如何使用 wireshark 觀察 BACnet MS/TP 通訊封包

元米科技 2017/6/19

本文目的

本文的對象是針對應用 BACnet MS/TP 通訊，但不熟悉 BACnet MS/TP 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 MS/TP 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 MS/TP Recorder 免費軟體搭配 RS485 轉換器記錄通訊內容，並匯出至 Wireshark 的分析結果。

實驗時必須搭配現有 BACnet MS/TP 網路設備，由於電腦無法直接接收速率 76800bps 的封包，因此如有此需求必須搭配 全芯智聯(www.tbacnet.com)的專用轉換器才能達成。

關於 wireshark

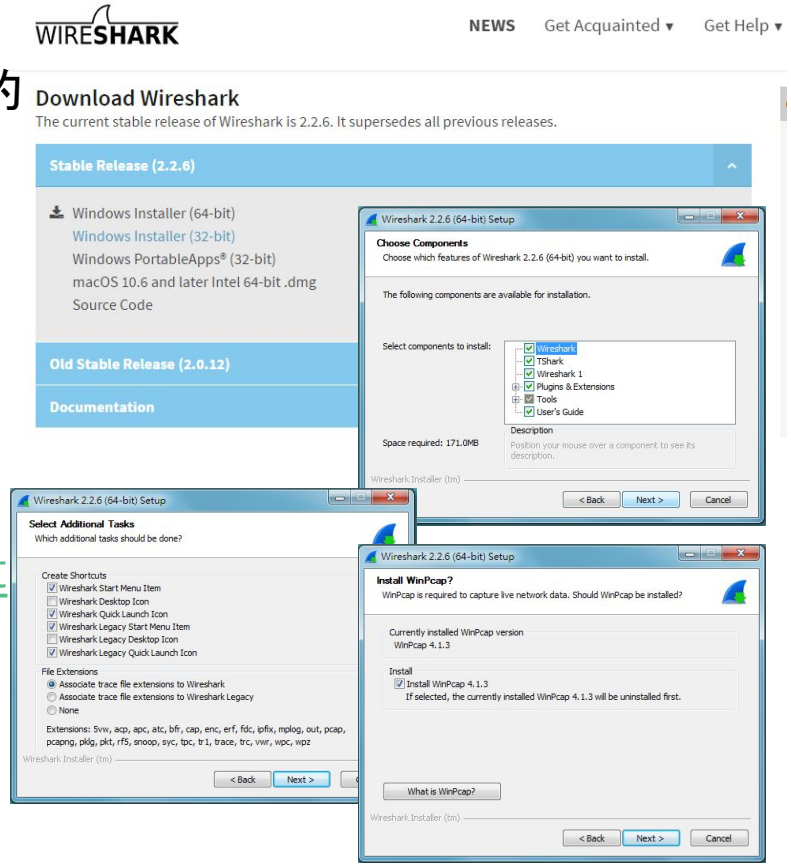
維基百科：Wireshark（前稱Ethereal）是一個免費開源的網路封包分析軟體。網路封包分析軟體的功能是截取網路封包，並盡可能顯示出最為詳細的網路封包資料。
在過去，網路封包分析軟體是非常昂貴，或是專門屬於營利用的軟體，Wireshark的出現改變了這一切。在GNU通用公眾授權條款的保障範圍底下，使用者可以以免費的代價取得軟體與其程式碼，並擁有針對其原始碼修改及客製化的權利。Wireshark是目前全世界最廣泛的網路封包分析軟體之一。

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。

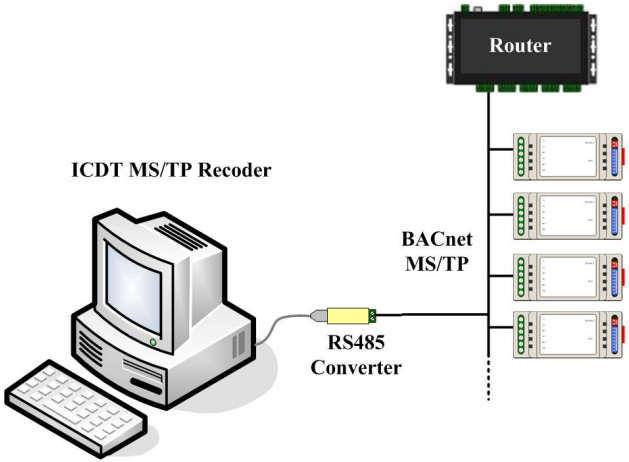
安裝時必須安裝於預設的 "C:\Program Files\Wireshark" 路徑下以正常執行。

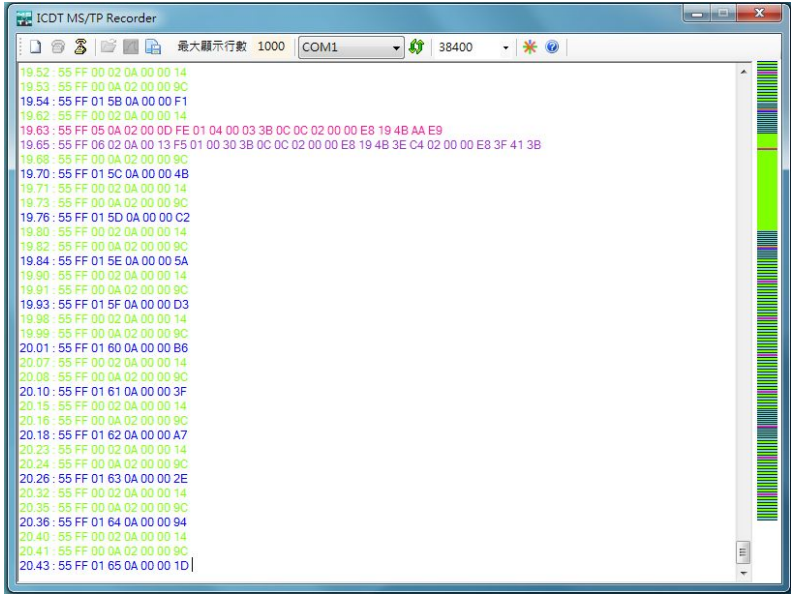
Wireshark 下載處:https://www.wireshark.org/download.html



安裝 ICDT MS/TP Recorder 免費軟體

- 自 元米科技下載並安裝 最新版 ICDT MS/TP Recorder 免費軟體
- 透過 RS485轉換器將 MS/TP 連接至電腦
- 選擇正確的 COM後開啟通訊
- 通訊內容可儲存並再次開啟





使用專用 USB MS/TP 轉換器

由於電腦的無法直接支援 76800 bps 傳輸速率，因此使用一般的RS485轉換器並不能監看 76800 bps 的網路狀態。

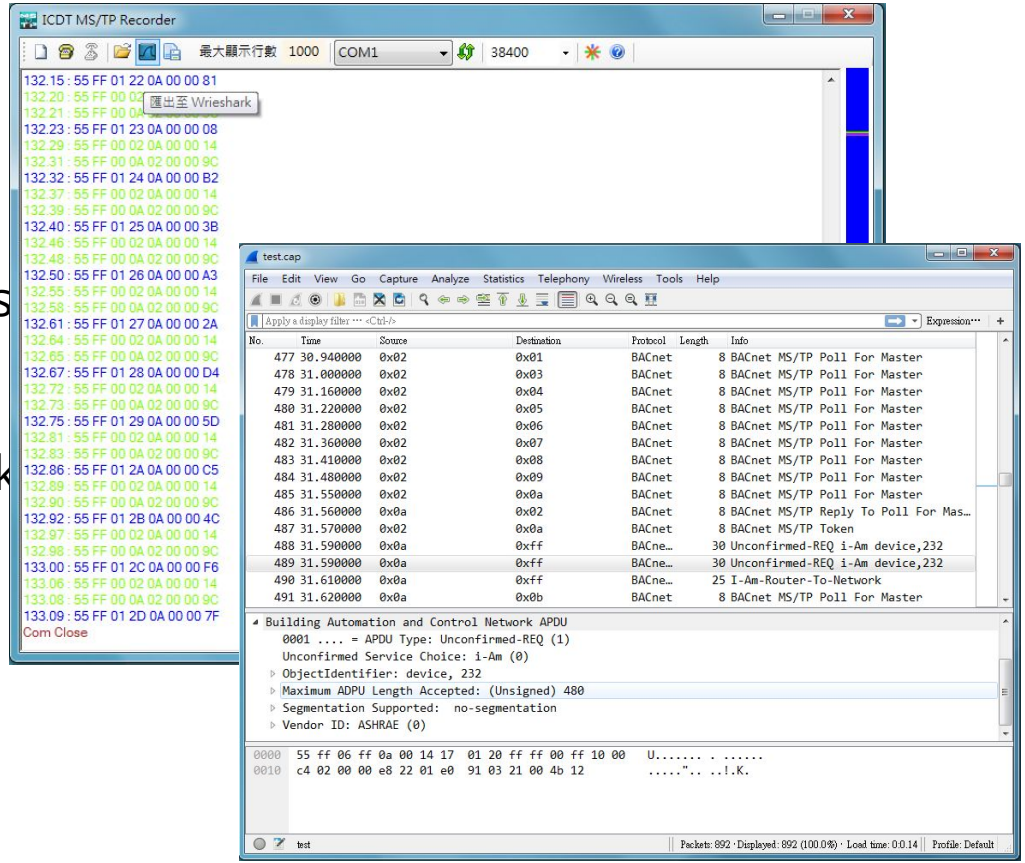
元米科技 與 全芯智聯(www.tbacnet.com/) 合作之 USB MS/TP 轉換器，除了可以直接搭配 ICDT BACnet Pioneer 與 ICDT WEB HMI 連接 MS/TP 網路設備，也可以做為 ICDT MS/TP Recorder 的 MS/TP 轉換器。當選擇通訊的 COM 設備為專用的 USB MS/TP 轉換器時，速率選擇欄位會被隱藏，轉換器將自動偵測正確的通訊速率。此轉換器適用的速率為 9600/19200/38400/76800 四種。

匯出至Wireshark

關閉通訊後按下"匯出至 Wireshark"可將內容匯出至 Wireshark，如需要保存，則於Wireshark->File->Save As另存新檔即可。

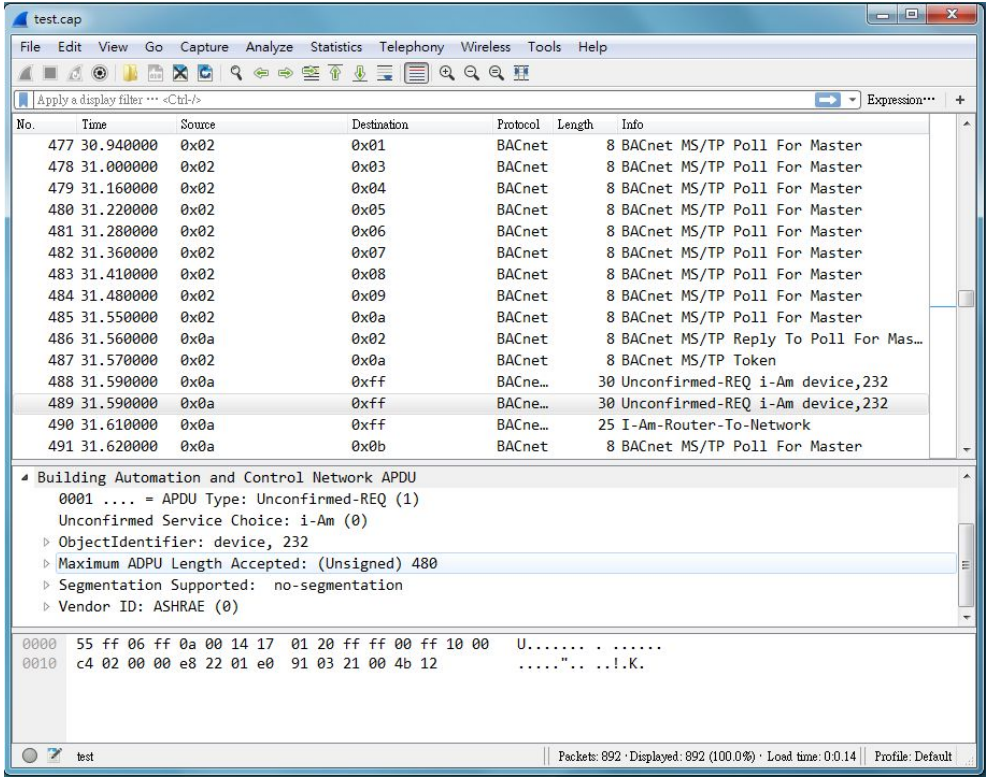
如果無法正常匯出，請確認Wireshark是否安裝在 "C:\Program Files\Wireshark\Wireshark.exe"

Wireshark 關閉後才能再匯出。



試著解讀 BACnet MS/TP 封包

記錄的封包包含時間(Time)、來源MAC(Source)、目的MAC(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。



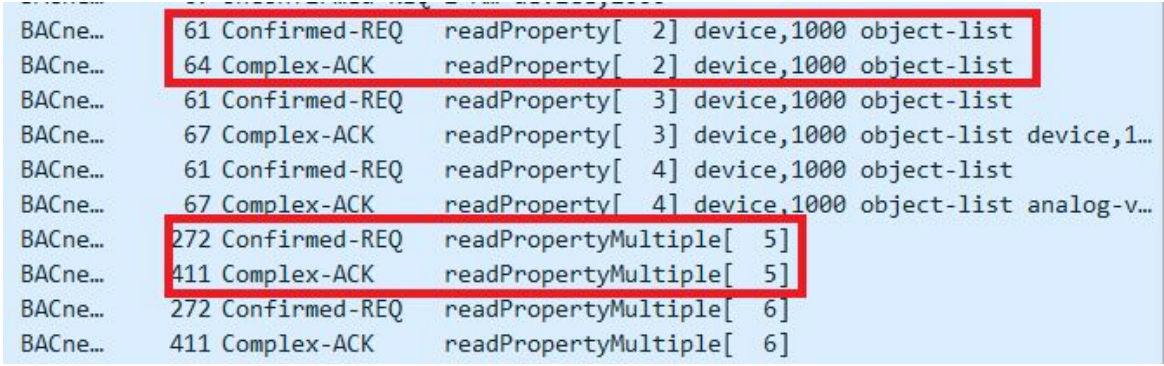
MS/TP封包 的類型

- 00 Token : 將全杖(Token)給目的 MAC 設備
- 01 Poll For Master : 詢問目的 MAC 設備是否存在
- 02 Reply To Poll For Master : 回覆 Poll For Master 的詢問
- 03 Test_Request : 測試詢問
- 04 Test_Response : 回覆 Test_Request 的詢問
- 05 BACnet Data Expecting Reply : 預期回覆的封包
- 06 BACnet Data Not Expecting Reply : 不需回覆(或回覆BACnet Data Expecting Reply) 的封包
- 07 Reply Postponed : 延遲回覆(針對 BACnet Data Expecting Reply 無法即時回覆)

以上僅 05 與 06 帶有資料(NPDU)，否則一律只有固定長度 8 的 MS/TP 層資料交握

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。



依照顏色柱快速判斷網路狀態

MS/TP Recorder 記錄通訊時會依照封包類型顯示顏色，並將顏色顯示於右側狀態柱中，以利快速判斷網路狀況，說明如下：

- 出現綠色塊狀(Token)或藍、綠交錯為正常通訊，無資料傳輸
- 出現藍色區塊(Poll For Master)為 Token 傳遞不順，影響通訊品質
- 粉紅(BACnet Data Expecting Reply)與紫色(BACnet Data Not Expecting Reply)成塊狀顯示越多，表示網路資料越忙碌
- 紅色為錯誤封包，成塊狀顯示可能為網路異常或速率選擇錯誤

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