Logo

Description automatically generated

# TFG Profinet & Profibus

Antonio Pérez Sánchez

Miguel Oleo Blanco



Table of Contents

[TFG Profinet & Profibus 1](#_Toc66565909)

[Protocolo 3](#_Toc66565910)

[Bibliografía 3](#_Toc66565911)

## Protocolo

Profinet y Profibus son dos protocolos de comunicación empleados en entornos industriales. Como otros protocolos tiene su versión basada en un bus de datos RS-485 (Profibus) y su estándar basado en Ethernet (Profinet). Para más detalles sobre las diferencias entre estos protocolos en la referencia [1]. Es importante saber que la tendencia en la industria se inclina por Profinet. La gran mayoría de equipos aceptan Profinet, mientras que Profibus pierde fuerza. En las redes existentes que emplean equipos Profibus y Profinet, se implementa un Proxi para traducir los mensajes entre los dos protocolos. Debido a esto, este trabajo se centrará en Profinet.

En la actualidad, Profinet es ampliamente usado en comunicaciones entre PLCs y equipos de visión artificial (cámaras) y lectores de RFID. Esto se debe al gran aumento de estos dos últimos dispositivos en la industria, ya que facilitan automatizar procesos y validad calidades y clasificar productos automáticamente. Este protocolo ha sido adaptado por muchos fabricantes, como puede ser Siemens y Phoenix Contact. Al ser un protocolo relativamente moderno, tiene las características de estos: es flexible, implementa seguridad, escalable, alta disponibilidad y desarrollo continuado.

En cuanto a los detalles técnicos de las topologías Profinet, como ya he citado, está basado en Ethernet y funciona sobre cobre, fibra óptica, PoE y en sistemas inalámbricos. Como en muchos otros protocolos industriales, en Profinet encontramos tres roles en la topología (tipos de equipos): controladores, dispositivos y surpervisores. Los controladores son los equipos que contienen un programa que se ejecuta en ellos y se intercambian datos con los dispositivos (PLC). Los dispositivos son cualquier equipo de capturación de datos o ejecución de instrucciones (sensores/actuadores). Un ejemplo actual de estos dispositivos son por ejemplo una cámara o un lector RFID, como ya he citado antes. Un equipo supervisor es aquel desde el cual podemos lanzar instrucciones, monitorear y llevar a cabo análisis de diagnósticos. Normalmente estos equipos suelen ser PCs o HMIs.

Graphical user interface, text, application

Description automatically generated A la hora de emplear Wireshark para poder analizar este tráfico, nos toparemos con que aparecen varios “protocolos” asociados a Profinet dependiendo del objetivo de esa transmisión. En la siguiente figura se muestran los nombres de los protocolos que aparecen y el tráfico al que están asociados:

Figura 1: Profinet en Wireshark [3]

Ahora vamos a ir viendo los principales con algo más de detalle. Para empezar, voy a desarrollar el DCP. Este está basado en la capa de enlace y se dedica a configurar las IPs y nombres de los equipos. Este es necesario en redes en las que no haya presentes un servidor DHCP, ya que hace la misma función que este. Profinet IO es un protocolo relacionado con los periféricos descentralizados y que utiliza Profinet RT para mandar los datos. Este último es usado para mandar datos cíclicos en tiempo real a un PLC. Esta comunicación hace de bypass de la interfaz TCP/IP que proporciona Profinet y nos permite mayor velocidad de transmisión (12MBd). Como ya he citado antes, Profinet IO se basa en RT para mandar los datos y esto se debe a que RT se diseñó para poder mandar datos de input/output con tiempos de envío críticos. El resto de las etiquetas profinet que aparecen en wireshark, serán explicadas cuando aparezcan en el documento.

## Implementación

Para generar este tráfico, vamos a aprovechar los recursos del laboratorio de la minifábrica. En concreto vamos a aprovechar una práctica que se realiza en este laboratorio en la que, se conecta el PLC con las cámaras Cognex. Vamos a implementarlo de esta forma ya que la cámara nos da la posibilidad de conectarse con el PLC usando el protocolo Profinet. Los documentos sobre esta implementación se adjuntarán.

En esta fase, es importante destacar que, por razones obvias hay que realizar un estudio de red importante. En el laboratorio hay switches y por defecto, para analizar tráfico no nos sirven, ya que envían el tráfico por el puerto que corresponde. Una vez conocido esto, nos podemos conectar a los switches scalance del laboratorio y activar el port mirroring. Esta función nos permite reenviar el tráfico de un puerto en otro. Analizando el tráfico del puerto que nos reenvía el tráfico del PLC, se aprecia que la ip de origen es cambiada por la del switch, lo cual no es mucho problema. El mayor problema lo vemos en que no somos capaces de ver el tráfico profinet, esto debe ser a que tiene algún tipo de filtro.

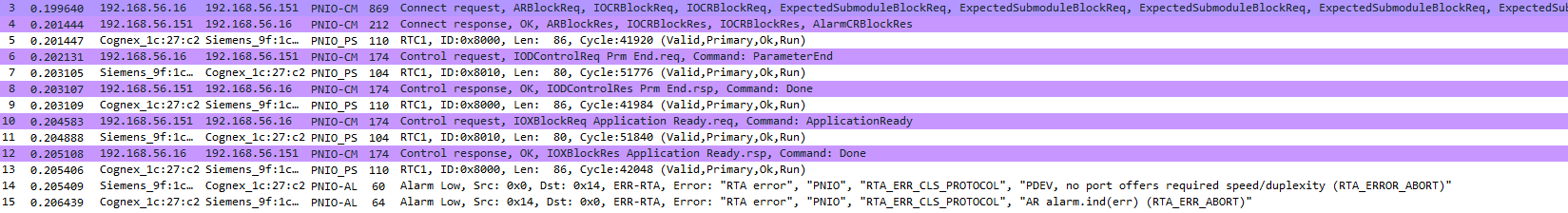
La siguiente opción es implementar un hub entre el PLC y el switch del laboratorio. En este hub conectaremos el ordenador del atacante y analizaremos el tráfico. Ahora si se puede observar tráfico Profinet, pero el PLC nos indica con la luz roja y en la pantalla que hay algún fallo. En la pantalla del PLC nos indica el error, pero también lo podemos ver en el tráfico generado.

Figura 2: Tráfico profinet con hub

Para empezar, se aprecia PNIO-CM (Profinet IO Context Manager). Este es el protocolo encargado de configurar las relaciones tanto de aplicación como de comunicación entre el controlador y el dispositivo Profinet. Entre otras cosas, es el encargado de determinar la cantidad y tipo de datos que se van a intercambiar entre los dos dispositivos. En concreto, es una request de tipo connect.

La otra etiqueta (PNIO\_PS) se refiere a los mensajes profinet IO Cyclic Service Data Unit. Los más importantes en este punto son los PNIO-AL, que nos avisan de una alarma (un error). Si vemos la información de estos mensajes, nos avisa de que hay un error ya que los puertos no cumplen los requisitos de velocidad o de dúplex. El hub empleado es de 10/100 Mbps y half-dúplex, por lo que procedemos a probar con un switch con mayor velocidad de conmutación y otras características.

Este nuevo switch se trata de un HP Procurve 2626 J4900C. Este es un switch más profesional el cual, tenemos que configurar para poder analizar el tráfico. Para ello, lo primero es saber que este se configura por la interfaz serial que tiene. Para configurarlo, empleo un terminal Linux de los del laboratorio de redes (6º Planta en ICAI) con el programa minicom o también las aplicaciones Serial y Serial Tools en MacOs empleando un adaptador serial a usb. En este punto es importante destacar que por defecto no podremos leer la información del serial, ya que el switch trabaja a una tasa de bits distinta a la por defecto. Para poder replicar esta configuración del mismo, debemos establecer en la aplicación que se utilice para configurarlo con una tasa de bits de 115200 baudios. También quiero destacar que con el Putty no hemos conseguido acceder, por lo que no lo recomendamos.

Una vez nos hemos conectado al swtich, lo único que debemos configurar es el dúplex, que debe estar en auto y el port fordwarding/mirroring. Se pueden configurar varios puertos para monitorear.

Una vez tenemos la configuración lista, cargamos de nuevo el proyecto de la cámara en el PLC y conectamos la aplicación de la cámara y podemos ver el tráfico generado por estos. El proyecto en concreto lo que hace es, la información que captura la cámara y se la envía al PLC. También esta cámara esta configurado con un disparador externo que es el PLC, y cuando activamos la entrada correspondiente, vemos como se realiza una foto en la aplicación de la cámara.

## Bibliografía

[1] Documentación Profinet y Profibus

<http://www.edcontrol.com/index.php/instrumentacion/instrumentacion-189/item/116-profibus-versus-profinet-estrategias-de-comparacion-y-migracion#:~:text=PROFIBUS%20es%20un%20bus%20de,m%C3%A1s%20r%C3%A1pida%20y%20m%C3%A1s%20flexible.>

[2] Documentación Profinet

<https://www.cursosaula21.com/profinet-que-es-y-como-funciona/#:~:text=PROFINET%20(Process%20Field%20Network)%20es,datos%20entre%20controladores%20y%20dispositivos.>

[3] Documentación Profinet Wireshark

<https://wiki.wireshark.org/PROFINET>

[4]

https://profibusgroup.files.wordpress.com/2013/01/w4-profinet-frame-analysis-handout-peter-thomas.pdf