UNIVERSIDAD AUTÓNOMA DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación

TRABAJO FIN DE GRADO

OPTIMIZACIÓN DE ROAMING EN APLICACIONES WIRELESS LAN PARA COMUNICACIÓN TREN-TIERRA BASÁNDONOS EN REDES REDUNDANTES RNA (PRP) Y SU OPTIMIZACIÓN MEDIANTE iPRP (SIEMENS)

Autor: Juan de la Merced de Usera
Tutor: Juan Carlos Pozas Bustos
Ponente: Jorge Enrique López de Vergara Méndez

JULIO 2020

OPTIMIZACIÓN DE ROAMING EN APLICACIONES WIRELESS LAN PARA COMUNICACIÓN TREN-TIERRA BASÁNDONOS EN REDES REDUNDANTES RNA (PRP) Y SU OPTIMIZACIÓN MEDIANTE iPRP (SIEMENS)

Autor: Juan de la Merced de Usera
Tutor: Juan Carlos Pozas Bustos
Ponente: Jorge Enrique López de Vergara Méndez

Siemens España
Digitalización Industrial
Automatización de Procesos
Comunicaciones Industriales
RC-ES DI PA CI

RESUMEN

Como sucede en cualquier transporte público, ya sea aviones, autobuses, etc., en los trenes, es imprescindible que el personal de circulación y de tierra tengan comunicación directa en todo momento por si fuera necesaria cualquier intervención inmediata. Para tener la capacidad de establecer esa comunicación, las comunicaciones tren-tierra han ido evolucionando a lo largo del tiempo, pero sin lugar a duda, el salto cualitativo más importante fue cuando se creó un sistema de comunicación digital inalámbrico denominado GSM-R (*GSM-Railway*).

Ahora mismo, las líneas en el entorno ferroviario en España tienen GSM-R, pero en los últimos años se están estudiando diferentes opciones para mejorar esta comunicación.

Una de ellas es la comunicación a través de tecnología de banda ancha, entre los puestos de mandos o estaciones fijas distribuidas por todo el recorrido de la vía y los trenes en movimiento, que utiliza tecnología WLAN (estándares IEEE 802.11) más en concreto su versión 802.11ac, en modelos industriales. Aunque, actualmente, se está sufriendo una revolución en este tipo de tecnología, la cual se está empezando a asentar y está empezando a coger mucha fuerza. Estas dos tecnologías son el 5G y el Wi-Fi 6 (estándar nuevo denominado 802.11ax) las cuales van a dar mucho que hablar.

Además de la propia gestión de los servicios básicos ferroviarios y del material rodante distribuido por la vía, los cuales demandan procesos de operación y decisión en tiempo real, los viajeros comienzan a solicitar servicios de alta calidad durante el viaje. Este es el principal motivo por el cual se están estudiando diferentes mejoras en este entorno o tipo de comunicación.

Por consiguiente, lo que se va a plantear en este proyecto es el diseño y la posterior validación de una arquitectura de red real utilizada en una comunicación tren-tierra. Para ello primero se estudiarán aquellos servicios que se demandan en el entorno ferroviario, analizando los requisitos mínimos necesarios para cada uno de ellos. Estos necesitan de una comunicación fiable y con una alta disponibilidad. Se comprobará si la tecnología que se quiere implementar, la cual se basa en una comunicación WLAN, cumple con esos requisitos mínimos en cuanto a ancho de banda y latencias mínimas se refiere. Al implementar una tecnología WLAN en una comunicación de este tipo, se derivan otros problemas en cuanto a la posible caída de dispositivos y fallos en la comunicación cableada y *Wireless*. Estos problemas se solventarán con el estudio previo y la aplicación de protocolos redundantes en la capa de enlace y red. Una vez analizado todo esto, se realizarán las configuraciones pertinentes en los dispositivos que compondrán la red, así como la integración de éstos para un correcto funcionamiento. Para finalizar el proyecto, se validará si se cumplen o no los requisitos mínimos demandados.

PALABRAS CLAVE

Comunicación tren-tierra, WLAN, PRP, RNA, iPRP, VRRP, Wi-Fi, VLAN, *Routing*

ABSTRACT

As with any public transport, whether it be airplanes, buses, etc., on trains it is essential that traffic and ground staff always have direct communication, if any immediate intervention is necessary. To have the ability to establish such communication, train-ground communications have evolved over time, but certainly, the most important qualitative leap was when a Wireless digital communication system called GSM-R (GSM-Railway) was created.

Right now, the lines in the railway environment in Spain have GSM-R, but in recent years different options are being studied to improve this communication.

One of them is the communication via broadband technology, between the control stations or fixed stations distributed throughout the track and the trains in motion, using WLAN technology (IEEE 802.11 standards) more specifically its 802.11ac version, in industrial models. Although a revolution is taking place in this type of technology which is starting to settle down and it is starting to take on a lot of strength. These two technologies are the 5G and Wi-Fi 6 (new standard called 802.11ax) which will give a lot to talk about.

In addition to the management of basic rail services and track-based rolling stock, which require real-time operational and decision-making processes, passengers begin to request high-quality services during the journey. This is the main reason why different improvements are being studied in this environment or type of communication.

Therefore, what is to be considered in this project is the design and subsequent validation of a real network architecture used in a train-ground communication. For this purpose, the services required in the railway environment will first be examined by analyzing the minimum requirements necessary for them. These require reliable communication and high availability. It will be checked whether the technology we want to implement, which will be using a WLAN communication, meets those minimum requirements in terms of bandwidth and minimal latencies. By implementing a WLAN technology in a communication of this type, other problems arise in terms of possible device failure and faults in wired and wireless communication, which we will solve with the study and application of redundant protocols in the data link and network layer. Once all this is analyzed, the relevant configurations will be made in the devices that will compose our network, as well as the integration of these for a correct functioning. To complete the project, it will be validated whether the required minimum requirements are met.

KEYWORDS

Train-ground communication, WLAN, PRP, RNA, iPRP, VRRP, Wi-Fi, VLAN, Routing

AGRADECIMIENTOS

Me gustaría aprovechar este apartado del proyecto tanto para agradecer a quienes me ha ayudado en este trabajo de fin de grado, como a todas aquellas personas que me han ayudado y han estado conmigo durante estos cuatro años de carrera y me han impulsado en cualquier momento de bajón y me han ayudado a madurar y a crecer como persona.

Obviamente, lo primero agradecer a mis padres y a mi hermano. A mis padres por darme la oportunidad de poder estudiar esta carrera y por estar siempre ahí cuando lo necesitaba, y a mi hermano por ayudarme también durante toda la carrera y por ser un apoyo incondicional en todas las decisiones que tomaba.

Lo segundo agradecer a mi tutor Juan Carlos, que fue quien me animó y me dio la oportunidad de realizar este proyecto. He tenido la suerte de poder aprender de una persona con una gran experiencia laboral en el sector de comunicaciones industriales. También, agradecer en general a todo el equipo de comunicaciones industriales que me han ayudado en la realización de este proyecto, con especial mención a Javier Bravo y Luís Acosta por ser aquellos que más me han ayudado.

Agradecer a Jorge por actuar como ponente de este proyecto y por revisarme la redacción de este trabajo.

A Jara por acompañarme durante estos 4 años y por ser una persona imprescindible que siempre me ayudaba a desconectar de todos los problemas de la carrera.

También agradecer a mi grupo de amigos de mi pueblo con los que llevo toda la vida y que son imprescindibles en mi día a día.

En la carrera, he conocido a mucha gente, pero en especial me quedo con 8 personas: Vinu, Bielza, Pitu, Rodrigo, Avello, Alberto, Iván y Alcalá. Con ellos he pasado la mayoría del tiempo en la universidad y siempre nos hemos ayudado entre nosotros. Me gustaría hacer una mención especial a Vinu, por ser mi compañero de estudio y prácticas durante toda la carrera. No solo ha sido un apoyo académico, sino también una persona con la que he compartido muchos momentos durante estos cuatro años.

Estoy seguro de que se me olvidan muchas personas por mencionar en este apartado las cuales han aportado su granito de arena durante este largo camino.

Juan de la Merced de Usera

Julio 2020

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

GLOSARIO DE ACRÓNIMOS

- **ATO:** *Automatic Train Operation* (Operación Automática de Trenes)
- **ATP:** *Automatic Train Protection* (Protección Automática de Trenes)
- **ATS:** *Automatic T*rain S*upervision* (Supervisión Automática de Trenes)
- **CBTC:** *Communications-Based Train Control* (Control de Trenes Basado en Comunicaciones)
- **CCTV:** *Closed Circuit Televisión* (Circuito Cerrado de Televisión)
- **DHCP:** *Dynamic Host Configuration Protocol* (Protocolo de Configuración Dinámica de Host)
- **ERTMS:** *European Rail Traffic Management System* (Sistema Europeo de Gestión del Tráfico Ferroviario)
- **ETCS:** *European Train Control System* (Sistema de Control Ferroviario Europeo)
- **GSM-R:** *Global System for Mobile - Railways* (Sistema Global para las Comunicaciones Móviles - Ferrocarril)
- **HD:** *High Definition* (Alta Definición)
- **ICMP:** *Internet Control Message Protocol* (Protocolo de Control de Mensajes de Internet)
- **IEC:** *International Electrotechnical Commission* (Comisión Electrotécnica Internacional)
- **IEEE:** *Institute of Electrical and Electronics Engineers* (Instituto de Ingeniería Eléctrica y Electrónica)
- **IP:** *Internet Protocol* (Protocolo de Internet)
- **iPRP:** *industrial Parallel Redundancy Protocol* (Protocolo de Redundancia en Paralelo Industrial)
- **OSI:** *Open Systems Interconnection* (Interconexión de Sistemas Abiertos)
- **PLC:** *Programmable Logic Controller* (Controlador Lógico Programable)
- **PRP:** *Parallel Redundancy Protocol* (Protocolo de Redundancia en Paralelo)
- **QoS:** *Quality of Service* (Calidad de Servicio)
- **RNA:** *Redundant Network Access* (Acceso a Red Redundante)
- **SSID:** *Service Set Identifier* (Identificador de Conjunto de Servicios)
- **TCMS:** *Train Control Management System* (Sistema de Control y Gestión de Trenes)
- **TETRA:** *Terrestrial Trunked Radio* (Radio Troncal Terrestre)
- **TIA:** *Totally Integrated Automation* (Automatización Totalmente Integrad

- **VAP:** *Virtual Access Point* (Punto de Acceso Virtual)
- **VLAN:** *Virtual Local Area Network* (Red de Área Local Virtual)
- **VoIP:** *Voice over Internet Protocol* (Voz sobre Protocolo de Internet)
- **VRRP:** *Virtual Router Redundancy Protocol* (Protocolo de Redundancia con Router Virtual)
- **Wi-Fi:** *Wireless Fidelity* (Fidelidad Inalámbrica)
- **WLAN:** *Wireless Local Area Network* (Red de Área Local Inalámbrica

1

INTRODUCCIÓN

1.1 MOTIVACIÓN

La comunicación ha sido y es un requisito clave dentro de un sistema ferroviario. Garantiza la seguridad de los viajeros y de las mercancías que transporta. La señalización y la comunicación entre las diferentes partes involucradas comenzó con simples banderas de colores que tenían diferentes significados, evolucionando a señales en las vías como semáforos o señales luminosas que indicaban cierto aviso. Junto con los sistemas de protección del tren operados como un sistema intermitente o sistema de bucle inductivo, todo tipo de sistemas de comunicación debe demostrar su fiabilidad y funcionamiento a prueba de fallos. Algunos de estos sistemas de protección de trenes datan de la década de 1920 y todavía están en uso. Sin embargo, la tendencia actual es ir evolucionando a mayores grados de automatización.

En Europa, el sistema de gestión de trenes utilizado hoy es el ERTMS (Sistema Europeo de Gestión de Trenes). ERTMS es una combinación de dos elementos; un servicio de soporte de radio + ETCS (Sistema Europeo de Control de Trenes), el cual admite diferentes niveles (1-3) de automatización. El servicio portador de radio utilizado para ERTMS hoy es el Sistema Global para Comunicaciones Móviles - Ferrocarril (GSM-R). GSM-R es un derivado específico del ferrocarril de la tecnología GSM 2G introducida a finales de la década de 1990. Si bien se espera que el final de la vida útil de GSM-R sea alrededor de 2030, GSM-R aún se está implementando en Europa. Incluso los sistemas de radio analógicos anticuados todavía se usan ampliamente, mientras que en otras regiones la tendencia se está moviendo hacia los sistemas *mmWave* para proporcionar altas velocidades de datos desde o hacia trenes en funcionamiento.

Cada vez más, se está empezando a demandar para la gestión y operación de la infraestructura ferroviaria, la integración inteligente de información en tiempo real para la decisión y operación de procesos. Además, los viajeros solicitan servicios de alta calidad durante todo el recorrido como, transporte sin interrupciones, puntualidad, transporte seguro, comodidad, entretenimiento durante el viaje, información del tráfico en tiempo real, etc. Todo esto obliga a tener que mejorar la comunicación entre el tren

en movimiento y los sistemas en la vía. Además, se espera que para el 2030, el tráfico ferroviario suburbano aumente en Alemania de 6 millones a 10 millones de pasajeros al día y que, para el 2050, aumente la capacidad de transporte ferroviario en los Estados Unidos a 4 mil millones de toneladas en mercancías cada año. Estos últimos datos hacen que los operadores de trenes en las ciudades tengan que reaccionar para maximizar su capacidad de transporte, aprovechar al máximo la infraestructura existente, hacer que el transporte público sea lo más atractivo posible, aumentar la aceptación de las opciones de transporte, etc. Por tanto, con la obsolescencia de GSM-R como tecnología utilizada para la radio de trenes y la demanda actual, el sector ferroviario se enfrenta a uno de sus mayores desafíos: la revolución en la comunicación ferroviaria. Un elemento clave es la digitalización del sector ferroviario, con un movimiento desde los sistemas de comunicación basados en conmutación de circuitos hacia sistemas basados en IP (Protocolo de Internet), lo que permite la separación de la capa de transporte y la capa de aplicación.

Para cubrir las necesidades de los clientes, se debe tener una disponibilidad garantizada, es decir, ser capaces de realizar un análisis inteligente de datos para infraestructuras y servicios del vehículo y combinar un alto rendimiento del vehículo o infraestructura con el mejor servicio y mantenimiento posible. En la **Figura 1.1** se puede observar las necesidades en una comunicación tren-tierra.

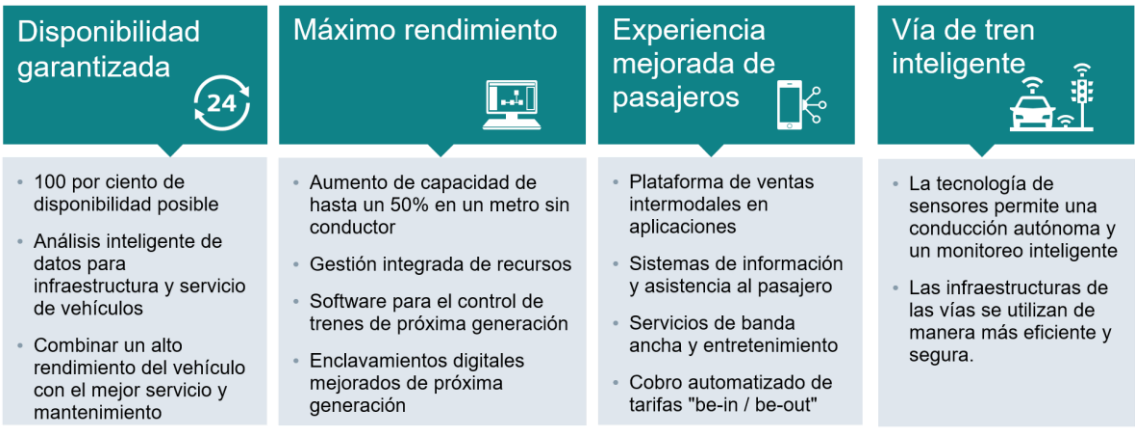


Figura 1.1: Necesidades comunicación tren-tierra

Para esta nueva era del ferrocarril, se pretende realizar una comunicación inalámbrica de alta velocidad de datos sin interrupciones. Para aumentar la seguridad y mejorar la comodidad, las comunicaciones inalámbricas para el ferrocarril están obligadas a evolucionar y mejorar de, solo enviar información de voz y control del tren, a servicios de alta velocidad de datos, incluidos video de Alta Definición (HD) y otros servicios que demandan los pasajeros con mayor ancho de banda, como la videovigilancia HD a bordo, servicios de alta velocidad en tiempo real, envío de secuencias de vídeo del tren en directo, billetes móviles ferroviarios y el IoT para los ferrocarriles.

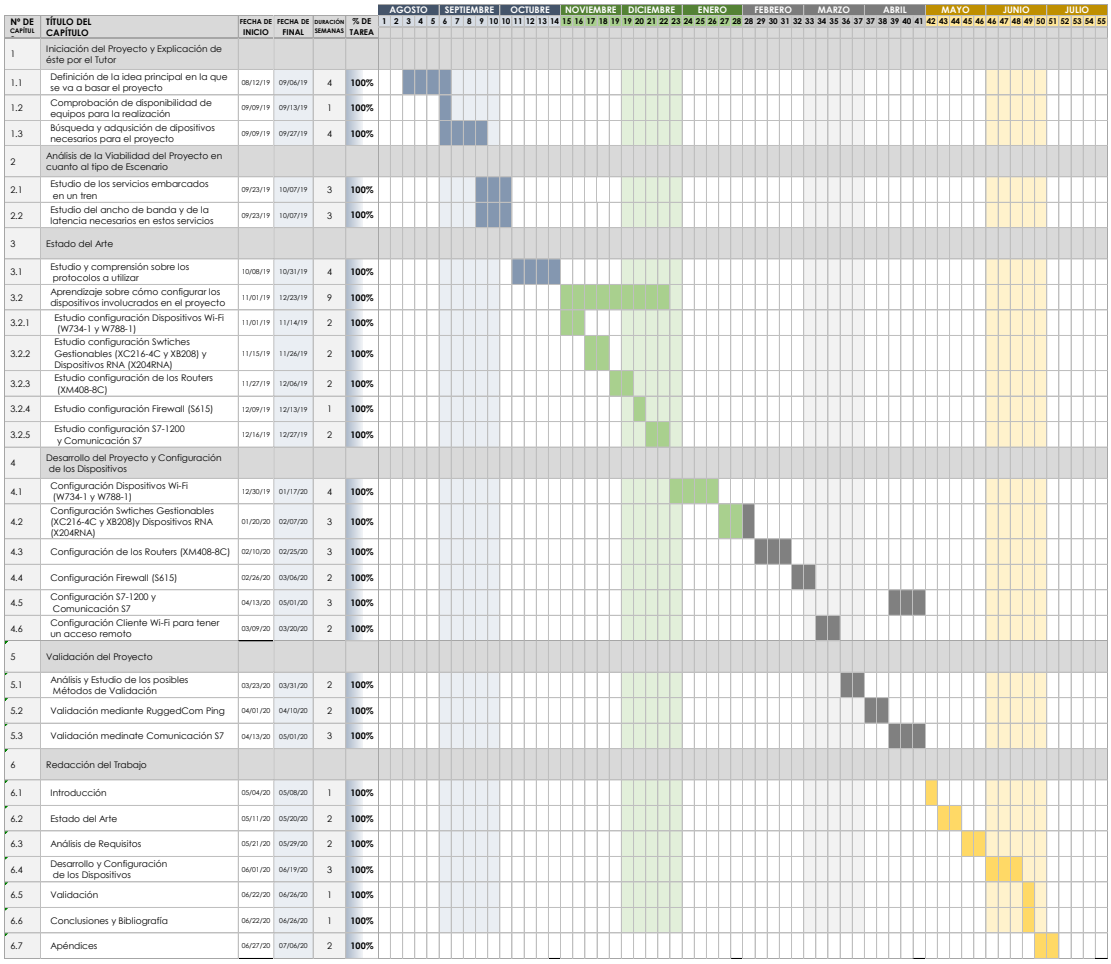
1.2 OBJETIVOS Y ENFOQUE

Este proyecto tiene como finalidad diseñar una arquitectura de red real basada en comunicación inalámbrica de banda ancha que sea capaz de dar soporte a la multitud

de servicios mencionados anteriormente que se están demandando en la actualidad, resolviendo los problemas que puede ocasionar una determinada comunicación Wireless en este entorno, y dando solución también a la posible pérdida de paquetes debida a la caída de dispositivos o fallos en el cableado.

1.3 FASES DE REALIZACIÓN

En este apartado se explican las fases seguidas durante el proyecto para la realización de éste. La **Figura 1.2** muestra el Diagrama de Gantt, donde se ve el tiempo que ha abarcado cada tarea.



Nº DE CAPÍTULO	TÍTULO DEL CAPÍTULO	FECHA DE INICIO	FECHA DE FINAL	DURACIÓN SEMANAS	% DE TAREA
1	Iniciación del Proyecto y Explicación de éste por el Tutor				
1.1	Definición de la idea principal en la que se va a basar el proyecto	08/12/19	09/06/19	4	100%
1.2	Comprobación de disponibilidad de equipos para la realización	09/09/19	09/13/19	1	100%
1.3	Búsqueda y adquisición de dipositivos necesarios para el proyecto	09/09/19	09/27/19	4	100%
2	Análisis de la Viabilidad del Proyecto en cuanto al tipo de Escenario				
2.1	Estudio de los servicios embarcados en un tren	09/23/19	10/07/19	3	100%
2.2	Estudio del ancho de banda y de la latencia necesarios en estos servicios	09/23/19	10/07/19	3	100%
3	Estado del Arte				
3.1	Estudio y comprensión sobre los protocolos a utilizar	10/08/19	10/31/19	4	100%
3.2	Aprendizaje sobre cómo configurar los dispositivos involucrados en el proyecto	11/01/19	12/23/19	9	100%
3.2.1	Estudio configuración Dispositivos Wi-Fi (W734-1 y W788-1)	11/01/19	11/14/19	2	100%
3.2.2	Estudio configuración Swtiches Gestionables (XC216-4C y XB208) y Dispositivos RNA (X204RNA)	11/15/19	11/26/19	2	100%
3.2.3	Estudio configuración de los Routers (XM408-8C)	11/27/19	12/06/19	2	100%
3.2.4	Estudio configuración Firewall (S615)	12/09/19	12/13/19	1	100%
3.2.5	Estudio configuración S7-1200 y Comunicación S7	12/16/19	12/27/19	2	100%
4	Desarrollo del Proyecto y Configuración de los Dispositivos				
4.1	Configuración Dispositivos Wi-Fi (W734-1 y W788-1)	12/30/19	01/17/20	4	100%
4.2	Configuración Swtiches Gestionables (XC216-4C y XB208)y Dispositivos RNA (X204RNA)	01/20/20	02/07/20	3	100%
4.3	Configuración de los Routers (XM408-8C)	02/10/20	02/25/20	3	100%
4.4	Configuración Firewall (S615)	02/26/20	03/06/20	2	100%
4.5	Configuración S7-1200 y Comunicación S7	04/13/20	05/01/20	3	100%
4.6	Configuración Cliente Wi-Fi para tener un acceso remoto	03/09/20	03/20/20	2	100%
5	Validación del Proyecto				
5.1	Análisis y Estudio de los posibles Métodos de Validación	03/23/20	03/31/20	2	100%
5.2	Validación mediante RuggedCom Ping	04/01/20	04/10/20	2	100%
5.3	Validación medinate Comunicación S7	04/13/20	05/01/20	3	100%
6	Redacción del Trabajo				
6.1	Introducción	05/04/20	05/08/20	1	100%
6.2	Estado del Arte	05/11/20	05/20/20	2	100%
6.3	Análisis de Requisitos	05/21/20	05/29/20	2	100%
6.4	Desarrollo y Configuración de los Dispositivos	06/01/20	06/19/20	3	100%
6.5	Validación	06/22/20	06/26/20	1	100%
6.6	Conclusiones y Bibliografía	06/22/20	06/26/20	1	100%
6.7	Apéndices	06/27/20	07/06/20	2	100%

Figura 1.2: Diagrama de Gantt

Se realiza primero un análisis de las tecnologías posibles decantándose por Wi-Fi (*Wireless Fidelity*) con el estándar IEEE (Instituto de Ingeniería Eléctrica y Electrónica) 802.11 viendo la posibilidad de que pueda ser posible aplicarlo en un entorno ferroviario. Se analiza posteriormente los tipos de estándares que hay dentro del IEEE 802.11 y se elige el que mejor se adecúe a la aplicación. Para esta elección, se han analizado una serie de requisitos (servicios, bandas de frecuencia, entorno, etc.) y, de acuerdo con los mismos, se ha planificado la arquitectura. Una vez realizada esta selección de comunicación tren-tierra, se procede a realizar un análisis de todos los problemas que pueden ocurrir tanto en la comunicación inalámbrica como en la cableada, y como ser

capaces de solventarlos. Se realiza un posible diseño real de una arquitectura de red contenida en el tren y la distribuida por toda la vía, pasando a explicar conceptos claves de la topología física y lógica. Durante este análisis se irán viendo los problemas uno a uno comenzando primero por los ocasionados por la red cableada y finalizando por la comunicación inalámbrica. Se darán soluciones específicas a cada uno mediante protocolos de red, dispositivos redundantes, modificación de la propia arquitectura, etc.

En el momento que se tiene la arquitectura completa, se valida la red diseñada comprobando los tiempos de *roaming* de los dispositivos Wi-Fi y se analizan las pérdidas de paquetes que sigue habiendo en la red aun habiendo diseñado ésta para limitar estos problemas.

1.4 ESTRUCTURA DEL DOCUMENTO

Este documento más los apéndices añadidos al final de éste, se dedicarán a la explicación de todas las etapas que se han seguido durante el proyecto. Cada capítulo se dedicará a explicar de manera precisa los pasos seguidos para cada tarea.

- En primer lugar, se realiza una **introducción,** donde se expone brevemente las tecnologías pasadas y actuales que se encuentran en el ámbito ferroviario, más concretamente en una comunicación tren-tierra, dando al mismo tiempo una explicación o motivación del porqué de esta mejora en este tipo de comunicación. También se comenta el proceso seguido durante todo el proyecto.
- En segundo lugar, se expone el **estado del arte,** donde se da una explicación teórica primero de los servicios y requisitos en un entorno ferroviario y explicación de qué es exactamente una comunicación tren-tierra. Posteriormente se comentan principales rasgos de las redes en la capa de enlace y la capa de red con sus respectivos protocolos y estándares con una ampliación en los apéndices.
- En tercer lugar, se realiza un **análisis de los requisitos** necesarios en una comunicación *Wireless* para considerarla efectiva en una comunicación tren-tierra real.
- El cuarto apartado tratará de explicar los pasos seguidos en el **desarrollo y diseño de la solución** al problema planteado. Se partirá primero de la arquitectura diseñada ya completa y se irá desglosando ésta por partes, dando explicación al proceso seguido de configuración en cada una de las partes que componen la red.
- La quinta parte de este documento consistirá en comprobar la **validez de la arquitectura** y de chequear el cumplimiento de los requisitos planteados en el apartado 3.
- Finalmente, en el sexto capítulo se expondrán las **conclusiones** del trabajo realizado, así como la disposición de la arquitectura en una situación real ferroviaria y la visualización real del diseño en el laboratorio.

2

ESTADO DEL ARTE

2.1 INTRODUCCIÓN

Durante este capítulo, se exponen los conocimientos previamente obtenidos no solo teóricos, sino también prácticos ineludibles para la elaboración y diseño de este proyecto. Valdrá también de ayuda para que el lector pueda tener la capacidad de entender algunos de los temas tratados más adelante.

2.2 SERVICIOS EN ENTORNO FERROVIARIO

Para la elaboración de este apartado se han utilizado los recursos [2] [9], más documentación privada de Siemens. En la actualidad, todos los servicios responsables de la operativa y el movimiento seguro del tren están estipulados en el estándar TCMS (Sistema de Control y Gestión de Trenes), donde además también se recogen aspectos de importancia como, el cierre y apertura de puertas, señalización, climatización, ventilación, etc. Aunque, como se ha comentado anteriormente, se está comenzando a demandar otro tipo de servicios debido a la evolución de la tecnología inalámbrica, donde los pasajeros reclaman que se les facilite las tareas de operación relacionadas con el tren, mantenimiento más ágil de las vías, aumentar la seguridad de los viajes y mejorar la experiencia a bordo de éstos.

En el momento de diseñar la red que tenga la capacidad de dar soporte a los servicios comentados, se debe tener en cuenta los parámetros de calidad de cada uno. Estos parámetros se comentarán en el siguiente apartado.

Debido a la cantidad de servicios que puede ofrecer un operador ferroviario en la actualidad, se va a realizar una división de éstos en función de la importancia que toman en el momento de garantizar la seguridad en el tren:

- Servicios vitales
- Servicios no vitales

En la **Figura 2.1** se puede observar la división de los servicios que hay en una comunicación tren-tierra y dónde se ubica cada uno:

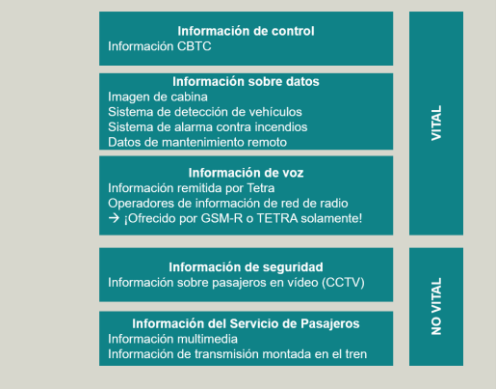


Figura 2.1: Subdivisión de los servicios en una comunicación tren-tierra

A continuación, se explican más detalladamente y a qué se refiere exactamente cada uno.

2.2.1 Servicios Vitales

En esta división se engloban aquellos servicios relacionados con la seguridad y el control del tren. Debido a la importancia que éstos toman en un entorno ferroviario, estos servicios o sistemas son muy rigurosos en cuanto a la disponibilidad de estos datos, fiabilidad en la transmisión, latencia y seguridad, con la ventaja de no demandar grandes anchos de banda. Dentro de estos servicios, también se englobarían aquellos relacionados con los sistemas de conducción automáticos del tren.

2.2.1.1 Información de Control y sobre Datos

El sistema de control y protección del tren más importante es el CBTC (Sistema de Control de Trenes basado en las Comunicaciones). El CBTC es un sistema automatizado de señalización ferroviaria que utiliza las telecomunicaciones entre el tren y los equipos de la vía para la gestión del tráfico y el control de la infraestructura. Mediante los sistemas CBTC, la posición exacta de un tren se conoce con mayor detalle y precisión que con los sistemas de señalización cotidianos. Esto se traduce en una manera más segura y eficaz de gestionar el tráfico ferroviario. Un sistema CBTC es un "sistema de control automático y continuo del tren que utiliza la localización del tren de alta resolución, independiente de los circuitos ubicados en la vía; comunicación tren-tierra continua y de alta disponibilidad de forma bidireccional; y procesadores en tren y en tierra capaces de implementar funciones de Protección Automática del Tren (ATP), así como funciones opcionales de Funcionamiento Automático del Tren (ATO) y Supervisión Automática del Tren (ATS)", tal y como se define en la norma IEEE 1474.

El principal objetivo del CBTC es aumentar la capacidad de trenes en las vías reduciendo la distancia entre ellos sin que exista riesgo de colisión o alcance entre trenes debido a la exactitud con la que es obtenida la posición de cada tren. En los sistemas actuales CBTC, los trenes calculan e informan continuamente sobre su estado

al material distribuido por toda la vía. Este estado, además de otros parámetros, contiene información como la dirección de desplazamiento del tren, la velocidad, la posición exacta y la distancia que tiene de frenado. Esta información permite determinar la superficie total abarcada por el tren en la vía. También posibilita al material de tierra precisar los puntos de la vía que no deben ser sobrepasados por los demás trenes en la misma línea. Se informa sobre estos puntos para que los trenes puedan ajustar su velocidad de forma automática y continua, manteniendo al mismo tiempo los requisitos de seguridad y confort. Por lo tanto, los trenes reciben y envían de manera continua información sobre la distancia al tren anterior y son capaces de ajustar su distancia de seguridad y velocidad.

La arquitectura típica de un sistema moderno de CBTC sigue el siguiente formato:

- Equipamiento CBTC a bordo del tren, incluyen los subsistemas ATP y ATO en los trenes.
  - Sistema ATP a bordo: Este subsistema se encarga del control continuo de la velocidad del tren en función de la zona de paso, seguridad, etc. y, si es necesario, de accionar el freno. También realiza la comunicación con el subsistema ATP desplegado por la vía para intercambiar la información necesaria para una operación segura (envío exacto de velocidad y distancia de frenado, y límites de movimiento del tren para una operación segura).
  - Sistema ATO a bordo: Es responsable del control automático de tracción y frenado para mantener el tren por debajo del umbral establecido por el subsistema ATP. Su principal tarea consiste en facilitar las funciones del conductor o del asistente, o incluso en operar el tren en un modo totalmente automático, manteniendo al mismo tiempo los objetivos de regulación del tráfico y la comodidad de los pasajeros. También permite la selección de diferentes estrategias de conducción automática para adaptar el tiempo de ejecución o disminuir el consumo de energía.
- Equipamiento CBTC a lo largo de la vía: que incluye el enclavamiento y los subsistemas que controlan cada zona de la vía (generalmente contienen las funcionalidades ATO y ATP de la línea). En función de los proveedores, las arquitecturas pueden ser centralizadas o distribuidas. El control de éste se efectúa desde un puesto ATS central, aunque los subsistemas de control local también pueden incluirse como alternativa.
  - Sistema ATP en la vía: Este subsistema se encarga de la gestión de todas las comunicaciones con los trenes de su zona. Al mismo tiempo, determina los límites de movimiento que todo tren debe respetar mientras opera en el lugar que controla el sistema. Por lo tanto, este sistema es fundamental para la seguridad.
  - Sistema ATO en la vía: Se encarga de chequear y regular la operativa de cada tren. El subsistema ATO proporciona a todos los trenes el lugar exacto de destino, así como otros datos como el tiempo de permanencia en las estaciones, etc. Además,

también puede realizar tareas complementarias y no relacionadas con la seguridad, como, por ejemplo, comunicación y gestión de alarmas/eventos, o manejar comandos de estación de espera.

En la **Figura 2.2** se puede ver una distribución real de los diferentes elementos presentes en un entorno ferroviario.

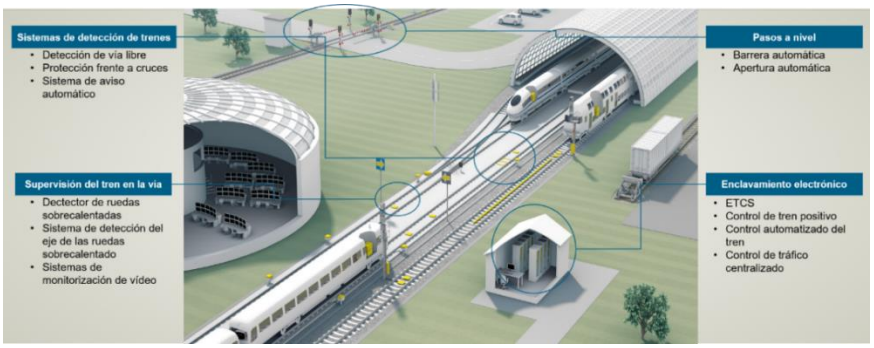


Figura 2.2: Arquitectura de los diferentes elementos que componen un sistema

- Comunicación tren-tierra, de la cual se habla más a fondo en el siguiente apartado.

2.2.1.2 Información de Voz

A esta división pertenecen los servicios conocidos como voz sobre IP (VoIP). Actualmente este tipo de información solo se transmite a través de dos sistemas y están orientados especialmente al intercambio de información entre el puesto de mando y el conductor para comunicar emergencias, control y operativa del tren, además permiten una comunicación segura con otros trenes, personas encargadas de la seguridad, etc.

- GSM-R: sistema de comunicación inalámbrico que confirma una correcta comunicación (voz y datos) entre instalaciones fijas y vehículos.
- TETRA (Radio Troncal Terrestre): estándar global para la radio *trunking* digital. Utiliza un conjunto avanzado de características, como la transmisión segura de voz y datos para gestionar los desafíos de las radios móviles modernas.

Es requisito indispensable que este tipo de servicios tengan un alto nivel en cuanto a seguridad y contengan mecanismos de autenticación y encriptación.

2.2.2 Servicios no Vitales

Este tipo de servicios no se consideran relevantes en cuanto a la seguridad del tren, sino que sirven exclusivamente para la explotación, mantenimiento y algo de operativa del tren. Están principalmente orientados para el intercambio de información entre tren-pasajero, información sobre pasajero en vídeo, servicios CCTV (Circuito Cerrado de Televisión).

No ha sido sencilla la diferenciación entre un servicio u otro en función de su importancia dentro del entorno ferroviario, debido a que es muy complicado diversificar

entre un servicio exclusivamente de control o uno crítico en la seguridad del tren. Por ejemplo, el fallo de una cámara CCTV, que controla el estado de los pasajeros en cada momento, puede tener determinadas consecuencias catastróficas en cuanto a la salud de un pasajero, pero al final se ha optado por diferenciar entre un servicio u otro en función de la seguridad en el propio movimiento del tren por la vía.

2.2.2.1 Información de la Seguridad (Sistemas CCTV)

Este tipo de sistemas son necesarios tenerlos en el tren para poder tener una supervisión y control del estado y de las acciones que realizan los pasajeros en cada momento. Esto permite hacer más eficiente la operativa del tren y dar mayor seguridad a los pasajeros. Por ejemplo, un tren siendo operado únicamente por el maquinista, las cámaras CCTV pueden permitir al maquinista confirmar que no hay personas en las compuertas del tren antes de cerrarlas y poner en marcha el tren.

Un sistema CCTV hace uso de cámaras de vídeo para mandar una señal a un sitio determinado, en un grupo máximo de monitores. Generalmente estas cámaras tienen una resolución HD de 720p. Hacen uso de sistemas de guardados.

2.2.2.2 Información sobre el Viaje al Pasajero y Servicios para Clientes

Los servicios de información sobre el viaje al pasajero se encargan de informar al pasajero sobre acontecimientos durante el viaje, como velocidad actual del tren, próxima estación en la que el tren parará, localización exacta del tren en todo momento, incluso en algunos se emiten películas para el entretenimiento del pasajero durante el viaje.

En los servicios orientados al cliente se engloban juegos on-line, acceso a internet, tráfico de VoIP, etc. Estos exigen un gran ancho de banda y velocidad a la hora de enviar información sobre voz y datos. Este tipo de servicios podría decirse que son adicionales en cuanto a disponibilidad se refiere, aunque cada vez se están haciendo más necesarios de ofrecer con altas tasas de disponibilidad. Es por este motivo principal por el que se está evolucionando a un tipo de comunicación más avanzada en este entorno.

2.2.3 Comunicación tren-tierra

La comunicación tren-tierra es la comunicación entre los diferentes servicios a bordo del tren, que necesitan establecer una comunicación con la vía y los diferentes puestos de mando para garantizar una funcionalidad adecuada. Como se comentó anteriormente, uno de los avances más importantes que ha sufrido este tipo de comunicación fue la implantación del sistema GSM-R, sistema de telefonía GSM, pero acondicionado al entorno ferroviario. A medida que mejora la calidad y la fiabilidad del transporte urbano masivo, la comunicación tren-tierra es un componente clave dentro de las estrategias de los operadores ferroviarios, ya que ofrece ahorros significativos de

costes y una mayor eficiencia operativa en cuanto a la seguridad del tren, funcionamiento del sistema de transporte, experiencia de los pasajeros, y también implica en una mejoría en la imagen de la propia marca, así como ingresos adicionales.

Actualmente, diferentes son las tecnologías que están teniendo cabida dentro de este ámbito. El uso de tecnologías inalámbricas e Internet está aumentando en la industria ferroviaria, lo que permite comunicaciones bidireccionales tren-tierra. Sin embargo, este tipo de enlaces de comunicación aplicados a este entorno, tienen que responder a varios retos relacionados con aspectos como cobertura, ancho de banda, interrupciones de comunicación, múltiples interfaces de red para comunicaciones y diferentes prioridades en la transmisión de datos, además de responder al mismo tiempo a la Calidad del Servicio (QoS) exigida por las aplicaciones.

En este tipo de comunicación se barajan muchas opciones, desde comunicaciones de telefonía móvil tradicional como GPRS, UMTS, LTE, etc. hasta comunicaciones de banda ancha, como Wi-Fi (IEEE 802.11) (ver **Apéndice 1**) o, incluso, WiMAX (IEEE 802.16.2). Por el momento, la velocidad de transmisión y la anchura de banda en el intercambio de información es mucho mayor en redes de área local Wi-Fi que en otras tecnologías. Además, el coste para la instalación de este tipo de tecnología es muy bajo en comparación con otros, eso sí, con la desventaja de tener una distancia de cobertura pequeña.

Este proyecto se ha centrado en dar una solución a este tipo de comunicación haciendo uso de tecnología Wi-Fi y solventando, además, aquellos problemas que surgen al insertar este tipo de tecnología en un tipo de comunicación que demanda una gran disponibilidad y fiabilidad en los datos. Un ejemplo de lo que se busca se puede contemplar en la **Figura 2.3**:

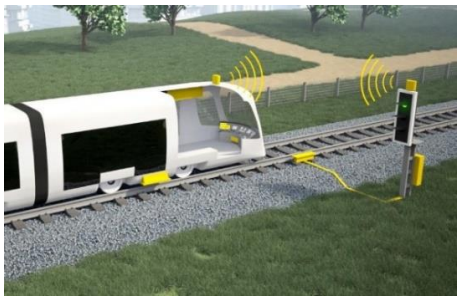


Figura 2.3: Ejemplo de una comunicación tren-tierra

A continuación, en la **Figura 2.4**, se presenta un esquema donde se visualiza la relación entre la disponibilidad de los datos y el ancho de banda que necesita cada uno de los servicios tren-tierra comentados anteriormente:

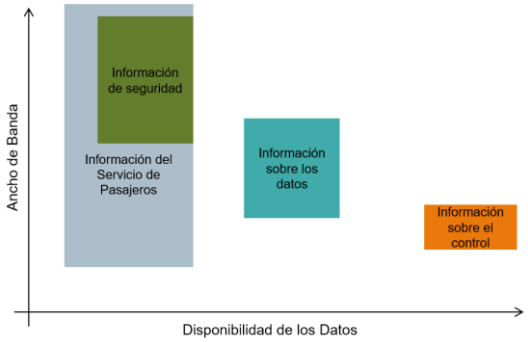


Figura 2.4: Ancho de banda y disponibilidad de datos para los servicios tren-tierra

En la **Figura 2.4** se observa qué tipo de información se debería priorizar para ser transmitida en el momento que se diseña este tipo de sistemas.

2.3 LA CAPA DE ENLACE

La capa de enlace se encarga del intercambio de tramas entre nodos por un medio de red físico. Habilita para que capas por encima de la capa de enlace puedan acceder a los medios y controlar cómo se colocan y reciben los datos en éstos. Se denomina nodo a los dispositivos conectados a un medio común. Esta capa, específicamente, se encarga de la realización de estas dos funciones básicas:

- Admite paquetes de la capa de red y los empaqueta en unidades de datos llamadas tramas.
- Realiza el control de acceso a medios y tiene la capacidad de detectar errores.

La capa de enlace se encarga de la separación efectiva entre las transiciones de un medio a otro que suceden a medida que la trama de datos es reenviada en el proceso de comunicación de las capas por encima de ésta. La capa de enlace toma los paquetes y dirige éstos a protocolos de capas superiores. Estas capas superiores no tienen que preocuparse en qué tipo de medio va a realizarse la comunicación. Con medio se quiere referir al material por el cual los datos viajan, ya puede ser cable de cobre, fibra óptica o aire.

Al final de este documento, más concretamente en el apéndice 1, se da una explicación técnica y teórica sobre los diferentes estándares que existen en la capa de enlace, con especial atención al Wi-Fi y su estándar 802.11, siendo estos un apartado fundamental para entender este proyecto. Se hace muy recomendable que el lector, antes de continuar con la lectura, se lea la explicación elaborada sobre el Wi-Fi y su funcionamiento. Además, se realiza una comparación entre el estándar 802.11n (estándar que se utiliza en los dispositivos Wi-Fi de este proyecto debido a su compatibilidad con éstos), y el estándar 802.11ac (estándar que más adelante se comprobará y verificará que será el ideal para el tipo de arquitectura que se va a realizar) (ver **Apéndice 1**).

2.4 LA CAPA DE RED. REDES IP Y PROTOCOLOS

Ubicada en la Capa 3 del modelo de Interconexión de Sistemas Abiertos (OSI), la función principal de la capa de red es mover paquetes de datos hacia y a través de otras redes. Los protocolos de la capa de red logran este objetivo empaquetando los datos con la información correcta de la dirección de red, seleccionando las rutas de red apropiadas y enviando los datos empaquetados a la capa de transporte (Capa 4). Los protocolos existentes que generalmente se relacionan con la capa de red OSI incluyen la parte IP del Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP).

La información en cuanto al enrutamiento contenido dentro de un paquete incluye la fuente del host emisor y el destino final del host remoto. Esta información está

contenida dentro de la cabecera de la capa de red que encapsula los paquetes de red en la capa de enlace (Capa 2). La diferencia clave entre la información de transporte contenida en la capa de enlace, en comparación con aquella contenida en la capa de red, es que la información puede moverse fuera de la propia red local para alcanzar a los hosts en ubicaciones de subredes distintas.

La capa de red tiene, como función principal, permitir la interconexión y el enlace entre diferentes redes. Esta funcionalidad la consigue enviando las tramas de datos a los *routers* ubicados en la red, que son los que se encargan del enrutamiento entre diferentes subredes. Es decir, utilizan diferentes algoritmos y protocolos para decretar las mejores rutas para que estos datos viajen. La capa de red se basa en el Protocolo de Control de Mensajes de Internet (ICMP) para el diagnóstico y detección de errores para garantizar que las tramas de datos se envían de manera correcta. La calidad del servicio (QoS) también está disponible, para permitir que cierto tráfico sea priorizado sobre otro tráfico.

Para el entendimiento de los protocolos utilizados para el diseño de la red en el apartado 4 del proyecto, se hace casi obligatorio hacer una lectura del apéndice 2 donde se explican, teóricamente, los protocolos ICMP, Ping y Tracert, VRRP (Protocolo de Redundancia de *Router* Virtual), PRP (Protocolo de Redundancia en Paralelo) e iPRP (Protocolo de Redundancia en Paralelo Industrial) de una manera no excesivamente profunda, pero van a resultar, sin lugar a duda, como ayuda al lector a la hora de entender el proceso seguido de elaboración de la arquitectura (ver **Apéndice 2**). Se ha decidido introducir esta parte del proyecto en un apéndice debido al número de páginas que abarcaban, pero no por ello es menos importante.

2.5 CONCLUSIONES

En este capítulo, se han definido los diferentes servicios embarcados en el tren, los cuales se han dividido en función de la importancia de cada uno a la hora de garantizar la seguridad del tren. También se ha expuesto qué es la comunicación tren-tierra junto con las posibles tecnologías que podrían tener cabida en una comunicación de este tipo. Además, se indican qué tipo de servicios se deberían priorizar en el momento de diseñar este tipo de sistemas.

Para finalizar con este apartado, se hace necesario introducir la capa de enlace y la capa de red del modelo OSI. Estas dos capas son imprescindibles de entender para poder solucionar los diferentes problemas que aparecían a medida que se iba configurando la red. En la capa de enlace se hace especial hincapié al estándar 802.11 (Wi-Fi) debido a que será la tecnología en la que se base la red. En la capa de red se definen los principales protocolos utilizados a lo largo del proyecto.

3

ANÁLISIS DE REQUISITOS

3.1 INTRODUCCIÓN

En esta sección del trabajo, se calcula una aproximación total del ancho de banda y latencia requerida en una comunicación tren-tierra teniendo en cuenta todos los servicios comentados en el apartado anterior, y se comprueba, por tanto, la posibilidad o viabilidad de usar una tecnología Wi-Fi en una comunicación de este tipo.

3.2 REQUISITOS EN UN ENTORNO FERROVIARIO

En el momento que se va a diseñar la red la cual tenga la capacidad de soportar a los servicios comentados, se debe tener en cuenta los parámetros de calidad de cada uno. Este parámetro viene determinado por el nivel de QoS (*Quality of Service*), que se trata de aquellas particularidades que indican y permiten saber si, un determinado servicio de telecomunicaciones tiene la capacidad de cumplir con las necesidades implícitas y explícitas del cliente que use este servicio. Este parámetro variará en función de los requerimientos e importancia que tengan cada uno de los servicios mencionados anteriormente, en este caso se valoran dos parámetros QoS:

- **Tasa binaria o *Troughput* (bits por segundo - b/s):** Capacidad de transmisión de datos por segundo por el medio.
- **Latencia (milisegundos - ms)**: Retardo que padece una trama dentro de la red desde un host origen hasta un host destino.

A continuación, se estudian los valores de los comentados parámetros de calidad para cada servicio específico.

3.2.1 Requisitos en cuanto a los Servicios Vitales

Dentro de este grupo se encontraban dos subgrupos que englobaban aquellos servicios relacionados con la seguridad y el control del tren.

3.2.1.1 Requisitos para Información de Control y sobre Datos

Para poder cumplir con las funcionalidades necesarias en este tipo de sistemas descritos anteriormente y conseguir su correcto funcionamiento, la arquitectura de red que se diseña debe cumplir con los siguientes requisitos.

La tasa binaria de un sistema CBTC es de aproximadamente **2-3 kb/s** [14], con eso sería más que suficiente para poder cumplir con todas las funcionalidades que tiene este sistema. Además de esta tasa binaria, se debe tener tiempos de latencia **menores a 100 ms**. Si un tren, por ejemplo, circula a una velocidad media de unos 100 km/h, que en metros por segundo son unos 27,8 m/s, si hubiera un retardo punto a punto superior a los 100 ms establecidos como máximo, al exclusivamente enviar datos de ubicación y velocidad, la información de posicionamiento y velocidad del tren que llega, no se podría tomar como dato real, debido a que el tren en el momento que esos datos llegan podría estar unos 2,78 metros más delante de lo que realmente indican los datos debido a este retardo.

Debido a que los dispositivos no son perfectos y pueden fallar e incluso llegar a caerse, al tratarse de un servicio vital para el correcto funcionamiento del tren, es necesario diseñar una red redundante.

3.2.1.2 Requisitos para Información de Voz

Para el correcto funcionamiento de una aplicación de comunicación de voz sobre IP no se necesitan más de **100 kb/s** [14].

En este tipo de comunicaciones que ocurren en tiempo real, es muy molesto para el cliente que se produzcan retardos muy elevados debido a la incomodidad que supone tener una comunicación intermitente con otra persona. De hecho, puede llegar al punto de no tener ninguna utilidad si los tiempos entre paquetes son muy elevados. Para la determinación de qué latencia máxima podría existir en una comunicación de este tipo, se analiza a partir de qué latencias el oído humando es capaz de detectar parones en la comunicación. Este tiempo se encuentra alrededor de los **150 ms** [1], por lo que lo deseable sería que el retardo fuera siempre inferior a este valor.

3.2.2 Requisitos en cuanto a los Servicios no Vitales

Dentro de este grupo de servicios se engloban otros dos subgrupos de aquellos servicios que no son tan relevantes a la hora de hablar de disponibilidad en una comunicación ferroviaria.

3.2.2.1 Requisitos en Información de la Seguridad (Sistemas CCTV)

Para tener una correcta visualización en tiempo real, se decide optar por cámaras con una resolución de 720P HD, con una calidad del vídeo media. El tamaño medio por *frame* en este tipo de cámaras es de 80 KB. Este tipo de cámaras sería suficiente en términos de calidad visual. Bastaría con utilizar una tasa de unas 15 *frames*/s, debido a que el ser humano procesa como imágenes individuales alrededor de las 12 imágenes por segundo, es decir, se perdería esa sensación de continuidad en el vídeo.

Para cumplir con las restricciones recientemente comentadas, se calcula la anchura de banda necesaria. Si se deseara tener una visualización al momento de cada cámara, se necesita una velocidad de transmisión de **9.6 Mb/s por cada cámara** que se coloca en cada tren con una latencia inferior a **150 ms** [1]. Se recuerda que esto no siempre es necesario debido al uso de sistemas de guardado, que permiten el acceso a contenido cuando se necesite.

3.2.2.2 Requisitos en Información sobre el Viaje al Pasajero y Servicios para Clientes

Sin lugar a duda, este ha sido el apartado más complicado de todos los servicios a la hora de definir qué tasa binaria y latencia se necesitaría para su correcto funcionamiento, debido al tipo de información más avanzada o menos que se puede ofrecer al cliente en función de lo moderno que pudiera ser el tren, y en función de la cantidad de datos por segundo que necesite o demande cada cliente. Por tanto, al tener tanta variedad de dispositivos de visualización o acústicos que se utilizan en un entorno ferroviario, se ha optado por elegir un ancho de banda y latencia medio entre todas las opciones. Así pues, una buena aproximación sería una tasa binaria de unos **500 kb/s por tren** [14] con un **retardo máximo de unos 100 ms**.

Para el caso de aquellos servicios orientados al cliente, como pueden ser los juegos online, descarga de vídeos y ficheros y el acceso a internet, los cuales son sin lugar a duda los servicios más complicados de implementar debido al gran ancho de banda que necesitan, se podría considerar una buena aproximación en cuanto a la tasa binaria de unos **700 kb/s necesarios para cada usuario** con una **latencia inferior a 100 ms** [14].

3.3 REQUISITOS TOTALES NECESARIOS

Para una cómoda visualización de todos los requisitos mínimos necesarios que se necesitan cumplir para tener un correcto funcionamiento en una comunicación tren-tierra, se adjunta la **Tabla 3.1**:

Tabla 3.1: Requisitos totales en un entorno ferroviario

TIPO DE SERVICIO	SERVICIO	TASA BINARIA MÍNIMA POR TREN	LATENCIA	TASA BINARIA EN UNA CELDA (DOS TRENES EN DIRECCIONES OPUESTAS)
Servicio Vital	Información de Control y sobre Datos (CBTC)	**2-3 kb/s**	**< 100 ms**	**4-6 kb/s**
Servicio Vital	Información de Voz	**100 kb/s**	**< 150 ms**	**200 kb/s**
Servicio no Vital	Información de la Seguridad (Sistemas CCTV)	9.6 Mb/s con una media de unas 6 cámaras operando simultáneamente = **57.6 Mb/s**	**< 150 ms**	9.6 Mb/s con una media de unas 6 x 2 cámaras operando simultáneamente = **115.2 Mb/s**
Servicio no Vital	Información sobre el Viaje al Pasajero y Servicios para Clientes	500 kb/s de información sobre el tren al pasajero + (700 kb/s por dispositivo x 280 usuarios conectados simultáneamente) = **196, 5 Mb/s**	**< 100 ms**	500 x 2 kb/s de información sobre el tren al pasajero + (700 kb/s por dispositivo x 560 usuarios conectados simultáneamente) = **393 Mb/s**
TOTAL		**254,2 Mb/s**	**< 100 ms**	**508,4 Mb/s**

Para la realización de esta tabla se han usado aproximaciones de una situación real que se pudiera dar en un servicio de tren urbano. Las aproximaciones son: se estima que el número máx. de pasajeros a bordo puede ser de unos **700 pasajeros**. Se supone un dispositivo por cada usuario y se plantea una situación en la que el tren estando al 100% ocupado, solo el **40%** de ellos solicitaran recursos a la red al mismo tiempo.

Otra aproximación más realizada es que el tren está compuesto por **6 coches**, en cada coche se ubicarán tres cámaras de vigilancia, lo que conforman **18 cámaras** en total que, debido a la imposibilidad de visualizar 18 cámaras a la vez por una persona, se supone para el cálculo una media de 6 cámaras operando al mismo tiempo.

3.4 CONCLUSIONES

Con los requisitos necesarios mínimos totales ya calculados, se comprueba que existe la posibilidad de realizar un diseño de un sistema de comunicación tren-tierra de banda ancha con tecnología Wi-Fi usando el estándar 802.11ac, dado que este cumple con las restricciones en cuanto a ancho de banda, siendo ésta de aproximadamente 1,3 Gbit/s (este valor variará en función de la distancia del cliente al punto de acceso en cada momento). Además, se comprueba que se tendrá la capacidad de utilizar los mismos puntos de acceso distribuidos por la vía para dos trenes, los cuales circulan en vías paralelas pero en direcciones opuestas, lo que permite un ahorro a la mitad en cuanto al número de puntos de acceso distribuidos por cada vía.

4

DESARROLLO Y DISEÑO DE LA SOLUCIÓN

4.1 INTRODUCCIÓN

En este apartado del trabajo, se va a ir explicando los pasos seguidos hasta obtener el diseño hardware final de la solución, con las características correspondientes para poder utilizarse en un ejemplo de aplicación ferroviaria, utilizando tecnología *Wireless*. Primero se muestra la estructura final del proyecto, el cual se comprueba que cumple con los requisitos necesarios de disponibilidad y fiabilidad y, por supuesto, de ancho de banda suficiente en el apartado 5 de este proyecto. A partir de este esquema, se irá desglosando éste en subgrupos en función del proceso seguido desde el comienzo hasta la solución final observada.

Primero de todo se comienza explicando las configuraciones realizadas en los dispositivos Wi-Fi, los cuales hay que parametrizarlos indicando el estándar en el que trabajarán, siendo éste el 802.11n (ya se indicó en apartados anteriores que éste no sería el ideal, pero por motivos de disponibilidad de dispositivos en la empresa se utiliza este estándar, dado que es el compatible con los dispositivos que se disponen), configurar el protocolo iPRP en ellos, configurarles sus puerta de enlace, asignar las diferentes VLANs (Red de Área Local Virtual) que tendrán en cada puerto, indicar qué tipo de antena utilizarán, etc.

Posteriormente, como se explica en el apéndice 2 (ver **Apéndice 2),** para ser capaces de trabajar con iPRP se necesita de dos dispositivos más a cada lado de los clientes y los puntos de acceso. Se necesita un *switch* gestionable a cada lado y, también, los dos *switches* tipo RNA (Acceso a Red Redundante) que trabajan con PRP, que se encargan de la duplicación de las tramas a un lado de la comunicación y, al otro lado, descartan aquella que llega más tarde, para no tener paquetes duplicados.

A continuación, debido al problema de disponibilidad que podría generar el fallo de dispositivos, fallos en el cableado, etc. se opta por utilizar el protocolo VRRP para dar solución a esto. Éste se explica también en el apéndice 2 (ver **Apéndice 2**). Para conseguir ese *router* virtual en VRRP, se necesita de un *router* adicional y, por tanto, de otro *switch* RNA más que, en función del *router* que esté funcionando, definido éste por el protocolo VRRP, será el que se encargue de duplicar o eliminar la trama ya duplicada

al otro lado de la comunicación.

Es importante que una vez ya se tiene la arquitectura bien configurada y que todos los equipos son capaces de comunicarse los unos con los otros (comprobación mediante Ping), añadir los dispositivos *firewall* al final de cada lado de la red para la protección frente a accesos no autorizados. Aunque en este proyecto no se entrará en detalle sobre la declaración de las reglas de *firewall* oportunas para un servicio real ferroviario, exclusivamente estos *firewalls* tienen funcionalidad *routing*.

Fuera de lo que sería el diseño de la red que se implantaría en los trenes y la vía, se añaden dos PLCs (Controlador Lógico Programable) S7-1200, uno de ellos simulará el funcionamiento de lo que sería el control de mandos de la estación pertinente, y el otro actuará como si fuera el sistema de control del propio tren. Lo que se busca con esto es, simular una comunicación que pudiera darse en una situación real en una comunicación tren-tierra para usarlo como validación de la arquitectura. Entre ambos PLCs se crea un enlace o comunicación S7. Esta comunicación S7 entre PLCs no es trivial configurarla ni programarla, pero debido a su extensión no se añade en este apartado. Puede acudir al apéndice 5 para ver el proceso de configuración seguido, concretamente en este proyecto, si fuese de su interés (ver **Apéndice 5**).

Además, también fuera de lo que sería la arquitectura ya diseñada para el tren y la distribuida por la vía, se añade a la red un cliente Wi-Fi más que, junto a un teléfono móvil con acceso a Internet o un módem (gama SCALANCE M Siemens), va a permitir el tener un acceso remoto a la red. Esto permitirá poder realizar un mantenimiento o gestión de la red de una forma remota y segura. Para conseguir esto, explicado *grosso modo* debido a que es algo adicional al proyecto, primero se configura la IP de cliente Wi-Fi y la IP del puerto externo del *firewall* (S615), al que estará conectado el cliente Wi-Fi vía *Ethernet*. Para ello se hace uso de DHCP (Protocolo de Configuración Dinámica de Host) para la asignación automática de IPs. El encargado de esta asignación será el teléfono móvil al que se conecte el cliente Wi-Fi. A continuación, una vez conectado el cliente Wi-Fi al teléfono móvil o módem pertinente, con las configuraciones correspondientes realizadas para que todo comunique correctamente, se conseguirá que la red completa salga a Internet a través del *firewall* (S615_AP). Una vez se comprueba que todos los dispositivos de la red tienen acceso a Internet, se necesita de un programa para poder acceder remotamente y de manera segura a ella. Para este acceso remoto se utiliza Sinema Remote Connect. Tampoco se hablará en detalle sobre este software o aplicación, pero básicamente, es un servidor contra el que cerrar túneles VPN (Red Privada Virtual) y donde se puede tener una gestión eficiente de éstos. Para la configuración de cómo conectar o dar de alta un dispositivo en Sinema Remote Connect, se deja en la bibliografía documentación para este proceso [15]. Una vez declarado el *firewall* (S615) en Sinema Remote Connect, se puede crear lo que se denomina una relación entre dispositivos, que no es más que una relación de comunicación entre grupos compuestos por dispositivos y/o usuarios con los que se quiere comunicar. En este caso, se crea una relación de comunicación con el usuario con el cual se iniciará sesión para acceder a la red, y otra relación con el PC donde se tiene instalada la plataforma para la gestión, mantenimiento y monitorización de dispositivos llamada Sinec NMS, con la que se podrá tener un control de la red.

4.2 ESTRUCTURA FINAL DEL DISEÑO HARDWARE

La **Figura 4.1** muestra la estructura final de lo que sería el proyecto.

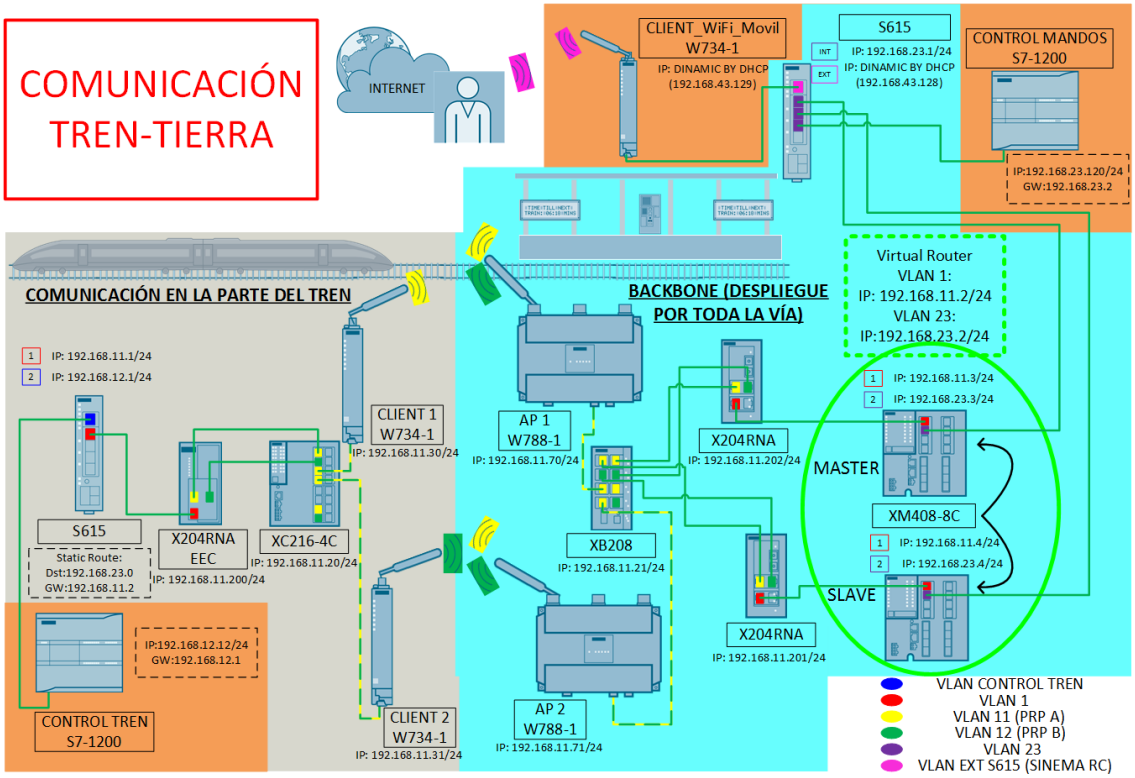


Figura 4.1: Estructura final hardware del proyecto

Se puede observar en la **Figura 4.1** la división de lo que sería la instalación de los dispositivos en la parte del tren, y la instalación o despliegue a realizar por toda la vía. Los dispositivos resaltados con un fondo naranja son dispositivos adicionales que se han utilizado durante el proyecto, pero que no tienen ningún tipo de afectación en la red en cuanto a funcionalidad. Han sido utilizados, exclusivamente, para el proceso de validación del proyecto y para poder tener un acceso remoto a la red para la gestión y parametrización de algunos dispositivos a través de Internet debido al confinamiento.

Además, se facilita una leyenda para poder entender bien a qué VLAN se referencia cada uno de los colores marcados en cada puerto. Las líneas rayadas de color verde y amarillo en los dispositivos Wi-Fi, indican que se transportan tramas *tagueadas* con ambas VLANs, VLAN 11 y VLAN 12.

Para proporcionar una red PRP funcional a través de WLAN (Red de Área Local Inalámbrica), a cada módulo o dispositivo se le asigna una tarea específica.

La **Tabla 4.1** a continuación resume básicamente de lo que se encarga cada módulo o dispositivo.

Tabla 4.1: Tarea de cada dispositivo

MÓDULO	TAREA
S7-1200	Son PLCs que simulan la comunicación que existiría entre un puesto de mandos y el control del tren. Se utilizan para crear una comunicación S7 y poder validar la arquitectura.
S615	El S615 es un *firewall* en capa de enlace y capa de red que se encargará de proteger la red frente a accesos no deseados, pero en este proyecto solo tendrá funcionalidad *routing*.
X204RNA / X204RNA EEC	El X204RNA es un RedBox y conecta SAN (Nodo adjunto estándar) a ambas redes (LAN A o LAN B) y asume las funciones de PRP en nombre de todas las SAN conectadas a él.
XC216-4C / XB208	El XC216-4C y XB208 son *switches* habilitados para VLAN. Separan las dos redes en el lado del punto de acceso y del cliente a través de VLAN y permite que se sincronicen entre sí clientes y puntos de acceso entre sí.
W734-1	El W734-1 es un cliente. Junto con el W788-1, el cliente establece una red inalámbrica.
W788-1	El W788-1 es un punto de acceso WLAN y construye una red inalámbrica junto con un cliente WLAN.
XM408-8C	El XM408-8C va a funcionar en la aplicación como *router* capaz de enrutar los dispositivos conectados a él ubicados en otra subred.

Algunos dispositivos aparecen varias veces en el esquema, como por ejemplo los puntos de acceso. Para poder distinguir entre ellos, se diferencian con un único nombre a cada uno. La **Tabla 4.2** muestra qué direcciones IP y nombres se usan, aunque esto se observa perfectamente en el esquema al comienzo de este apartado:

Tabla 4.2: Asignación de IP y nombre a dispositivos

Componente	Dirección IP	Nombres
S7-1200 (Lado de los Clientes)	192.168.12.12	Control_Tren
S615(Lado de los Clientes)	192.168.11.1	S615_Cliente
X204RNA EEC	192.168.11.200	RedBox_Cliente
XC216-4C	192.168.11.20	XC216_Cliente
W734-1 (Cliente 1)	192.168.11.30	Client_LAN_A
W734-1 (Cliente 2)	192.168.11.31	Client_LAN_B
W734-1 (Wi-Fi Móvil)	192.168.43.129 (Dynamic by DHCP)	Cliente_WiFi_Movil
W788-1(AP 1)	192.168.11.70	AP_LAN_A
W788-1(AP 2)	192.168.11.71	AP_LAN_B
XB208	192.168.11.21	XB208_AP
X204RNA (Master)	192.168.11.202	RedBox_AP_Master
X204RNA (Slave)	192.168.11.201	RedBox_AP_Slave
XM408-8C (*Router* Virtual)	192.168.11.2	
XM408-8C (Master)	192.168.11.3	XM408_Master
XM408-8C (Slave)	192.168.11.4	XM408_Slave
S615 (Lado de los AP)	192.168.23.1	S615_AP
S7-1200 (Lado de los AP)	192.168.23.120	Control_Mandos

4.3 PARAMETRIZACIÓN DE DISPOSITIVOS Wi-Fi - PUNTOS DE ACCESO (W788-1) Y CLIENTES (W734-1) EN MODO iPRP

Para aumentar la redundancia de los enlaces de radio, se puede configurar la WLAN para que los clientes puedan comunicarse, teóricamente, con cada punto de acceso. iPRP va a evitar que ambos clientes escaneen simultáneamente la misma red de radio y que los dos clientes inicien sesión en la misma interfaz de un punto de acceso.

En esta aplicación, las redes independientes requeridas por PRP (LAN A o LAN B) están diseñadas de forma redundante con Puntos de Acceso Virtuales (VAP).

La **Tabla 4.3** muestra qué SSID se usaron:

Tabla 4.3: Interfaz y nombre de cada SSID para cada PRP

Punto de Acceso	Interfaz	SSID	Red PRP
AP_LAN_A	VAP 1.1	PRP_A	LAN A
AP_LAN_A	VAP 1.2	PRP_B	LAN B
AP_LAN_B	VAP 1.1	PRP_A	LAN A
AP_LAN_B	VAP 1.2	PRP_B	LAN B

Para implementar las redes independientes requeridas por PRP (LAN A o LAN B), la red está separada por VLANs para iPRP.

La **Tabla 4.4** muestra qué VLAN está asignada a qué puerto:

Tabla 4.4: Asignación de VLANs a cada puerto de dispositivos Wi-Fi

Módulo	Puerto	VLAN	Nota
AP_LAN_A AP_LAN_B	VAP 1.1	VLAN 11	VLAN para la red PRP LAN A
	VAP 1.2	VLAN 12	VLAN para la red PRP LAN B
	P1	VLAN 11 + VLAN 12	Para sincronizar los puntos de acceso
Client_LAN_A	VAP 1.1	VLAN 11	VLAN para la red PRP LAN A
	P1	VLAN 11 + VLAN 12	Sincronización de los clientes
Client_LAN_B	VAP 1.1	VLAN 12	VLAN para la red PRP LAN B
	P1	VLAN 11 + VLAN 12	Sincronización de los clientes

Una vez explicado a qué corresponde cada VLAN y VAP en los dispositivos Wi-Fi, se va a ir explicando qué parámetros como el estándar Wi-Fi, potencia de transmisión, antena utilizada, etc. se ha configurado en cada dispositivo, pero sin ir en detalle de cómo se ha realizado esta configuración, debido a que se extendería demasiado.

La **Figura 4.2** expone un resumen de los parámetros establecidos en el punto de acceso 1 (**AP_LAN_A**) [23]:

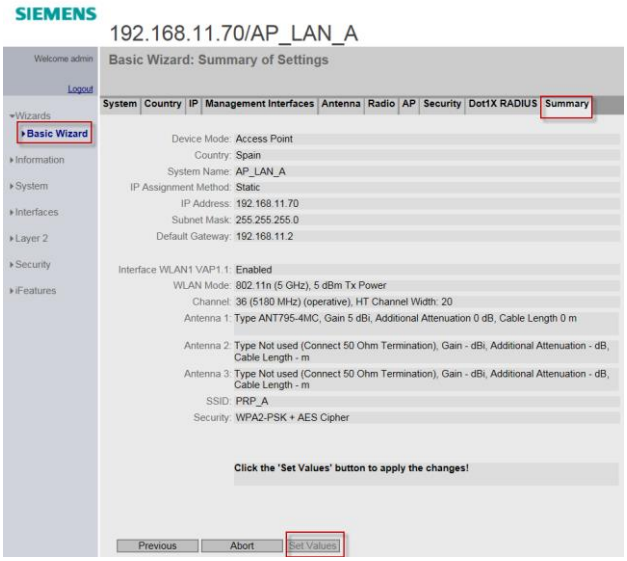


Figura 4.2: Resumen parámetros Punto de Acceso 1

En la figura superior se observa el país donde se va a trabajar con el dispositivo, esto es importante indicarlo debido a que, una vez hecho esto, el equipo automáticamente proporcionará al usuario aquellos canales y antenas disponibles de acuerdo con la selección de este país. Además, el dispositivo puede proporcionar información sobre la potencia de transmisión permitida en ese país. Se indica también el nombre que se quiere asignar al dispositivo y se parametriza también la máscara de subred, puerta de enlace del dispositivo y dirección IP.

Se configura también el estándar o modo en el que trabajará el dispositivo que, como se había comentado en apartados anteriores será el 802.11n, utilizando 5 GHz como frecuencia con una potencia máxima de transmisión de 5 dBm (más que suficiente en este caso, debido a la cercanía entre clientes y APs (Puntos de Acceso) en la instalación realizada en el laboratorio). Se configura también un canal fijo de comunicación usando el canal 36 como canal de comunicación.

En cuanto a la antena, se usará una de tipo ANT795-4MC (ver **Apéndice 4**), la cual tiene una ganancia de 5 dBi conectada directamente al dispositivo. Las conexiones no utilizadas deben estar provistas de una resistencia de 50 Ω.

Se define un SSID (Identificador de Conjunto de Servicios) para la interfaz WLAN siendo esta “PRP_A”. Además, se configura un cifrado y autenticación para proteger así la red. Estas configuraciones de seguridad se establecen de manera idéntica en las configuraciones de seguridad del Cliente "Client_LAN_A".

Debido a que en esta aplicación que se está implementando los enlaces de radio están diseñados de forma redundante, para hacer que la red inalámbrica sea redundante, se configura las mismas redes inalámbricas en cada punto de acceso para que los clientes puedan conectarse, teóricamente, a cada punto de acceso cada uno. Con iPRP configurado se evitará que ambos clientes escaneen la misma red inalámbrica al mismo tiempo y que los dos clientes inicien sesión en la misma interfaz de un punto de acceso. En la **Figura 4.3** se observa esta configuración:

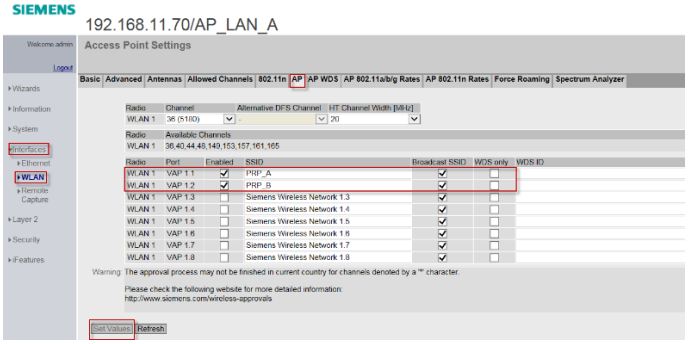
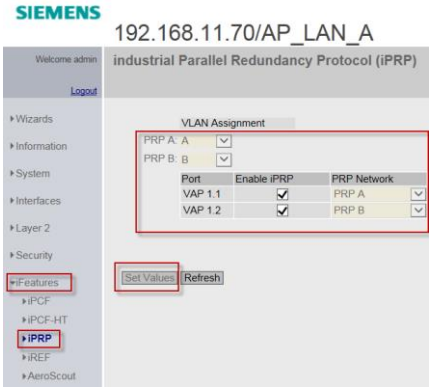


Figura 4.3: Configuración de ambos SSID en Punto de Acceso 1

También se configura un cifrado y autenticación para proteger así el acceso a través de este SSID.

Por último, se realiza la configuración iPRP y se asigna como VLAN de gestión la VLAN A, como se contempla en la **Figura 4.4** y la **Figura 4.5**:



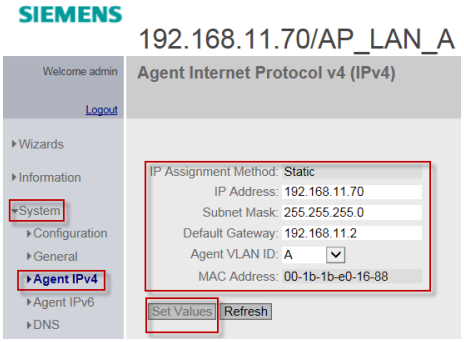


Figura 4.4: Asignación VLAN de gestión Punto de Acceso 1

Figura 4.5: Configuración iPRP en Punto de Acceso 1

A continuación, se indican los mismos parámetros, pero para el punto de acceso 2 (**AP_LAN_B**) [23] que, en este caso, al ser parecida la configuración con el anterior punto de acceso, solo se comentarán en qué detalles se diferencian.

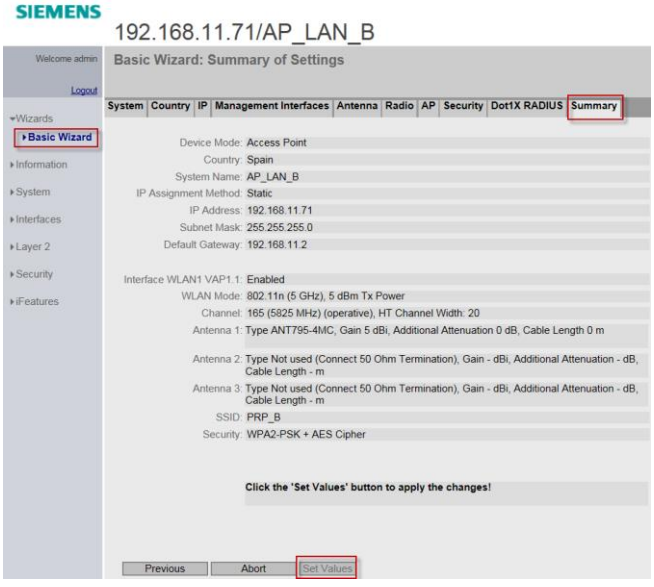


Figura 4.6: Resumen parámetros Punto de Acceso 2

Como se puede observar en la **Figura 4.6**, se configura otro canal fijo de comunicación, en este caso el 165 (para que no haya solape junto con el otro AP) y el nombre del SSID será “PRP_B”.

Se realiza el proceso contrario que en el punto de acceso anterior, se crea una nueva interfaz WLAN añadida con el nombre “PRP_A” como se ve en la **Figura 4.7**.

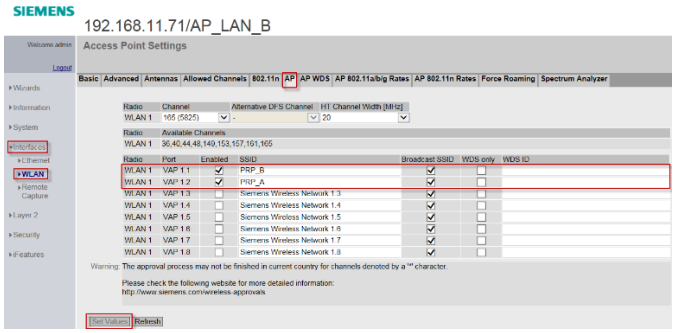
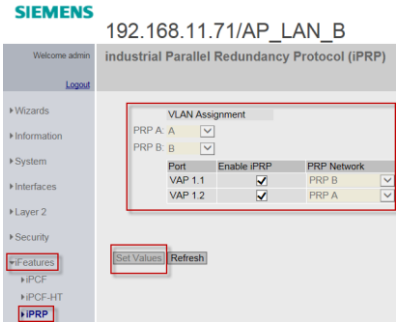


Figura 4.7: Configuración de ambos SSID en Punto de Acceso 2

Por último, se realiza la configuración iPRP (ver **Figura 4.9**), diferente en este caso que la realizada en el AP 1 y se asigna como VLAN de gestión la VLAN B (ver **Figura 4.8**).



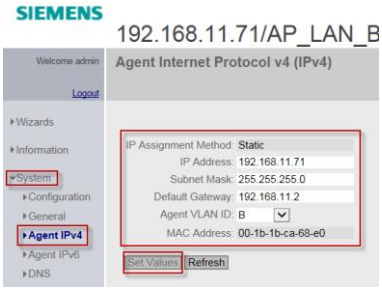


Figura 4.8: Asignación VLAN de gestión Punto de Acceso 2

Figura 4.9: Configuración iPRP en Punto de Acceso 2

La **Figura 4.10** presenta un resumen de los parámetros establecidos ahora en el Cliente 1 (**Client_LAN_A**) [22]:

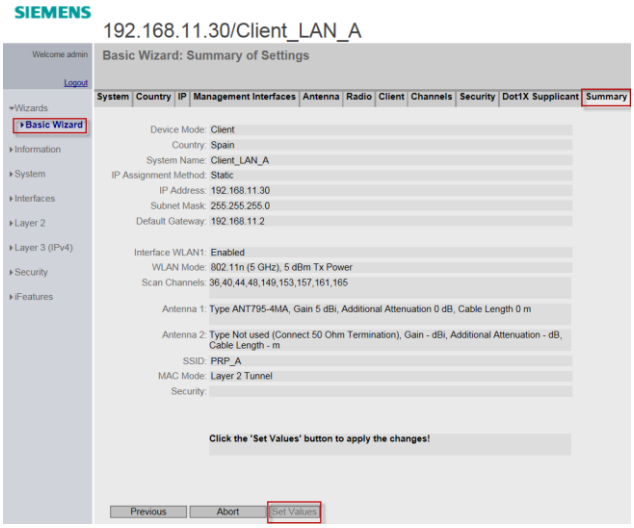


Figura 4.10: Resumen parámetros Cliente 1

En la **Figura 4.10** se observa la máscara de subred, puerta de enlace y dirección IP configurada. Se elige como puerta de enlace la IP del *router* virtual debido a que será el dispositivo con mayor disponibilidad debido a la redundancia de *routers*. Aunque de esto se habla más adelante, en ambos XM408-8C se crea una ruta estática al S615 del lado de los clientes para que los dispositivos puedan comunicar también con la subred 12, teniendo como *gateway* el *router* virtual.

Se indica la zona en la que se va a trabajar, España, esto sirve para que solo se pueda configurar los canales, antenas, potencia máxima, etc. legales o disponibles en el país seleccionado.

En este caso se usa la antena de tipo ANT795-4MA (ver **Apéndice 4**), se configura una transmisión máxima de potencia de 5 dBm, esto es más que suficiente debido a la distancia entre cliente y punto de acceso y no se utiliza ningún tipo de cableado en la antena. La frecuencia a la que se trabaja será 5 GHz del estándar 802.11n. También se ha configurado en qué canales puede trabajar el cliente. Según la configuración de ambos puntos de acceso, solo interesan el canal 36 y 165.

Se indica el nombre SSID que será PRP_A, y se parametriza el cliente para que use la dirección MAC (Control de Acceso al Medio) de la interfaz Ethernet para la interfaz WLAN, esto se hace indicando "*Layer 2 Tunnel*" en "*MAC Mode*".

Otro parámetro clave es que, mientras el cliente está enlazado con un punto de acceso, el cliente sigue buscando puntos de acceso adicionales a los que puede conectarse si es necesario. Si se está utilizando iPRP, se debe cambiar el modo de escaneo en segundo plano. Cuando iPRP está habilitado, el cliente cada vez que realiza *roaming* envía tramas especiales de aviso de *roaming* al otro cliente. Al cliente redundante no se le permite realizar *roaming* durante 500 ms después de la recepción. Para ello, se modifica el escaneo en segundo plano a "*Always*". Estas dos configuraciones se pueden observar en la **Figura 4.11**:

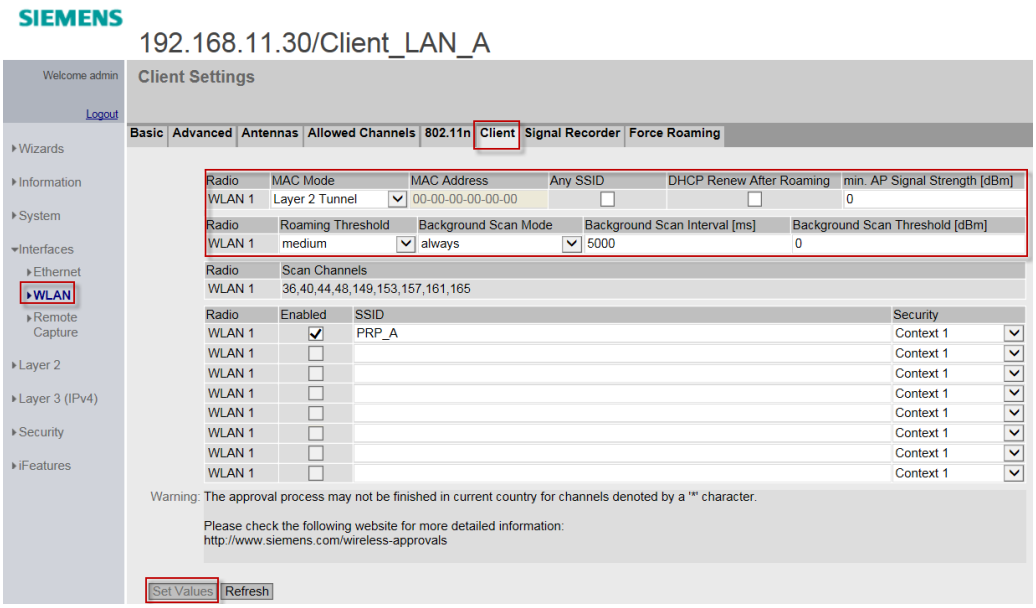


Figura 4.11: Configuración modo de escaneo en segundo plano

Por último, se realiza la configuración iPRP (ver **Figura 4.13**), y se asigna como VLAN de gestión la VLAN A (ver **Figura 4.12**).

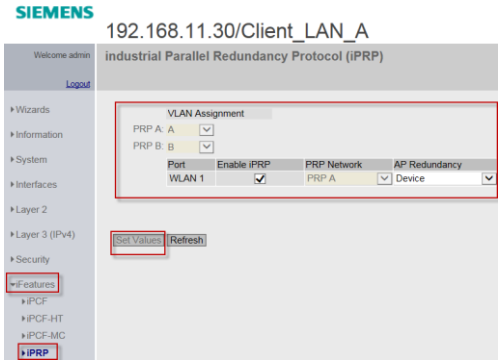


Figura 4.13: Configuración iPRP en Cliente 1

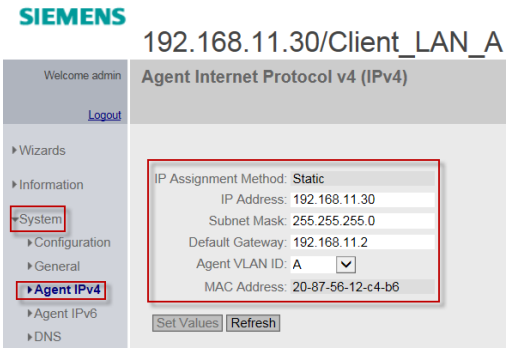


Figura 4.12: Asignación VLAN de gestión Cliente 1

A continuación, en la **Figura 4.14**, se presentan los mismos parámetros, pero para el Cliente 2 (**Client_LAN_B**) [22] que, en este caso, al ser parecida la configuración con el anterior cliente, no se argumenta el porqué de cada parámetro:

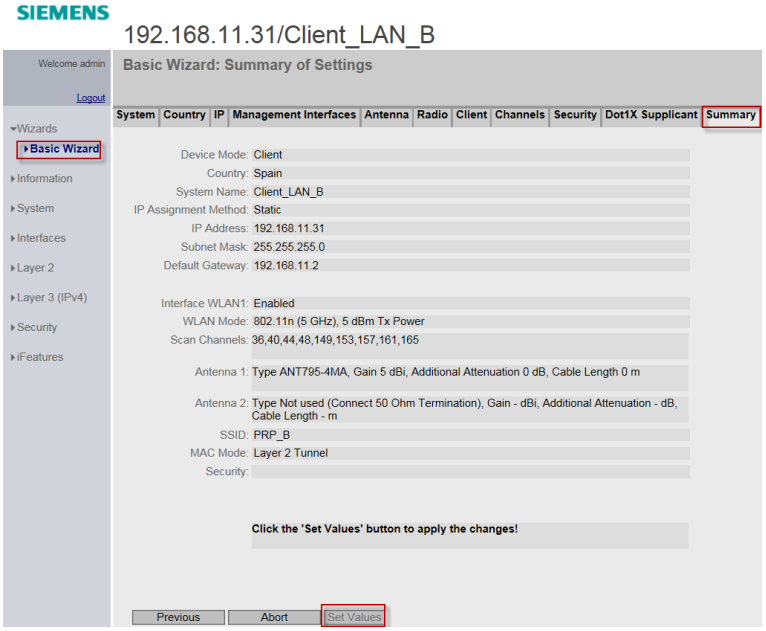


Figura 4.14: Resumen parámetros Cliente 2

Se modifica también el escaneo en segundo plano, se asigna la VLAN de gestión y se configura iPRP. Estas dos últimas configuraciones se observan en la **Figura 4.15** y en la **Figura 4.16**:

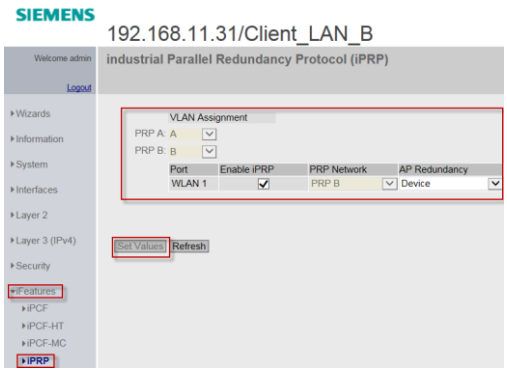


Figura 4.16: Configuración iPRP en Cliente 2

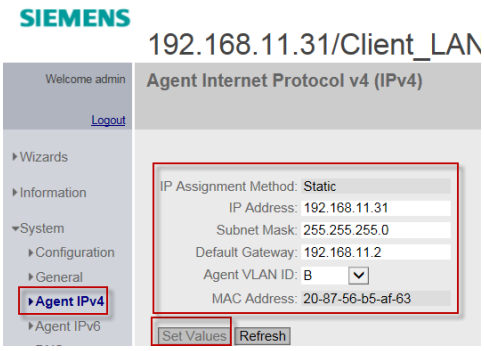


Figura 4.15: Asignación VLAN de gestión Cliente 2

4.4 PARAMETRIZACIÓN DE *SWITCHES* GESTIONABLES (XC216-4C) (XB208) Y DE LOS *SWITCHES* RNA (X204RNA)

Para separar las dos redes PRP y sincronizar los puntos de acceso y clientes al mismo tiempo, se debe configurar las respectivas VLANs en ambos *switches* gestionables. En la **Tabla 4.5** se indica a qué VLAN está asignada cada puerto y cuál es su función.

Tabla 4.5: Asignación de VLAN a cada puerto en los switches gestionables y RNA

Módulo	Puerto	VLAN	Nota
XB208	P1.1 y P1.5	VLAN 11	VLAN para la red PRP LAN A
	P1.2 y P1.6	VLAN 12	VLAN para la red PRP LAN B
	P1.3 y P1.4	VLAN 11 + VLAN 12	Para sincronizar puntos de acceso y clientes
	P1.7	VLAN 11	Para acceder a los dispositivos después de configuración.
	P1.8	VLAN 12	Para acceder a los dispositivos después de configuración.
XC216-4C	P1.1	VLAN 11	VLAN para la red PRP LAN A
	P1.2	VLAN 12	VLAN para la red PRP LAN B
	P1.3 y P1.4	VLAN 11 + VLAN 12	Para sincronizar puntos de acceso y clientes
	P1.7	VLAN 11	Para acceder a los dispositivos después de configuración.
	P1.8	VLAN 12	Para acceder a los dispositivos después de configuración.
X204RNA EEC	PA	PRP A	Duplicación de trama cada una *tagueada* con su RCT
	PB	PRP B	Duplicación de trama cada una *tagueada* con su RCT
	P1	Sin configuración VLAN	
Los dos X204RNA	PA	PRP A	Duplicación de trama cada una *tagueada* con su RCT
	PB	PRP B	Duplicación de trama cada una *tagueada* con su RCT
	P1	Sin configuración VLAN	

Antes de profundizar en la configuración de cada dispositivo, se explica qué significa cada letra configurada en cada puerto:

- "-": El puerto no es miembro de la VLAN especificada.
- "M": El puerto es miembro de la VLAN. Las tramas enviadas en esta VLAN se reenvían con la etiqueta de VLAN correspondiente, sin quitársela.
- “U” (letra mayúscula): El puerto se encarga de etiquetar o eliminar si es un puerto de salida, las tramas que entran o salen con la VLAN correspondiente. Por este motivo, las tramas sin una etiqueta VLAN se envían por este puerto.
- “u” (letra minúscula): Este puerto recibe los telegramas sin etiqueta y con etiqueta de esa VLAN, pero no tiene la capacidad de quitarles la etiqueta de su propia VLAN como si tiene la U mayúscula.

Para la configuración del **SCALANCE XC216-4C** [20] se realiza lo siguiente:

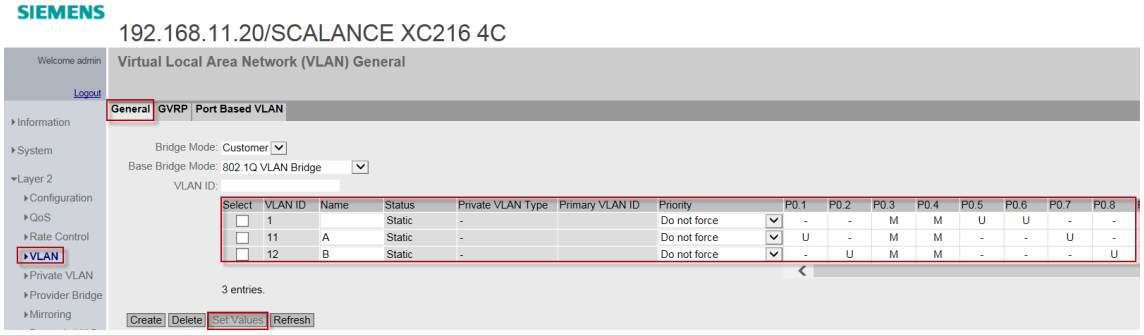


Figura 4.17: Asignación de VLANs a puertos en XC216-4C

En la **Figura 4.17** se puede observar la creación de cada VLAN en cada puerto, siguiendo la nomenclatura explicada arriba. Además de esto, se le asigna su puerta de enlace en la **Figura 4.19** y se indica que la VLAN por la que comunicar con el dispositivo, si se quiere acceder a él, sea la VLAN 11 (VLAN A). Esto es asignar el "TIA Interface" a la VLAN que se desee, como se observa en la **Figura 4.18**.

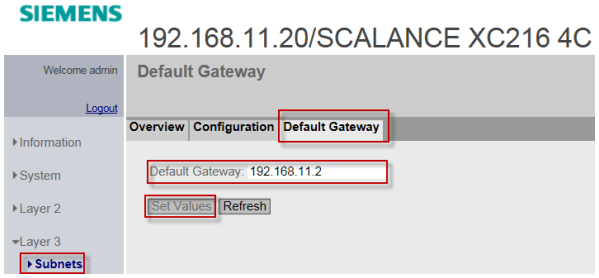


Figura 4.19: Configuración de Puerta de Enlace en XC216-4C

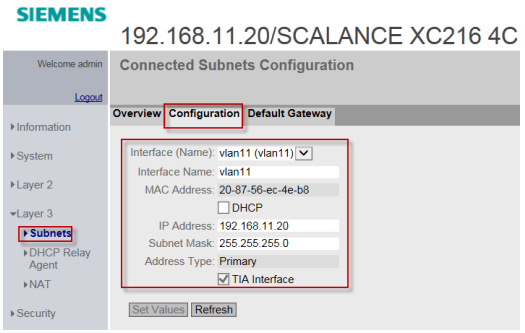


Figura 4.18: Asignación de TIA Interface a VLAN 11 en XC216-4C

Para la configuración del **SCALANCE XB208** [19] se realiza lo siguiente:

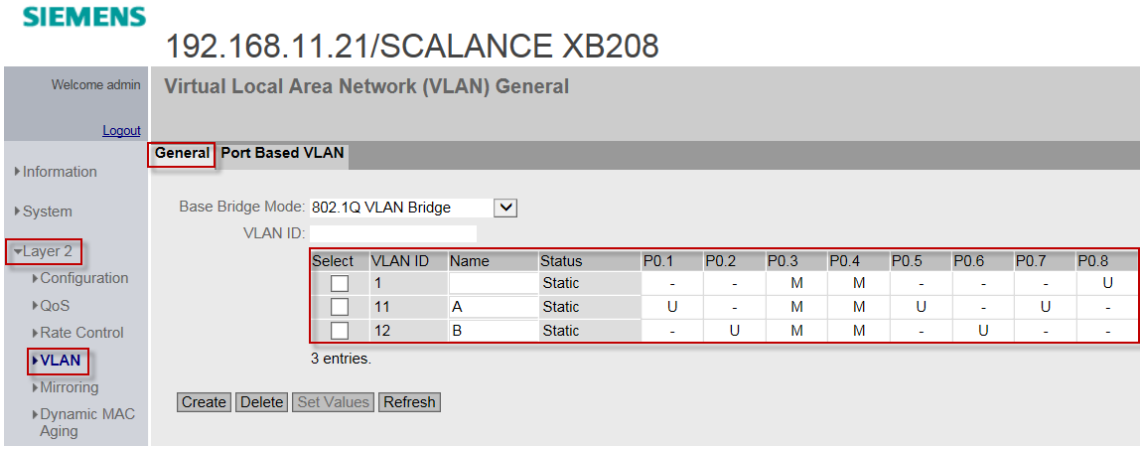


Figura 4.20: Asignación de VLANs a puertos en XB208

Se asigna, como se ha hecho en el anterior dispositivo, a cada puerto su VLAN correspondiente en el modo correcto de funcionamiento, como se ve en la **Figura 4.20**.

También se configura su puerta de enlace y VLAN de gestión (ver **Figura 4.21**).

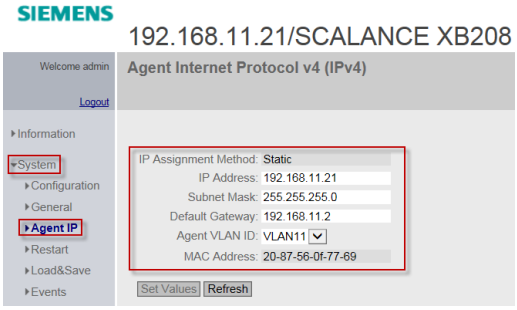


Figura 4.21: Asignación de VLAN de gestión en XB208

Para los dispositivos **X204RNA y X204RNA EEC** [18] se adjuntan, únicamente, dos capturas de la configuración final debido a que los tres dispositivos se configuran exactamente de la misma manera a excepción de la dirección IP. Se configura el modo por defecto de trabajo de estos *switches* (ver **Figura 4.22**), que será PRP, y dirección de puerta de enlace e IP (ver **Figura 4.23**).

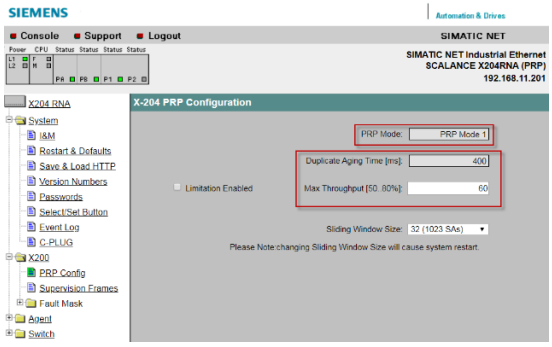


Figura 4.22: Configuración por defecto modo de trabajo PRP para switches RNA

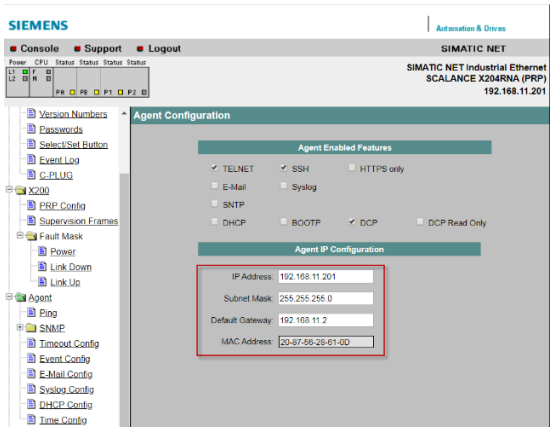


Figura 4.23: Configuración de dirección IP, máscara de subred y puerta de enlace

4.5 PARAMETRIZACIÓN DE *ROUTERS* (XM408-8C) (VRRP)

Se va a proceder ahora a la configuración de los dos XM408-8C que van a permitir crear VLANs con distintas subredes y, además, va a tener la capacidad de enrutar los paquetes que le llegan. Debido a que ambos *routers* se configuran de la misma forma, dado que ambos realizan la misma función, a excepción de su dirección

IP y configuración del protocolo VRRP en cada uno, se mostraran las configuraciones en el XM408-8C que actúa como maestro y las diferencias que existen en la *backup*.

Para la configuración de ambos **XM408-8C** [21] se realiza lo siguiente:

1. Configuración de *routing* (ver **Figura 4.24**).

Figura 4.24: Habilitar Routing en XM408-8C

2. Creación de VLANs y asignación de puertos (ver **Figura 4.25**).

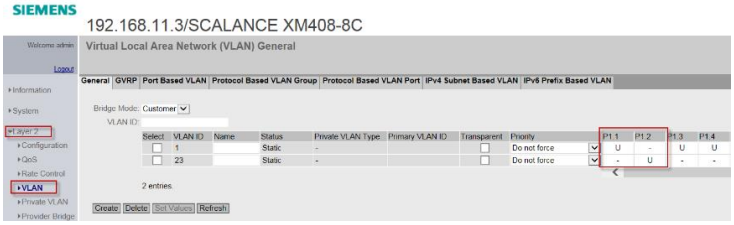


Figura 4.25: Asignación de VLANs a puertos en XM408-8C

3. Asignación de subredes a cada VLAN creada (ver **Figura 4.26**).

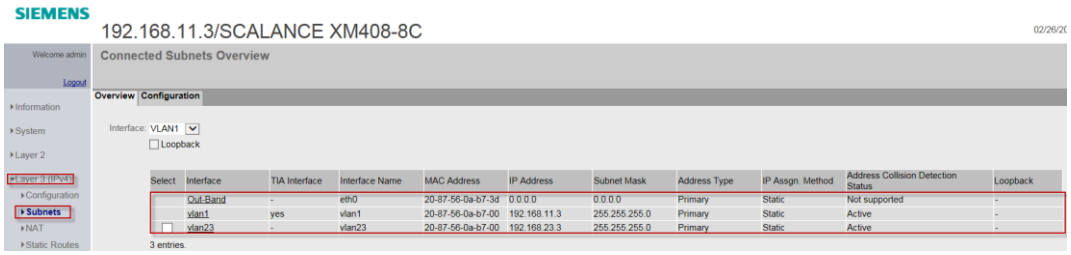


Figura 4.26: Asignación de subredes a cada VLAN

4. Creación de rutas estáticas hacia los *firewalls* (ver **Figura 4.27**).

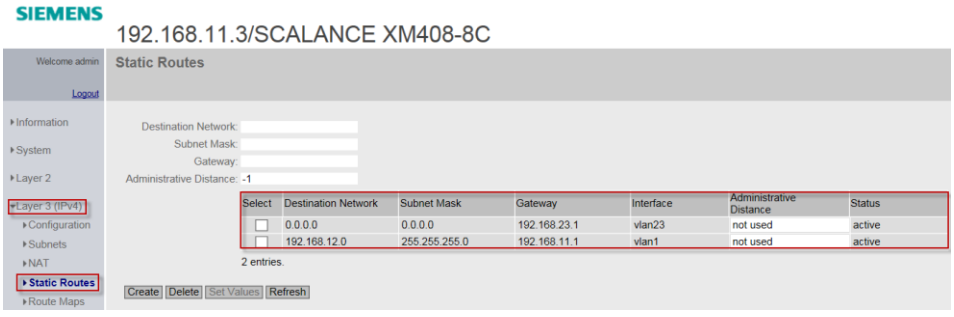


Figura 4.27: Creación de rutas estáticas en XM408-8C

En la **Figura 4.27** se observan dos rutas estáticas creadas. El objetivo de éstas es redireccionar todos los paquetes con la subred de destino que sea, al S615 del lado de los APs, excepto aquellos con destino a la subred 192.168.12.0, que los enviará al otro S615 en el lado de los clientes.

5. Configuración del protocolo VRRP (ver **Figura 4.28**).

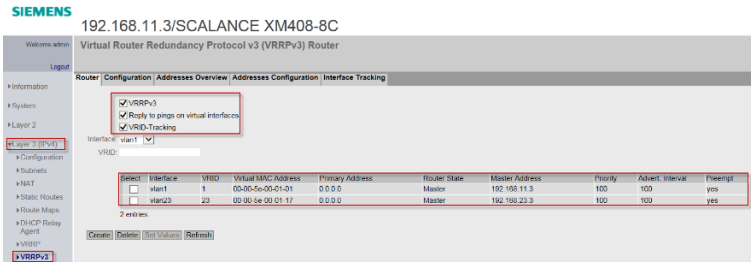


Figura 4.28: Overview del protocolo VRRP configurado en XM408-8C maestro

En las siguientes figuras se puede observar cómo configurar la redundancia del *router*, los dos SCALANCE XM408-8C se combinan en un grupo lógico (VRID). El XM408-8C con IP 192.168.11.3 es el *router* maestro y el XM408-8C con IP 192.168.11.4 es el *router backup*. En la realidad, ambos conforman un único *router* virtual. La estación 1 (vlan1) está conectada a través de la interfaz P1. Durante el funcionamiento normal, todo el tráfico de datos se maneja a través de la interfaz del *router* maestro. Cuando el estado de una interfaz monitorizada cambia en el *router* maestro de "*up*" a "*down*", la prioridad del *router* maestro se reduce. La dirección IP virtual y la dirección MAC se transfieren al *router backup* que asume las tareas del *router* maestro. Una vez que la conexión a través del XM408-8C con IP 192.168.11.3 es posible de nuevo, la prioridad original del *router* VRRP se restaura, es decir, volvería a asumir una vez más el papel de *router* maestro.

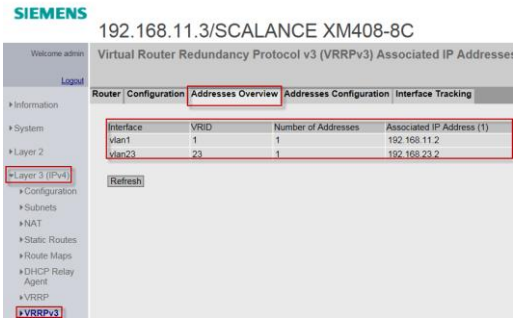


Figura 4.29: Overview de las IPs virtuales asociadas a cada VLAN en XM408-8C maestro

Se asigna una dirección IP virtual para que los dispositivos conectados no sean conscientes del cambio. Esta dirección IP virtual se introduce como dirección de acceso en los dispositivos (ver **Figura 4.29**).

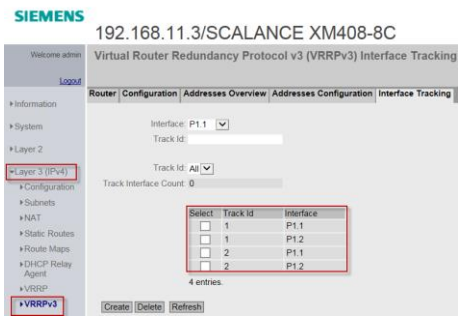


Figura 4.30: Asignación de puertos a su Track ID en XM408-8C maestro

Las interfaces son traqueadas. El "*Track Interfaz Count*" 1 significa que cuando el estado de conexión en una interfaz cambia de "*up*" a "*down*", la prioridad del *router* VRRP asignado se reduce (ver **Figura 4.30**). El valor por el cual la prioridad se reduce se puede observar en la **Figura 4.31** siendo este el "*Decrement Priority*" eligiendo 10 como valor suficiente debido a que la prioridad del otro *router* es 99, entonces 100-10 = 90 que es menor que 99. Cuando el estado de la conexión cambia de "*down*" a "*up*", la prioridad original es restaurada.

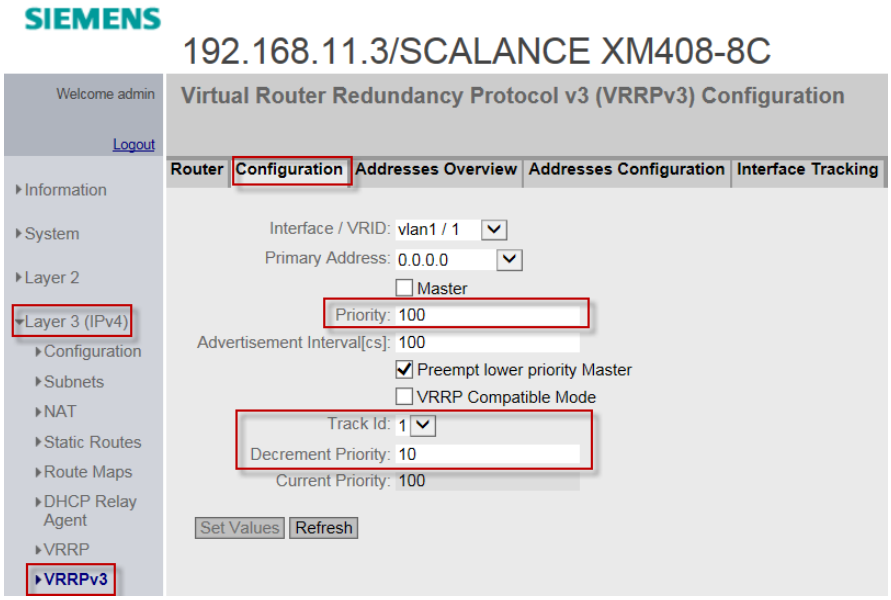


Figura 4.31: Asignación de prioridad y decremento de éste configurado en XM408-8C maestro en protocolo VRRP

Debido a la similitud de las configuraciones realizadas en el XM408-8C en modo *backup*, no se adjuntan capturas de la parametrización realizada. Se comenta que sería igual que la configuración del *router* maestro, a excepción de dar a éste una prioridad menor en el protocolo VRRP y en cuanto a las direcciones IPs.

Como se ha destacado al comienzo de este apartado, en este proyecto se han añadido diferentes dispositivos y se han realizado determinadas parametrizaciones y configuraciones para la validación de la arquitectura y para el acceso remoto a la red. Por motivos de dimensión del escrito y debido a su afectación en la red, se ha optado por añadir el apartado de configuración de los *firewalls* (ver **Apéndice 3**) y toda la configuración y programación de la comunicación S7 entre los dos PLCs (ver **Apéndice 5**) al apartado de apéndices.

4.6 CONCLUSIONES

En este apartado se ha fijado la infraestructura de red final que, una vez definidos los parámetros y los distintos protocolos de cada uno de los dispositivos, y transferidos a cada uno de ellos, ya se está en disposición de verificar su funcionalidad, disponibilidad y fiabilidad en el siguiente apartado.

5

VALIDACIÓN DE LA ARQUITECTURA

5.1 INTRODUCCIÓN

En este capítulo se va a proceder a la validación de la red en términos de disponibilidad y fiabilidad, es decir, se comprobará si la latencia máxima en la red es lo suficientemente baja para cumplir con los requisitos del apartado 3.

Debido a las dimensiones del escrito, se adjuntan las imágenes que cercioran la validez del diseño realizado, no los pasos seguidos hasta llegar a esa validación.

5.2 VALIDACIÓN DE LA RED COMPROBANDO EL ESTADO DE LA COMUNICACIÓN S7 ENTRE PLCs

Mediante la comunicación S7 establecida entre PLCs (ver **Apéndice 5**). El "Control de mandos" pone a disposición de la comunicación su marca de ciclo, y el "Control de tren" obtiene esta marca de ciclo a una frecuencia definida de 5 Hz, es decir, cada 200 ms obtiene la marca de ciclo que tenga el "Control de mandos" en ese momento y la añade a su bloque de datos.

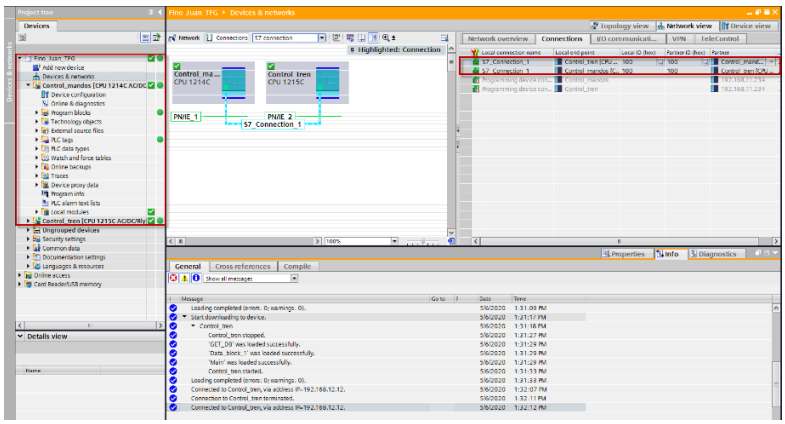


Figura 5.1: Conexión establecida en comunicación S7 en TIA PORTAL

En la **Figura 5.1** se muestra, en el recuadro rojo de arriba a la derecha, la correcta comunicación entre ambos PLCs.

Las tres figuras siguientes muestran lo siguiente:

- Comunicación entre PLCs con *router* maestro (192.168.11.3) apagado (ver **Figura 5.2**).

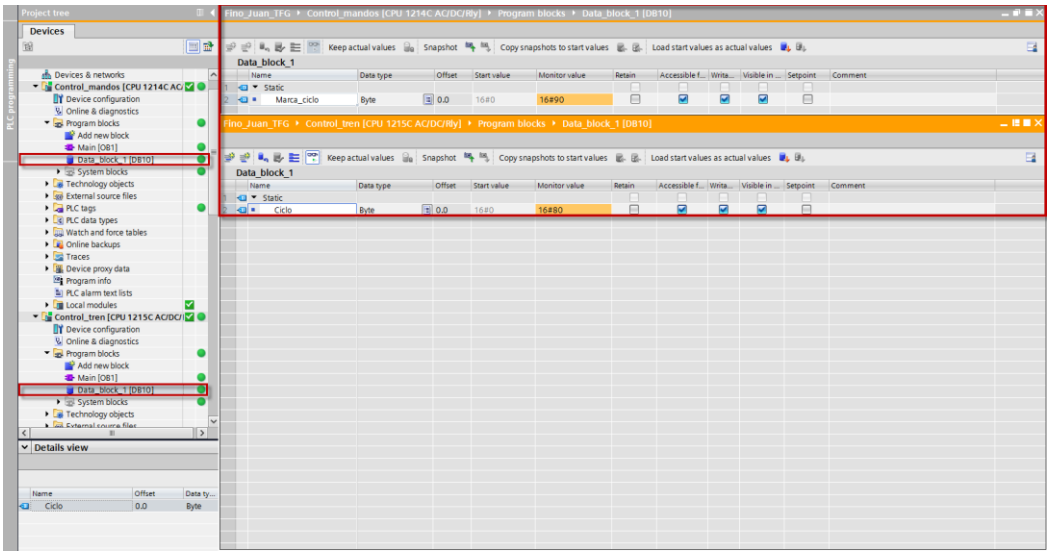


Figura 5.2: Comprobación conexión establecida en comunicación S7 con XM408-8C tirado

Se puede observar en la **Figura 5.2** como ambos PLCs están comunicando, se puede observar en el valor monitorizado.

- Comunicación entre PLCs con punto de acceso 1 (192.168.11.70) y *router* maestro (192.168.11.3) apagados (ver **Figura 5.3**).

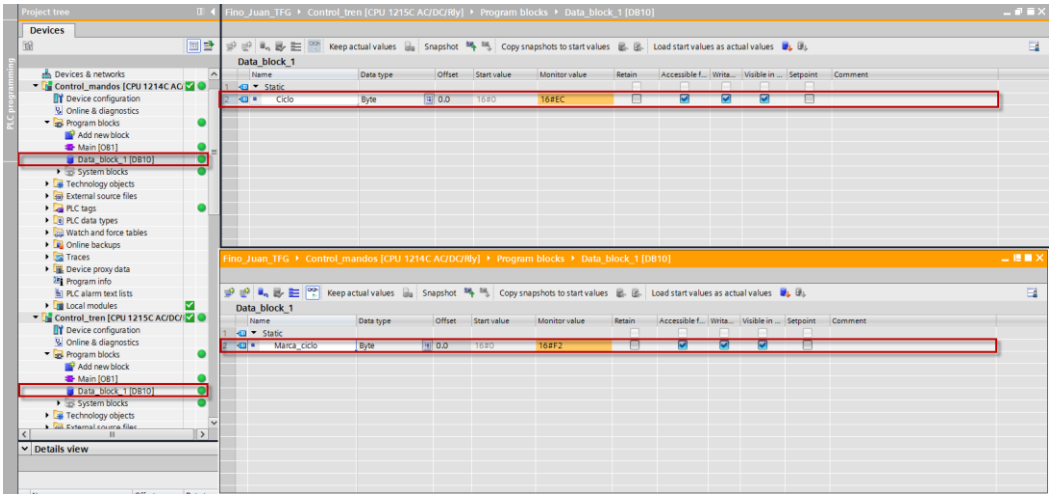


Figura 5.3: Comprobación conexión establecida en comunicación S7 con XM408-8C tirado y AP 1 también

Se puede observar en la **Figura 5.3** como ambos PLCs están comunicando aun apagando el punto de acceso 1 y el *router* maestro a la vez, se puede observar en el valor monitorizado.

- Comunicación entre PLCs con ambos puntos de accesos (192.168.11.70 y 192.168.11.71) apagados (ver **Figura 5.4**).

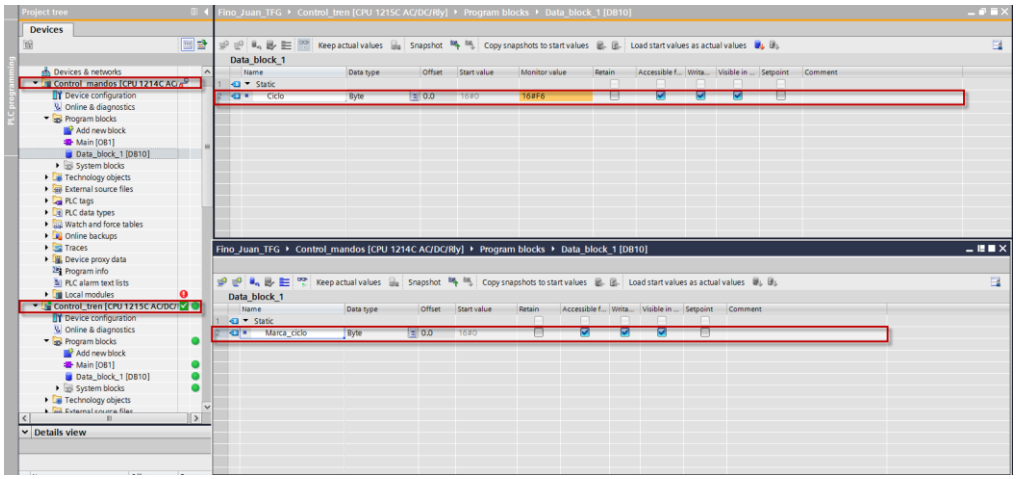


Figura 5.4: Comprobación conexión caída en comunicación S7 con ambos APs tirados

Se puede observar en la **Figura 5.4** que, obviamente, al tirar ambos puntos de accesos, se pierde la comunicación con el otro PLC. Ya no se puede monitorizar el valor y avisa también el propio programa que no ha sido capaz de cerrar la comunicación.

5.3 VALIDACIÓN DE LA RED MEDIANTE EL SOFTWARE RUGGEDCOM PING

Para la segunda prueba se sustituye el PLC “Control del tren” por una SIMATIC PG (ordenador/programadora) donde se utiliza el software RuggedCom Ping instalado en ésta. RuggedCom Ping es un software que hace uso del comando ping con una precisión muy alta muy útil para monitorizar una lista de dispositivos con el fin de medir en detalle el rendimiento y el comportamiento de las soluciones implementadas en aquellas redes tolerantes a fallos.

RuggedCom Ping está diseñado para medir el tiempo que tarda la red desde el momento en que el dispositivo activo se cae, hasta el momento en que se recupera la conectividad a través del dispositivo que estaba en modo inactivo o en modo de espera.

RuggedCom Ping solo requiere que los dispositivos a testear soporten el omnipresente Protocolo de Mensajes de Control de Internet (ICMP), mejor conocido como "Ping", que es implementado por la gran mayoría de los dispositivos IP. RuggedCom Ping permite enviar mensajes de eco ICMP y obtener tiempos de respuesta con precisiones de 1ms.

A continuación, se puede analizar en el informe elaborado por el propio software donde, indicando que la IP de destino contra la que se quiere hacer ping es la 192.168.23.120 (IP del PLC “Control de mandos”), se muestra el tiempo medio de respuesta, total de paquetes enviados y recibidos, etc.

RUGGEDCOM
INDUSTRIAL STRENGTH NETWORKS

RuggedPing Test Report

Prueba_iPRP

Tested By: Juan

Date: 8/5/2020
Time: 11:08:48

Test Summary:

Duration	Number of Devices	Number of Events
0:02:58	1	0

Total Packets:

Sent	Received	Lost
8916	8916	0

System Recovery time (ms):

Minimum	Maximun	Average
0	0	0

Device Summary:
Response Summary:

Device IP	Ping Packets			Response Time (ms)		
	Sent	Received	Lost	Minimum	Maximum	Average
192.168.23.120	8916	8916	0	2	92	9

Incident Summary:

Device IP	Ping Packets			Recovery Time (ms)		
	Sent	Received	Lost	Minimum	Maximum	Average
192.168.23.120	8916	8916	0	0	0	0

Figura 5.5: Comprobación comunicación entre PG ubicada en S615 al lado cliente contra "Control de mandos" a través del software RuggedCom Ping

Entrando más en detalle en la **Figura 5.5**, se observa cierta información necesaria de comentar. Se configura para que el programa mande “Pings” aproximadamente cada 20 ms. Esto se comprueba al observar el número de paquetes enviados en el tiempo de ejecución del programa. Se observa también que el número de paquetes perdidos es 0 (requisito indispensable en la red) y que el tiempo medio de respuesta en la red es de 9 ms, tiempo suficientemente bajo para el tipo de aplicación que se está buscando. Además, tampoco se superan los 100 ms en el tiempo máximo de respuesta. Añadir también que hay que tener presente que esta validación se ha realizado utilizando el estándar 802.11n.

5.4 CONCLUSIONES

Para concluir con este apartado, se puede confirmar que la red diseñada en el apartado 4 tiene la capacidad, en términos de ancho de banda y latencia, de soportar todos los servicios embarcados en el tren.

Esto se ha podido comprobar mediante dos pruebas, una mediante una comunicación S7 y observando el valor monitorizado por cada PLC, y la otra a través de un programa llamado RuggedCom Ping el cual permite obtener tiempos de respuesta mediante Ping.

6

CONCLUSIONES SOBRE EL DISEÑO ELABORADO

6.1 CONCLUSIONES

Debido a factores tan limitadores como la cobertura, el trazado de las vías, la propia estructura que tiene el tren y la movilidad, resulta muy complicado la implementación de una nueva estructura de red en un entorno ferroviario.

La única forma de hacer frente a estos problemas es diseñar una red de banda ancha que tenga la capacidad suficiente para transmitir información a una velocidad mínima, con una cobertura durante toda la línea y que tenga los recursos necesarios demandados por todos los servicios embarcados en el tren.

Se ha visto que la tecnología Wi-Fi, más en concreto el estándar 802.11ac, tiene la capacidad suficiente para afrontar la demanda de banda ancha requerida por los servicios. También solventa el problema de cobertura necesaria durante toda la vía, pero se encontraban limitaciones en cuanto a tiempos de *roaming* entre los puntos de acceso distribuidos por la vía y los clientes. Para reducir todo lo que se pueda la posibilidad de tener pérdidas en la comunicación provocadas por caídas de dispositivos se opta por la utilización de protocolos de redundancia. Estos dos últimos problemas mencionados son clave el poder solucionarlos, debido a que el parámetro más importante en una comunicación ferroviaria es la disponibilidad en la red y su fiabilidad en la información.

Como conclusión del proyecto y como se comprueba en el capítulo de validación, se puede afirmar que, las soluciones planteadas y la infraestructura de red diseñada, podrían ser válidas y viables en un entorno ferroviario, tecnológicamente hablando.

Asignaturas como Arquitectura de Redes 1 y Arquitectura de Redes 2 han resultado de gran utilidad para el alumno, debido al uso continuado de conceptos claves de la capa de enlace y la capa de red que se hacen durante el transcurso del proyecto. También, han sido de utilidad para el uso herramientas como Wireshark para detectar errores en la comunicación o en la topología de red.

En la **Figura 6.1,** se puede ver la disposición de los diferentes dispositivos de la red diseñada, en una situación real.

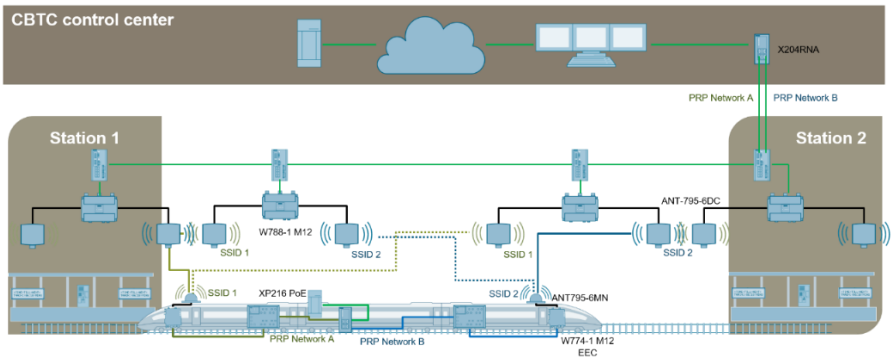


Figura 6.1: Diseño de lo que sería la arquitectura de red en un entorno ferroviario real

Además, al alumno le gustaría aprovechar este apartado para mostrar el resultado final físico del diseño realizado en el laboratorio, separando ambos despliegues (ver **Figura 6.2**).

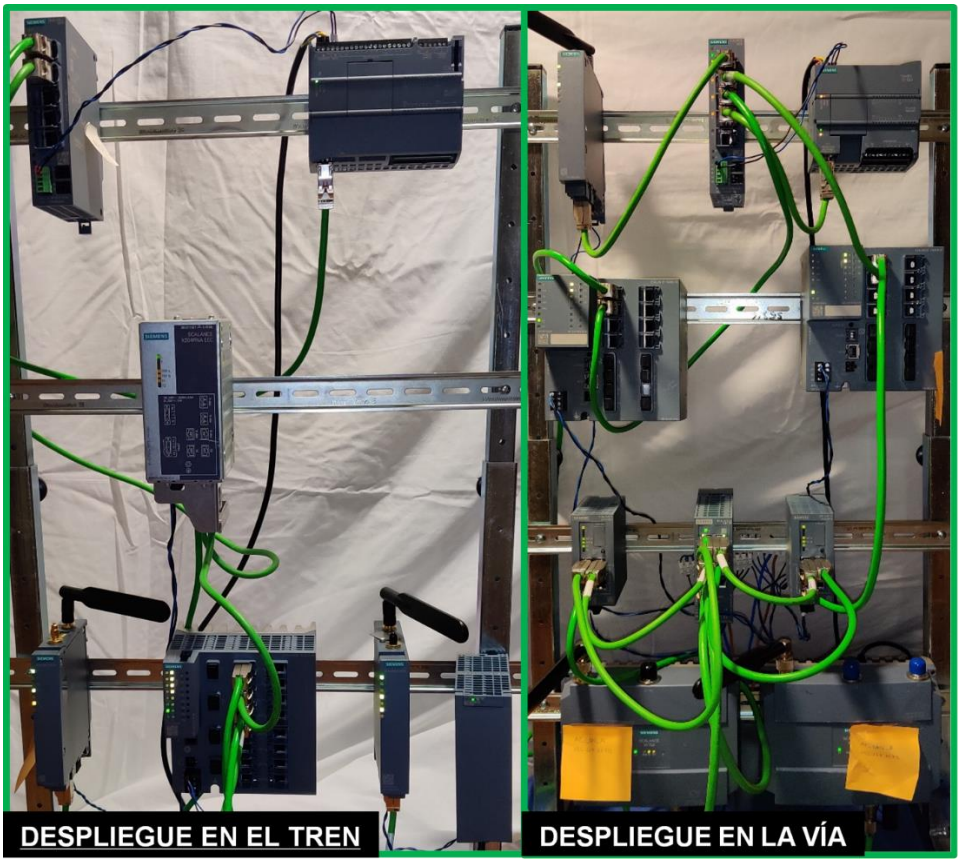


Figura 6.2: Diseño hardware real elaborado en el laboratorio

6.2 TRABAJO FUTURO

Como se menciona en el resumen, al comienzo de este proyecto, diferentes tecnologías están cogiendo fuerza estos últimos años, como son el 5G y el Wi-Fi 6 (IEEE 802.11ax). Un posible trabajo futuro sería la implementación de una infraestructura de red que haga uso de alguna de estas dos tecnologías en un entorno ferroviario.

B

BIBLIOGRAFÍA

1. Al Maimouni, Hassan (2015). *Estudio sobre la integración de sistemas de telecomunicaciones, control y protección al tren en sistemas ferroviarios de transporte urbano*. Proyecto/Trabajo final de carrera. Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona (UPC).

2. B. Ai et al., "Future railway services-oriented mobile communications network," in IEEE Communications Magazine, vol. 53, no. 10, pp. 78-85, October 2015, doi: 10.1109/MCOM.2015.7295467.

3. Braden, R., "Requirements for Internet Hosts -- Communication Layers", RFC 1122, Octubre de 1989.

4. H. Yang and L. Cheng, "Bounding Network-Induced Delays of Wireless PRP Infrastructure for Industrial Control Systems," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-7, doi: 10.1109/ICC.2019.8761893.

5. Hinden, R., "Virtual Router Redundancy Protocol (VRRP)", RFC 3768, Abril de 2004.

6. How do you configure and program an S7 connection and the "PUT" and "GET" instructions for data transfer between an S7-1500 CPU and an S7-1200 CPU?. (2020). Retrieved 13 May 2020, from https://cache.industry.siemens.com/dl/files/115/82212115/att_108330/v2/82212115_s7_communication_s7-1500_en.pdf

7. Incibe. "PRP y HSR: Protocolos redundantes". (2017, Agosto 03). Retrieved 2 May 2020, from https://www.incibe-cert.es/blog/prp-y-hsr-protocolos-redundantes

8. J. A. Araujo, J. Lázaro, A. Astarloa, A. Zuloaga and A. García, "PRP and HSR version 1 (IEC 62439-3 Ed.2), improvements and a prototype implementation," IECON 2013 - 39th Annual Conference of the IEEE Industrial Electronics Society, Vienna, 2013, pp. 4410-4415, doi: 10.1109/IECON.2013.6699845.

9. M. Aguado, E. Jacob, P. Saiz, J. J. Unzilla, M. V. Higuero and J. Matias, "Railway signaling systems and new trends in wireless data communication," VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference, 2005., Dallas, TX, USA, 2005, pp. 1333-1336, doi: 10.1109/VETECF.2005.1558143.

10. M. Rentschler and H. Heine, "The Parallel Redundancy Protocol for industrial IP networks," 2013 IEEE International Conference on Industrial Technology (ICIT), Cape Town, 2013, pp. 1404-1409, doi: 10.1109/ICIT.2013.6505877.

11. NETWORK LAYER/INTERNET PROTOCOLS. (n.d.). Retrieved 20 May 2020, from https://www.pearsonhighered.com/assets/samplechapter/0/6/7/2/0672322080.pdf

12. Patricia Nazar, Pablo Jara Werchau. “Estándar IEEE 802.11 X de las WLAN” Departamento de Ingeniería en Sistemas de Información. Universidad Tecnológica Nacional - edutecne.utn.edu.ar. (n.d.). Retrieved 14 May 2020, from http://www.edutecne.utn.edu.ar/monografias/standard_802_11.pdf

13. Postel, J., “Internet Control Message Protocol”, RFC 792, Septiembre de 1981.

14. Sánchez Millán, Marina (2017). *Dimensionamiento y planificación de un sistema de radiocomunicaciones tren-tierra de banda ancha*. Proyecto Fin de Carrera / Trabajo Fin de Grado, E.T.S.I. y Sistemas de Telecomunicación (UPM), Madrid

15. Setting up a secure VPN Connection between SINEMA Remote Connect Client, SCALANCE S615 and SINEMA Remote Connect Server. (2020). Retrieved 28 May 2020, from https://cache.industry.siemens.com/dl/files/599/109479599/att_858210/v2/109479599_S615_RCClient_RC_StatischeIP_DOKU_V10_en.pdf

16. Sharon, Oran & Alpert, Yaron. (2014). MAC level Throughput comparison: 802.11ac vs. 802.11n. Physical Communication. 12. 10.1016/j.phycom.2014.01.007.

17. SIMATIC NET: Industrial Ethernet Security SCALANCE S615 Web Based Management. (2020). Retrieved 21 May 2020, from https://cache.industry.siemens.com/dl/files/632/109751632/att_1006477/v1/PH_SCALANCE-S615-WBM_76.pdf

18. SIMATIC NET: Industrial Ethernet switches SCALANCE X-200RNA. (2020). Retrieved 17 May 2020, from https://cache.industry.siemens.com/dl/files/817/91255817/att_986434/v1/BA_SCALANCE-X-200RNA_76.pdf

19. SIMATIC NET: Industrial Ethernet switches SCALANCE XB-200/XC-200/ XF-200BA/XP-200/XR-300WG Web Based Management. (2020). Retrieved 17 May 2020, from https://cache.industry.siemens.com/dl/files/837/109762837/att_969706/v1/PH_SCALANCE-XB-200-XC-200-XF-200BA-XP-200-XR-300WG-WBM_76.pdf

20. SIMATIC NET: Industrial Ethernet switches SCALANCE XC-200. (2020). Retrieved 17 May 2020, from https://cache.industry.siemens.com/dl/files/149/109743149/att_1013398/v1/BA_SCALANCE-XC-200_76.pdf

21. SIMATIC NET: Industrial Ethernet switches SCALANCE XM-400/XR-500 Web Based Management (WBM). (2020). Retrieved 17 May 2020, from https://cache.industry.siemens.com/dl/files/840/109760840/att_962665/v1/PH_SCALANCE-XM-400-XR-500-WBM_76.pdf

22. SIMATIC NET: Industrial Wireless LAN SCALANCE W770/W730 to IEEE 802.11n Web Based Management. (2020). Retrieved 17 May 2020, from https://cache.industry.siemens.com/dl/files/613/109759613/att_1005891/v1/PH_SCALANCE-W770-W730-WBM_76.pdf

23. SIMATIC NET: Industrial Wireless LAN SCALANCE W780/W740 to IEEE 802.11n Web Based Management. (2020). Retrieved 17 May 2020, from https://cache.industry.siemens.com/dl/files/652/109759652/att_1005859/v1/PH_SCALANCE-W780-W740-WBM_76.pdf

24. Yunquera Torres, Juan José. CAPÍTULO 3 EL ESTÁNDAR IEEE 802. (n.d.). Retrieved 2 May 2020, from http://bibing.us.es/proyectos/abreproy/11138/fichero/memoria%252FCap%C3%ADtulo+3.pdf+

A

APÉNDICES

A.1 ESTÁNDARES EN LA CAPA DE ENLACE - Wi-Fi Y EL ESTANDAR 802.11

A.1.1 Estándares en la Capa de Enlace

Para este capítulo ha servido de gran utilidad la utilización del recurso [3]. Los protocolos de la capa de enlace comúnmente no están determinados por *Request for Comments* (RFCs). Aunque el *Internet Engineering Task Force* (IETF) conserva la funcionalidad de los protocolos y servicios del protocolo TCP/IP en las capas por encima de ésta, el IETF no precisa el funcionamiento de la capa de acceso a la red de éste. Precisamente, las especificaciones y los servicios de la capa de enlace están definidos por múltiples estándares establecidos en una diversidad de medios y tecnologías en los que se usan los protocolos. Unos cuantos de estos estándares contienen servicios de la capa física y de la capa de enlace. Los servicios y protocolos utilizables en la capa de enlace son definidos por:

- Organizaciones de ingeniería que instauran normas y protocolos abiertos y públicos.
- Empresas del sector de las comunicaciones las cuales crean y usan protocolos para aprovechar los nuevos progresos tecnológicos o tener ventaja en nuevas oportunidades de mercado.

Las organizaciones de ingenieros que crean y concretan protocolos y normas abiertas que se emplean en la capa de enlace son:

- Instituto Nacional Americano de Estándares (ANSI)
- Organización Internacional de Estandarización (ISO)
- Unión Internacional de Telecomunicaciones (UIT)
- Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)

La **Tabla A.1** muestra varias organizaciones de estándares y unos de sus protocolos de la capa de enlace más significativos.

Tabla A.1: Organizaciones de estándares y sus protocolos. Recuperado de http://www.ingenieriasystems.com/2016/11/Estandares-de-la-capa-de-enlace-de-datos-y-control-de-acceso-a-los-medios-CCNA1-V5-CISCO-C4.html

Organización de Estándares	Estándares de Red
IEEE	802.2: Logical Link Control (LLC) 802.3: Ethernet 802.4: Token bus 802.5: Token ring 802.11: Wireless LAN (WLAN) & Mesh (Wi-Fi certification) 802.15: Bluetooth 802.16: WiMax
ITU-T	G.992: ADSL G.8100 - G.8199: MPLS over Transport aspects Q.921: ISDN Q.922: Frame Relay
ISO	HDLC (High Level Data Link Control) ISO 9314: FDDI Media Access Control (MAC)
ANSI	X3T9.5 and X3T12: Fiber Distributed Data Inter

A.1.2 Wi-Fi y norma IEEE 802.11

Para el desarrollo de este apartado se han utilizado los recursos [3] [12] [16] [24]. Wi-Fi es un protocolo de red inalámbrica que permite a los dispositivos comunicarse sin conexiones directas por cable. Es, técnicamente, un término industrial que representa un tipo de protocolo de red local inalámbrica basado en el estándar de red IEEE 802.11. La norma IEEE 802.11 (Wi-Fi) es hoy en día la solución más importante dentro de la gama de redes inalámbricas de área local (LAN).

En la **Figura A.1** se puede observar donde se ubica estos protocolos en función de la tasa binaria y hasta que distancia pueden abarcar:

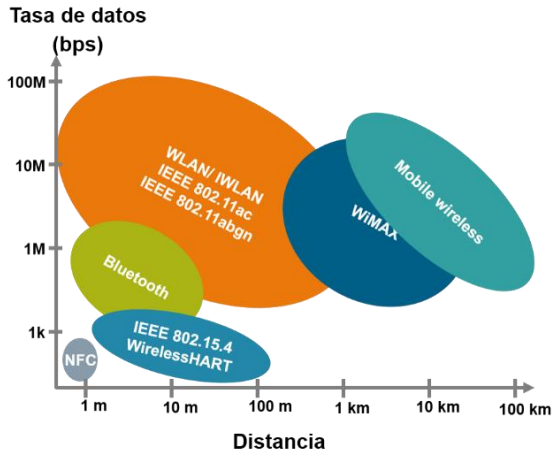


Figura A.1: Relación tasa binaria/distancia entre diferentes enlaces

Desde su primera introducción a mediados de los años 90, el estándar se ha mejorado de muchas maneras. Uno de los principales objetivos de estas mejoras es aumentar el rendimiento de la capa MAC. Para ello, se han ido creando diferentes versiones de este estándar donde en la **Tabla A.2** se recogen algunas de sus características principales:

Tabla A.2: Especificaciones de distintos estándares 802.11

	IEEE 802.11b	IEEE 802.11g	IEEE 802.11a	IEEE 802.11h	IEEE 802.11n	IEEE 802.11ac
Frecuencia	2.4 GHz	2.4 GHz	5 GHz	5 GHz	2.4 GHz/ 5 GHz	5 GHz
Cobertura (dependiendo de la antena y del entorno)	Interior: 30 m Exterior: 140 m	Interior: 30 m Exterior: 140 m	Interior: 30 m Exterior: 120 m	Interior: 30 m Exterior: 120 m	Interior: 70 m Exterior: 250 m	
Potencia transmitida	Interior y exterior: 20 dBm	Interior y exterior: 20 dBm	Interior: 23 dBm	Interior y exterior: 23 dBm/ 30 dBm	Interior y exterior: 23 dBm/ 30 dBm	Interior y exterior: 23 dBm/ 30 dBm
Canales no superpuestos	3	3	4	8 + 11	2,4 GHz: 3 5 GHz: 8 + 11	8 + 11
Tasa de datos bruta	11 MBit/s	54 MBit/s	54 MBit/s	54 MBit/s	600 MBit/s	1.3 GBit/s
Especialidades	Fiable debido a DSSS			DFS requerido, hasta canal 64 sólo interior	DFS requerido a 5 GHz	DFS requerido

De los estándares definidos en la **Tabla A.2** este proyecto se centrará en dos, uno debido al uso que se hace de él en las configuraciones de los dispositivos Wi-Fi y otro, debido a que sería el estándar ideal para una situación de comunicación tren-tierra por las características que se comentan ahora.

Primero se habla del estándar usado durante las pruebas en el laboratorio, el estándar 802.11n. Realmente se le denomina IEEE 802.11n-2009, aunque comúnmente se abrevia este nombre a 802.11n. Es un estándar de red *wireless* que usa varias antenas para acrecentar las tasas de envío de paquetes. La Alianza Wi-Fi (organización comercial cuya marca es Wi-Fi) también etiquetó retroactivamente la tecnología para el estándar como Wi-Fi 4. Estandarizó el soporte para múltiples entradas de salida múltiple, implementó agregación de marcos y realizó avances en cuanto a la seguridad, entre otras particularidades, y existe la posibilidad de utilizarse en las bandas de frecuencia de 2,4 GHz o 5 GHz.

Fue el primer estándar Wi-Fi que introdujo el soporte MIMO (Entrada Múltiple y Salida Múltiple), a veces los dispositivos/sistemas que soportan estándar 802.11n (o versión de prueba del estándar) se denominan MIMO (productos Wi-Fi), especialmente antes de la introducción del estándar de nueva generación. El uso de MIMO-OFDM para aumentar la tasa de datos manteniendo el mismo espectro que 802.11a fue demostrado por primera vez por *Airgo Networks*.

El objetivo de este estándar es aumentar la productividad de la red en relación a ambos estándares que existían anteriormente que eran el 802.11a y 802.11g, con una gran mejora de la máxima tasa de datos netos de 54 Mbit/s a 72 Mbit/s con un flujo espacial único en un canal de 20 MHz, y 600 Mbit/s (tasa de bits bruta ligeramente superior, incluidos, por ejemplo, códigos de corrección de errores, y rendimiento máximo

ligeramente inferior) utilizando cuatro flujos espaciales con un ancho de canal de 40 MHz.

Las tasas binarias de datos máximas (de 600 Mbit/s) sólo se alcanzan usando el máximo de cuatro flujos espaciales utilizando un canal de 40 MHz de ancho. Varios esquemas de modulación y tasas de codificación están definidos por el estándar y están representados por un valor en el Esquema de Modulación y Codificación (MCS).

El canal de 20 MHz utiliza una FFT de 64, de los cuales: 56 subportadora OFDM, 52 son para datos y 4 son tonos piloto (Señal, normalmente a una única frecuencia, transmitida a través de un sistema de comunicaciones con fines de supervisión, control, ecualización, continuidad, sincronización o referencia) con un espacio de portadora de 0,3125 MHz (20 MHz/64) (3,2 µs). Cualquiera de estas subportadoras podría ser un QPSK, BPSK, 64-QAM o 16-QAM. La anchura de banda ocupada es de 17,8 MHz de los 20 MHz del ancho de banda total. El tiempo total del símbolo es de 3,6 o 4 microsegundos, que incluye un intervalo de guardia de 0,4 o 0.8 microsegundos.

Ahora se hablará más en detalle del estándar 802.11ac que apareció para cumplir la promesa de aumentar el rendimiento de la norma 802.11 y, eficazmente, poder tener más dispositivos clientes en una red, el grupo de trabajo IEEE 802.11 introdujo la quinta generación de estándares de red 802.11, denominada 802.11ac, también conocida como *Very High Throughput* (VHT). 802.11ac está diseñado para transmisión rápida de datos de alta calidad y casi instantánea sincronización de datos y copia de seguridad a los portátiles, tabletas y teléfonos móviles.

La especificación IEEE 802.11ac añade anchuras de banda de 80 MHz y 160 MHz con canales contiguos y no contiguos de 160 MHz para una asignación flexible de canales. Añade una modulación de orden superior en forma de modulación de amplitud de 256 cuadraturas (QAM), proporcionando una mejora adicional del 33% en la tasa de datos. Se consigue una duplicación adicional de la tasa de datos aumentando el número máximo de flujos espaciales a ocho.

El estándar IEEE 802.11ac introduce una nueva tecnología revolucionaria para soportar múltiples transmisiones simultáneas de enlace descendente, conocida como “multiusuario de entrada múltiple, salida múltiple” (MU MIMO). Con MU MIMO se consigue un mayor ancho de banda del sistema, facilita utilizar de manera más eficaz el espectro, y permite tener un retardo reducido al aguantar hasta cuatro envíos al mismo tiempo del usuario. Esto lo hace a través de la utilización de la tecnología de antenas inteligentes. Resulta de gran utilidad para aquellos dispositivos con un límite en cuanto al número de antenas, como *tablets* y smartphones.

Este estándar específico sería ideal para la comunicación que se desea debido a que es el único estándar que actualmente trabaja a 5 GHz, junto con la versión 802.11n ya comentada anteriormente. Esto es un factor muy a tener en cuenta debido a que, actualmente, el número de dispositivos que trabajan a esta frecuencia es bajo, lo que lleva a tener un nivel de fiabilidad y disponibilidad mayor en la red. En cambio, trabajar a 2,4 GHz, la cual es una banda saturada, podría provocar una no disponibilidad del servicio de control de datos del tren (CBTC) lo que sería crítico para el correcto funcionamiento del tren.

A.2 PROTOCOLOS CAPA DE RED: ICMP, PING Y TRACERT, VRRP, PRP E iPRP

A.2.1 Protocolo ICMP

Para el desarrollo de este capítulo se ha hecho uso de los recursos [11] [13]. El protocolo IP proporciona un medio poco fiable y de máximo esfuerzo para transportar tramas de datos. Una trama de datos pasa varios *routers* en su camino al host de destino, en los cuales el *router* es capaz de entregar el paquete directamente, o lo pasa a otro *router*. Esto continúa hasta que el paquete finalmente alcanza su destino, o un error en la transmisión que hace que el paquete se pierda. Si se produce tal error, es necesario informar al host de origen de que esa trama de datos ha sido perdida, y por qué. Ese es el propósito del *Internet Control Message Protocol* (ICMP).

Siempre que un *router* detecta algún tipo de error sea de la índole que sea, envía un mensaje ICMP de vuelta al remitente del paquete. Este mensaje ICMP es un paquete totalmente independiente que se transporta a través de la red al igual que cualquier otro paquete, no hay prioridad especial o garantía extra de que el mensaje finalmente llegará, ya que puede cumplir con una condición de error el mismo.

Puesto que las cabeceras IP sólo nombran las direcciones de los dos puntos finales que se comunican, a saber, el origen y el destino, los *routers* no tienen más opción que informar al remitente del error ocurrido, incluso si no pueden proporcionar una solución. Sin embargo, es preferible informar al remitente de los problemas que ocurren antes que ignorarlos. En los casos en que el remitente no es capaz de solucionar el problema reportado, se confía en la comunicación entre los administradores de red de todas las redes afectadas, por ejemplo, un usuario doméstico cuya conexión a Internet ya no funciona debe llamar a la línea directa del servicio que le permite este acceso a Internet.

Sin embargo, dado que un mensaje ICMP es sólo un paquete IP ordinario, puede encontrar algún tipo de error en sí mismo, por ejemplo, si no hay ruta de regreso al remitente, que activaría un nuevo mensaje ICMP. Para evitar inundar la red con mensajes ICMP sobre mensajes ICMP, cada *router* comprueba si el paquete erróneo era un mensaje ICMP, y si es así, ignora el error, esperando que, eventualmente, alguien se dé cuenta del problema. Además, la mayoría de los fallos de la red son sólo temporales, por lo que simplemente volver a enviar los datos puede ser suficiente.

Es importante tener en cuenta que ICMP, aunque utiliza paquetes IP para el transporte de sus mensajes, no se considera un protocolo de nivel superior, sino una parte requerida por IP. Para poder transportar fácilmente mensajes ICMP a través de una red IP, los mensajes ICMP se encapsulan en paquetes IP.

Los mensajes ICMP se mandan utilizando la cabecera básica IP. Los primeros 8 bits corresponden al campo de tipo ICMP. Estos 8 bits indican el tipo de trama ICMP. El campo que no se utiliza deber ser etiquetado con "*unused*" y tiene que ser cero cuando se envía, pero esta información no se debe utilizar en los receptores, se debe ignorar. El formato de los paquetes de este protocolo se puede observar en la **Figura A.2**.

Paquete ICMP

	Bit 0 - 7	Bit 8 - 15	Bit 16 - 23	Bit 24 - 31
Encabezado IP (20 bytes)	Versión/IHL	Tipo de servicio	Longitud	
	Identificación		*flags* y *offset*	
	Tiempo de vida (TTL)	Protocolo	Checksum	
	Dirección IP origen			
	Dirección IP destino			
ICMP Carga (8 + bytes)	Tipo de mensaje	Code	Checksum	
	Identificador + Secuencia numérica			
	Datos (*opcional*)			

Figura A.2: Paquete ICMP. Recuperado de https://cl0udswxsequre.wordpress.com/2017/10/

Se hablarán de dos tipos de mensaje ICMP en concreto debido al uso continuado de estos en este proyecto. Estos mensajes son: ICMP *Echo Request* y ICMP *Echo Reply*.

Los *Echo Request* son mensajes ICMP en los que un dispositivo de origen solicita a un determinado dispositivo de destino que le conteste. La estructura de un mensaje ICMP tipo *Echo Request* se puede ver en la **Figura A.3**:

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Tipo = 8								Código = 0								Checksum															
Identificador																Número de secuencia															
Datos :::																															

Figura A.3: Estructura ICMP Echo Request. Recuperado de https://es.wikipedia.org/wiki/Protocolo_de_control_de_mensajes_de_Internet

El número de secuencia y el identificador se utilizan por el cliente para comprobar si coinciden o no la respuesta con la petición que causó la respuesta. En la realidad, casi todos los sistemas Linux usan un identificador único para cada ping, y el número de secuencia es un número que va aumentando dentro de ese proceso. Windows utiliza un identificador fijo, que varía entre las versiones de Windows, y un número de secuencia que sólo se reinicia en el momento del arranque.

Los mensajes *Echo Reply* son mensajes ICMP generados en respuesta a un Echo *Request*; es obligatorio para todos los hosts, y debe incluir la carga útil exacta recibida en la solicitud. La estructura de un mensaje ICMP tipo *Echo Reply* se puede ver en la **Figura A.4**:

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Tipo = 0								Código = 0								Checksum															
Identificador																Número de secuencia															
Datos :::																															

Figura A.4: Estructura ICMP Echo Reply. Recuperado de https://es.wikipedia.org/wiki/Protocolo_de_control_de_mensajes_de_Internet

El número de secuencia y el identificador se pueden usar para asociar cada *Echo Request* con su respuesta.

A.2.2 Ping y Tracert

Para este capítulo la utilización del recurso [11] ha sido de gran utilidad. Ping es un comando de administración de redes utilizado para tantear la accesibilidad de un host en una red IP. Este comando se puede utilizar en casi todos los sistemas operativos que tienen capacidad de red, incluyendo la mayoría de los programas informáticos de administración de red integrados.

Ping realiza una medición entre el tiempo de ida y el tiempo de vuelta de los mensajes enviados desde un host de origen a un host de destino. Calcula el momento de salida con el momento en el que vuelve al propio host de origen.

Ping funciona a través del envío de paquetes de *Echo Request* del protocolo ICMP al host con el que se quiere comunicar y se espera un mensaje ICMP *Echo Reply*. El programa informa de errores, pérdida de paquetes, y muestra un resumen estadístico de los resultados, típicamente incluyendo el mínimo, el máximo, la media del tiempo de ida y vuelta y la desviación típica de la media.

Las opciones de línea de comandos de ping y su salida varían entre las numerosas implementaciones posibles que hay. Las opciones pueden incluir el tamaño de la carga útil, conteo de pruebas, límites para el número de saltos de red (TTL) que las sondas atraviesan, intervalo entre las solicitudes y tiempo para esperar una respuesta.

Tracert es una de las herramientas de diagnóstico más utilizadas, por no decir indispensable, para analizar el comportamiento de la red a diseñar. Tracert permite examinar la ruta que un paquete toma a través de la red, mostrando cada uno de los *routers* individuales que manejan el paquete, así como también permite medir el tiempo (latencia) que se necesita para entregar el paquete a cada *router*. Utilizar Tracert es similar a tener una vista de pájaro de una unidad de coche de un lugar a otro, mostrando cada una de las carreteras (caminos) e intersecciones (*routers*) que se encuentran a lo largo del camino.

Usando los datos proporcionados en un Tracert, se puede verificar que los paquetes están siendo enrutados a través de rutas óptimas, así como solucionar problemas de red como pérdida de paquetes y latencia excesiva.

Microsoft Windows y ReactOS proporcionan este programa llamado Tracert. Tracert envía paquetes ICMP *Echo Request*.

El valor de tiempo de vida (TTL) se usa para comprobar los *routers* que se atraviesan hasta llegar al host de destino. Tracert envía paquetes con valores TTL que aumentan gradualmente de paquete en paquete, comenzando con el valor TTL de uno. Los *routers* van reduciendo los valores TTL de los paquetes en uno al enrutar y desechan los paquetes cuyo valor TTL ha llegado a cero, devolviendo el mensaje de error ICMP *Time Exceeded*. Para el primer conjunto de paquetes, el primer *router* recibe el paquete, decrementa el valor TTL y lo tira debido a que tiene valor TTL cero. El *router* envía un mensaje ICMP *Time Exceeded* a la fuente. Al siguiente conjunto de paquetes se le da un valor TTL de dos, así que el primer *router* envía los paquetes, pero el segundo *router* los tirará y responderá con ICMP *Time Exceeded*. Procediendo de esta manera, Tracert utiliza los mensajes ICMP *Time Exceeded* devueltos para ir

construyendo una lista de *routers* que los paquetes van atravesando, hasta que se alcance el destino y devuelva un mensaje ICMP *Echo Reply*.

A.2.3 Protocolo VRRP

Para la elaboración de este apartado ha servido de gran utilidad el recurso [5]. VRRP (*Virtual Router Redundancy Protocol*) trata de un protocolo de tipo elección, es decir, se establece de forma dinámica la responsabilidad de actuar como *router* virtual a uno de los *routers* configurados como VRRP. El *router* VRRP que controla las direcciones IP asociadas a este *router* virtual se denomina maestro, y es el encargado de redireccionar los paquetes de datos enviados a las diferentes direcciones IP que haya en la red. El proceso de elección proporciona un fallo dinámico en la responsabilidad del redireccionamiento de paquetes en caso de que el maestro no esté disponible. La ventaja que se obtiene con el uso de VRRP es una ruta predeterminada de mayor disponibilidad sin necesidad de configuración de enrutamiento dinámico o de protocolos de descubrimiento de *routers* en cada dispositivo de la red.

Hay una serie de métodos con los cuales un host final puede utilizar para determinar su primer *router* para llegar a un destino IP particular. Estos incluyen ejecutar un protocolo de enrutamiento dinámico como *Routing Information Protocol* (RIP) o OSPF versión 2, ejecutar otro protocolo llamado ICMP *Internet Router Discovery Protocol* para el descubrimiento de *routers* en la red (DISC) o usar rutas estáticas.

Ejecutar un protocolo de enrutamiento dinámico en cada dispositivo puede ser inviable por una serie de razones, incluyendo gastos generales administrativos, procesamiento de gastos generales, problemas de seguridad, o la falta de implementación de un protocolo para algunas plataformas. Protocolos vecinos o de descubrimiento de *router* pueden requerir la participación activa de todos los dispositivos en una red, lo que lleva a grandes valores de temporización para reducir la sobrecarga de tramas de este protocolo en el caso de tener muchos dispositivos. Esto puede resultar en un retraso significativo en el caso de detección de un dispositivo perdido (es decir, muerto), que puede introducir períodos inaceptablemente largos de "agujero negro".

El uso de rutas estáticas es bastante popular; minimiza la configuración y el procesamiento de la sobrecarga en los dispositivos y es soportado por cualquier implementación de IP virtual. Es probable que este modo de operación persista a medida que se desplieguen protocolos como DHCP. A grandes rasgos, este protocolo proporciona la configuración de una dirección puerta de enlace predeterminada y una dirección IP a un dispositivo. Sin embargo, esto crea un único punto de fallo. La pérdida del *router* predeterminado puede resultar ser catastrófico, aislando a todos los dispositivos ubicados más adelante en la red que serán incapaces de detectar cualquier ruta alternativa que pueda estar disponible.

El Protocolo de Redundancia a través de *Router* Virtual (VRRP) está diseñado para eliminar este punto único de fallo inherente cuando se implementa enrutado estático. Esto lo hace a través de la ruta predeterminada de mayor disponibilidad sin necesidad de configuración de enrutamiento dinámico o protocolos de descubrimiento de *routers* en cada dispositivo de la red.

VRRP proporciona una funcionalidad similar a la que se tiene en protocolos como HSRP (*Hot Standby Router Protocol*) e IPSTB (*IP Standby Protocol*).

Todos los mensajes de este protocolo se realizan utilizando datagramas *multicast* IP, por lo que el protocolo puede operar sobre una variedad de tecnologías LAN multiacceso que soportan IP *multicast*. Cada *router* virtual VRRP tiene asignada una única dirección MAC bien conocida. La dirección MAC del *router* virtual se utiliza como fuente en todos los mensajes VRRP periódicos enviados por el *router* maestro para permitir el aprendizaje de puentes en una LAN extendida.

Un *router* virtual se define por su identificador de *router* virtual (VRID) y un conjunto de direcciones IP. Un *router* VRRP puede asociarse a un *router* virtual con sus direcciones IP reales en una interfaz, y también puede ser configurado con asignaciones adicionales de este *router* virtual y asignar prioridades para los *routers* virtuales que está dispuesto a respaldar. El mapeo entre VRID y direcciones IP debe ser coordinado entre todos los *routers* VRRP en una LAN. Sin embargo, no hay ninguna restricción contra la reutilización de un VRID con una asignación de direcciones IP diferente en distintas LANs.

Para minimizar el tráfico en la red, sólo el maestro envía mensajes de aviso VRRP periódicos. Un *router* en modo *backup* no intentará adelantarse al maestro a menos que tenga mayor prioridad. Esto elimina las interrupciones en el servicio a menos que una ruta mejor esté disponible. También es posible prohibir administrativamente todos los intentos preventivos. La única excepción es que un *router* VRRP siempre se convertirá en maestro de cualquier *router* virtual asociado con las direcciones que posee. Si el maestro pasa a estar no disponible, el *router* que estaba en modo *backup* de mayor prioridad pasará a ser maestro después de un breve retraso, proporcionando una transición controlada de la responsabilidad del *router* virtual con una mínima interrupción del servicio.

El diseño del protocolo VRRP proporciona una transición rápida de *backup* a maestro para minimizar la interrupción del servicio, e incorpora optimizaciones que reducen la complejidad del protocolo al tiempo que garantiza una transición a maestro controlada para escenarios típicos. Las optimizaciones resultan en un protocolo de tipo elección con requisitos mínimos de estado de ejecución, estados mínimos de protocolo activo, y un único tipo de mensaje y remitente. Los escenarios operativos típicos se definen como dos *routers* redundantes y/o distintas preferencias en las rutas entre cada *router*. Un efecto secundario cuando estas suposiciones son violadas (es decir, más de dos rutas redundantes todas con igual preferencia) es que los paquetes duplicados pueden ser redireccionados por un breve período durante la elección del *router* maestro. Sin embargo, los supuestos planteados en un escenario típico son muy probables de que se cumplan en la mayoría de los despliegues en redes, que la pérdida del *router* maestro sea infrecuente y la duración prevista en la convergencia de las elecciones generales sea bastante pequeña (<< 1 segundo). Así las optimizaciones VRRP representan simplificaciones significativas en el diseño del protocolo mientras que incurren en una probabilidad insignificante de degradación breve de la red.

A.2.4 Protocolo PRP e iPRP

Para la elaboración de este apartado se ha hecho uso de los recursos [4] [7] [8] [10] y documentación privada de Siemens. Varias tecnologías de redundancia se han establecido en el entorno Ethernet, lo que garantiza que la red continúe funcionando sin problemas incluso si fallan las conexiones individuales. Una tecnología de redundancia que se ha establecido en el mundo de Ethernet por cable es el "*Parallel Redundancy Protocol*" (abreviado como: PRP). Para lograr la redundancia, en este método los datos se transmiten al mismo tiempo entre dos o más dispositivos en caminos físicamente diferentes. Hasta ahora, los usuarios tenían que enfrentarse a los desafíos de la comunicación por radio con respecto a los problemas de fiabilidad. El uso del "*Parallel Redundancy Protocol*" puede ayudar aquí.

Se puede usar PRP en redes de comunicación industrial cableadas e inalámbricas. Sin embargo, en un entorno inalámbrico, el efecto del protocolo PRP es diferente al de un entorno cableado, a pesar de ser el mismo método. Si se utiliza PRP en redes cableadas, entonces cambiar entre dos redes es sencillo. Si se usa PRP para enlaces de radio, se puede llegar a compensar la interferencia. Para lograr esto, los paquetes se transmiten con PRP en dos enlaces de radio diferentes simultáneamente. Esto permite compensar un error en la transmisión en un enlace mediante la transmisión en paralelo por el otro enlace.

PRP solo funciona con dos rutas de aproximadamente la misma velocidad. Sin embargo, en el área WLAN, los cambios dentro de una red de celdas pueden conducir rápidamente a caminos con diferentes velocidades. El principal desafío es proporcionar el principio de PRP en WLAN también.

Si se utiliza PRP en redes inalámbricas, se tienen los siguientes valores añadidos:

- En comparación con la comunicación por cable, el uso de WLAN en sistemas industriales ofrece una variedad de ventajas en términos de flexibilidad y rentabilidad.
- WLAN se puede usar para implementar aplicaciones las cuales no se pueden lograr con soluciones cableadas.
- Gracias a PRP, se puede crear una comunicación con alta disponibilidad, redundante e ininterrumpida.
- PRP permite múltiples topologías de redes inalámbricas y cableadas y sus respectivas configuraciones de seguridad

Para hacer que el principio de PRP también esté disponible en enlaces de radio con rutas de diferentes velocidades, Siemens ofrece una solución con el "*industrial Parallel Redundancy Protocol*" (iPRP) patentado por *iFeature*. iPRP es la extensión de PRP mediante transmisión inalámbrica de datos a través de iWLAN.

Cuando se utiliza iPRP se tienen las siguientes ventajas:

- Se puede usar IWLAN en una red PRP.

- Con iPRP, se puede realizar una comunicación inalámbrica con alta disponibilidad, redundante e ininterrumpida.
- Evita cargar innecesariamente la red inalámbrica con telegramas redundantes, los clientes iPRP se sincronizan entre sí.

A.2.4.1 Conocimientos básicos del protocolo PRP

Para lograr la redundancia, el método de redundancia PRP transfiere datos entre dos o más dispositivos en rutas separadas físicamente. En el caso de que una falla, la ruta intacta puede continuar transmitiendo todo el flujo de datos sin interrupción o pérdida de rendimiento.

PRP es un protocolo de redundancia para redes cableadas. Se define en la Parte 3 de la norma IEC 62439. La gran ventaja del protocolo PRP es la conmutación ininterrumpida, que evita cualquier tiempo de conmutación en caso de fallo y, por lo tanto, ofrece la mayor disponibilidad posible.

PRP pertenece a la categoría de redundancia de red y se basa en dos redes independientes de cualquier topología (LAN A o LAN B). A diferencia de otros métodos de redundancia, PRP se implementa en los dispositivos terminales. Los *switches* en la red son *switches* estándar y no necesitan saber nada sobre PRP. Cada uno de los dispositivos terminales tiene al menos dos conexiones de red separadas que están conectadas a redes independientes (ver **Figura A.5**).

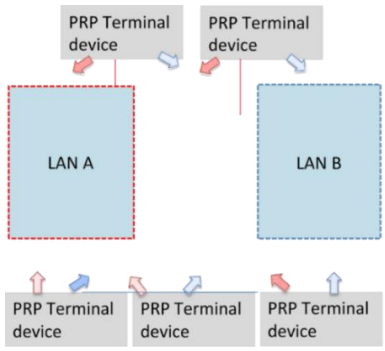


Figura A.5: Principio de operación de PRP

Para lograr la mayor disponibilidad posible, la especificación para PRP proporciona dos mecanismos principales:

- Duplicación en el lado del remitente
- Eliminación en el lado del receptor

La topología de una red PRP consta de dos subredes Ethernet independientes y terminales PRP. Puede construir una red PRP a partir de componentes estándar o terminales PRP. Las dos redes (LAN A o LAN B) pueden tener estructuras idénticas o pueden diferir en topología o rendimiento. Un dispositivo con funcionalidad PRP se denomina "Nodo de doble conexión para PRP". (abreviado a: DAN P). Una interfaz DAN P tiene al menos dos conexiones de red separadas que se conectan a las redes (LAN A o LAN B). Componentes estándar ("Nodo adjunto estándar", abreviado a: SAN) con una única interfaz de red, puede conectarse directamente a una de las dos redes (LAN

A o LAN B). Dado que un SAN no tiene una ruta redundante disponible en caso de fallo, un SAN no se beneficia de la redundancia de la red. Para conectar también un SAN de forma redundante, use un *Redundancy Box* (RedBox). Un RedBox conecta una o más SAN a ambas redes (LAN A o LAN B) y se hace cargo de las funciones de PRP en nombre de todas las SAN conectadas a él. La **Figura A.6** muestra de manera simple cómo se puede configurar una red PRP con los componentes mencionados.

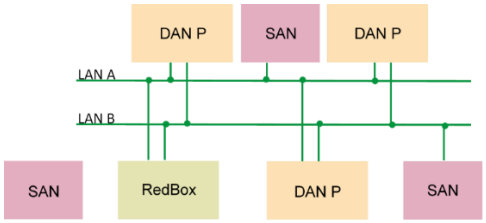


Figura A.6: Configuración de red PRP

Cuando un dispositivo PRP envía un telegrama, el procedimiento aproximado que sigue es el siguiente:

- El dispositivo PRP duplica el telegrama.
- Para marcar los telegramas como duplicados, el dispositivo PRP amplía las tramas redundantes añadiendo un "*Redundancy Control Trailer*" (RCT) adicional.
- El dispositivo PRP envía un telegrama (duplicación) a cada red conectada (LAN A o LAN B).

Los dos telegramas pasan a través de las dos redes independientes con diferentes retardos que pueda haber en cada red. El dispositivo PRP recibe dos paquetes de datos idénticos durante la operación sin problemas. El procedimiento de recepción se describe a continuación:

- El primer paquete entrante al dispositivo PRP es reenviado directamente a su destino.
- Para reconocer un telegrama duplicado, el dispositivo PRP 'recuerda' su número de secuencia de paquetes del RCT durante un tiempo determinado.
- El dispositivo PRP reconoce el segundo paquete entrante como duplicado por el número de secuencia del paquete en el RCT.
- El dispositivo PRP descarta el paquete duplicado (eliminación).

Dado que el RCT se inserta al final de la trama, todo el tráfico permanece completamente legible para los SAN. Un SAN solo interpreta el RCT como bits de relleno insertados adicionalmente sin significado.

Con PRP, puede usar dos redes independientes con cualquier topología (incluidos los anillos), rendimiento y latencia. Hay que tener en cuenta que la latencia de la red y las diferencias de tiempo de ejecución en las redes pueden diferir solo hasta cierto límite.

PRP es un protocolo de ventana deslizante basado en números de secuencia de paquetes con capacidad de ventana finita. Para detectar duplicados, PRP define una

ventana de tiempo máximo de 400 ms. Durante este tiempo, el telegrama y su duplicado deben llegar al dispositivo PRP.

Si los telegramas redundantes llegan al dispositivo PRP con grandes diferencias de tiempo, puede suceder que su filtro duplicado se omita porque la diferencia de tiempo es demasiado grande. El resultado es que los telegramas duplicados se envían a uno o más SAN.

Las dos redes deben estar diseñadas de tal manera que fallen independientemente una de la otra. Si un cable se extrae de una red, el otro no debe verse afectado. Por lo tanto, no debe haber conexión directa entre las dos LAN.

A.2.4.2 Conocimientos básicos del protocolo iPRP

La tecnología PRP requiere ciertos tiempos de transmisión para las dos redes independientes (LAN A o LAN B), que están diseñadas para redes Ethernet. En el área de WLAN, debido a los cambios dentro de una red de celdas, el medio compartido y el acceso al canal no determinista, pueden generarse rutas con diferentes velocidades y, por tanto, que los tiempos de latencia en ambas redes puedan ser distinto.

El "*industrial Parallel Redundancy Protocol*" patentado por *iFeature* de Siemens (iPRP para abreviar) es una solución para la comunicación inalámbrica a través de las dos redes independientes. iPRP se basa en PRP.

Si se usa iPRP, se puede usar WLAN para las dos redes independientes (LAN A o LAN B). Se activa iPRP en todos los componentes WLAN. En la red cableada, se continúa utilizando dispositivos PRP estándar que duplican el telegrama.

El tiempo de transmisión en una red WLAN puede variar mucho debido a la intensidad de la señal. Para informarse mutuamente sobre el estado de la transmisión, los clientes y los puntos de acceso se sincronizan entre sí a través de la red cableada en iPRP. La **Figura A.7** muestra la estructura básica en una representación simplificada:

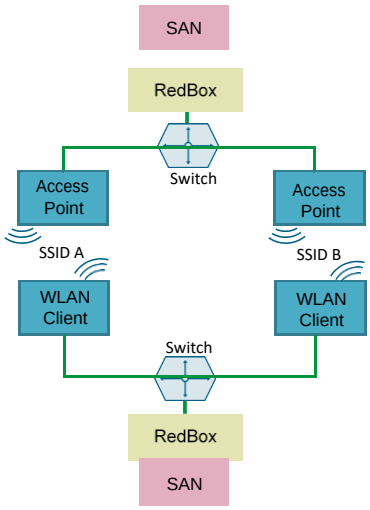


Figura A.7: Estructura básica iPRP

Con iPRP, se puede usar WLAN en las redes independientes (LAN A o LAN B) requeridas por PRP. Dado que los puntos de acceso y los clientes se sincronizan entre sí a través de la interfaz Ethernet, los puntos de acceso y los clientes están conectados

entre sí a través de un *switch* en la red cableada. Las redes locales virtuales (abreviadas: VLAN) se utilizan para implementar las redes independientes requeridas por PRP. Los dispositivos PRP estándar (RedBox) en la red cableada proporcionan funcionalidad PRP. Se puede configurar la WLAN para que los clientes puedan conectarse teóricamente a cada punto de acceso, lo que aumenta la redundancia de los enlaces de radio. iPRP evita que ambos clientes escaneen simultáneamente la red inalámbrica y que los dos clientes inicien sesión en la misma interfaz de un punto de acceso. No es posible conectar directamente los puntos de acceso y los clientes a un RedBox dado que las interfaces para las redes PRP (LAN A o LAN B) en RedBox no están conectadas internamente entre sí, por lo que no sería posible la sincronización entre los puntos de acceso o clientes.

La duplicación de los telegramas redundantes se realiza mediante terminales PRP estándar en la red cableada. Los puntos finales PRP no necesitan saber sobre iPRP. Al igual que con PRP, el telegrama se duplica en la red cableada por dispositivos PRP estándar y se enruta a los dos dispositivos de transmisión (clientes o puntos de acceso). Los dispositivos de transmisión almacenan el telegrama en su búfer de transmisión. El tiempo de transmisión en una red WLAN puede variar mucho debido a la intensidad de la señal. Para evitar cargar innecesariamente la red inalámbrica de telegramas con largos tiempos de transmisión, se aplica la siguiente característica a la transmisión de telegramas con iPRP: Si una unidad de transmisión pudo transmitir el telegrama más rápido y con éxito al receptor debido a una mejor conexión de radio, entonces la unidad de transmisión notifica a la otra unidad de transmisión que ha enviado con éxito el telegrama y le solicita que elimine el telegrama del búfer de transmisión. Con este método, el dispositivo PRP recibe solo un telegrama en el lado cableado. Por lo tanto, no es necesario eliminar los telegramas redundantes. Si la unidad de transmisión redundante ha transmitido el telegrama antes de recibir la confirmación de envío de la otra unidad de transmisión, entonces el dispositivo PRP recibe ambos telegramas en el lado cableado y elimina el telegrama redundante de la manera mencionada anteriormente. En una red inalámbrica, el más rápido de los dos telegramas generalmente es el que siempre se reenvía. De esta manera, los telegramas con largos tiempos de transmisión, como es el caso de WLAN, pueden eliminarse en gran medida.

Para poder usar iPRP, se deben cumplir los siguientes requisitos previos:

- Las dos redes independientes deben estar separadas a través de VLAN. Esto requiere *switches* habilitados para VLAN.
- El RCT adicional aumenta el tamaño del paquete Ethernet a otros seis bytes. Todos los componentes estándar utilizados deben poder procesar marcos de gran tamaño.
- Los siguientes dispositivos SCALANCE W son obligatorios para iPRP:
    - SCALANCE W780 o SCALANCE W740
    - **SCALANCE W770 o SCALANCE W730 (utilizados)**
    - SCALANCE W722
- Para usar el *iFeature* iPRP, se necesita la KEY-PLUG W740 para los clientes y la KEY-PLUG W780 para los puntos de acceso.

A.3 PARAMETRIZACIÓN DE LOS *FIREWALL* (S615)

Para este apartado ha sido clave el estudio y comprensión del recurso [17]. En este caso, la configuración de ambos S615 es algo distinta, se explica primero la configuración realizada en el S615 ubicado en el lado clientes y, a continuación, la configuración realizada en el S615 en el lado de los puntos de acceso. En este proyecto no se entrará en detalle sobre la creación de las reglas de *firewall* para lo que sería un entorno real ferroviario, exclusivamente se utilizan con funcionalidad de *routing*.

Para la configuración del S615 ubicado en el control del tren **(S615_Cliente)**, se siguen los siguientes pasos:

1. Configuración de *routing* con sus rutas estáticas (ver **Figura A.8**).

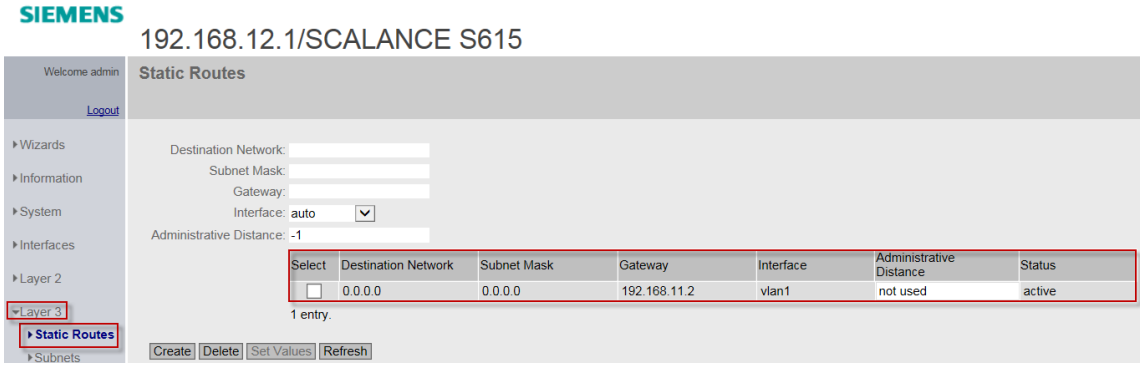


Figura A.8: Configuración de rutas estáticas en S615 en el lado cliente

2. Asignación de VLANs a diferentes subredes (ver **Figura A.9**).

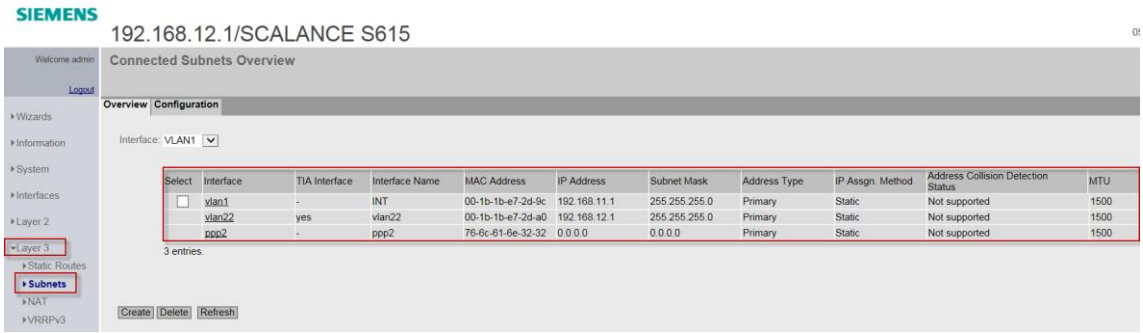


Figura A.9: Asignación de VLANs a diferentes subredes en S615 en el lado cliente

Para la configuración del S615 ubicado en el control de mandos **(S615_AP)**, se siguen los siguientes pasos:

1. Configuración de *routing* con sus rutas estáticas (ver **Figura A.10**).

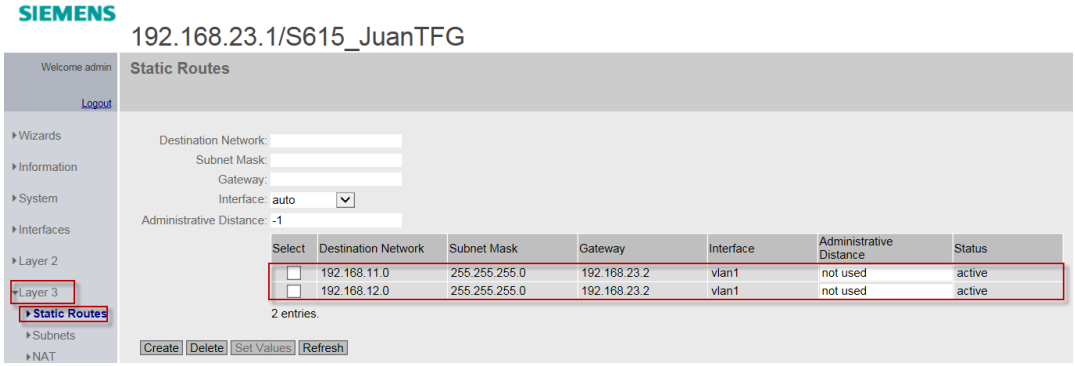


Figura A.10: Configuración de rutas estáticas en S615 en el lado AP

2. Asignación de puertos a VLANs con diferentes subredes (una de ellas con IP dinámica por DHCP) (ver **Figura A.11**).

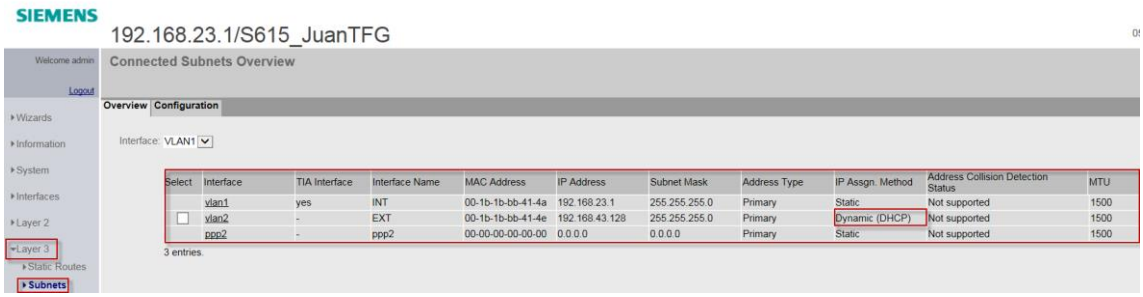


Figura A.11: Asignación de VLANs a diferentes subredes en S615 en el lado AP

A.4 *DATASHEETS* DE LOS DISPOSITIVOS UTILIZADOS

En este apéndice se van a insertar o compartir los enlaces a cada uno de los *datasheets* públicos de cada uno de los dispositivos o materiales utilizados en este proyecto. En un principio se había optado por añadirlos al proyecto sin el enlace, sino como una parte más del proyecto, pero por motivos del Turnitin y también debido al tamaño que ocupaban, se ha optado por añadirlos en formato de enlace a página web.

- Clientes Wi-Fi (W734-1) (6GK5734-1FX00-0AA0): https://mall.industry.siemens.com/mall/es/es/Catalog/Product/6GK5734-1FX00-0AA0
- Puntos de acceso (W788-1) (6GK5788-1GD00-0AA0): https://mall.industry.siemens.com/mall/es/es/Catalog/Product/6GK5788-1GD00-0AA0
- *Switches* gestionables:
    - XB208 (6GK5208-0BA00-2AB2): https://mall.industry.siemens.com/mall/es/es/Catalog/Product/6GK5208-0BA00-2AB2
    - XC216-4C (6GK5216-4BS00-2AC2): https://mall.industry.siemens.com/mall/es/es/Catalog/Product/6GK5216-4BS00-2AC2
- *Switches* RNA:
    - X204RNA (6GK5204-0BA00-2KB2): https://mall.industry.siemens.com/mall/es/es/Catalog/Product/6GK5204-0BA00-2KB2
    - X204RNA EEC (6GK5204-0BS00-3LA3): https://mall.industry.siemens.com/mall/es/WW/Catalog/Product/6GK5204-0BS00-3LA3
- *Routers* (XM408-8C) (6GK5408-8GS00-2AM2): https://mall.industry.siemens.com/mall/es/WW/Catalog/Product/6GK5408-8GS00-2AM2
- *Firewalls* (S615) (6GK5615-0AA00-2AA2): https://mall.industry.siemens.com/mall/es/WW/Catalog/Product/6GK5615-0AA00-2AA2
- PLCs (S7-1200) (6ES7214-1BG40-0XB0): https://mall.industry.siemens.com/mall/es/es/Catalog/Product/6ES7214-1BG40-0XB0
- Alimentación Despliegue en tren (S7-1500 PM1507) (6EP1332-4BA00): https://mall.industry.siemens.com/mall/es/WW/Catalog/Product/6EP1332-4BA00
- Alimentación Despliegue en vía (S7-1500 PM1507) (6EP1333-4BA00): https://mall.industry.siemens.com/mall/es/es/Catalog/Product/6EP1333-

4BA00

- Conector M12 8 hilos (6GK1901-0DB30-6AA0): https://mall.industry.siemens.com/mall/es/es/Catalog/Product/6GK1901-0DB30-6AA0
- Conector RJ45 4 hilos (6GK1901-1BB10-2AA0): https://mall.industry.siemens.com/mall/es/es/Catalog/Product/6GK1901-1BB10-2AA0
- Ethernet 4 hilos (6XV1840-2AH10): https://mall.industry.siemens.com/mall/es/ww/Catalog/Product/6XV1840-2AH10
- Ethernet 8 hilos (6XV1878-2A): https://mall.industry.siemens.com/mall/en/us/Catalog/Product/6XV18782A
- Antena Clientes Wi-Fi (ANT795-4MA) (6GK5795-4MA00-0AA3): https://mall.industry.siemens.com/mall/es/es/Catalog/Product/6GK5795-4MA00-0AA3
- Antena Puntos de accesos (ANT795-4MC) (6GK5795-4MC00-0AA3): https://mall.industry.siemens.com/mall/es/es/Catalog/Product/6GK5795-4MC00-0AA3

A.5 PROYECTO COMUNICACIÓN S7 TIA PORTAL V15.1

Para la realización de este apartado se ha utilizado el recurso [6] y documentación privada de Siemens. En este apartado se explica cómo es la comunicación S7 entre los dos S7-1200 y se muestra un par de figuras donde se comprueba que la conexión está establecida entre ambos.

La comunicación S7 es un protocolo propietario de Siemens que funciona entre controladores lógicos programables (PLCs) de la familia Siemens S7-300/400 y S7-1200/1500. Se utiliza para la programación de PLCs, para el intercambio de datos entre PLCs, para el acceso a datos del PLC a un SCADA (Control de Supervisión y Adquisición de Datos) y para fines de diagnóstico. Los datos en este protocolo S7 vienen como carga útil de paquetes de datos COTP (Protocolo de Transporte Orientado a la Conexión). El primer byte es siempre 0x32 como identificador de protocolo.

A continuación, en la **Figura A.12**, se presenta un ejemplo en Wireshark del tipo de trama que se tendría en este tipo de comunicación:

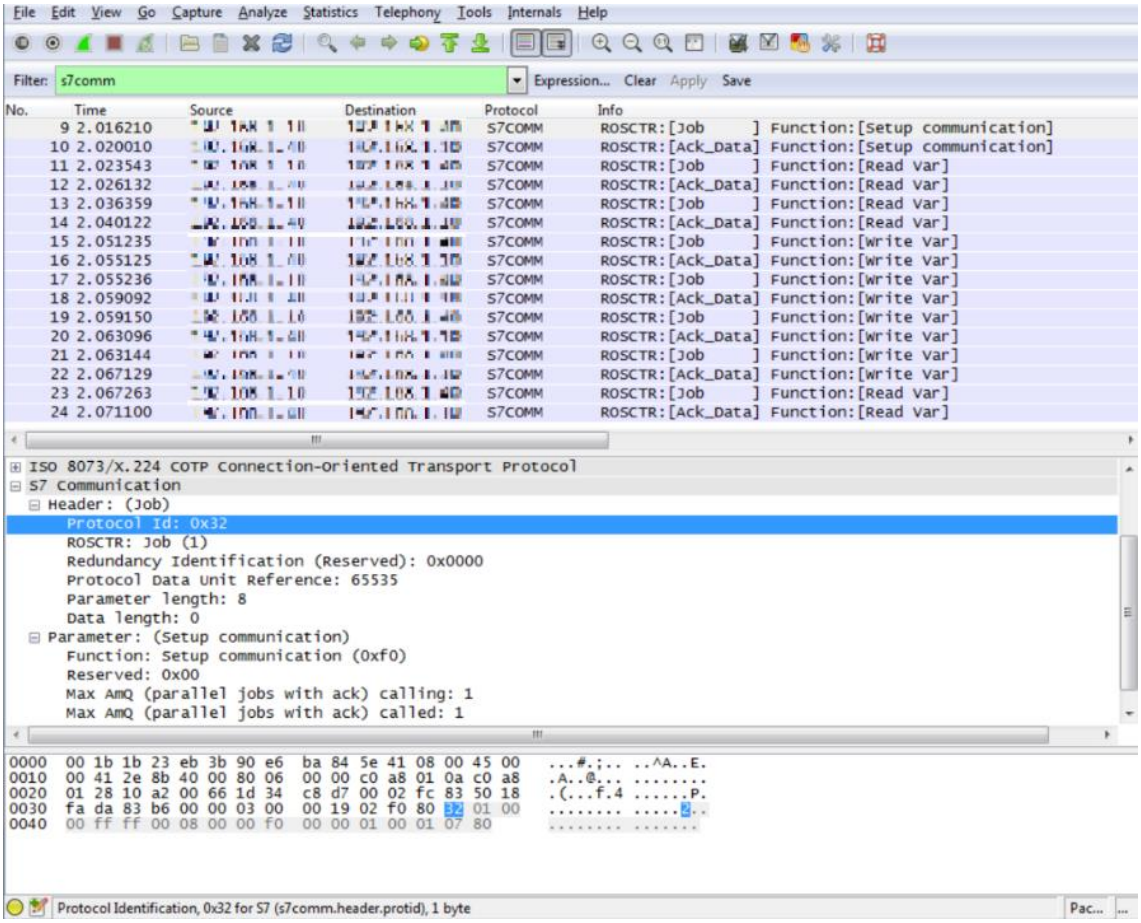


Figura A.12: Trama comunicación S7 en Wireshark. Recuperado de https://wiki.wireshark.org/S7comm

En las figuras a continuación, **Figura A.13** y **Figura A.14**, se muestra la conexión establecida entre ambos PLCs:

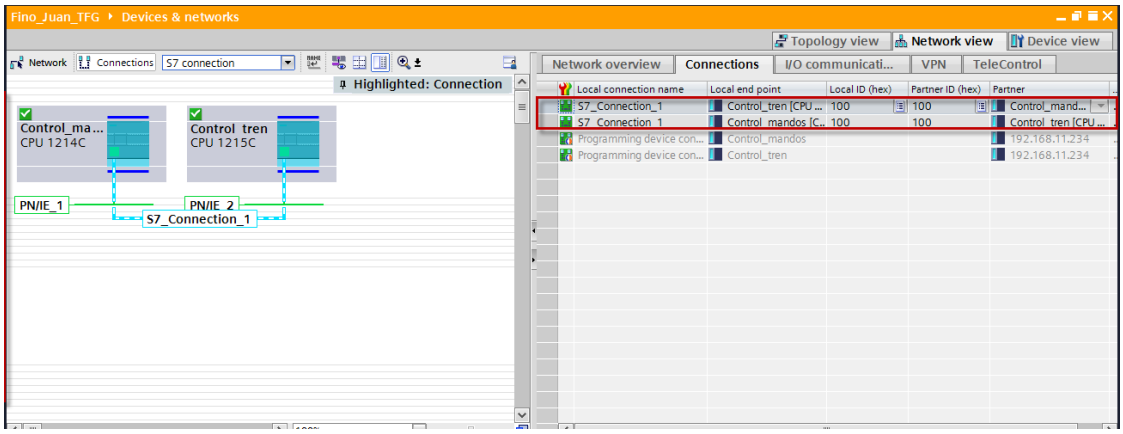


Figura A.13: Comprobación conexión establecida en comunicación S7 en TIA PORTAL

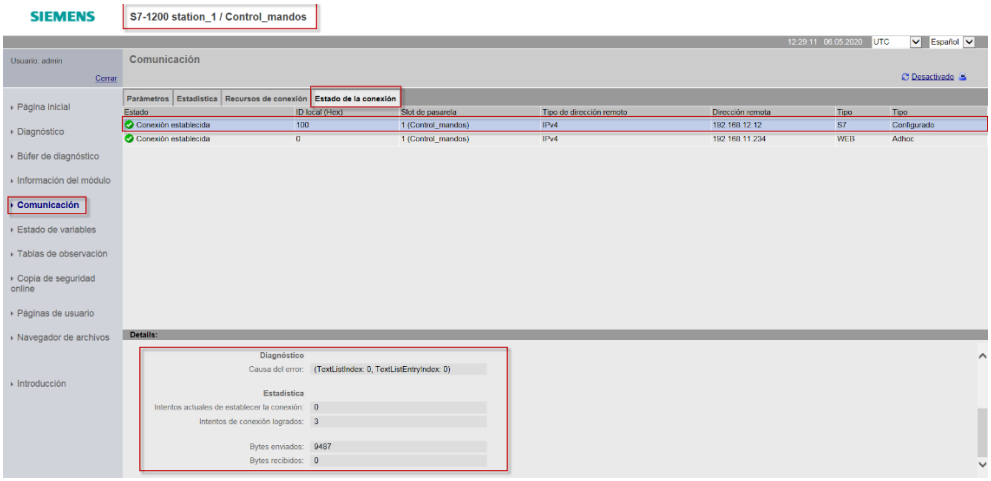
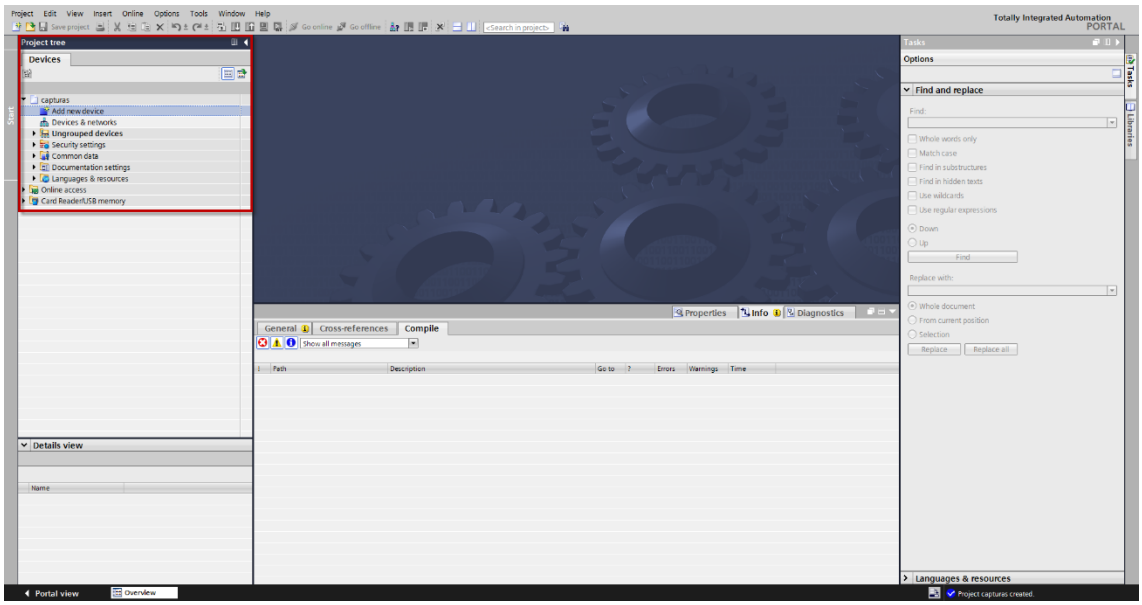
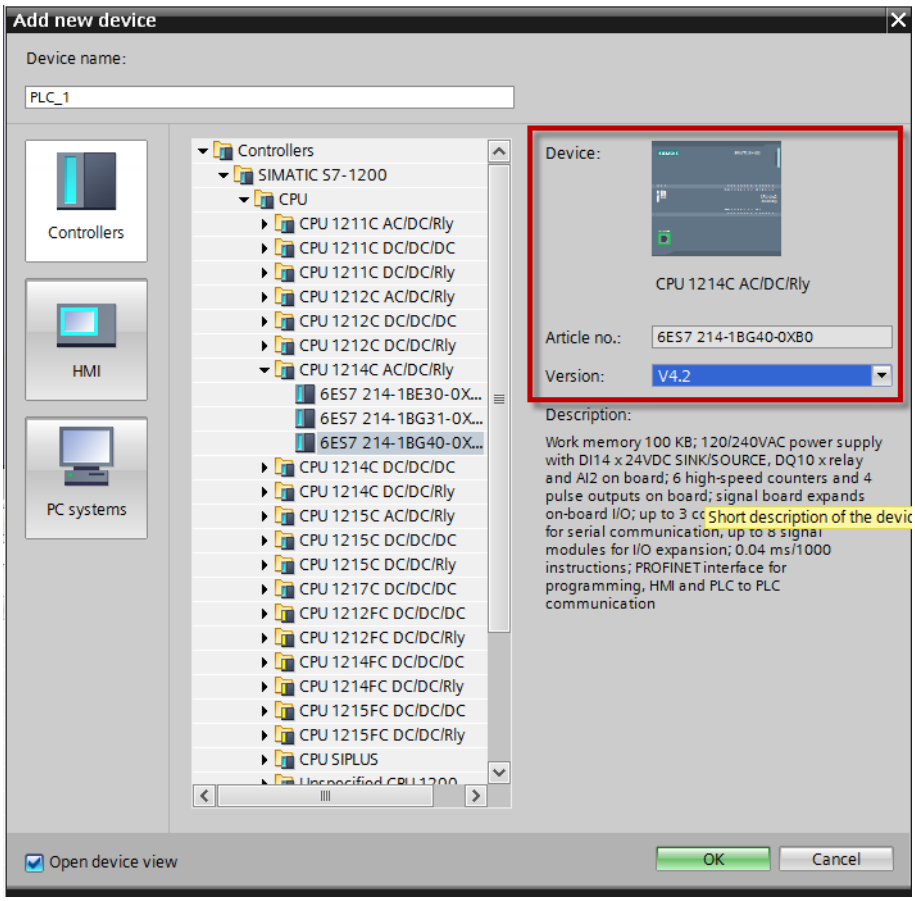


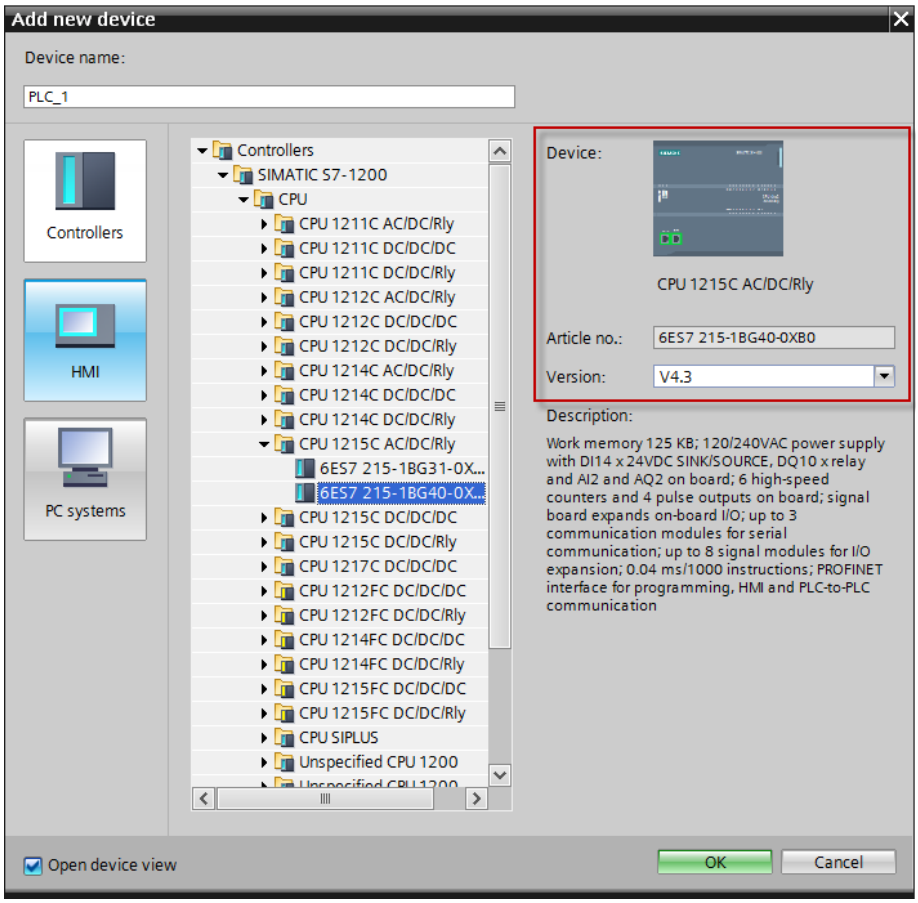
Figura A.14: Comprobación conexión establecida en comunicación S7 en Web Server del "Control de mandos"

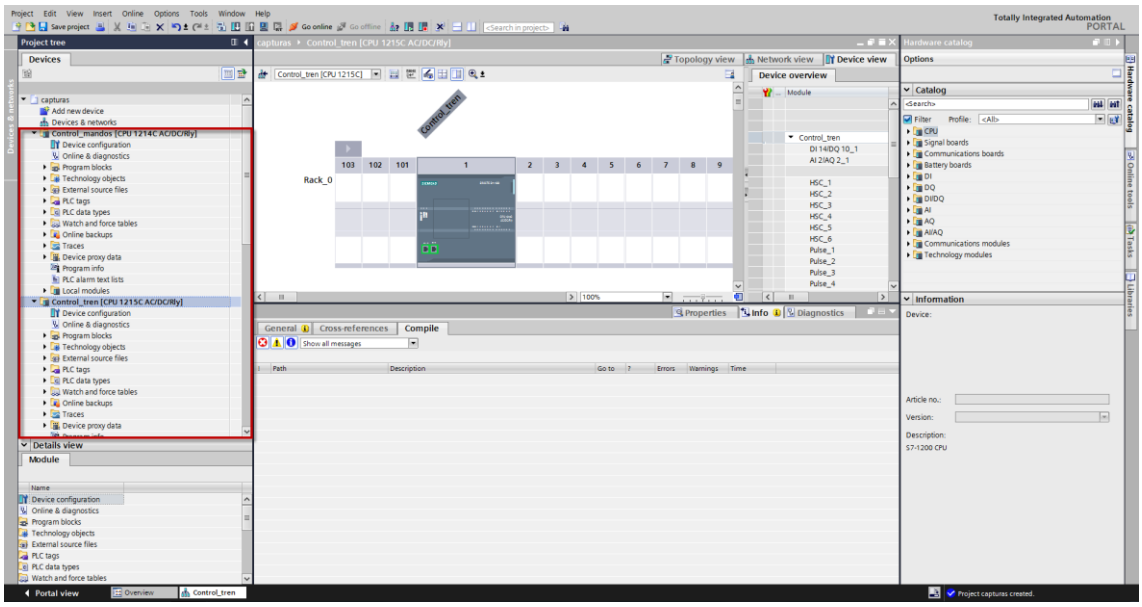
A continuación, se muestra el proceso paso a paso para establecer esta comunicación S7 entre ambos PLCs.

1. Para comenzar con el proyecto de TIA Portal V15.1, primero se añaden los dos PLCs que se utilizarán en este proyecto, siendo un S7-1214 AC/DC/RLY y un S7-1215 AC/DC/RLY con sus respectivas versiones de firmware:

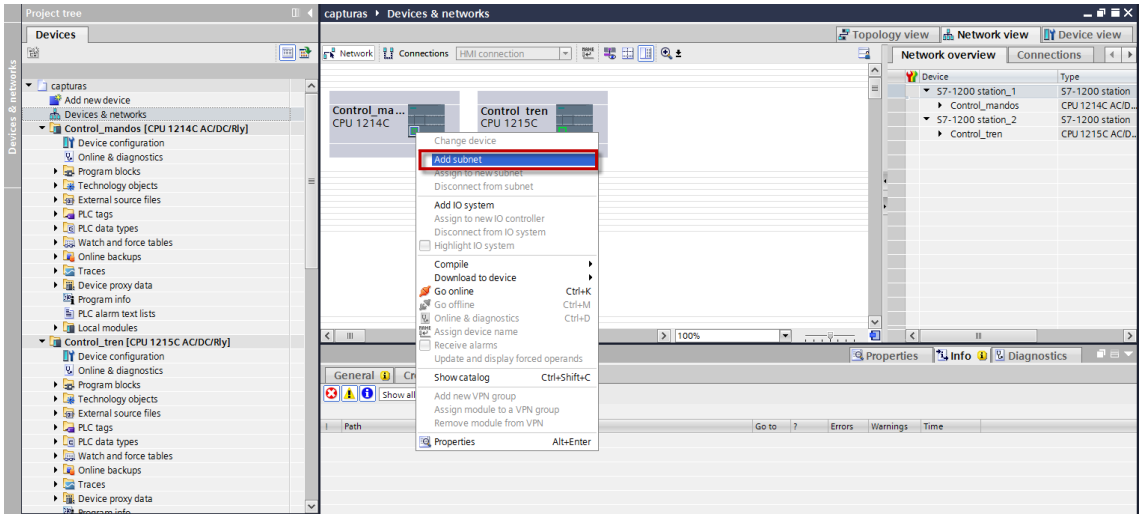


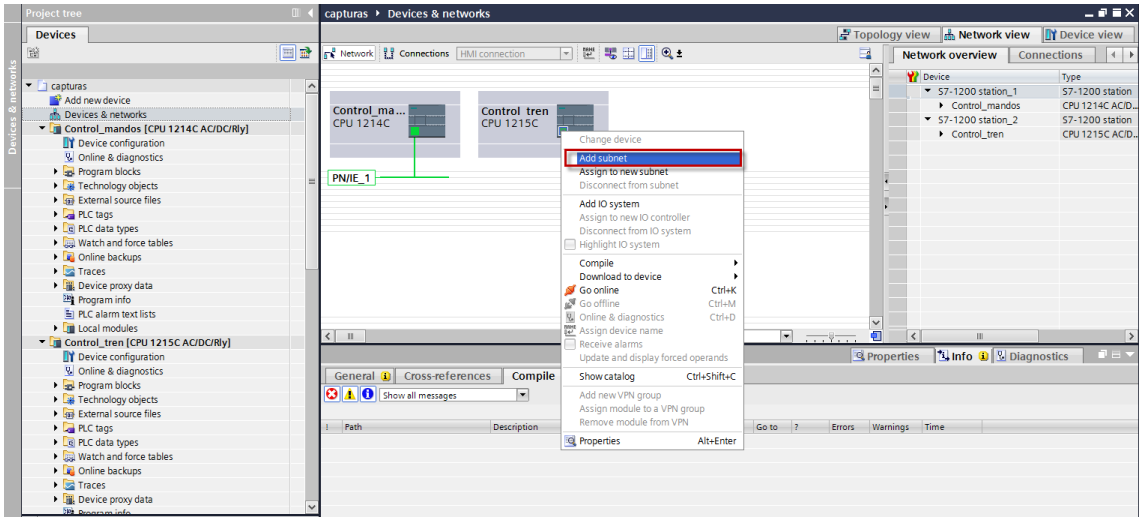

Add new device
Device name:
PLC_1
Controllers
HMI
PC systems
Controllers
SIMATIC S7-1200
CPU
CPU 1211C AC/DC/Rly
CPU 1211C DC/DC/DC
CPU 1211C DC/DC/Rly
CPU 1212C AC/DC/Rly
CPU 1212C DC/DC/DC
CPU 1212C DC/DC/Rly
CPU 1214C AC/DC/Rly
6ES7 214-1BE30-0X...
6ES7 214-1BG31-0X...
6ES7 214-1BG40-0X...
CPU 1214C DC/DC/DC
CPU 1214C DC/DC/Rly
CPU 1215C AC/DC/Rly
CPU 1215C DC/DC/DC
CPU 1215C DC/DC/Rly
CPU 1217C DC/DC/DC
CPU 1212FC DC/DC/DC
CPU 1212FC DC/DC/Rly
CPU 1214FC DC/DC/DC
CPU 1214FC DC/DC/Rly
CPU 1215FC DC/DC/DC
CPU 1215FC DC/DC/Rly
CPU SIPLUS
Device:
CPU 1214C AC/DC/Rly
Article no.:
6ES7 214-1BG40-0XB0
Version:
V4.2
Description:
Work memory 100 KB; 120/240VAC power supply with DI14 x 24VDC SINK/SOURCE, DQ10 x relay and AI2 on board; 6 high-speed counters and 4 pulse outputs on board; signal board expands on-board I/O; up to 3 c
Short description of the devic
for serial communication, up to 8 signal modules for I/O expansion; 0.04 ms/1000 instructions; PROFINET interface for programming, HMI and PLC to PLC communication
Open device view
OK
Cancel


Add new device
Device name:
PLC_1
Controllers
HMI
PC systems
Controllers
SIMATIC S7-1200
CPU
CPU 1211C AC/DC/Rly
CPU 1211C DC/DC/DC
CPU 1211C DC/DC/Rly
CPU 1212C AC/DC/Rly
CPU 1212C DC/DC/DC
CPU 1212C DC/DC/Rly
CPU 1214C AC/DC/Rly
CPU 1214C DC/DC/DC
CPU 1214C DC/DC/Rly
CPU 1215C AC/DC/Rly
6ES7 215-1BG31-0X...
6ES7 215-1BG40-0X...
CPU 1215C DC/DC/DC
CPU 1215C DC/DC/Rly
CPU 1217C DC/DC/DC
CPU 1212FC DC/DC/DC
CPU 1212FC DC/DC/Rly
CPU 1214FC DC/DC/DC
CPU 1214FC DC/DC/Rly
CPU 1215FC DC/DC/DC
CPU 1215FC DC/DC/Rly
CPU SIPLUS
Unspecified CPU 1200
Device:
CPU 1215C AC/DC/Rly
Article no.:
6ES7 215-1BG40-0XB0
Version:
V4.3
Description:
Work memory 125 KB; 120/240VAC power supply with DI14 x 24VDC SINK/SOURCE, DQ10 x relay and AI2 and AQ2 on board; 6 high-speed counters and 4 pulse outputs on board; signal board expands on-board I/O; up to 3 communication modules for serial communication; up to 8 signal modules for I/O expansion; 0.04 ms/1000 instructions; PROFINET interface for programming, HMI and PLC-to-PLC communication
Open device view
OK
Cancel

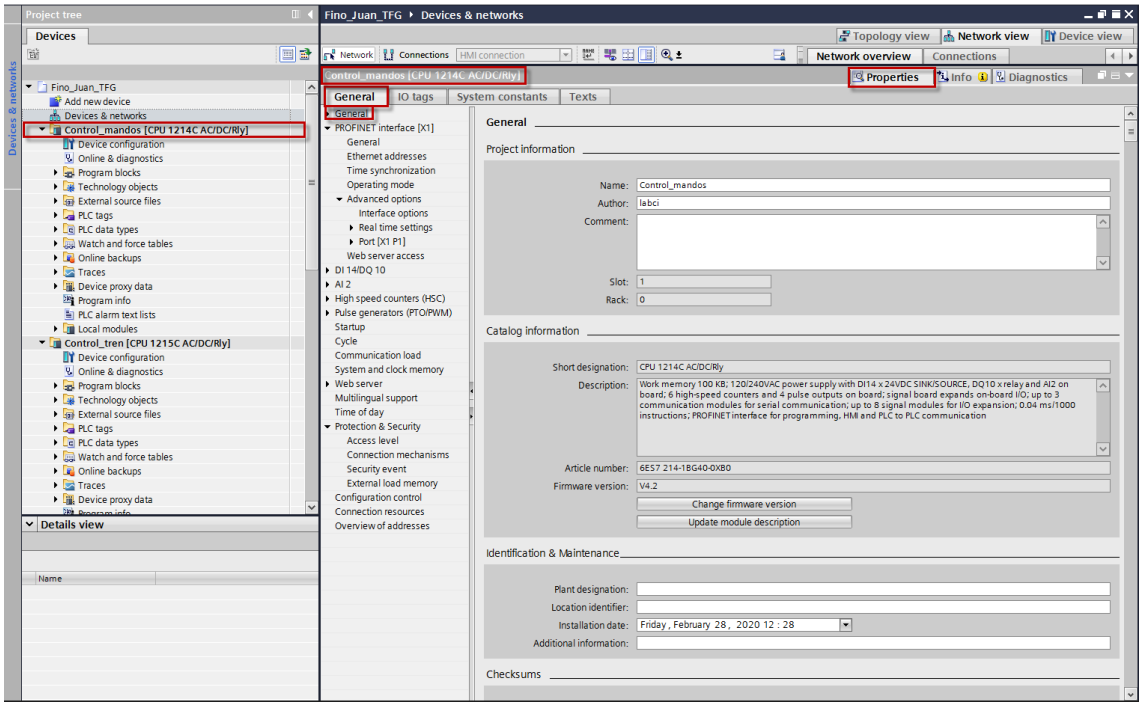


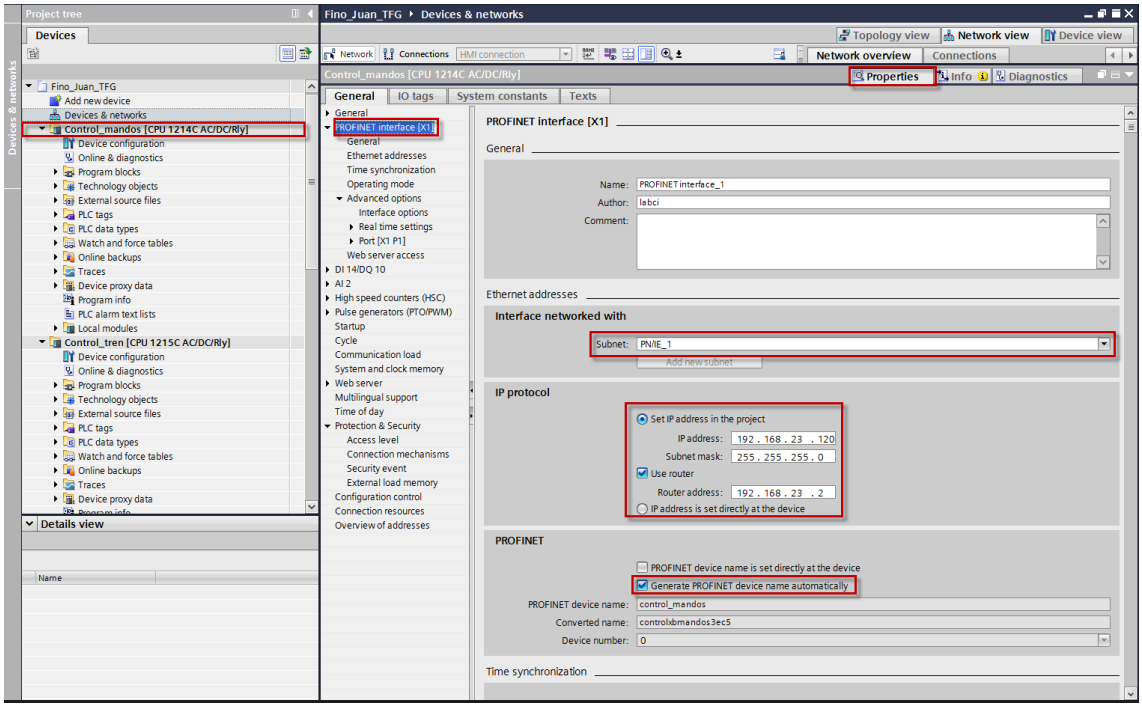
2. A continuación, se añaden ambos PLCs a diferentes subredes de la siguiente forma como se muestra en las figuras inferiores:

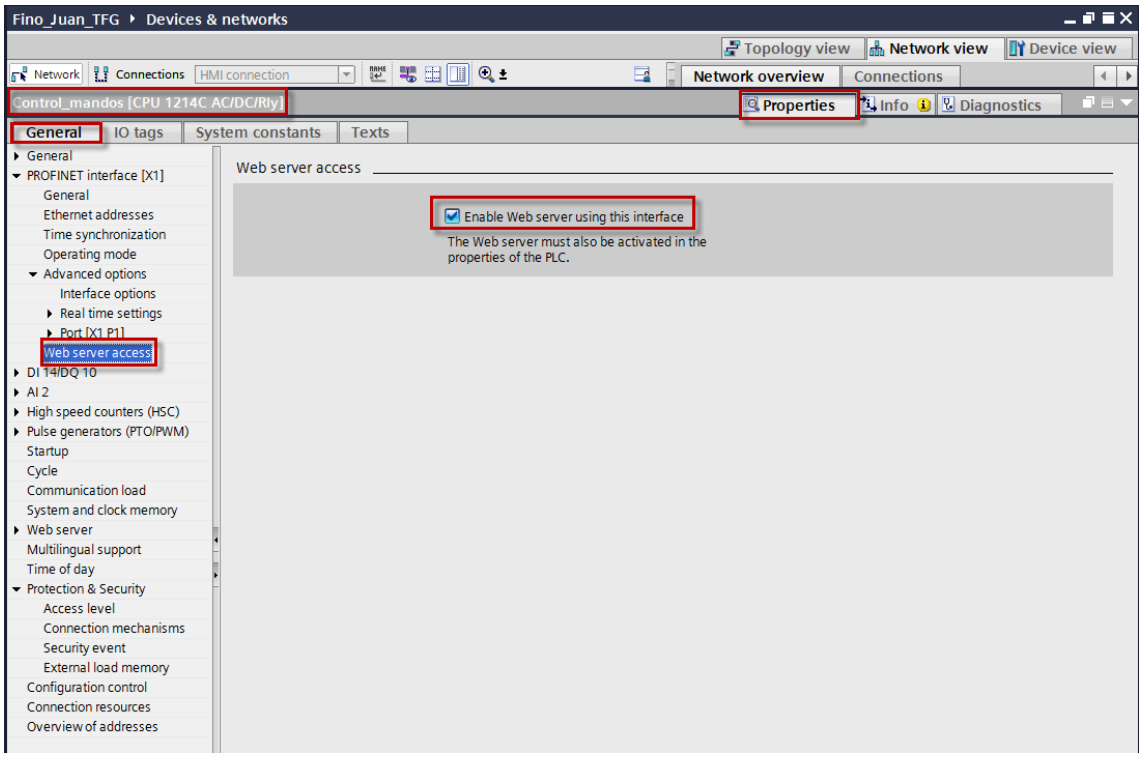


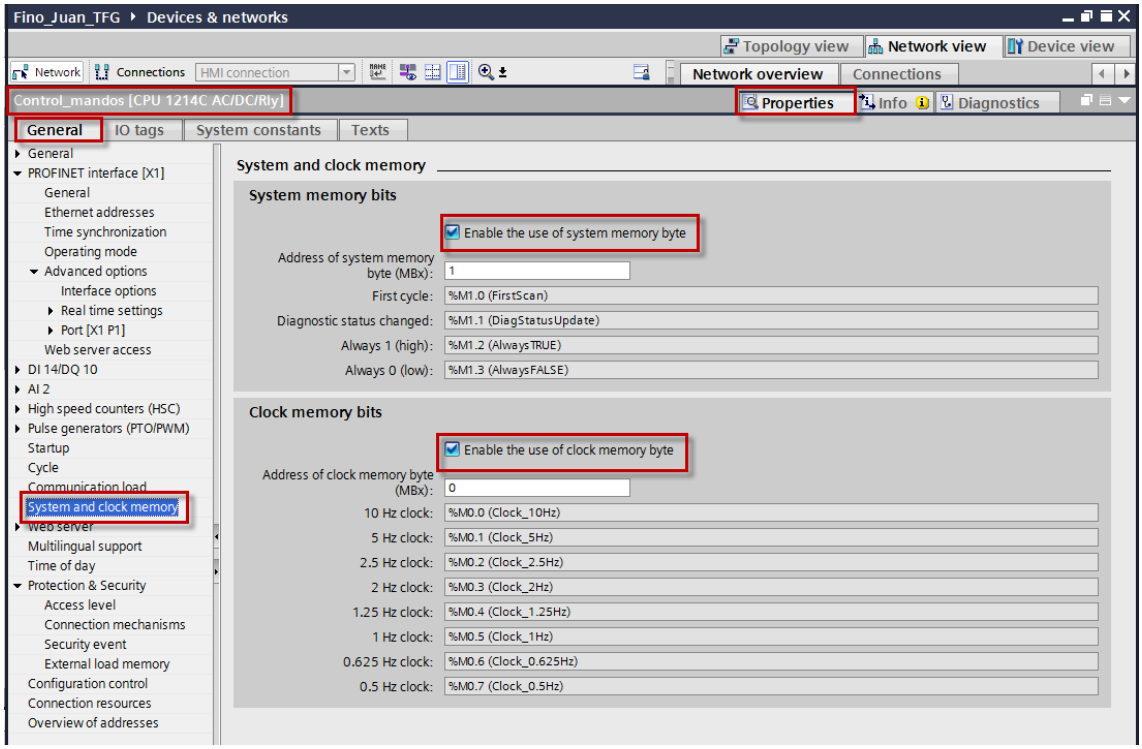


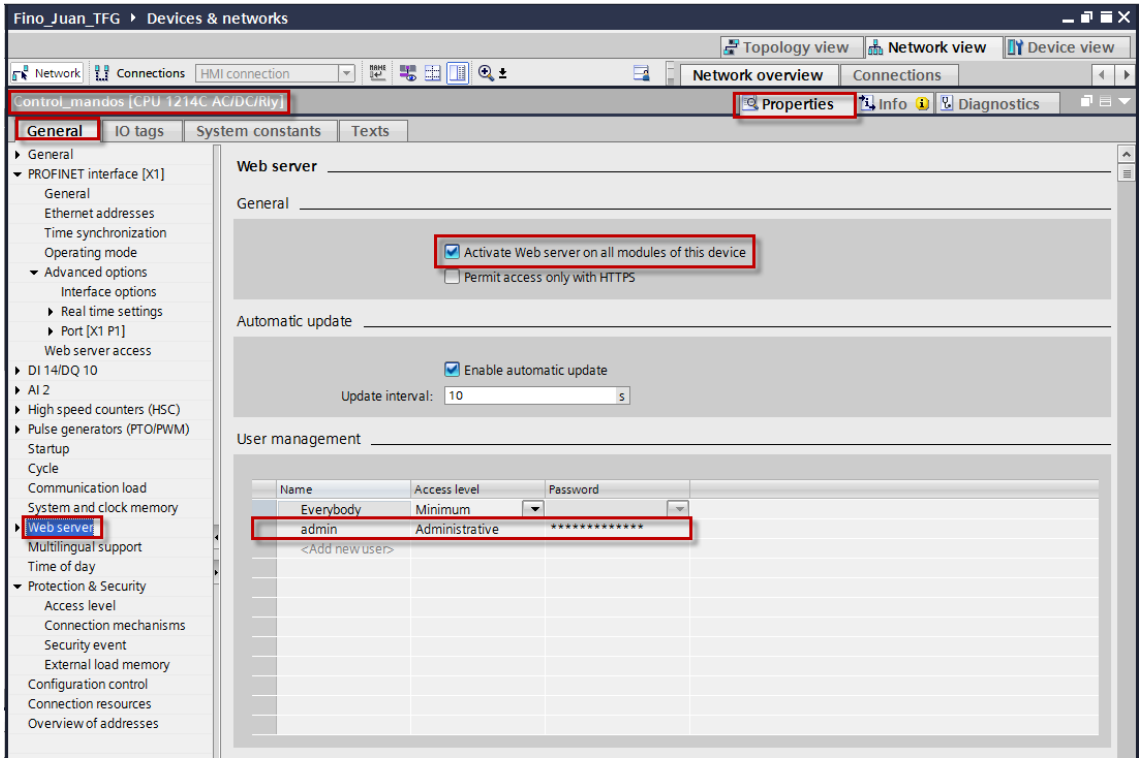
3. Una vez ya se tienen ambos PLCs añadidos cada uno a sus respectivas subredes, se procede a la configuración del S7-1214C AC/DC/RLY asignado con nombre “Control_mandos”. No se explicará una a una cada captura de la configuración de “Control_mandos” del proyecto, pero se recuadra en rojo las partes más importantes configuradas en cada apartado.

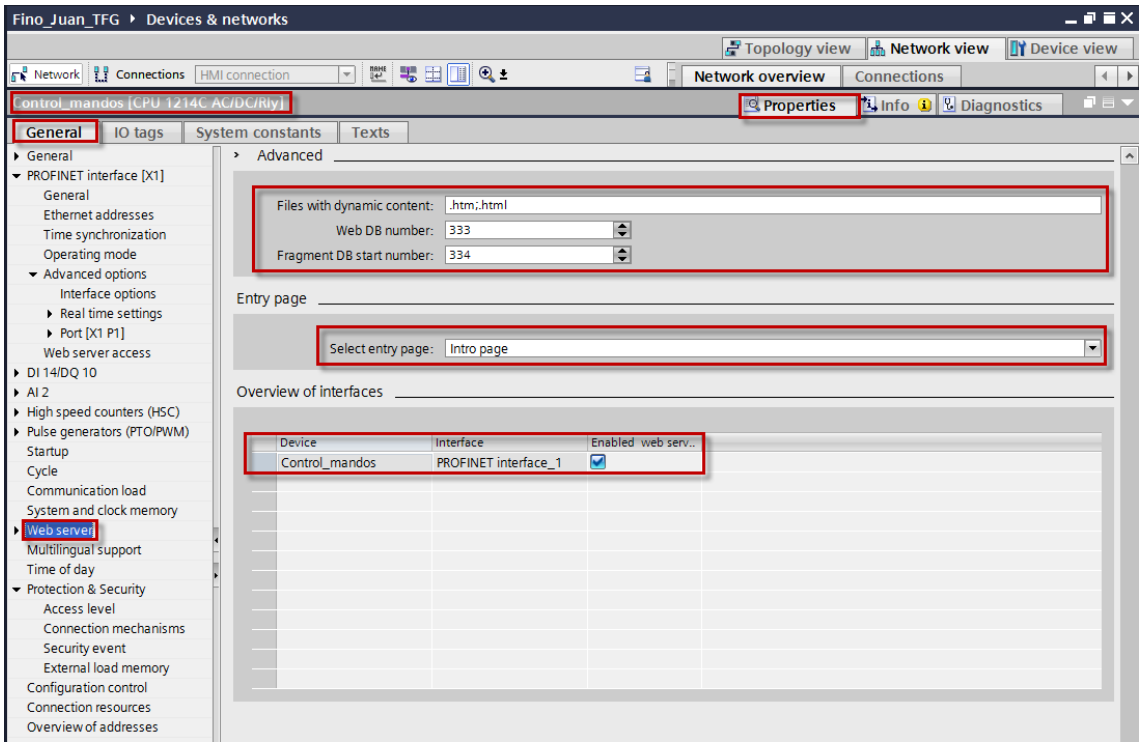


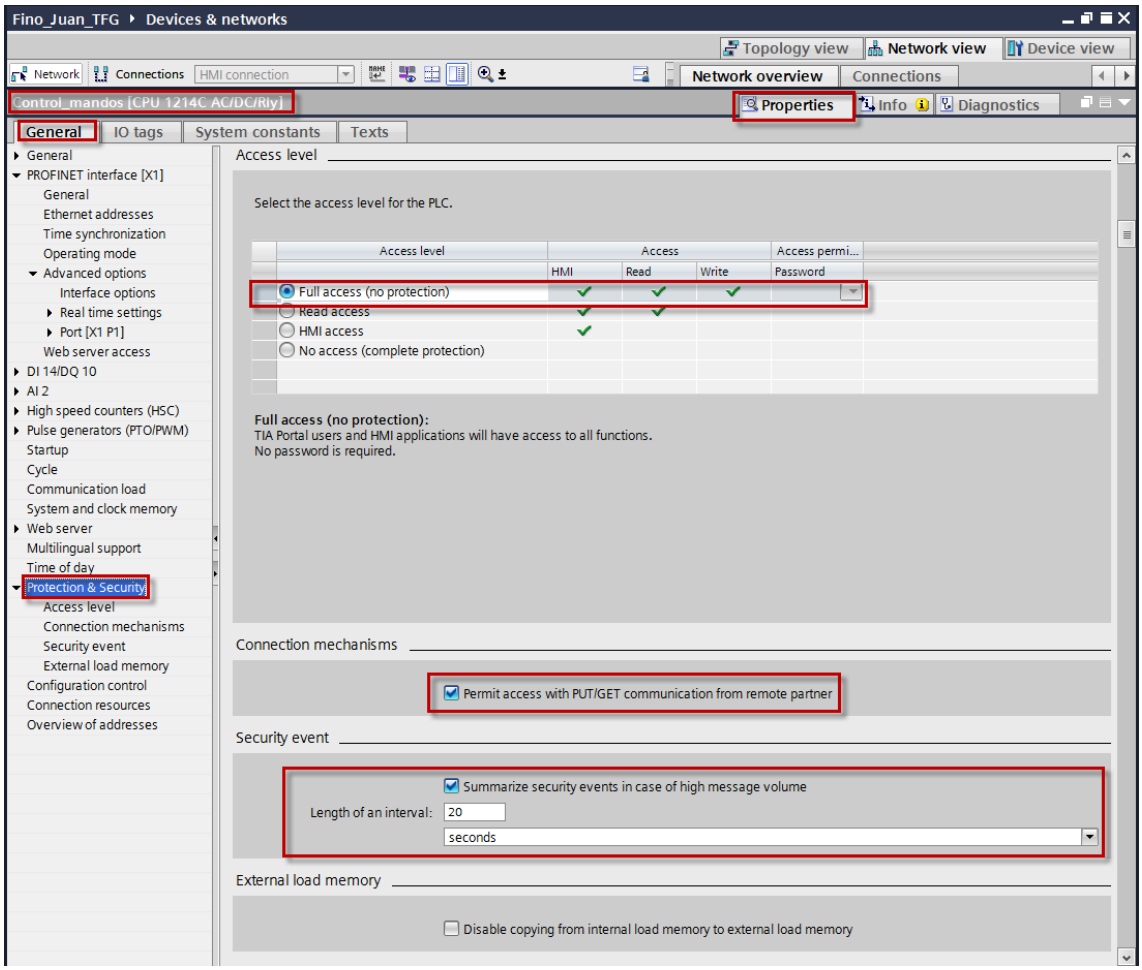



Fino_Juan_TFG ▸ Devices & networks
Topology view
Network view
Device view
Network
Connections
HMI connection
Network overview
Connections
Control_mandos [CPU 1214C AC/DC/Rly]
Properties
Info
Diagnostics
General
IO tags
System constants
Texts
General
PROFINET interface [X1]
General
Ethernet addresses
Time synchronization
Operating mode
Advanced options
Interface options
Real time settings
Port [X1 P1]
Web server access
DI 14/DQ 10
AI 2
High speed counters (HSC)
Pulse generators (PTO/PWM)
Startup
Cycle
Communication load
System and clock memory
Web server
Multilingual support
Time of day
Protection & Security
Access level
Connection mechanisms
Security event
External load memory
Configuration control
Connection resources
Overview of addresses
Web server access
Enable Web server using this interface
The Web server must also be activated in the properties of the PLC.

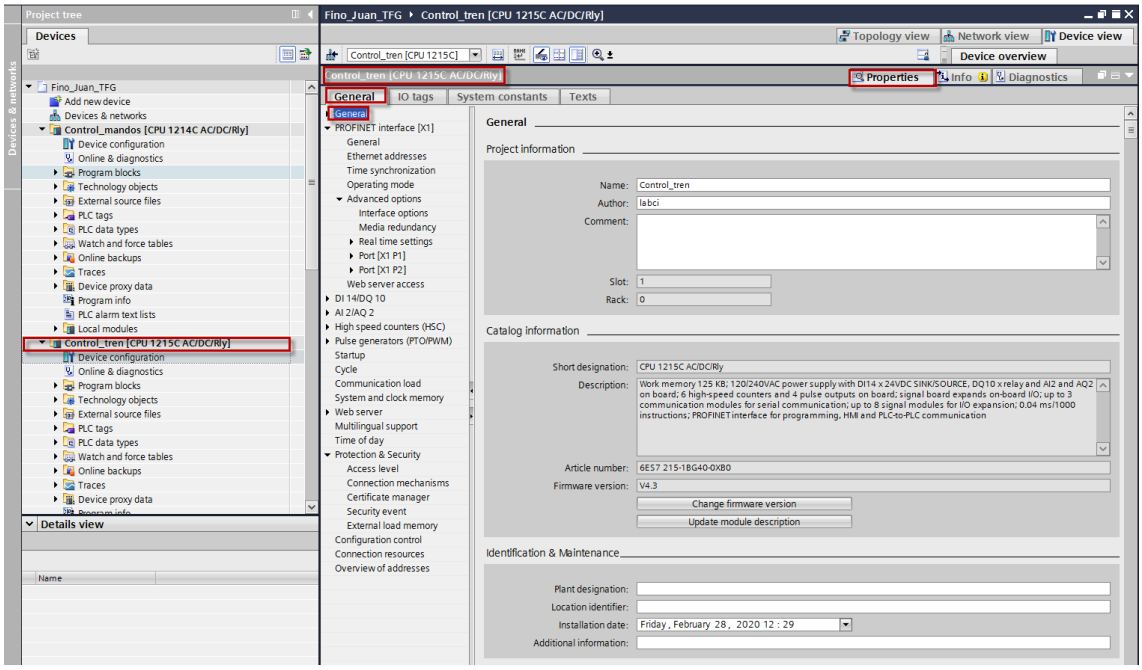

Fino_Juan_TFG ▸ Devices & networks
Topology view
Network view
Device view
Network
Connections
HMI connection
Network overview
Connections
Control_mandos [CPU 1214C AC/DC/Rly]
Properties
Info
Diagnostics
General
IO tags
System constants
Texts
General
PROFINET interface [X1]
General
Ethernet addresses
Time synchronization
Operating mode
Advanced options
Interface options
Real time settings
Port [X1 P1]
Web server access
DI 14/DQ 10
AI 2
High speed counters (HSC)
Pulse generators (PTO/PWM)
Startup
Cycle
Communication load
System and clock memory
Web server
Multilingual support
Time of day
Protection & Security
Access level
Connection mechanisms
Security event
External load memory
Configuration control
Connection resources
Overview of addresses
System and clock memory
System memory bits
Enable the use of system memory byte
Address of system memory byte (MBx): 1
First cycle: %M1.0 (FirstScan)
Diagnostic status changed: %M1.1 (DiagStatusUpdate)
Always 1 (high): %M1.2 (AlwaysTRUE)
Always 0 (low): %M1.3 (AlwaysFALSE)
Clock memory bits
Enable the use of clock memory byte
Address of clock memory byte (MBx): 0
10 Hz clock: %M0.0 (Clock_10Hz)
5 Hz clock: %M0.1 (Clock_5Hz)
2.5 Hz clock: %M0.2 (Clock_2.5Hz)
2 Hz clock: %M0.3 (Clock_2Hz)
1.25 Hz clock: %M0.4 (Clock_1.25Hz)
1 Hz clock: %M0.5 (Clock_1Hz)
0.625 Hz clock: %M0.6 (Clock_0.625Hz)
0.5 Hz clock: %M0.7 (Clock_0.5Hz)

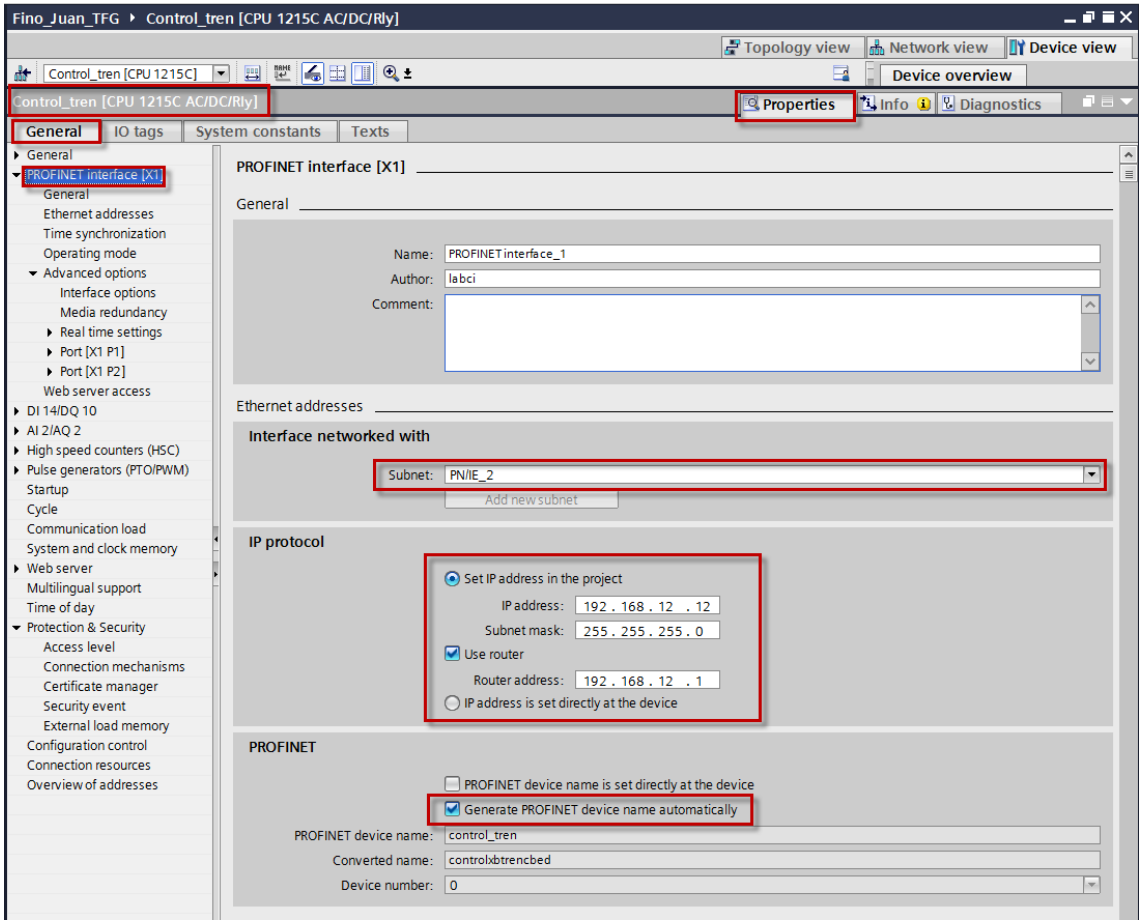

Fino_Juan_TFG ▸ Devices & networks
Topology view
Network view
Device view
Network
Connections
HMI connection
Network overview
Connections
Control_mandos [CPU 1214C AC/DC/Rly]
Properties
Info
Diagnostics
General
IO tags
System constants
Texts
General
PROFINET interface [X1]
General
Ethernet addresses
Time synchronization
Operating mode
Advanced options
Interface options
Real time settings
Port [X1 P1]
Web server access
DI 14/DQ 10
AI 2
High speed counters (HSC)
Pulse generators (PTO/PWM)
Startup
Cycle
Communication load
System and clock memory
Web server
Multilingual support
Time of day
Protection & Security
Access level
Connection mechanisms
Security event
External load memory
Configuration control
Connection resources
Overview of addresses
Web server
General
Activate Web server on all modules of this device
Permit access only with HTTPS
Automatic update
Enable automatic update
Update interval:
10
s
User management
Name
Access level
Password
Everybody
Minimum
admin
Administrative
****
<Add new user>

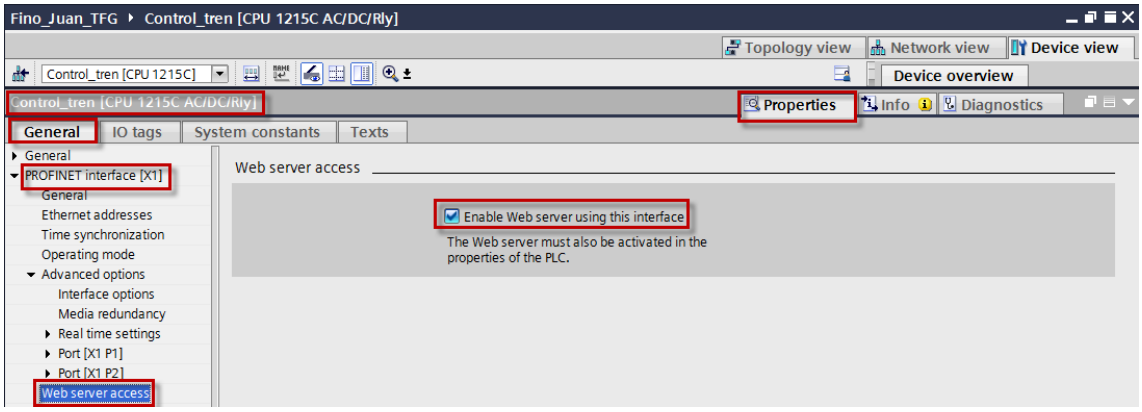

Fino_Juan_TFG ▸ Devices & networks
Topology view
Network view
Device view
Network
Connections
HMI connection
Network overview
Connections
Control_mandos [CPU 1214C AC/DC/Rly]
Properties
Info
Diagnostics
General
IO tags
System constants
Texts
General
PROFINET interface [X1]
General
Ethernet addresses
Time synchronization
Operating mode
Advanced options
Interface options
Real time settings
Port [X1 P1]
Web server access
DI 14/DQ 10
AI 2
High speed counters (HSC)
Pulse generators (PTO/PWM)
Startup
Cycle
Communication load
System and clock memory
Web server
Multilingual support
Time of day
Protection & Security
Access level
Connection mechanisms
Security event
External load memory
Configuration control
Connection resources
Overview of addresses
Advanced
Files with dynamic content:
.htm;.html
Web DB number:
333
Fragment DB start number:
334
Entry page
Select entry page:
Intro page
Overview of interfaces
Device
Interface
Enabled web serv..
Control_mandos
PROFINET interface_1

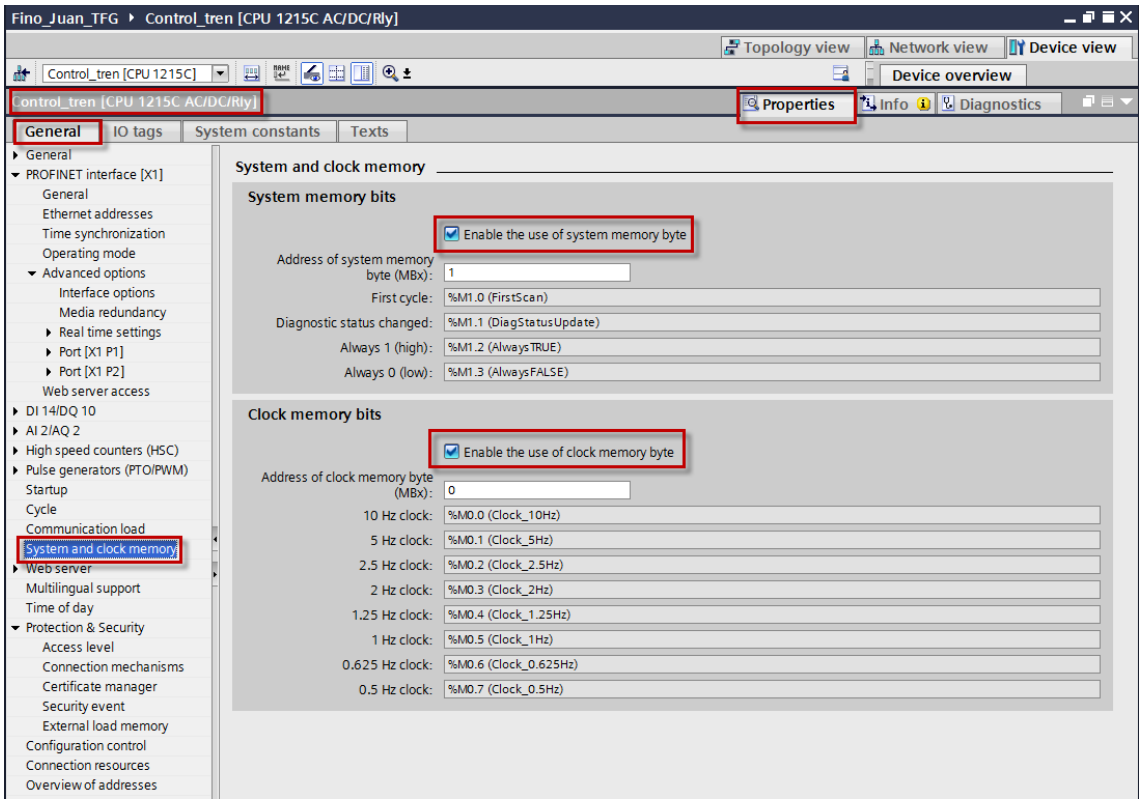


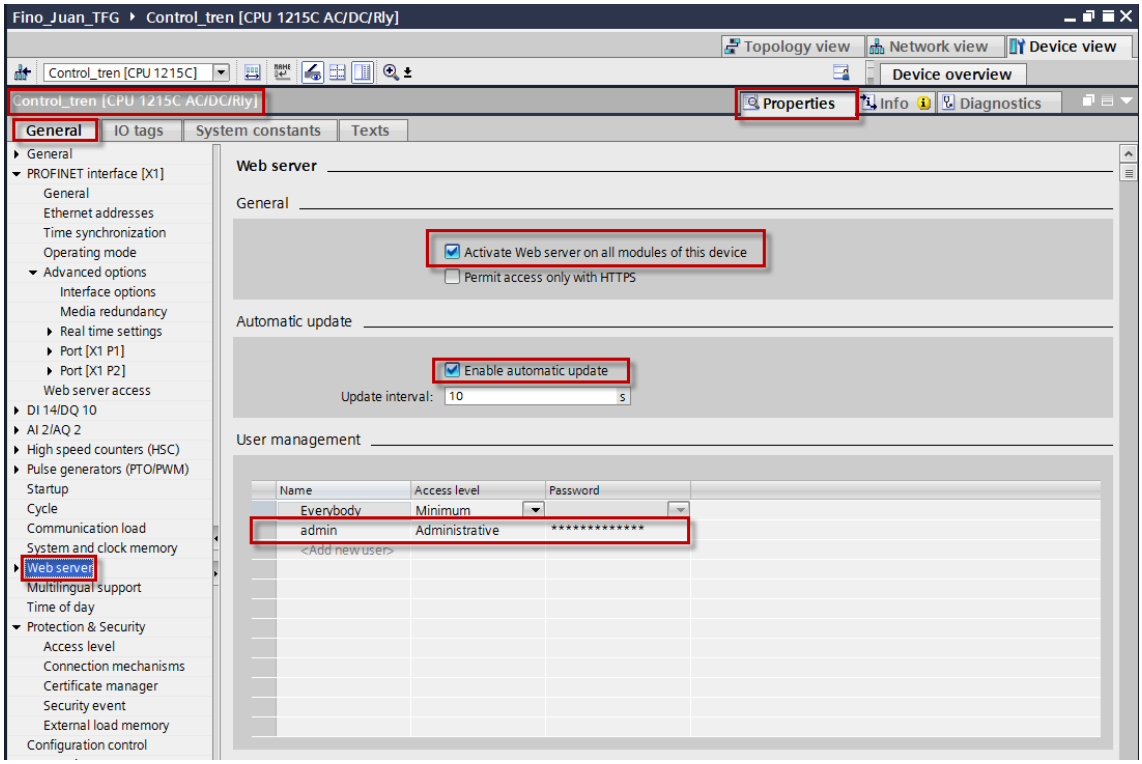
4. Una vez realizada la configuración en cuanto a parámetros se refiere, se procede ahora a realizar la configuración del S7-1215 AC/DC/RLY asignado como nombre “Control_tren”.

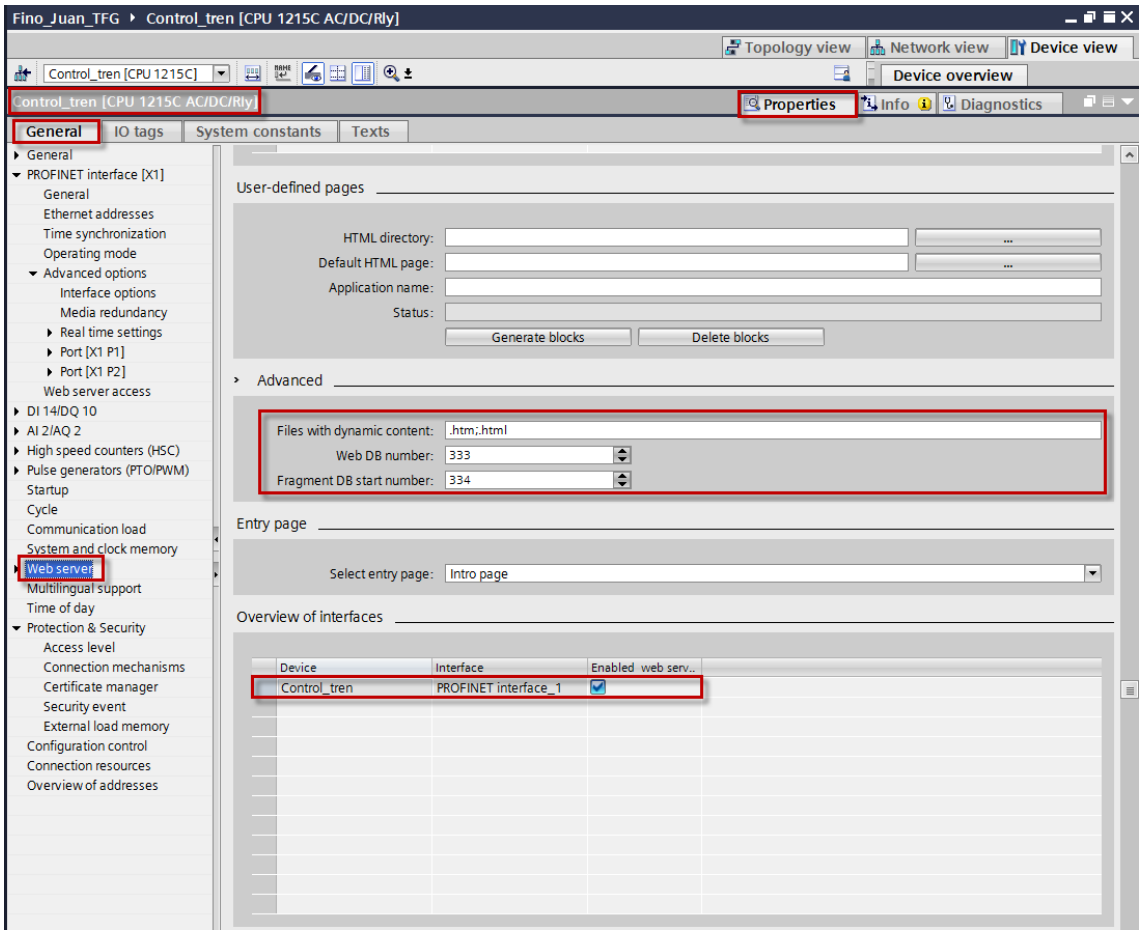


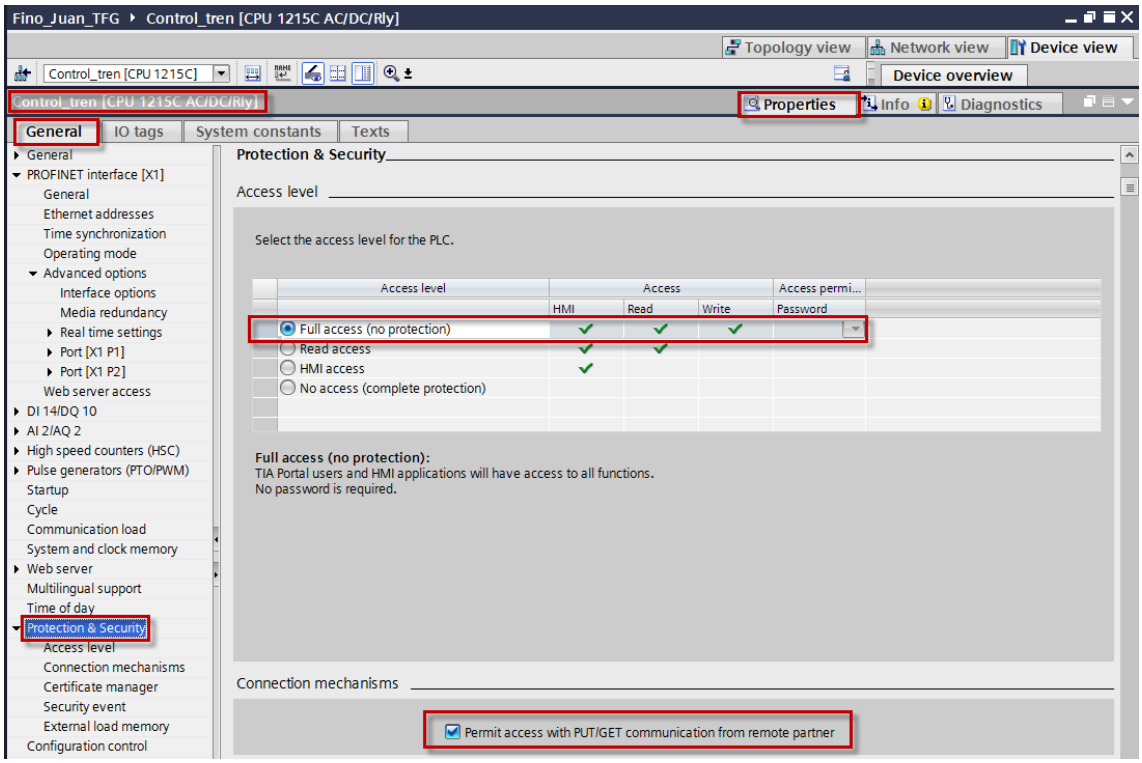

Fino_Juan_TFG ▸ Control_tren [CPU 1215C AC/DC/Rly]
Topology view
Network view
Device view
Control_tren [CPU 1215C]
Device overview
Control_tren [CPU 1215C AC/DC/Rly]
Properties
Info
Diagnostics
General
IO tags
System constants
Texts
General
PROFINET interface [X1]
General
Ethernet addresses
Time synchronization
Operating mode
Advanced options
Interface options
Media redundancy
Real time settings
Port [X1 P1]
Port [X1 P2]
Web server access
DI 14/DQ 10
AI 2/AQ 2
High speed counters (HSC)
Pulse generators (PTO/PWM)
Startup
Cycle
Communication load
System and clock memory
Web server
Multilingual support
Time of day
Protection & Security
Access level
Connection mechanisms
Certificate manager
Security event
External load memory
Configuration control
Connection resources
Overview of addresses
PROFINET interface [X1]
General
Name: PROFINET interface_1
Author: labci
Comment:
Ethernet addresses
Interface networked with
Subnet: PN/IE_2
Add new subnet
IP protocol
Set IP address in the project
IP address: 192 . 168 . 12 . 12
Subnet mask: 255 . 255 . 255 . 0
Use router
Router address: 192 . 168 . 12 . 1
IP address is set directly at the device
PROFINET
PROFINET device name is set directly at the device
Generate PROFINET device name automatically
PROFINET device name: control_tren
Converted name: controlxbtrencbed
Device number: 0


Fino_Juan_TFG ▸ Control_tren [CPU 1215C AC/DC/Rly]
Topology view
Network view
Device view
Control_tren [CPU 1215C]
Device overview
Control_tren [CPU 1215C AC/DC/Rly]
Properties
Info
Diagnostics
General
IO tags
System constants
Texts
General
PROFINET interface [X1]
General
Ethernet addresses
Time synchronization
Operating mode
Advanced options
Interface options
Media redundancy
Real time settings
Port [X1 P1]
Port [X1 P2]
Web server access
Web server access
Enable Web server using this interface
The Web server must also be activated in the properties of the PLC.

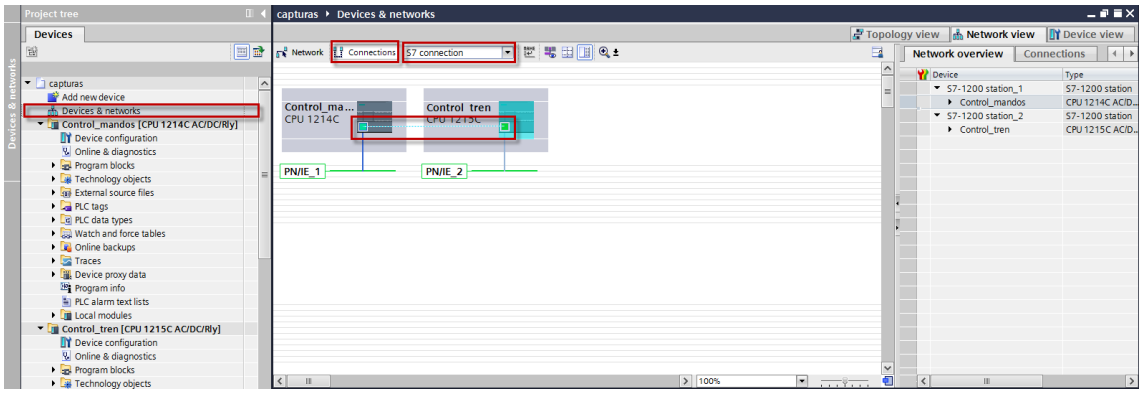

Fino_Juan_TFG ▸ Control_tren [CPU 1215C AC/DC/Rly]
Topology view
Network view
Device view
Control_tren [CPU 1215C]
Device overview
Control_tren [CPU 1215C AC/DC/Rly]
Properties
Info
Diagnostics
General
IO tags
System constants
Texts
General
PROFINET interface [X1]
General
Ethernet addresses
Time synchronization
Operating mode
Advanced options
Interface options
Media redundancy
Real time settings
Port [X1 P1]
Port [X1 P2]
Web server access
DI 14/DQ 10
AI 2/AQ 2
High speed counters (HSC)
Pulse generators (PTO/PWM)
Startup
Cycle
Communication load
System and clock memory
Web server
Multilingual support
Time of day
Protection & Security
Access level
Connection mechanisms
Certificate manager
Security event
External load memory
Configuration control
Connection resources
Overview of addresses
System and clock memory
System memory bits
Enable the use of system memory byte
Address of system memory byte (MBx):
1
First cycle:
%M1.0 (FirstScan)
Diagnostic status changed:
%M1.1 (DiagStatusUpdate)
Always 1 (high):
%M1.2 (AlwaysTRUE)
Always 0 (low):
%M1.3 (AlwaysFALSE)
Clock memory bits
Enable the use of clock memory byte
Address of clock memory byte (MBx):
0
10 Hz clock:
%M0.0 (Clock_10Hz)
5 Hz clock:
%M0.1 (Clock_5Hz)
2.5 Hz clock:
%M0.2 (Clock_2.5Hz)
2 Hz clock:
%M0.3 (Clock_2Hz)
1.25 Hz clock:
%M0.4 (Clock_1.25Hz)
1 Hz clock:
%M0.5 (Clock_1Hz)
0.625 Hz clock:
%M0.6 (Clock_0.625Hz)
0.5 Hz clock:
%M0.7 (Clock_0.5Hz)

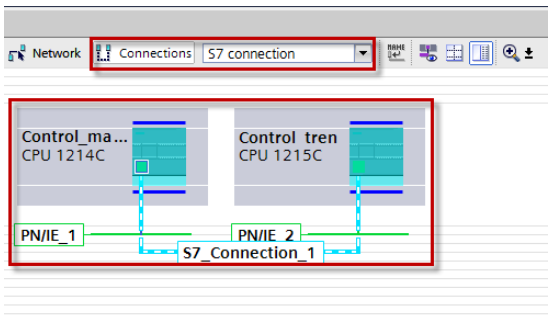

Fino_Juan_TFG ▸ Control_tren [CPU 1215C AC/DC/Rly]
Topology view
Network view
Device view
Control_tren [CPU 1215C]
Device overview
Control_tren [CPU 1215C AC/DC/Rly]
Properties
Info
Diagnostics
General
IO tags
System constants
Texts
General
PROFINET interface [X1]
General
Ethernet addresses
Time synchronization
Operating mode
Advanced options
Interface options
Media redundancy
Real time settings
Port [X1 P1]
Port [X1 P2]
Web server access
DI 14/DQ 10
AI 2/AQ 2
High speed counters (HSC)
Pulse generators (PTO/PWM)
Startup
Cycle
Communication load
System and clock memory
Web server
Multilingual support
Time of day
Protection & Security
Access level
Connection mechanisms
Certificate manager
Security event
External load memory
Configuration control
Web server
General
Activate Web server on all modules of this device
Permit access only with HTTPS
Automatic update
Enable automatic update
Update interval:
10
s
User management
Name
Access level
Password
Everybody
Minimum
admin
Administrative
****
<Add new user>

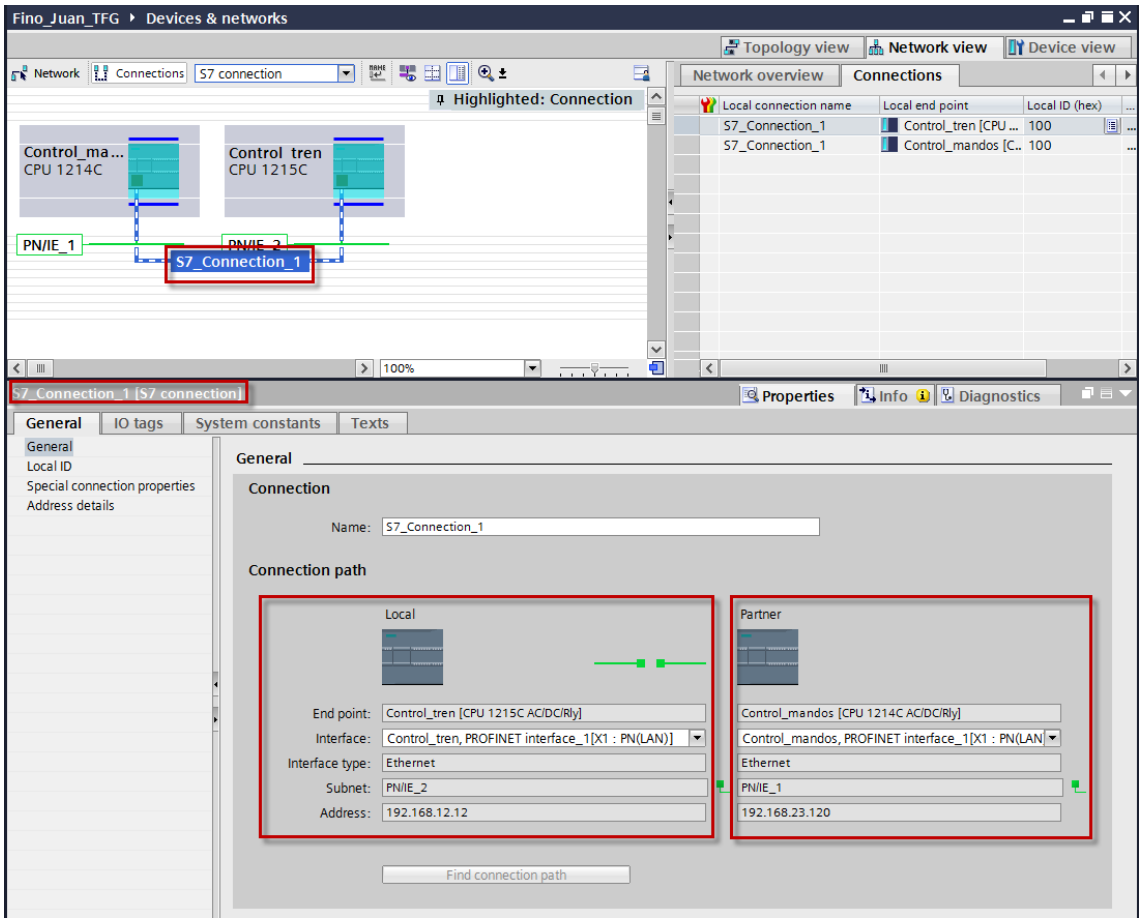

Fino_Juan_TFG ▸ Control_tren [CPU 1215C AC/DC/Rly]
Topology view
Network view
Device view
Control_tren [CPU 1215C]
Device overview
Control_tren [CPU 1215C AC/DC/Rly]
Properties
Info
Diagnostics
General
IO tags
System constants
Texts
General
PROFINET interface [X1]
General
Ethernet addresses
Time synchronization
Operating mode
Advanced options
Interface options
Media redundancy
Real time settings
Port [X1 P1]
Port [X1 P2]
Web server access
DI 14/DQ 10
AI 2/AQ 2
High speed counters (HSC)
Pulse generators (PTO/PWM)
Startup
Cycle
Communication load
System and clock memory
Web server
Multilingual support
Time of day
Protection & Security
Access level
Connection mechanisms
Certificate manager
Security event
External load memory
Configuration control
Connection resources
Overview of addresses
User-defined pages
HTML directory:
Default HTML page:
Application name:
Status:
Generate blocks
Delete blocks
Advanced
Files with dynamic content:
.htm;.html
Web DB number:
333
Fragment DB start number:
334
Entry page
Select entry page:
Intro page
Overview of interfaces
Device
Interface
Enabled web serv..
Control_tren
PROFINET interface_1

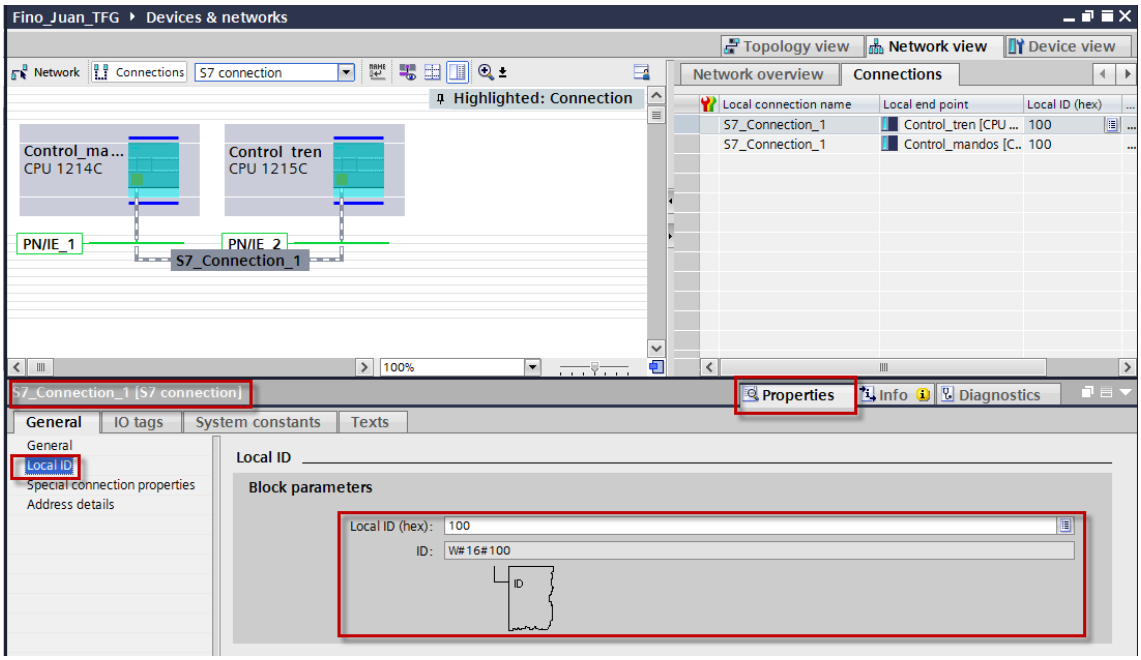

Fino_Juan_TFG ▸ Control_tren [CPU 1215C AC/DC/Rly]
Topology view
Network view
Device view
Control_tren [CPU 1215C]
Device overview
Control_tren [CPU 1215C AC/DC/Rly]
Properties
Info
Diagnostics
General
IO tags
System constants
Texts
Protection & Security
Access level
Select the access level for the PLC.
Access level
Access
Access permi...
HMI
Read
Write
Password
Full access (no protection)
Read access
HMI access
No access (complete protection)
Full access (no protection):
TIA Portal users and HMI applications will have access to all functions.
No password is required.
Connection mechanisms
Permit access with PUT/GET communication from remote partner

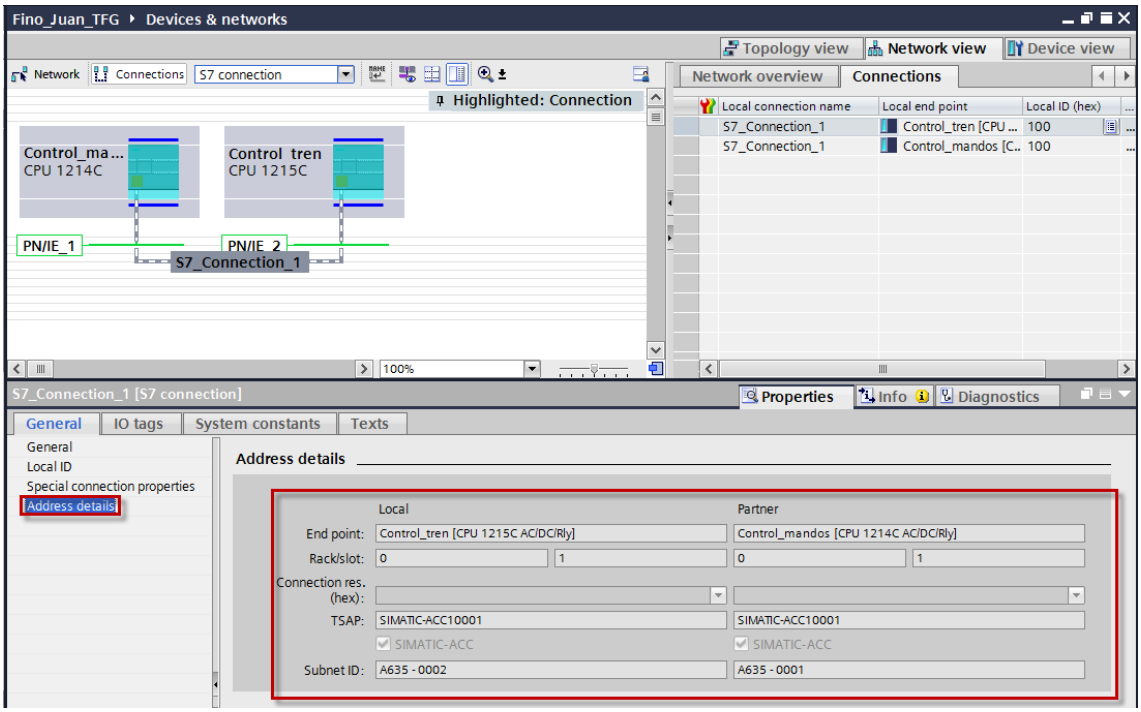
5. Con ambos PLCs ya configurados, se realiza la configuración de la comunicación S7 entre ambos PLCs, como antes se ha mencionado, los recuadros rojos indican la parametrizaión mas importante en cada captura del proyecto.

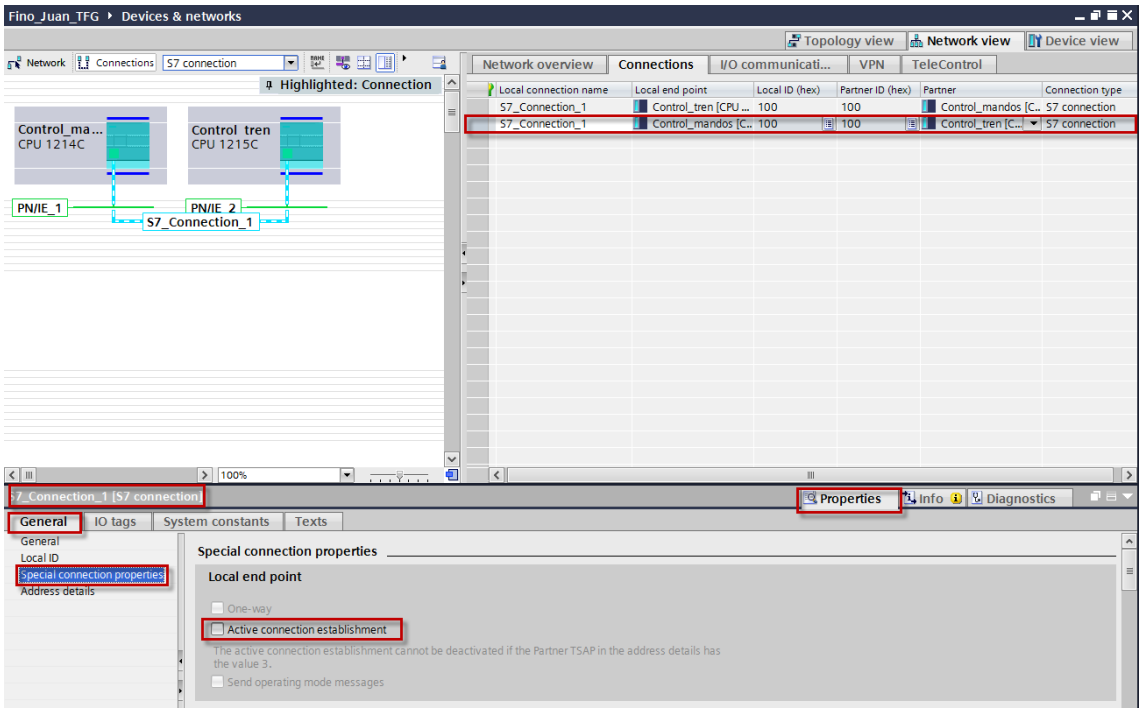


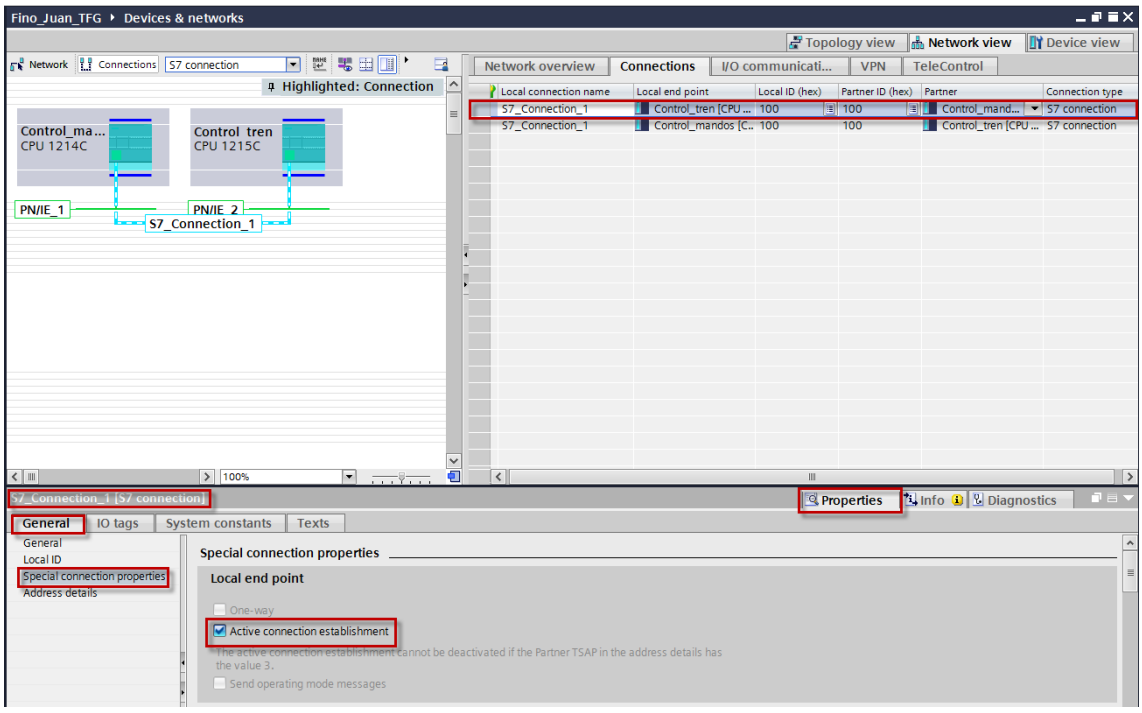


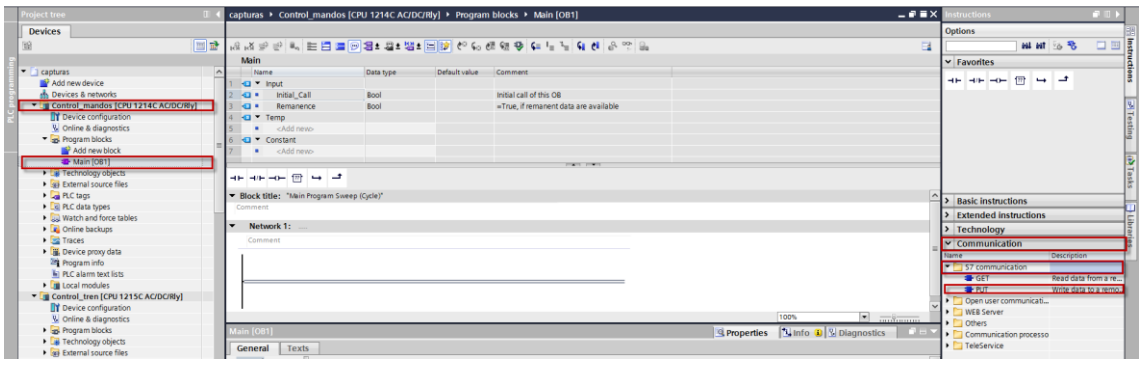



Fino_Juan_TFG ▸ Devices & networks
Topology view
Network view
Device view
Network
Connections
S7 connection
Highlighted: Connection
Network overview
Connections
Local connection name
Local end point
Local ID (hex)
S7_Connection_1
Control_tren [CPU ...
100
Control_mandos [C...
Control_ma...
CPU 1214C
Control_tren
CPU 1215C
PN/IE_1
PN/IE_2
S7_Connection_1
100%
S7_Connection_1 [S7 connection]
Properties
Info
Diagnostics
General
IO tags
System constants
Texts
General
Local ID
Special connection properties
Address details
Local ID
Block parameters
Local ID (hex):
100
ID:
W#16#100
ID

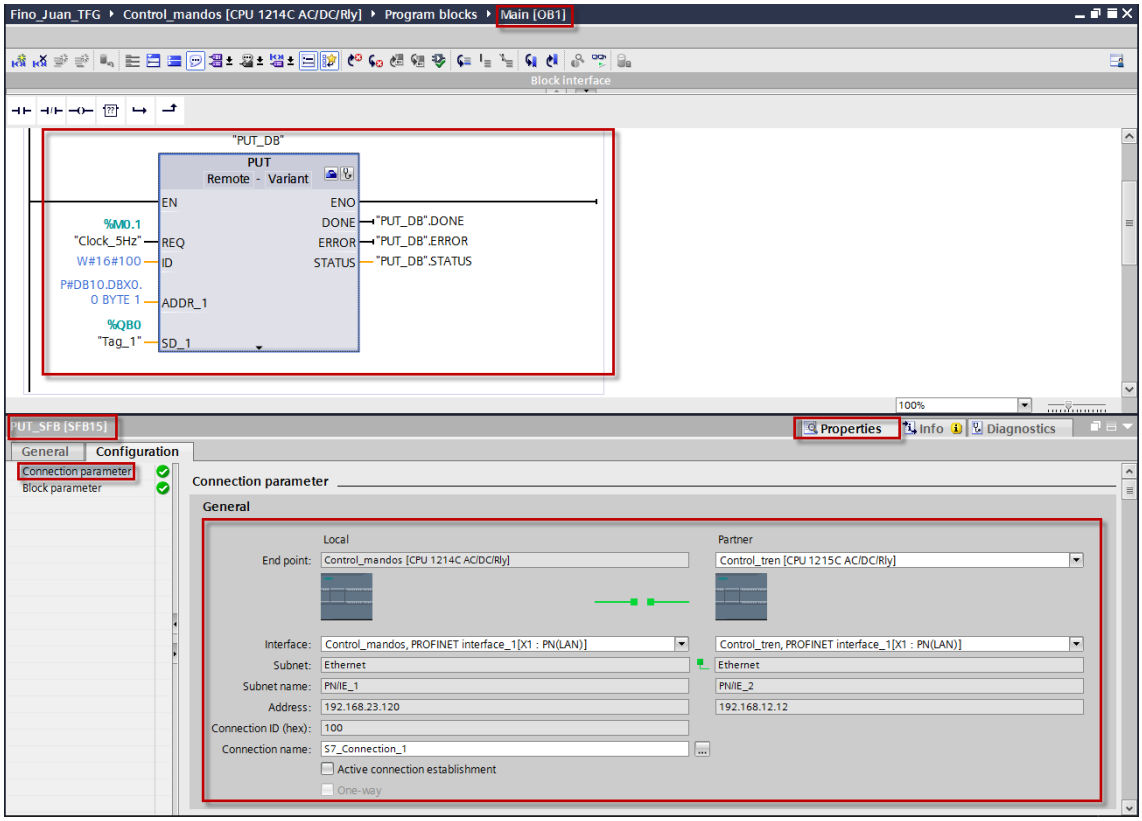

Fino_Juan_TFG ▸ Devices & networks
Topology view
Network view
Device view
Network
Connections
S7 connection
Highlighted: Connection
Network overview
Connections
Local connection name
Local end point
Local ID (hex)
S7_Connection_1
Control_tren [CPU ...
100
Control_mandos [C...
Control_ma...
CPU 1214C
Control_tren
CPU 1215C
PN/IE_1
PN/IE_2
S7_Connection_1
100%
S7_Connection_1 [S7 connection]
Properties
Info
Diagnostics
General
IO tags
System constants
Texts
General
Local ID
Special connection properties
Address details
Address details
Local
Partner
End point:
Control_tren [CPU 1215C AC/DC/Rly]
Control_mandos [CPU 1214C AC/DC/Rly]
Rack/slot:
0
1
0
1
Connection res. (hex):
TSAP:
SIMATIC-ACC10001
SIMATIC-ACC10001
SIMATIC-ACC
SIMATIC-ACC
Subnet ID:
A635 - 0002
A635 - 0001

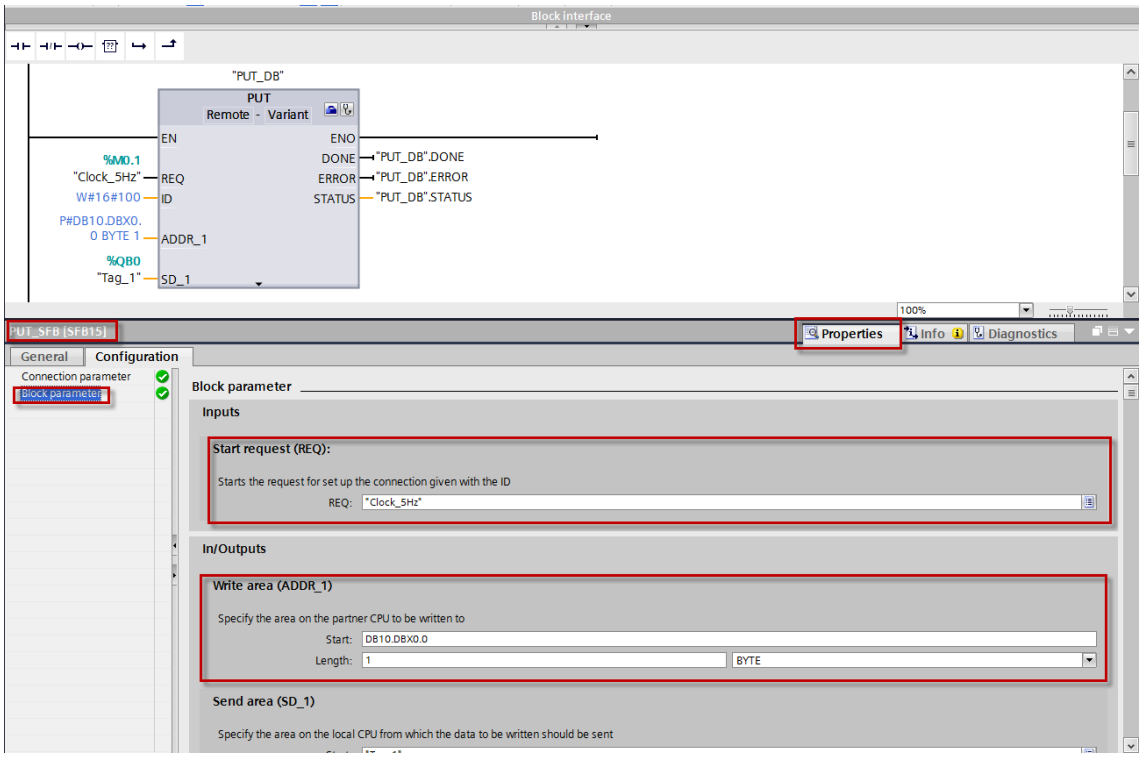

Fino_Juan_TFG ▸ Devices & networks
Topology view
Network view
Device view
Network
Connections
S7 connection
Highlighted: Connection
Network overview
Connections
I/O communicati...
VPN
TeleControl
Local connection name
Local end point
Local ID (hex)
Partner ID (hex)
Partner
Connection type
S7_Connection_1
Control_tren [CPU ...
100
Control_mandos [C...
S7 connection
Control_ma...
CPU 1214C
Control_tren
CPU 1215C
PN/IE_1
PN/IE_2
S7_Connection_1
100%
S7_Connection_1 [S7 connection]
Properties
Info
Diagnostics
General
IO tags
System constants
Texts
General
Local ID
Special connection properties
Address details
Special connection properties
Local end point
One-way
Active connection establishment
The active connection establishment cannot be deactivated if the Partner TSAP in the address details has the value 3.
Send operating mode messages

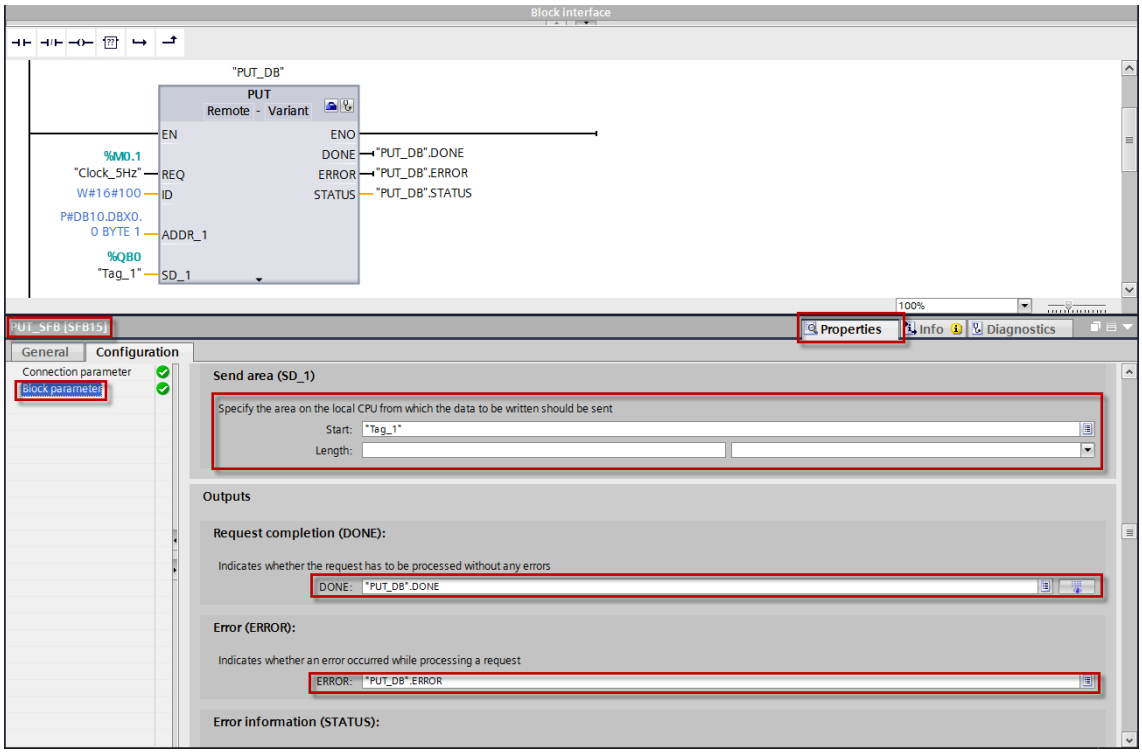

Fino_Juan_TFG ▸ Devices & networks
Topology view
Network view
Device view
Network
Connections
S7 connection
Highlighted: Connection
Network overview
Connections
I/O communicati...
VPN
TeleControl
Local connection name
Local end point
Local ID (hex)
Partner ID (hex)
Partner
Connection type
S7_Connection_1
Control_tren [CPU ...
100
Control_mandos [C...
S7 connection
Control_ma...
CPU 1214C
Control_tren
CPU 1215C
PN/IE_1
PN/IE_2
S7_Connection_1
100%
S7_Connection_1 [S7 connection]
Properties
Info
Diagnostics
General
IO tags
System constants
Texts
General
Local ID
Special connection properties
Address details
Special connection properties
Local end point
One-way
Active connection establishment
The active connection establishment cannot be deactivated if the Partner TSAP in the address details has the value 3.
Send operating mode messages

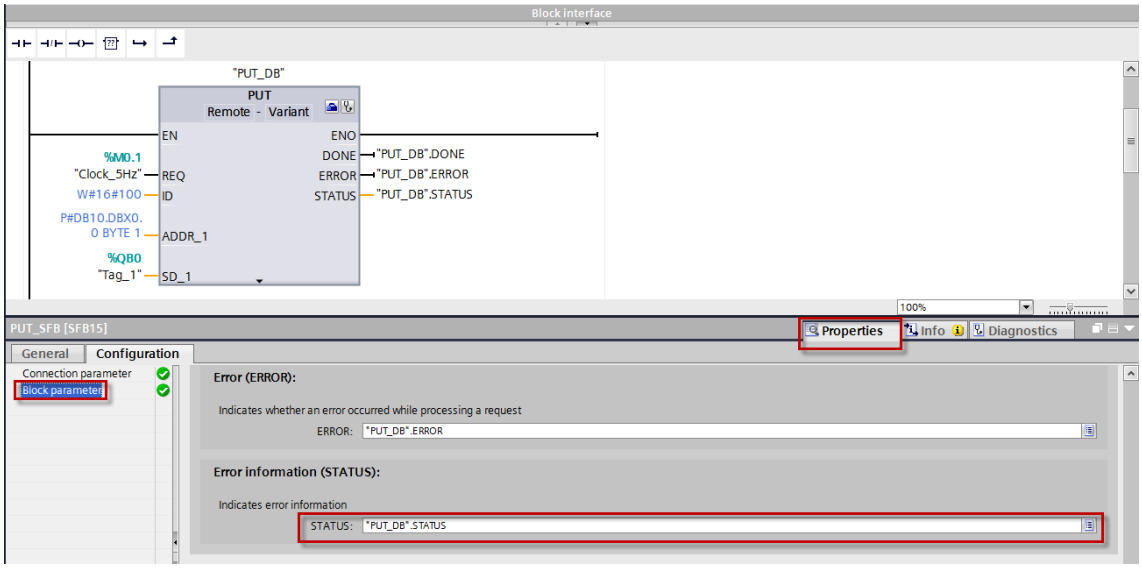

Project tree
Devices
capturas
Control_mandos [CPU 1214C AC/DC/Rly] ▸ Program blocks ▸ Main [OB1]
Main
Name
Data type
Default value
Comment
Input
Initial_Call
Bool
Initial call of this OB
Remanence
Bool
=True, if remanent data are available
Temp
Constant
Block title: "Main Program Sweep (Cycle)"
Network 1:
Instructions
Options
Favorites
Basic instructions
Extended instructions
Technology
Communication
S7 communication
Open user communicati...
WEB Server
Others
Communication processo
TeleService
Main [OB1]
Properties
Info
Diagnostics
General
Texts

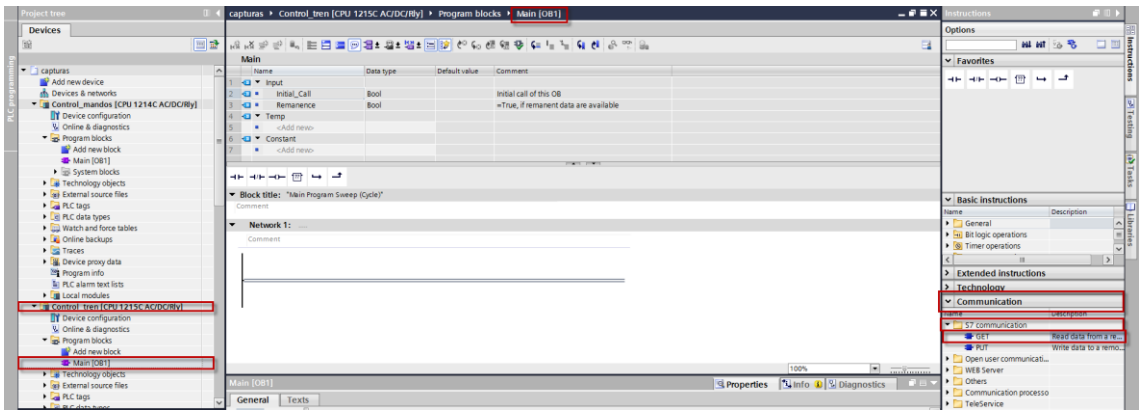
6. Con la configuración S7 parametrizada correctamente, indicando cuál de los dos será el pasivo de la comunicación y cual el activo, quedaría la programación de los bloques GET/PUT cada uno para el “Control_tren” y el “Control_mandos, respectivamente.

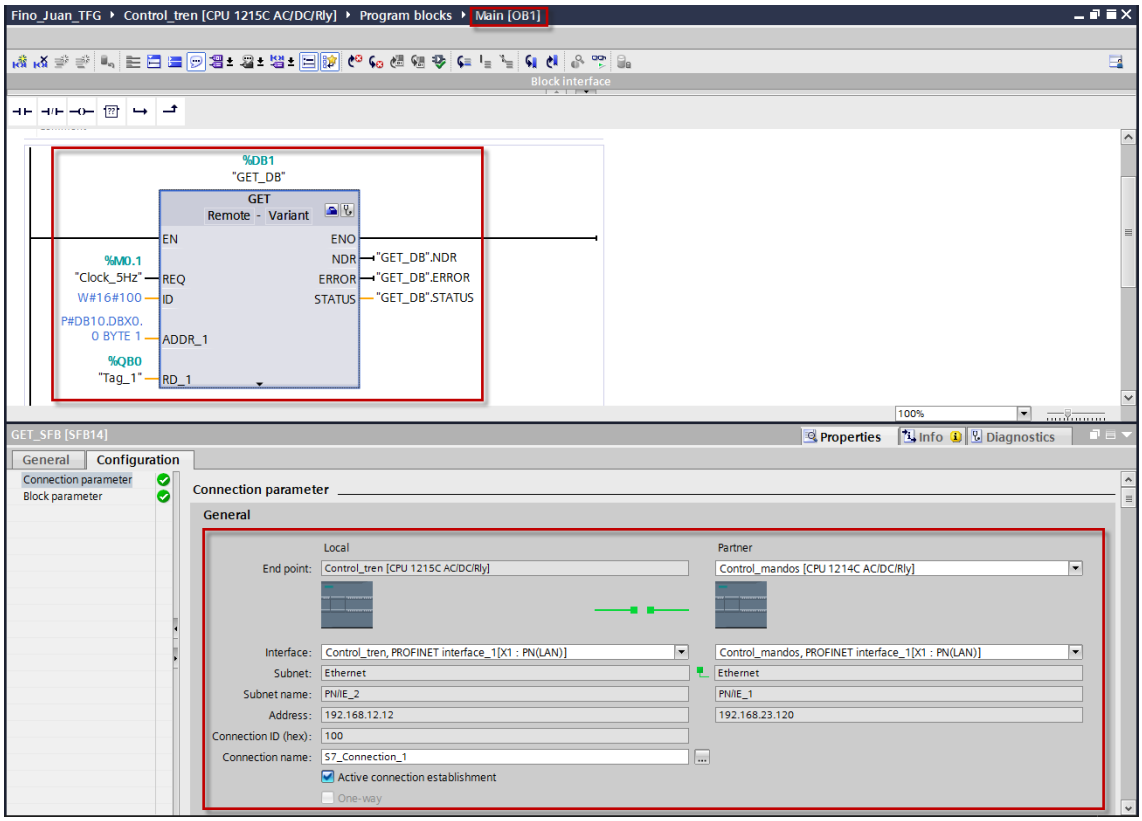


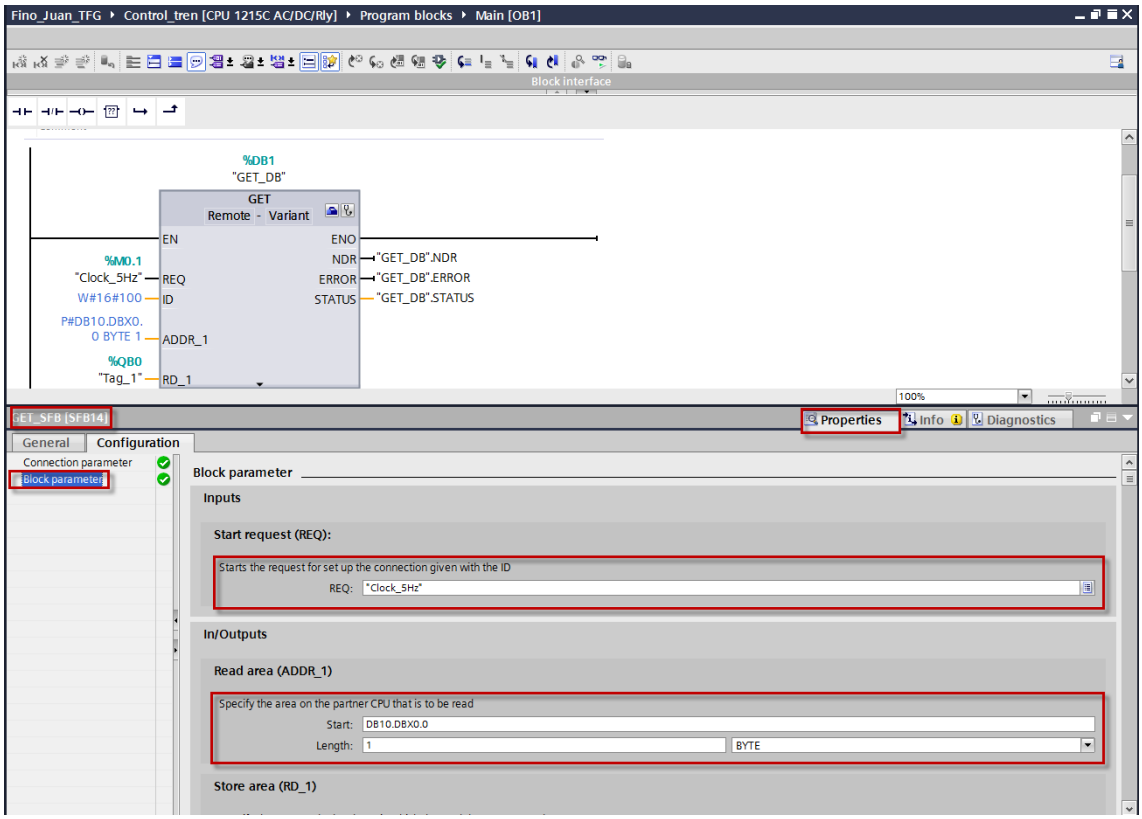



Block interface
"PUT_DB"
PUT
Remote - Variant
EN
ENO
%M0.1
"Clock_5Hz"
REQ
DONE
"PUT_DB".DONE
ERROR
"PUT_DB".ERROR
W#16#100
ID
STATUS
"PUT_DB".STATUS
P#DB10.DBX0.
0 BYTE 1
ADDR_1
%QB0
"Tag_1"
SD_1
100%
PUT_SFB [SFB15]
Properties
Info
Diagnostics
General
Configuration
Connection parameter
Block parameter
Send area (SD_1)
Specify the area on the local CPU from which the data to be written should be sent
Start:
"Tag_1"
Length:
Outputs
Request completion (DONE):
Indicates whether the request has to be processed without any errors
DONE:
"PUT_DB".DONE
Error (ERROR):
Indicates whether an error occurred while processing a request
ERROR:
"PUT_DB".ERROR
Error information (STATUS):


Block interface
"PUT_DB"
PUT
Remote - Variant
EN
ENO
%M0.1
"Clock_5Hz"
REQ
DONE
"PUT_DB".DONE
ERROR
"PUT_DB".ERROR
W#16#100
ID
STATUS
"PUT_DB".STATUS
P#DB10.DBX0.
0 BYTE 1
ADDR_1
%QB0
"Tag_1"
SD_1
100%
PUT_SFB [SFB15]
Properties
Info
Diagnostics
General
Configuration
Connection parameter
Block parameter
Error (ERROR):
Indicates whether an error occurred while processing a request
ERROR:
"PUT_DB".ERROR
Error information (STATUS):
Indicates error information
STATUS:
"PUT_DB".STATUS


Project tree
Devices
capturas
Control_tren [CPU 1215C AC/DC/Rly]
Program blocks
Main [OB1]
Main
Block title: "Main Program Sweep (Cycle)"
Network 1:
Instructions
Basic instructions
Extended instructions
Communication
S7 communication
Properties
Info
Diagnostics
General
Texts


Fino_Juan_TFG ▸ Control_tren [CPU 1215C AC/DC/Rly] ▸ Program blocks ▸ Main [OB1]
Block interface
%DB1
"GET_DB"
GET
Remote - Variant
EN
ENO
%M0.1
"Clock_5Hz"
REQ
NDR
"GET_DB".NDR
ERROR
"GET_DB".ERROR
W#16#100
ID
STATUS
"GET_DB".STATUS
P#DB10.DBX0.
0 BYTE 1
ADDR_1
%QB0
"Tag_1"
RD_1
100%
GET_SFB [SFB14]
Properties
Info
Diagnostics
General
Configuration
Connection parameter
Block parameter
Connection parameter
General
Local
Partner
End point:
Control_tren [CPU 1215C AC/DC/Rly]
Control_mandos [CPU 1214C AC/DC/Rly]
Interface:
Control_tren, PROFINET interface_1[X1 : PN(LAN)]
Control_mandos, PROFINET interface_1[X1 : PN(LAN)]
Subnet:
Ethernet
Ethernet
Subnet name:
PN/IE_2
PN/IE_1
Address:
192.168.12.12
192.168.23.120
Connection ID (hex):
100
Connection name:
S7_Connection_1
Active connection establishment
One-way


Fino_Juan_TFG ▸ Control_tren [CPU 1215C AC/DC/Rly] ▸ Program blocks ▸ Main [OB1]
Block interface
%DB1
"GET_DB"
GET
Remote - Variant
EN
ENO
%M0.1
"Clock_5Hz"
REQ
NDR
"GET_DB".NDR
ERROR
"GET_DB".ERROR
W#16#100
ID
STATUS
"GET_DB".STATUS
P#DB10.DBX0.
0 BYTE 1
ADDR_1
%QB0
"Tag_1"
RD_1
100%
GET_SFB [SFB14]
Properties
Info
Diagnostics
General
Configuration
Connection parameter
Block parameter
Block parameter
Inputs
Start request (REQ):
Starts the request for set up the connection given with the ID
REQ:
"Clock_5Hz"
In/Outputs
Read area (ADDR_1)
Specify the area on the partner CPU that is to be read
Start:
DB10.DBX0.0
Length:
1
BYTE
Store area (RD_1)