Universidad Zaragoza
1542

Trabajo Fin de Grado

Análisis e implementación de un módulo de monitorización de transmisiones de Datos de Operación en un sistema de comunicaciones críticas TETRA

Analysis and implementation of an Operation Data transmission monitoring module in a TETRA critical communications system

Autor

Daniel Gómez Blasco

Director

Juan Millán Belsué

Ponente

María Paloma García Ducar

Escuela de Ingeniería y Arquitectura

TÍTULO DEL PROYECTO

Análisis e implementación de un módulo de monitorización de transmisiones de Datos de Operación en un sistema de comunicaciones críticas TETRA.

RESUMEN

El monitoreo de los diferentes flujos de paquetes que atraviesan cualquier elemento de una red de un sistema de comunicaciones críticas es un aspecto clave a la hora de analizar el funcionamiento de un sistema. A la hora de resolver un problema en un sistema de comunicaciones críticas es imprescindible poder saber lo que está ocurriendo en cada momento, es decir, ante la aparición de posibles contratiempos, el proveedor del sistema de comunicaciones debe ser capaz de visualizar mediante una herramienta de monitoreo de datos, el origen, el destino, el tamaño y el instante de transmisión de cada paquete que atraviesa dicho sistema.

Ante la imposibilidad de poder visualizar el tráfico de paquetes de datos en un sistema de comunicaciones, se corre el riesgo de llegar a ser incapaces de poder descubrir el origen de un problema cualquiera. Es por ello por lo que en este proyecto se aborda la implementación de una herramienta de monitoreo en la red de transporte de un sistema de comunicaciones, la cual sea capaz de poder ofrecer la granularidad deseada por el proveedor a la hora de analizar el flujo de paquetes del sistema. Gracias a la implementación de este producto, el proveedor del sistema de comunicaciones podrá ser capaz de comunicar al cliente si el origen del contratiempo ha sido producido en la red de transporte suministrada al cliente, y de no ser así, comunicar al cliente que ha surgido debido a un fallo en su infraestructura.

Durante la realización de este proyecto, se plantean 3 bloques principales. El primer bloque está centrado en el análisis de todas las opciones disponibles en el mercado que permitan resolver el problema mencionado anteriormente. El segundo bloque trata sobre la verificación de la viabilidad del producto elegido en un sistema de comunicaciones para misión crítica TETRA. Por último, en el tercer bloque se llevará a cabo la configuración del módulo de monitorización (generación de gráficos y KPIs que permitan visualizar el comportamiento actual de la infraestructura), y la realización de todas las pruebas necesarias en la maqueta final de pruebas para certificar la correcta configuración e implementación llevada a cabo en el módulo de monitorización.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

1.1. CONTEXTO DEL TRABAJO

Las empresas de radiocomunicación diseñan, fabrican y despliegan equipos y sistemas de comunicaciones para misión crítica, con la innovación y la más alta calidad como objetivos. Estas empresas suministran soluciones completas de comunicaciones inalámbricas a sectores estratégicos como la seguridad pública, el transporte, la energía, la minería o el petróleo y gas.

En estos entornos, donde la disponibilidad y fiabilidad de las comunicaciones son esenciales, contar con un módulo de monitorización de datos de operación se vuelve fundamental. La capacidad de supervisar en tiempo real el rendimiento de la red, detectar anomalías y anticipar posibles fallos permite optimizar los recursos y garantizar la continuidad del servicio en condiciones críticas.

En sectores como la minería, la energía y el gas natural, donde los entornos de trabajo son altamente exigentes y cualquier interrupción en las comunicaciones puede representar un riesgo significativo, disponer de herramientas avanzadas para la gestión y análisis de datos es clave. Estos módulos permiten asegurar la continuidad operativa, mejorar la respuesta ante incidentes y optimizar el mantenimiento de la red.

Este proyecto se ha llevado a cabo en una empresa dedicada al suministro de infraestructuras de radiocomunicación para misión crítica debido a la aparición de un problema de monitorización del flujo de datos en un cliente dedicado al sector del gas natural. A petición del cliente, se ha llevado a cabo el diseño e implementación de un módulo de monitorización de Datos de Operación capaz de facilitar la optimización de la infraestructura, garantizando un mejor rendimiento a largo plazo y una gestión más eficiente de los recursos.

El desarrollo de estos módulos de monitorización no solo mejora la seguridad y la eficiencia operativa, sino que también facilita la integración con sistemas avanzados de telemetría y telecontrol, como SCADA (Supervisory Control and Data Acquisition). En la Figura 1 se puede ver un ejemplo de un Centro de Control para entornos de gas natural, el cual permite una supervisión más detallada del estado de la infraestructura, el análisis de patrones de tráfico y la toma de decisiones basada en datos en tiempo real.

Figura 1 – Interfaz Centro de Control SCADA [1]

Es por ello por lo que, antes de proseguir con diferentes aspectos del proyecto, es imprescindible conocer la infraestructura sobre la cual vamos a trabajar. Un sistema SCADA es una plataforma de software y

hardware diseñada para el almacenamiento, procesado y análisis de todos los Datos de Operación que diariamente son enviados en una red de comunicaciones para misión crítica. Su propósito principal es permitir a los operadores monitorear y gestionar las operaciones de una red o infraestructura en tiempo real, recopilando datos de dispositivos remotos y actuando sobre ellos de forma automática o manual según sea necesario. Esto es especialmente importante en entornos industriales y de infraestructura crítica, donde la disponibilidad y fiabilidad de los sistemas es esencial para garantizar la seguridad, la eficiencia operativa y el cumplimiento de los estándares.

En la Figura 2 están representados los diferentes elementos que constituyen una infraestructura SCADA:

1. SCADA HMI (Human-Machine Interface): interfaz que vincula al operario con el sistema de telemetría. Presenta en diferentes pantallas de un Centro de Control todas las gráficas y KPIs (Key Performance Indicator) que muestran el estado actual de todos los componentes de la infraestructura.

2. MTU (Master Terminal Unit): ordenador central encargado de recopilar toda la información que proviene de cada RTU, almacenar dicha información en una base de datos, y enviar instrucciones a los dispositivos conectados.

3. Red de transporte: red que conecta los componentes de la infraestructura, en este caso el SCADA con las diferentes RTUs, mediante diferentes tecnologías como Ethernet, Wi-Fi, TETRA, fibra óptica…

4. RTU (Remote Terminal Unit): dispositivo encargado de convertir una señal analógica, como puede ser la temperatura, presión, flujo o el voltaje, en datos digitales para ser enviados al SCADA.

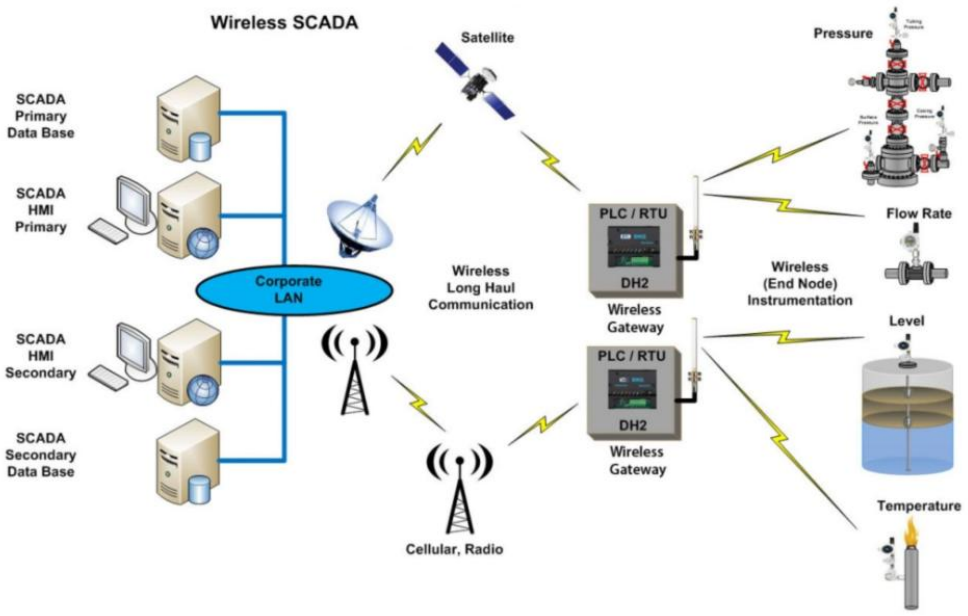


Figura 2 – Infraestructura Sistema SCADA [2]

El núcleo de un sistema SCADA está constituido por las RTUs, que se comunican con sensores, maquinaria y dispositivos finales. El software del SCADA instalado en el MTU es el encargado de encuestar a todas las RTUs de la infraestructura solicitando diferentes Datos de Operación correspondientes, por ejemplo, a la

presión, temperatura o flujo del gas natural en un gasoducto. Una vez son enviados al SCADA, es allí donde se procesan y distribuyen para que en caso de detectar un anomalía en la infraestructura, el operario sea capaz de analizarlos a través del HMI y evitar posibles daños.

Para la realización de este proyecto, nos vamos a centrar en el análisis de los Datos de Operación que atraviesan una red de transporte basada en TETRA. Pese a que el ancho de banda que proporciona TETRA no permite intercambiar una gran cantidad de datos, es suficiente para enviar información muy relevante en relación con el estado global de la infraestructura. Además, las RTUs están situadas en diferentes emplazamientos remotos, lo que puede llegar a complicar la comunicación mediante una red de transporte basada en fibra óptica por parte del SCADA, algo que no ocurre si la comunicación se lleva a cabo mediante TETRA ya que se precisa de una menor infraestructura y coste.

1.2. MOTIVACIÓN Y DESAFÍOS QUE SE ABORDAN

En el contexto de las redes de radiocomunicación de emisión crítica, es fundamental desarrollar un método que permita la monitorización del tráfico de datos intercambiado entre el sistema SCADA y las RTUs de los distintos sitios, independientemente de la tecnología de comunicación utilizada en la infraestructura.

Los sistemas de gestión actuales permiten visualizar mediante el sistema SCADA información sobre el estado actual de los diferentes elementos de la red, pero no proporcionan detalles específicos sobre el tráfico de datos intercambiado. Esta falta de visibilidad genera incertidumbre a la hora de analizar el comportamiento de la red y detectar posibles problemas de rendimiento o seguridad.

Por ello, la principal motivación de este proyecto radica en la necesidad de implementar una solución que permita visualizar detalladamente el tráfico de datos que circula a través de la red de transporte existente. Esto facilitará el análisis y diagnóstico de problemas, la optimización del rendimiento del sistema y la detección de anomalías que puedan comprometer la operatividad de los servicios críticos.

Uno de los mayores desafíos de este proyecto reside en la implementación e integración en una red de comunicaciones críticas de un método que permita representar gráficamente todos los detalles del tráfico intercambiado entre el SCADA y una o varias RTUs, así como realizar análisis forenses para identificar el origen de posibles fallos o interrupciones en el servicio.

Además, la escasez de soluciones comerciales que cumplan con estos requisitos plantea retos adicionales, especialmente en lo que respecta a los costos de desarrollo e implementación de la opción final elegida. No solo es necesario garantizar que la solución cumpla con los requerimientos funcionales, sino también evaluar su viabilidad en términos de coste y facilidad para su integración en la infraestructura existente.

1.3. OBJETIVO Y ALCANCE DEL PROYECTO

El objetivo principal de este proyecto es analizar el comportamiento del tráfico de datos en una red de radiocomunicación de emisión crítica cuando el sistema SCADA del cliente realiza una consulta a una RTU. En caso de que se produzca una pérdida de servicio en cualquier RTU dentro de la infraestructura, es esencial poder identificar y explicar el origen y la causa de dicha incidencia.

La implementación de un método de monitorización del tráfico de datos permitirá proporcionar información precisa al cliente sobre si el problema ha sido causado porque el SCADA no ha generado correctamente la consulta a la RTU o porque la RTU no ha respondido adecuadamente. Esto mejorará

significativamente la capacidad de diagnóstico, facilitando una rápida resolución de problemas y garantizando la continuidad operativa de los sistemas críticos.

El alcance de este proyecto no se limita únicamente al análisis del mercado en busca de la opción más adecuada, ni a su correcta implementación en una red de comunicaciones críticas. Su verdadero propósito es desarrollar una solución que pueda ser ofrecida como un producto final capaz de mejorar la monitorización y gestión del tráfico de datos en redes de comunicación de misión crítica, con el objetivo de facilitar al cliente final la visualización y comprensión del estado actual de su infraestructura.

1.4. ESQUEMA DE LA MEMORIA

El proyecto tiene como primer capítulo una introducción a los principales protocolos que, en la actualidad, son los más utilizados en el ámbito del análisis de datos en cualquier infraestructura de comunicaciones. En el segundo capítulo quedan expuestas las opciones analizadas durante el análisis de mercado que más se adaptaban a nuestros requerimientos y necesidades, y también se presentan los diferentes motivos por los que se eligió el producto final. En el Anexo C – Análisis de mercado completo quedan detalladas todas las opciones restantes estudiadas y analizadas durante el análisis de mercado.

Por otra parte, en el tercer capítulo de la memoria se lleva a cabo el diseño y configuración de la maqueta de pruebas inicial que tiene como único fin el estudio de la viabilidad de la opción escogida tras el análisis de mercado. En el cuarto y quinto capítulo se llevarán a cabo el montaje de la maqueta final de pruebas, la cual simula la infraestructura del cliente a pequeña escala, y se llevará a cabo el diseño del módulo de monitorización y su posterior optimización siguiendo los requisitos específicos del cliente.

Por último, en el Anexo A – Términos y definiciones técnicas, se muestra una recopilación de todos los términos técnicos a los que se harán referencia a lo largo de la memoria, en el Anexo B – Sistema de comunicaciones críticas TETRA, se aborda el funcionamiento e infraestructura que conforma un sistema de comunicaciones críticas basados en TETRA para facilitar la compresión de su infraestructura.

2. PROTOCOLOS DE ANÁLISIS DEL TRÁFICO DE DATOS DE OPERACIÓN EN UN RED DE COMUNICACIONES CRÍTICAS

El análisis de tráfico de datos de Operación en un sistema de comunicaciones críticas es una función imprescindible a implementar si se precisa conocer con exactitud el tráfico que atraviesa dicho sistema. En la actualidad, existen varios protocolos que realizan la monitorización del tráfico red, entre los que destacan los siguientes: SNMP, NetFlow y Port-Mirroring.

2.1. SNMP

SNMP [6] (Simple Network Management Protocol) es un protocolo de capa de aplicación para intercambiar información de administración entre dispositivos de red perteneciente al conjunto de protocolos TCP/IP. Proporciona información en tiempo real sobre el ancho de banda y el uso de la red, si bien no diferencia el tráfico por servicio/protocolo. Utiliza los puertos 161/162 (UDP) para realizar las comunicaciones con administradores y agentes SNMP. Actualmente hay tres versiones principales (SNMP v1, SNMP v2 y SNMP v3), si bien se utilizan mayoritariamente SNMP v1 y SNMP v2, debido a la complejidad de configuración de la última versión. Consta de 4 componentes básicos:

1. Administrador SNMP: Entidad responsable de comunicarse con los dispositivos de red implementados por el agente SNMP. Normalmente suele ser un equipo de la entidad administradora. Sus funciones clave son:

    - Obtener respuestas de agentes
    - Establecer variables en agentes
    - Reconocer eventos asincrónicos en agentes

2. Dispositivos administrados: Elemento de la red que requiere algún tipo de monitorización y administración de datos. Este elemento es generalmente un router, un switch o un servidor.
3. Agente SNMP: Programa empaquetado dentro del dispositivo administrado. La habilitación del agente permite recopilar la información de administración del dispositivo administrado y la pone a disposición del administrador SNMP. Las funciones del agente SNMP son:

    - Recopilar información de administración sobre su entorno local
    - Almacenar y recuperar información de gestión según se define en la MIB
    - Señalar un evento al administrador
    - Actuar como proxy para los nodos de la red que no son SNMP

4. Manage Information Base (MIB): Cada agente posee una base de datos de información que describe los parámetros del dispositivo administrado. Está formada por objetos administrados identificados mediante el identificador de objeto (OID). Cada identificador es único y señala características específicas de un dispositivo administrado. Compartida con el administrador SNMP, usa esta base de datos para solicitar al agente información específica y traducirla según sea necesario.

El protocolo SNMP utiliza una serie de comandos que facilitan el intercambio de información entre los componentes del protocolo. Son los siguientes:

- GET: Solicitud enviada por el administrador al dispositivo administrado. Se realiza para recuperar uno o más valores del dispositivo administrado.

- GET NEXT: Recuperación del siguiente valor del dispositivo administrado.
- GET BULK: Recuperar datos voluminosos de la MIB.
- SET: Modificar o asignar un valor al dispositivo administrado.
- TRAPS: Señalización al administrador SNMP por parte del agente sobre la repetición de un evento.
- INFORM: Confirmación de recepción de mensaje del administrador SNMP.
- RESPONSE: Comando utilizado para transportar los valores o la señal de las acciones dirigidas por el administrador de SNMP.

2.2. NETFLOW

NetFlow [7] es el estándar más utilizado para la monitorización y registro de todo el tráfico IP que atraviesa una red. Desarrollado por Cisco, está basado en la creación de flujos a medida que los paquetes atraviesan un dispositivo donde NetFlow ha sido configurado, por ejemplo, un router. Estos flujos son creados dependiendo de siete atributos que caracterizan cada paquete:

1. IP origen
2. IP destino
3. Puerto de origen
4. Puerto de destino
5. Tipo de servicio
6. Tipo de protocolo
7. Interfaz de entrada

Es decir, por cada paquete que atraviese el dispositivo donde el NetFlow ha sido configurado, se creará un flujo nuevo cada vez que cualquiera de los siete atributos mencionados anteriormente difiera de los atributos pertenecientes a los flujos creados anteriormente. Si los paquetes subsiguientes contienen los mismos atributos se añaden al flujo creado anteriormente, sino se crea un flujo nuevo. Una vez capturados los flujos de paquetes, NetFlow los envía mediante UDP a un recolector de NetFlow para que posteriormente sean analizados.

La arquitectura del estándar NetFlow descrita en la Figura 3 está formada por un NetFlow Exporter, encargado de recopilar los flujos IP entrante y saliente del dispositivo mediante el protocolo UDP, un NetFlow Collector, encargado de almacenar los flujos de datos, y un NetFlow Analyzer, encargado de analizar los flujos de datos:

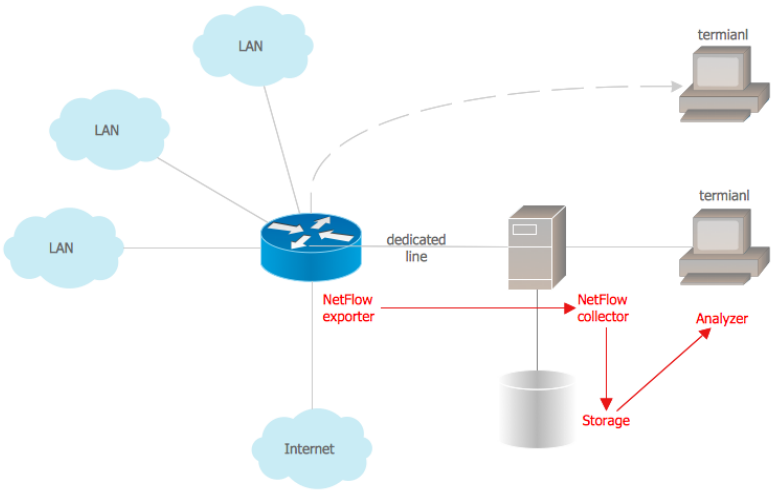


Figura 3 – Arquitectura protocolo NetFlow [3]

Una vez el flujo ha terminado, ya sea porque la conexión TCP ha concluido o porque la conexión TCP o UDP excede el tiempo de espera de datos en el caché (tiempo máximo que una conexión activa o inactiva puede permanecer almacenada en el caché esperando a ser exportada), el NetFlow Exporter envía un registro del flujo al NetFlow Collector para que sea analizado. Dicho registro contiene información granular sobre el flujo, que incluye:

- Comienzo y final del flujo
- Número de bytes y de paquetes
- Interfaz de entrada y salida
- Información de encabezado y enrutamiento de la capa 3 (IP origen y destino, puerto origen y destino…)

Ahora vamos a centrarnos en explicar detalladamente la configuración del protocolo NetFlow en un Firewall ubicado en una red de comunicaciones críticas TETRA. Comenzamos por el *flow record* el cual se basa en dos comandos principales:

- Match: Define los criterios que determinan cómo se agrupan los flujos de datos. Cuando un paquete difiere en alguno de los atributos especificados en *match*, se genera un nuevo flujo.

- Collect: Define qué información adicional se captura sin que su variación genere un nuevo flujo.

Para este proyecto, se ha definido el *flow record* denominado **RECORD-1**, el cual genera nuevos flujos cada vez que cambian el protocolo, la dirección IP de origen y destino, el puerto de origen y destino o la interfaz de entrada. Además, captura información sobre la interfaz de salida, el número total de paquetes y bytes transmitidos, así como los tiempos de inicio y finalización de cada flujo.

Proseguimos con el *flow exporter*, el cual define cómo se exportan los flujos de datos al *NetFlow Collector* para su posterior análisis y visualización. En esta configuración, se ha creado el **NFAexporter**, con los siguientes parámetros:

- Puerto de exportación: 9996 (protocolo UDP)

- Dirección IP del NetFlow Collector: 172.20.200.200
- Interfaz de salida: 0/0/1
- Template Data Timeout: 60 segundos

El protocolo NetFlow utiliza plantillas para estructurar los datos exportados. El parámetro *template data timeout* garantiza que, cada cierto intervalo de tiempo, el *NetFlow Exporter* envíe las plantillas actualizadas al *NetFlow Collector*, asegurando una correcta interpretación de los flujos capturados.

Y finalizamos con el *flow monitor* que es el componente responsable de supervisar y capturar los flujos de red de acuerdo con las configuraciones previas. Para este proyecto, se ha definido el *flow monitor* denominado **NFAmonitor**, al cual se le asignan el *flow record* y el *flow exporter* configurados anteriormente. Además, se establecen los siguientes parámetros clave:

- Cache Timeout Active: 30 segundos
- Cache Timeout Inactive: 15 segundos (valor por defecto)

El *cache timeout active* limita el tiempo que una sesión de datos activa puede permanecer en la memoria caché del router antes de ser enviada al *NetFlow Collector*. Esto optimiza la utilización de la memoria y evita problemas de almacenamiento. De manera similar, el *cache timeout inactive* determina el tiempo máximo que un flujo inactivo puede permanecer en caché antes de ser considerado expirado.

Todas las configuraciones anteriormente explicadas se pueden visualizar en la Figura 4, llevadas a cabo para configurar el protocolo NetFlow en el firewall asociado a una red de comunicaciones para misión crítica TETRA.

```
flow record RECORD-1
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 collect interface output
 collect counter bytes long
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!
!
```

```
!
flow exporter NFAexporter
 destination 172.20.200.200
 source GigabitEthernet0/0/1
 transport udp 9996
 template data timeout 60
!
!
flow monitor MONITOR-1
 exporter EXPORTER01
 cache timeout active 30
 record RECORD-1
!
```

Figura 4 – Configuración Protocolo NetFlow

Actualmente, existen numerosas versiones de NetFlow desarrolladas por Cisco entre las que destacan NetFlow v5 y v9, siendo NetFlow v5 la versión más común la cual soporta tráfico unicast y multicast IPV4, mientras que NetFlow v9 cuenta con todas las características de la versión anterior incorporando tráfico IPV6 unicast y multicast. También existen versiones basadas en NetFlow desarrolladas por otros fabricantes (jFlow desarrollada por Juniper, NetStream desarrollado por Huawei o IPFIX desarrollado por la IETF). Utilizaremos NetFlow v9 ya que es el protocolo que soporta el router Cisco 4331 instalado como Firewall entre el SCADA del cliente y la red de comunicaciones.

A diferencia del protocolo SNMP, mediante NetFlow podemos obtener información acerca de la IP origen y destino del paquete o el puerto de origen y destino de este, algo que SNMP no proporciona. No obstante, mediante el protocolo NetFlow no somos capaces de capturar paquetes en tiempo real, ya que solo proporciona el instante de tiempo inicial y final de la comunicación entre dos interfaces (mediante SNMP, somos capaces de capturar tráfico en tiempo real).

2.3. PORT-MIRRORING

Por otro lado, existe un protocolo denominado port-mirroring [4] que básicamente se implementa en un dispositivo (normalmente suele ser un router o un switch), para enviar una copia de todos los paquetes que atraviesan un puerto específico de origen a otro puerto específico de destino. Mediante la duplicación de puertos locales, el dispositivo es capaz de reenviar una copia de todos los paquetes que entren por el puerto de origen al puerto de destino.

El protocolo port-mirroring se implementa siguiendo una serie de pasos:

1. Elección de puerto origen y puerto destino: Se escoge un puerto origen en el cual se quiere copiar el tráfico que lo atraviesa, y se escoge otro puerto destino por donde el tráfico copiado será enviado.
2. Configuración del dispositivo: Se configuran internamente los puertos origen y destino para poder realizar la copia y envío de paquetes correctamente.
3. Análisis del tráfico: Conexión al puerto destino de un dispositivo que sea capaz de almacenar el tráfico copiado para poder ser analizado en el futuro.

En la Figura 5 se puede ver la sencillez del proceso de copia de paquetes que se implementa en el port-mirroring.

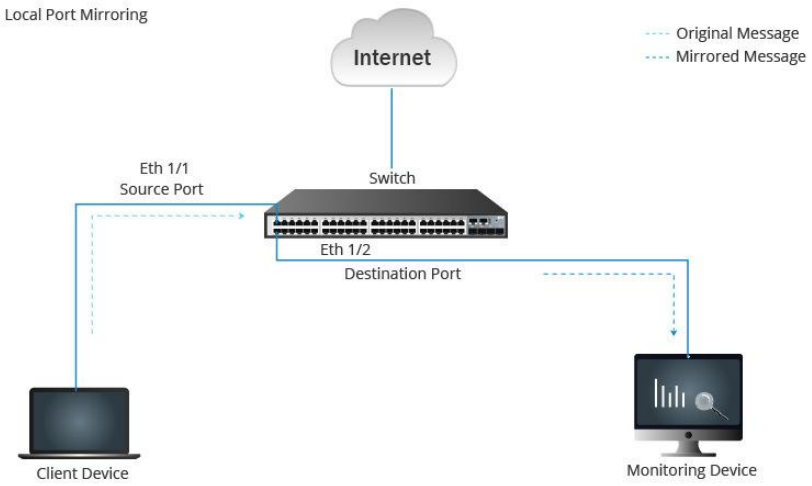


Figura 5 – Funcionamiento protocolo port-mirroring [4]

Pese a la sencillez del protocolo, mediante port-mirroring es posible capturar todas las tramas de paquetes que atraviesan los puertos configurados como origen y destino, algo que no es posible realizar mediante los dos protocolos explicados anteriormente. Esto es realmente útil, ya que a la hora de realizar un análisis forense en un sistema de comunicaciones, el mostrar una simple gráfica donde se pueda ver que en un momento concreto no hay comunicación entre dos IPs es inadmisible. Es necesario mostrar todas las tramas de paquetes que se han capturado en ese momento y verificar que entre esas dos IPs no se ha intercambiado ningún paquete, es decir, se precisa poder ver todos los paquetes intercambiados, con una gráfica no es suficiente.

3. ANÁLISIS DE MERCADO

Tras haber introducido los principales métodos utilizados en la actualidad para monitorizar el tráfico que atraviesa un sistema de comunicaciones, vamos a realizar un análisis de mercado explorando todas las opciones existentes hoy en día relacionadas con la obtención, almacenamiento y análisis del tráfico de Datos de Operación. Para ello, dividiremos las opciones analizadas según el tipo de solución que ofrecen (hardware o software), y según el tipo de protocolo que utilizan para obtener todo el tráfico de Datos de Operación.

El análisis de cada opción se basará en la instalación de su demo o de una pequeña prueba de concepto realizada por las diferentes compañías proveedoras donde se mostrarán las principales características y funcionalidades del producto.

Especialmente, me he centrado en la visualización del tráfico que fluye entre dos IPs en un intervalo de tiempo concreto. Es decir, la característica principal que buscamos en los productos a analizar radica en la posibilidad de filtrar el tráfico de Datos de Operación que atraviesa el firewall del sistema por IP y por intervalos de tiempos, pues es el requisito principal impuesto por el cliente. Además, el producto deberá poder ofrecer la opción de mostrar las capturas de todos los paquetes enviados entre esas dos IPs para poder verificar lo que realmente estamos visualizando en las gráficas.

La gran parte de productos analizados ofrecen una infinidad más de características relacionadas con la filtración de datos, la seguridad y estado del sistema, la programación de alerta o la calidad del servicio, las cuales han sido obviadas en este análisis debido a los requisitos principales del cliente (si bien es cierto que su inclusión en el producto ofrece una serie de ventajas añadidas a los requisitos principales).

En la Tabla 1 se reflejan los requerimientos considerados para la elección del producto final a implementar a posteriori tras haber sido evaluados durante las numerosas pruebas de concepto realizadas con distintos proveedores:

REQUERIMIENTOS	PRODUCTO FINAL
FILTRAR TRÁFICO POR IP, PUERTO, PROTOCOLO E INTERVALO DE TIEMPO	✓
MONITORIZACIÓN ANCHO DE BANDA DEL ENLACE	✓
GENERACIÓN ARCHIVO PCAP	✓
ELEMENTO INVISBLE PARA LA RED	✓
ROBUSTEZ FRENTE A ALTAS TASAS DE PAQUETES/S	✓
PERSONALIZACIÓN GRÁFICOS	✓
GENERACIÓN DE ALARMAS ANTE COMPORTAMIENTOS ANÓMALOS	✓

Tabla 1– Requerimientos durante el proceso de selección y del producto final

A continuación, expondremos las opciones que más se ajustaban a los requerimientos anteriormente mencionados y justificaremos la elección del producto final. Las demás opciones analizadas quedarán descritas en el Anexo C – Análisis de mercado completo debido a que no cumplían varios de los requerimientos de la Tabla 1 o por razones de coste total de implementación en el cliente final.

3.1. SOLUCIÓN SOFTWARE MEDIANTE NETFLOW Y PORT-MIRRORING

3.1.1. Flowmon Network Monitoring

Flowmon ofrece una solución software basada en la adquisición del tráfico de un sistema de comunicaciones mediante el protocolo NetFlow y el port-mirroring. La combinación de ambos productos permite realizar numerosas configuraciones en cuanto a la aplicación de filtros del tráfico que atraviesa la red, así como, mediante su herramienta Flowmon Packet Investigator, son capaces de mostrar las tramas de todos los paquetes capturados en dicha red.

En la Figura 6, podemos los tipos de protocolos utilizados en la transmisión de paquetes, los puertos más utilizados o todas las IP que han enviado paquetes. Por otro lado, en la Figura – Flujo de paquetes entre dos IPs, podemos ver la cantidad de paquetes transmitidos entre las dos IPs y el tipo de protocolo al que pertenece cada paquete.

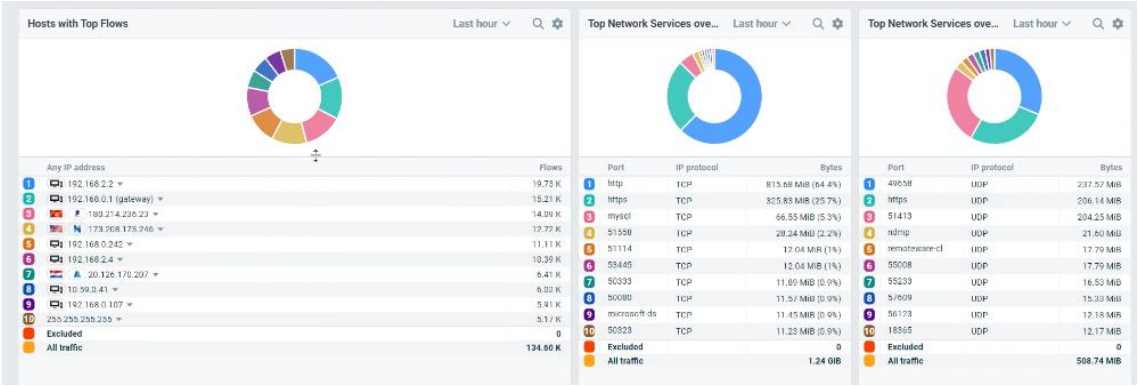


Figura 6 – Resumen tráfico del sistema

Finalmente, mediante la herramienta Packet Investigator, podemos generar la captura de las tramas de todos los paquetes intercambiados entre ambas IPs en un intervalo determinado de tiempo, comúnmente conocido como un archivo PCAP. En la Figura 7 queda reflejado el instante exacto de transmisión de cada paquete junto con diferentes características de este (IP origen y destino, tamaño del paquete, puerto de entrada y tipo de protocolo).

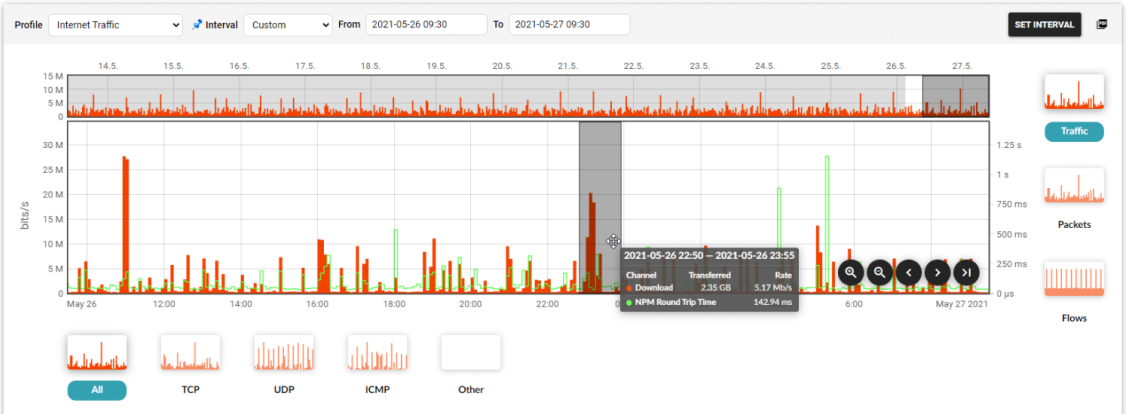


Figura 7 – Archivo PCAP del envío de paquetes entre dos IPs

3.2. SOLUCIÓN HARDWARE MEDIANTE NETFLOW Y PORT-MIRRORING

3.1.2. Viewtisight

Desarrollado por la compañía Viewtinet, proporcionan hardware dedicado al almacenamiento de todos los paquetes que atraviesan los puertos configurados para el port-mirroring. En el hardware proporcionado, es donde corre el software que permite visualizar las gráficas de la Figura 8. Se pueden observar diferentes aspectos relacionados con el número de paquetes y flows que atraviesan el sistema, así como, diferentes aspectos del rendimiento del sistema (tiempo de respuesta del servidor, tiempo de transporte de los datos…).

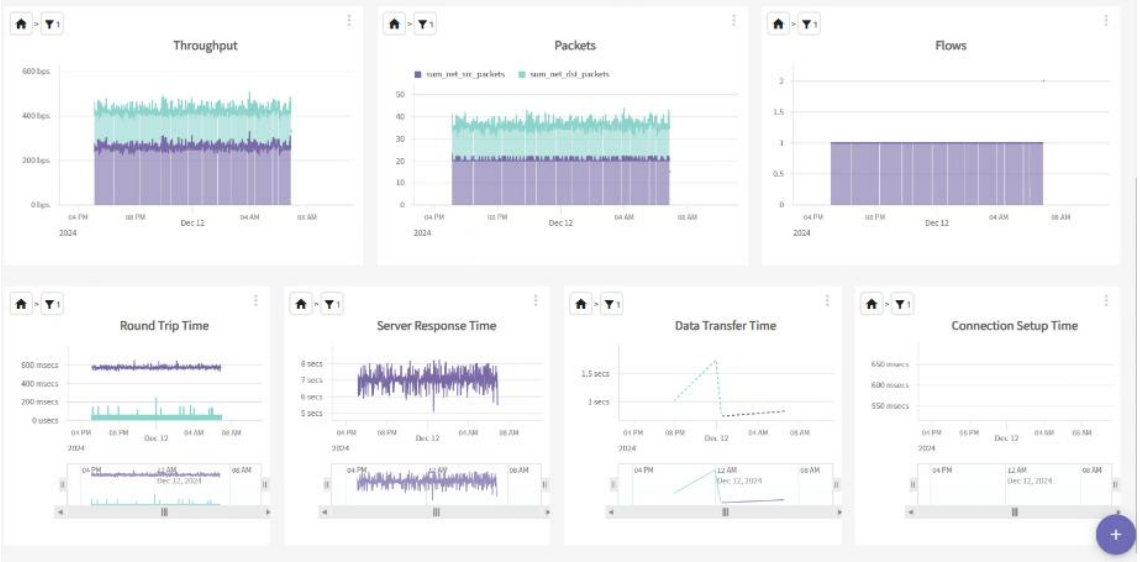


Figura 8 – Resumen del tráfico del sistema

Por otro lado, Viewtinet ofrece Viewtimon Packet-Sniffer como una herramienta para realizar archivos PCAP de los paquetes analizados tanto en tiempo real como en comunicaciones pasadas. Proporciona la opción de configurar la información del paquete que se quiere almacenar, algo que es realmente útil, ya que permite no almacenar el payload del paquete (mediante la cabecera del paquete obtenemos toda la información necesaria, así que almacenar el payload supone un consumo extra del disco duro).

3.1.3. IOTA 1G

IOTA 1G es un dispositivo diseñado por ProfiTap cuya función principal es la de almacenar y analizar el tráfico en tiempo real que se transmite en una red de comunicaciones. Cuenta con una base de datos interna encriptada que permite el almacenamiento de todo el tráfico que captura, y también posee su propio software integrado que le facilita el análisis del tráfico capturado en tiempo real. Destacar que es un elemento pasivo en la red, es decir, su instalación no afecta al tráfico ni al comportamiento de la red ya que es invisible e inocuo. Cuenta con dos puertos de monitoreo encargados de interconectar el dispositivo en el enlace de la red que se quiere monitorizar, y con un puerto de gestión para poder acceder al dispositivo mediante conexión IP.

Este hardware opera como un equipo que se sitúa entre dos nodos de una red en donde se quiere capturar el tráfico que atraviesa dichos nodos. Gracias a la combinación de su software junto con GRAFANA, el IOTA 1G es capaz ofrecer en tiempo real numerosas características y aspectos del tráfico capturado

mediante diferentes KPIs y gráficos. Permite realizar diversas configuraciones a la hora de filtrar el tráfico capturado (IP, puerto, protocolo, aplicación…), como se puede ver en la Figura 9.

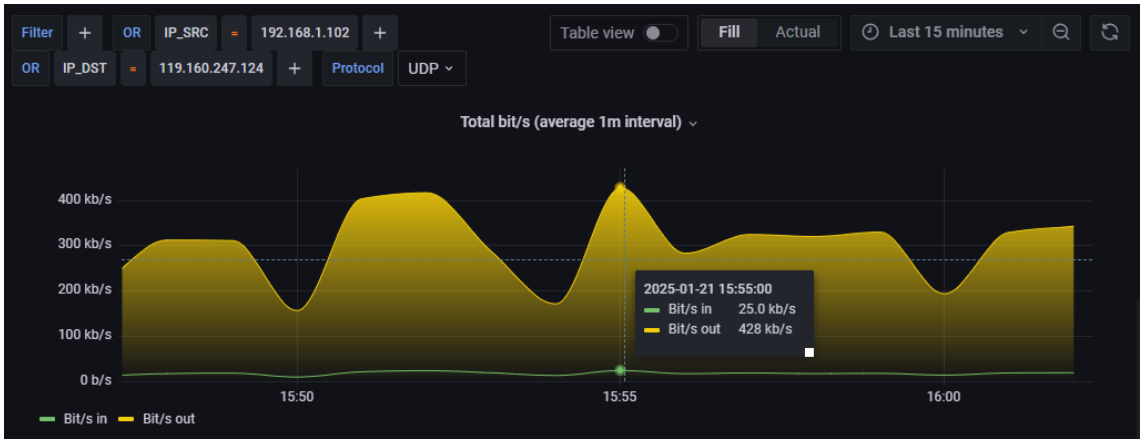


Figura 9 – Tráfico UDP promedio entre dos IPs.

Por otro lado, el IOTA 1G también proporciona la generación de un archivo PCAP correspondiente con cualquier comunicación de datos que deseemos, algo que es de suma importancia ya que se precisa poder visualizar explícitamente los paquetes enviados en dichas comunicaciones. Finalmente, gracias al uso de GRAFANA para la generación de los KPIs, nos permite tener una gran versatilidad a la hora de representar los gráficos que queramos debido a que GRAFANA ofrece una gran variedad de gráficos personalizables.

3.3. CONCLUSIONES TRAS EL ANÁLISIS DE MERCADO Y PRODUCTO FINAL ESCOGIDO

Tras haber expuesto las características principales de todas las opciones valoradas, se puede ver como la gran mayoría de las opciones cumplían con los requerimientos de granularidad, filtrado de datos por IP, puerto, protocolo o sentido de comunicación; no obstante, son pocas las opciones que además proporcionen la capacidad de poder visualizar el archivo PCAP de una transmisión de datos entre el SCADA del cliente y cualquier RTU, es decir, de poder visualizar los paquetes transmitidos mediante una trama y no una simple tabla. Dicho esto, tres opciones son las que logran cumplir todos los requisitos mencionados anteriormente: Viewtisight desarrollado por Viewtinet, IOTA 1G desarrollado por ProfiTap y Flowmon Network Monitoring desarrollado por Progress.

Una vez recibida una oferta formal por parte de las tres opciones mencionadas anteriormente, se optó por la opción proporcionada por ProfiTap debido a las siguientes razones:

- Menor coste de adquisición con respecto a la opción ofrecida por la competencia.
- Menor coste de implementación y desarrollo del producto en el cliente final.
- Facilitación del hardware para realizar la prueba de concepto en las diferentes maquetas de pruebas elaboradas.
- Representación de los KPIs y gráficos mediante GRAFANA, lo que permite una amplia libertad para generar los gráficos solicitados por el cliente.

Además, en la Tabla 2 podemos ver el grado de conformidad en diferentes aspectos de cada uno de los 3 productos mencionados anteriormente. Mediante un simple vistazo a la Tabla 2 se podrá observar los puntos fuertes y débiles de cada producto.

	IOTA 1G	VIEWTISIGHT	FLOWMON NETWORK MONITORING
COSTE			
PERSONALIZACIÓN DE GRÁFICOS			
FACILITACIÓN HARDWARE			
EXPORTACIÓN GRÁFICOS A ARCHIVO CSV Y ARCHIVO PCAP			
SEGURIDAD DE DATOS			
OPCIÓN DE RACK			
ROBUSTEZ FRENTE A ALTAS TASAS DE DATOS			

Tabla 2 – Valoración de las características de cada producto

4. DISEÑO Y CONFIGURACIÓN DE LA MAQUETA INICIAL DE PRUEBAS

Tras realizar el correspondiente análisis de mercado y habiendo elegido la opción facilitada por ProfiTap, pasamos a efectuar la integración e implementación del IOTA 1G en un sistema de comunicaciones críticas. Como primera prueba a llevar a cabo sobre el producto adquirido, vamos a realizar el montaje y configuración de una maqueta de pruebas inicial, cuyo objetivo será el de simular todas las comunicaciones existentes en una red de transporte de un sistema de comunicaciones críticas formado por un SCADA y diversas RTUs.

Es muy importante destacar que, a la hora de simular correctamente el tráfico existente entre el SCADA y las RTUs, debemos tener en cuenta el número total de paquetes por segundo que atravesarán el IOTA 1G, más que el Throughput total que lo atraviese. Esto es debido a que el sistema SCADA está encuestando a cada RTU según un intervalo temporal (1, 3, 5, 10 o 15 minutos), por lo que se llegan a tener un número elevado de conexiones por segundo, que desemboca en un número elevado de paquetes por segundo a procesar por el IOTA 1G. Además, la información intercambiada en dichos paquetes no supone una gran cantidad de bytes, lo que supone que a pesar de enviar un número elevado de paquetes por segundo, el ancho de banda consumido en todas las comunicaciones entre el SCADA y las RTUs no será tan elevado en comparación con el número de paquetes, y por consiguiente, no supondrá un problema para el IOTA 1G.

Por tanto, como la gran mayoría de redes de comunicación dedicadas al monitoreo de datos a través del sistema SCADA se caracterizan por una gran cantidad de conexiones por segundo y sus paquetes no transportan un gran volumen de datos, los paquetes por segundo es la métrica más crítica a tener en cuenta para verificar la viabilidad de la red de transporte y de los diferentes elementos que la conforman.

Dicho esto, procedemos a ilustrar la maqueta de pruebas realizada, así como su configuración. En la Figura 10 se pueden observar los elementos que conformen la maqueta, que son los siguientes:

1. PC / SCADA: ordenador encargado de realizar la función del sistema SCADA mediante el envío de diferentes pings (Request) a las distintas RTUs.

2. IOTA 1G: dispositivo a cargo de almacenar y procesar todos los paquetes de datos de operación que lo atraviesen. Invisible a la red, desempeña la función de TAP (Terminal Access Point, que comentaremos más adelante en profundidad) entre los dos nodos de la red que se quieren monitorizar. Conectado al SCADA mediante un cable Ethernet a su primer puerto de monitoreo y al switch mediante otro cable Ethernet a su segundo puerto de monitoreo.

3. PC Monitoreo: ordenador conectado al puerto de gestión del IOTA 1G. Mediante conexión IP se accede al GRAFANA del IOTA 1G para poder visualizar los distintos KPIs generados.

4. Switch: elemento responsable de realizar la conexión entre el IOTA 1G y ambos routers.

5. Router 1 y 2 / RTU 1 y 2: routers de realizar la función de las RTUs mediante el envío de los pings de respuesta (Reply).

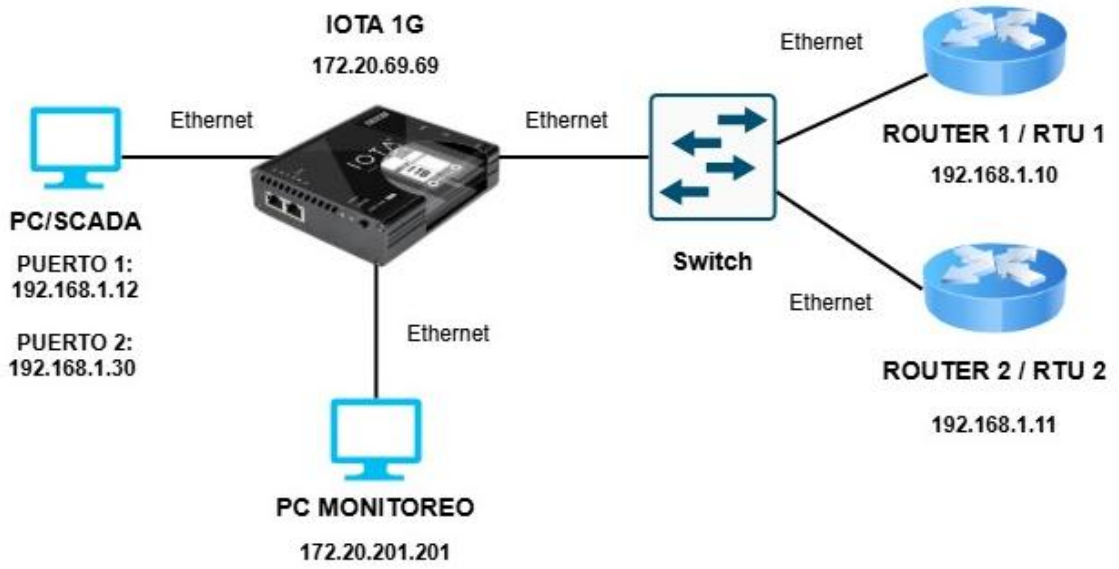


Figura 10 – Maqueta inicial de pruebas

En relación con la configuración de la maqueta, únicamente hay que realizar la configuración del PC para poder llevar a cabo los pings hacia las RTUs. Comenzamos definiendo las IPs asociadas a los dos puertos que vamos a emplear como direcciones fuente de nuestros pings, y definiendo los Gateway para cada puerto, que posteriormente se especificarán como direcciones destino de nuestros pings. En La Figura 11 podemos ver como para el puerto 1 le asignamos la IP 192.168.1.12 y la IP 192.168.1.10 como Gateway, y al puesto 2 le asignamos la IP 192.168.1.30 y la IP 192.168.1.11 como Gateway.

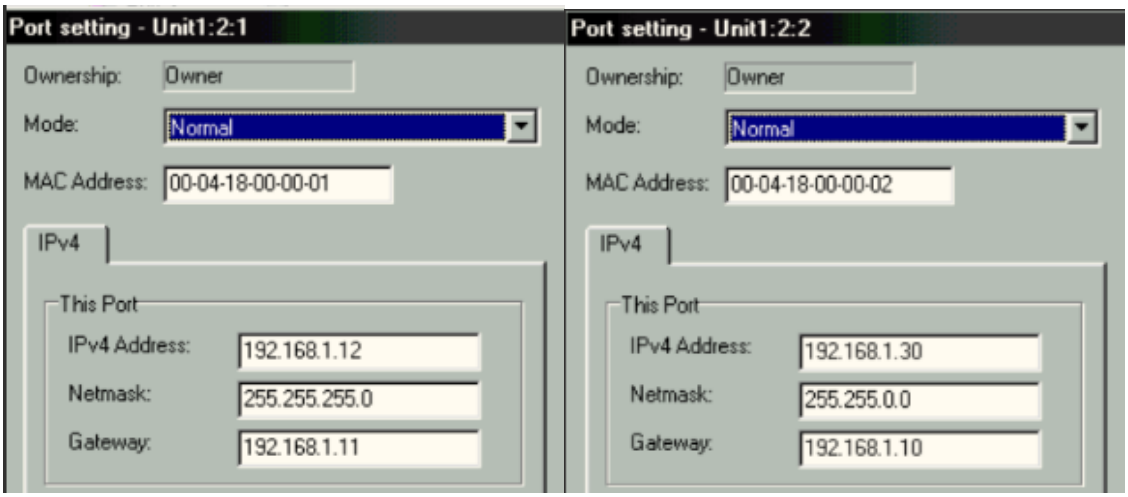


Figura 11 – Configuración de los puertos

A continuación, vamos a configurar el protocolo a utilizar en cada puerto para efectuar los pings, que en este caso va a ser IPV4/ICMP. En la Figura 12, podemos ver como para el puerto 2, definimos como se ha comentado anteriormente, la IP del puerto como la dirección fuente y la IP 192.68.1.10 como la dirección destino. Asimismo, realizamos la misma configuración a nivel Ethernet. Para el puerto 1, se han llevado a cabo las mismas configuraciones que para el puerto 2, únicamente variando la IP de la dirección destino a la 192.168.1.11.

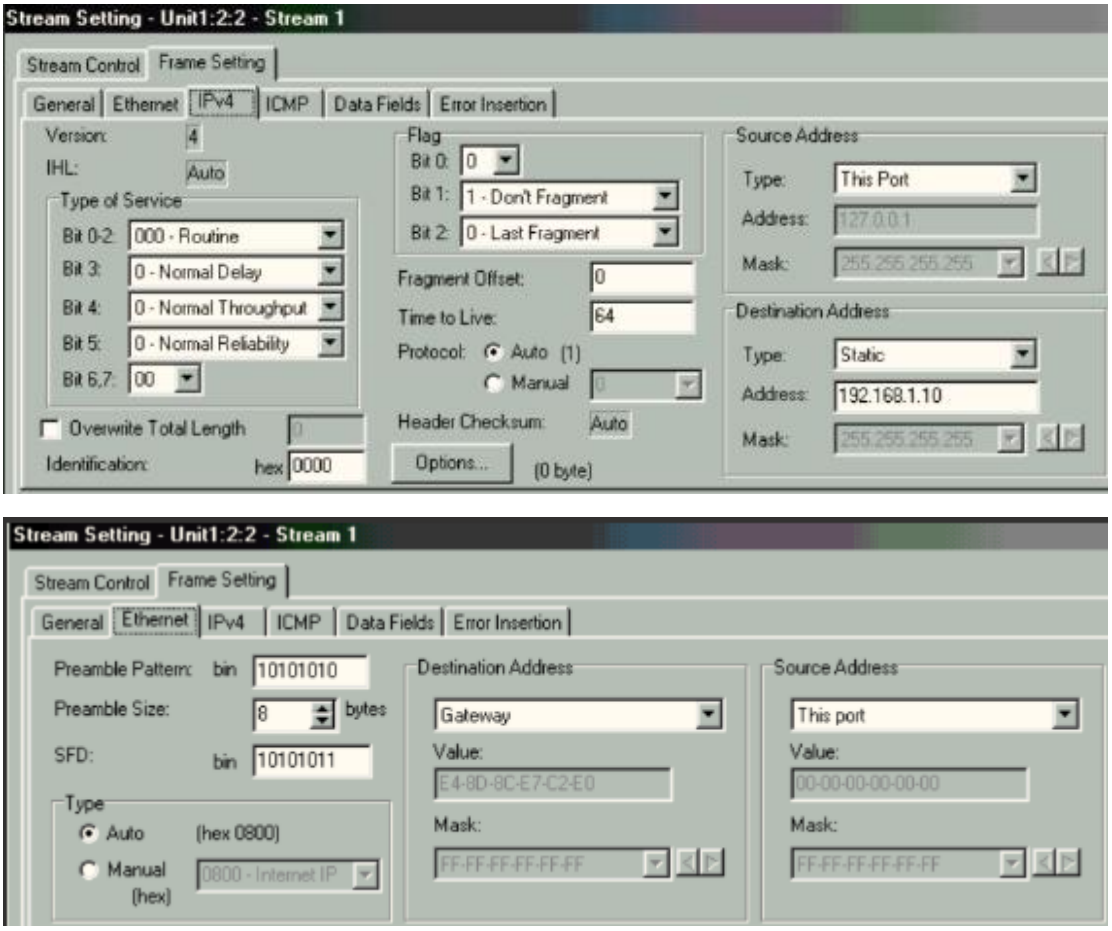


Figura 12 – Configuración protocolo IPV4/ICMP

Por último, sólo nos queda especificar la tasa de paquetes por segundo, que para esta prueba inicial se ha fijado a 400. Se ha escogido la cifra anterior mediante el análisis de diferentes redes de monitorización desplegadas hoy en día por parte de las compañías dedicadas a la radiocomunicación para misión crítica, las cuales están ubicadas en diferentes partes del mundo y en diferentes sectores.

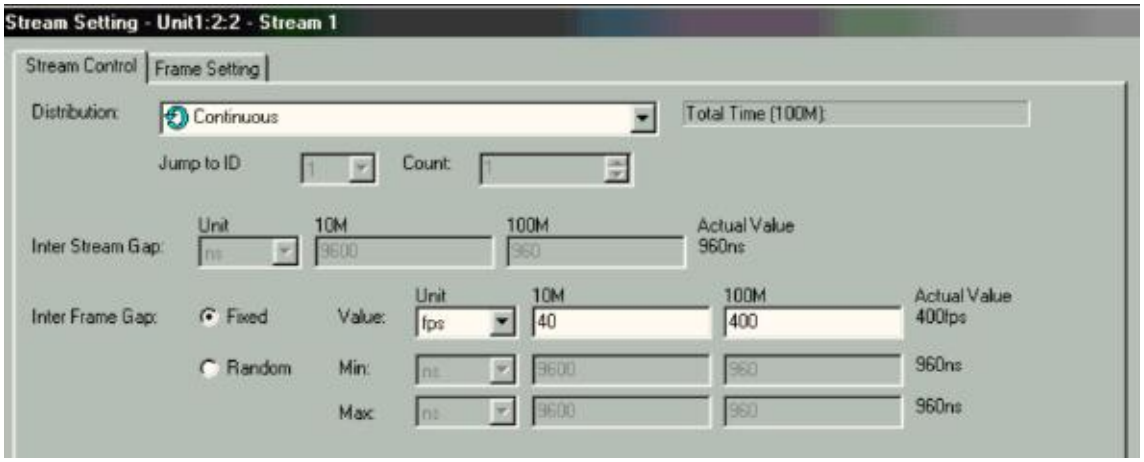


Figura 13 – Configuración paquetes/s

Tras realizar todas las configuraciones pertinentes, se llevó a cabo la prueba inicial que resultó ser superada con éxito por parte del IOTA 1G, ya que a la hora de interactuar con los diferentes dashboards no se tuvo ningún problema ni comportamiento extraño por parte del mismo, lo que significa que el dispositivo fue capaz de soportar la elevada tasa de paquetes por segundo a la hora de acceder a la base de datos para obtener los datos necesarios para su representación o a la hora de cargar todos los dashboards.

Esto significa que una vez sometido al IOTA 1G a altas tasas de paquetes, como los que se encontrará en la infraestructura del cliente, la navegación por la interfaz del IOTA 1G era fluida y sin apenas cortes. Por tanto, podemos llegar a la conclusión de que el cliente final podrá tener una correcta experiencia de usuario una vez el producto sea instalado en su infraestructura.

Por último también se llevaron otras pruebas como la representación de todos los Datos de Operación analizados en intervalos grandes de tiempo, como es un mes, con el objetivo de ver cómo se comporta el IOTA 1G ante la carga de numerosos bytes de datos almacenados en su base de datos. Esta prueba tuvo el mismo resultado que la anterior, así que a la hora de realizar el informe mensual de disponibilidad de la infraestructura del cliente, tampoco se tendrá problema alguno de carga y navegación a través de los diferentes KPIs.

5. MÓDULO DE MONITORIZACIÓN DE DATOS DE OPERACIÓN

Tras verificar que el IOTA 1G es capaz de soportar correctamente el volumen máximo de paquetes por segundo que atraviesan la red de comunicaciones del cliente, vamos a centrarnos en explicar el alcance, las características y los principales objetivos del módulo de datos de operación desarrollado mediante GRAFANA, el cual permitirá al cliente visualizar y entender de una manera sencilla y eficaz lo que está sucediendo en tiempo real en su infraestructura. Antes de comenzar con la explicación del módulo de monitorización para datos de operación, voy a realizar una pequeña introducción sobre GRAFANA, que es la herramienta empleada en el IOTA 1G para la generación de los dashboards, destacando sus principales funcionalidades y características, prestando especial atención al tratamiento de los datos capturados.

GRAFANA es una plataforma de código abierto utilizada para la visualización y el monitoreo de datos en tiempo real. Se emplea principalmente en la creación de KPIs y dashboards interactivos a partir de los datos provenientes de diversas fuentes, comúnmente bases de datos. Existen numerosas bases de datos empleadas para almacenar y tratar los datos en GRAFANA como Prometheus, Influx DB, MySQL o PostgreSQL; sin embargo, la base de datos empleada en el IOTA 1G es ClickHouse.

ClickHouse es un sistema de gestión de bases de datos de código abierto basado en SQL y orientado a columnas, diseñado específicamente para consultas analíticas y procesamiento de grandes volúmenes de datos en tiempo real. A diferencia de la mayoría de bases de datos propietarias, ClickHouse es impulsada por cientos de usuarios colaboradores enfocados a crear una mejor funcionalidad y resolver problemas que pueden degradar su rendimiento. Las principales características y ventajas de ClickHouse respecto a otras bases de datos son las siguientes:

1. Arquitectura orientada a columnas: almacena los datos por columnas en lugar de filas, optimizando el acceso a datos específicos y acelerando las consultas analíticas.
2. Procesamiento vectorizado: opera en bloques de datos en lugar de filas individuales, logrando así un procesamiento paralelo altamente eficiente.
3. MergeTree Engine: motor de almacenamiento desarrollado por ClickHouse, el cual optimiza el tratamiento de los datos especialmente para series temporales, que son las más utilizadas en el ámbito de monitorización de datos en infraestructuras eléctricas, mineras o gasoductos.
4. Compatibilidad SQL: utiliza como lenguaje de código un dialecto SQL compatible con ANSI SQL. Además, posee numerosos APIs para realizar su integración con aplicaciones externas.

Ahora bien, a la hora de generar un dashboard en tiempo real en GRAFANA se debe realizar una consulta a la base de datos en donde estén almacenados los datos que queremos mostrar, lo que comúnmente es conocido como Query. Básicamente, mediante la Query definimos qué datos se muestran, cómo se procesan y cómo se visualizan en tiempo real. En la Figura 14 se pueden ver las diferentes partes básicas de una Query, que son las siguientes:

1. SELECT: se especifican las columnas (datos) que deseemos escoger de la tabla.
2. FROM: detalla la tabla de la cual se van a extraer los datos anteriores.
3. WHERE: establece los filtros que se van a utilizar para filtrar los datos.
4. GROUP BY: agrupación de los datos que comparten valores comunes.
5. ORDER BY: define el orden de presentación de los datos.

Figura 14 – Formato estándar de una Query y su dashboard resultante

Además de las diferentes partes de la Query comentada anteriormente, existen numerosos parámetros editables en el propio GRAFANA como son el tipo de panel que se quiere representar, el rango de refresco de este, condiciones de alarma (threshold), anotaciones automatizadas o ajustes relacionados con la estética del panel. Mediante la configuración de todos estos parámetros se puede llegar a ofrecer una gran variedad de paneles al cliente en donde podemos configurar numerosas alertas visuales que permitan identificar un comportamiento anómalo en la red de transporte instantáneamente.

Como ya he comentado previamente en la introducción de este proyecto, existen numerosas industrias (minera, eléctrica, ferroviaria, gasoductos…) donde, aparte de toda la información que el SCADA puede aportar al cliente en relación con el estado actual de su red de comunicaciones, es necesario incorporar una herramienta extra la cual permita únicamente mediante el análisis del payload del tráfico capturado, poder presentar al cliente numerosos paneles que escenifiquen que está ocurriendo en tiempo real con un mayor detalle y granularidad de la que ofrece el SCADA.

Dicho lo anterior, el principal objetivo del módulo de monitorización de datos de operación es el de analizar el tráfico que atraviesa la red de transporte de una infraestructura crítica, presentando diferentes paneles, gráficas o KPIs que permitan poder realizar, por ejemplo, un informe de resultados mensual acerca del estado de la red de comunicaciones en cualquier instante de tiempo requerido. Es muy importante destacar que, esta herramienta de monitorización no realiza dicho informe, sino que proporciona todos los datos necesarios para su posterior realización.

Es decir, esta herramienta está enfocada en la disponibilidad de la red de transporte proporcionada al cliente, la cual se está monitorizando mediante el IOTA 1G. Gracias al análisis de todos los datos capturados, es posible realizar dicho informe de resultados, el cual tiene un valor vital para poder resumir la disponibilidad ofrecida por la infraestructura proporcionada al cliente. También, tiene la capacidad de demostrar quién es el culpable ante la aparición de un comportamiento anómalo en la infraestructura del cliente, ya que posee todos los registros de los paquetes intercambiados en la red pudiendo así demostrar legalmente si la culpa es del propio cliente o de la red de transporte proporcionada por la compañía de radiocomunicación.

Por otro lado, es imprescindible que no afecte a la disponibilidad de la infraestructura de comunicaciones del cliente, es decir, debe comportarse como un elemento invisible para la red de transporte, lo que

comúnmente se conoce como TAP. Un TAP es un dispositivo hardware, como en este caso es el IOTA 1G, que se coloca entre dos dispositivos conectados para monitorizar el tráfico de red que lo atraviesa. Como es un dispositivo independiente, está diseñado para funcionar en segundo plano sin alterar el rendimiento de la red, así pues si en algún momento ocurre algún problema con el dispositivo, las comunicaciones de toda la red de transporte no se verán afectadas en ningún caso.

Por último, hay que destacar como se va a llevar a cabo la integración del módulo de monitorización en el sistema NMS que proporciona una compañía del sector de radiocomunicación para misión crítica, para poder gestionar y operar su infraestructura. Mediante la creación de un nuevo icono en la barra de herramientas de la aplicación, como se puede ver redondeado mediante un círculo rojo en la Figura 15, al pulsar sobre el mismo se mostrará al usuario un desplegable donde pueda seleccionar el módulo al que quiera acceder, principal o redundante.

Figura 15 – Barra de herramientas NMS

Por tanto, podemos resumir el alcance y las principales funcionalidades del módulo de monitorización de datos de operación en los siguientes puntos:

- Monitorización y análisis en tiempo real del tráfico entre el SCADA y cada RTU, garantizando una rápida detección de cada incidencia ocurrida en la red.
- Elaboración de paneles y KPIs del tráfico total entre el SCADA y las diferentes RTUs, que aporten la información necesaria para la futura realización de un informe de resultados acerca de la disponibilidad de la infraestructura proporcionada al cliente.
- Almacenamiento de los datos de tráfico para su posterior análisis.
- Generación de archivos PCAP de cada flujo de datos monitorizado para su posible uso legal.
- Accesibilidad desde la barra de herramientas del Cliente NMS.

A la hora de representar el estado de la red de transporte se han desarrollado tres dashboards en los cuales quedan reflejados diferentes aspectos de la red que posteriormente comentaremos.

5.1. DASHBOARD DE MONITORIZACIÓN DEL TRÁFICO GLOBAL ENTRE SCADA Y RTUS

El primer dashboard del módulo de monitorización es el encargado de mostrar diferentes características sobre el tráfico global que atraviesa la red de transporte. Ofrece una visión holística del tráfico total entre el SCADA y todas las RTUs, permitiendo evaluar el rendimiento global del sistema. En la Figura 16 se pueden ver los diferentes paneles que lo conforman.

En este dashboard destaca el panel encargado de mostrar el estado de cada RTU, así como el histórico de actividad de todas las RTUs. Mediante este histórico de actividad, podremos tener reflejado la inactividad de cualquier RTU del sistema mediante intervalos temporales, algo muy útil ya que nos ayuda a saber cuándo finalizó la comunicación entre el SCADA y la RTU. Es decir, simboliza lo mismo que las alertas del Panel 1 sólo que en formato histórico de actividad.

También destacar que, para cada apunte generado en el histórico de actividad, se genera adicionalmente una alerta en forma de línea roja vertical discontinua en el primer panel del dashboard. Para facilitar la

compresión del gráfico, únicamente podrá aparecer una alerta por RTU y por día. De esta forma, si la RTU permanece una semana sin transmitir, tendremos una alerta por hora en vez de una alerta en cada instante de tiempo que no transmita hacia el SCADA.

5.2. DASHBOARD DE MONITORIZACIÓN DEL TRÁFICO DE UNA ÚNICA RTU

El segundo dashboard del módulo de monitorización está diseñado para detallar el tráfico compartido entre una RTU concreta y el sistema SCADA del cliente. En la Figura 17 se observan todos los paneles del dashboard.

En este segundo dashboard destaca la presencia del último panel en el cual aparecen todos los flujos de Datos de Operación entre el SCADA y la RTU concreta. Permite descargar el PCAP correspondiente a cada flujo, algo esencial para saber si un determinado paquete ha sido enviado/recibido. Pulsando en un flujo determinado podremos acceder al último panel del módulo de monitorización, donde se podrán consultar características más específicas acerca de dicho flujo.

5.3. DASHBOARD DE CARACTERIZACIÓN DEL FLUJO DE DATOS ENTRE SCADA Y RTU

Este último dashboard aporta información muy específica al cliente acerca de cada flujo de datos, algo que es clave a la hora de poder vislumbrar, por ejemplo, si se ha llegado a establecer o no la conexión TCP entre SCADA y RTU, o si se ha cerrado correctamente la conexión. En la Figura 18 se pueden visualizar todos los paneles que conforman este dashboard.

Mediante este panel se proporciona la opción al cliente de corroborar que ha ocurrido realmente en cada flujo de datos, mediante numerosos detalles adicionales acerca del flujo: IP, MAC, bytes y paquetes enviados, ancho de banda consumido…

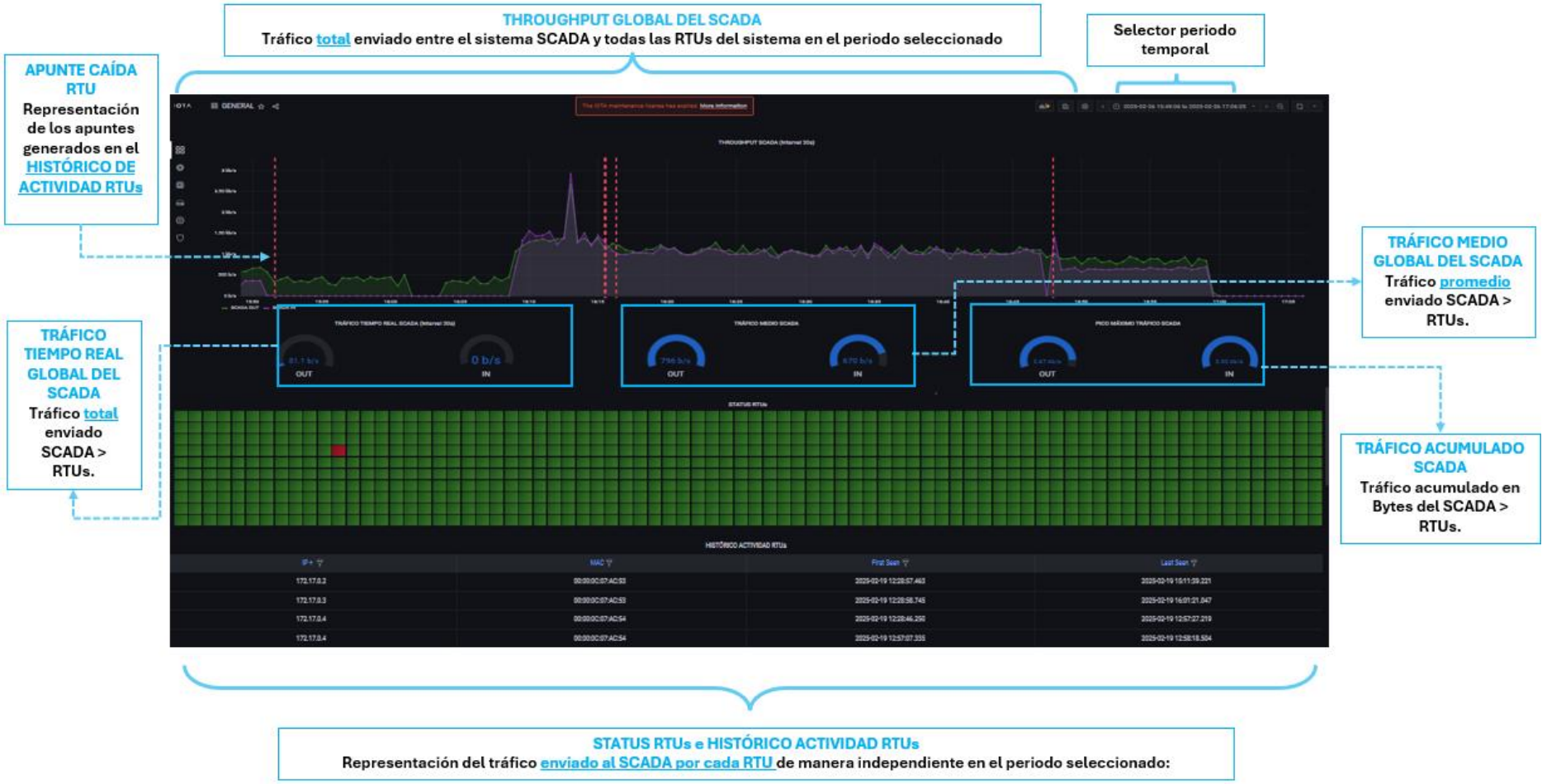


Figura 16 – Dashboard de monitorización del tráfico global del sistema

Figura 17 – Dashboard de monitorización del tráfico de una RTU

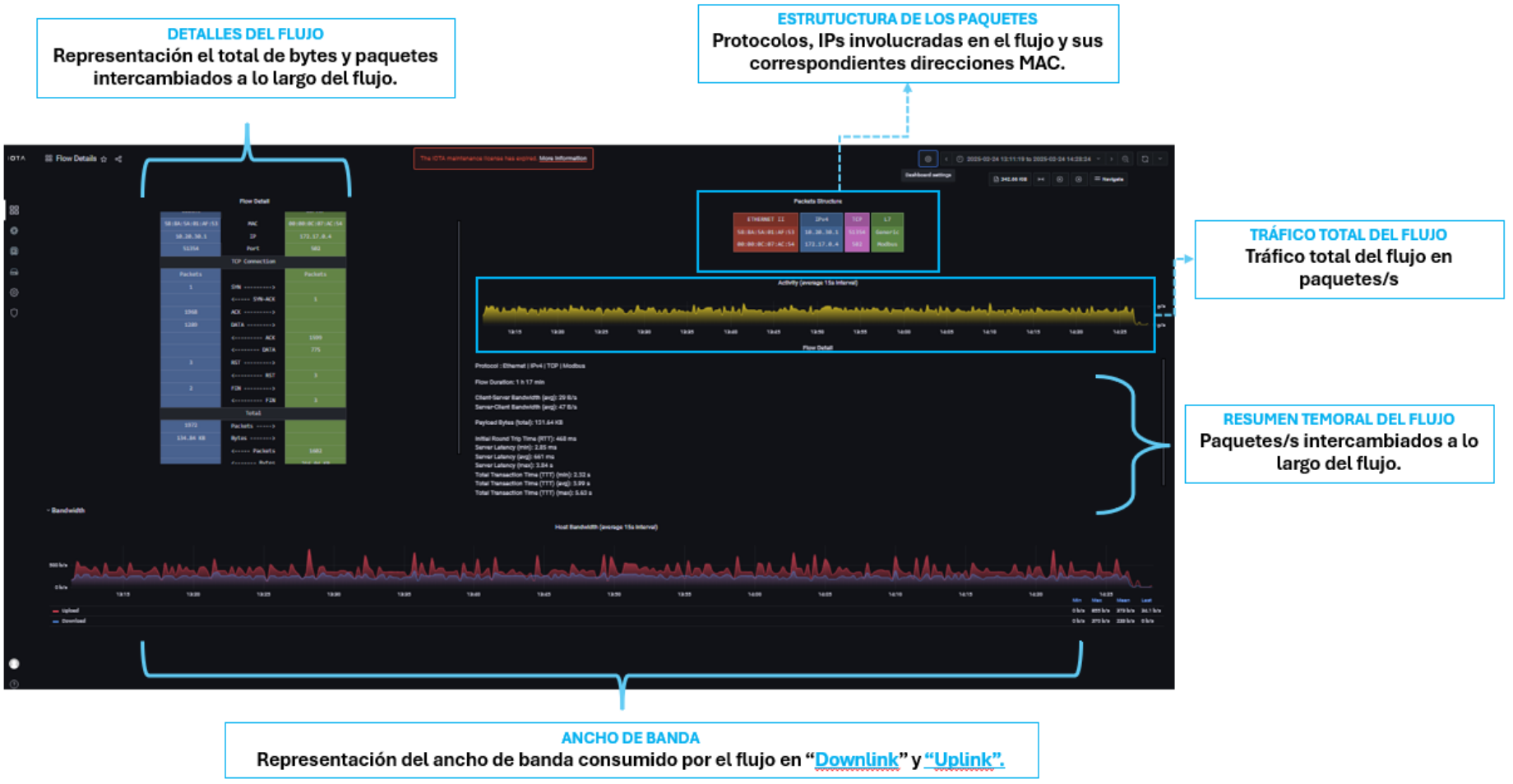


Figura 18 – Dashboard de caracterización de flujo entre SCADA y RTU

6. PRUEBA DE CONCEPTO FINAL DEL PRODUCTO

El último paso para lograr una correcta implementación del IOTA 1G consiste en realizar una prueba de concepto final en una red de comunicaciones críticas TETRA. Para ello, se comenzará con el diseño de una maqueta de pruebas que simula la comunicación IP entre dos SCADAS (principal y redundante), y cuatro RTUs. Como se puede ver en la Figura 19 la conexión de la mayoría de los componentes es realizada mediante Ethernet, salvo la conexión entre la MCBS y el terminal TETRA que es mediante radio TETRA, y la conexión entre terminal TETRA y módem TETRA que es mediante conexión serie.

A continuación, vamos a explicar todas las configuraciones realizadas en los dispositivos presentes en la maqueta de pruebas final, detallando también la función de cada elemento en el proceso de comunicación entre los SCADA y las RTUs del emplazamiento.

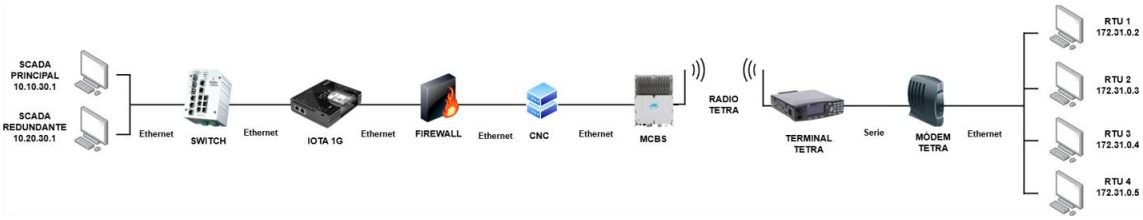


Figura 19 – Esquema de la maqueta final de pruebas

El primer componente de la maqueta son dos equipos que simulan el comportamiento del SCADA gracias a una aplicación de tráfico ModBus instalada en el mismo. A la hora de realizar las consultas a las diferentes RTUs, los SCADA las realizarán mediante el protocolo TCP al puerto 502 y a la IP 172.17.0.X, la cual no es la real de la RTU ya que para el segundo octeto se ha aplicado un NAT para poder diferenciar si la consulta a la RTU se realiza vía TETRA o vía satélite (algo muy común en la redes de comunicaciones críticas para prevenir posibles fallos en la red de comunicación vía TETRA). En la Figura 20 se puede ver como ambos SCADA tienen configurado el gateway por defecto, lo que significa que a la hora de realizar una consulta a cualquier RTU, usarán siempre ese gateway ya que no poseen las rutas para encaminar los paquetes hacia cualquier RTU. Dicha IP asociada al gateway por defecto corresponde a la boca externa del Firewall, que es el encargado de enrutar los paquetes hacia cada RTU.

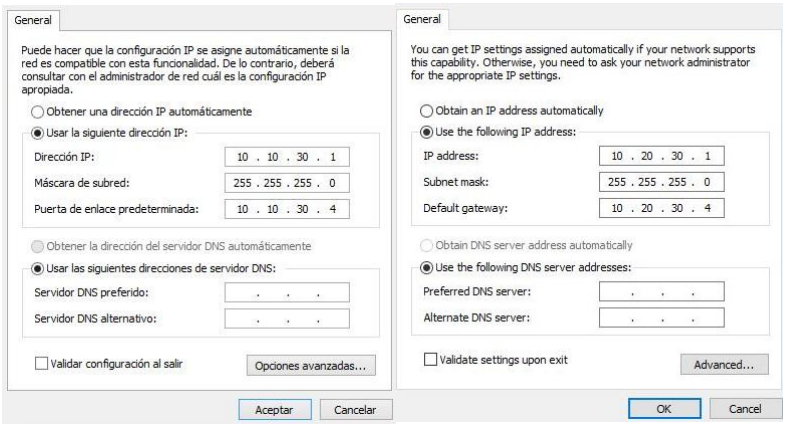


Figura 20 – IP y Gateway SCADA principal y redundante

Por otra parte, en la Figura 21 se pueden observar todos los parámetros configurables para la conexión TCP entre el SCADA y la RTU. Además, muestra un histórico de actividad en el cual se pueden visualizar

todos los paquetes entregados correctamente, o por el contrario, perdidos en el intento de comunicación. Para las demás RTUs la interfaz es exactamente idéntica, únicamente variando la IP de la RTU 1 por la correspondiente IP de las RTUs restantes.

Figura 21 – Interfaz aplicación ModBus RTU 1

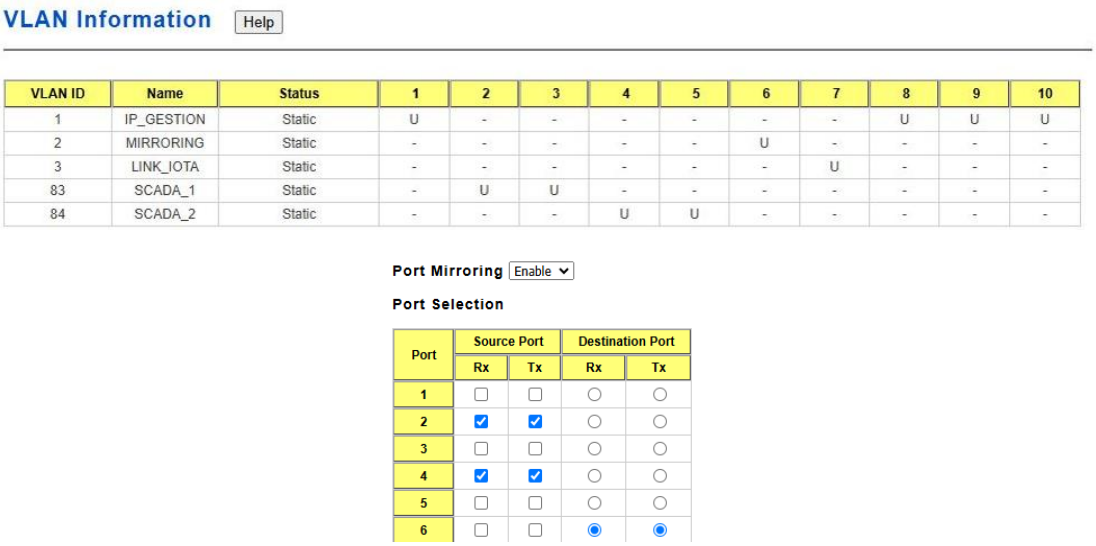
Antes de que el paquete llegué a la boca externa del Firewall, debe atravesar tanto el switch como el IOTA 1G. La principal función de este switch es la de combinar el tráfico proveniente de cada SCADA y agruparlo en un único puerto mediante el protocolo port-mirroring para su posterior análisis por parte del IOTA 1G. De esta forma se evita tener que adquirir un IOTA 1G para analizar el tráfico de cada SCADA, ahorrando costes en la adquisición del producto y en su posterior implementación.

Como se puede observar en la Figura 22, tenemos diferentes VLANs asociadas a los puertos del Switch:

- VLAN 1 (Puertos 1, 8, 9 y 10): asociada a la gestión del dispositivo, permite acceder a la IP del dispositivo para realizar labores de gestión de este, no se ejerce ninguna labor de operación en estos puertos.
- VLAN 2 (Puerto 6): vinculada a la realización del port-mirroring de las VLANs 83 y 84. En la Figura 22, se puede ver como todo el tráfico que transmitan y reciban los puertos 2 y 4, es enviado al puerto 6 para su posterior análisis. Este puerto se conecta con el puerto 1 de monitorización del IOTA 1G.
- VLAN 3 (Puerto 7): realiza la función de interconexión interna del IOTA 1G, ya que si el segundo puerto de monitorización queda en el aire, el dispositivo no es capaz de capturar correctamente dicho tráfico.
- VLAN 83 (Puertos 2 y 3): encargada de recibir el tráfico IP por parte del SCADA principal y enviarlo hacia el Firewall.
- VLAN 84 (Puertos 4 y 5): encargada de recibir el tráfico IP por parte del SCADA redundante y enviarlo hacia el Firewall.

En cuanto al IOTA 1G, conectaremos a su puerto de gestión al ordenador encargado de acceder mediante conexión IP al GRAFANA del dispositivo. Como para esta prueba el ordenador encargado de acceder al GRAFANA del dispositivo se encontraba en la misma subred que el IOTA 1G, no se necesitó de ninguna

configuración. En caso de no pertenecer a la misma subred, valdría con configurar el gateway del IOTA 1G como el gateway de la subred en donde se ubica. Por otro lado, más adelante quedarán especificadas más detalladamente todas las conexiones realizadas en el switch, para facilitar su comprensión.



VLAN Information Help

VLAN ID	Name	Status	1	2	3	4	5	6	7	8	9	10
1	IP_GESTION	Static	U	-	-	-	-	-	-	U	U	U
2	MIRRORING	Static	-	-	-	-	-	U	-	-	-	-
3	LINK_IOTA	Static	-	-	-	-	-	-	U	-	-	-
83	SCADA_1	Static	-	U	U	-	-	-	-	-	-	-
84	SCADA_2	Static	-	-	-	U	U	-	-	-	-	-

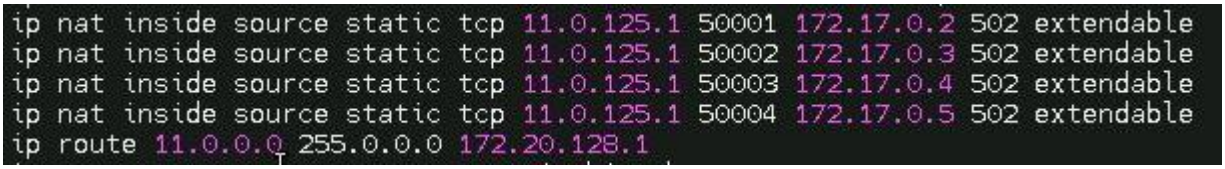
Port Mirroring Enable

Port Selection

Port	Source Port		Destination Port	
	Rx	Tx	Rx	Tx
1	☐	☐	○	○
2	☑	☑	○	○
3	☐	☐	○	○
4	☑	☑	○	○
5	☐	☐	○	○
6	☐	☐	◉	◉

Figura 22 – Configuración VLANs Switch y port-mirroring

Tras atravesar el switch y el IOTA 1G, los paquetes llegan al Firewall de la red. Aquí, se aplica un nuevo NAT a los paquetes tal y como se puede visualizar en la Figura 23. Por ejemplo, para la primera línea, tenemos que todos los paquetes que tengan como dirección IP destino 172.17.0.2 y puerto destino 502; se convierte a la IP 11.0.125.1 con el puerto 50001. De la misma forma, se realiza para la RTUs restantes. Al aplicar el NAT, se le asigna la misma IP a todas las RTUs debido a que es la IP PDP que el módem TETRA le asigna al ordenador en donde están ubicadas las cuatro RTUs de esta maqueta. Se asigna un puerto diferente a cada RTU para poder diferenciarlas entre sí.



```
ip nat inside source static tcp 11.0.125.1 50001 172.17.0.2 502 extendable
ip nat inside source static tcp 11.0.125.1 50002 172.17.0.3 502 extendable
ip nat inside source static tcp 11.0.125.1 50003 172.17.0.4 502 extendable
ip nat inside source static tcp 11.0.125.1 50004 172.17.0.5 502 extendable
ip route 11.0.0.0 255.0.0.0 172.20.128.1
```

Figura 23 – Configuración NAT Firewall

Una vez aplicado el NAT a las diferentes RTUs y configurado el protocolo NetFlow, los paquetes con dirección IP destino 11.0.125.1 son enrutados al CNC (Computer Numerical Control) de la red TETRA, el cuál cumple la función de Gateway PDP, es decir, es el encargado de encaminar el tráfico PDP a todos los terminales registrados a lo largo de la red. El CNC envía la consulta hacia la MCBS en la que se encuentra registrado el terminal TETRA correspondiente a la dirección IP de destino del paquete. La MCBS transmite vía radio TETRA el paquete hacia el terminal TETRA correspondiente y éste lo encamina hacia el módem TETRA.

Ya en el módem TETRA, se realiza el último NAT de la comunicación, el cual intercambia la dirección IP origen del SCADA por su propia dirección IP para que la RTU puede contestar directamente al módem TETRA ya que están dentro de la misma subred. En la Figura 24 se puede visualizar como la IP que se asigna como dirección IP origen es la 172.31.0.1, mientas que, la IP PDP que el módem asigna al ordenador es la 11.0.125.1 como ya hemos comentado previamente.

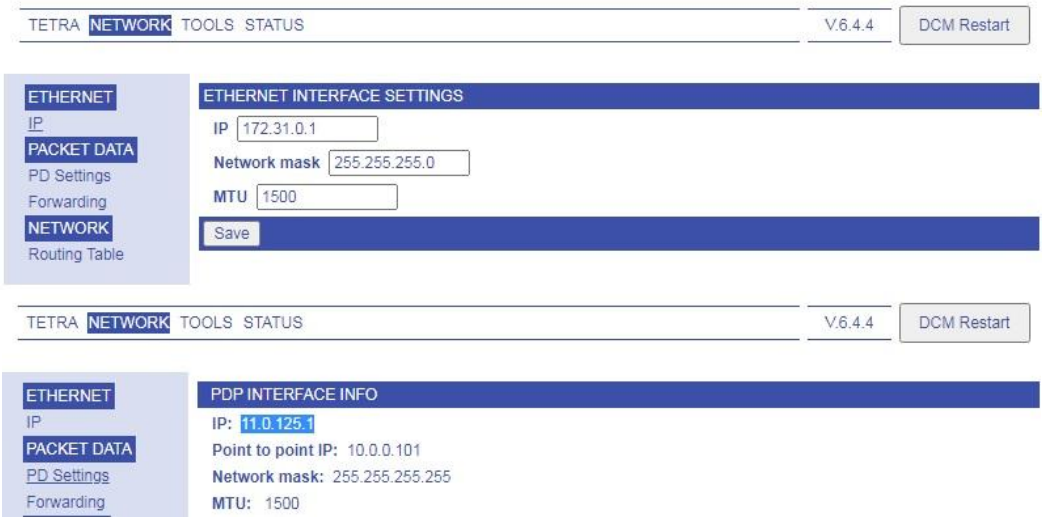


Figura 24 – IP e IP PDP Módem TETRA

Junto con el NAT también se realiza la configuración para encaminar correctamente los paquetes hacia las RTUs. En la Figura 25, se establece que todos los paquetes procedentes de la IP 11.0.125.1 con su puerto asociado, serán enviados a la IP 172.31.0.X con el puerto 502.

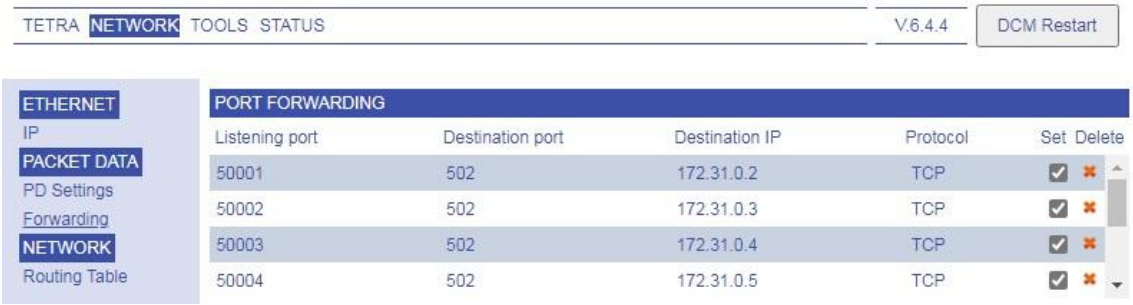


Figura 25 – Configuración encaminamiento de los paquetes del Módem TETRA

Finalmente, solo nos queda configurar las cuatro RTUs. Para ello, utilizamos de la misma forma que para ambos SCADA, un software que simula el comportamiento real de una RTU en un sistema de comunicaciones críticas. En la Figura 26 se puede observar cómo únicamente es necesario asignar el puerto e IP correspondientes a la RTU. Cada vez que la RTU reciba una consulta por parte de cualquier SCADA, se iluminará en verde el círculo situado a la derecha de "Run" para poder saber si se están recibiendo correctamente los paquetes sin necesidad de otra herramienta.

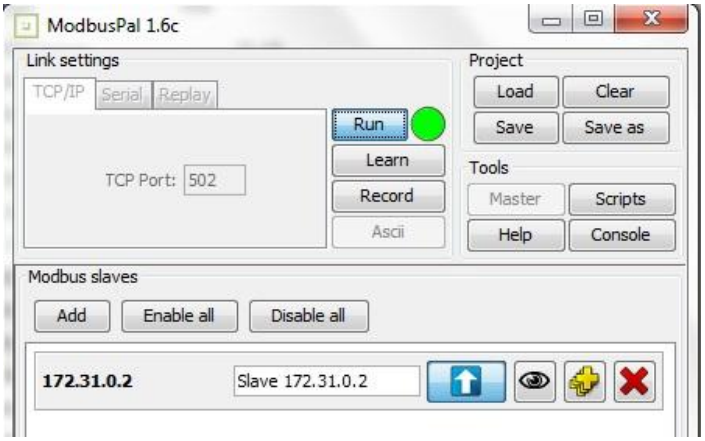


Figura 26 – Interfaz software RTU 1

Adicionalmente, se tendrán que configurar las cuatro IPs correspondientes a cada RTU para poder ejecutar el software para cada una de ellas. Ya que el módem TETRA modifica la dirección IP origen del paquete por la suya, no se necesitará especificar ningún Gateway debido a que la RTU no necesita ninguna ruta extra para responder a un IP que se encuentra dentro de su misma subred. En la Figura 27 queda detallada la configuración IP de todas las RTUs en el equipo.

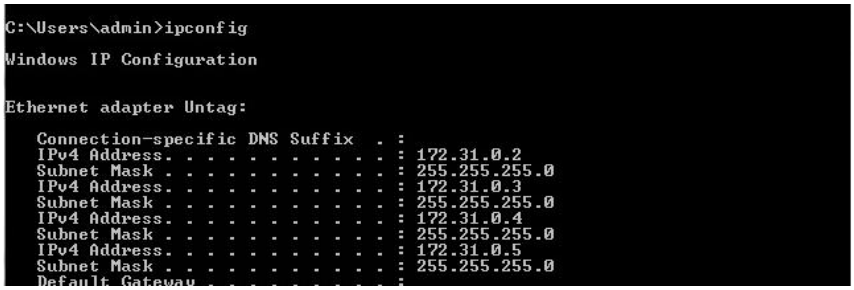


Figura 27 – Configuración IPs para cada RTU

Una vez configurados todos los elementos de la maqueta final de pruebas, las consultas por parte de ambos SCADAS serán recibidas correctamente por parte de las distintas RTUs. En cuanto a la respuesta por parte de la RTU hacia el SCADA, se realizarán los mismos NATs y configuraciones de direccionamiento de los paquetes de forma inversa a la explicada anteriormente.

El resultado final de la implementación y configuración de esta maqueta de pruebas se puede ver en la Figura 16, en donde se pueden ver que se han generado los cuatro cuadros correspondientes a cada RTU que los SCADA están encuestando, y en la Figura 17 y Figura 18, en donde se puede ver el comportamiento específico de una RTU durante el intervalo de tiempo seleccionado.

Gracias a la implementación de esta maqueta final de pruebas, se pudieron llevar a cabo numerosas pruebas relacionadas con la programación de los diferentes gráficos y KPIs de cada dashboard. Principalmente, se hicieron numerosas pruebas que verificaran el correcto funcionamiento de cada KPI, pues que cada KPI programado exprese realmente lo que está ocurriendo en cada instante de tiempo al cliente es clave en un módulo de monitorización.

Especialmente, me he centrado en realizar pruebas relacionadas con la pérdida intencionada de los paquetes enviados por el SCADA hacia una RTU concreta. Por ejemplo, con únicamente inhabilitar la conectividad entre el switch y el firewall somos capaces de que el IOTA 1G sea capaz de capturar el

paquete en DL pero este no sea capaz de llegar a la RTU, provocando así que el paquete en UL no sea capaz de llegar nunca al SCADA. Con esta simple acción conseguimos simular a la perfección la situación más típica que puede ocurrir en campo: el SCADA hacia una pregunta a una RTU, y ésta por alguna razón u otra no es capaz de enviar la repuesta hacia el SCADA.

También se llevaron a cabo diferentes pruebas relacionadas con la aparición de alertas, el diseño de cada KPI, la configuración de las variables de cada dashboard, el valor del umbral que dispara la alarma, el ajuste de los detalles a mostrar para cada flujo o la configuración de diferentes aspectos de cada dashboard como el tiempo de actualización o la selección del periodo temporal más acorde para su visualización.

Como he dicho antes, el principal objetivo de todas estas pruebas es verificar el comportamiento de todos los KPIs programados. Es por ello por lo que, durante las pruebas realizadas se comprobó que las alertas relacionadas con algún comportamiento anómalo por parte de cualquier RTU de la infraestructura se notificaban cuando es debido. Es decir, se corroboró que en el producto final a entregar al cliente no existía ninguna posibilidad de aparición de algún falso positivo relacionado con el estado de cada RTU de la infraestructura.

Por otro lado, se cronometró el tiempo en el que sistema notificaba la caída de una RTU, con el objetivo de poder saber cuánto es el tiempo que transcurre desde que la RTU está inactiva hasta que el módulo de monitorización es capaz de notificar dicha caída.

Tanto la aparición de un falso positivo, como el tiempo hasta la notificación al cliente de la caída de la RTU, son aspectos vitales a tener en cuenta en una red de comunicaciones para misión crítica pues se precisa de la máxima seguridad y de tiempos de reacción muy cortos a la hora de solventar algún percance que puede poner en riesgo la vida de trabajadores o civiles. Con todas las pruebas realizadas nos aseguremos de que el módulo de monitorización cumple su función con la máxima eficacia posible.

Para concluir este apartado, vamos a mostrar diferentes imágenes acerca de la conectividad de los diferentes elementos empleados para el montaje de la maqueta final de pruebas. Comenzamos con Figura 28 en donde podemos ver todos los elementos que la conforman.

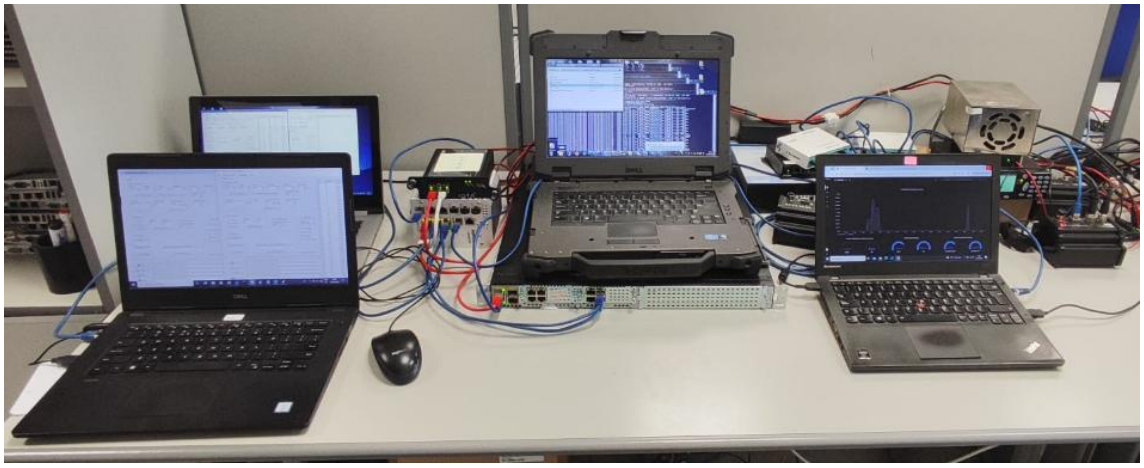


Figura 28 – Maqueta final de pruebas

Debido a la cantidad de cables existentes en la maqueta final, la Figura 29 muestra más detalladamente como se ha llevado a cabo dicha conexión. Quiero destacar que, la conectividad llevada a cabo ha sido resultado de la infraestructura ya existente en el cliente final, con el objetivo principal de abaratar costes y de cumplimentar las exigencias de seguridad demandadas por el cliente final. Además, la conectividad

de todos los elementos se ha llevado de esta forma para permitir utilizar un único IOTA 1G para la monitorización de datos del SCADA principal y redundante. Con esto conseguimos abaratar costes, evitando la adquisición de un segundo IOTA 1G.

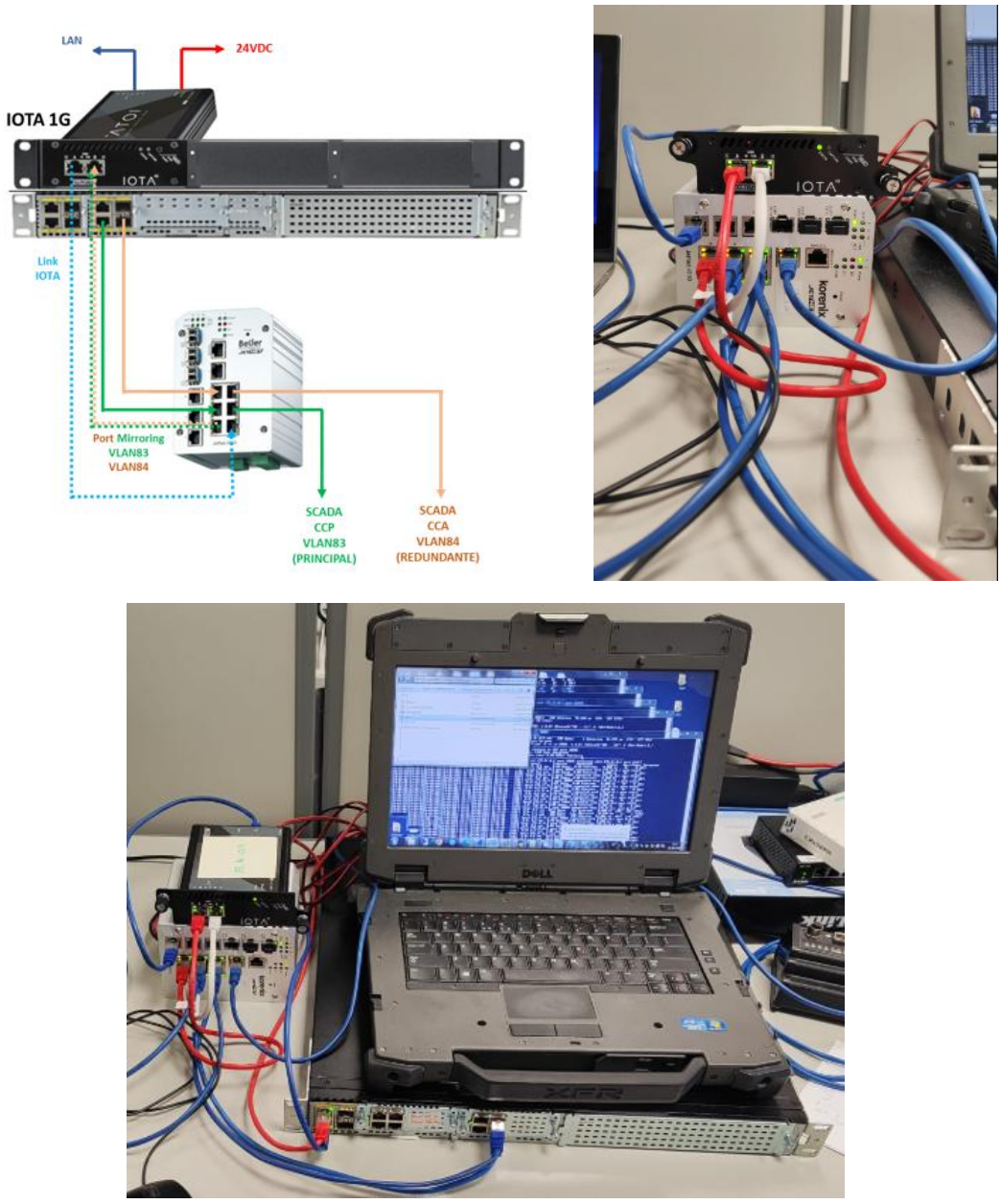


Figura 29 – Conectividad entre los diferentes dispositivos de la maqueta final

En la Figura 30 de podemos ver más en detalle la conexión realizada entre el módem y el terminal TETRA, así como en la Figura 31 se puede observar el montaje del IOTA 1G en el rack de 19" que será instalado en la infraestructura del cliente.

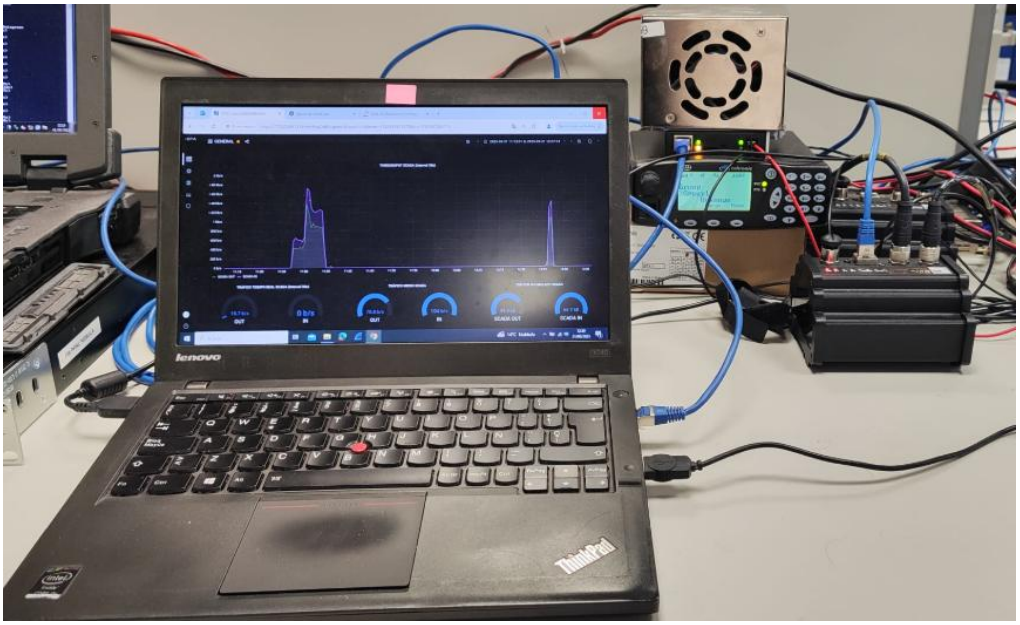


Figura 30 – Módem y terminal TETRA

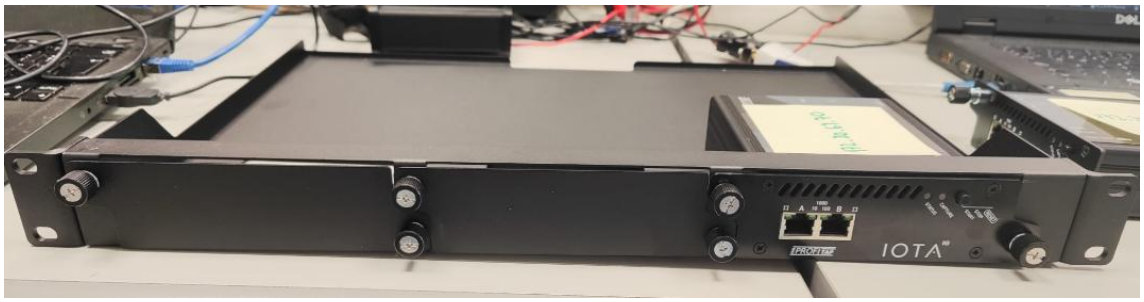


Figura 31 – Instalación final IOTA 1G en rack

Finalmente, vamos a ilustrar la conectividad actual del cliente y la final, una vez instalado el IOTA 1G. En la Figura 32 se muestra la conectividad inicial del cliente, mientras que en la Figura 33 de muestra la conexión lógica una vez instalado el IOTA 1G. Por último en la Figura 34 se puede observar la instalación real que se llevará tanto en el servidor principal como en el redundante.

Figura 32 – Conectividad inicial del cliente

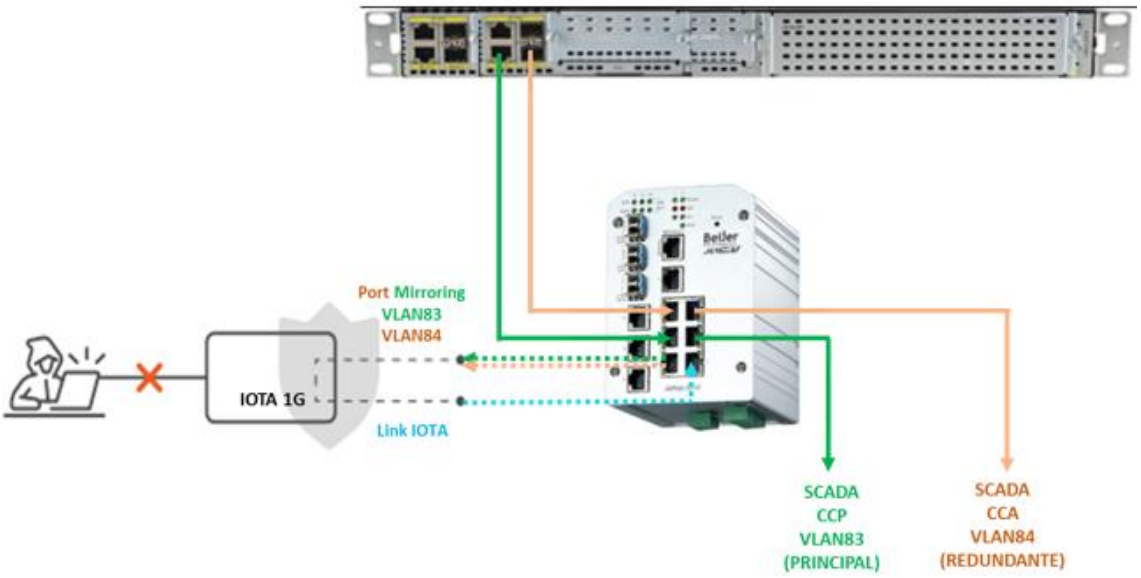


Figura 33 – Conectividad lógica final del cliente

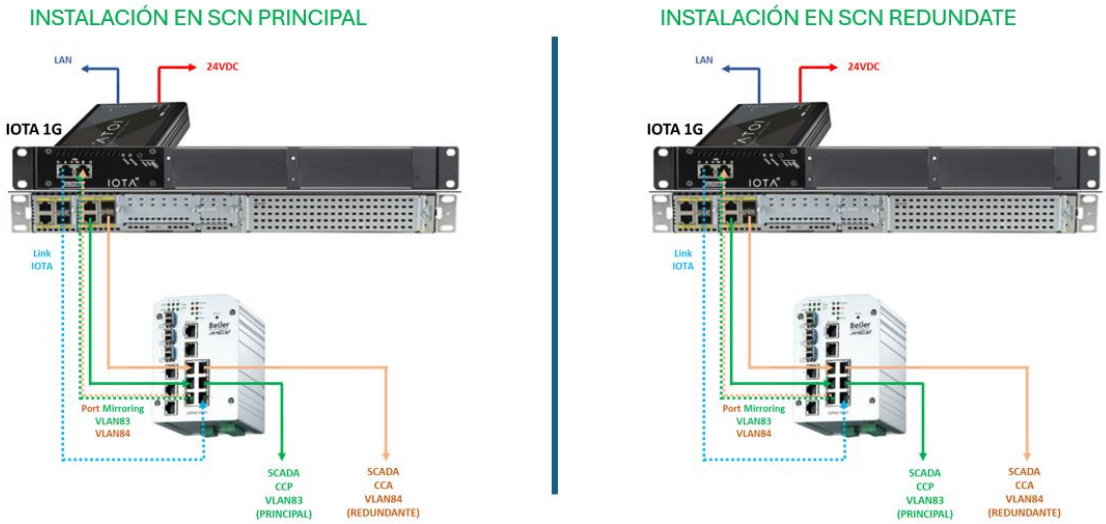


Figura 34 – Instalación real en el servidor principal y redundante

7. CONCLUSIONES DEL PROYECTO

A lo largo de este proyecto he podido abordar con profundidad un problema real y existente en las compañías dedicadas al despliegue de infraestructuras de radiocomunicación para misión crítica, el cual radica en la falta de conocimiento acerca del tráfico de Datos de Operación que circula entre los distintos elementos de una infraestructura basada en el sistema SCADA.

Para remediar dicho problema se ha optado por la implementación de un módulo de monitorización mediante el dispositivo IOTA 1G, el cual mediante GRAFANA, ha permitido no sólo solventar la falta de visibilidad del tráfico de Datos de Operación que atraviesa la infraestructura, sino también abrir nuevas posibilidades de análisis, supervisión y visualización de todos los datos que atraviesan una red de infraestructura para misión crítica. Este dispositivo representa una solución no intrusiva y altamente eficaz en sistemas donde la interrupción del servicio puede suponer consecuencias críticas para la población.

Gracias a la implementación de este dispositivo el cliente será capaz de visualizar en tiempo real el estado de su infraestructura, así como en tiempo pasado, algo imprescindible a la hora de generar, por ejemplo, un informe de resultados acerca de la disponibilidad de la infraestructura durante el último mes.

En definitiva, mediante la incorporación del IOTA 1G a una red de infraestructura para misión crítica, no sólo somos capaces de visualizar en tiempo real lo que está sucediendo en dicha infraestructura, sino que realmente somos capaces de ser conscientes en todo de momento de por qué un paquete no ha llegado a donde debería y poder obtener el motivo que se lo ha impedido. Poder evitar la incertidumbre del por qué ha sucedido un comportamiento anómalo en tu red es la principal característica del módulo de monitorización llevado a cabo durante este proyecto, algo que no todas las redes de comunicaciones son capaces de implantar.

7.1. LECCIONES APRENDIDAS Y TAREAS LLEVADAS A CABO

Durante el desarrollo del proyecto he podido adquirir numerosos conocimientos esenciales relacionados con el funcionamiento de las redes de comunicaciones críticas, especialmente de aquellas basadas en el estándar TETRA. Gracias al diseño e implementación de las maquetas de pruebas utilizadas para realizar numerosas pruebas con el producto final, he podido conocer de primera mano todos los elementos que la componen, como deben configurar e interconectar entre sí.

Por otro lado, he asimilado las diferentes características de los principales protocolos y tecnologías que actualmente se utilizan en el análisis de datos a gran escala. Esto me ha permitido comprender sus ventajas y limitaciones, lo cual ha sido clave a la hora de la toma de decisión del producto final.

También he aprendido el funcionamiento y organización de una base de datos, así como la programación de sentencias basadas en el lenguaje SQL, ya que para poder diseñar un KPI en GRAFANA es imprescindible tener los conocimientos necesarios sobre el diseño de la base de datos y las sentencias a utilizar para poder mostrar los datos requeridos por el cliente.

Asimismo, he profundizado en el diseño e integración de arquitecturas de monitoreo invisibles a la red de comunicación (TAPs), puesto que una de las mayores complicaciones del proyecto ha sido la de llevar a cabo la incorporación del IOTA 1G a la infraestructura existente del cliente.

Sin embargo, el principal reto de este proyecto ha residido en el diseño y posterior optimización del módulo de monitorización basado en GRAFANA. Como se puede ver en la Figura 35, la configuración del módulo de monitorización ha sido la tarea en la que más tiempo se ha invertido. Esto se debe principalmente a las exigencias del cliente acerca de los diferentes dashboards y KPIs que precisaban

visualizar. La programación y solución de los diferentes errores que iban surgiendo conforme se avanzaba en la configuración del módulo de monitorización ha sido lo más complejo de abordar durante todo el proyecto.

Quiero destacar también que, además de todas las tareas de la Figura 35, se han llevado a cabo infinidad de reuniones (casi diariamente) durante todo el proyecto para tratar diferentes aspectos como la elección del producto final, la integración del IOTA 1G en la infraestructura del cliente, la puesta en común de los avances o la optimización de los dashboards a presentar al cliente.

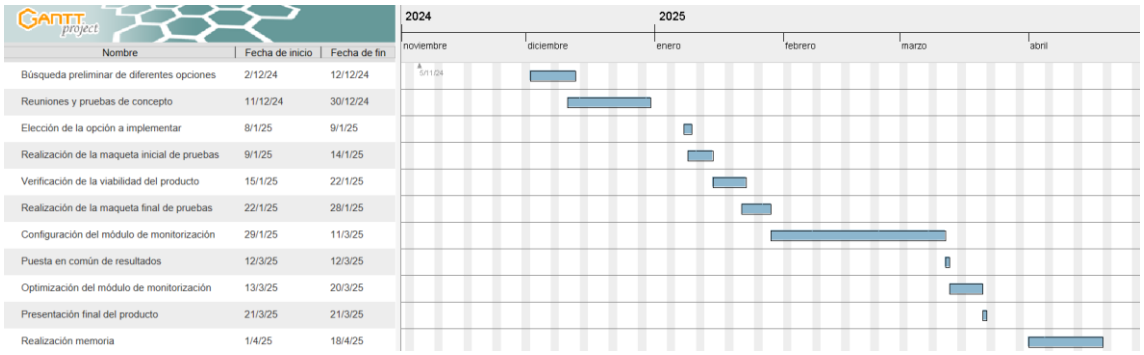


Figura 35 – Diagrama de Gantt de las tareas llevadas a cabo durante el proyecto

7.2. IDEAS A FUTURO

El trabajo realizado durante este proyecto constituye una base sólida para futuras implementaciones en otros sectores críticos como son el ferroviario o el energético. Como ya he comentado anteriormente, el alcance real de este proyecto es el de poder ofrecer el módulo de monitorización de Datos de Operación como un producto final, el cual puede ser utilizado en diferentes sectores críticos.

Actualmente, el módulo de monitorización ha sido instalado en una compañía referente dedicada a la gestión, almacenamiento y abastecimiento de gas natural. Debido a que el producto ha sido probado únicamente en maquetas de pruebas, inconvenientes relacionados con el tratamiento de los Datos de Operación surgirán una vez haya sido incorporado a la infraestructura del cliente. No obstante, tras haber solucionado dichos inconvenientes, todo el trabajo llevado a cabo durante este proyecto no habrá sido en vano pues ofrecerá al cliente el conocimiento del estado de su infraestructura, además de suponer el punto de partida para la implementación del módulo de monitorización en otras compañías dedicadas a otras actividades críticas que precisen el mismo servicio.

BIBLIOGRAFÍA

[1] *SCADA – Supervisión, control y adquisición de datos de energía y acueducto*

https://wmsas.co/site/supervision-control-y-adquisicion-de-datos-de-energia-y-acueducto/

[2] *Infraestructura sistema SCADA*

https://www.researchgate.net/figure/Remote-Sites-Connected-to-SCADA-Network-System-15-IMPLEMENTING-IP-SCADA-NETWORK-The_fig3_369905486

[3] *Arquitectura protocolo NetFlow*

https://repository.dinamika.ac.id/id/eprint/7068/1/4-Jurnal-Aisindo-Slamet-revisi-updated.pdf

[4] *¿Qué es el port-mirroring y como configurarlo?*

https://www.fs.com/es/blog/port-mirroring-explained-basis-configuration-and-fa-qs-5160.html

[5] *¿Qué es un sistema SCADA y para qué sirve?*

https://mesautomation.com/que-es-un-sistema-scada-y-como-puede-ayudar-a-tu-fabrica/

[6] *Conceptos básicos del protocolo SNMP*

https://www.manageengine.com/es/network-monitoring/what-is-snmp.html#:~:text=SNMP%20es%20uno%20de%20los,administraci%C3%B3n%20de%20red%20(NMS).

[7] *¿Qué es NetFlow?*

https://www.manageengine.com/latam/netflow/que-es-netflow.html

[8] *Acerca de NetFlow*

https://www.watchguard.com/help/docs/help-center/es-xl/Content/en-US/Fireware/basicadmin/netflow_about.html?TocPath=Monitorear%20el%20Tr%C3%A1fico%20de%20Red%7CAnalizar%20el%20Tr%C3%A1fico%20de%20Red%20con%20NetFlow%7C_____0

[9] *¿Qué es la MPLS?*

https://www.hpe.com/es/es/what-is/mpls.html

[10] *ClickHouse: ¿Qué es y cómo funciona?*

https://vasexperts.com/es/resources/glossary/clickhouse/

[11] *Comunicaciones TETRA*

https://www.redestelecom.es/especiales/comunicaciones-tetra/

[12] *Modos de funcionamiento TETRA*

https://bzgz.blogspot.com/2014/12/funcionalidad-gateway-en-los-equipos.html

[13] *Constelación π/4 – DQPSK*

https://es.m.wikiversity.org/wiki/Archivo:Pi-by-4-QPSK_Gray_Coded.svg

[14] *Estructura trama TDMA*

https://www.researchgate.net/figure/An-example-of-TDMA-frame-structure-To-prevent-unnecessary-power-consumption-each-node_fig3_269654078

[15] *Espectro UL y DL TETRA*

https://poliformat.upv.es/access/content/group/OCW_6511_2010/Unidad%20Did%C3%A1ctica%201.%20Telefon%C3%ADa%20M%C3%B3vil%20Privada/1.2.TETRA.pdf

[16] *ETSI EN 300 392-2 V3.8.1. EUROPEAN STANDARD. Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI).*

https://www.etsi.org/deliver/etsi_en/300300_300399/30039202/03.08.01_60/en_30039202v030801p.pdf

ANEXO A: TÉRMINOS Y DEFINICIONES TÉCNICAS

- **SCADA**: un sistema SCADA, acrónimo de Supervisory Control and Data Acquisition, es una aplicación basada en plataformas de software que generalmente reside en servidores. Su función principal es interactuar con dispositivos de control industrial de procesos, como válvulas, motores o sensores, mediante dispositivos de adquisición de datos o controladores lógicos programables (PLC y DCS). Estos dispositivos utilizan protocolos de comunicación para intercambiar datos y comandos con la interfaz de visualización del SCADA en tiempo real, a través de una red de control.

- **TETRA (Terrestrial Trunked Radio)**: Estándar de radio digital definido por el Instituto Europeo de Normas de Telecomunicaciones (ETSI). Proporciona comunicaciones de datos y voz seguras, fiables y eficientes, ofreciendo funcionalidades específicas para usuarios críticos como llamadas de grupo, de emergencia, comunicaciones críticas, geolocalización…

- **NMS (Network Management System)**: Sistema de gestión de red basado en la arquitectura cliente-servidor y en el estándar de la industria FCAPS (fallos, configuración, contabilización, rendimiento y seguridad), permite configurar, monitorizar, y comprobar el funcionamiento de todos los componentes de la red, y gestionar de forma unificada los suscriptores.

- **TCP/IP (Transmission Control Protocol/Internet Protocol)**: Protocolo de enlace de datos que determina las normas que permiten la transmisión de datos a través de redes, como Internet. Es el estándar global para las comunicaciones de Internet.

- **UDP (User Datagram Protocol)**: Protocolo de comunicación en la capa de transporte del modelo TCP/IP que permite la transmisión de datos sin establecer conexión previa entre emisor y destinatario.

- **Packet-Data Protocol (PDP):** Protocolo utilizado en redes de comunicaciones y redes móviles para proporcionar la entrega de datos, permitiendo el intercambio de información entre dispositivos y sistemas (paquetes IP).

- **Payload:** Conjunto de datos transmitidos útiles de un paquete, que se obtiene al excluir cabeceras, metadatos o información de control del propio paquete.

- **Network Address Translation (NAT):** Proceso que consiste en la modificación de las direcciones IP de los paquetes que atraviesan, generalmente, un router o un firewall.

- **NAT Masquerade:** Tipo de NAT que se emplea principalmente para proporcionar acceso a Internet a IP privadas mediante una única dirección pública.

- **Multiprotocol Label Switching (MPLS)**: Tecnología de red que ofrece un enrutamiento de paquetes mediante el uso etiquetas en lugar de direcciones IP. Ampliamente utilizado en las redes de telecomunicaciones, proporciona un manejo del tráfico más eficiente.

- **IPsec (Internet Protocol Security):** Conjunto de protocolos diseñados para garantizar la comunicación segura entre dispositivos a través de Internet o cualquier red pública. También es un método frecuente para autenticar el tráfico y proteger los datos dentro de una red privada.

- **KPI (Key Performance Indicator):** Serie de métricas utilizadas para sintetizar la información sobre la eficacia y la productividad de los diferentes componentes de una red como medida para analizar y evaluar su funcionamiento.

- **SCN (Switching Central Node):** Nodo central de la red en el que se aloja el controlador central de la red (CNC), el cual gestiona en tiempo real toda la señalización de control, permisos y prioridades de todas las llamadas de voz o datos de cada equipo de la red TETRA.

- **MCBS (Multi Carrier Base Station):** Repetidor radio TETRA instalada en la estación base (EB) que proporciona cobertura radio TETRA a una determinada área geográfica.

- **RTU (Remote Terminal Unit):** Dispositivo diseñado para el telecontrol de instalaciones, en particular, de aquellas instalaciones aisladas que requieren un refuerzo en la gestión de control. Su función principal es recopilar datos de sensores y dispositivos, procesarlos y transmitirlos a un sistema centralizado para su análisis y control.

- **Archivo PCAP:** Archivo que almacena datos de red capturados en forma de paquetes. Son comúnmente utilizados para analizar el tráfico de red, depurar problemas, realizar auditorías o investigar incidentes.

ANEXO B: SISTEMA DE COMUNICACIONES CRÍTICAS TETRA

TETRA [16], siglas en inglés de Terrestrial Trunked Radio, es un sistema y estándar de comunicación digital desarrollado por el Instituto Europeo de Normas de Telecomunicaciones. TETRA se utiliza para brindar una comunicación segura, confiable y eficiente en áreas críticas de nuestra sociedad, donde la continuidad del servicio es vital. Desde su establecimiento en la década de 1990, los sistemas TETRA se han ido implementando en más de 120 países. Actualmente, se ha implementado en policía, ambulancias, servicios de rescate, transportes, energía, y muchas más áreas comerciales y críticas.

De esta forma, se envían mensajes de voz y datos al mismo tiempo, lo que crea una oportunidad para operar servicios de voz y servicios de datos al mismo tiempo. El subsistema acepta la comunicación unidireccional, bidireccional y de difusión. El sistema opera otras funciones originales, como el botón para hablar PTT (Push To Talk) que permite establecer la comunicación de manera inmediata, lo que es vital en situaciones de emergencia.

Por otra parte, TETRA cuenta con una serie de ventajas y características clave que hay que conocer para tener una idea más clara de en qué consiste este estándar y, sobre todo, para tener en cuenta cómo se puede aplicar dicho estándar en una infraestructura de comunicaciones críticas:

- Infraestructura de red propia, es decir, está completamente diferenciada de las redes móviles del país en donde esté ubicada la red de comunicaciones.
- Opción de establecer la red de comunicaciones con únicamente terminales en caso de que exista algún inconveniente en las comunicaciones.
- Sistema digital más modernizado que GSM (Global System for Mobile Communications).
- Ofrece una calidad de sonido mayor que GSM puesto permite una mayor compresión de datos.
- Mejor aprovechamiento del canal debido a que permite las comunicaciones semidúplex (hacer uso de canales desocupados).
- Tiene una mayor saturación, por lo que se encarga de garantizar una capacidad por defecto superior a los canales de comunicación convencionales.
- Ofrece comunicaciones grupales.
- Posee encriptación en sus comunicaciones de voz y datos.

Una vez introducido el estándar TETRA, vamos a pasar a explicar más detalladamente sus características tecnológicas. Comenzamos mediante los dos modos de funcionamiento que proporciona TETRA, que se pueden observar en la Figura 36:

1. *Trunked Mode Operation (TMO):* el modo troncalizado es el modo básico de funcionamiento de la red TETRA. Se precisa de la presencia de una o más estaciones base para realizar la comunicación con los diferentes móviles para prestar un servicio de voz o datos, usando el aire como interfaz de comunicación entre estación base y móvil.
2. *Direct Mode Operation (DMO):* este modo de funcionamiento permite que los terminales TETRA se comuniquen entre si independientemente del área de cobertura de la red, es decir, son capaces de comunicarse entre sí sin necesidad de la estación base. Es el uso más frecuente de

comunicación TETRA debido a que facilita una extensión de red para llevar a cabo comunicaciones en ubicaciones geográficas con poca cobertura.

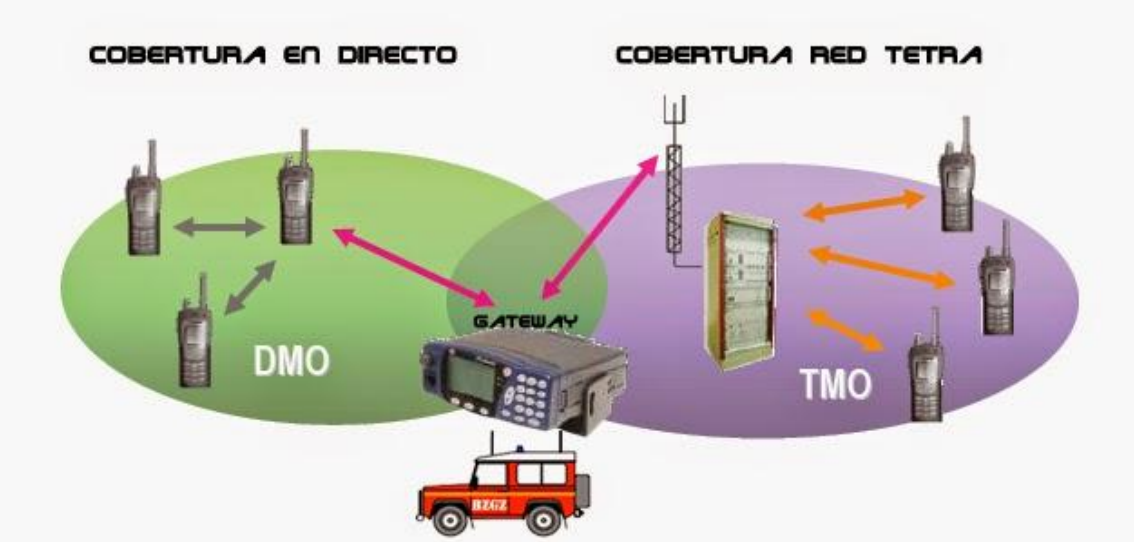


Figura 36 – Modos de funcionamiento TETRA [12]

El primer estándar TETRA que se desarrolló por parte del ETSI recibió el nombre de *TETRA Voice Plus Data (V+D),* el cual marcó el comienzo del desarrollo de la tecnología TETRA. El paso de los años ha provocado la derivación del primer estándar en su actual nombre, *TETRA Release I*, cuyo objetivo es el de continuar con el desarrollo tecnológico del estándar para poder garantizar las nuevas necesidades por parte de los clientes.

Proseguimos comentando algunas de las principales características del estándar *TETRA Release I:*

1. Modulación π/4 - DQPSK *(Differential Quaternary Phase-Shift Keying)* junto con un filtro modulador tipo coseno realzado y un factor de *roll-off* en torno 0.35. Para las modulaciones en fase, canalización de 25 kHz, la tasa de modulación es de 36 kbit/s. En la Figura 37 podemos observar la constelación de los símbolos de dicha modulación:

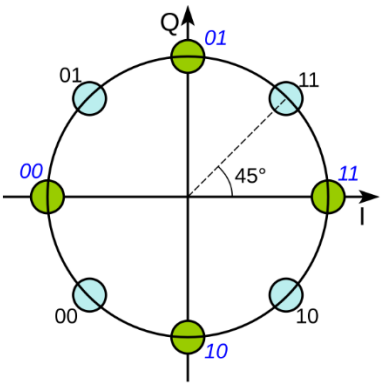


Figura 37 – Constelación modulación π/4 – DQPSK [13]

2. TDMA (*Time Division Multiple Access*): Respecto al esquema de acceso, TETRA emplea la técnica TDMA, organizando cada portadora en cuatro canales físicos o ranuras temporales. En un sistema TDMA, cada usuario recibe asignados determinados intervalos de tiempo (*timeslots*) en los que

puede transmitir y recibir datos, optimizando así el uso del canal radioeléctrico. En la Figura 38 podemos ver la estructura de una trama TDMA:

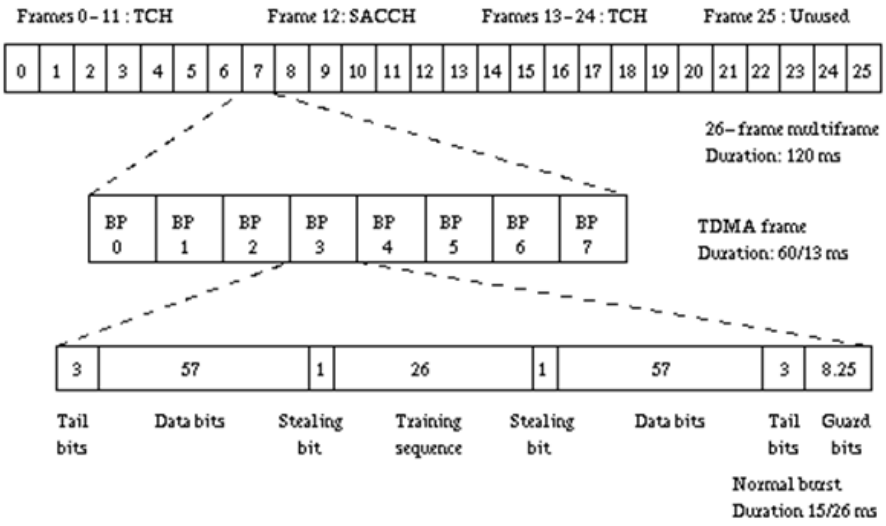


Figura 38 – Estructura trama TDMA [14]

La organización temporal más elevada en TETRA es la hipertrama, con una duración de 61.200 ms, compuesta por 60 multitramas. Cada multitrama se divide, a su vez, en 18 tramas, sumando un total de 1020 ms por multitrama. Dentro de esta estructura, la trama número 18 corresponde habitualmente a tareas de control. Cada trama estándar tiene una duración de 56,67 ms y se subdivide en cuatro slots de 14,17 ms cada uno.

3. FDD (Frequency Division Duplex): En cuanto al sistema de duplexado, TETRA utiliza FDD. Esto significa que es un sistema combinado TDMA/FDD, donde las frecuencias de UL (*uplink*) y DL (*downlink*) se encuentran separadas dentro del espectro radioeléctrico. Esta separación de frecuencias, conocida como Duplex Spacing, varía según la banda de operación específica. En la Figura 39 se puede observar cómo está conformado el espectro en uplink y downlink para el estándar TETRA:

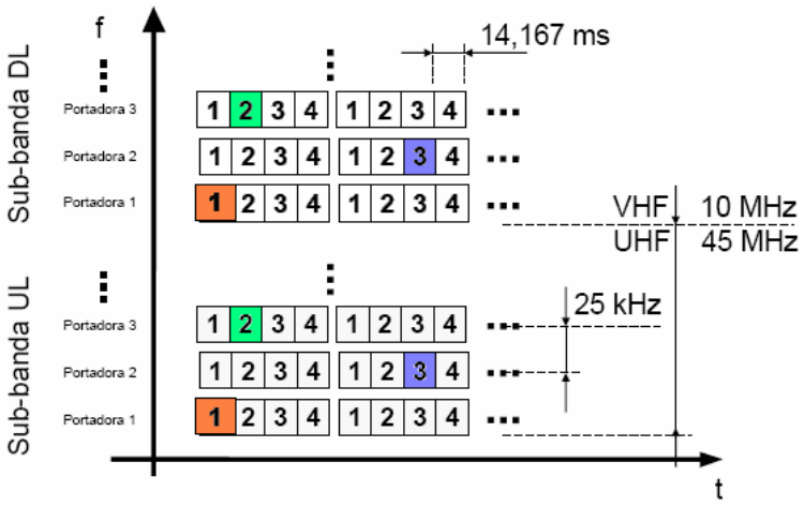


Figura 39 – Espectro TETRA: UL y DL [15]

También hay que destacar las bandas frecuenciales en las cuales opera TETRA. En Europa, la banda de 800 MHz no está considerada para su uso con sistemas TETRA. No obstante, en otras regiones del mundo, las frecuencias empleadas corresponden a un UL de 806-824 MHz y un DL de 851-869 MHz. En la Tabla 3 se ilustran las bandas frecuenciales empleadas para el estándar TETRA en Europa:

ENLACE UL	ENLACE DL	USO
380 – 390 MHZ	**390 – 400 MHz**	**Seguridad y emergencias**
410 – 420 MHZ	**420 – 430 MHz**	**Sistemas civiles**
450 – 460 MHZ	**470 – 480 MHz**	

Tabla 3 – Bandas frecuenciales estándar TETRA

Y, en cuanto a niveles de potencia, el estándar TETRA establece diez clases de potencia que abarcan desde 0,6 W (28 dBm) hasta 40 W (46 dBm), con incrementos de 2 dB entre niveles consecutivos. En el caso de las estaciones base (RBST), existen dos variantes principales en función de la potencia máxima nominal de transmisión: una de 40 W (46 dBm) y otra de 75 W (48,75 dBm). El modelo de 75 W está diseñado para situaciones en las que se combinan múltiples transmisores en una única antena; de este modo, considerando las pérdidas inherentes al sistema de combinación, cada transmisor entrega una potencia efectiva de aproximadamente 40 W.

En definitiva, TETRA continúa siendo una herramienta indispensable en términos de radiocomunicación crítica. Su diseño robusto, su fiabilidad operativa, sus funcionalidades específicas para la gestión de emergencias y su capacidad de integración con nuevas tecnologías lo convierten en un pilar fundamental para garantizar comunicaciones seguras en múltiples sectores críticos estratégicos.

ANEXO C: ANÁLISIS DE MERCADO COMPLETO

Además de las 3 opciones comentadas anteriormente en el capítulo 2, se llevaron a cabo numerosas pruebas de concepto de diferentes opciones que quedaron descartadas tras no cumplir nuestros requerimientos y necesidades principales. Dichas opciones fueron las siguientes:

C.1. Solución software mediante NetFlow

C.1.1. OpManager

OpManager es un software desarrollado por la compañía ManageEngine, especializado en el análisis de tráfico mediante el protocolo NetFlow. Tras instalar la demo, he podido comprobar las principales funcionalidades que ofrece. Entre ellas, destacan la posibilidad de filtrar el tráfico que atraviesa el router Cisco 4331 por IP, además de poder personalizar el intervalo de tiempo en el cual queremos ver el intercambio de paquetes entre esas dos IPs. En la Figura 40 podemos ver el tráfico total que se han intercambiado ambas IPs, junto con el puerto utilizado, el tipo de protocolo o el tráfico enviado en cada instante de tiempo.

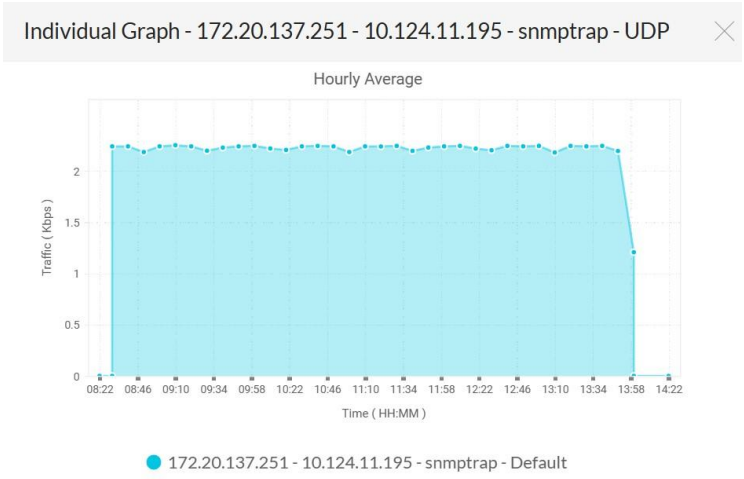


Figura 40 – Flujo de paquetes entre dos IPs

En la Figura 41 se puede observar la cantidad total de tráfico que ha atravesado el firewall en el intervalo de tiempo que tú desees, mientras que en la Figura 42 se pueden ver el porcentaje de bytes transmitidos por cada protocolo y aplicación, la interfaz utilizada para la transmisión de datos…

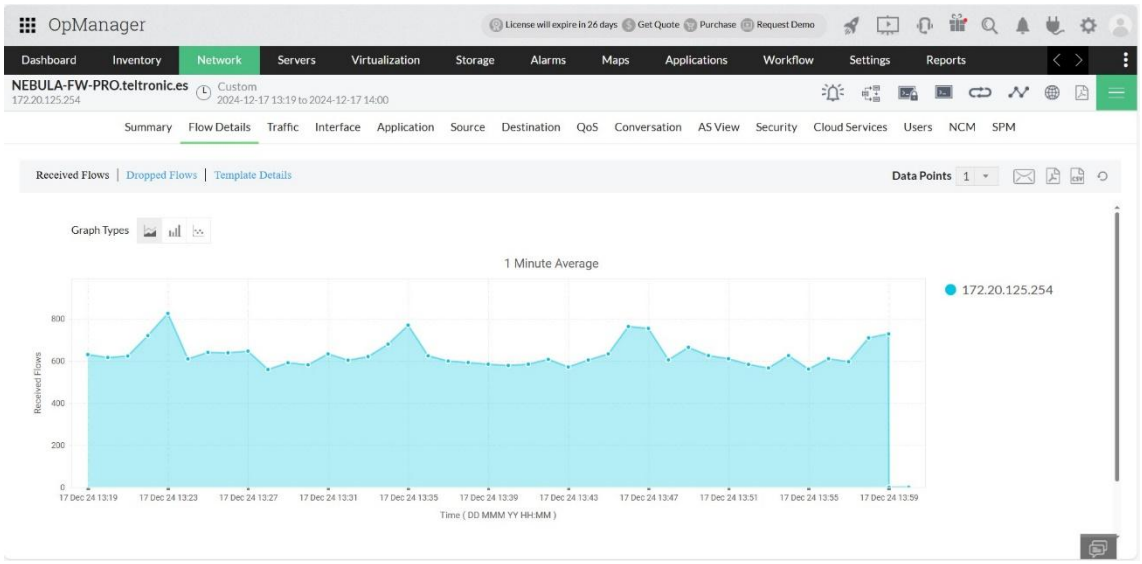


Figura 41 – Tráfico PDP que atraviesa el firewall

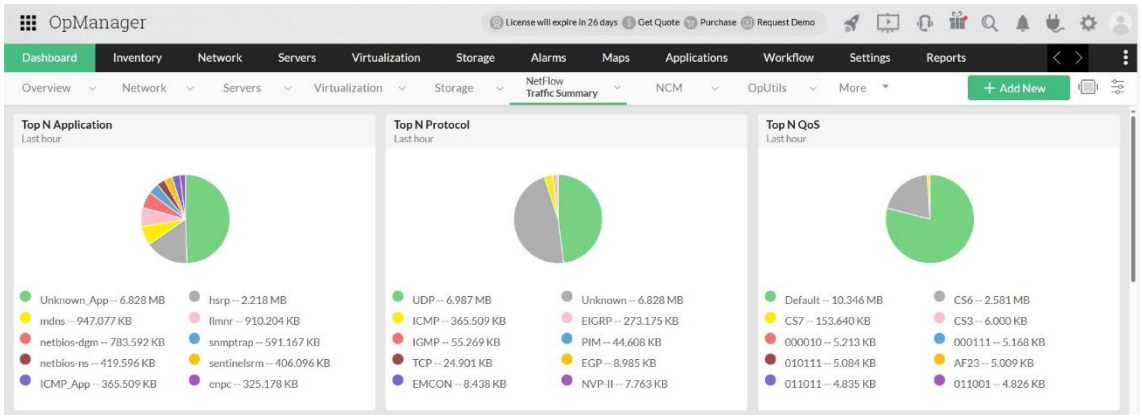


Figura 42 – Resumen tráfico NetFlow

En definitiva, OpManager ofrece la granularidad requerida por el cliente ya que nos permite filtrar el tráfico por diferentes IPs y en el intervalo de tiempo que uno quiera, además de ofrecer numerosos datos y configuraciones sobre el estado del firewall y el tráfico del sistema. No obstante, no ofrece la posibilidad de extraer las capturas de los paquetes que, por ejemplo, se han compartido las IP 172.20.137.251 y 10.124.11.195 en la Figura 40.

C.2. Solución software mediante NetFlow y SNMP

C.2.1. Network Traffic Analyzer

Network Traffic Analyzer es un software desarrollado por SolarWinds el cual está basado en los protocolos SNMP y NetFlow para monitorizar todo el tráfico que atraviesa una red de comunicaciones. Como se puede ver en la Figura 43, mediante este software somos capaces de visualizar el número de paquetes por aplicación que han atravesado el firewall, no obstante; no son capaces de mostrar el flujo de datos entre dos IPs en un intervalo de tiempo concreto. Como se puede ver en la Figura 44, solamente ofrecen la posibilidad de filtrar el tráfico total que envía o recibe una determinada IP. Únicamente se aprecian

subidas y bajadas del flujo de datos de dicha IP, por tanto, no somos capaces de ver si realmente se ha perdido un paquete, ni tampoco hacia una IP a la que había sido enviado ese paquete.

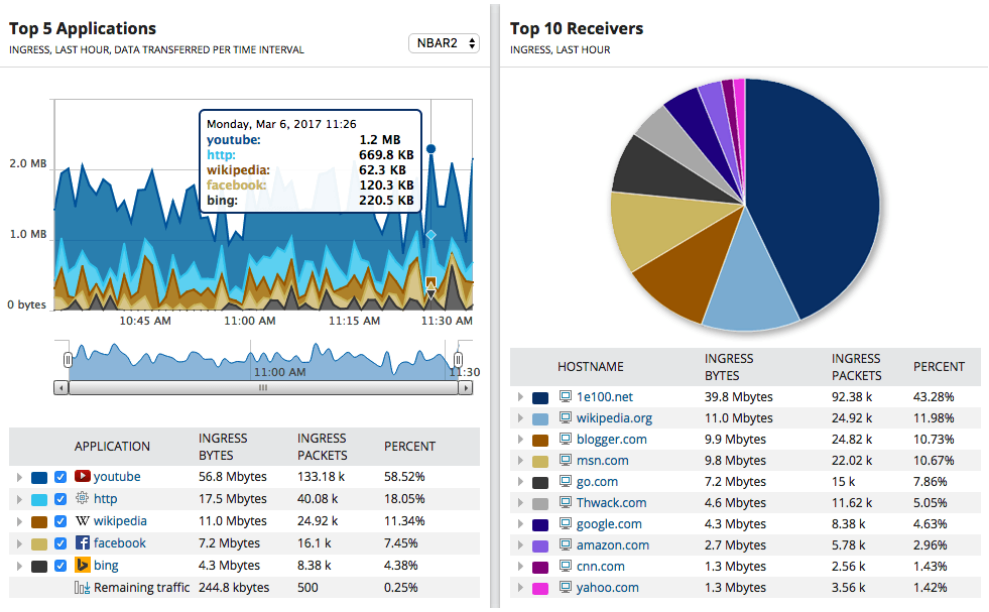


Figura 43 – Resumen del tráfico NetFlow

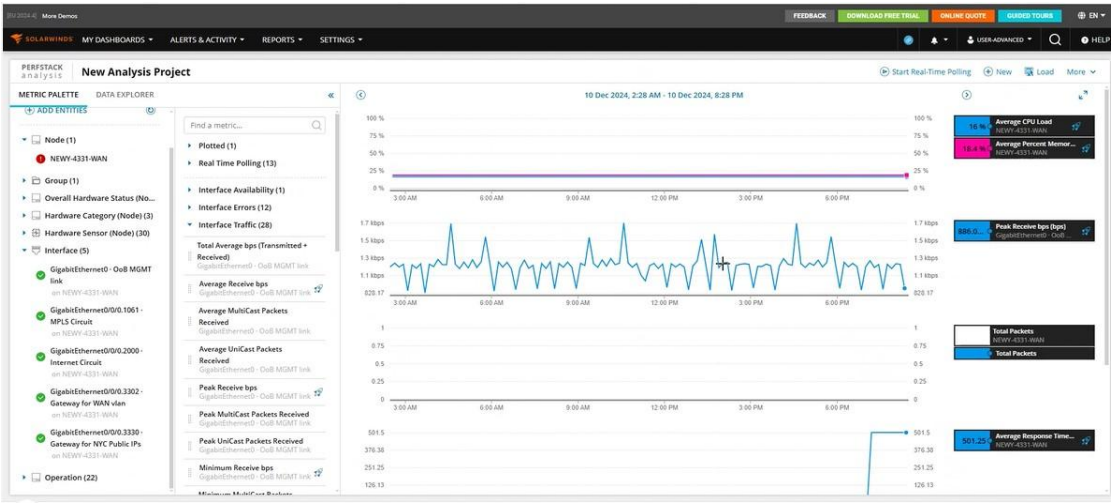


Figura 44 – Tráfico PDP total por IP

Por otro lado, el software no ofrece la opción de mostrar las tramas de datos de una determinada IP, por lo que resulta imposible visualizar los paquetes intercambiados entre dos IPs. Debido a la imposibilidad de mostrar las tramas de datos de una comunicación PDP en un archivo PCAP, esta opción queda descartada.

C.2.2. Noction Flow Analyzer

Desarrollado por Noction, es otro software especializado en el análisis y monitorización del tráfico que atraviesa una red. Basado en SNMP y NetFlow, permite filtrar el tráfico por IP, puerto, protocolo o interfaz. En la Figura 45 se puede ver el tráfico que ha sido transmitido por una interfaz determinada entre dos IPs.

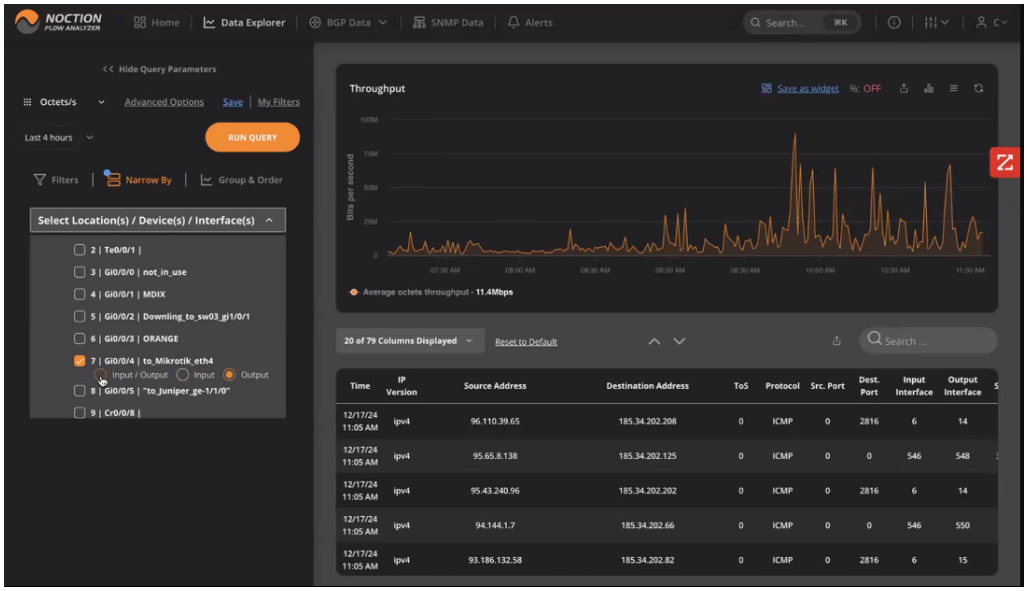


Figura 45 – Tráfico PDP transmitido por una determinada interfaz

También ofrecen la posibilidad de visualizar el tráfico SNMP que atraviesa el sistema en un intervalo de tiempo determinado, como se puede comprobar en la Figura 46 del sistema. Al igual que el software proporcionado por SolarWinds, Noction NetFlow Analyzer es incapaz de mostrar las tramas de los paquetes que atraviesan el sistema, así que de nuevo es imposible saber si realmente las caídas del throughput son debidas a la pérdida de paquetes. Por ello, esta opción queda descartada al no cumplir todos los requerimientos exigidos.

Figura 46 – Tráfico total SNMP del sistema

C.3. Solución software mediante NetFlow y port-mirroring

C.3.1. Plixer One

La compañía estadounidense Plixer brinda la opción de capturar el tráfico PDP que es enviado en una red de comunicaciones mediante el uso de los protocolos NetFlow y port-mirroring. Ofrecen la opción de incorporar numerosos filtros a la hora de visualizar el tráfico entre dos IPs concretas como se puede ver en la Figura 47. Además, ponen a disposición del cliente numerosos filtros adicionales, un monitor de alarmas que ocurren en tiempo real o la capacidad de generar un archivo PCAP sobre una determinada comunicación PDP entre dos IPs.

Figura 47 – Tráfico por IP en una red de comunicaciones

No obstante, pese a utilizar el protocolo port-mirroring, todos los paquetes capturados son mostrados al cliente en intervalos de un minuto, como es común en el protocolo NetFlow. Esto quiere decir que la granularidad máxima que son capaces de facilitar es de un minuto, por tanto, está opción no es válida para la solución que se busca implantar debido a que se requiere una granularidad máxima de 100 milisegundos.