Taiwan Power Research Institute TPRI

IEC 61850標準相關通訊協定分析

林哲毅
電力研究室
台電綜合研究所
June 29, 2015

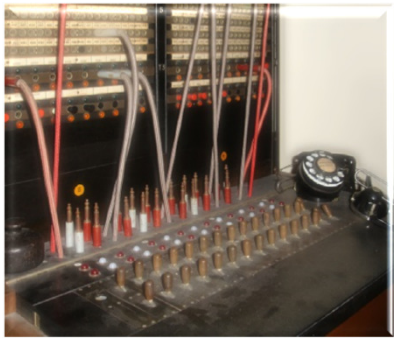
Contents

資料擷取系統之通訊演進

1930以前

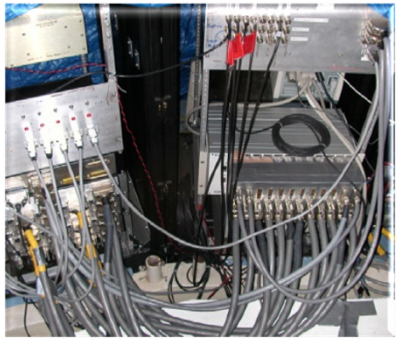
運轉員必須使用電話傳達變電所投切訊息

1930年代



利用電話線使運轉員遠端監控現場少許點數

1960年代



利用資料擷取系統傳達變電所量測資料，但有頻寬限制

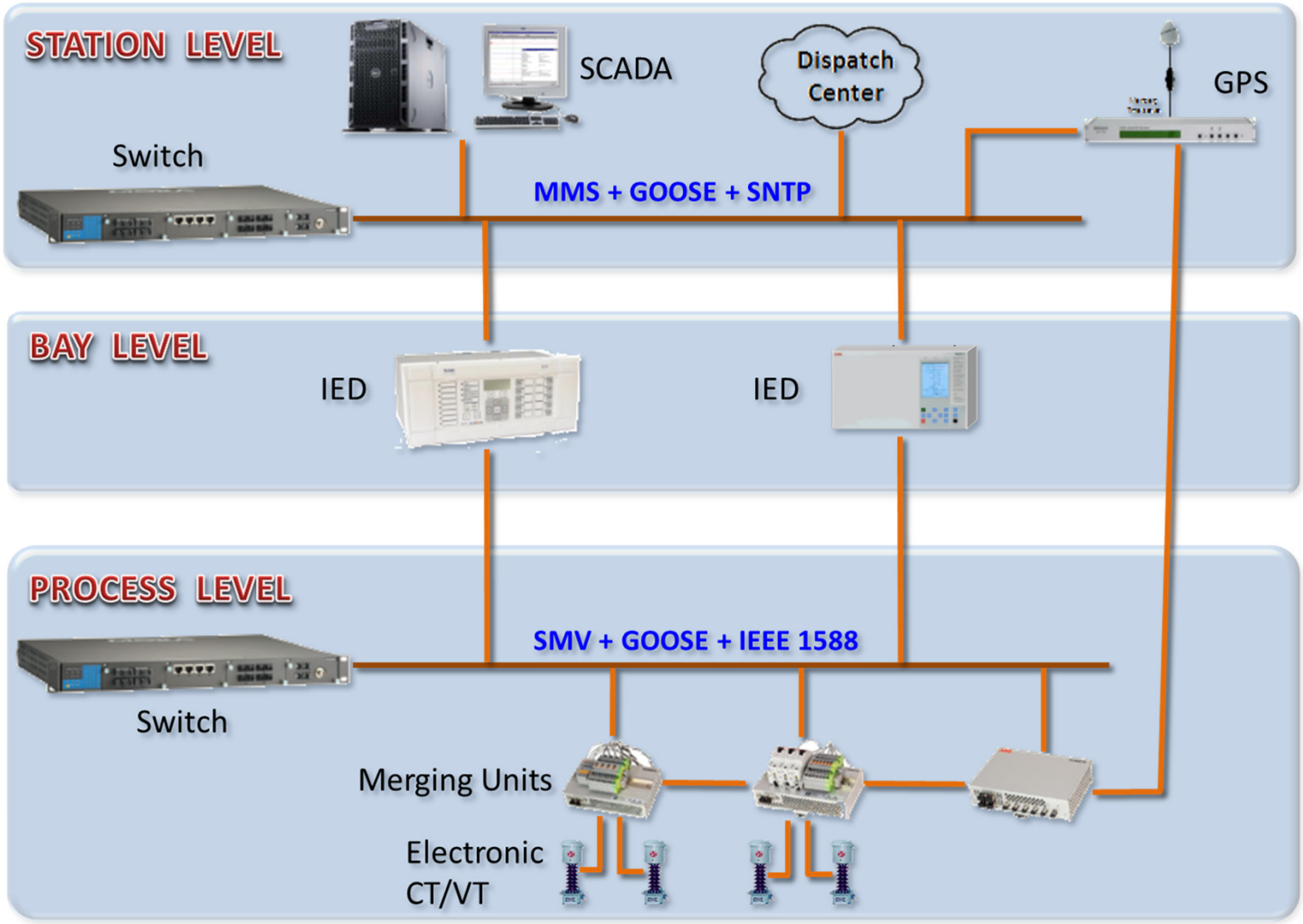
1980年代

頻寬不再有限制，並具備處理數千個類比及數位訊號能力

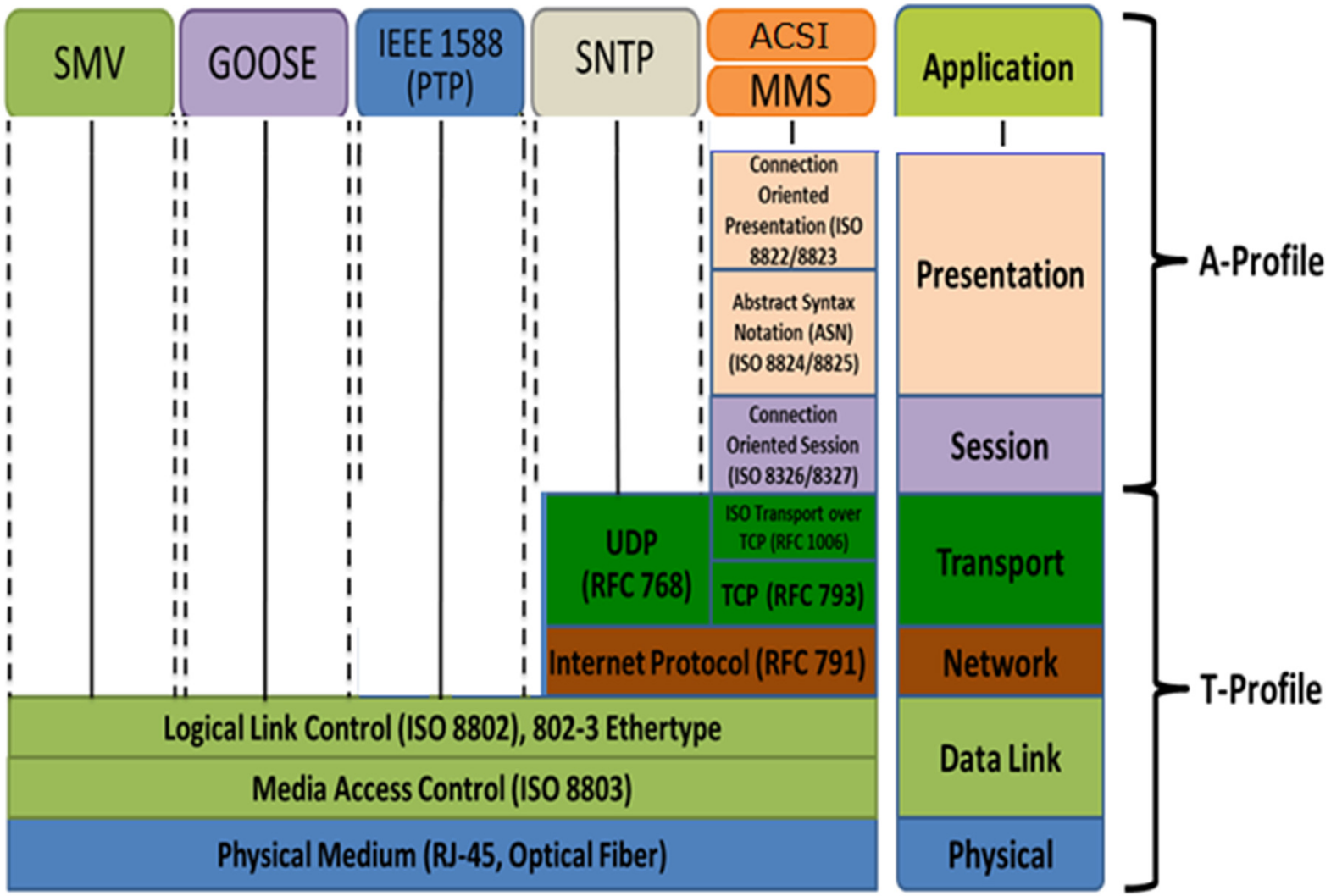
UCA所制定之變電所自動化要件

1. 高速IED對IED點對點通訊
2. 變電所內所有通訊網路的集中管理
3. 封包傳遞時間保證
4. 統一標準
5. 多設備商設備的互用性
6. 支援數位電壓電流訊號傳輸
7. 支援檔案傳輸(File Transfer)
8. 支援安全防護(Security)

IEC 61850 架構及資料傳輸

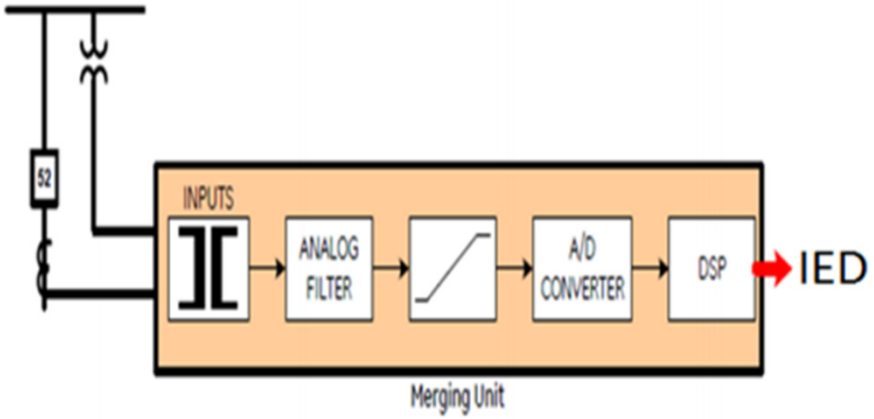


IEC 61850 封包種類及其協定



電壓電流採樣數值(SMV)

- 利用合併單元同步採集三相電流和電壓輸出的類比訊號、通過類比數位轉換器(A/D Converter)轉為IEC 61850-9-2所規定的SMV數位訊號讓所需要的IED存取



- IEC 61850-9-1的標準已被IEC於61850 Ed.2中廢除
- IEC 61850-9-2 Light Edition (LE)的制定

物件導向事件快速傳輸(GOOSE)

- 當事故發生時，IED必須及時發送訊號通知另一IED採取相對應的動作，因此IED間的資料必須是快速且正確的
- 而IEC 61850-8-1中定義使用GOOSE (Generic Object Oriented Substation Event)為IED間的資料傳輸協定
- 為了加速訊息傳遞速度，GOOSE將應用層中的資料放在資料連結層後通過實體層傳出

精密時間協定(IEEE 1588)

- IEEE 1588是專門為了工業網路量測與控制系統所特別開發的乙太網路時間同步技術
- 只有主鐘會連結到GPS或其他同步時間源已取得精確的時間做為同步的基準
- 精準度可到達1μs

簡單網路時間協定(SNTP)

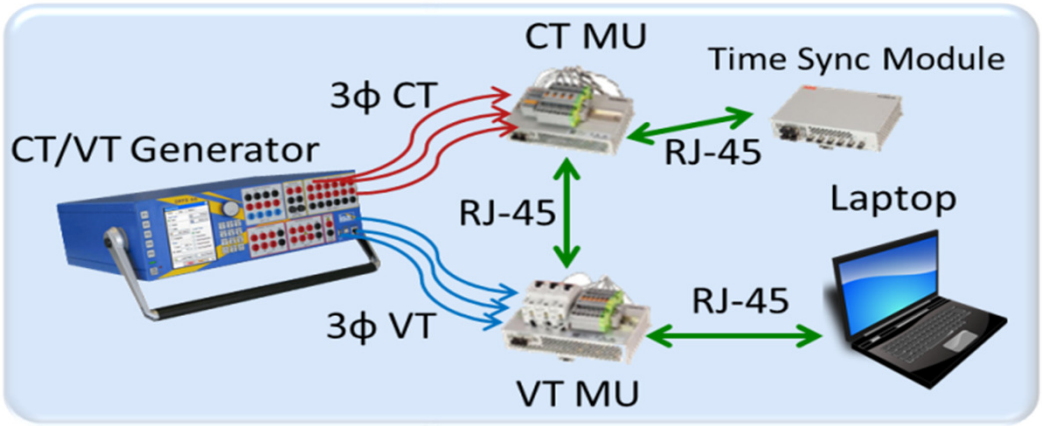
- 用於SCADA等時間精準度並沒有太大要求的設備
- SNTP是基於在NTP version 3上的乙太網路時間同步協定，卻簡化了客戶端與伺服器端之間的存取
- 其精準度約為1ms
- 工作模式可分為(1)多播/廣播模式(2)程序呼叫模式(3)程序呼叫模式

製造商訊息規範(MMS)

- MMS是個用來交換即時資料與監控訊息的國際協定
- MMS也對於在網路上的即時監控資料做了特別設計，利用VMD(Virtual Manufacturing Device)的架構讓使用者可自行設定要使用簡單或複雜的伺服器/客戶端環境
- VMD的概念主要是讓一個設備同時具備伺服器與客戶端的能力，並事情況去調整角色

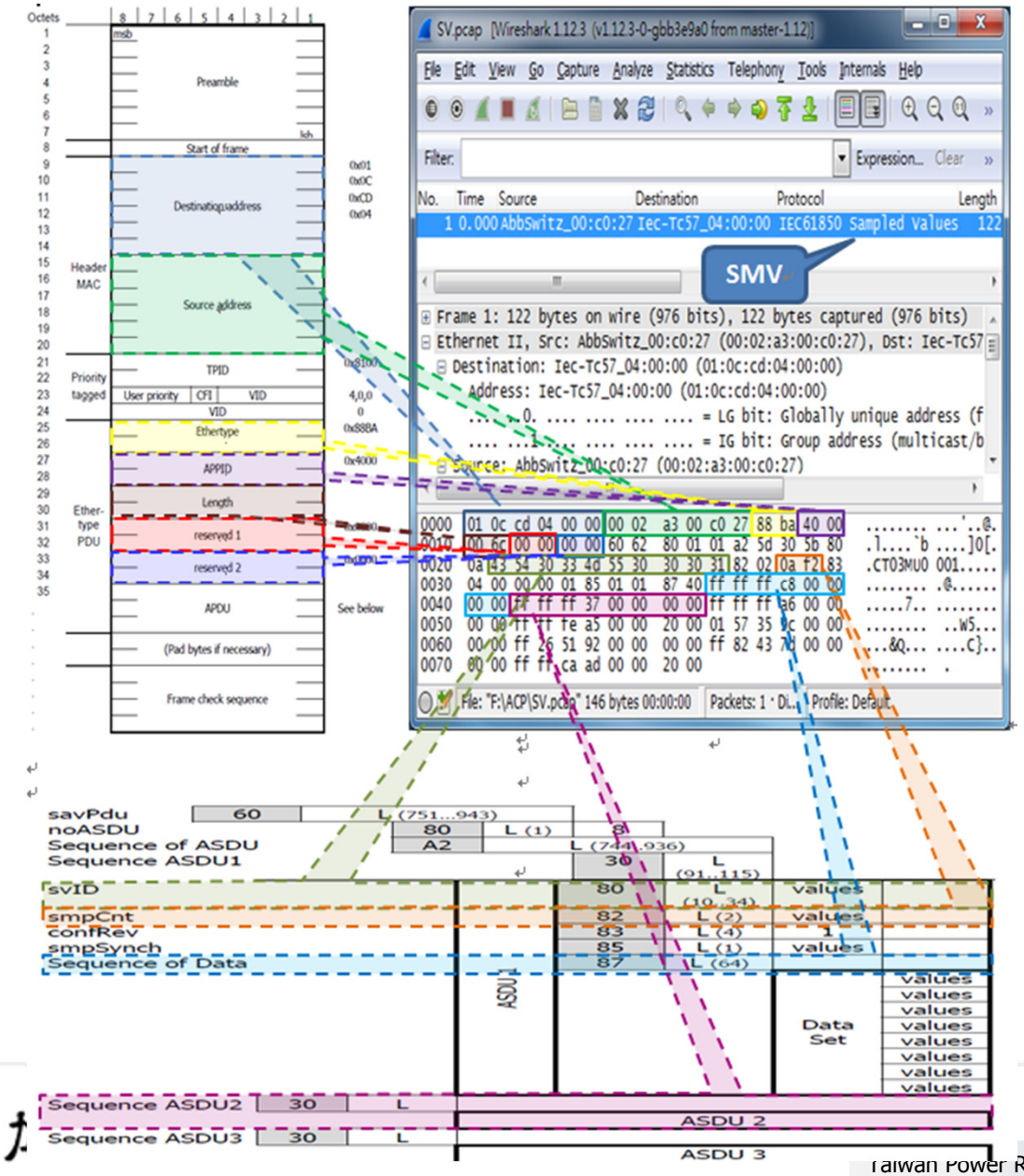
SMV 封包測試與解析

- SMV封包擷取測試環境



- 在IEC 61850-9-2 LE規範中的Appendix A明確的規劃出SMV所使用的 ISO/IEC 8802-3的乙太網路封包格式及其以ASN.1 BER 為基礎的 APDU 之架構

SMV 封包測試與解析


Octets
Preamble
Start of frame
Destination address
Source address
Header MAC
TPID
Priority tagged
User priority
CFI
VID
Ethertype
APPID
Length
reserved 1
reserved 2
Ether-type PDU
APDU
(Pad bytes if necessary)
Frame check sequence
See below
SV.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear
No. Time Source Destination Protocol Length
1 0.000 AbbSwitz_00:c0:27 Iec-Tc57_04:00:00 IEC61850 Sampled Values 122
SMV
Frame 1: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
Ethernet II, Src: AbbSwitz_00:c0:27 (00:02:a3:00:c0:27), Dst: Iec-Tc57
Destination: Iec-Tc57_04:00:00 (01:0c:cd:04:00:00)
Address: Iec-Tc57_04:00:00 (01:0c:cd:04:00:00)
Source: AbbSwitz_00:c0:27 (00:02:a3:00:c0:27)
File: "F:\ACP\SV.pcap" 146 bytes 00:00:00
Packets: 1 · Di...
Profile: Default
savPdu
noASDU
Sequence of ASDU
Sequence ASDU1
svID
smpCnt
confRev
smpSynch
Sequence of Data
Data Set
values
ASDU 1
Sequence ASDU2
Sequence ASDU3
ASDU 2
ASDU 3

SMV 封包測試與解析

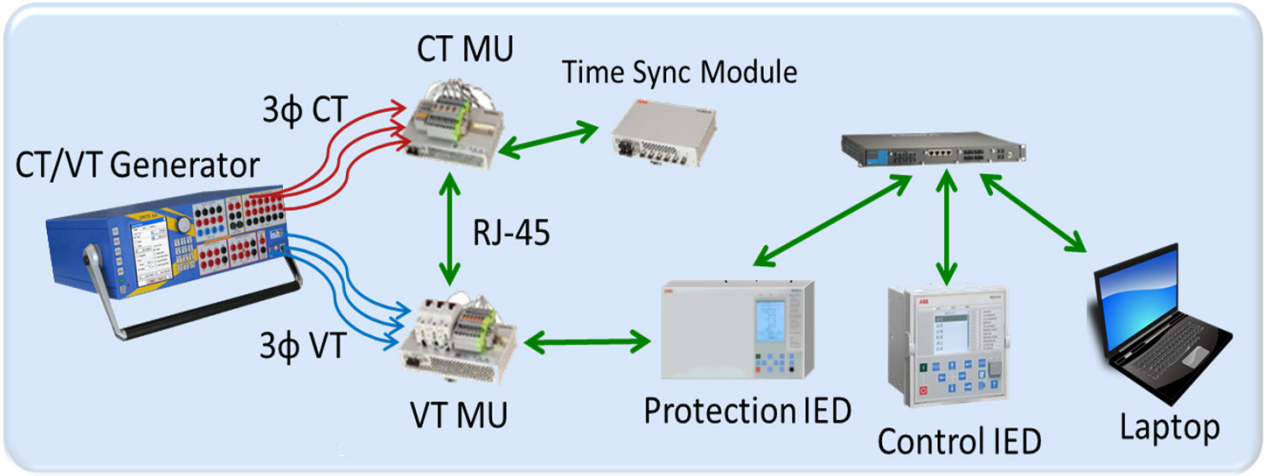
- 每個ASDU包含一個資料集，而每個資料集的長度為128個byte，內容依序為
  - TCTR1.Amp.instMag.i、TCTR1.Amp.q、
    TCTR2.Amp.instMag.i、TCTR2.Amp.q、
    TCTR3.Amp.instMag.i、TCTR3.Amp.q、
    TCTR4.Amp.instMag.i、TCTR4.Amp.q、
    TVTR1.Vol.instMag.i、TVTR1.Vol.q、
    TVTR2.Vol.instMag.i、TVTR2.Vol.q、
    TVTR3.Vol.instMag.i、TVTR3.Vol.q、
    TVTR4.Vol.instMag.i、TVTR4.Vol.q
- 其CT、VT的數值為具方向性的浮點數，故需使用二補數(Two’s Complement)去計算。
- 而訊號品質方面0x00000000為正常(Good)，0x00000010為斷訊(Bad)，0x00000020則為MU系統計算值(Derived)

SMV 封包測試與解析

- 本次實驗所擷取到的ASDU內容為：
  - TCTR1.Amp.instMag.i：-56 (0xFFFFFFC8)
  - TCTR1.Amp.q：Good (0x00000000)
  - TCTR2.Amp.instMag.i：-201 (0xFFFFFF37)
  - TCTR2.Amp.q：Good (0x00000000)
  - TCTR3.Amp.instMag.i：-90 (0xFFFFFFA6)
  - TCTR3.Amp.q：Good (0x00000000)
  - TCTR4.Amp.instMag.i：-347 (0xFFFFFEA5)
  - TCTR4.Amp.q：Derived (0x00000020)
  - TVTR1.Vol.instMag.i：22492572 (0x0157359C)
  - TVTR1.Vol.q：Good (0x00000000)
  - TVTR2.Vol.instMag.i：-14265966 (0xFF265192)
  - TVTR2.Vol.q：Good (0x00000000)
  - TVTR3.Vol.instMag.i：-8240259 (0xFF82437D)
  - TVTR3.Vol.q：Good (0x00000000)
  - TVTR4.Vol.instMag.i：-13651 (0xFFFFCAAD)
  - TVTR4.Vol.q：Derived (0x00000020)

GOOSE 封包測試與解析

- GOOSE封包擷取測試環境



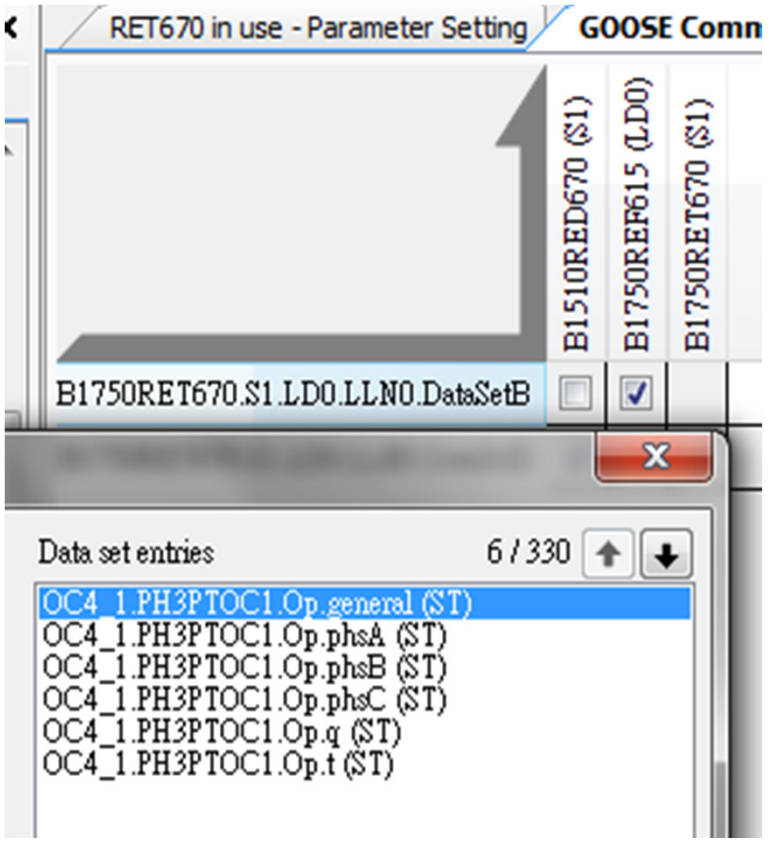
- 在IED規劃方面，將過流保護PTOC邏輯節點的三相的電流閥值設為IBase+30，一旦超過此值，保護用IED 將會發送GOOSE訊號至控制用IED

GOOSE 封包測試與解析

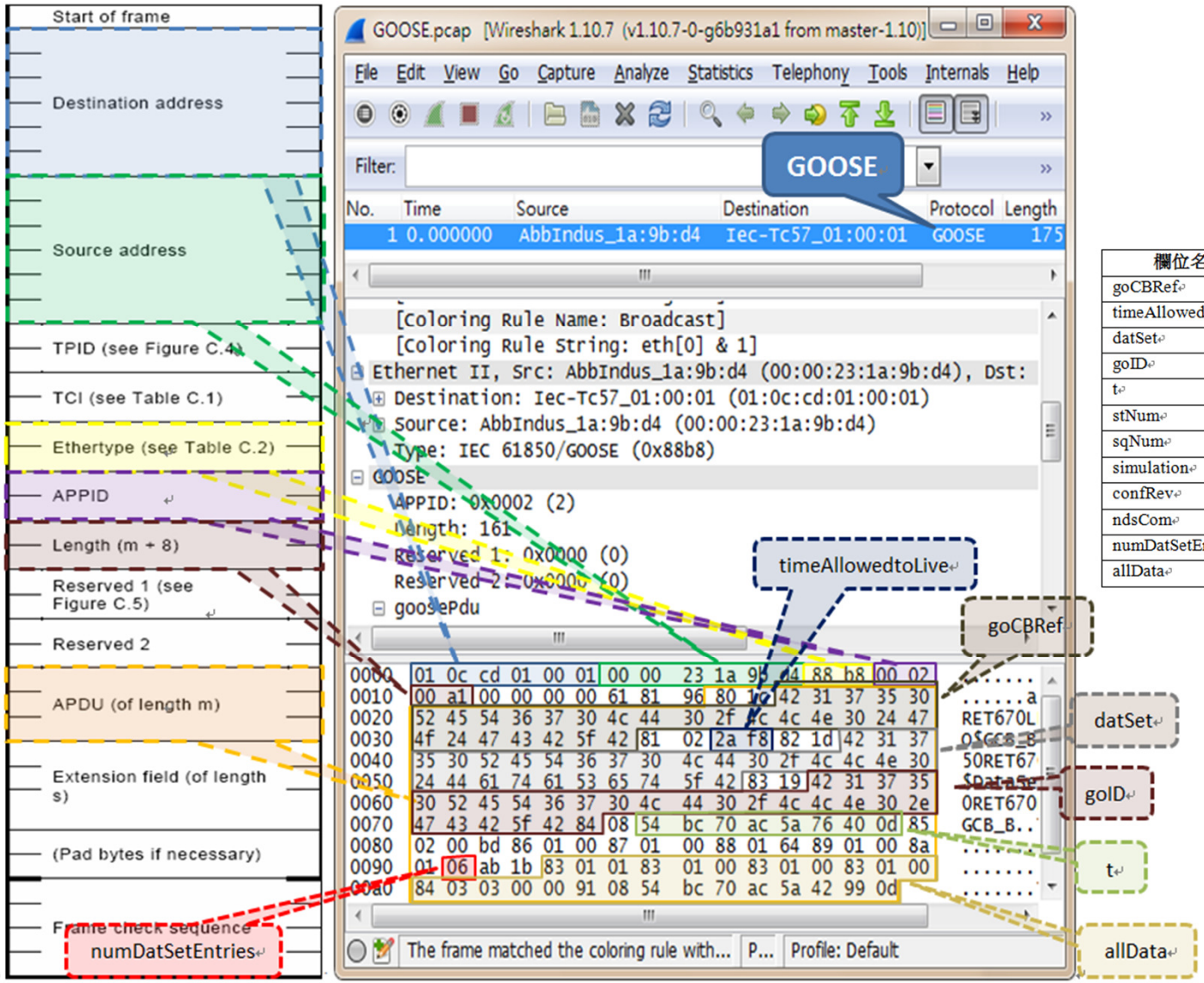
RET670 in use - Parameter Setting

Group / Parameter Name	IED Valu	PC Value	Unit	Min	Max
GBASVAL: 1					
UBase		161.00	kV	0.05	2000.00
IBase		300	A	1	99999
SBase		30.00	MVA	1.00	200000.00

Group / Parameter Name	IED Valu	PC Value	Unit	Min	Max
OC4PTOC: 1					
General					
GlobalBaseSel		1		1	12
MeasType		RMS			
Setting Group1					
Operation		On			
StartPhSel		1 out of 3			
Step 1					
Setting Group1					
DirMode1		Non-directional			
Characterist1		IEC Def. Time			
I1>		30	%IB	5	2500
t1		0.000	s	0.000	60.000
IMin1		100	%IB	1	10000
I1Mult		1.0		1.0	10.0



GOOSE 封包測試與解析



GOOSE 應用層 APDU 封包架構[8]

欄位名稱	封包格式
goCBRef	IMPLICIT VISIBLE-STRING
timeAllowedtoLive	IMPLICIT INTEGER
datSet	IMPLICIT VISIBLE-STRING
goID	IMPLICIT VISIBLE-STRING OPTIONAL
t	IMPLICIT UtcTime
stNum	IMPLICIT INTEGER
sqNum	IMPLICIT INTEGER
simulation	IMPLICIT BOOLEAN DEFAULT FALSE
confRev	IMPLICIT INTEGER
ndsCom	IMPLICIT BOOLEAN DEFAULT FALSE
numDatSetEntries	IMPLICIT INTEGER
allData	IMPLICIT SEQUENCE OF Data

GOOSE 封包測試與解析

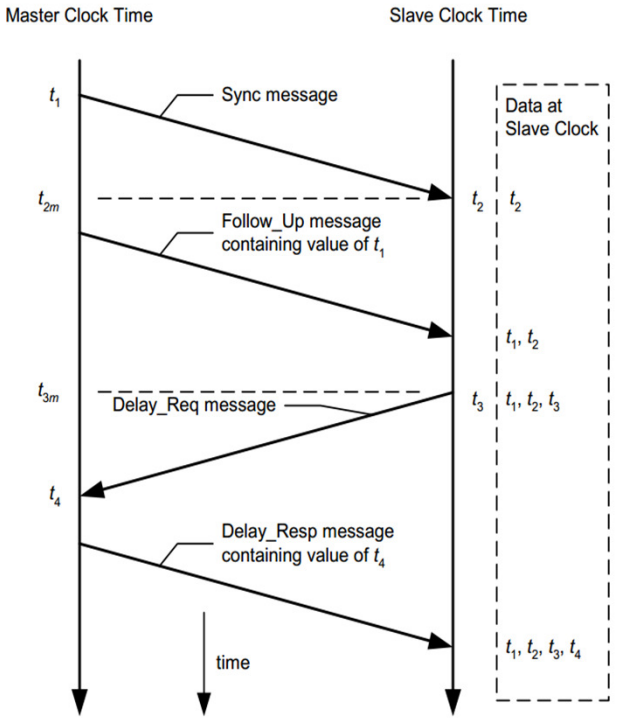
欄位名稱	欄位值	封包解析
goCBRef	B1750RET670LD0/LLN0GOGCB_B	為此GOOSE封包所連結到的Goose Control Block (GoCB)，格式為「邏輯設備/GoCB位址」
datSet	B1750RET670LD0/LLN0$DataSet_B	為GoCB所包含的資料集位址，格式為「邏輯設備/資料集位址」
t	Jan19, 2015 02:49:16.353366851 UTC	t為GOOSE封包所傳出的UTC時間標籤
numDatSetEntries	6	為GoCB的DataSet資料量。

GOOSE 封包測試與解析

欄位名稱	欄位值	封包解析
allData	Data: boolean : True Data: boolean: False Data: boolean: False Data: boolean: False Data: bit-string Bit-string: 0x000000000000 Data: utc-time: Jan 19,2015 02:49.16.352578699UTC	上述DataSet中的每項資料都會依照這些資料的格式及順序傳出其偵測點的值，因本實驗DataSet包含6項資料，故allData也會有6個值。

IEEE 1588 封包測試與解析

- IEEE 1588的工作流程與其他時間同步機制比較算是相對複雜，需要主鐘與從鐘不斷的溝通交換訊息以計算並回補傳輸時間的誤差值
- 2002年發布的PTPv1與2008年改版後的PTPv2差別主要在於v2導入了透明時鐘的概念，將交換器的處理時間也考慮在內，進一步的減少主從鐘之間的誤差值



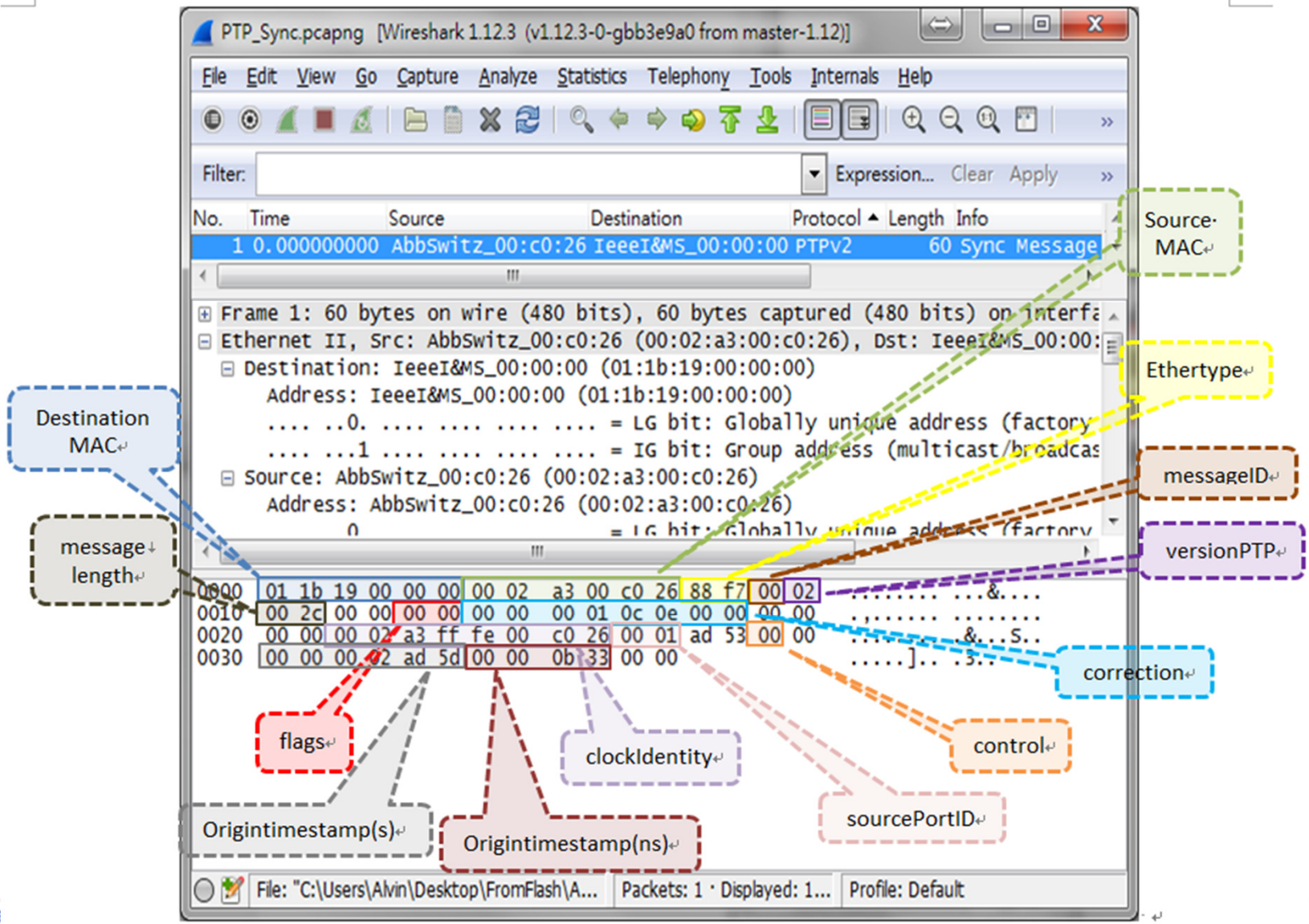
IEEE 1588 封包測試與解析

- 主鐘與從鐘的校對過程中需要四種不同資料型態的傳輸，其為Sync、Follow_Up、Delay_Req與Delay_Resp
- IEEE 1588 的實驗環境架設方面，我們將一台連接GPS的主鐘與一台與負責所有 MU 間的同步 MU TS模組相連，再將此MU時間同步模組與CT/VT的MU串起

IEEE 1588 PTPv2 應用層資料結構

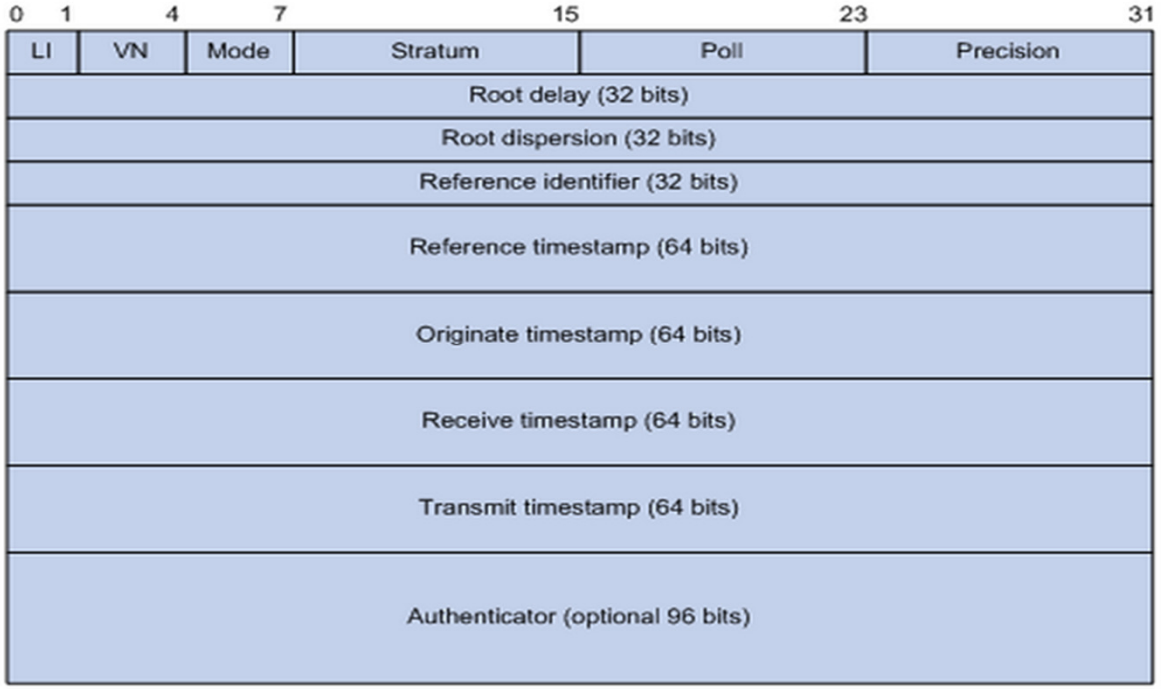
Bits								Octets	Offset
7	6	5	4	3	2	1	0		
transportSpecific				messageType				1	0
reserved				versionPTP				1	1
messageLength								2	2
domainNumber								1	4
reserved								1	5
flags								2	6
correctionField								8	8
reserved								4	16
sourcePortIdentity								10	20
sequenceId								2	30
controlField								1	32
logMessageInterval								1	33

IEEE 1588 封包測試與解析

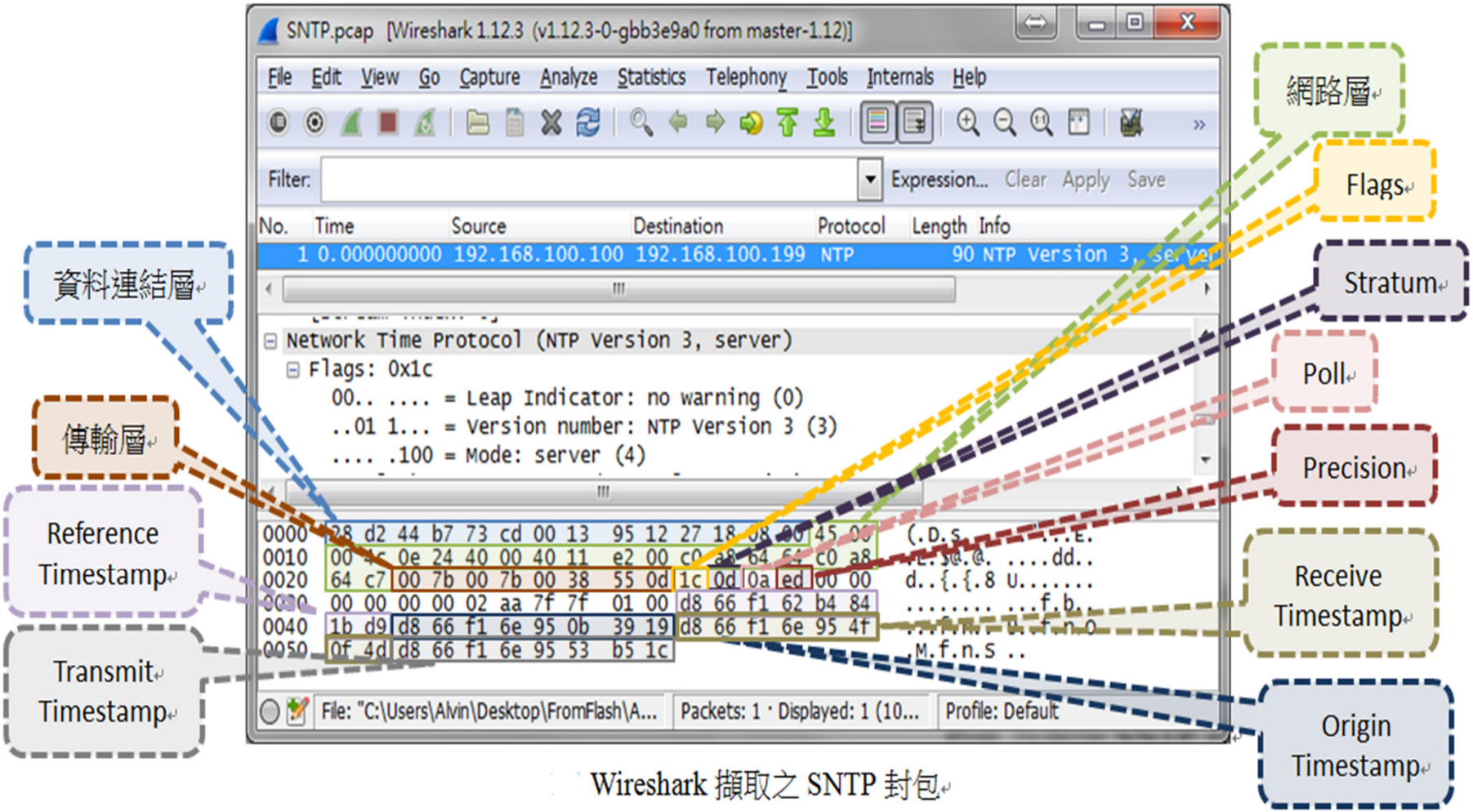


SNTP 封包測試與解析

- 實驗室購買之主鐘支援多種時間同步協定，包含IEEE 1588、1PPS、SNTP、IRIG-B等，在SNTP封包擷取的實驗環境架設上只須將主鐘的SNTP IP位址設定好即可使電腦與此主鐘執行時間同步的動作



SNTP 封包測試與解析



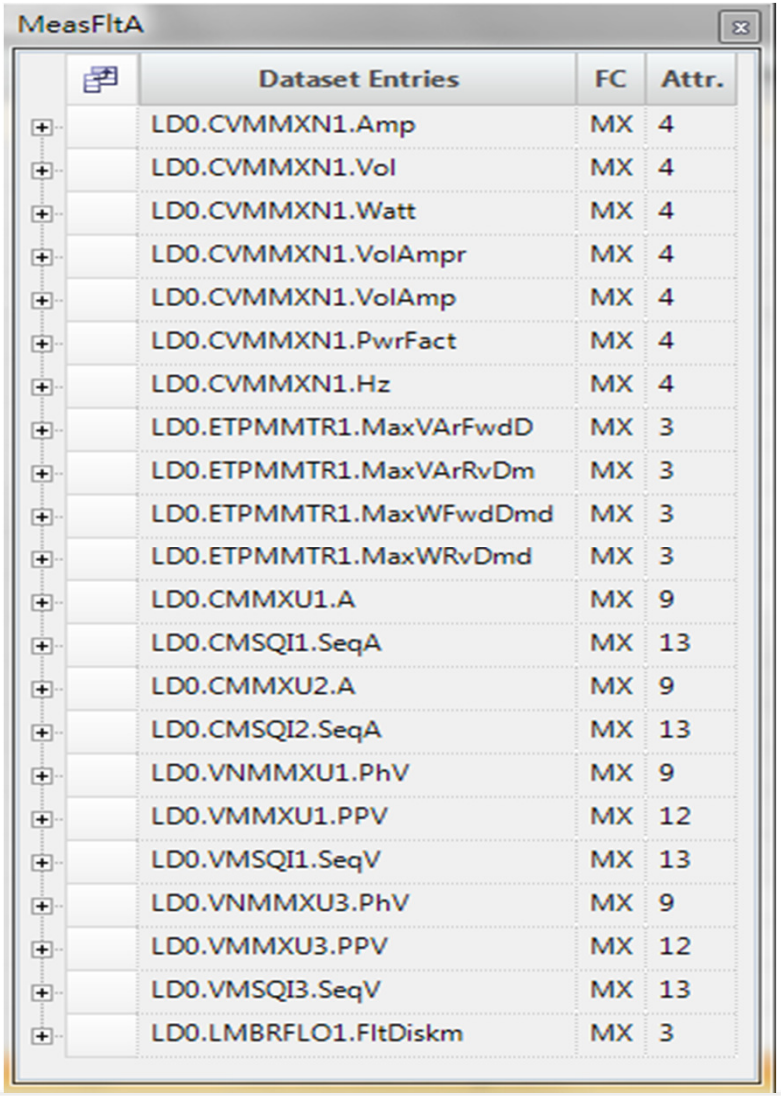
Wireshark 擷取之 SNTP 封包

SNTP 封包測試與解析

欄位名稱	欄位值	封包解析
Reference timestamp	Jan 19, 2015 02:58:42.7514 0000 UTC	系統時中最後一次被設定或更新的時間
Original timestamp	Jan 19, 2015 02:58:54.5822 02000 UTC	SNTP請求封包離開發送端時發送端的本地時間
Receive timestamp	Jan 19, 2015 02:58:54.5832 37000 UTC	SNTP請求封包到達接收端時接收端的本地時間
Transmit timestamp	Jan 19, 2015 02:58:54.5833 08000 UTC	回應封包離開回應者時回應者的本地時間

MMS 封包測試與解析

- MMS的測試封包擷取將使用與GOOSE封包擷取相同的設備連接環境
- 在規劃上，我們必須先將需要Report出去的資料物件放入一名為MeasFltA的DataSet中，其中包含了22個資料物件，然後再增加一個Report Control Block (RCB)並連結到上述DataSet


MeasFltA

Dataset Entries	FC	Attr.
LD0.CVMMXN1.Amp	MX	4
LD0.CVMMXN1.Vol	MX	4
LD0.CVMMXN1.Watt	MX	4
LD0.CVMMXN1.VolAmpr	MX	4
LD0.CVMMXN1.VolAmp	MX	4
LD0.CVMMXN1.PwrFact	MX	4
LD0.CVMMXN1.Hz	MX	4
LD0.ETPMMTR1.MaxVArFwdD	MX	3
LD0.ETPMMTR1.MaxVArRvDm	MX	3
LD0.ETPMMTR1.MaxWFwdDmd	MX	3
LD0.ETPMMTR1.MaxWRvDmd	MX	3
LD0.CMMXU1.A	MX	9
LD0.CMSQI1.SeqA	MX	13
LD0.CMMXU2.A	MX	9
LD0.CMSQI2.SeqA	MX	13
LD0.VNMMXU1.PhV	MX	9
LD0.VMMXU1.PPV	MX	12
LD0.VMSQI1.SeqV	MX	13
LD0.VNMMXU3.PhV	MX	9
LD0.VMMXU3.PPV	MX	12
LD0.VMSQI3.SeqV	MX	13
LD0.LMBRFLO1.FltDiskm	MX	3

MMS 封包測試與解析

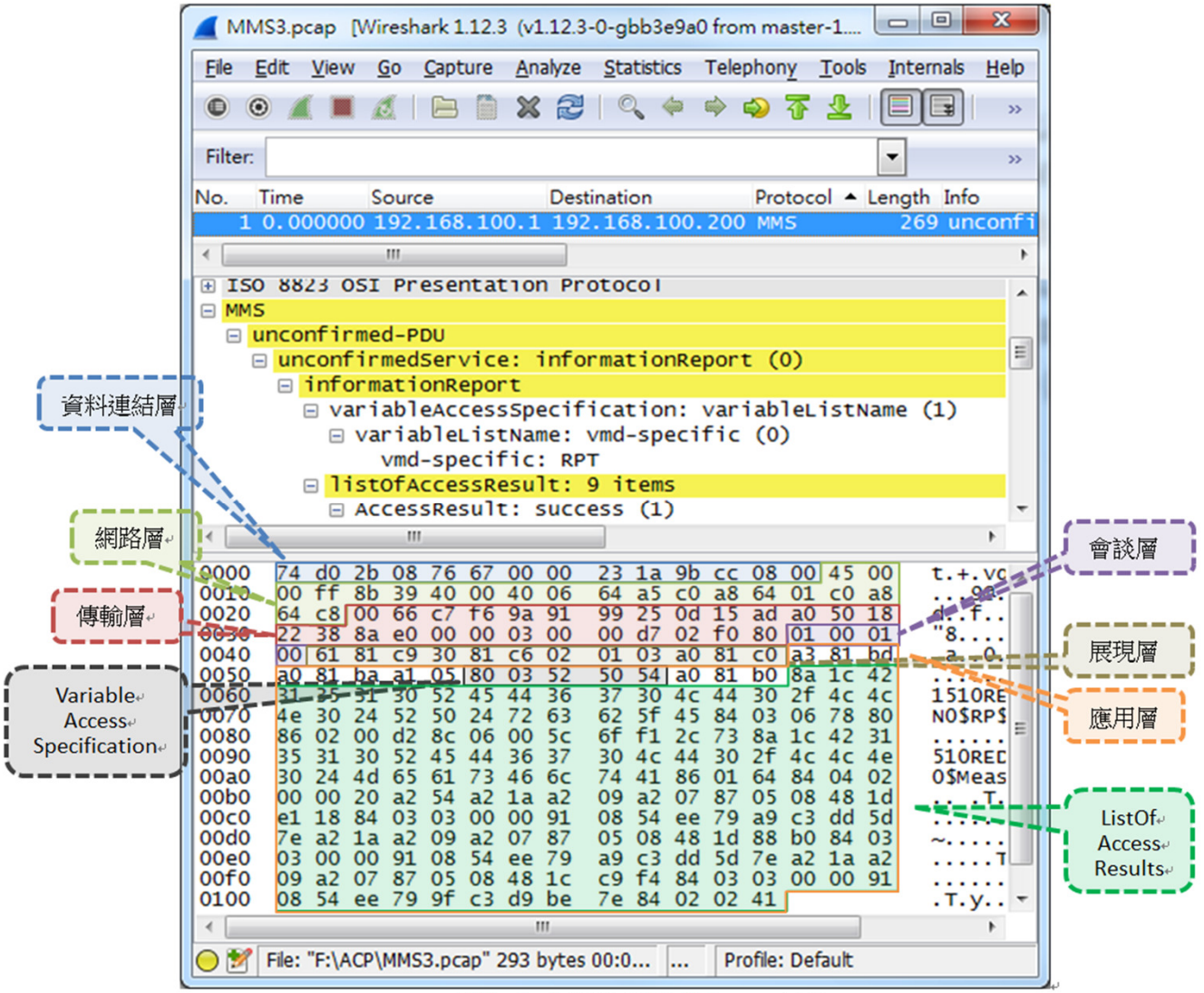
- 最後規劃GCB中的觸發條件(Trigger Option)及緩衝型態 (Buffered/ Unbuffered)等參數
- 因本實驗目的為擷取需要大量頻率傳輸的量測值(MMXU)，故選擇不使用緩衝以降低系統負擔。觸發條件則選擇DChg(數值改變)與QChg(品質改變)

IED	LD	LN	RCB	Status	Attached	Con	Buffered	Buffer Time	Enabled	DChg	QChg	DUpd	Cyclic
B1510RED670	LD0	LLN0	rcb_E	IED-defined, configurable	MeasFltA	100	☐	500	6	☑	☑	☐	☐

MMS 封包測試與解析

- MMS因為自由度高，可以通用於各種場合，因此制定的規則相當嚴謹，封包解析過程相較其他不同協定也比較複雜
- 因本部分實驗目的是擷取並解析report的封包，我們可在IEC 61850-7-2或IEC 61850-8-1中找到report封包的格式
- 其中許多欄位是由”OptFlds”去制定是否顯示於此MMS封包當中，因此，我們必須利用第二欄的”Reported OptFlds”並對照表三的內容來得知這項訊息

MMS 封包測試與解析



Wireshark 擷取之 MMS Report 封包

MMS 封包測試與解析

IEC 61850 Report 封包格式

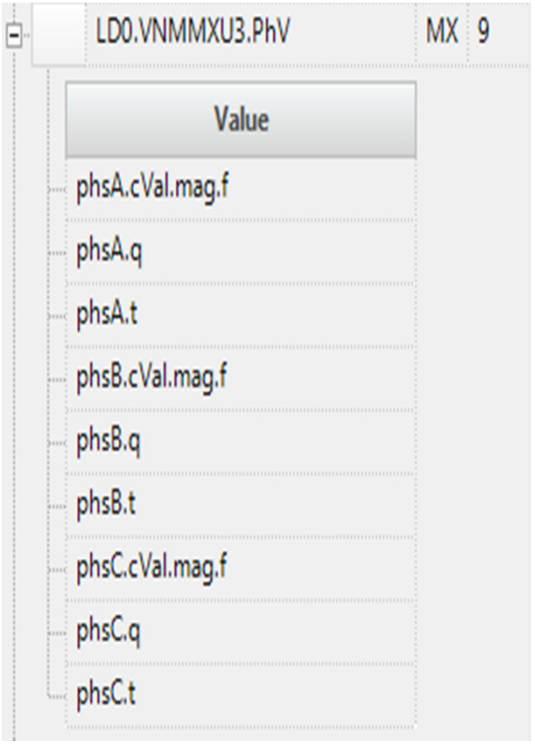
IEC 61850-7-2 report format parameter name	Condition
RptID	Shall always be present
Reported OptFlds	Shall always be present
SeqNum	Shall be present if OptFlds.sequence-number is TRUE
TimeOfEntry	Shall be present if OptFlds.report-time-stamp is TRUE
DatSet	Shall be present if OptFlds.data-set-name is TRUE
BufOvfl	Shall be present if OptFlds.buffer-overflow is TRUE
EntryID	Shall be present if OptFlds.entryID is TRUE
ConfRev	Shall be present if OptFlds.conf-rev is TRUE
SubSeqNum	Shall be present if OptFlds.segmentation is TRUE
MoreSegmentsFollow	Shall be present if OptFlds.segmentation is TRUE
Inclusion-bitstring	Shall be present
data-reference(s)	Shall be present if OptFlds.data-reference is TRUE
value(s)	See AccessResult for value(s)
ReasonCode(s)	Shall be present if OptFlds.reason-for-inclusion is TRUE

IEC 61850 Report 的 OptFlds 欄位代表意義

ACSI value of BRCState	MMS bit position
Reserved	0
sequence-number	1
report-time-stamp	2
reason-for-inclusion	3
data-set-name	4
data-reference	5
buffer-overflow	6
entryID	7
conf-revision	8
segmentation	9

MMS 封包測試與解析

欄位名稱	欄位值	封包解析
RptID	B1510RED670LD0/LLN0/RP/rcb_E	RCB的位址，格式為LD/LNRPRCB_Name
Reported OptFlds	0x7880	轉換為二進制後為01111000 10000000，代表表3中的第2、3、4、5、9項資料欄位的內容將會隨著本封包傳出
DatSet	B1510RED670LD0/LLN0$MeasFltA	傳出的RCB所連結到的DatSet
Inclusion-bitstring	0x000020	代表的是在DataSet中哪幾項的資料物件隨著本封包傳出，本封包換為二進制後為00000000 00000000 00100000，代表本MMS的內容為DataSet中的第19項資料



MMS 封包測試與解析

欄位名稱	欄位值	封包解析
Value(s)		value欄位為上述Inclusion-bitstring的內容，若Inclusion-bitstring有超過不只一個資料物件，則value的數量也會隨著改變。本封包分別為三項的電壓值、品質及時間標記
ReasonCode(s)	0x41	Reasoncode為本report封包是因達到何種條件而被觸發的。其中判讀方式如下： Bit 0： Reserved。 Bit 1： data-change。 Bit 2： quality-change。 Bit 3： data-update。 Bit 4： integrity。 Bit 5： general-interrogation。 Bit 6： application-trigger。

結論

- IEC 61850是電力自動化通訊網路及系統的國際標準，此標準之技術內涵含資料模型、資訊交換服務、通訊協定、及規劃配置等議題
- 本研究使用免費的封包解析軟體Wireshark擷取封包後，與各協定規範中的格式比對
- 結果顯示本實驗室所使用的設備均有符合規範所要求，在本實驗所使用到的所有設備，如MU、IED、時間同步裝置、交換器及SCADA，實際設備間的通訊因為彼此溝通傳遞使用的協定皆符合規範，因此也都沒有任何通訊上的問題

Thank You for Your Attention!