

如何使用 wireshark 觀察 BACnet/IP 通訊封包

元米科技 2017/4/17





本文的對象是針對應用 BACnet/IP 通訊, 但不熟悉 BACnet/IP 協定與 Wireshark 操作的工程人員。說明如何利用免費的網路封包軟體 Wireshark, 判讀 BACnet/IP 的封包, 進而幫助專案異常排除, 同時學會系統整合責任釐清的利器。

文中將依序說明 如何安裝 Wireshark, 並以 ICDT BACnet Pioneer 免費軟體連接 另一台安裝 ICDT BACnet Pioneer 電腦為例, 展示 Wireshark 的分析結果。

由於 Wireshark 只能分析電腦網卡收到的訊息, 因此 Wireshark 軟體必須與 CDT BACnet Pioneer 安裝在同一台電腦。

關於 wireshark

#基百科:Wireshark(前稱Ethereal)是一個免費開源的網路封包分析 軟體。網路封包分析軟體的功能是截取網路封包. 並盡可能顯示 出最為詳細的網路封包資料。 在過去,網路封包分析軟體是非常昂貴,或是專門屬於營利用的 軟體. Wireshark的出現改變了這一切。在GNU通用公眾授權條款的 保障範圍底下,使用者可以以免費的代價取得軟體與其程式碼。 並擁有針對其原始碼修改及客製化的權利。Wireshark是目前全世 界最廣泛的網路封包分析軟體之一。

安裝 Wireshark

至 Wireshark 官網依照電腦版本下載最新版的 Wireshark 後進行安裝, 安裝時連同相關的程式一起安裝。

Wireshark 下載處:

tml

https://www.wireshark.org/download.h



NEWS Get Acquainted ▼ Get Help ▼

Cancel

Download Wireshark

The current stable release of Wireshark is 2.2.6. It supersedes all previous releases.

Stable Release (2.2.6)	^
 Windows Installer (64-bit) Windows Installer (32-bit) Windows PortableApps[®] (32-bit) macOS 10.6 and later Intel 64-bit .dmg Source Code 	
Old Stable Release (2.0.12)	^
Documentation	

shark 2.2.6 (64-bit) Se	tup	Wireshark 2.2.6 (64-bit) Se	etup	X	📕 Wireshark 2.2.6 (64-bit) Setup	
se Components se which features of Wire	shark 2.2.6 (64-bit) you want to install.	Select Additional Tasks Which additional tasks should b	be done?	4	Install WinPcap? WinPcap is required to capture live network data. Sho	ould WinPcap be installed?
ollowing components are	available for installation.	Create Shortcuts	tem 1	Tr.	Currently installed WinPcap version WinPcap 4.1.3	
t components to install:		Virteshark Legacy Start Virteshark Legacy Start Wreshark Legacy Deakt Virteshark Legacy Quekt Virteshark Legacy Quekt File Extensions @ Associate trace file exten	i Icon Wenu Item top Icon c Launch Icon ensions to Wireshark ensions to Wireshark Lenary		Install WinPcap 4.1.3 Vinstall WinPcap 4.1.3 If selected, the currently installed WinPcap 4.1	1.3 will be uninstalled first.
e required: 171.0MB	Description Position your mouse over a component to see its description.	○ None Extensions: Svw, acp, apc, pcapra, pklg, pkt, rf5, snor	, atc, bfr, cap, enc, erf, fdc, ipfix, mplog, out, p op, syc, tpc, tr1, trace, trc, vwr, wpc, wpz	cap,	What is WinPcap?	
rk Installer (tm) ———	< Back Next > Car	wireshark Installer (tm)	<back next=""></back>	Cancel	Wireshark Installer (tm)	Back Next >

安裝 ICDT BACnet pioneer 免費軟體

自 <u>元米科技</u>下載 最新版 <u>ICDT BACnet pioneer</u> 免費軟體

安裝在與 Wireshark 相同的電腦中,如果已安裝較舊的版本,必須先移除後安裝。如果手上沒有其他 BACnet/IP 的設備,則必須有另一台電腦安裝 ICDT BACnet pioneer





執行 Wireshark

執行 wireshark 後在正確的網路 卡上點兩下,以進行記錄。

由於電腦本身可能有乙太網路、 無線網路或者多個虛擬網路,請 選擇與其他 BACnet 設備連接的 網路介面,範例中為"區域網路" 也就是乙太網路。如圖看到 區域 網路 右邊資料量的曲線,表示該 網路是目前主要運作的網路。

Welcome to Wireshark

Open

C:\Users\Eric\AppData\Loca\Microsoft\Windows\Temporary.Internet Files\OLKF47C\CDT BACnetIP-new.pcapng (not found)
C:\Users\Eric\AppData\Loca\Microsoft\Windows\Temporary.Internet Files\OLKF47C\stop at AV20 reading (2).pcapng (not found)
C:\Users\Eric\AppData\Loca\Microsoft\Windows\Temporary.Internet Files\OLKF47C\stop at AV20 reading (2).pcapng (not found)
C:\Users\Eric\AppData\Loca\Microsoft\Windows\Temporary.Internet Files\OLKF47C\stop at AV20 reading pcapng (not found)
C:\Users\Eric\AppData\Loca\Microsoft\Windows\Temporary.Internet Files\OLKF47C\cOV abies stat.pcapng (not found)
C:\Users\Eric\Desktop\bacnet cov.pcapng (11 K8)
C:\Users\Eric\Desktop\bacnet cov.pcapng (not found)
C:\Users\Eric\AppData\Loca\Microsoft\Windows\Temporary.Internet Files\OLKF47C\poptagng (not found)
C:\Users\Eric\AppData\Loca\Microsoft\Windows\Temporary.Internet Files\OLKF47C\PES20160506\pcapng (not found)

Capture

Wireshark 記錄中

如果電腦對外有網路通訊 , wireshark 就開始記錄通訊封包。 按下左上的紅色停止鍵會停止記錄 , 再按下旁邊的綠色鯊魚鰭會詢問 儲存或放棄記錄, 如果不儲存, 則先 前的記錄將會被放棄。

Capturing from 區域連續	線					
File Edit View Go	Capture Analyze Statisti	cs Telephony Wireless To	ols Help			
🖌 🔳 🦽 💿 💷 🛅 🗎						
Annly a display filter of					Evonession	-
No Time	Source	Destination	Protocol Length	Info		
- 1.0.000000	fo8059c1.404.9a	102: ff02::c	SSDP	208 M-SEARCH * HT	TP/1 1	
2 0 108789	192 168 1 9	203 205 149 188	0100	89 OTCO Protocol		E
3 0 117097	172 217 18 131	192 168 1 9	OUTC	72 Pavload (Encr	voted) PKN: 5	
4 0 311688	203 205 149 188	192 168 1 9	0100	89 OICO Protocol	jpcca), half 5	
5 0 504606	192 168 1 9	31 13 95 36	TI Sv1	130 Application D	lata	
6 0.504921	192.168.1.9	31,13,95,36	TLSv1	100 Application D	lata	
7 0.504972	192,168,1,9	31, 13, 95, 36	TI Sv1	913 Application D	lata	
8 0.572742	31,13,95,36	192.168.1.9	TCP	60 443 → 50841 [ACK] Seg=1 Ack=77 Win=2043 Len=0	
9 0.572744	31.13.95.36	192.168.1.9	TCP	60 443 → 50841 [.	ACK] Seg=1 Ack=123 Win=2043 Len=0	
10 0.572745	31.13.95.36	192.168.1.9	TCP	60 443 → 50841 [ACK] Seg=1 Ack=982 Win=2040 Len=0	
11 0.572746	31.13.95.36	192.168.1.9	TLSv1	96 Application D	lata	
12 0.572748	31.13.95.36	192.168.1.9	TLSv1	100 Application D	lata	
13 0.572896	192.168.1.9	31.13.95.36	TCP	54 50841 → 443 [ACK] Seq=982 Ack=89 Win=993 Len=0	
14 0.717180	31.13.95.36	192.168.1.9	TLSv1	360 Application D	lata	
15 0 717317	192 168 1 9	31 13 95 36	тср	51 50811 - 113 F	ACK1 Son=987 Ack=395 Win=997 Lon=0	-
> Frame 1: 208 byt	es on wire (1664 bits	s), 208 bytes captured	(1664 bits) on ir	nterface 0		
Ethernet II, Src	:: HewlettP_47:08:55 ((64:51:06:47:08:55), Ds	t: IPv6mcast_0c ((33:33:00:00:00:0c)		
Internet Protoco	ol Version 6, Src: feb	80::59c1:404:9ae2:341a,	Dst: ++02::c			
Diser Datagram Pr	otocol, Src Port: 654	476, Dst Port: 1900				
Simple Service D	Discovery Protocol					
	▲ *臣诚谦绝					
			* 1 1 1 1 1 1	· 1 · 1 · 1		
	File Edit View Go C	apture Analyze Statistics	Telephony Wireless	Tools Help		
	🚺 🗏 🖉 🔍 🔛 🔀	। 🖸 🤇 🗢 🗢 🗟 १ 👲 :	<u> </u>	2		
	Apply a display filter … «Ctrl	-/>				🖃 🕶 Ex
0000 33 33 00 00	No. Time	Source	Destination	Protocol Length	Info	
0010 00 00 00 9a	1 0.000000	fe80::59c1:404:9ae2:	ff02::c	SSDP	208 M-SEARCH * HTTP/1.1	
0020 04 04 9a e2	2 0.108789	192.168.1.9	203.205.149.188	3 OICQ	89 OICQ Protocol	
0030 00 00 00 00	3 0.117097	172.217.18.131	192.168.1.9	QUIC	72 Payload (Encrypted), PKN: 5	
0040 55 45 41 52	4 0.311688	203.205.149.188	192.168.1.9	0100	89 OICQ Protocol	
◎ Z 區域連線: Live c	5 0.504606	192.168.1.9	31.13.95.36	TLSV1	130 Application Data	
	6 0.504921	192.168.1.9	31.13.95.36	TLSV1	100 Application Data	
	/ 0.5049/2	192.168.1.9	31.13.95.30	TLSVI	913 Application Data	1
	8 0.572742	31.13.95.36	192.168.1.9	TCP	60 443 → 50841 [ACK] Seq=1 ACK=// W1N=2043	Len=0
	9 0.5/2/44	31.13.95.36	192.168.1.9	TCP	60 443 → 50841 [ACK] Seq=1 ACK=123 W1n=204:	3 Len=0
	10 0.572745	31.13.95.36	192.168.1.9	TCP	60 443 + 50841 [ACK] Seq=1 ACK=982 W1n=2044	J Len=0
	12 0 572740	J1 12 Unsaved pack	ets			
	13 0 572896	192 16		1 1 1 1 1 1 1 1	4/3 [ACK] Seg=982 Ack=89 Win=993	3 Lon=0
	14 0 717180	31 13 Do you	want to save the captur	ed packets before starting	a new capture? [445 [ACK] SEq-562 ACK-65 WIII-55.	5 Len-0
	15 0 717317	192 16 Your ca	ptured packets will be lo	ost if you don't save them.	1/13 [ACK] Seg=982 Ack=395 Win=99	92 Lon=0
	< [
	> Frame 1: 208 bytes	s on wire	Save	Continue without Saving	Cancel	
	Ethernet II, Src:	HewlettP			00:0c)	
	Internet Protocol	Version 6, Src: fe80::	59c1:404:9ae2:34	La, Dst: ff02::c		
	User Datagram Prot	tocol, Src Port: 65476,	Dst Port: 1900			
	Simple Service Dis	scovery Protocol				
	0000 33 33 00 00 0	0 0c 64 51 06 47 08 5	5 86 dd 60 00 3	3dQ .G.U`.		
	0010 00 00 00 9a 1	1 01 fe 80 00 00 00 0	0 00 00 59 c1 .	······································		
	0020 04 04 9a e2 3	4 10 tt 02 00 00 00 0	a 2a fd 4d 2d	1 * M		
	50 00 00 00 0	2 40 20 2 20 40 54 5	1 50 05 04 0 0	CADCU & UTTD/4		

ICDT BACnet pioneer 的網路設定

點選 齒輪狀的 Setup 鍵, 開啟設定視窗 , 將網路介面 Interface 選擇 BACnet 連 接的網路介面。這點非常重要, 因為 BACnet 的廣播必須從正確的網路發出 , 否則是無法正常通訊的。

下方的 UDP Port 選擇 BACnet/IP 的 UDP 編號,預設為 47808。而 Device Instance 編號則不可以與其他 BACnet 設備重複,因此兩台電腦不能相同。本 例中裝有 wireshark 電腦為預設 4194302,另一台設為 1000



執行 ICDT BACnet pioneer 以掃描設備

點選放大鏡的 who is 鍵. 旁邊選單會 出現本身的 4194302 以及另一個 BACnet pioneer 的 1000, 選取 1000 會對該設備(Device)進行物件(Object) 的掃描. 結束後點選 DEVICE 的 1000 處,則會掃描並顯示 DEVICE-1000 物 件的所有屬性(Property)。其餘操作說 明可點選 "About" 的 "幫助" 以開啟線 上手冊



Wireshark 記錄 BACnet/IP 封包

按下 wireshark 綠色鯊魚鰭進行記錄, 並按下 BACnet pioneer Who is 旁的 Read All 三角形, 以讀取全部 Device 1000 的全部物件屬性, 這個動作需要較長時間, 此

時可以看到 wireshark 記錄了 BACnet 通訊封包, 同時夾雜了其 他網路資訊。

此時在左上記錄與停止鍵下欄位輸入 bacnet, 可以將不是 bacnet 的封包濾除。

💋 Capturing from 區域連線			X)		
File Edit View Go Capture Analyze	Statistics Telephony Wireless Tools	Help			_ _ ×	•
🖉 📕 🧟 🛞 🕼 🖻 🗙 📴 🍳 👄 🖷	ICDT BAChet Pioneer					,
Apply a display filter … <ctrl-></ctrl->	📕 Who is 🔹 🔹 🙀	s 🖩 🌵 🔆 😶				
No. Time Source	P 1000 + 0 🐳	~ 4194302 🚑				
- 10.000000 192.168.1.9	• Event State : Normal					1
2 0.000133 192.168.1.9	• Object Identifier : ANALOG ¥	ALUE 1				
3 0.000204 192.168.1.9	• Object Name : AV1					
4 0.022084 31.13.87.36	Ottject Type : Analog value Out Of Service : False					
E 0 011006 21 12 07 26	• Present Value : 0					
Frame 1: 130 bytes on wire (10)	 Status Flags : In Alarm=False, 	Fault=False, Overridden=False, (Out Of Service=False,			
Ethernet II, Src: HewlettP_47	Units : No Units	🥂 *區域連線				
Internet Protocol Version 4, 1	Description :	File Edit View Go	Capture Analyze St	atistics Telephony Wi	reless Tools	Help
Transmission Control Protocol	• Event State : Normal				0.55	neip
Secure Sockets Layer	Object Identifier : ANALOG Object Name : AW2			१ 👲 🖃 🗏 🔍 🔍	. e. ±	
	- • Object Type : Analog Value	bacnet				
	• Out Of Service : False	No. Time	Source	Destination	Protocol L	ength Info
		L 18 1.134516	192.168.1.9	192.168.1.102	BACne	59 Conf
	- O Units : No Units	19 1.138341	192.168.1.102	192.168.1.9	BACne	60 Erro
	e- • 3	20 1.323511	192.168.1.9	192.168.1.102	BACne	59 Conf
	• Description :	21 1.324940	192.168.1.102	192.168.1.9	BACne	60 Erro
	Object Identifier : ANALOG	22 1.443521	192.168.1.9	192.168.1.102	BACne	216 Conf
	• Object Name : AV3	23 1.452546	192.168.1.102	192.168.1.9	BACne	315 Comp
	• Object Type : Analog Value	24 1.528826	192.168.1.9	192.168.1.102	BACne	59 Conf
	Out Of Service : Palse Present Value : 0	25 1.529794	192.168.1.102	192.168.1.9	BACne	62 Comp
	• Status Flags : In Alarm=False,	26 1.615671	192.168.1.9	192.168.1.102	BACne	61 Conf
9000 9c db 43 c9 23 b4 64 51	Units : No Units	27 1,616549	192.168.1.102	192.168.1.9	BACne	60 Erro
0010 00 74 05 07 40 00 80 06 0020 57 24 d8 es 01 bb 76 36	Description :	28 1,633438	192,168,1,9	192,168,1,102	BACne	59 Conf
0030 3f 60 38 49 00 00 17 03	- • Event State : Normal	29 1,634930	192,168,1,102	192,168,1,9	BACne	65 Comp
0040 00 00 4d 94 c5 96 15 75	· · · · · · · · · · · · · · · · · · ·	30 1, 714530	192.168.1.9	192.168.1.102	BACne	59 Conf
◎ 🍸 區域連線: «live capture in progress»	ANALOG VALUE-4 Present Value : 0	31 1,715391	192.168.1.102	192.168.1.9	BACne	60 Erro
		54 4.713371	192.100.1.102	192.100.1.9	Drieffem	55 LI I 0

如果不是 47808 port

BACnet/IP不一定得採用 47808 port, 此時輸入 bacnet 並不適用。以 47809 port 為例, 可以試著輸入 udp.port==47809, 再按右鍵選擇 Decode As ,如圖選擇 BVLC

後即可看到

(BACnet Virtual Link Control)

**Ext### ** ** * <th< th=""><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></th<>													
"#Edd# Upper - 47809 Capture Analyze Statistics Telephony Wireless Tool Boot P/DP/DP Image: Source Destination Protocol Protocol Boot P/DP/DP							Wireshark · Deco	ode As		Transaction of		hant longh its	8 2
ie Edit View Go Capture Analyze Statistics Telephony Wireless Toc Immu Value type Default Cumert immu Value type Default Cumert Record	*	區域連線					Gald		Malua	Tune	Default	Comment	
Image: Source Destination Protect Prot	ile	Edit View Go	Capture	Analyze Statistics Telephon	y Wireless Toc		Field		value	Type	Delault	Current	
Import Source Destination Protocol 18 1.075193 192.1 And Acce + 402.1 Import 19 1.076055 192.11 Mark/Umark/Packet Ctrl+M 21 1.575054 192.11 Mark/Umark/Packet Ctrl+D 23 1.576242 192.11 Set/Unset Time Reference Ctrl+T 24 1.635092 192.11 Packet Comment Ctrl+Aht+C 26 1.706771 192.11 Packet Comment Ctrl+Aht+C 28 1.815615 192.11 Apply as Filter Prepare a Filter Prepare a Filter 21 1.326044 192.11 Apply as Filter Prepare a Filter Prepare 3 11 18.26044 192.168 1.02 BACne	1	= 1 @ 🗎 🏊			θ Θ Β Π		UDP port	•	4/809	 Integer, base 1 	.0 (none)	(none)	
Image point Source Destination Protocol 18 1.075103 192.1 Mark/Umark Packet Ctrl+M 19 1.076655 192.1 Ignore/Unignore Packet Ctrl+M 23 1.575054 192.1 Set/Unset Time Reference Ctrl+Shift+T 25 1.636050 192.1 Time Shift Ctrl+Alt+C 26 1.705101 192.1 Facet Comment Ctrl+Alt+C 26 1.705101 192.1 Facet Comment Ctrl+Alt+C 27 1.706771 192.1 Facet Conversation Filter Image Statistics Telephony Wireless Tools Help 20 1.825073 192.1 Conversation Filter Image Statistics Telephony Wireless Tools Help 31 1.825044 192.1 Conversation Filter Image Statistics Telephony Wireless Tools Help Conversation Filter 33 1.937253 192.1 File Edit Wire Go Capture Analyze Statistics Telephony Wireless Tools Help Conversation Filter Image Statistics Telephony Wireless Tools Help Conversation Filter Image Statistics Telephony Wireless Tools Help Conversation Filt					イイイ曲							BOOTP/DHCP	
Time Source Destination Probool 18 1.075193 192.11 Act	U	1dp.port—47809										BT-DHT	
18 1.075193 192.1 100.40.0 <t< td=""><td>٩o.</td><td>Time</td><td>Source</td><td>Destination</td><td>Protocol</td><td></td><td></td><td></td><td></td><td></td><td></td><td>BT-uTP</td><td></td></t<>	٩o.	Time	Source	Destination	Protocol							BT-uTP	
19 1.076055 192.1 Mark/Umark Packet Ctrl+M 22 1.575054 192.11 Ignore/Unignore Packet Ctrl+D 23 1.576242 192.11 Set/Unset Time Reference Ctrl+T 24 1.635092 192.11 Time Shift Ctrl+Akirt-T 25 1.636050 192.11 Packet Comment Ctrl+Akirt-T 26 1.705101 192.12 Packet Comment Ctrl+Akirt-T 28 1.815615 192.11 Apply as Filter Prepare a Filter Prepare a Filter 30 1.825073 192.11 Conversation Filter Pilt 8 1.075193 192.168.1.192 192.168.1.102 BACne 61 Confirmed-REQ readPrope 31 1.826044 192.11 SCTP File 51555 192.168.1.102 192.168.1.102 BACne 61 Confirmed-REQ readPrope 22 1.936387 192.11 ScTP	-	18 1.075193	192.16	1 0 100 100 1	100 000							BVLC	
22 1.575054 192.1 Ignore/Unignore Packet Ctrl + D 23 1.576242 192.11 Set/Unset Time Reference Ctrl + T 24 1.635092 192.11 Time Shift Ctrl + Shift.+T 25 1.636050 192.11 Packet Comment Ctrl + At+c 26 1.705101 192.11 Packet Comment Ctrl + At+c 28 1.815615 192.11 Apply as Filter Prepare a Filter 29 1.819931 192.11 Onversation Filter Prepare a Filter 20 1.825073 192.12 Colorize Conversation SCTP 31 1.826044 192.11 SCTP Pielow SCTP 23 1.936387 192.12 Follow SCTP 23 1.575624 192.168.1.102 BACne 60 Error readPrope 24 1.635092 192.168.1.102 BACne 60 Error readPrope 25		19 1.076055	192.10	Mark/Unmark Packet	Ctrl+M							Bundle	
23 1.576242 192.1 24 1.635092 192.1 24 1.635092 192.1 25 1.636050 192.1 26 1.705101 192.1 27 1.706771 192.1 28 1.815615 192.1 29 1.819931 192.1 30 1.825073 192.1 20 conversation Filter		22 1.575054	192.10	Ignore/Unignore Packet	Ctrl+D							C12.22	
24 1.635092 192.1 25 1.636050 192.1 26 1.705101 192.1 27 1.706771 192.1 28 1.815615 192.1 29 1.819931 192.1 30 1.825073 192.1 31 1.826044 192.1 32 1.936387 192.1 33 1.937253 192.1 Follow 23 1.576242 Follow 24 1.635092 Protocol Preferences protocol Preferences User Datagram Protocol Vers Protocol Preferences Decode As Show Packet in New Window		23 1.576242	192.10	Set/Unset Time Reference	Ctrl+T							CAPWAP-CONTROL	
25 1.636050 192.1 26 1.705101 192.1 27 1.706771 192.1 28 1.815615 192.1 30 1.825073 192.1 31 1.825044 192.1 31 1.826044 192.1 31 1.937253 192.1 33 1.937253 192.1 Frame 18: 61 bytes on Ethernet II, Src: Heal Internet Protocol Vers User Datagram Protocol Data (19 bytes) Packet Comment Ctrl + Alt+C		24 1.635092	192.10	Time Shift	Ctrl+Shift+T								
26 1.705101 192.11 27 1.706771 192.11 28 1.815615 192.11 29 1.819931 192.11 30 1.825073 192.11 31 1.826044 192.11 32 1.936387 192.11 33 1.937253 192.11 Frame 18: 61 bytes on Ethernet II, Src: Heul Internet Protocol Vers Follow Ver Datagram Protocol Data (19 bytes) Decode As File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help Frame 18: 61 bytes on Ethernet II, Src: Heul Follow Follow Fotocol Preferences Show Packet in New Window Show Packet in New		25 1.636050	192.10	Packet Comment	Ctrl+Alt+C	4	*區域連線						
Z7 1.706771 192.11 Z8 1.815615 192.11 Z9 1.819931 192.11 Apply as Filter Prepare a Filter 11.826044 192.11 31.826044 192.11 23.1.936387 192.11 Frame 18: 61 bytes on Colver station Ethernet II, Src: Hewl Follow User Datagram Protocol Protocol Preferences Data (19 bytes) Show Packet in New Window		26 1.705101	192.16			File	e Edit View Go	Capture Analyze	Statistics	Telephony W	ireless To	ols Help	
28 1.815615 192.1 29 1.819931 192.1 30 1.825073 192.1 31 1.826044 192.1 23 1.936387 192.1 33 1.937253 192.1 Frame 18: 61 bytes on Ethernet II, Src: Hewl Internet Protocol Vers User Datagram Protocol Data (19 bytes) Follow Decode As Show Packet in New Window		27 1 706771	192 10	Edit Resolved Name		4	I 🖉 🛞 🕌 📷	X C 9 0 0 5	2 A 8	= = e e			
29 1. 819931 192.1 30 1. 825073 192.1 31 1. 826044 192.1 32 1. 936387 192.1 33 1. 937253 192.1 Frame 18: 61 bytes on Ethernet II, Src: Hewl Internet Protocol Vers User Datagram Protocol Data (19 bytes) Follow Decode As Show Packet in New Window		28 1 815615	192 10	Analysia Eilter		F	udn nort-47809					X	- Expression
10:1:000 Prepare a Filter 10:000 Prepare a Filter 10:0000 Prepare a Filter 10:000		29 1 819931	192.1	Apply as Filter		No	Time	Source	De	stination	Protocol	Length Info	
31 1.826044 192.11 32 1.936387 192.14 33 1.937253 192.14 Conversation Filter 19 1.076055 192.168.1.102 192.168.1.9 BACne 64 Complex.ACK readPrope 33 1.937253 192.14 SCTP 23 1.575242 192.168.1.9 192.168.1.102 BACne 64 Complex.ACK readPrope Frame 18: 61 bytes on Ethernet II, Src: Heul Internet Protocol Vers Follow 23 1.576242 192.168.1.9 192.168.1.102 BACne 60 Error readPrope 22 1.57510 192.168.1.102 192.168.1.102 BACne 60 Error readPrope 23 1.576242 192.168.1.102 192.168.1.102 BACne 60 Error readPrope 24 1.635092 192.168.1.102 192.168.1.102 BACne 59 Confirmed-REQ readPrope 25 1.636050 192.168.1.102 192.168.1.102 BACne 59 Confirmed-REQ readPrope 26 1.705101 192.168.1.102 192.168.1.102 BACne 39 Confirmed-REQ readPrope User Datagram Protocol Decode As Show Packet in New Window 30 1.825073 192.168.1.102 192.168.1.9 BACne 52 Complex-ACK readPrope 30 1.825073 192.168		20 1 925073	102.10	Prepare a Filter	•	-	18 1.075193	192.168.1.9	19	2.168.1.102	BACne.	61 Confirmed-REO	readPrope
32 1.936367 192.11 Colorize Conversation 22 1.575054 192.168.1.9 192.168.1.102 BACne 59 Confirmed-REQ readPrope 33 1.937253 192.11 Frame 18: 61 bytes on Follow 22 1.575054 192.168.1.9 192.168.1.9 BACne 60 Error readPrope Ethernet II, Src: Hewl Copy 1 Copy 1 22 1.576074 192.168.1.9 192.168.1.9 BACne 60 Error readPrope User Datagram Protocol Data (19 bytes) Decode As Show Packet in New Window 1 12.168.1.9 192.168.1.102 BACne 59 Confirmed-REQ readPrope 31 1.937253 192.16 192.168.1.9 192.168.1.9 192.168.1.9 BACne 59 Confirmed-REQ readPrope 24 1.635092 192.168.1.9 <t< td=""><td></td><td>21 1 926044</td><td>102.10</td><td>Conversation Filter</td><td>•</td><td></td><td>19 1.076055</td><td>192.168.1.102</td><td>19</td><td>2.168.1.9</td><td>BACne.</td><td> 64 Complex-ACK</td><td>readPrope</td></t<>		21 1 926044	102.10	Conversation Filter	•		19 1.076055	192.168.1.102	19	2.168.1.9	BACne.	64 Complex-ACK	readPrope
32 1.936367 192.11 33 1.937253 192.11 33 1.937253 192.11 Frame 18: 61 bytes on Ethernet II, Src: Hewl Internet Protocol Vers User Datagram Protocol Data (19 bytes) SCTP Decode As Copy Show Packet in New Window Copy Show Packet in New Window Show Packet in New Window		31 1.020044	192.10	Colorize Conversation	•		22 1.575054	192.168.1.9	19	2.168.1.102	BACne.		readPrope
331.93/233 192.16 Follow 241.635092 192.168.1.9 192.168.1.102 BACne 59 Confirmed-REQ readPrope Frame 18: 61 bytes on Copy 251.636050 192.168.1.02 192.168.1.9 BACne 60 Error readPrope Internet II, Src: Hewl Protocol Preferences 271.706771 192.168.1.9 BACne 39 Confirmed-REQ readPrope User Datagram Protocol Decode As Decode As 291.819931 192.168.1.102 192.168.1.102 BACne 39 Confirmed-REQ readPrope Show Packet in New Window Show Packet in New Window 192.168.1.02 192.168.1.102 BACne 60 Error readPrope 101 102 103 112 Decode As Decode As 192.168.1.102 BACne 59 Confirmed-REQ readPrope 11 102 104 112 Decode As Decode As 192.168.1.102 192.168.1.102 BACne 82 Complex-ACK readPrope 12 11 12 12 14 12 12 14 12 12 14 12 14 14 14 14 14 14 14 14 14 14 14 14 14		32 1.936387	192.10	SCTP	•		23 1.576242	192.168.1.102	19	92.168.1.9	BACne.	60 Error	readPrope
Frame 18: 61 bytes on Ethernet II, Src: Hewl Internet Protocol Vers User Datagram Protocol Data (19 bytes) Copy 25 1.636050 25 1.636050 192.168.1.102 192.168.1.90 BACne 60 Error readPrope 20 confirmed-REQ 20 1.705101 192.168.1.102 192.168.1.102 BACne 234 Confirmed-REQ 234 Confirmed-REQ 27 1.706771 192.168.1.102 BACne 234 Confirmed-REQ 234 Confirmed-REQ 27 1.706771 192.168.1.102 BACne 349 Complex-ACK 29 0.681.102 192.168.1.102 BACne 349 Complex-ACK 29 0.681.102 readPrope 20 taggram Protocol Data (19 bytes) Decode As 29 1.81931 192.168.1.102 192.168.1.102 BACne 52 Complex-ACK readPrope 30 1.825073 192.168.1.102 192.168.1.102 BACne 61 Confirmed-REQ readPrope 30 1.825073 192.168.1.102 192.168.1.102 BACne 61 Confirmed-REQ readPrope 30 1.825073 192.168.1.102 192.168.1.102 BACne 61 Confirmed-REQ readPrope		33 1.93/253	192.10	Follow			24 1.635092	192.168.1.9	19	2.168.1.102	BACne.	59 Confirmed-REQ	readPrope
Copy Copy <thcopy< th=""> Copy Copy <thc< td=""><td>F</td><td>rame 18. 61 by</td><td>tes on</td><td>AC 2010</td><td>5</td><td></td><td>25 1.636050</td><td>192.168.1.102</td><td>19</td><td>2.168.1.9</td><td>BACne.</td><td> 60 Error</td><td>readPrope.</td></thc<></thcopy<>	F	rame 18. 61 by	tes on	AC 2010	5		25 1.636050	192.168.1.102	19	2.168.1.9	BACne.	60 Error	readPrope.
Internet Protocol Vers Protocol Preferences 27 1.706771 192.168.1.102 192.168.1.9 BACne 349 Complex-ACK readPrope User Datagram Protocol Decode As Decode As 59 Confirmed-REQ readPrope 29 1.819931 192.168.1.102 BACne 59 Confirmed-REQ readPrope Data (19 bytes) Show Packet in New Window Show Packet in New Window 192.168.1.9 192.168.1.9 192.168.1.102 BACne 61 Confirmed-REQ readPrope	F	thernet II Sr	C: Hew]	Сору	+ [26 1.705101	192.168.1.9	19	92.168.1.102	BACne.	234 Confirmed-REQ	readPrope
User Datagram Protocol Protocol Preterences 28 1.815615 192.168.1.9 192.168.1.102 BACne 59 Confirmed-REQ readPrope Data (19 bytes) Decode As Show Packet in New Window 29 1.819931 192.168.1.02 192.168.1.102 BACne 82 Complex-ACK readPrope 30 1.825073 192.168.1.9 192.168.1.02 BACne 61 Confirmed-REQ readPrope	1	Internet Protoc	ol Vens	D			27 1.706771	192.168.1.102	19	92.168.1.9	BACne.	349 Complex-ACK	readPrope
Data (19 bytes) Decode As Decode As 29 1.819931 192.168.1.102 192.168.1.9 BACne 82 Complex-ACK readPrope 30 1.825073 192.168.1.9 192.168.1.102 BACne 61 Confined-REQ readPrope	-	Icon Detagner	notocol	Protocol Preferences	•		28 1.815615	192.168.1.9	19	92.168.1.102	BACne.	59 Confirmed-REQ	readPrope
Vata (19 bytes) Show Packet in New Window 36 1.8250/3 192.168.1.9 192.168.1.102 BACne 61 Confirmed-REQ readPrope. 11 8260/4 102.168.1.40 102.168.1.40 102.168.1.102 BACne 61 Confirmed-REQ readPrope.	-	Diser Datagram P	1010001	Decode As			29 1.819931	192.168.1.102	19	92.168.1.9	BACne.	82 Complex-ACK	readPrope
	L	Data (19 Dytes)		Show Packet in New Window	v		30 1.8250/3	192.168.1.9	19	2.168.1.102	BACne.	61 Confirmed-REQ	readPrope

試著解讀 BACnet/IP 封包

記錄的封包包含時間 (TIme)、來源 IP(Source)、目 的IP(Destination)、協議 (Protocol)、長度(Length)、 資訊(Info)等欄位。點開中間 可以看到通訊各層的解析. 以及最下方的通訊碼 16 進 制數值。剛開始可以先試著 理解 Info 欄。

-	Edit View Go	Capture Analyze St			нер			
	🔲 🔬 🧐 🤳 🚥		* ⊻⊑≡ ચવ	9,12			Rear and Rear and	
Mo	Time	Samma	Destination	Protocol Lo	noth Info		Expression	ur
NU.	2 0 072214	192 168 1 9	192 168 1 255	BACne	60 Unconfirmed_REO	who-Ts 0 /19/30	22	-
E	3 0 072501	192.168.1.9	192.168.1.255	BACne	67 Unconfirmed-REQ	i-Am device 419	94302	-
	1 0 072911	192.168 1 102	192.168.1.255	BACne	67 Unconfirmed_REQ	i-Am device, 41.	202	
	11 1 676086	192.168.1.9	192.168.1.102	BACne	61 Confirmed_REO	readProperty[21 device 1	
	12 1 716108	192.168 1 102	192.168.1.9	BACne	64 Complex-ACK	readProperty[2] device 1	
	13 2 200087	192.168.1.9	192.168.1.102	BACne	61 Confirmed_REO	readProperty[3] device 1	
	14 2 201401	192.168 1 102	192.168.1.9	BACne	67 Complex-ACK	readProperty[3] device 1	
	15 2 379532	192.168.1.9	192.168.1.102	BACne	61 Confirmed_REO	readProperty[Al device 1	
	16 2 3806/1	192.168.1.102	192.168.1.9	BACne	67 Complex-ACK	readProperty[Al device 1	
	17 2 525516	192.168.1.9	192.168.1.102	BACne	272 Confirmed_REO	readPropertyMul	+	
	18 2 633002	192.168.1.102	192.168.1.9	BACne	A11 Complex-ACK	readPropertyMul	ltinle[5]	
	19 2 699573	192.168.1.9	192.168.1.102	BACne	272 Confirmed-REO	readPropertyMul	ltiple[6]	
	20 2 700636	192 168 1 102	192 168 1 9	BACne	411 Complex-ACK	readPropertyMul	ltinle[6]	
▷ F ▷ E ▷ 1	rame 2: 60 byt thernet II, Sr internet Protoc Jser Datagram P	es on wire (480 bi c: HewlettP_47:08: ol Version 4, Src: rotocol, Src Port: Link Control	ts), 60 bytes captu 55 (64:51:06:47:08: 192.168.1.9, Dst: 47808, Dst Port: 4	red (480 b 55), Dst: 192.168.1. 17808	its) on interface 0 Broadcast (ff:ff:ff:f 255	f:ff:ff)		
⊳ L ⊳ E ⊳ E	Building Automa	tion and Control N	etwork NPDU					

BACnet Confirmed 與 Unconfirmed 封包

BACnet 封包的發出主要區分 confirmed 與 unconfirmed 兩類, 顧名思 義:unconfirmed 是不需要回覆確認資訊的, 例如 who is、I am 等廣播訊息(但不必 然是廣播), 而confirmed 則必須要以 simple-ACK、complex-ACK等回復資訊例如讀 屬性(ReadProperty)(不可以廣播)。 confirmed 類的封包都會帶一個 Invoke ID(調用 編號, 如圖的[]內), 在一定的時間內, 必須收到相同 Invoke ID 的回應封包, 否則會逾 時(Timeout)而重試(Retry), 直到重試次數到達都沒回應, 則會告知應用層(圖控軟體) 連線失敗。

BACne	61 Confirmed-REQ	<pre>readProperty[2] device,1000 object-list</pre>
BACne	64 Complex-ACK	<pre>readProperty[2] device,1000 object-list</pre>
BACne	61 Confirmed-REQ	<pre>readProperty[3] device,1000 object-list</pre>
BACne	67 Complex-ACK	<pre>readProperty[3] device,1000 object-list device,1</pre>
BACne	61 Confirmed-REQ	<pre>readProperty[4] device,1000 object-list</pre>
BACne	67 Complex-ACK	<pre>readProperty[4] device,1000 object-list analog-v</pre>
BACne	272 Confirmed-REQ	<pre>readPropertyMultiple[5]</pre>
BACne	411 Complex-ACK	readPropertyMultiple[5]
BACne	272 Confirmed-REQ	<pre>readPropertyMultiple[6]</pre>
BACne	411 Complex-ACK	readPropertyMultiple[6]

如何判斷 BACnet Client 端過高頻率的發送封包

部分撰寫或設定不良的 BACnet Client 端圖控程式, 可能為了滿足短時間或取大量 的點數值的需求, 而將讀取間隔時間設定過小。由於 BACnet/IP 始採用 UDP 方式通 訊, 因此這樣的封包可能很快塞滿網路, 必須注意 BACnet/IP 網路能夠負荷的網路 流量, 不一定是 MS/TP 等較低頻寬網路所能負擔的。

要判斷是否有上述狀況發生,可以在 BACnet Client 的電腦上安裝 Wireshark 進行 監看。如果觀察到本身 IP 快速發出 confirmed 封包而對應 Invoke ID 的回覆封包零 零落落,除了考慮網路(尤其是 MS/TP網路)品質外,也可能必須檢討 Client 端讀取間 隔時間是否合理。要判斷 MS/TP 網路的品質可以利用免費的 <u>ICDT BACnet MS/TP</u> 通訊記錄程式,但由於該程式僅以 16 進制數值記錄,必須對於 MS/TP 網路有一定理 解才能解讀。

如何判讀 BACnet 廣播風暴(Broadcast Storm)

廣播風暴(Broadcast Storm): BACnet Router 網路不可短循環, 否則會造成廣播風 暴, 進而使網路過度忙碌而癱瘓。例如網路上同時有兩個 BACnet/IP 與 MS/TP 的 Router, 又將其 MS/TP 網路線相連結, 或者將具備兩個以上 MS/TP 迴路的 BACnet Router, 將兩個 MS/TP 線路相接, 如此一來會使 BACnet 廣播在兩個 Router 間不斷 傳遞, 造成網路壅塞。判斷此狀況可以從 BACnet/IP 網路端用 Wireshark 進行監看, 如果同一(可能每秒數百個)時間產生大量相同的廣播, 即可斷定此一狀況。

如右為造成廣播風暴的網路示意 圖。但先決條件是接起來的兩個 MS/TP 迴路速率必須相同且 MAC 不可重複



廣播風暴範例

這是一個將 BACnet Router 兩個 MS/TP 迴路相接造成廣 播風暴的案例, 觀察 Time 欄 在 200mSec 內湧入 13 個以 上相同的廣播封包。

	區域連線							
File	e Edit View Go	Capture Analyze	Statistics Telephony Win	eless Too	ls Help			
4	🔳 🥂 🛞 🛄 🔚	X C Q @ @	≊ ₩	Q II				
	bacnet							Expression
No.	Time	Source	Destination	Protocol	Length Info			
	215 7.999783	192.168.1.110	192.168.1.255	BACne	76 Uncon	firmed-REQ i	-Am device,4194302	
	216 8.012942	192.168.1.110	192.168.1.255	BACne	76 Uncon	firmed-REQ i	-Am device, 4194302	
	217 8.026104	192.168.1.110	192.168.1.255	BACne	76 Uncon	firmed-REQ i	-Am device,4194302	
	218 8.039304	192.168.1.110	192.168.1.255	BACne	76 Uncon	firmed-REQ i	-Am device,4194302	
	219 8.052508	192.168.1.110	192.168.1.255	BACne	76 Uncon	firmed-REQ i	-Am device,4194302	
	220 8.065714	192.168.1.110	192.168.1.255	BACne	76 Uncon	firmed-REQ i	-Am device,4194302	
	221 8.078900	192.168.1.110	192.168.1.255	BACne	76 Uncon	firmed-REQ i	-Am device,4194302	
	222 8.092107	192.168.1.110	192.168.1.255	BACne	76 Uncon	firmed-REQ i	-Am device,4194302	
	223 8.105303	192.168.1.110	192.168.1.255	BACne	76 Uncon	firmed-REQ i	-Am device,4194302	
	224 8.118494	192.168.1.110	192.168.1.255	BACne	76 Uncon	firmed-REQ i	-Am device,4194302	
	225 8.131702	192.168.1.110	192.168.1.255	BACne	76 Uncon	firmed-REQ i	-Am device,4194302	
	226 8.144898	192.168.1.110	192.168.1.255	BACne	76 Uncon	firmed-REQ i	-Am device,4194302	
	227 8.158079	192.168.1.110	192.168.1.255	BACne	76 Uncon	firmed-REQ i	-Am device,4194302	
	Frame 7: 60 byt Ethernet II, Sr Internet Protoc User Datagram P BACnet Virtual Building Automa	tes on wire (480 rc: HewlettP_47:0 col Version 4, Sr Protocol, Src Por Link Control ution and Control	bits), 60 bytes captu 8:55 (64:51:06:47:08: c: 192.168.1.9, Dst: t: 47808, Dst Port: 4 Network NPDU	red (480 55), Dst 192.168. 7808	bits) on int : Broadcast (1.255	erface 0 ff:ff:ff:ff:	ff:ff)	
00	00 ff ff ff f	f ff ff 64 51 00	5 47 08 55 08 00 45 0	ð	dQ .G.UE.			
00	00 2e 4e 8	2 00 00 80 11 6	/ e4 c0 a8 01 09 c0 a8	5N.	···· g			
00	30 ff ff 00 f	f 10 08 09 00 11	+ 04 01 00 00 12 01 20 0 3f ff fe					
	wiresbark BF23F	7BD5-7BCD-4934-B744-3F	TERARCANO2 20170417003756	a06900		Packets: 863 · Dis	nlaved · 874 /05 5%)	Profile: Defeul



停止記錄後按下 save 可以記錄所有封包, 但必須注 意這會記錄下包含 bacnet 以及其他通訊的所有封 包, 如果將這樣的封包存檔對外提供, 除了檔案過大 外, 也會有將電腦中要資訊外流的風險。

選擇 File->Export Specified Packets.. 將 All Packets Displayed 進行存檔,此時只存 檔看到的 bacnet 封包,就沒有 上述疑慮了。

ile	Edit	View	Go	Capture	Analyze	Stati				
	Open			C	trl+0	1				
	Open	Recent				۰ F				
	Merge	·								
	Import from Hex Dump									
	Close			C	trl+W					
	Save			C	trl+S					
	Save A	s		C	trl+Shift+S	s _				
	File Se	t				•				
	Export	Specifie	ed Pad	:kets		1				
	Export	Packet	Dissec	tions		► E				
	Export	Packet	Bytes.	C	trl+H					
	Export									
	Export	SSL Ses	ision K	eys		1				
	Export	Objects	5			•				
	Print			C	trl+P					



關於 BACnet 協議

關於 BACnet 的資訊, 可以在元米科技網站獲得更多訊息

http://www.icdt.com.tw/main/index.php/using-joomla/extensions/component s/search-component/search?searchword=bacnet&searchphrase=all

例如 <u>BACnet 網路問題分析</u> 與 關於 <u>BACnet 的重要網址連結</u> 等都是極重要值得參 考的資訊。

元米科技提供 BACnet 相關軟硬體設計服務, 如有需求請洽 <u>eric.icdt@msa.hinet.net</u>, 更進一步資訊請上元米網站 <u>http://www.icdt.com.tw</u>