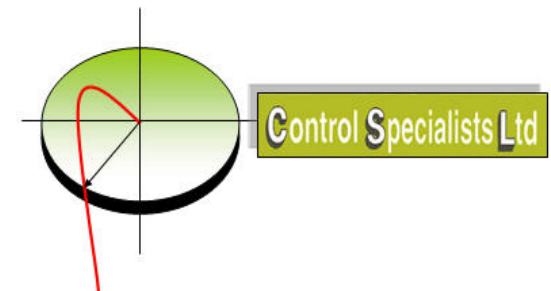


**An Introduction to
PROFINET Frame
Analysis using**



Peter Thomas
Control Specialists Ltd

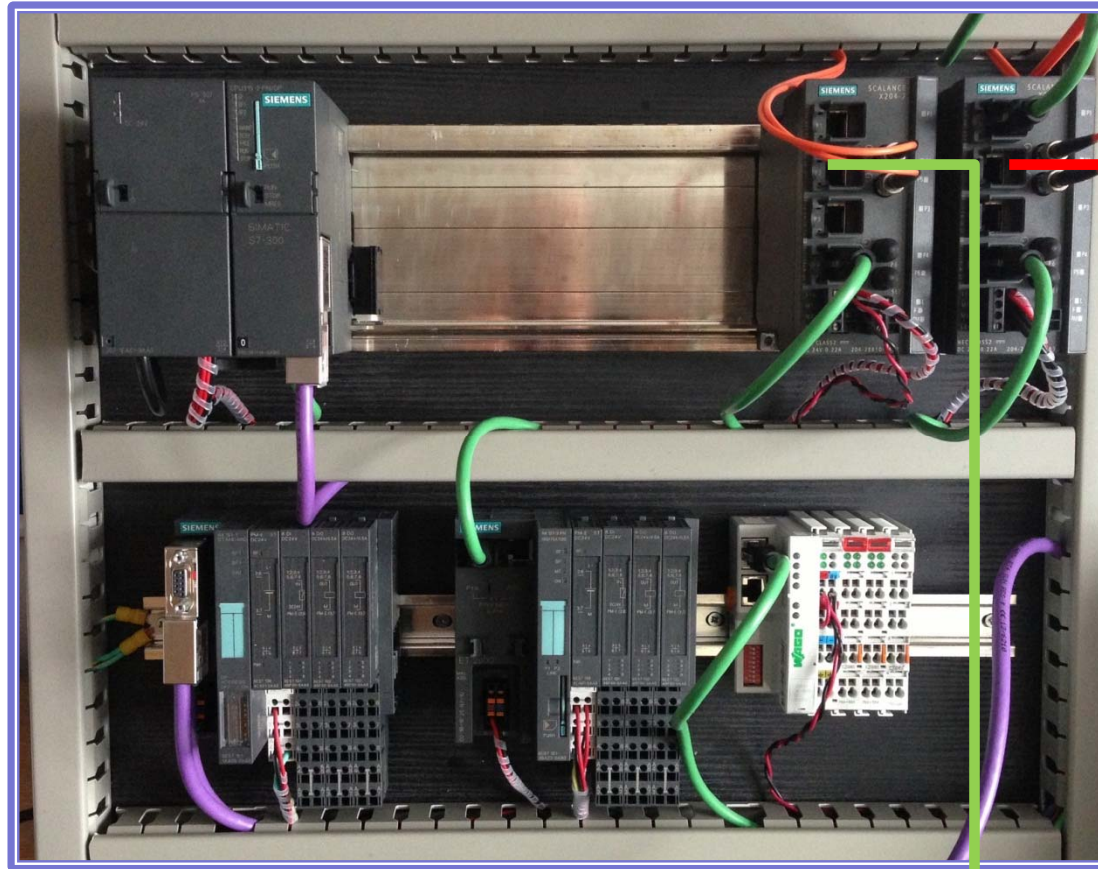
www.controlspecialists.co.uk



- To gain an understanding of the way in which PROFINET devices communicate with one another over Ethernet.
- To learn how to capture the PROFINET Frames using Wireshark®.
- To analyse the captured frames to gain an understanding and purpose of the various protocols.
- This is a topic covered in more detail in the Certified Profinet Engineers Course

- Wireshark® is a network protocol analyser. It lets you capture and interactively browse the traffic running on a computer network.
- It is not dedicated to Profinet and as such cannot be compared to ProfiTrace.
- It is free to download and available from www.wireshark.org

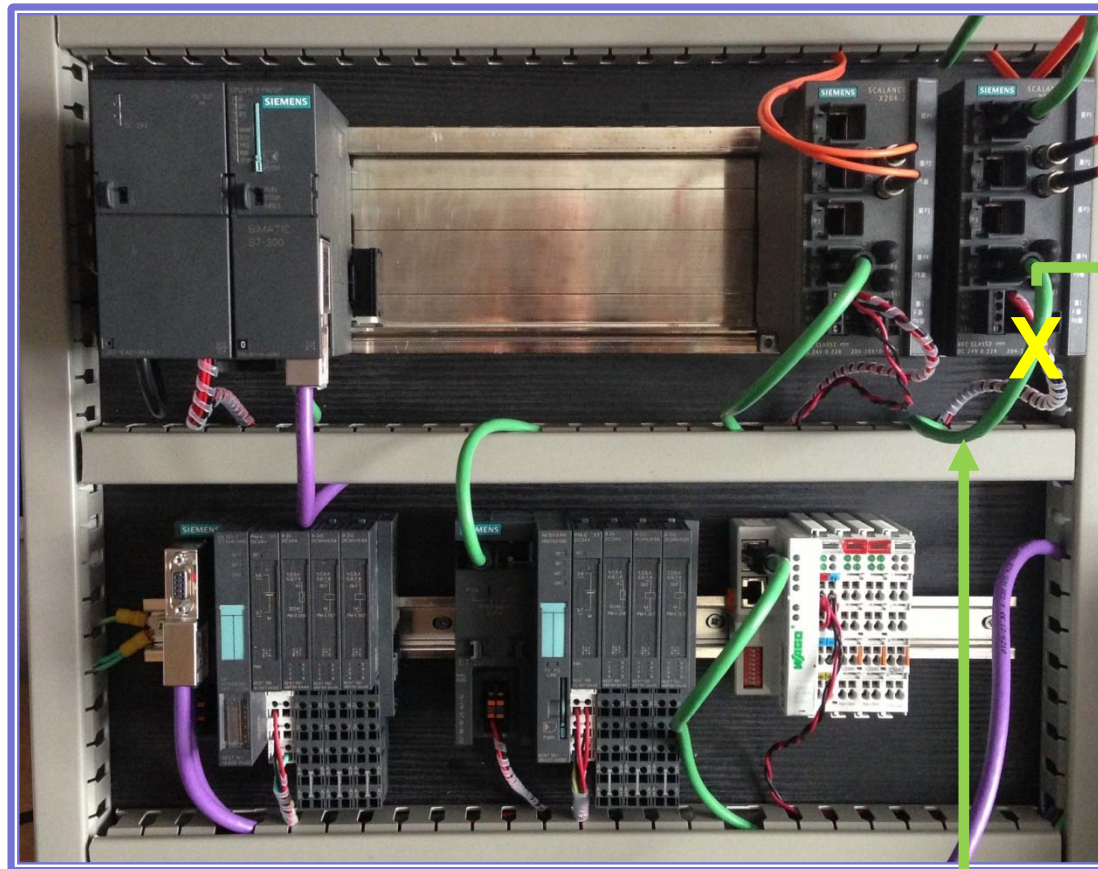




↑ LAN ↑ LAN

Switch B – Port 2
(IM153-3 ONLY)

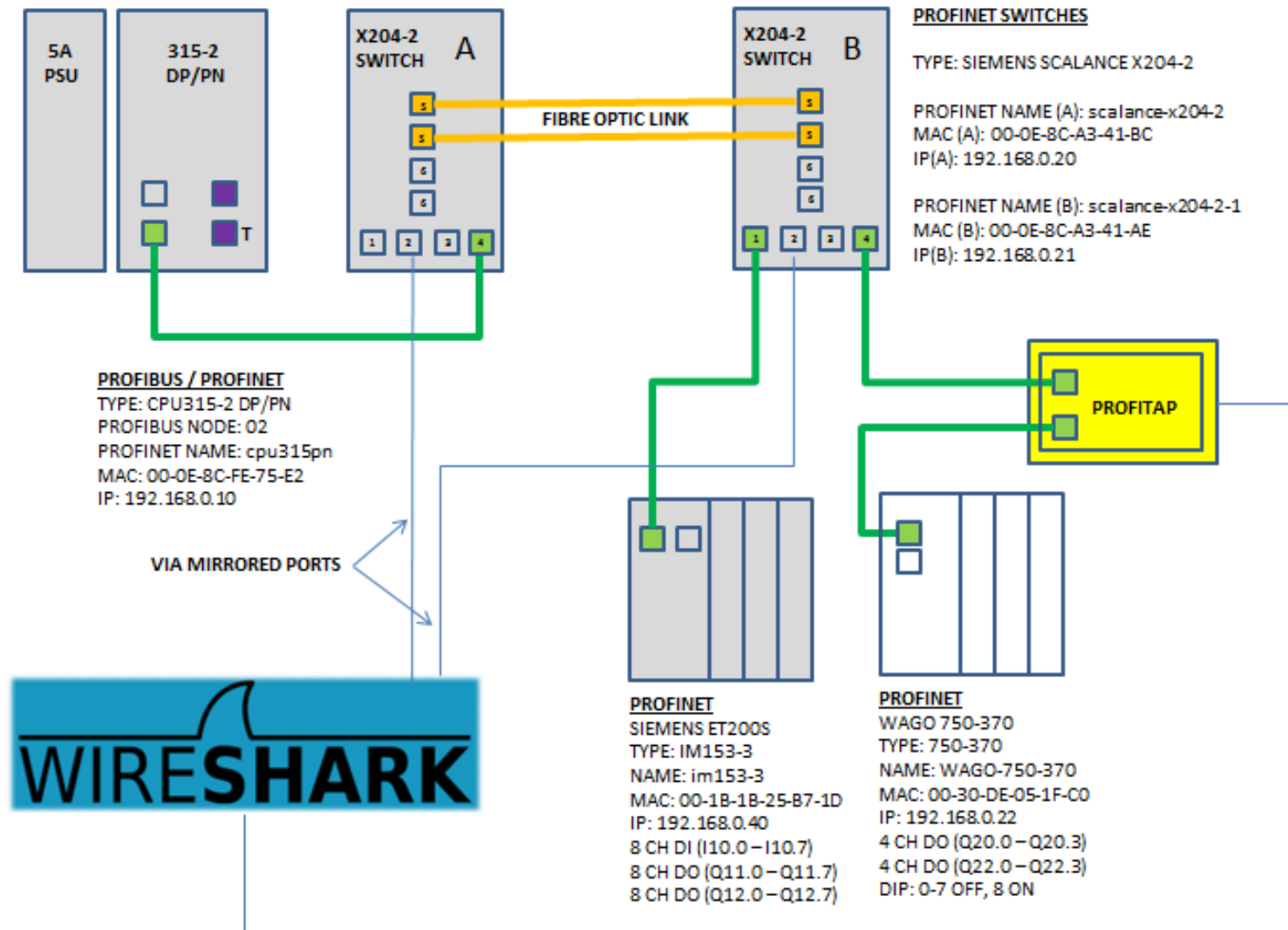
Switch A – Port 2
(IM153-3 & WAGO)



USB



PROCENTEC



- Wireshark® will be used to capture and analyse Profinet traffic during the following events:-
 - Start-Up
 - Data Exchange
 - Loss of Module
 - Loss of Communications
 - Duplicate Device Name

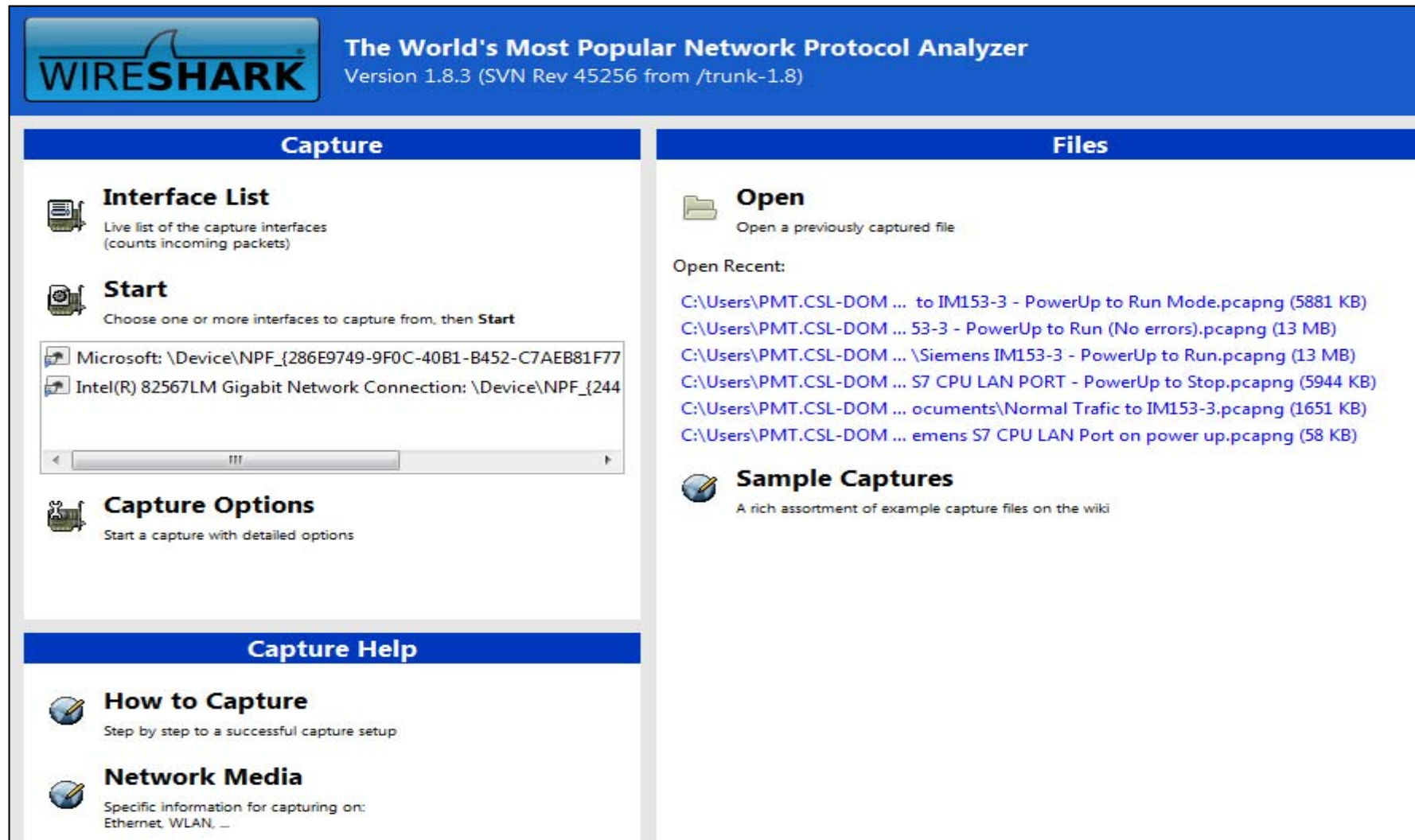
SIEMENS

PROCENTEC

WAGO[®]
INNOVATIVE CONNECTIONS

- Siemens S7 PLC Hardware & Switches.
- Wago IO
- ProfiTap & Netilities from Procentec
- Wireshark[®] Network Protocol Analyser.





The screenshot shows the Wireshark homepage with a blue header and two main columns. The left column is titled 'Capture' and contains sections for 'Interface List', 'Start', and 'Capture Options'. The right column is titled 'Files' and contains sections for 'Open' and 'Sample Captures'. Below the 'Capture' column is a 'Capture Help' section with links for 'How to Capture' and 'Network Media'.

WIRESHARK The World's Most Popular Network Protocol Analyzer
Version 1.8.3 (SVN Rev 45256 from /trunk-1.8)

Capture

Interface List
Live list of the capture interfaces
(counts incoming packets)

Start
Choose one or more interfaces to capture from, then **Start**

- Microsoft: \Device\NPF_{286E9749-9F0C-40B1-B452-C7AEB81F77}
- Intel(R) 82567LM Gigabit Network Connection: \Device\NPF_{244

Capture Options
Start a capture with detailed options

Files

Open
Open a previously captured file

Open Recent:

- C:\Users\PMT.CSL-DOM ... to IM153-3 - PowerUp to Run Mode.pcapng (5881 KB)
- C:\Users\PMT.CSL-DOM ... 53-3 - PowerUp to Run (No errors).pcapng (13 MB)
- C:\Users\PMT.CSL-DOM ... \Siemens IM153-3 - PowerUp to Run.pcapng (13 MB)
- C:\Users\PMT.CSL-DOM ... S7 CPU LAN PORT - PowerUp to Stop.pcapng (5944 KB)
- C:\Users\PMT.CSL-DOM ... ocuments\Normal Traffic to IM153-3.pcapng (1651 KB)
- C:\Users\PMT.CSL-DOM ... emens S7 CPU LAN Port on power up.pcapng (58 KB)

Sample Captures
A rich assortment of example capture files on the wiki

Capture Help

How to Capture
Step by step to a successful capture setup

Network Media
Specific information for capturing on:
Ethernet, WLAN, ...

The screenshot shows the Wireshark interface with the following components highlighted by yellow callout boxes:

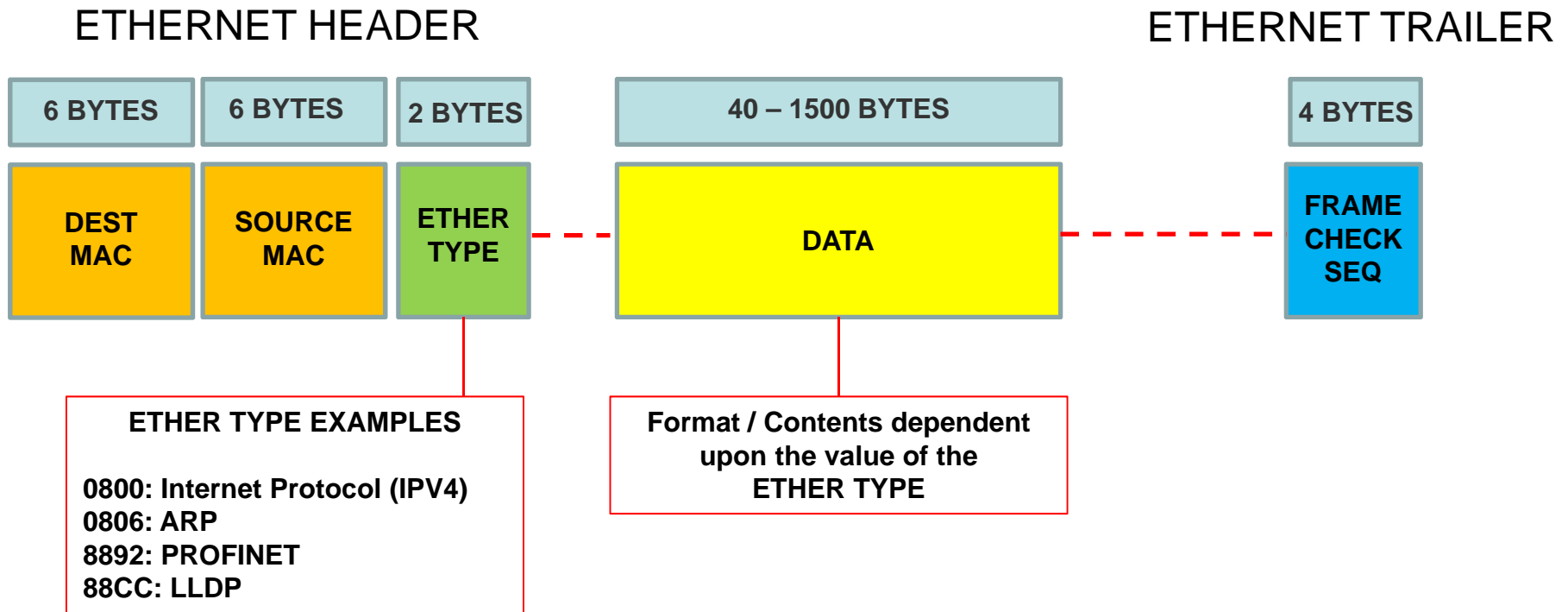
- Packet Filter:** The filter bar at the top left containing the expression `pn_io.ioxs == 0x80`.
- Expression Filter Buttons:** A row of buttons below the filter bar, including 'Clear', 'Apply', 'Save', 'ARP', 'Profinet DCP', 'Profinet CM', 'Profinet Data (Bad)', 'Profinet Data (Good)', and 'Profinet Alarms'.
- Packet List Window:** The main table of captured packets, showing columns for No., Time, Source, Destination, Protocol, Length, and Info.
- Packet Details Window:** The pane below the packet list showing the hierarchical structure of the selected packet (Frame 63296), including Ethernet II, PROFINET cyclic Real-Time, and IOxS: 0x80 (good).
- Packet Bytes Window:** The bottom pane showing the raw packet bytes in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
63283	64.6125	Siemens_25:b7:1d	SiemensA_fe:75:e2	PNIO	60	RTC2, ID:0x8061, Len: 40, cycle:18624 (valid,Primary,ok,Run)
63284	64.6132	SiemensA_fe:75:e2	Siemens_25:b7:1d	PNIO	60	RTC2, ID:0x8000, Len: 40, cycle: 5504 (valid,Primary,ok,Run)
63285	64.6145	Siemens_25:b7:1d	SiemensA_fe:75:e2	PNIO	60	RTC2, ID:0x8061, Len: 40, cycle:18624 (valid,Primary,ok,Run)
63286	64.6152	SiemensA_fe:75:e2	Siemens_25:b7:1d	PNIO	60	RTC2, ID:0x8000, Len: 40, cycle: 5768 (valid,Primary,ok,Run)
63287	64.6165	Siemens_25:b7:1d	SiemensA_fe:75:e2	PNIO	60	RTC2, ID:0x8061, Len: 40, cycle:18752 (valid,Primary,ok,Run)
63288	64.6172	SiemensA_fe:75:e2	Siemens_25:b7:1d	PNIO	60	RTC2, ID:0x8000, Len: 40, cycle: 5632 (valid,Primary,ok,Run)
63289	64.6185	Siemens_25:b7:1d	SiemensA_fe:75:e2	PNIO	60	RTC2, ID:0x8061, Len: 40, cycle:18816 (valid,Primary,ok,Run)
63290	64.6190	SiemensA_fe:75:e2	Siemens_25:b7:1d	PNIO	60	RTC2, ID:0x8000, Len: 40, cycle: 5696 (valid,Primary,ok,Run)
63291	64.6205	Siemens_25:b7:1d	SiemensA_fe:75:e2	PNIO	60	RTC2, ID:0x8061, Len: 40, cycle:18880 (valid,Primary,ok,Run)
63292	64.6211	SiemensA_fe:75:e2	Siemens_25:b7:1d	PNIO	60	RTC2, ID:0x8000, Len: 40, cycle: 5760 (valid,Primary,ok,Run)
63293	64.6225	Siemens_25:b7:1d	SiemensA_fe:75:e2	PNIO	60	RTC2, ID:0x8061, Len: 40, cycle:18944 (valid,Primary,ok,Run)
63294	64.6231	SiemensA_fe:75:e2	Siemens_25:b7:1d	PNIO	60	RTC2, ID:0x8000, Len: 40, cycle: 5824 (valid,Primary,ok,Run)
63295	64.6245	Siemens_25:b7:1d	SiemensA_fe:75:e2	PNIO	60	RTC2, ID:0x8061, Len: 40, cycle:19008 (valid,Primary,ok,Run)
63296	64.6251	SiemensA_fe:75:e2	Siemens_25:b7:1d	PNIO	60	RTC2, ID:0x8000, Len: 40, cycle: 5888 (valid,Primary,ok,Run)
63297	64.6265	Siemens_25:b7:1d	SiemensA_fe:75:e2	PNIO	60	RTC2, ID:0x8061, Len: 40, cycle:19072 (valid,Primary,ok,Run)
63298	64.6271	SiemensA_fe:75:e2	Siemens_25:b7:1d	PNIO	60	RTC2, ID:0x8000, Len: 40, cycle: 5952 (valid,Primary,ok,Run)
63299	64.6285	Siemens_25:b7:1d	SiemensA_fe:75:e2	PNIO	60	RTC2, ID:0x8061, Len: 40, cycle:19136 (valid,Primary,ok,Run)
63300	64.6291	SiemensA_fe:75:e2	Siemens_25:b7:1d	PNIO	60	RTC2, ID:0x8000, Len: 40, cycle: 6016 (valid,Primary,ok,Run)
63301	64.6305	Siemens_25:b7:1d	SiemensA_fe:75:e2	PNIO	60	RTC2, ID:0x8061, Len: 40, cycle:19200 (valid,Primary,ok,Run)

```

0000  00 1b 1b 25 b7 1d 00 0e 8c fe 75 e2 88 92 80 00  ...%.... ..u....
0010  80 80 80 80 80 80 aa 80 80 80 00 00 00 00 00 00  ..5.....
0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0030  00 00 00 00 00 00 00 00 17 00 35 00  .....5.
  
```

ETHERNET FRAME



Note – VLAN Tags, IFG, Preamble and SFD bytes not shown.

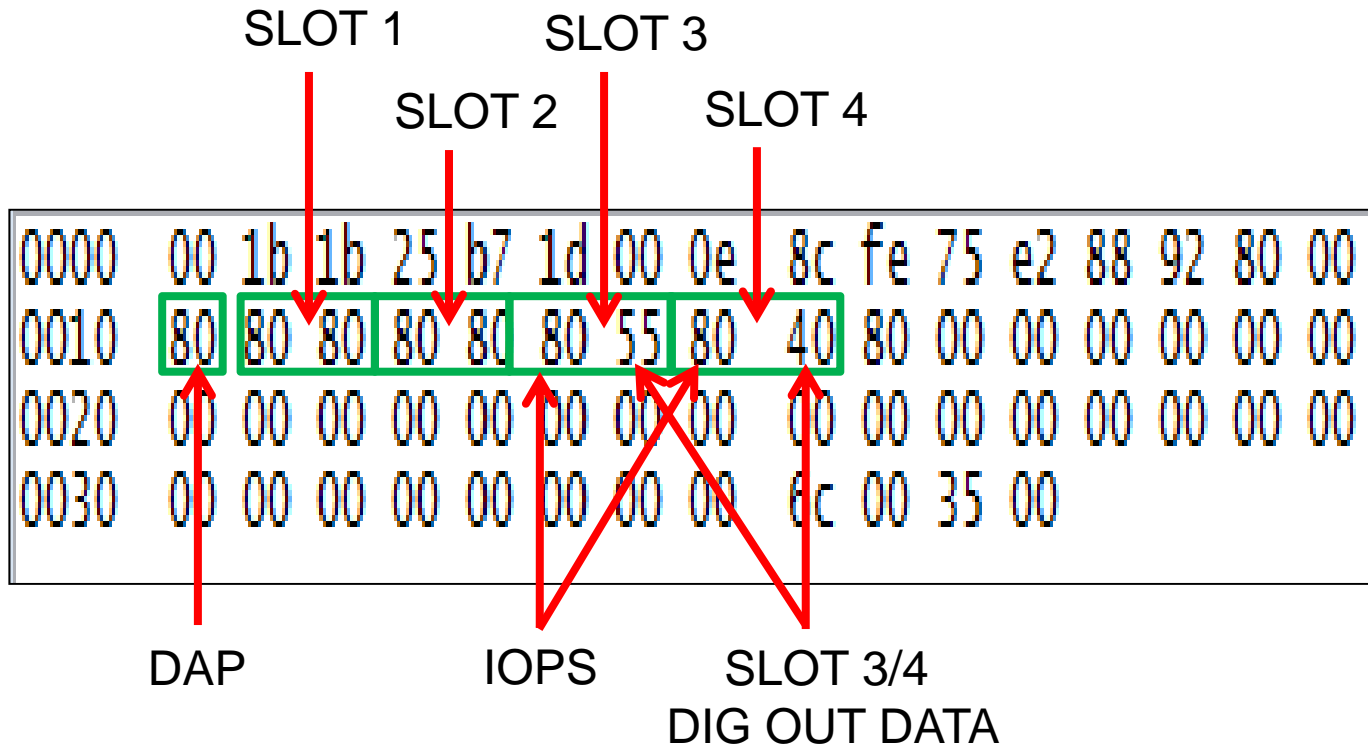
SOURCE ADDRESS DESTINATION ADDRESS ETHERTYPE FRAME ID

0000	00	1b	1b	25	b7	1d	00	0e	8c	fe	75	e2	88	92	80	00
0010	80	80	80	80	80	80	55	80	40	80	00	00	00	00	00	00
0020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0030	00	00	00	00	00	00	00	00	ba	80	35	00				

PROFINET IO DATA

CYCLE COUNTER DATA STATUS TXFR STATUS
 -- APPLICATION PROTOCOL DATA UNIT STATUS --

ETHERTYPE 8892 = PROFINET, FRAME ID 8000 = REAL TIME CLASS 2



DAP = DEVICE ACCESS POINT (IO DEVICE STATUS) 00 = BAD, 80 = GOOD

IOPS = IO PROVIDER STATUS (DATA STATUS @ CPU) 00 = BAD, 80 = GOOD

- PNIO-DCP – Name / IP Address Assignment
- PNIO-CM – Start-up Services.
- PNIO – Cyclic IO Data Exchange

- PN-PTCP – Time Synchronisation
- PNIO-AL – Acyclic Alarms / Events

- ARP – IP Address – MAC Address Lookup
- LLDP – Device Identity & Properties.

* DEVICE NAME ASSIGNMENT

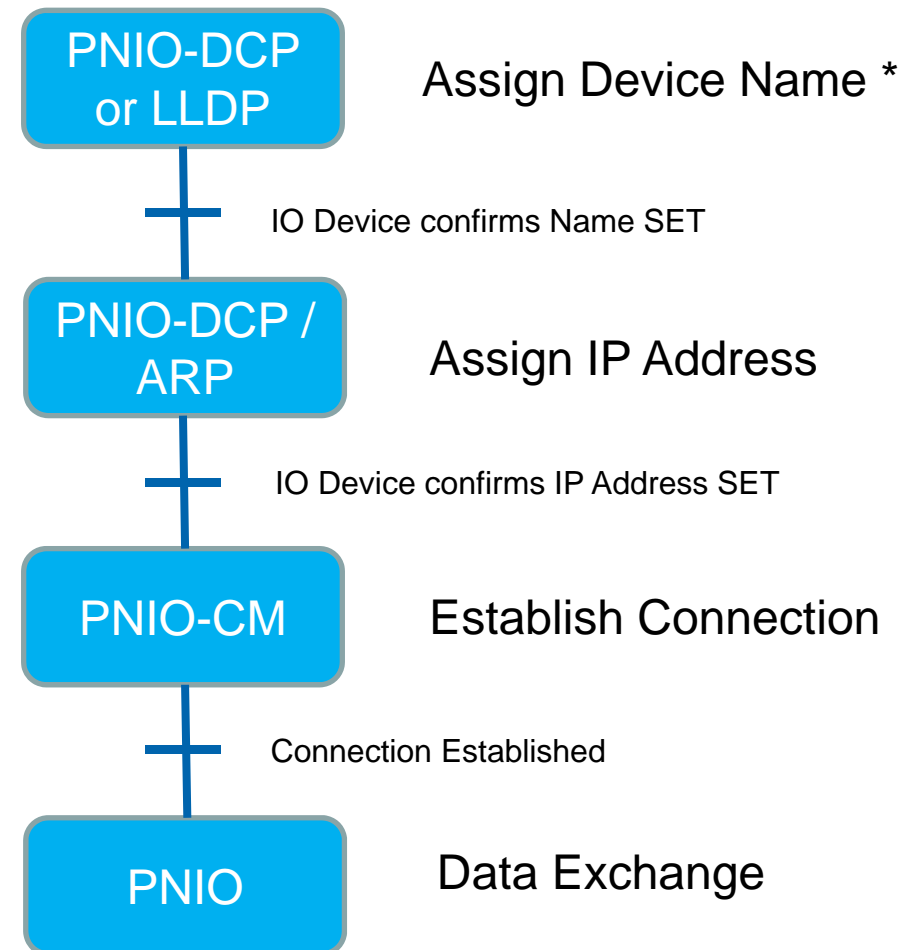
Device Names can be set up Manually, prior to connecting to the network, or Automatically on power-up.

Manual name assignment uses PNIO-DCP and tools such as the Primary Set-Up Tool from Siemens or Netilities from Procentec.


Automatic name assignment uses the LLDP protocol and requires the use of a Profinet Topology Configuration Tool.

SIEMENS
Primary Setup Tool

NET
ILITIES
PROCENTEC



Profinet Frame Analysis Workshop

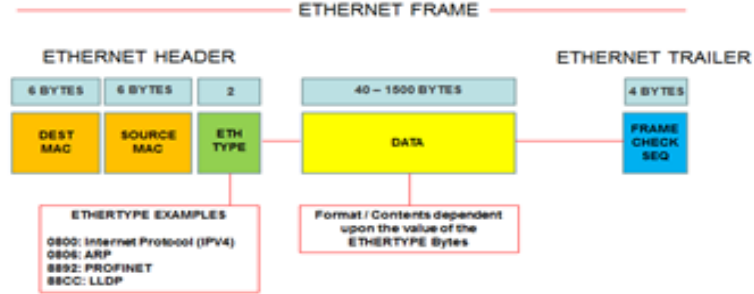


INTRODUCTION

This workshop will introduce you to Profinet Frame Analysis using Wireshark. The type of traffic that will be captured for offline analysis will be dependent upon the point in the network that you are capturing from and the method used. Wireshark is a free to download, established method of frame analysis and is used extensively in the IT world.

ETHERNET FRAME STRUCTURE (GENERAL)

The format of an Ethernet Frame is shown below. The structure and contents of the Data part of the frame are dependent upon the protocol being used of which there are many.



ETHERNET FRAME

ETHERNET HEADER

6 BYTES	6 BYTES	2	40 – 1500 BYTES	4 BYTES
DEST MAC	SOURCE MAC	ETH TYPE	DATA	FRAME CHECK SEQ

ETHERTYPE EXAMPLES

- 0800: Internet Protocol (IPv4)
- 0806: ARP
- 8892: PROFINET
- 88CC: LLDP

Format / Contents dependent upon the value of the ETHERTYPE Bytes

Note – IFG, Preamble and SFD bytes not shown.

Control Specialists Ltd. PO Box 1048 Warrington Cheshire WA1 9SU United Kingdom. Tel +44(0)1925 824002

- Step-by-Step Guide
- Overview