]: deviceCommunicationControl 92.168.0.5 192.168.0. 66 0.023194 192,168,0,13 192,168.0.5 192.168.0.13 BACnet-A Unconfirmed-Request : who-Is BACnet-A Unconfirmed-Request : who-Is 68 13.975170 192.168.0.13 192,168,0,255 AlertonT_00:15:d5 AlertonT_00:15:d5 69 0.03180 Broadcast BACnet-A Unconfirmed-Request : i-Am 70 0.040143 Broadcast 71 0.004860 BACnet-A Unconfirmed-Request : 192.168.0.5 192.168.0.255 1-Am ■ Frame 60 (67 bytes on wire, 67 bytes captured) Ethernet II, Src: Asustekc_b0:3c:15 (00:0c:6e:b0:3c:15), Dst: AlertonT_00:15:d5 (00:60:2d:00:15:d5) Internet Protocol, Src: 192.168.0.13 (192.168.0.13), Dst: 192.168.0.5 (192.168.0.5) E User Datagram Protecol Sec Dort . hace * (47808), Dst Port: bacnet (47808) Expand Subtrees BACnet Virtual Link Expand All Type: BACnet/IP (Collapse All Function: Origina BVLC-Length: 4 of ength Apply as Filter Building Automation Prepare a Filte Selected version: 0x01 (AS Colorize with Filte Not Selected ■ Control: 0x24 ... and Selected Destination Netwo ... gr Selected Follow UDP Stream Destination MAC L ... and not Sele DADR: 61 . or not Selec Copy Hop Count: 255 Export Selected Packet Bytes Building Automation 0000 = APDU 🥑 Wiki Protocol Page (0) E 0000 = PDU F Filter Field Reference ed Request 0... = Sec0.. = Mor nts Follow 0. = SA: 2 Decode As... ccepted : Unspecified (0) .000 = Max R Disable Protocol. 0011 = size Up to 480 octets (fits in an ARCNET frame) (3) Resolve Name Invoke ID: 1 B ObjectIdentifier: analog-output object, 0 ■ Dronarty Identifier . nrecent_value (85) O0 O0 O1 O1 O1 O2 O2 O3 O3 O3 O3 O3 O3 O4 O1 D5 C1 O3 O3 O4 O1 D5 S2 C1 O3 O4 O4 O1 D5 S2 C1 O3 O4 O4 O1 D5 S2 C1 O3 O4 O4 O4 O4 D5 C1 A3 O4 O4 D4 D5 C1 A3 D6 D4 O4 D4 D5 S2 C1 D6 D4 D4 D4 D4 D4 D5 D3 D0 D4 <thD4</th> D4 D4 D4</ . 0010 .5..6.6. .U.... 0020 0030 0040!

Figure 4: Wireshark default display, showing the ability to prepare or apply a display filter.

or Unix). The first tshark command line option that I normally use is "-D", which provides me an enumerated list of interfaces that I can use for capturing. Then I use the "-i 2" or whichever interface number I want to capture from as the command line option to tshark. The "-w filename.cap" command line option is useful when I want to capture to a file, but don't necessarily want to launch the Wireshark GUI. The amount of disk space or number of files stored during a capture can be controlled using the "-b" command line option followed by duration, file size, or number of files options. More details about the specific options can be found by asking tshark for help using the "--help" command line option. Other command line tools are shipped with Wireshark including:

• dumpcap—captures network traffic but does not display the network traffic;

Profile: Default

- capinfos—reads a saved capture file and displays statistics about that file;
- editcap—edit and translate the format of a capture file;
- mergecap—merges multiple capture files into one file;
- text2pcap—generates a capture file from an ASCII hexadecimal dump of packets; and
- rawshark—a tool for displaying packets and specified fields from a capture file.

Service Choice (bacapp.confirmed_service), 1 b... Packets: 113 Displayed: 113 Marked: 0

bacnet-stack-services.cap - Wireshark

- 0 ×

Free to Download, Use, and Share

It is not always convenient for me to travel to a site that is experiencing BACnet-related network problems so that I can analyze and solve the problem. I was asked to help diagnose an installation where two BACnet vendors were unable to communicate using BACnet/IP. I asked for a Wireshark capture of the communication attempts. They did not have Wireshark installed on their laptop computers, so they went to the Wireshark Web site to download the free tool. I guided them through the capture process after successful installation of the tool, and they emailed me the results. They also shared Wireshark with the local site technicians who would be able to perform Wireshark network analysis and send us the captures.

I pondered the WhoIs and I-Am requests from the capture for a clue into the problem, but both requests appeared to be well formed. Although both devices were using the standard BACnet/ IP port number 47808, I did notice that each was using a different IP broadcast address. Further investigation revealed that the site was using an unusual IP subnet mask for their control systems on the network: 255.255.254.0. The BACnet device using an older GNU/ Linux operating system was unable to form the correct IP broadcast address by using just the IP subnet mask. The vendor changed the network configuration script in their device to calculate and set the broadcast address directly. The local technicians installed the patch, performed some Wireshark network analysis, and sent us the captures that showed that the broadcast problem was solved.

Summary

Wireshark is software that understands the detailed structure of many different networking protocols, including BACnet. The software is able to capture, display, and save the various BACnet messages, services, attributes, and properties along with their meanings. It has powerful display filters that can be used to selectively

Capture Filters		
udp port 47808	BACnet/IP packets on UDP port 47808	
udp port 47808 or udp port 47809	BACnet/IP packets on UDP port 47808 or 47809	
Display Filters		
bvlc bacnet bacapp	BACnet packets	
bacnet	BACnet NPDU packets	
bacnet.mesgtyp	BACnet Network Layer (router) packets	
bvlc	BACnet/IP packets	
bvlc.function == 0x0b	BACnet/IP Broadcast packets	
bacapp	BACnet APDU packets	
bacapp.confirmed_service == 12	BACnet ReadProperty packets	
bacapp.confirmed_service == 15	BACnet WriteProperty packets	
bacapp.unconfirmed_service == 0	BACnet I-Am packets	
bacapp.unconfirmed_service == 8	BACnet WhoIs packets	
<pre>bacapp.unconfirmed_service == 2</pre>	BACnet UnconfirmedCOVNotifica- tion packets	

Table 1:A list of commonly used Wireshark filters for BACnet. Display filter expressions can be combined using logical operators such as "and", "or", "xor", and "not". A display filter expression can use a variety of comparison operators such as "==","!=",">","<"," =",","<"," =","," = ",



Figure 5: Wireshark "Decode As" dialog showing BACnet/IP port 47809 decoded as BVLC.

highlight and color packet information. The software runs on most computer platforms, whether graphical or command line. It can import and export a variety of network analyzer file formats. Best of all, Wireshark is free!