

Profinet Frame Analysis Workshop

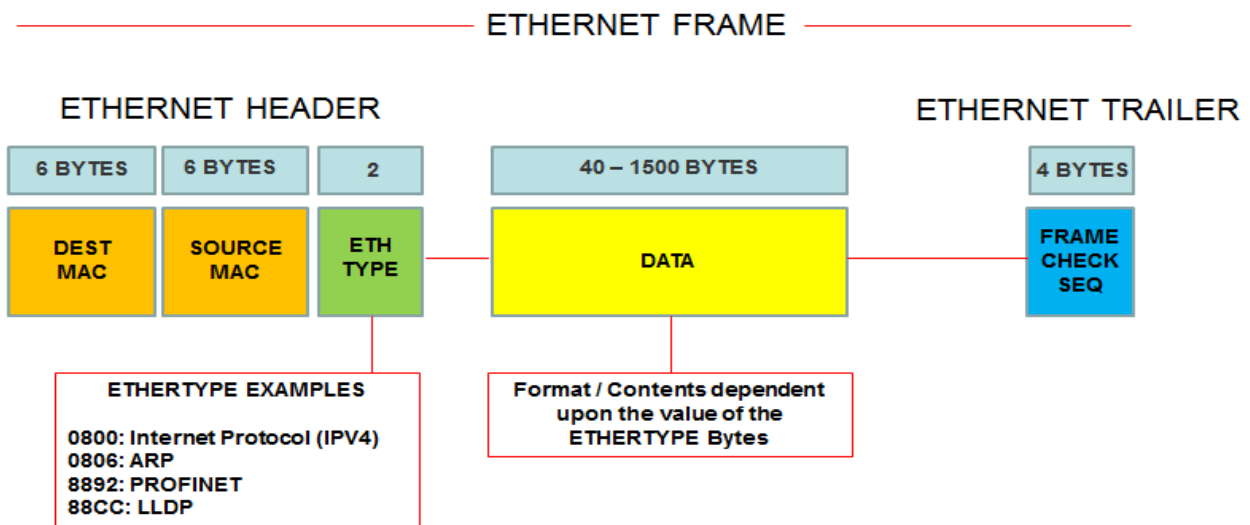


INTRODUCTION

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)

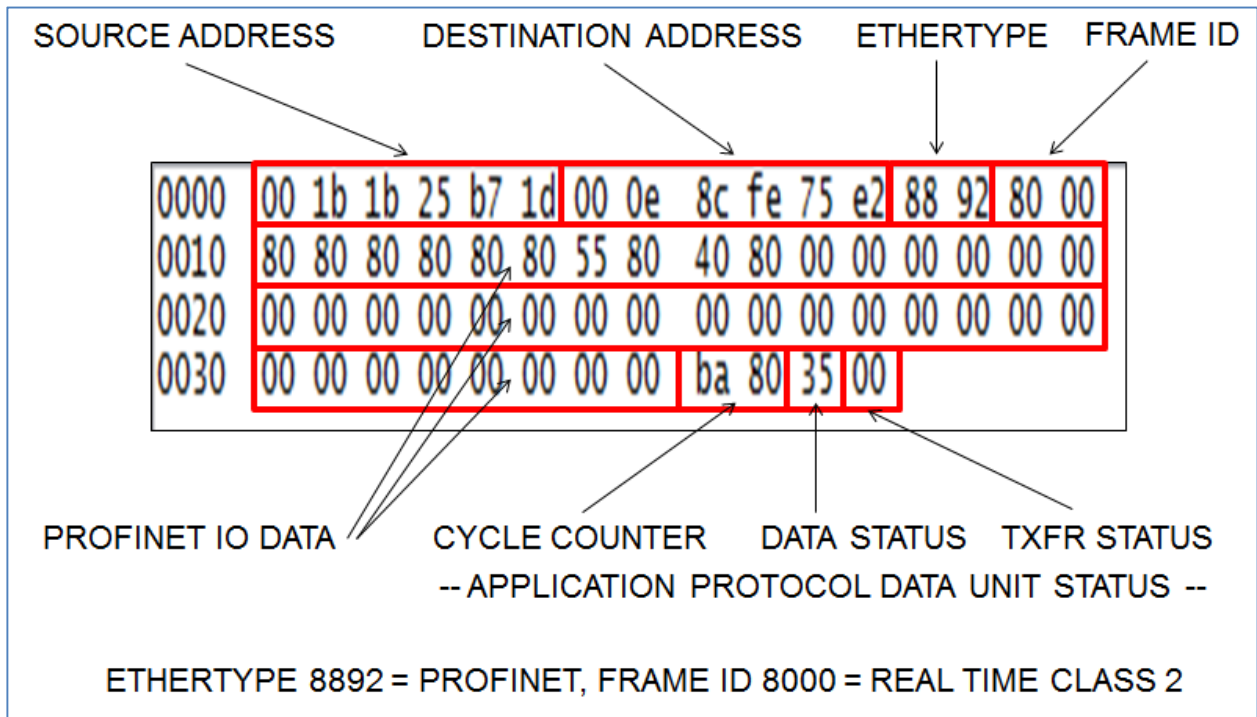
The format of an Ethernet Frame is shown below. The structure and contents of the Data part of the frame are dependent upon the protocol being used of which there are many.



Note – IFG, Preamble and SFD bytes not shown.



ETHERNET FRAME STRUCTURE (WIRESHARK - PNIO)



COMMON PROTOCOLS

For each frame, Wireshark will identify the protocol that the frame conforms to. For Profinet networks, the most common are:-

- ARP (Address Resolution Protocol)

This is a protocol that is used to associate the hardware (MAC) address of a device with an IP address. Initially, a request is made using the format “who has this IP address? Send answer to me”. The response from the device with the given IP address is “I have the requested IP address and my MAC address is as follows”. By definition, ARP’s are sent to broadcast addresses so that every device has the opportunity of responding.

- LLDP (Link Layer Discovery Protocol)

A protocol used by devices to announce their presence on the network and their capabilities. This Protocol can be used by a Profinet System to determine who is connected to who and for automatic assignment of a device name to a device when a replacement is added to the network.

- PN-DCP (Discovery and Configuration Protocol)

This is a Profinet-specific protocol that has two main functions:

1. Used by the Supervisor (PC) to assign a unique name (Siemens Primary Setup Tool / Procentec Netilities).
2. Used by the IO Controller (CPU) to assign a unique IP address (as defined in the hardware config) in conjunction with ARP above.

- PNIO-CM (Profinet IO Context Manager)

This is a Profinet-specific protocol that is used to configure the AR (Application Relations) and CR (Communication Relations) between a controller and an IO device. This process will ultimately determine the amount and type of data that will be transmitted between the pair.

There are several stages of the start-up procedure using the Context Manager with the flow usually being as follows:-

- CONNECT request from IO Controller followed by a CONNECT response from IO Device
- WRITE request from IO Controller followed by a WRITE response from IO Device
- DCONTROL request from IO Controller followed by a DCONTROL response from IO Device
- CCONTROL request from IO Controller followed by a CCONTROL response from IO Device

- PN-PTCP (Precision Transparent Clock Protocol)

This is a layer 2 Profinet-specific protocol used to ensure time synchronisation on the network.

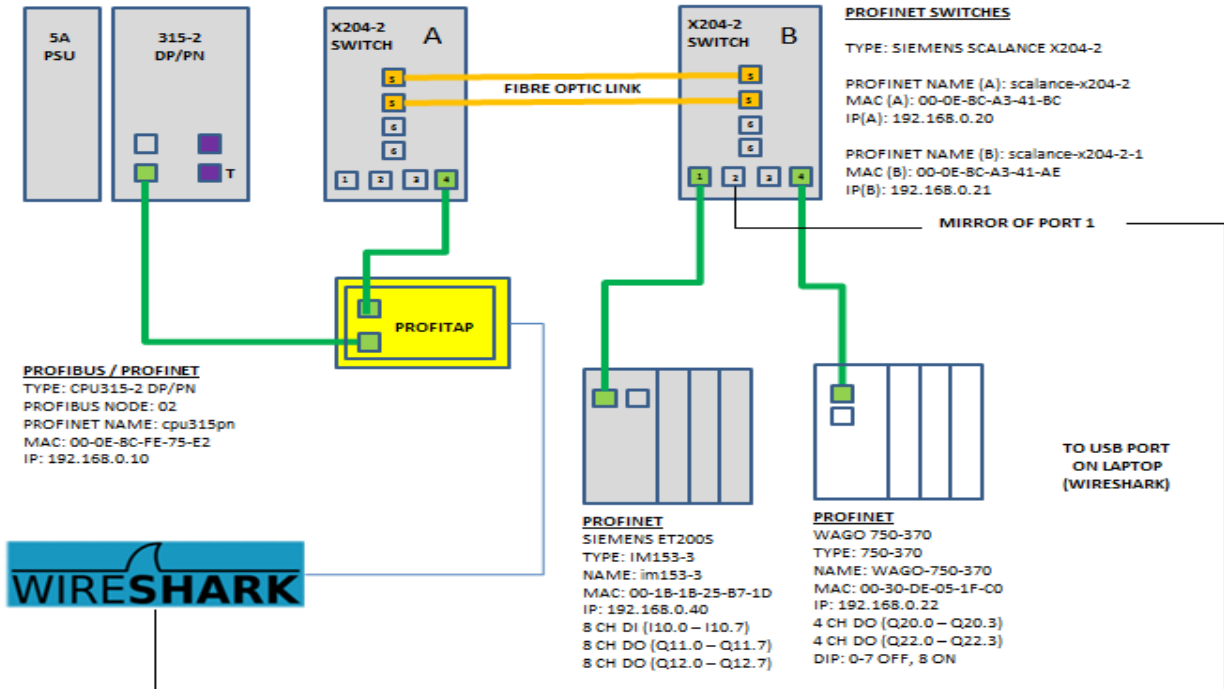
- PNIO

Profinet Data Exchange Traffic

- PNIO-AL

Profinet Alarm Events

NETWORK 1



EX01 Start-Up, Data Exchange, Loss of Module

EX01 - FRAME CAPTURE

- Put the CPU into STOP Mode and remove power from it.
- Launch WireShark.
- Select the Interface that Wireshark will capture frames from.
- Start the Capturing process.
- Apply power to the CPU.
- After approx. 15s, put the CPU into RUN mode.
- After a further 15s, remove an IO module.
- Insert the module back into its slot shortly after.
- Stop the capture process after approx. 30s.

EX01 Start-Up, Data Exchange, Loss of Module (Continued)

EX01 - FRAME ANALYSIS

ARP Profinet DCP Profinet CM Profinet Data (Bad) Profinet Data (Good) Profinet Alarms

- Click on the “**Profinet DCP**” Filter Expression Button and observe to CPU setting the IP addresses of the Profinet devices.
- Click on the “**ARP**” Filter Expression Button and observe the CPU looking for devices with specific IP addresses.
- Click on the “**Profinet CM**” Filter Expression Button and look for PNIO-CM entries that show the CONNECT – WRITE – APP READY start-up procedure.
- Click on the “**Profinet Data (Good)**” Filter Expression Button and look for PNIO entries that show data exchange.
- Click on the “**Profinet Data (Bad)**” Filter Expression Button and look for PNIO entries that show data exchange.
- Click on the “**Profinet Alarms**” Filter Expression Button and look for PNIO-AL entries that show alarm events.

EX02 Duplicate Device Name

EX02 - FRAME CAPTURE

- Put the CPU into STOP Mode.
- Make a direct Ethernet connection from the laptop to the IM153-3.
- Use the Primary Setup Tool to rename the device to “wago-750-370” – without the quotes.
- Connect the IM153-3 onto the original network.
- Put the CPU into RUN Mode.
- Note the status of the IM153-3:

- Note the status of the WAGO 750-370

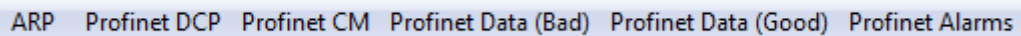
- Remove power from the CPU for a few seconds and then reapply.
- Wait a few seconds for the PLC to go into RUN mode.
- Note the status of the IM153-3:

- Note the status of the WAGO 750-370:

- Launch WireShark.
- Select the Interface that Wireshark will capture frames from.
- Start the Capturing process.
- Stop the capture process after approx. 30s.

EX02 Duplicate Device Name (Continued)

EX02 - FRAME ANALYSIS



ARP Profinet DCP Profinet CM Profinet Data (Bad) Profinet Data (Good) Profinet Alarms

- Click on the “**Profinet DCP**” Filter Expression Button and observe attempts by the CPU to find the Profinet devices.
-