如何使用 wireshark 觀察 BACnet/IP 通訊封包

元米科技 2017/4/17

本文目的

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

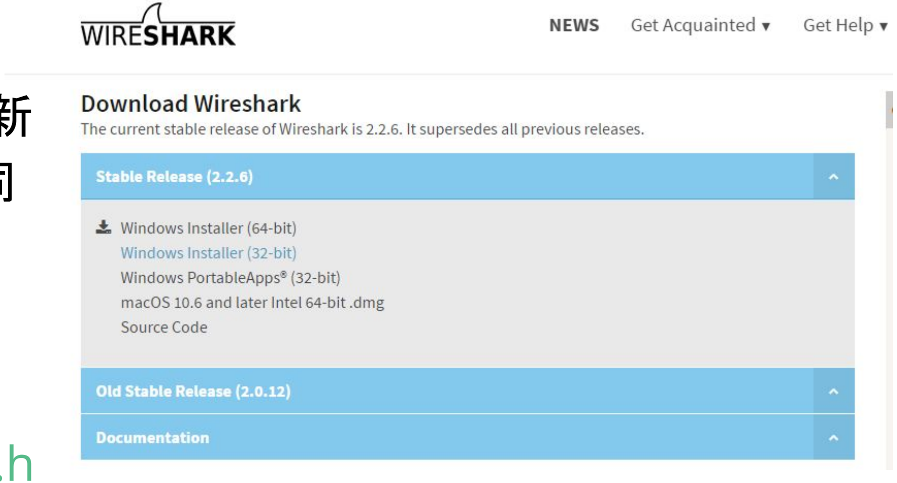
維基百科 : Wireshark（前稱Ethereal）是一個免費開源的網路封包分析軟體。網路封包分析軟體的功能是截取網路封包，並盡可能顯示出最為詳細的網路封包資料。
在過去，網路封包分析軟體是非常昂貴，或是專門屬於營利用的軟體，Wireshark的出現改變了這一切。在GNU通用公眾授權條款的保障範圍底下，使用者可以以免費的代價取得軟體與其程式碼，並擁有針對其原始碼修改及客製化的權利。Wireshark是目前全世界最廣泛的網路封包分析軟體之一。

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:

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



Download Wireshark

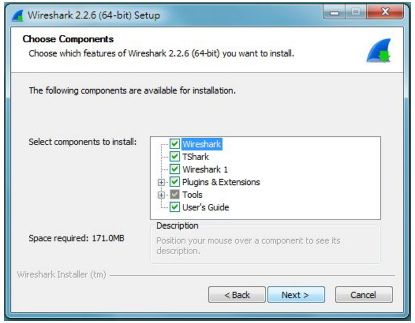
The current stable release of Wireshark is 2.2.6. It supersedes all previous releases.

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



Wireshark 2.2.6 (64-bit) Setup

Choose Components

Choose which features of Wireshark 2.2.6 (64-bit) you want to install.

The following components are available for installation.

Select components to install:

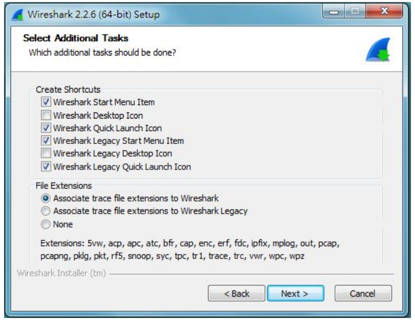
- ☑ Wireshark
- ☑ TShark
- ☑ Wireshark 1
- ☑ Plugins & Extensions
- ☑ Tools
- ☑ User's Guide

Space required: 171.0MB

Description

Position your mouse over a component to see its description.

Wireshark Installer (tm)



Wireshark 2.2.6 (64-bit) Setup

Select Additional Tasks

Which additional tasks should be done?

Create Shortcuts

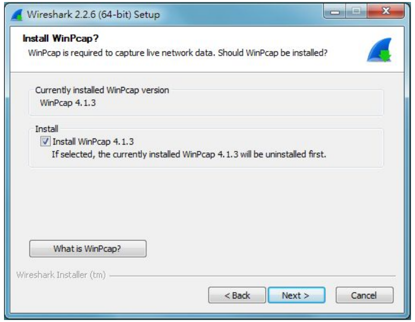
- ☑ Wireshark Start Menu Item
- □ Wireshark Desktop Icon
- ☑ Wireshark Quick Launch Icon
- ☑ Wireshark Legacy Start Menu Item
- □ Wireshark Legacy Desktop Icon
- ☑ Wireshark Legacy Quick Launch Icon

File Extensions

- ● Associate trace file extensions to Wireshark
- ○ Associate trace file extensions to Wireshark Legacy
- ○ None

Extensions: 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, ipfix, mplog, out, pcap, pcapng, pklg, pkt, rf5, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, wpz

Wireshark Installer (tm)



Wireshark 2.2.6 (64-bit) Setup

Install WinPcap?

WinPcap is required to capture live network data. Should WinPcap be installed?

Currently installed WinPcap version

WinPcap 4.1.3

Install

☑ Install WinPcap 4.1.3

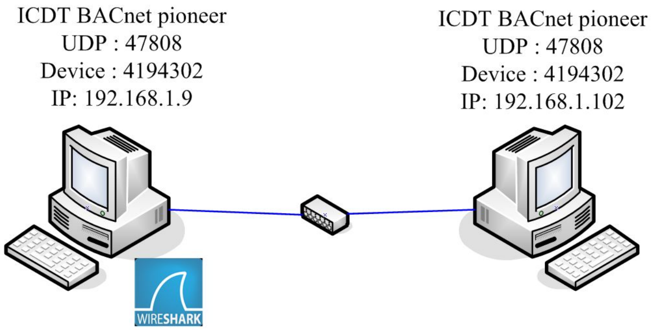
If selected, the currently installed WinPcap 4.1.3 will be uninstalled first.

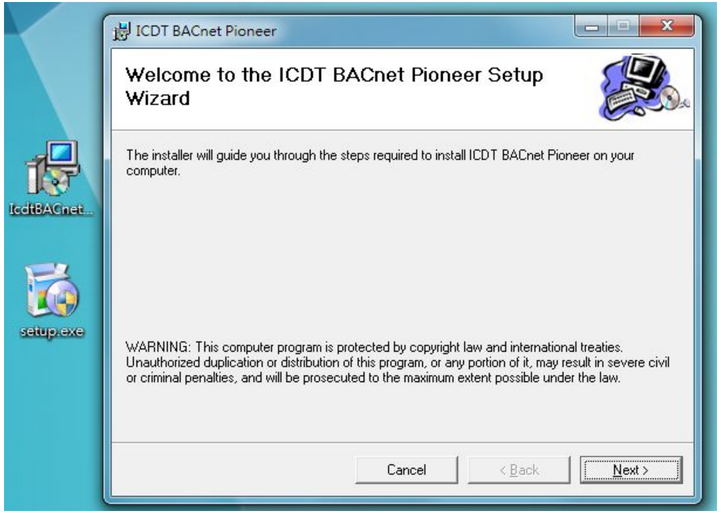
Wireshark Installer (tm)

安裝 ICDT BACnet pioneer 免費軟體

自 元米科技下載 最新版 ICDT BACnet pioneer 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





Welcome to the ICDT BACnet Pioneer Setup Wizard

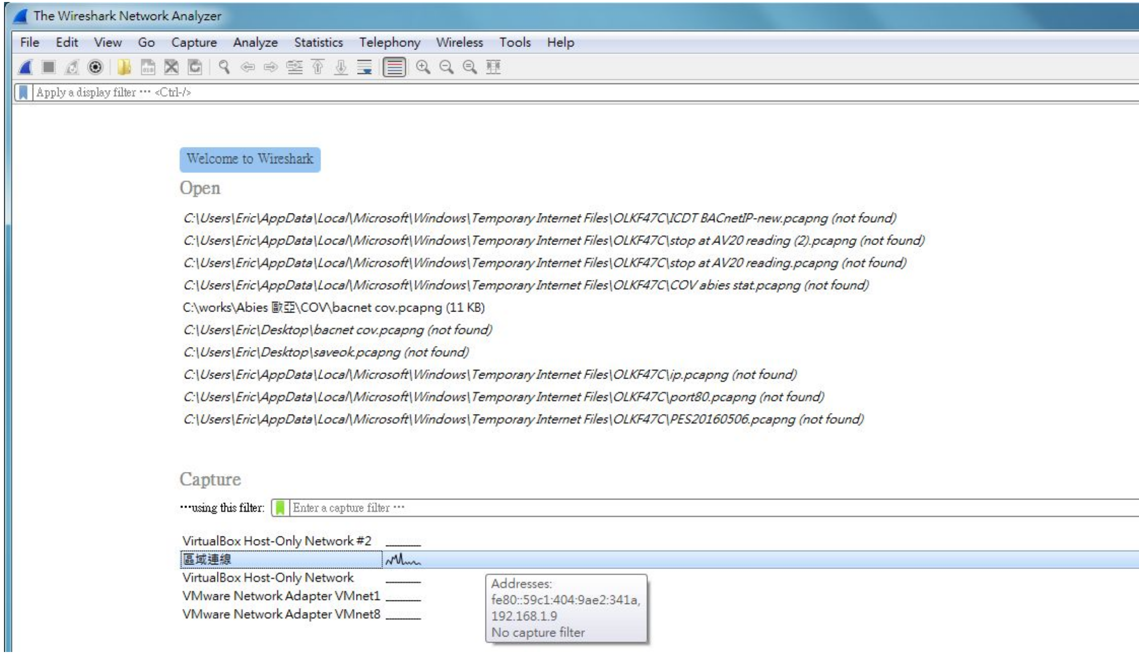
The installer will guide you through the steps required to install ICDT BACnet Pioneer on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

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。



Open

C:\Users\Eric\AppData\Local\Microsoft\Windows\Temporary Internet Files\OLKF47C\ICDT BACnetIP-new.pcapng (not found)
C:\Users\Eric\AppData\Local\Microsoft\Windows\Temporary Internet Files\OLKF47C\stop at AV20 reading (2).pcapng (not found)
C:\Users\Eric\AppData\Local\Microsoft\Windows\Temporary Internet Files\OLKF47C\stop at AV20 reading.pcapng (not found)
C:\Users\Eric\AppData\Local\Microsoft\Windows\Temporary Internet Files\OLKF47C\COV abies stat.pcapng (not found)
C:\works\Abies 歐亞\COV\bacnet cov.pcapng (11 KB)
C:\Users\Eric\Desktop\bacnet cov.pcapng (not found)
C:\Users\Eric\Desktop\saveok.pcapng (not found)
C:\Users\Eric\AppData\Local\Microsoft\Windows\Temporary Internet Files\OLKF47C\ip.pcapng (not found)
C:\Users\Eric\AppData\Local\Microsoft\Windows\Temporary Internet Files\OLKF47C\port80.pcapng (not found)
C:\Users\Eric\AppData\Local\Microsoft\Windows\Temporary Internet Files\OLKF47C\PES20160506.pcapng (not found)

Capture

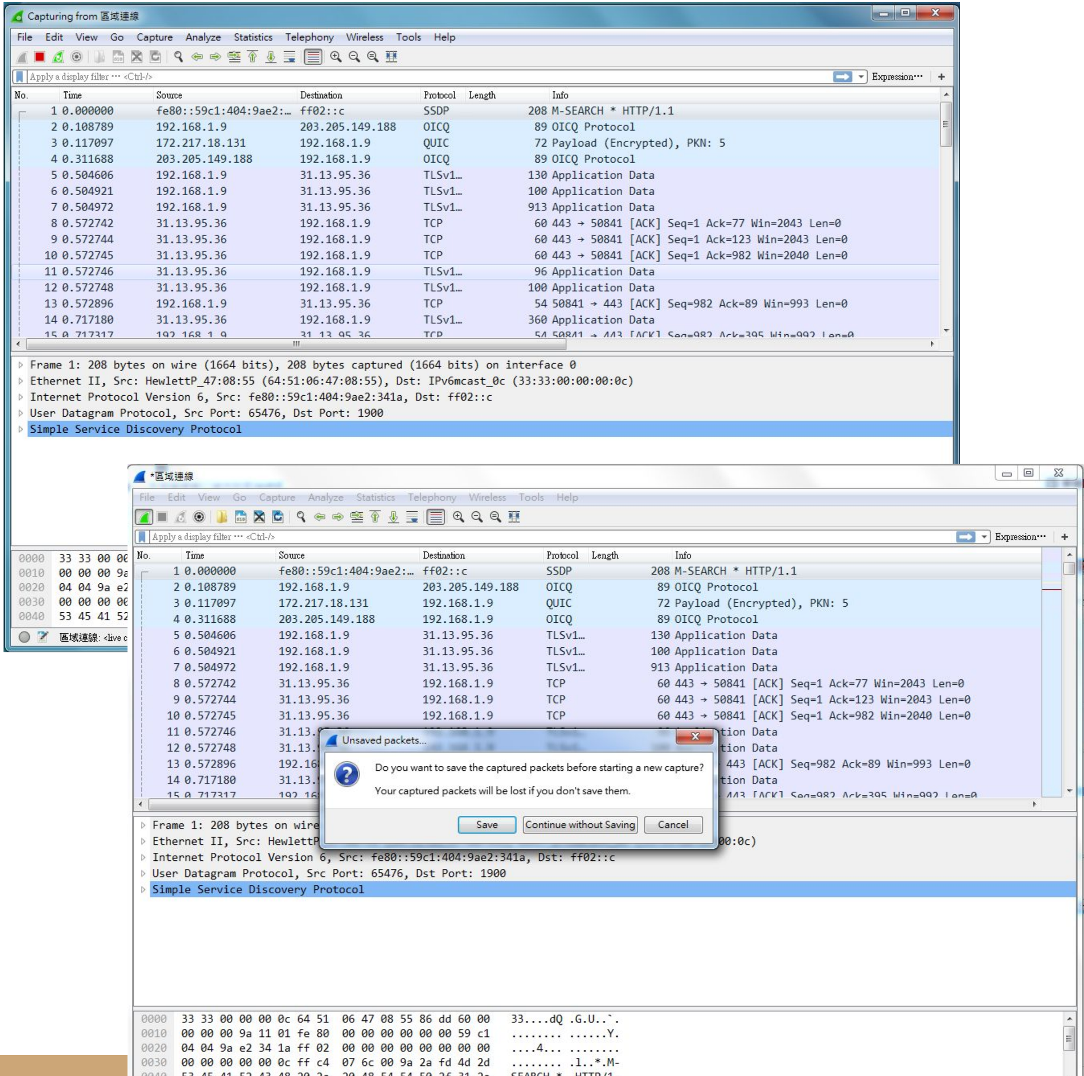
…using this filter: Enter a capture filter …

VirtualBox Host-Only Network #2
區域連線
VirtualBox Host-Only Network
VMware Network Adapter VMnet1
VMware Network Adapter VMnet8

Addresses:
fe80::59c1:404:9ae2:341a,
192.168.1.9
No capture filter

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 區域連線
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
*區域連線
區域連線: <live c

```
No.  Time      Source              Destination      Protocol Length Info
  1 0.000000  fe80::59c1:404:9ae2:… ff02::c          SSDP      208 M-SEARCH * HTTP/1.1
  2 0.108789  192.168.1.9         203.205.149.188  OICQ       89 OICQ Protocol
  3 0.117097  172.217.18.131      192.168.1.9      QUIC       72 Payload (Encrypted), PKN: 5
  4 0.311688  203.205.149.188     192.168.1.9      OICQ       89 OICQ Protocol
  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
  7 0.504972  192.168.1.9         31.13.95.36      TLSv1…    913 Application Data
  8 0.572742  31.13.95.36         192.168.1.9      TCP        60 443 → 50841 [ACK] Seq=1 Ack=77 Win=2043 Len=0
  9 0.572744  31.13.95.36         192.168.1.9      TCP        60 443 → 50841 [ACK] Seq=1 Ack=123 Win=2043 Len=0
 10 0.572745  31.13.95.36         192.168.1.9      TCP        60 443 → 50841 [ACK] Seq=1 Ack=982 Win=2040 Len=0
 11 0.572746  31.13.95.36         192.168.1.9      TLSv1…     96 Application Data
 12 0.572748  31.13.95.36         192.168.1.9      TLSv1…    100 Application Data
 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 Data
```

```
Frame 1: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface 0
Ethernet II, Src: HewlettP_47:08:55 (64:51:06:47:08:55), Dst: IPv6mcast_0c (33:33:00:00:00:0c)
Internet Protocol Version 6, Src: fe80::59c1:404:9ae2:341a, Dst: ff02::c
User Datagram Protocol, Src Port: 65476, Dst Port: 1900
Simple Service Discovery Protocol
```

```
0000  33 33 00 00 00 0c 64 51  06 47 08 55 86 dd 60 00   33....dQ .G.U..`.
0010  00 00 00 9a 11 01 fe 80  00 00 00 00 00 00 59 c1   ........ ......Y.
0020  04 04 9a e2 34 1a ff 02  00 00 00 00 00 00 00 00   ....4... ........
0030  00 00 00 00 00 0c ff c4  07 6c 00 9a 2a fd 4d 2d   ........ .l..*.M-
```

Unsaved packets...

Do you want to save the captured packets before starting a new capture?

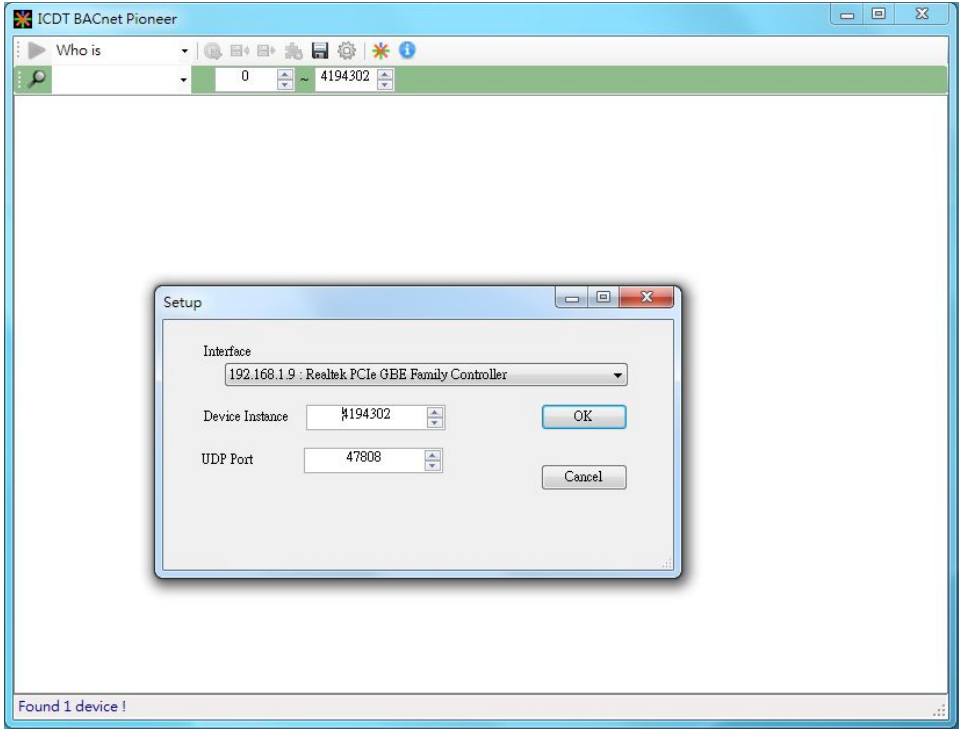
Your captured packets will be lost if you don't save them.

Save | Continue without Saving | Cancel

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



0 ~ 4194302

Interface: 192.168.1.9 : Realtek PCIe GBE Family Controller

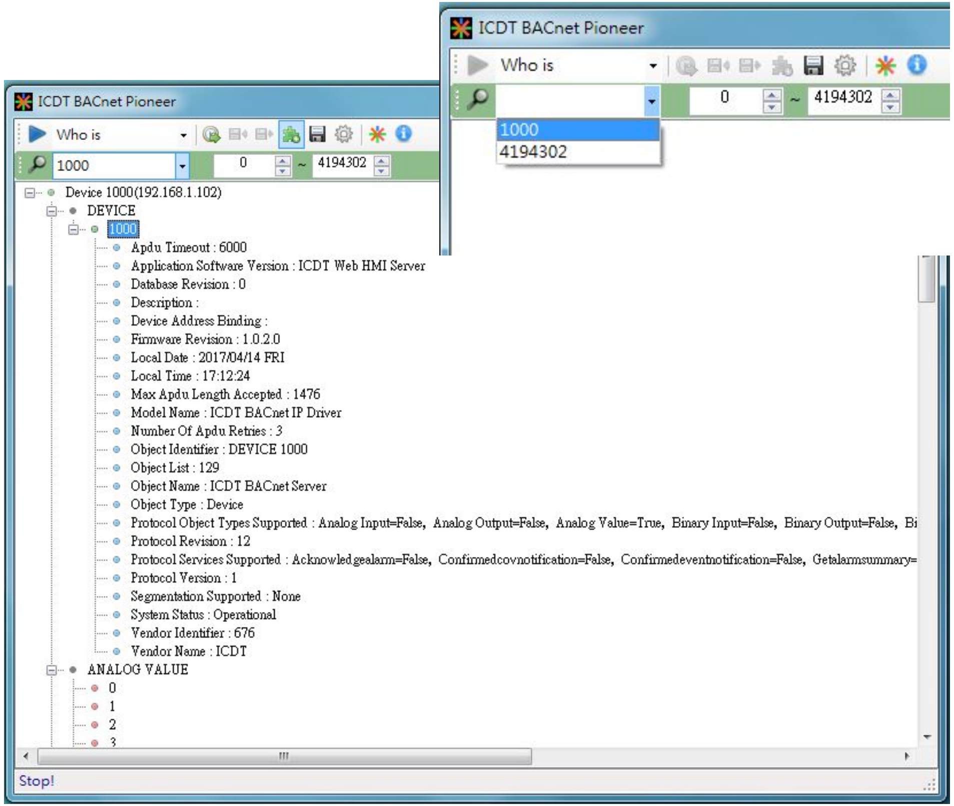
Device Instance: 4194302

UDP Port: 47808

Found 1 device !

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

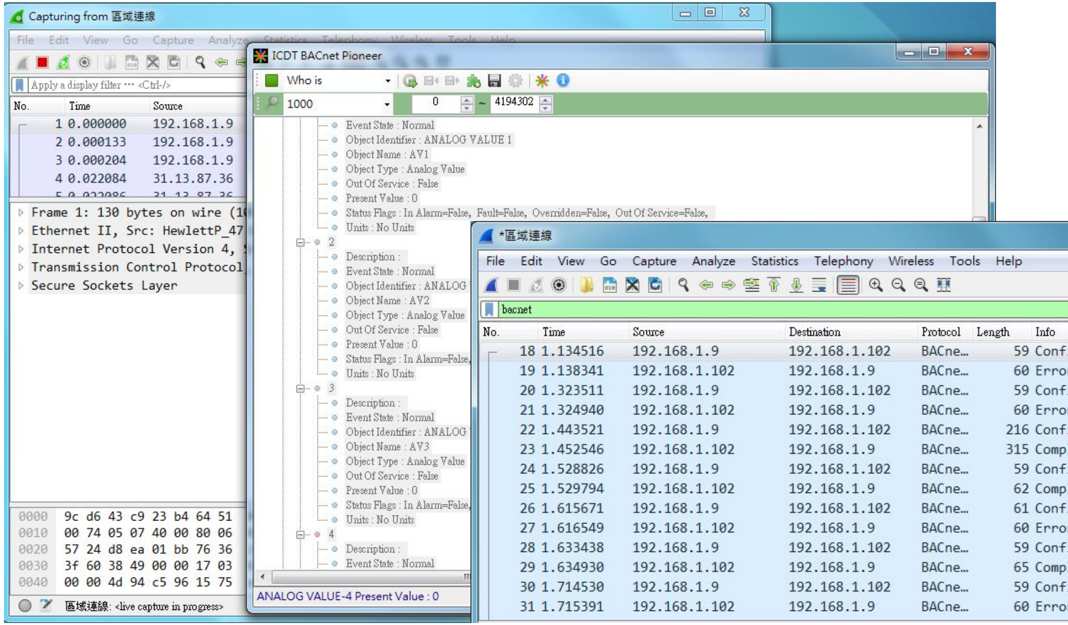


```
Device 1000(192.168.1.102)
  DEVICE
    1000
      Apdu Timeout : 6000
      Application Software Version : ICDT Web HMI Server
      Database Revision : 0
      Description :
      Device Address Binding :
      Firmware Revision : 1.0.2.0
      Local Date : 2017/04/14 FRI
      Local Time : 17:12:24
      Max Apdu Length Accepted : 1476
      Model Name : ICDT BACnet IP Driver
      Number Of Apdu Retries : 3
      Object Identifier : DEVICE 1000
      Object List : 129
      Object Name : ICDT BACnet Server
      Object Type : Device
      Protocol Object Types Supported : Analog Input=False, Analog Output=False, Analog Value=True, Binary Input=False, Binary Output=False, Bi
      Protocol Revision : 12
      Protocol Services Supported : Acknowledgealarm=False, Confirmedcovnotification=False, Confirmedeventnotification=False, Getalarmsummary=
      Protocol Version : 1
      Segmentation Supported : None
      System Status : Operational
      Vendor Identifier : 676
      Vendor Name : ICDT
  ANALOG VALUE
    0
    1
    2
    3
```

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
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
ICDT BACnet Pioneer
Who is
1000
0
~
4194302
*區域連線
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
No.   Time       Source
  1 0.000000    192.168.1.9
  2 0.000133    192.168.1.9
  3 0.000204    192.168.1.9
  4 0.022084    31.13.87.36
```

```
▷ Frame 1: 130 bytes on wire (1
▷ Ethernet II, Src: HewlettP_47
▷ Internet Protocol Version 4,
▷ Transmission Control Protocol
▷ Secure Sockets Layer
```

```
0000  9c d6 43 c9 23 b4 64 51
0010  00 74 05 07 40 00 80 06
0020  57 24 d8 ea 01 bb 76 36
0030  3f 60 38 49 00 00 17 03
0040  00 00 4d 94 c5 96 15 75
```

區域連線: <live capture in progress>

```
Event State : Normal
Object Identifier : ANALOG VALUE 1
Object Name : AV1
Object Type : Analog Value
Out Of Service : False
Present Value : 0
Status Flags : In Alarm=False, Fault=False, Overridden=False, Out Of Service=False,
Units : No Units
2
  Description :
  Event State : Normal
  Object Identifier : ANALOG
  Object Name : AV2
  Object Type : Analog Value
  Out Of Service : False
  Present Value : 0
  Status Flags : In Alarm=False,
  Units : No Units
3
  Description :
  Event State : Normal
  Object Identifier : ANALOG
  Object Name : AV3
  Object Type : Analog Value
  Out Of Service : False
  Present Value : 0
  Status Flags : In Alarm=False,
  Units : No Units
4
  Description :
  Event State : Normal
```

ANALOG VALUE-4 Present Value : 0

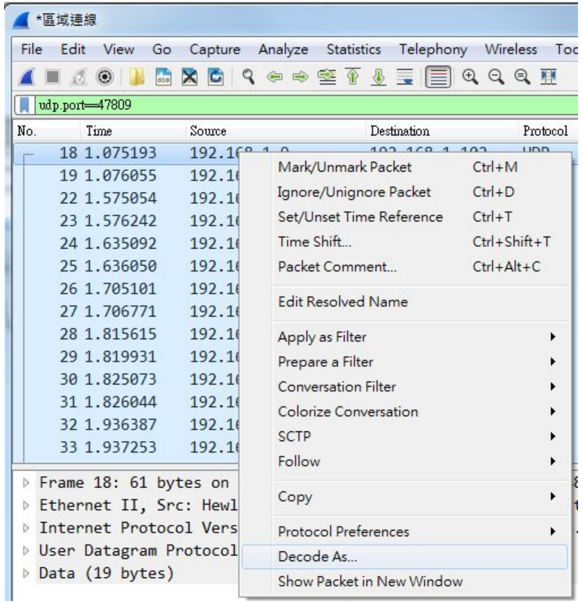
bacnet

No.	Time	Source	Destination	Protocol	Length	Info
18	1.134516	192.168.1.9	192.168.1.102	BACne…	59	Conf
19	1.138341	192.168.1.102	192.168.1.9	BACne…	60	Erro
20	1.323511	192.168.1.9	192.168.1.102	BACne…	59	Conf
21	1.324940	192.168.1.102	192.168.1.9	BACne…	60	Erro
22	1.443521	192.168.1.9	192.168.1.102	BACne…	216	Conf
23	1.452546	192.168.1.102	192.168.1.9	BACne…	315	Comp
24	1.528826	192.168.1.9	192.168.1.102	BACne…	59	Conf
25	1.529794	192.168.1.102	192.168.1.9	BACne…	62	Comp
26	1.615671	192.168.1.9	192.168.1.102	BACne…	61	Conf
27	1.616549	192.168.1.102	192.168.1.9	BACne…	60	Erro
28	1.633438	192.168.1.9	192.168.1.102	BACne…	59	Conf
29	1.634930	192.168.1.102	192.168.1.9	BACne…	65	Comp
30	1.714530	192.168.1.9	192.168.1.102	BACne…	59	Conf
31	1.715391	192.168.1.102	192.168.1.9	BACne…	60	Erro

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

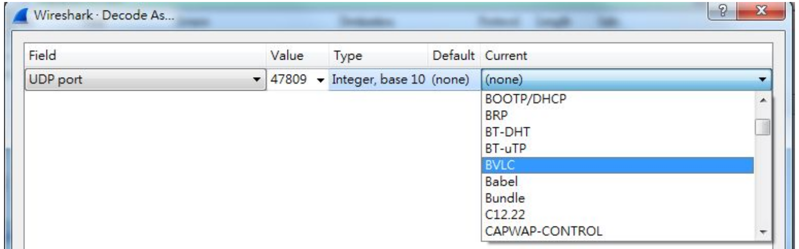
(BACnet Virtual Link Control)


*區域連線
File Edit View Go Capture Analyze Statistics Telephony Wireless Toc
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window

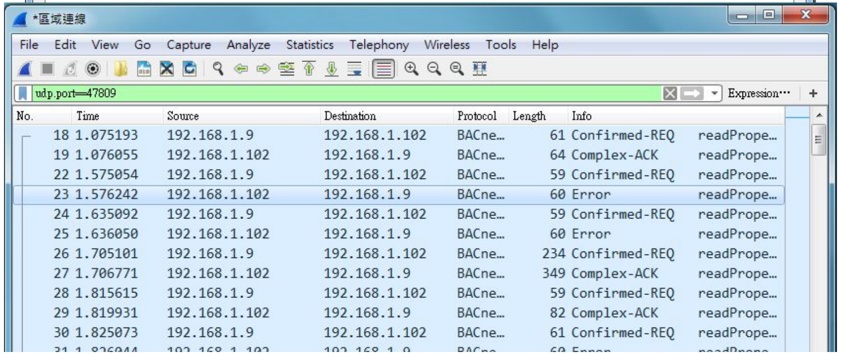
udp.port==47809

```
No.   Time       Source        Destination          Protocol
   18 1.075193   192.168.1.9   192.168.1.102        UDP
   19 1.076055   192.16
   22 1.575054   192.16
   23 1.576242   192.16
   24 1.635092   192.16
   25 1.636050   192.16
   26 1.705101   192.16
   27 1.706771   192.16
   28 1.815615   192.16
   29 1.819931   192.16
   30 1.825073   192.16
   31 1.826044   192.16
   32 1.936387   192.16
   33 1.937253   192.16

▷ Frame 18: 61 bytes on
▷ Ethernet II, Src: Hewl
▷ Internet Protocol Vers
▷ User Datagram Protocol
▷ Data (19 bytes)
```



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

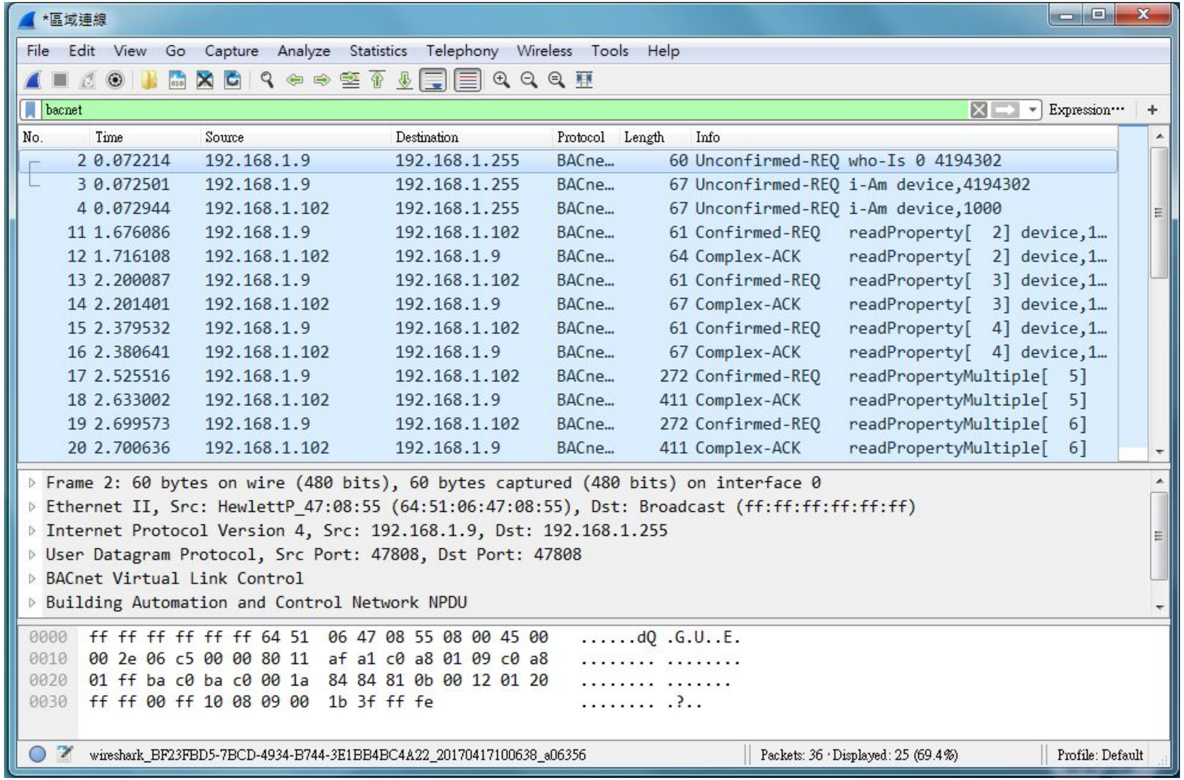

*區域連線
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

udp.port==47809

```
No.  Time       Source         Destination    Protocol Length Info
  18 1.075193   192.168.1.9    192.168.1.102  BACne...     61 Confirmed-REQ   readPrope...
  19 1.076055   192.168.1.102  192.168.1.9    BACne...     64 Complex-ACK     readPrope...
  22 1.575054   192.168.1.9    192.168.1.102  BACne...     59 Confirmed-REQ   readPrope...
  23 1.576242   192.168.1.102  192.168.1.9    BACne...     60 Error           readPrope...
  24 1.635092   192.168.1.9    192.168.1.102  BACne...     59 Confirmed-REQ   readPrope...
  25 1.636050   192.168.1.102  192.168.1.9    BACne...     60 Error           readPrope...
  26 1.705101   192.168.1.9    192.168.1.102  BACne...    234 Confirmed-REQ   readPrope...
  27 1.706771   192.168.1.102  192.168.1.9    BACne...    349 Complex-ACK     readPrope...
  28 1.815615   192.168.1.9    192.168.1.102  BACne...     59 Confirmed-REQ   readPrope...
  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 Confirmed-REQ   readPrope...
  31 1.826044   192.168.1.102  192.168.1.9    BACne...     60 Error           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。


*區域連線
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
bacnet
Expression…
+

```
No.  Time      Source         Destination    Protocol Length Info
   2 0.072214  192.168.1.9    192.168.1.255  BACne…      60 Unconfirmed-REQ who-Is 0 4194302
   3 0.072501  192.168.1.9    192.168.1.255  BACne…      67 Unconfirmed-REQ i-Am device,4194302
   4 0.072944  192.168.1.102  192.168.1.255  BACne…      67 Unconfirmed-REQ i-Am device,1000
  11 1.676086  192.168.1.9    192.168.1.102  BACne…      61 Confirmed-REQ   readProperty[  2] 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-REQ   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-REQ   readProperty[  4] device,1…
  16 2.380641  192.168.1.102  192.168.1.9    BACne…      67 Complex-ACK     readProperty[  4] device,1…
  17 2.525516  192.168.1.9    192.168.1.102  BACne…     272 Confirmed-REQ   readPropertyMultiple[  5]
  18 2.633002  192.168.1.102  192.168.1.9    BACne…     411 Complex-ACK     readPropertyMultiple[  5]
  19 2.699573  192.168.1.9    192.168.1.102  BACne…     272 Confirmed-REQ   readPropertyMultiple[  6]
  20 2.700636  192.168.1.102  192.168.1.9    BACne…     411 Complex-ACK     readPropertyMultiple[  6]
```

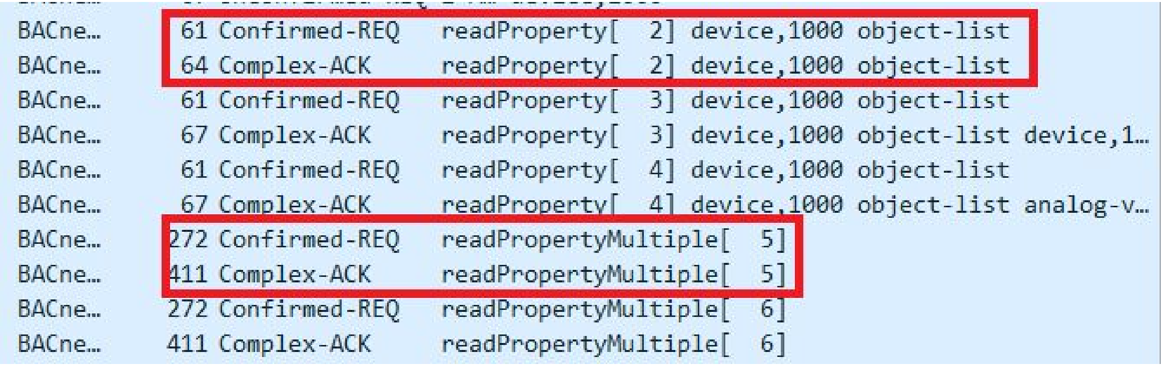
```
▷ Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▷ Ethernet II, Src: HewlettP_47:08:55 (64:51:06:47:08:55), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Internet Protocol Version 4, Src: 192.168.1.9, Dst: 192.168.1.255
▷ User Datagram Protocol, Src Port: 47808, Dst Port: 47808
▷ BACnet Virtual Link Control
▷ Building Automation and Control Network NPDU
```

```
0000  ff ff ff ff ff ff 64 51  06 47 08 55 08 00 45 00   ......dQ .G.U..E.
0010  00 2e 06 c5 00 00 80 11  af a1 c0 a8 01 09 c0 a8   ........ ........
0020  01 ff ba c0 ba c0 00 1a  84 84 81 0b 00 12 01 20   ........ .......
0030  ff ff 00 ff 10 08 09 00  1b 3f ff fe               ........ .?..
```

wireshark_BF23FBD5-7BCD-4934-B744-3E1BB4BC4A22_20170417100638_a06356 | Packets: 36 · Displayed: 25 (69.4%) | Profile: Default

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

如何判斷 BACnet Client 端過高頻率的發送封包

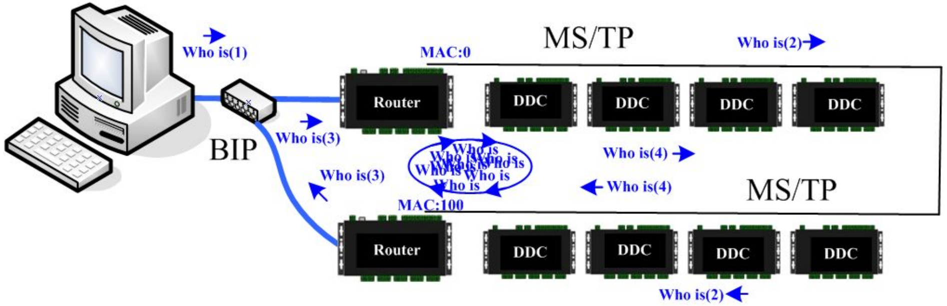
部分撰寫或設定不良的 BACnet Client 端圖控程式，可能為了滿足短時間或取大量的點數值的需求，而將讀取間隔時間設定過小。由於 BACnet/IP 始採用 UDP 方式通訊，因此這樣的封包可能很快塞滿網路，必須注意 BACnet/IP 網路能夠負荷的網路流量，不一定是 MS/TP 等較低頻寬網路所能負擔的。

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 ICDT BACnet MS/TP 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）

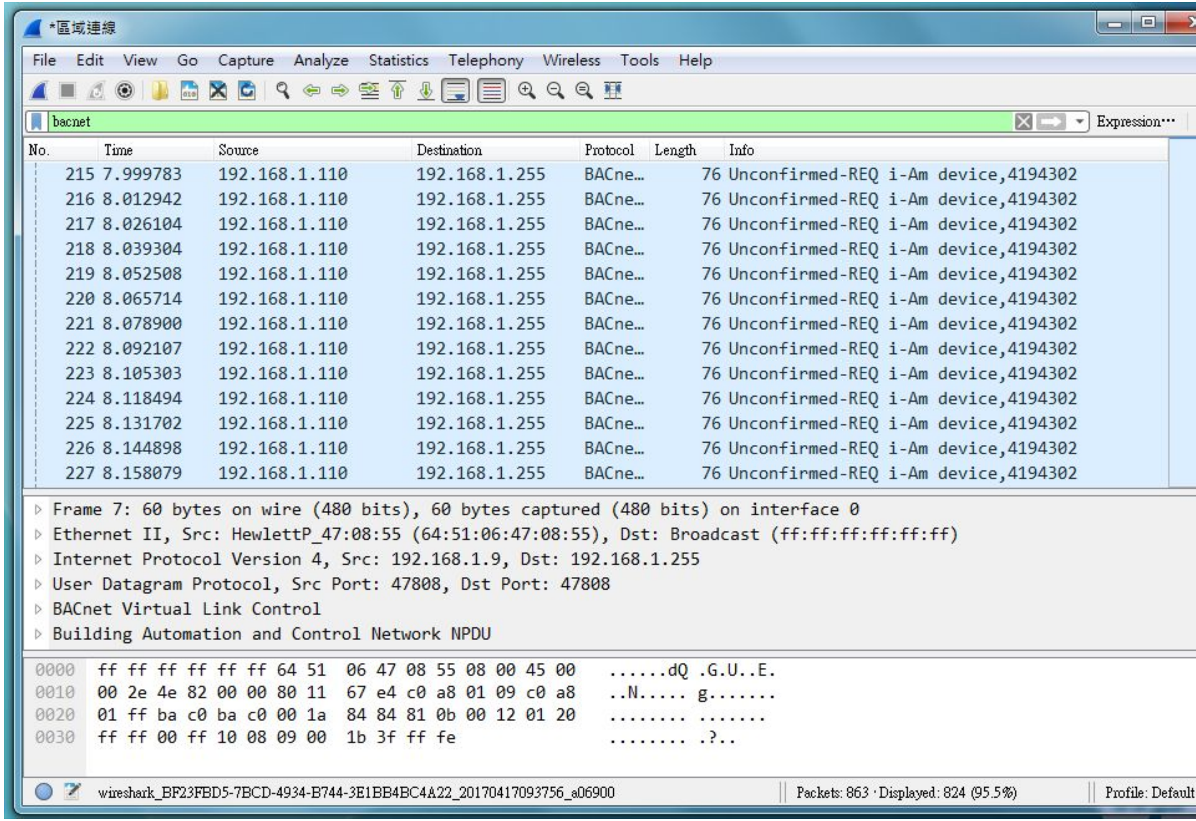
廣播風暴（Broadcast Storm）：BACnet Router 網路不可短循環，否則會造成廣播風暴，進而使網路過度忙碌而癱瘓。例如網路上同時有兩個 BACnet/IP 與 MS/TP 的 Router，又將其 MS/TP 網路線相連結，或者將具備兩個以上 MS/TP 迴路的 BACnet Router，將兩個 MS/TP 線路相接，如此一來會使 BACnet 廣播在兩個 Router 間不斷傳遞，造成網路壅塞。判斷此狀況可以從 BACnet/IP 網路端用 Wireshark 進行監看，如果同一(可能每秒數百個)時間產生大量相同的廣播，即可斷定此一狀況。

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 Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
bacnet
Expression…

```
No.  Time      Source         Destination    Protocol Length Info
 215 7.999783  192.168.1.110  192.168.1.255  BACne…      76 Unconfirmed-REQ i-Am device,4194302
 216 8.012942  192.168.1.110  192.168.1.255  BACne…      76 Unconfirmed-REQ i-Am device,4194302
 217 8.026104  192.168.1.110  192.168.1.255  BACne…      76 Unconfirmed-REQ i-Am device,4194302
 218 8.039304  192.168.1.110  192.168.1.255  BACne…      76 Unconfirmed-REQ i-Am device,4194302
 219 8.052508  192.168.1.110  192.168.1.255  BACne…      76 Unconfirmed-REQ i-Am device,4194302
 220 8.065714  192.168.1.110  192.168.1.255  BACne…      76 Unconfirmed-REQ i-Am device,4194302
 221 8.078900  192.168.1.110  192.168.1.255  BACne…      76 Unconfirmed-REQ i-Am device,4194302
 222 8.092107  192.168.1.110  192.168.1.255  BACne…      76 Unconfirmed-REQ i-Am device,4194302
 223 8.105303  192.168.1.110  192.168.1.255  BACne…      76 Unconfirmed-REQ i-Am device,4194302
 224 8.118494  192.168.1.110  192.168.1.255  BACne…      76 Unconfirmed-REQ i-Am device,4194302
 225 8.131702  192.168.1.110  192.168.1.255  BACne…      76 Unconfirmed-REQ i-Am device,4194302
 226 8.144898  192.168.1.110  192.168.1.255  BACne…      76 Unconfirmed-REQ i-Am device,4194302
 227 8.158079  192.168.1.110  192.168.1.255  BACne…      76 Unconfirmed-REQ i-Am device,4194302
```

```
▷ Frame 7: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▷ Ethernet II, Src: HewlettP_47:08:55 (64:51:06:47:08:55), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Internet Protocol Version 4, Src: 192.168.1.9, Dst: 192.168.1.255
▷ User Datagram Protocol, Src Port: 47808, Dst Port: 47808
▷ BACnet Virtual Link Control
▷ Building Automation and Control Network NPDU
```

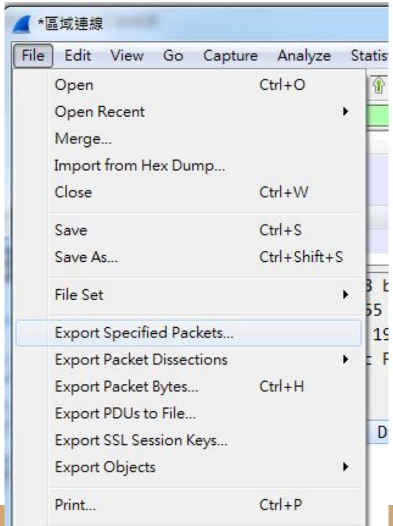
```
0000  ff ff ff ff ff ff 64 51  06 47 08 55 08 00 45 00   ......dQ .G.U..E.
0010  00 2e 4e 82 00 00 80 11  67 e4 c0 a8 01 09 c0 a8   ..N..... g.......
0020  01 ff ba c0 ba c0 00 1a  84 84 81 0b 00 12 01 20   ........ .......
0030  ff ff 00 ff 10 08 09 00  1b 3f ff fe               ........ .?..
```

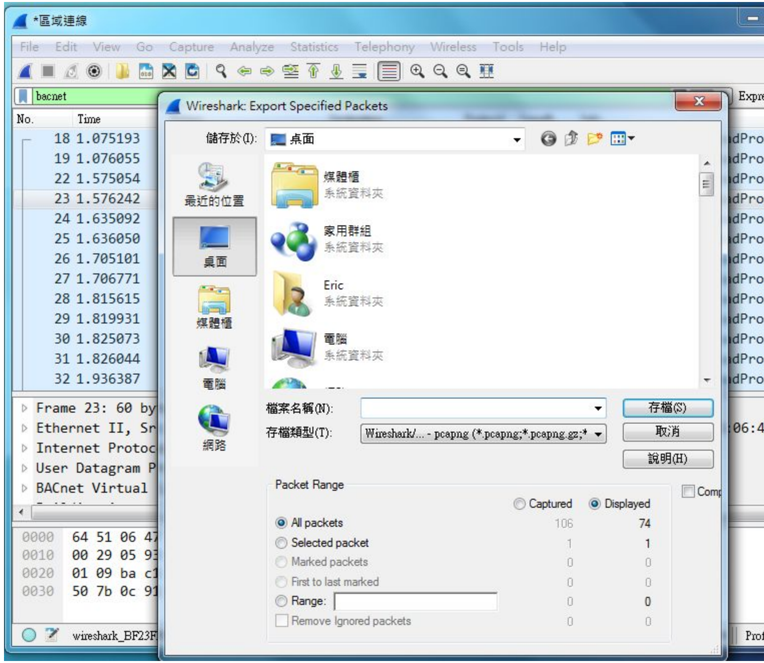
```
wireshark_BF23FBD5-7BCD-4934-B744-3E1BB4BC4A22_20170417093756_a06900 || Packets: 863 · Displayed: 824 (95.5%) || Profile: Default
```

儲存記錄

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。




*區域連線
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
bacnet
Wireshark: Export Specified Packets
儲存於(I): 桌面
最近的位置
桌面
媒體櫃
電腦
網路
媒體櫃 系統資料夾
家用群組 系統資料夾
Eric 系統資料夾
電腦 系統資料夾
檔案名稱(N):
存檔類型(T): Wireshark/... - pcapng (*.pcapng;*.pcapng.gz;*
存檔(S)
取消
說明(H)

```
No.  Time
 18 1.075193
 19 1.076055
 22 1.575054
 23 1.576242
 24 1.635092
 25 1.636050
 26 1.705101
 27 1.706771
 28 1.815615
 29 1.819931
 30 1.825073
 31 1.826044
 32 1.936387
```

```
▷ Frame 23: 60 by
▷ Ethernet II, Sr
▷ Internet Protoc
▷ User Datagram P
▷ BACnet Virtual
```

```
0000  64 51 06 47
0010  00 29 05 93
0020  01 09 ba c1
0030  50 7b 0c 91
```

Packet Range

	○ Captured	● Displayed
● All packets	106	74
○ Selected packet	1	1
○ Marked packets	0	0
○ First to last marked	0	0
○ Range:	0	0
□ Remove Ignored packets	0	0

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/components/search-component/search?searchword=bacnet&searchphrase=all

例如 BACnet 網路問題分析 與 關於 BACnet 的重要網址連結 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 eric.icdt@msa.hinet.net，更進一步資訊請上元米網站 http://www.icdt.com.tw