Universidad Zaragoza
1542

Trabajo Fin de Grado

IMPLEMENTACIÓN DE NUEVOS PROTOCOLOS DE RED EN EL REGIMIENTO DE TRANSMISIONES Nº1

C.A.C Javier Fernández Santos

Director académico: D. Francisco Aznar Tabuenca

Director militar: Tte. D. Roberto Vázquez De Inés

Centro Universitario de la Defensa-Academia General Militar

2022

Agradecimientos

Quiero agradecer el gran esfuerzo dedicado a todas las personas que, de una manera u otra, han contribuido al cumplimiento de los objetivos y a la elaboración del presente Trabajo de Fin de Grado.

En primer lugar, al Dr. D. Francisco Aznar Tabuenca, por su constante seguimiento y asesoramiento continuo a lo largo del desarrollo del trabajo, ofreciendo siempre una implicación y dedicación plenas desde el primer día hasta el último.

Al Teniente D. Roberto Vázquez De Inés, por su orientación y disponibilidad permanente para cualquier tipo de duda durante las semanas de prácticas, aportando siempre su ayuda en todo lo necesario tanto acerca de este trabajo como del regimiento.

Al Sargento Primero D. Emilio Cabezas de Mena, por ofrecerme unos conocimientos y matices iniciales clave para la satisfactoria consecución del trabajo además de su ayuda para encauzar el mismo por el camino correcto.

Al Sargento D. Jesús Navarro Pérez, quien ha estado desde el primer momento del desarrollo de la parte práctica del trabajo asesorando, apoyándome, ofreciéndome todo el material que demandase el proyecto y aportando sus conocimientos sobre la materia necesarios para el cumplimiento de todos los objetivos planteados en el trabajo.

Finalmente, a todo el resto del personal de la Compañía de Centros de Transmisiones de Puestos de Mando del Regimiento de Transmisiones Nº1, por todas sus aportaciones al trabajo, por el trato recibido de su parte y por ser un excelente ejemplo de profesionalidad y de lo que debe ser un militar de la especialidad de Transmisiones del Ejército de Tierra.

RESUMEN

Debido a la constante evolución que se está experimentando actualmente en las telecomunicaciones y al material sensible con el que se trabaja en las Fuerzas Armadas (FFAA), es de una gran importancia para la protección de este material e información poseer una estructura de red actual y robusta en términos de seguridad para que los datos que se manipulan viajen de forma segura.

En este ámbito, los ataques a las redes con el fin de obtener información son cada vez más frecuentes y están mejor elaborados. Es por ello por lo que se demanda una actualización en las redes militares y, concretamente, la situación mencionada será abordada dentro del Regimiento de Transmisiones Nº1 (RT 1) debido a que es la entidad sobre la que se ha desarrollado este proyecto.

Actualmente existen multitud de protocolos de red encargados de actualizar, reforzar y modernizar las redes de datos. Es por ello por lo que el objetivo del presente trabajo de fin de grado (TFG) consiste en la propuesta de implementación de nuevos protocolos de red en el RT 1 con el fin de mejorar, modernizar y satisfacer las necesidades actuales de las redes en el ámbito del Ejército de Tierra (ET). Para ello, se ha llevado a cabo una selección de los protocolos de red más adecuados para los objetivos que demanda el RT 1 y, posteriormente se han elegido los cuatro más factibles para su implementación.

En lo que respecta al estudio, para formalizarlo, se ha recopilado información de gran relevancia a través de Internet y de la Compañía de Centros de Transmisiones de Puesto de Mando (CTPC) del Batallón de Transmisiones I/1 (BT I/1), así como del personal del RT 1 experto en la materia. Además, se ha creado un laboratorio para poner a prueba los protocolos seleccionados con el objetivo de comprobar de forma práctica y lo más real posible la efectividad de los escogidos. Una vez finalizado el desarrollo del proyecto se ha recopilado en una tabla de forma breve las características que se han visto modificadas en una red de uso típico en el RT 1 tras la implementación de los protocolos respecto a esa misma red sin la implementación de estos. Cabe mencionar las características que se han visto sustancialmente mejoradas como son la seguridad, la escalabilidad y el control sobre las redes alcanzando un grado de modernización y mejora de la red acorde a los objetivos planteados.

La parte final de esta memoria presenta las conclusiones extraídas de este proyecto y unas posibles líneas futuras para tener en cuenta en el estudio realizado en este TFG entre las que destaca la necesidad de hacer ver al personal del RT 1 que unas ligeras modificaciones en el esquema de red general permitirían una gran mejora y versatilidad en sus redes a la hora de realizar ejercicios y maniobras tanto individuales como conjuntas.

Palabras clave

Protocolo, red, seguridad, actualización, implementación experimental.

ABSTRACT

Due to the constant evolution that is currently being experienced in telecommunications and the sensitive material with which the Armed Forces work, it is of great importance for the protection of this material and information to have a current and robust in terms of security network structure that the data that is manipulated travels safely.

In this area, attacks on networks to obtain information are becoming more frequent and better prepared. That is why an update is required in the military networks, specifically in the Signals Regiment No. 1, which is the entity on which this project has been developed.

Currently, there are many network protocols responsible for updating, strengthening, and modernizing data networks. That is why the objective of this final degree project consists of the proposal for the implementation of new network protocols in RT 1 to improve, modernize and satisfy the current needs of networks in the field of the Army. Therefore, a selection of the most suitable network protocols for the objectives demanded by RT 1 has been carried out and, subsequently, the four most feasible have been chosen for its implementation.

Regarding the study, to formalize it, highly relevant information has been compiled through the Internet and from the Command Post Signals Centers Company of the Signals Battalion I/1, as well as the personnel of the RT 1 expert in the matter. In addition, a laboratory has been created to test the selected protocols to verify the effectiveness of the chosen in a practical way and as real as possible. Once the development of the project has been completed, the characteristics that have been modified in a network of typical use in RT 1 have been compiled in a brief table after the implementation of the protocols with respect to that same network without the implementation of these. It is worth mentioning the characteristics that have been substantially improved such as security, scalability, and control over the networks, reaching a degree of modernization and improvement of the network according to the objectives set.

The final part of this document presents the conclusions drawn from this project and some possible future lines to consider in the study carried out in this TFG, among which the need to make the RT 1 staff see that some slight modifications in the scheme stands out general network systems would allow a great improvement and versatility in their networks when carrying out exercises and maneuvers, both individual and joint.

KEYWORDS

Protocol, network, security, update, experimental implementation.

INDICE DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

ABREVIATURAS, SIGLAS Y ACRÓNIMOS

AF	Reenvío Asegurado *(Assured Forwarding)*
AGM	Academia General Militar
AS	Sistema Autónomo *(Autonomous System)*
BGP	Protocolo de Puerta de Enlace Fronteriza *(Border Gateway Protocol)*
BT I/1	Batallón de Transmisiones I/1
CTPC	Centros de Transmisiones de Puestos de Mando *(Post Command)*
CS	Selector de Clase *(Class Selector)*
CT AVA	Centro de transmisiones avanzado
CT PPAL	Centro de transmisiones principal
CT TAC	Centro de transmisiones táctico
DiffServ	Servicios Diferenciados *(Differentiated Services)*
DMVPN	Red Privada Virtual Multipunto Dinámica *(Dynamic Multipoint Virtual Private Network)*
EF	Reenvío Acelerado *(Expedited Forwarding)*
EGP	Protocolo de Puerta de Enlace Exterior *(Exterior Gateway Protocol)*
ET	Ejército de Tierra
FFAA	Fuerzas Armadas
GRE	Encapsulación de Enrutamiento Genérico *(Generic Routing Encapsulation)*
IGP	Protocolo de Puerta de Enlace Interior *(Interior Gateway Protocol)*
IntServ	Servicios Integrados *(Integrated Services)*
IP	Protocolo de Internet *(Internet Protocol)*
IP SLA	Acuerdo de Nivel de Servicio IP *(Internet Protocol Service Level Agreement)*
IPSec	Seguridad IP *(Internet Protocol Security)*

Mb/s	Megabits por segundo
mGRE	Multipunto GRE o MultiGRE
NHRP	Protocolo de Resolución del Siguiente Salto *(Next Hop Resolution Protocol)*
NHS	Servidor del Siguiente Salto *(Next Hop Server)*
OTAN	Organización del Tratado del Atlántico Norte
OSI	Interconexión de Sistemas Abiertos *(Open Systems Interconnection)*
PC	Ordenador Personal *(Personal Computer)*
QoS	Calidad de Servicio *(Quality of Service)*
RAE	Real Academia Española
RT 1	Regimiento de Transmisiones Nº1
SIMACET	Sistema para el Mando y Control del Ejército de Tierra
TFG	Trabajo de Fin de Grado
VLAN	Red de Área Local Virtual *(Virtual Local Area Network)*
VoIP	Voz sobre IP *(Voice over Internet Protocol)*
VRF	Enrutamiento y Reenvío Virtual *(Virtual Routing and Forwarding)*
VTC	Videoteleconferencia
VTP	Protocolo de Enlace Virtual *(VLAN Trunking Protocol)*
WAN	Red de Área Extensa *(Wide Area Network)*

INTRODUCCIÓN

El presente Trabajo fin de Grado (TFG) ha sido realizado en la Compañía de Centros de Transmisiones de Puestos de Mando (CTPC) del Batallón de Transmisiones I/1 (BT I/1), encuadrado en el Regimiento de Transmisiones Nº1 (RT 1), localizado en la Base Militar "Cid Campeador", en el municipio de Castrillo del Val, Burgos(*Ejército de tierra*, 2012). Esta memoria recoge el estudio y análisis de diversos protocolos de red, además de la implementación básica de los mismos con el fin de dotar a las redes que utilice el RT 1 de unas posibilidades mayores en cuanto a su modernización y novedad.

Las redes utilizadas en el RT 1 varían según el esquema que demande la maniobra que corresponda. En varias ocasiones el personal del regimiento se ha encontrado ante la necesidad de implementar una red relativamente sencilla debido a la exigencia de la maniobra y en muchas otras ocasiones ha debido implementar redes muy complejas para satisfacer las necesidades requeridas. Es por ello por lo que en esta memoria se han realizado las pruebas, estudios y prácticas pertinentes tomando como referencia redes concretas aplicadas en el regimiento. Sin embargo, esta situación no limita los resultados a una red en cuestión, pues los protocolos que se han estudiado, analizado e implementado no se ven afectados, a priori, por el tamaño de la red en la que se implementen.

La situación actual de las redes del RT 1 está al nivel de otras vistas con anterioridad en otras unidades durante el curso académico 2020-2021. Pese a ello, se demanda una posible actualización de estas añadiendo algunos protocolos de red que no se han utilizado hasta el momento en el regimiento. Las razones por las que no se hayan implementado una serie de protocolos de red que se van a incluir en esta memoria son debidas principalmente al desconocimiento de su posible implementación por parte de los administradores de las redes, aunque también existen algunas situaciones en las que simplemente no es posible implementar algunas de las medidas planteadas.

Ante la situación mencionada en el párrafo anterior, es necesario definir una serie de conceptos clave para la entera comprensión de esta memoria: router, *switch*, protocolo de internet (IP), protocolo de red, voz sobre IP (VoIP), etc. Son conceptos con los que se trabaja a diario en el ámbito en el que se desarrolla este proyecto. También es necesario conocer información acerca de los protocolos de red sobre los que se va a realizar el análisis e implementación y que se desarrollan en el Capítulo 4 de esta memoria.

1.1 ESTRUCTURA DE LA MEMORIA

Esta memoria se ha articulado en cinco capítulos los cuales se han enriquecido con anexos útiles para ampliar la información y entender mejor todos los elementos con los que se ha trabajado en este proyecto.

El primer capítulo de la memoria consta de la introducción, en la que se exponen de forma breve las razones que han motivado a la realización de este proyecto, el ámbito sobre el que trabaja y la situación sobre la que se parte.

El segundo capítulo se centra en los objetivos que se pretenden alcanzar y la metodología utilizada para cumplir dichos objetivos. Se integra además en este capítulo el alcance del que consta este proyecto.

El tercer capítulo comprende los antecedentes del tema que trata esta memoria y el marco teórico o estado del arte sobre el que se plantea. Además, se desarrollan con más detalle los conceptos clave mencionados en el primer capítulo con el fin de dar un contexto y un

conocimiento mucho más amplio a las labores realizadas durante el desarrollo de esta memoria.

El cuarto capítulo corresponde al desarrollo íntegro del proyecto que se plantea en esta memoria. Se integran una muestra del laboratorio de trabajo utilizado para este proyecto y todos los protocolos elegidos con sus correspondientes implementaciones. Además, también recoge el análisis y los resultados de todas las tareas realizadas durante la parte más práctica del proyecto.

Finalmente, el quinto capítulo expone las conclusiones que se han conseguido elaborar a partir de todo el desarrollo que ha tenido este proyecto, aportando además unas posibles líneas de planteamientos futuros para el regimiento.

OBJETIVOS Y METODOLOGÍA

2.1 OBJETIVOS Y ALCANCE

El objetivo general de este trabajo consiste en implementar una serie de nuevos protocolos de red que sean capaces de dotar a las redes del RT 1 de unas capacidades que hagan de la misma una red más novedosa y segura dentro de los límites que marcan los propios protocolos de red.

Con este ámbito presente, se han planteado una serie de objetivos específicos necesarios para el cumplimiento del objetivo principal del proyecto.

Los objetivos específicos son:

- Conocer la arquitectura de la red del RT 1 y distintos protocolos que se pudieran implementar para mejorar sus capacidades.
- Analizar en detalle los protocolos de red seleccionados con el fin de poder valorar la viabilidad de implementación dentro de las redes del RT 1.
- Realizar las pruebas pertinentes para la comprobación del correcto funcionamiento de los protocolos en la red del regimiento.
- Comparar unos protocolos de red con otros con el propósito de observar las ventajas que ofrezcan para dar prioridad a la implementación de unos respecto de otros.

Respecto al alcance del proyecto, está limitado a la parte de la red que no implica el uso de los cifradores utilizados por el ET, ya que la modificación de su configuración supondría un acto constitutivo de delito ante la posibilidad de vulnerar la seguridad de las redes militares. Teniendo esto en cuenta, el alcance por tanto llegaría a cualquier red del RT 1 que cuelgue por debajo de los cifradores e incluso, en un futuro, podría estudiarse la implementación de los nuevos protocolos de red en otras unidades del ET que lo demandasen y que sean compatibles con los medios de los que dispone el RT 1. Dichas unidades podrían ser para una entidad tipo regimiento, como por ejemplo el Regimiento de Transmisiones Nº21 ubicado en Valencia. En el caso de las brigadas del ET, este proyecto podría llevarse a cabo incluso a nivel compañía (puesto que es esta la entidad de transmisiones que posee una brigada en el ET). En definitiva, se trata de un proyecto cuyo alcance podría llegar a prácticamente cualquier unidad de transmisiones del ET.

2.2 METODOLOGÍA

Con el fin de cumplir los objetivos planteados en este TFG, el proyecto se ha estructurado con una parte teórica y otra práctica.

En lo que respecta a la parte teórica, se han realizado consultas en manuales y documentos de la Academia General Militar (AGM) así como documentos de la propia Compañía de CTPC. Además, se ha ampliado la información en base a búsquedas halladas en Internet sobre aplicaciones, propiedades y características de los protocolos de red a implementar. También se han tenido muy en cuenta las aportaciones del personal de la propia Compañía de CTPC con el fin de establecer un marco teórico sólido en cuanto a los conocimientos previos requeridos.

Sobre la parte práctica del proyecto, se ha colaborado con personal de la compañía de CTPC para poder realizar una simulación lo más realista posible de una red típica con una herramienta informática de simulación de redes. Seguidamente, se ha llevado esa simulación a materiales y equipos reales con el fin de mostrar in situ los resultados obtenidos en la simulación

anterior. Posteriormente, se han realizado análisis y estudios de los diferentes protocolos de red a implementar en las redes del RT 1 y se han obtenido resultados cuyo análisis ha permitido obtener diversas conclusiones acerca de su utilización en el regimiento. Además, se han tenido en cuenta las ventajas de estos y se han realizado las comparaciones pertinentes con el objetivo de priorizar los protocolos que sean más recomendables en función de los resultados obtenidos tal y como se ha mencionado en el apartado 2.1 de esta memoria.

ANTECEDENTES Y MARCO TEÓRICO

Teniendo en cuenta que hoy en día todo lo referente a las redes y telecomunicaciones evoluciona a pasos agigantados y se encuentra en constante cambio, el RT 1 se encuentra ante la necesidad de dotar a sus redes de nuevos protocolos que hagan poner sus configuraciones a la vanguardia del ET. Esto no implica que las redes actuales se hayan quedado anticuadas, sino que se observa una constante necesidad de actualización. Día tras día surgen nuevas posibles configuraciones para una red, nuevos mecanismos de seguridad y una serie de elementos en los que, especialmente en el ámbito militar, se debe estar a la vanguardia.

Además, las amenazas informáticas a las que se enfrenta cualquier red en la actualidad son cada vez más frecuentes y están mejor elaboradas. Es por ello por lo que una prioridad para el ET (entre otras como puede ser la eficiencia de la red) debe ser la constante actualización y mejora de la seguridad general de sus redes tanto a nivel externo como a nivel local.

Dentro de este marco es donde se plantea la implementación de nuevos protocolos de red a fin de cumplir los objetivos ya mencionados. Dichos protocolos no necesariamente se deben centrar en un solo ámbito como puede ser la seguridad, sino también en ámbitos como el de su configuración a fin de obtener los mismos resultados con una mayor comodidad y un tiempo de implementación menor produciendo un diseño de red más eficiente en general.

Ante la situación mencionada en el párrafo anterior, en lo que respecta a redes de internet, es necesario definir una serie de conceptos clave para la entera comprensión de esta memoria:

- **Red:** En informática, se trata del conjunto de equipos conectados por cables, ondas o cualquier otro método de transporte de datos, que comparten información, recursos y servicios, etc. (Gorgona, 2015).

- **Router:** En español “encaminador” o “enrutador”, es un dispositivo que interconecta equipos que funcionen dentro del marco de una red. Básicamente encamina los paquetes de datos que recibe (Cisco, 2020). Por ser un término inglés aceptado por la Real Academia Española (RAE), se utilizará como tal en esta memoria.

- ***Switch*:** En español “conmutador”, es un dispositivo de interconexión utilizado para conectar equipos en red siguiendo el estándar Ethernet (IEEE 802.3 (IEEE Computer Society, 2012)) (Universidad Nacional de La Plata, 2018). La principal diferencia respecto a un router es el hecho de que los routers trabajan en el nivel de red del Modelo de Interconexión de Sistemas Abiertos (OSI) mientras que la mayoría de los *switches* trabajan en el nivel de enlace de este modelo. Por tanto, su función se limita a las conexiones físicas, mientras que un router se centra en las redes y su configuración. El Anexo I muestra un esquema del Modelo OSI. Se considera necesario mencionar el uso de este término como anglicismo por ser utilizado más ampliamente de esta manera dentro del contexto en el que se fundamenta esta memoria.

- **Túnel:** Es una técnica que se basa en la encapsulación de un protocolo de red sobre otro. Establece un enlace punto a punto virtual por el que los paquetes de un determinado protocolo pueden pasar encapsulados dentro de otro. Normalmente esta técnica se utiliza para incrementar la seguridad de protocolos que por sí solos, no son lo suficiente seguros (Sutil Web, 2021).

- **Protocolo de red:** Consiste en una serie de reglas implementadas vía software que se erigen en un lenguaje común a los dispositivos para que éstos puedan “dialogar” a través de una

red (González, 2017).

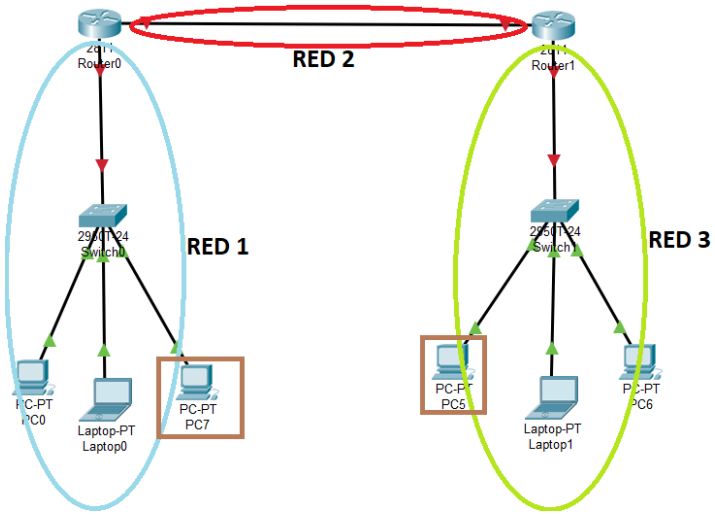

Figura 1 Ejemplo de un esquema de red

Para poner en contexto estas definiciones y visualizar mejor los conceptos sobre los que se está hablando, en la Figura 1 se muestra un ejemplo muy sencillo de un esquema de red cualquiera en el que participan routers, *switches* y equipos finales como son ordenadores portátiles y ordenadores personales (PC). Si, por ejemplo, el PC7 quiere enviar información al PC5, esta viajará hacia el *switch* sobre el que cuelgan el resto de los equipos de la red 1, posteriormente el router entre las redes 1 y 2 redirigirá la información que le llegue a la red que tenga por destino la información (el router entre las redes 2 y 3 en este caso) y, finalmente viajará por el swit*ch* de la red 3 hasta el PC5.

Por otro lado, es necesario también introducir brevemente los protocolos de red sobre los que se centrará este proyecto. Dichos protocolos son:

- **Calidad de Servicio (QoS):** Básicamente, es el rendimiento promedio de una red. Mide aspectos como rendimiento, ancho de banda, etc. Además, realiza funciones específicas para solventar los problemas que surjan al respecto (Cabello, 2015; Sobreviela and Romero Martínez, 2017; eClassVirtual, 2020).

- **Protocolo de Enlace Virtual (VTP):** Es un protocolo utilizado para centralizar en un solo *switch* todas las Redes de Área Local Virtuales (VLAN). Simplifica mucho las configuraciones que haya que realizar en la red dentro de los *switches* (Veato, 2016).

- **Protocolo de Enrutamiento y Reenvío Virtual (VRF):** Permite al router que ejecute más de una tabla de enrutamiento simultáneamente, pudiendo utilizar la misma dirección IP en dos interfaces diferentes (MediaCloud, 2018; Davila, 2019).

- **Protocolo de Encapsulación de Enrutamiento Genérico (GRE):** Es uno de los protocolos de red encargados del establecimiento de túneles a través de la red (Walton, 2020; Sutil Web, 2021).

- **Seguridad del Protocolo de Internet (IPSec):** Se trata de un conjunto de protocolos que garantizan unos altos niveles de seguridad IP. Asegura las comunicaciones mediante el uso de autenticaciones de cada paquete IP e incluye protocolos que pueden establecer claves de cifrado (Mocan, 2019; De Luz, 2021).

- **Red Privada Virtual Multipunto Dinámica (DMVPN):** De una manera muy general, es

el resultado de la combinación de múltiples túneles GRE. De este modo, se consiguen enlaces punto a punto virtuales generados automáticamente por DMVPN sin necesidad de implementarlos a mano (dinámicos). Dichos enlaces suelen ser más eficientes para el viaje de los paquetes que las rutas introducidas manualmente (Cisco, 2009).

- **Acuerdo de Nivel de Servicio IP (IP SLA):** Esta herramienta analiza niveles de servicio. Por ello, permite monitorizar de forma continua el tráfico que navega por la red, lo cual proporciona un gran control de esta (Gerometta, 2019).

- **Protocolo de Puerta de Enlace Fronteriza (BGP):** Es un protocolo de enrutamiento dinámico que permite compartir su información entre otros routers de otros sistemas originando una base de datos que intercambia con el resto de los sistemas que utilicen BGP. Además, posee su propia encriptación, lo que añade mayor seguridad al enrutado de los paquetes de datos (Watchguard, 2018).

DESARROLLO: ANÁLISIS Y RESULTADOS

En este capítulo se van a seleccionar los protocolos de red a implementar. Todos ellos han sido ya introducidos brevemente en el capítulo 3 de esta memoria. Seguidamente, se mostrará la simulación llevada a cabo y la instalación de los equipos físicos utilizados formando así el laboratorio de trabajo para el proyecto y obteniendo de esta manera un esquema de red factible para la implementación de los protocolos. A continuación, se describirán los protocolos seleccionados y se mostrará la implementación de estos con el fin de poder comprobar su correcto funcionamiento y cumplir con los objetivos fijados en el capítulo 2. Finalmente, se expondrán los resultados obtenidos en las pruebas realizadas y se llevarán a cabo las comparativas pertinentes en cuanto a las posibilidades que ofrecen estos protocolos que no se habían implementado con anterioridad en el regimiento.

4.1 ELECCIÓN DE LOS PROTOCOLOS DE RED

En base a las aportaciones del personal del RT 1 y, especialmente, la Compañía de CTPC, se han seleccionado seis de los protocolos de red mencionados en el Capítulo 3 para implementar en el regimiento. En esta memoria son clasificados en cuatro protocolos puesto que GRE es una versión simplificada de DMVPN, siendo este último el que va a ser implementado. El otro caso es IPSec ya que va a ser implementado en varias áreas combinado con otros protocolos, por lo que se considera innecesario dedicarle un apartado exclusivamente para él. Los dos que restan, por diferentes motivos, no se cree conveniente su implementación en las redes del RT 1. Los protocolos en cuestión son VRF y VTP:

- En lo que respecta al protocolo VRF, su desarrollo va enfocado principalmente a redes de un tamaño importante. Teniendo en cuenta la limitación de este proyecto debido a la imposibilidad de configurar los equipos cifradores que posee el regimiento, las redes que se permiten utilizar para este proyecto reducen su tamaño. Por ello, la implementación y los requisitos que demanda el protocolo de red VRF son excesivos para los beneficios que se podrían llegar a obtener si se implementa en una red de tamaño medio.

- En cuanto al protocolo VTP, el RT 1 ya implementa este protocolo en sus redes de una forma eficiente y simplifica mucho las labores de configuración de las VLANs. Por ello, no es necesario profundizar en el protocolo mencionado, ya que su desarrollo en el regimiento ya es óptimo actualmente.

Por tanto, una vez descartados los protocolos anteriormente mencionados, los protocolos elegidos finalmente para su desarrollo e implementación serían QoS, DMVPN, IP SLA y, finalmente, BGP.

4.2 SIMULACIÓN EN CISCO PACKET TRACER

Para el desarrollo del proyecto, se ha utilizado un esquema de red muy similar a una red típica que pudiera usar el RT 1 en sus ejercicios y maniobras. Se ha considerado una buena práctica simular la red primero para detectar posibles fallos en el concepto general del proyecto y, posteriormente, llevar esa simulación a equipos físicos una vez han estado disponibles para su utilización en este trabajo.

En lo que respecta a la simulación, se ha decidido utilizar la herramienta gratuita Cisco Packet Tracer.

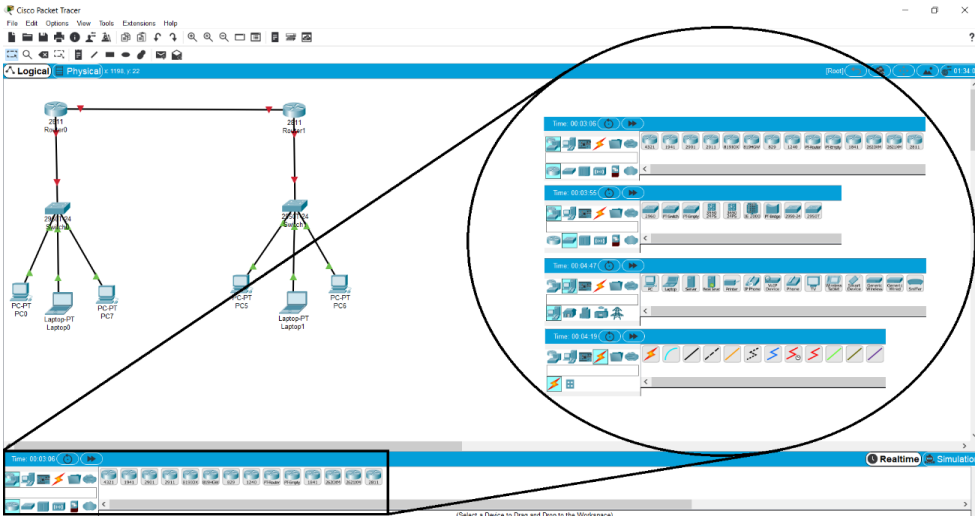

Figura 2 Interfaz de la herramienta Cisco Packet Tracer

Como muestra la Figura 2, esta herramienta ofrece multitud de dispositivos a simular. Existen diversos tipos de routers, *switches*, servidores, equipos de usuarios finales, etc. Todos ellos utilizables con el fin de aproximar a la realidad lo máximo posible la red que se desee implementar.

Se trata de un simulador de redes propietario de la empresa Cisco que permite montar redes de cierta complejidad. Su utilización se ha debido a la imposibilidad de utilizar equipos físicos reales hasta ya iniciado este proyecto. Por ello, se ha iniciado el desarrollo en un simulador fiable como lo es Cisco Packet Tracer para, posteriormente, llevarlo a equipos físicos donde su implementación y configuración es prácticamente idéntica a la empleada con la herramienta de simulación.

4.3 IMPLEMENTACIÓN DE LA RED

Como ya se ha mencionado, la situación planteada en el simulador se ha llevado posteriormente a equipos físicos con el fin de dotar al proyecto del realismo y utilidad apropiados.

Seguidamente, se detalla la función de cada uno de los equipos utilizados:

- **Router Cisco 4351 Series:** Tres de los routers son los encargados de cada uno de los centros de transmisiones: el centro de transmisiones principal (CT PPAL), el centro de transmisiones táctico (CT TAC) y el centro de transmisiones avanzado (CT AVA). Por otro lado, el cuarto tiene como función simular la red de área extensa (WAN) IPC2, encargada de interconectar entre sí todos los equipos y facilitar el mando y control de las operaciones.

- ***Switch* Cisco Catalyst 2950:** Encargado de simular los enlaces con los terminales satélite que se utilizarían en ámbito real en base a enlaces a través de VLANs.

- ***Switch* Allied Telesis x510-52GPX:** Encargado de ampliar el número de conexiones posibles. Se conecta al router del CT PPAL simulando que extendería la red a todo ese centro. Perfectamente podría haberse utilizado un *switch* para cada centro, sin embargo, se considera innecesario puesto que estos *switches* prácticamente no requieren configuración ninguna para este proyecto, simplemente amplían la red extendiéndola a todos sus interfaces.

- **Ordenadores portátiles:** Tienen como función administrar y configurar los equipos utilizados. Mediante una conexión entre router y ordenador, se puede acceder a la consola de

comandos de configuración del router e iniciar las implementaciones pertinentes.

Figura 3 Equipos utilizados para la elaboración del proyecto. Un router (izquierda) y dos switches (derecha) (Cisco, 2018a, 2018b; Julieta, 2020)

La Figura 3 muestra los equipos utilizados. De izquierda a derecha: Router Cisco 4351 Series, *Switch* Cisco Catalys 2950 y *Switch* Allied Telesis x510-52GPX.

Una vez definidos los equipos a utilizar para el laboratorio, es interesante plantear un esquema de red inicial con las conexiones básicas y los roles que van a tener cada uno de los routers y *switches*. Una forma útil de visualizar dicho esquema, es utilizar el simulador Cisco Packet Tracer para obtener la visión general requerida como si se tratase de un croquis:

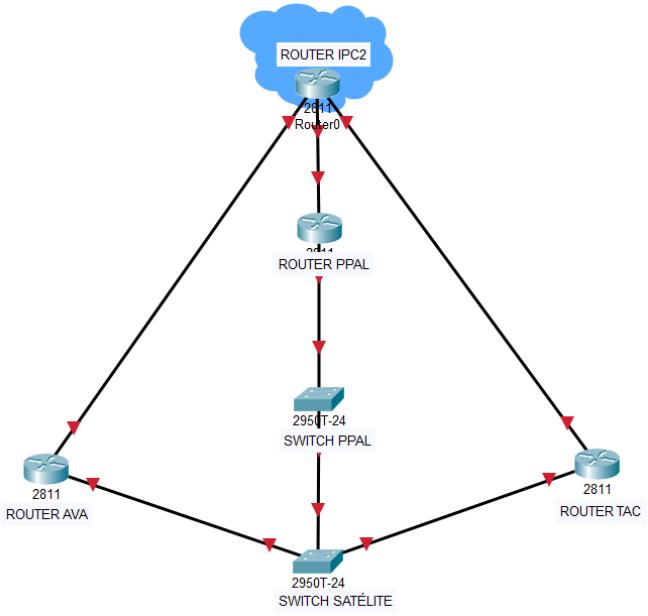

Figura 4 Esquema de red inicial del laboratorio

La Figura 4 muestra cómo quedaría formado inicialmente el esquema de red del laboratorio planteado utilizando el simulador Cisco Packet Tracer como elemento de diseño. Se trata de conexiones sencillas entre los equipos que se han utilizado y que, una vez iniciadas las configuraciones previas, el resultado permitirá iniciar las tareas de implementación de los protocolos.

Para ampliar el contexto de este proyecto, el Anexo II muestra un esquema de red ideal con los equipos que se utilizarían y otro esquema de red que pretende simular los equipos que no han podido ser utilizados para el trabajo (equipos de terminales satélite, básicamente).

Una vez expuestos los equipos utilizados, se han instalado y conectado siguiendo el esquema de red mostrado en la figura 4. De esta forma, el laboratorio resultante sobre el que se

ha realizado la mayor parte del trabajo que ha requerido este proyecto ha quedado de la siguiente manera:

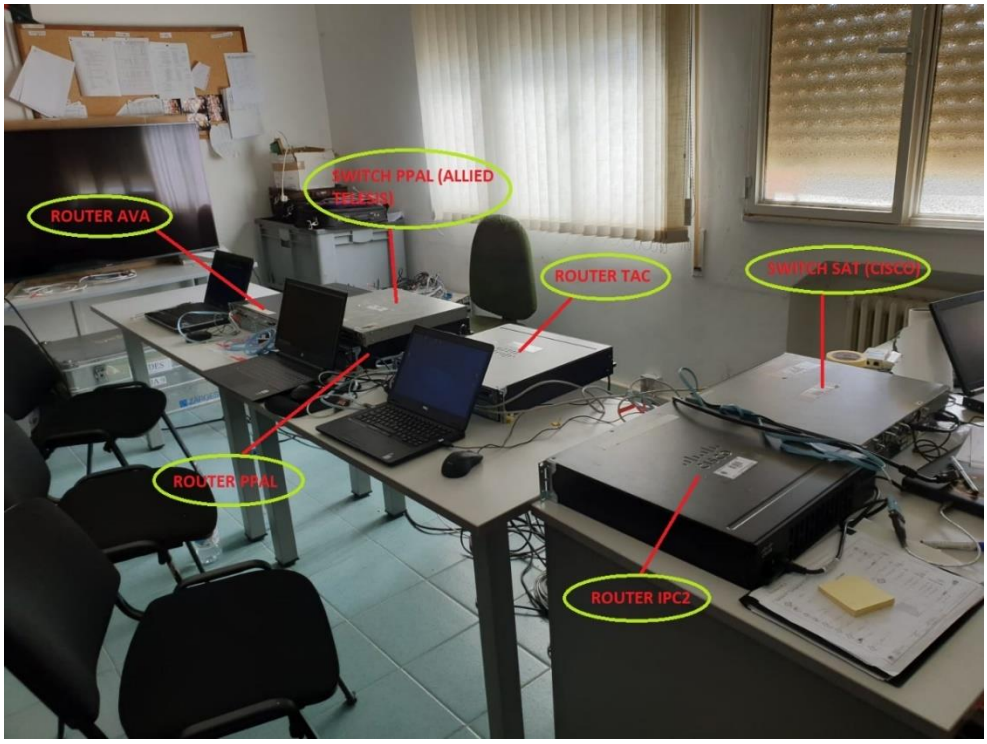

Figura 5 Laboratorio utilizado para el desarrollo del proyecto

La Figura 5 muestra el planteamiento del laboratorio para la realización del proyecto. Se han dispuesto un total de cuatro routers Cisco 4351 Series, un *switch* Cisco Catalyst 2950 y un *switch* Allied Telesis x510-52GPX además de cuatro ordenadores portátiles para administrar y configurar todos los equipos mencionados.

Se puede observar además cómo a cada equipo ya se le ha asignado su rol: bien como un router de uno de los centros de transmisiones, bien como el *switch* que hace las veces de los enlaces de los terminales satélite.

A fin de complementar esta parte descriptiva del laboratorio utilizado, el Anexo III recoge una serie de ilustraciones sobre la instalación de estos equipos in situ.

4.4 CONFIGURACIÓN BÁSICA DE LA RED

Una vez realizadas las conexiones entre los distintos equipos utilizados, es necesario plantear una serie de configuraciones previas en los mismos a fin de que la implementación de los protocolos sea satisfactoria. Por ello, se requieren cierta información de los enlaces planteados entre los distintos equipos. Nuevamente, la herramienta Cisco Packet Tracer es muy útil para poder mostrar toda la información requerida.

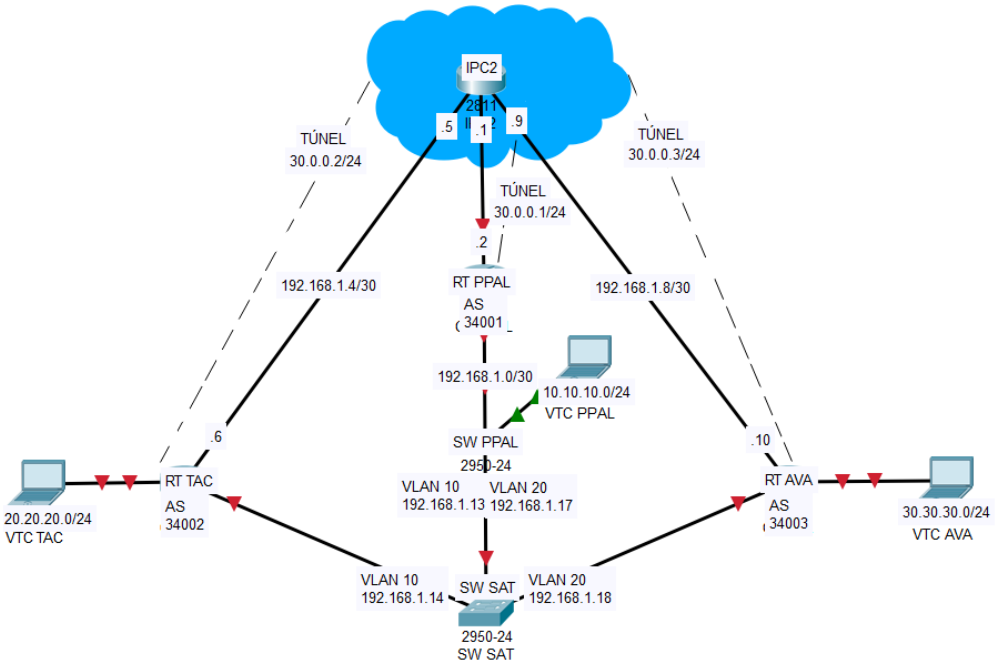

Figura 6 Desarrollo del esquema de red del laboratorio

La Figura 6 muestra el esquema de red planteado y desarrollado para la simulación que demanda este proyecto. Pueden observarse multitud de diferentes direccionamientos IP y datos que facilitan la comprensión de lo que se quiere realizar. Con este esquema presente, llevar la simulación a equipos reales se convierte en una tarea más sencilla gracias a poder disponer de todos los datos necesarios en su correspondiente posición preestablecida.

Concretamente, y como ya se ha mencionado, el Anexo II, en su Figura 26 recoge una versión ilustrativa del esquema de red mostrado con el fin de complementar la situación que se desea abordar de forma más simplificada sin entrar al detalle de direccionamientos de redes, enlaces, etc.

Una vez finalizadas estas instalaciones y configuraciones previas, el proyecto ya se encuentra en condiciones de comenzar con la implementación de los diferentes protocolos de red seleccionados anteriormente.

4.5 DESCRIPCIÓN DE LOS PROTOCOLOS DE RED

A continuación, y ya con todos los equipos instalados y las configuraciones previas realizadas, se procede a la descripción de los protocolos a implementar. El objetivo de este apartado es poder dar una visión más detallada y comprensible de la labor que realiza cada uno de los protocolos de red.

4.5.1 Calidad de Servicio

En lo que respecta a las redes que utiliza el RT 1 (y las redes militares en general), el problema más destacado es el escaso ancho de banda del que se suele disponer para sus comunicaciones. Generalmente, la maniobra demanda unos servicios mínimos que muchas veces son difíciles de alcanzar debido a la falta de un ancho de banda mayor. Una solución a este problema es QoS.

Respecto a las redes militares, QoS puede ser muy útil para una gestión óptima del escaso ancho de banda disponible. Su implementación en el RT 1 supone una minimización de los posibles problemas de rendimiento, los retardos, los errores en los paquetes de datos, etc.

Se considera necesario destacar que, al ser esta unidad de entidad regimiento, el número de usuarios que hacen uso de los servicios típicos que se dan en una maniobra es bastante superior al que suele haber en las compañías de transmisiones de las brigadas ya que los regimientos son capaces de dar su apoyo incluso hasta la entidad cuerpo de ejército. Teniendo esto en mente, es lógico pensar en un consumo de recursos y de ancho de banda mucho mayor. Un ejemplo puede ser una videoteleconferencia (VTC). No es lo mismo realizar una VTC en la que participen 3 o 4 usuarios durante unos minutos que una videollamada en la que tomen parte una veintena de usuarios durante periodos más largos de tiempo.

Todos esos recursos que se destinan a la VTC mencionada pueden llegar a tumbar el resto de los sistemas si no se hace una gestión eficiente del rendimiento de la red. Por ello, implementar QoS en las redes del RT 1 puede ser una buena medida.

Si no se aplica ninguna medida de QoS, el tráfico que circula por la red se trata por igual sin importar su procedencia (los paquetes de VTC y de otros servicios serían iguales para los routers). Sin embargo, gracias a QoS se le pueden dar prioridad a los paquetes de un determinado servicio o reservar un determinado porcentaje del ancho de banda para ese servicio. De esta forma, ese servicio se ve beneficiado incrementando su calidad.

Es necesario diferenciar dos grandes modelos o mecanismos distintos en los que trabaja QoS:

- Modelo priorizado de servicios integrados (IntServ).
- Modelo priorizado de servicios diferenciados (DiffServ).

El modelo IntServ, deja la función de reserva de recursos a las propias aplicaciones implementando sus protocolos específicos. Respecto al modelo DiffServ, cada paquete es marcado con su tipo para ser identificado por QoS y es éste quien les da una prioridad u otra a los paquetes. Dentro del ámbito del regimiento, es recomendable la utilización del modelo DiffServ, puesto que lo que se pretende conseguir es dar prioridad a determinados servicios como pueden ser la VTC o la VoIP. La Figura 7 muestra un croquis del funcionamiento del modelo DiffServ de QoS:

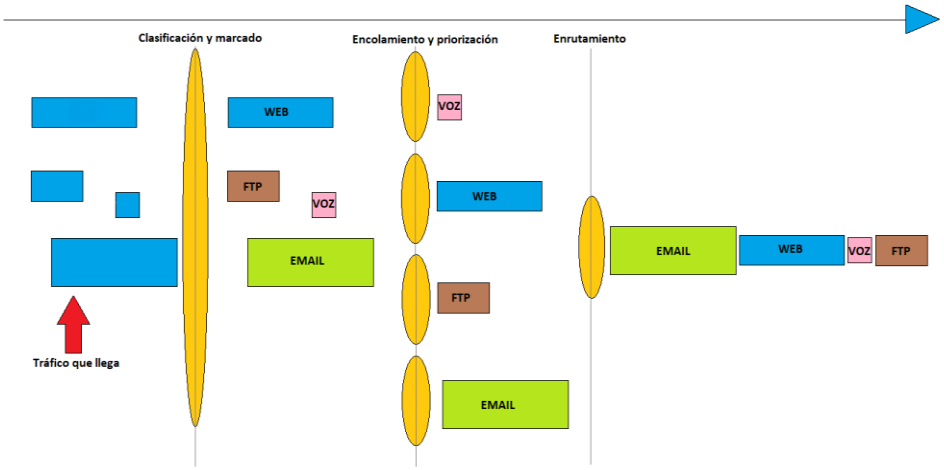

Figura 7 Modelo DiffServ de QoS

Como se observa en la Figura 7, QoS usando el modelo DiffServ recibe todos los paquetes sin ningún tipo de clasificación para, seguidamente, consultar qué tipo de paquete es (un servicio web, un paquete de voz, un mero conjunto de datos, etc.). En el siguiente proceso, QoS prepara los paquetes para su envío según las directrices de prioridad que haya recibido para, finalmente, enrutarlos en el orden que se haya estipulado, un paquete tras otro.

QoS no sólo permite diferenciar y priorizar paquetes en función de su tipo, sino que también es capaz de dedicar un determinado ancho de banda exclusivamente a un tipo de paquetes. Si, por ejemplo, se desea que en un enlace dedique 3 megabits por segundo (Mb/s) exclusivamente a los paquetes de VTC, QoS permite hacerlo. De esta manera, parte del total del ancho de banda que puede pasar por ese enlace tiene dedicación exclusiva a los paquetes de VTC.

El ejemplo mencionado en el párrafo anterior se basa en las opciones de configuración y personalización que permite QoS para cada enlace pudiendo incluso asignar los Mb/s deseados en base a un porcentaje. Por ejemplo, si se tiene un enlace que limita el ancho de banda a 10 Mb/s y se quiere que un 80% de los paquetes estén dedicados a la VoIP, se puede implementar. De esta manera, los paquetes de VoIP tendrían por ese enlace un total de 8 Mb/s exclusivamente para ellos asegurando, obviamente, una excelente calidad en la VoIP.

4.5.2 Red Virtual Multipunto Dinámica

En lo referente a la seguridad de las redes del RT 1, parte de ella está basada en el hecho de que la red no deja de ser una red interna o local cuya salida al exterior se encuentra cifrada mediante el uso de los correspondientes cifradores. Sin embargo, a nivel interno, carecen de este tipo de mecanismos puesto que todo lo que se realiza a nivel local, viaja en claro hasta su paso por los cifradores de salida al exterior. Puesto que una limitación de este proyecto es la imposibilidad de usar los equipos cifradores, reforzar a nivel local la seguridad es una excelente posibilidad. Durante el estudio de la situación del RT 1, una posible solución sería la implementación de Redes Virtuales Multipunto Dinámicas en base a túneles GRE.

Tal y como ya se ha introducido en el capítulo 3, DMVPN utiliza las posibilidades que ofrece

un túnel GRE, ilustrado en la Figura 8a). Sin embargo, el hecho de que sea un multipunto GRE (mGRE) implica una diferencia sustancial con el concepto de túnel punto a punto. La idea de un túnel multipunto mGRE, mostrado en la Figura 8b), es exactamente la misma que la de un túnel, pero con la ventaja de que existan más de dos extremos y éstos resulten más eficientes (Cisco, 2009).

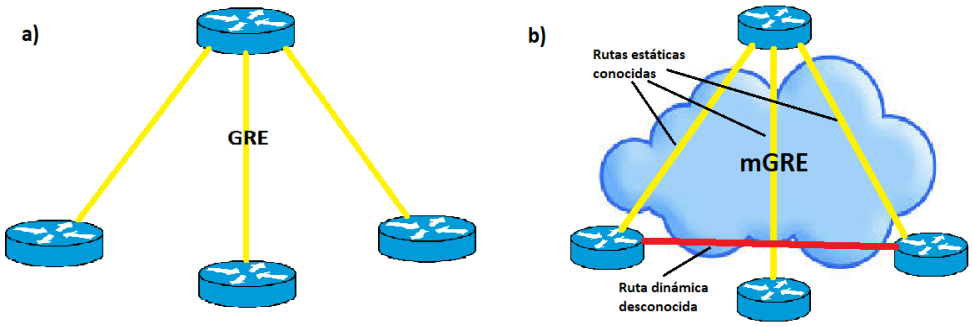

Figura 8 Ejemplo de enlaces GRE y mGRE

En la Figura 8 se puede apreciar la diferencia entre GRE y mGRE. En el caso de la Figura 8a), un paquete que vaya de uno de los routers inferiores a otro router inferior debe pasar por el router superior (como si de una jerarquía se tratase). En cambio, en la Figura 8b) se genera automáticamente una ruta virtual dinámica que conecta directamente ambos routers inferiores sin necesidad de pasar por el superior. De este modo, la congestión de tráfico que debe soportar el router superior se ve sustancialmente mermada.

Gracias a la existencia de más de dos extremos, los caminos posibles por los que pueden viajar los paquetes ya no son fijos. De esta forma, se originan automáticamente rutas virtuales dinámicas que previamente no existían, reduciendo el tráfico por otros lugares al viajar por caminos más eficientes para su llegada al destino.

En lo que respecta a su seguridad, DMVPN por sí solo no la ofrece. Si se quiere incrementar la seguridad en estos enlaces virtuales se les puede añadir el protocolo de red IPSec, el cual permite encriptar los enlaces deseados con múltiples opciones diferentes. De esta forma, se consigue un incremento bastante sensible en la seguridad total de la red. Posee un nivel de implementación medio-alto debido a las múltiples opciones que permite y es capaz de dotar a la red de una robustez en términos de seguridad mucho mayor.

4.5.3 Acuerdo de Nivel de Servicio

El principal cometido de las unidades de transmisiones del ET es facilitar la función de Mando y Control y mantener el enlace. Respecto a esto último, existen herramientas que son capaces de monitorizar las conexiones existentes e informar ante cualquier problema. En el ámbito del RT 1, esta práctica no se realiza normalmente durante los ejercicios y maniobras. Por ello, se considera eficaz y novedoso para el RT 1 un monitoreo de las conexiones que se realicen. De esta forma, se puede saber en todo momento si los enlaces están arriba o alguno ha caído y saber exactamente qué enlace es el que ha caído, aumentando la eficacia y la rapidez para la detección y corrección del problema que haya surgido.

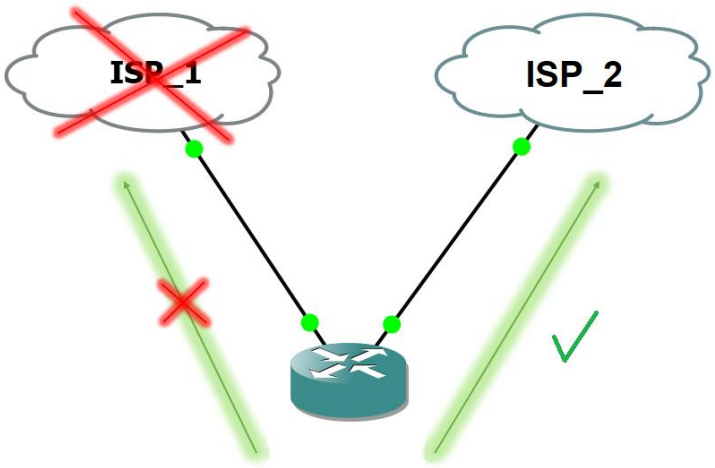

Figura 9 Funcionamiento del protocolo IP SLA (Gabriel, 2020)

La Figura 9 representa el método de funcionamiento del protocolo IP SLA. Como se puede observar, IP SLA irá monitoreando constantemente los enlaces y en el momento que uno de ellos no esté disponible o haya caído (ISP_1 en el caso de la Figura 9), se lo notificará al router. Es necesario destacar que es una herramienta perteneciente a la empresa Cisco, por lo que su utilización sólo es posible en equipos de la marca Cisco. Sin embargo, se debe añadir que la mayoría de los equipos de telecomunicaciones (en lo referente a redes) que utilizan las unidades del ET son de la empresa Cisco. Para el resto de los equipos, existen herramientas muy similares tanto en funcionamiento como en su configuración.

La seguridad de los enlaces IP SLA también puede ser sustancialmente mejorada aplicando nuevamente el protocolo IPSec. La idea es exactamente la misma que la de la implementación en DMVPN solo que aplicada esta vez a IP SLA.

Dado que se trata de un monitoreo para el control de los enlaces pertinentes, se ha tenido en cuenta su aplicación dentro del centro de transmisiones principal ya que es éste el superior a nivel jerárquico. De esta manera, la información sobre el estado de los enlaces llegará a un único controlador dentro de este superior jerárquico, quien será el encargado de notificar la caída de un enlace en caso de que así suceda. No obstante, sus posibilidades no quedan limitadas sólo a un único controlador. En este proyecto se ha decidido realizar de esta manera para mantener la jerarquía de los diferentes centros de transmisiones, aunque no habría problema ninguno si se desease notificar también el estado de los enlaces en los otros centros.

4.5.4 Protocolo de Puerta de Enlace Fronteriza

Cuando se trata de enlazar unas redes con otras, un problema que suele ocurrir es la unificación de éstas para que tengan comunicación entre ellas. Los enrutamientos típicos que se utilizan en el ET funcionan muy bien en el nivel interior. Sin embargo, los protocolos de enrutamiento utilizados no son los más eficaces cuando se trata de comunicarse con una red exterior. Esto es debido a que, generalmente, los protocolos de enrutamiento utilizados en el nivel interior se centran en determinar la ruta más rápida mientras que el objetivo de BGP es determinar la mejor ruta (que no necesariamente es siempre la más rápida).

Además, y dado que cada vez es más frecuente la realización de ejercicios y maniobras conjuntas con ejércitos de otro país, BGP permite una estandarización entre las diferentes configuraciones que posea cada país que colabore en un ejercicio conjunto. Un claro ejemplo de

esto serían los ejercicios que se realizan entre los países pertenecientes a la Organización del Tratado del Atlántico Norte (OTAN), ya que este tipo de colaboraciones son cada vez más frecuentes. Por ello, BGP puede ser configurado en los enlaces de nivel OTAN mientras que, en niveles inferiores, cada país puede poseer unas configuraciones totalmente diferentes de las de otro.

La situación planteada en los párrafos anteriores adquiere mayor sentido cuando se pone en contexto: para las redes en niveles interiores denominadas también sistemas autónomos (AS), es lógico pensar que un enrutamiento rápido es lo más necesario ya que el tamaño de la red no suele implicar una complejidad que suponga problemas. En cambio, en niveles exteriores donde se comunican sistemas autónomos entre sí, es de suponer que es más importante asegurar la información llevándola por la mejor ruta posible, aunque esto lleve un poco más de tiempo.

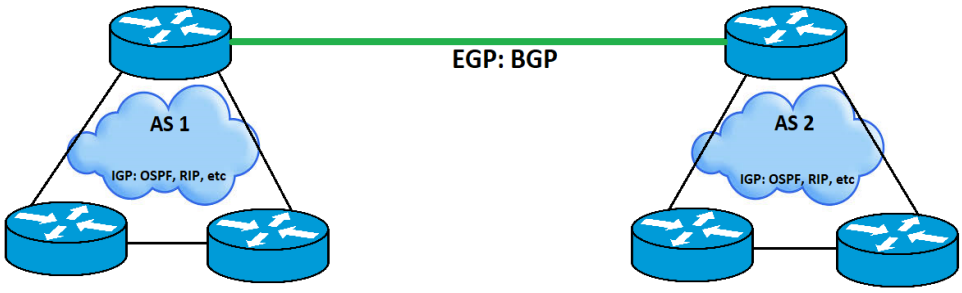

Figura 10 Topología implementando BGP

La Figura 10 muestra una topología sencilla implementando BGP como protocolo de enrutamiento externo (EGP) entre diferentes AS mientras que, a nivel interno se implementan protocolos de enrutamiento internos (IGP).

Es necesario destacar que el protocolo BGP posee encriptación propia. Esto no se da en otros protocolos de enrutamiento y, por ello, BGP se muestra como un excelente candidato para un enrutamiento seguro de los paquetes que se envíen a través de las redes. Se considera necesario destacar además la unificación que permite ya que, a nivel interno poco importa si un AS utiliza unos protocolos u otros ya que para la comunicación entre diferentes AS se utiliza el protocolo BGP. De esta manera, se evitan problemas de compatibilidad por utilizar distintos protocolos a nivel interno.

4.6 IMPLEMENTACIÓN DE PROTOCOLOS

En este apartado se van a abordar los elementos utilizados y las configuraciones necesarias para la implementación de los protocolos de red seleccionados. Además, se explicarán conceptos clave para facilitar la comprensión del funcionamiento de éstos.

4.6.1 Implementación de Calidad de Servicio

Como ya se ha mencionado en el apartado 4.5.1, el mecanismo de implementación que se va a utilizar para QoS es DiffServ. Su funcionamiento está basado en la marcación de los paquetes IP en función del tipo que sean (para VoIP, para VTC, etc.). Dicha marcación se realiza en el campo Tipo de Servicio (ToS) de la cabecera IP.

0-3	4-7	8-15	16-18	19-31
Versión	Tamaño Cabecera	Tipo de Servicio	Longitud Total	
Identificador			Flags	Posición de Fragmento
Time To Live		Protocolo	Suma de Control de Cabecera	
Dirección IP de Origen				
Dirección IP de Destino				
Opciones				Relleno

Figura 11 Cabecera IP de un paquete (Gutierrez, 2015)

La Figura 11 muestra el formato que sigue la cabecera IP de un paquete. Pueden observarse los distintos campos de los que se compone ocupando cada uno de ellos un determinado número de bits hasta completar los 32 bits de los que se compone. Nótese además la localización del campo ToS con una longitud de hasta 8 bits.

Dentro del campo ToS, existe un campo denominado Punto de Código de Servicios Diferenciados (DSCP) el cual posee un valor u otro en función de la prioridad/calidad que requiera el paquete en función de los selectores de clase (CS). Existen valores que proporcionan el reenvío asegurado (AF) y otros que proporcionan un reenvío acelerado (EF). El Anexo IV muestra los diferentes valores que puede tomar DSCP (Aguilera, 2019; Lorge *et al.*, 2019).

Toda esta información puede ser consultada en la propia cabecera IP del paquete en el apartado correspondiente a la información sobre el DSCP.

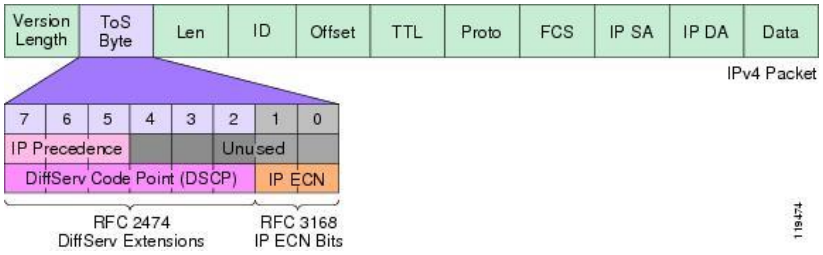

Figura 12 Desglose del campo ToS en un paquete (Cat, 2012)

Como se observa en la Figura 12, en el apartado DSCP localizado dentro del campo ToS irían indicados los valores pertinentes en función de tipo de paquete que se demande con una longitud máxima de 6 bits (del bit nº2 al bit nº7 ambos incluidos). Como ya se ha mencionado antes, se observa además que el campo ToS ocupa 8 de los 32 bits de la cabecera IP.

Respecto a la configuración para implementar QoS en la red, no se trata de un desarrollo excesivamente extenso, pero requiere implementar cada línea de configuración de forma precisa puesto que se trata de una configuración cuyas implementaciones generan una dependencia respecto de las implementaciones configuradas anteriormente. De este modo, cada línea de código debe ir exactamente donde le corresponde.

Para el caso del router del centro de transmisiones principal (CT PPAL), la implementación sería la que sigue:

```
class-map match-all VTC_SALIDA
match ip dscp af41
class-map match-all VTC
match access-group name VTC
```

Se crean dos clases nuevas VTC, una para la salida de los paquetes y otra para la entrada. A la salida de los paquetes se le asigna el DSCP AF41. Este valor indica una anulación del *flash* con una probabilidad de descarte de paquetes baja, lo cual se corresponde con el objetivo deseado puesto que se está trabajando con el servicio de VTC y la transmisión de los paquetes de datos es crítica (se puede consultar el resto de los valores que puede tomar el DSCP en la Tabla 3 dentro del Anexo IV). A la entrada no se le asigna puesto que esta acción se realizará en la configuración siguiente en forma de una nueva política de QoS:

```
policy-map VTC
class VTC
set ip dscp af41
```

Como se ha mencionado anteriormente, a la VTC de entrada se le asigna el valor de DSCP AF41 en otro apartado. Esto es así puesto que esta política será cargada en el interfaz correspondiente a la VTC mientras que la VTC de salida no lleva asociada ningún interfaz directamente, sino que aparecerá como una clase agregada a otra política de QoS.

Hasta este punto, únicamente se han implementado datos correspondientes al marcado de paquetes mediante DSCP para poder identificarlos como paquetes de VTC. Para comprobar el ancho de banda actual que posee el enlace sobre el que se están realizando estas implementaciones, se ha utilizado una herramienta gratuita llamada Iperf.

Iperf consigue mostrar el ancho de banda del enlace en base a dos dispositivos conectados a través de dicho enlace. Un equipo actúa como servidor (se limita a escuchar) mientras que el otro actúa como cliente y se dedica a enviar paquetes con el fin de obtener datos acerca del ancho de banda que posee el enlace.

Esta herramienta no requiere de instalación previa en el equipo, basta con ejecutarla a través del símbolo del sistema del equipo sobre el que se va a utilizar. Por ello, en la situación actual sin haber aplicado aún QoS al enlace, la herramienta Iperf muestra lo siguiente desde el equipo que actúa como servidor:

```
C:\Users\javi_\OneDrive\Escritorio\AGM\Trabajos\5º Curso\TFG\iperf-3.1.3-win64>iperf3.exe -s
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
Accepted connection from 30.30.30.30, port 1594
[  5] local 10.10.10.2 port 5201 connected to 30.30.30.30 port 1595
[ ID] Interval           Transfer     Bandwidth
[  5]   0.00-1.00   sec  11.2 MBytes  94.1 Mbits/sec
[  5]   1.00-2.00   sec  22.4 MBytes   188 Mbits/sec
[  5]   2.00-3.00   sec  22.4 MBytes   188 Mbits/sec
[  5]   3.00-4.00   sec  22.4 MBytes   188 Mbits/sec
[  5]   4.00-5.00   sec  22.4 MBytes   188 Mbits/sec
[  5]   5.00-6.00   sec  22.4 MBytes   188 Mbits/sec
[  5]   6.00-7.00   sec  22.4 MBytes   188 Mbits/sec
[  5]   7.00-8.00   sec  22.4 MBytes   188 Mbits/sec
[  5]   8.00-9.00   sec  22.4 MBytes   188 Mbits/sec
[  5]   9.00-10.00  sec  22.4 MBytes   188 Mbits/sec
[  5]  10.00-10.13  sec  2.84 MBytes   187 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  5]   0.00-10.13  sec  0.00 Bytes  0.00 bits/sec                  sender
[  5]   0.00-10.13  sec   215 MBytes   178 Mbits/sec                  receiver
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
```

Figura 13 Resultados de Iperf (servidor) sin aplicar QoS

Como se puede observar, la Figura 13 muestra que el enlace sin haber aplicado aún QoS posee un ancho de banda medio de 178 Mb/s. Un ancho de banda tan elevado debido a que se trata de una conexión directa mediante un cable Ethernet conectado a interfaces GigabitEthernet.

Para la situación en cuestión, se ha decidido implementar un ancho de banda de aproximadamente 3 Mb/s donde un 95% esté dedicado exclusivamente al enlace VTC. Pese a que el enlace en cuestión posee mucha más capacidad (como se ha observado en la Figura 13) es necesario recordar el limitado ancho de banda máximo del que se suele disponer (con carácter general, no más de 2 Mb/s por cada enlace con terminales satélite). Es por ello por lo que, al configurar el enlace con cerca de 3 Mb/s para VTC aplicando QoS, se les dará prioridad a estos paquetes respecto de cualquier otro tipo, asegurando una calidad de enlace VTC más que razonable.

Otro motivo por el que limitar el ancho de banda del enlace radica en el alto consumo de este en otros sistemas y servicios. Existen servicios como el Sistema para el Mando y Control del Ejército de Tierra (SIMACET/SC2NET) que implican un gran consumo de ancho de banda. Por ello, si este servicio navegase por un enlace compartido con la VTC, lo saturaría y no quedaría prácticamente ancho de banda para la VTC. Al limitar el ancho de banda del enlace y gracias a QoS, este servicio se ve forzado a viajar por otro enlace que se haya configurado.

En lo que respecta a los routers del centro de transmisiones táctico (CT TAC) y del centro de transmisiones avanzado (CT AVA), su configuración es prácticamente la misma que la del router del CT PPAL. La única variación son los interfaces a los que se corresponden los enlaces pertinentes. En el Anexo V se puede consultar la configuración completa de todos los equipos utilizados en este proyecto.

Por tanto, la configuración en el router del CT PPAL sería:

policy-map *3M*

class *VTC_SALIDA*

bandwidth percent *95*

class *class-default*

fair-queue

random-detect

policy-map *SHAPE-INTRATEATRO*

class *class-default*

shape average 3072000

service-policy *3M*

Se crean dos políticas de QoS. La primera, denominada 3M (3 Mb/s), se le asocia la clase VTC de salida creada anteriormente y se le dedica un ancho de banda del 95%. Además, se le aplica una clase por defecto para que, en caso de fallo, QoS funcione mediante su configuración por defecto. La segunda, denominada SHAPE-INTRATEATRO es la correspondiente a los enlaces con los terminales satélites, a los que se les aplica la política 3M para que posean las limitaciones del ancho de banda deseadas.

Finalmente, se le asocia la política SHAPE-INTRATEATRO a cada interfaz de los enlaces con los terminales satélite mientras que al interfaz correspondiente a la VTC se le asocia la política VTC creada inicialmente:

service-policy output *SHAPE-INTRATEATRO* → En el interfaz del satélite al CT TAC

service-policy output *SHAPE-INTRATEATRO* → En el interfaz del satélite al CT AVA

service-policy input *VTC* → En el interfaz de la VTC

Nótese que las dos políticas correspondientes a los enlaces con los terminales satélites son de salida mientras que la correspondiente a la VTC es de entrada. Como ya se ha mencionado, esto se debe a que, por el interfaz de la VTC, los paquetes de datos entran ya con QoS en funcionamiento a los equipos que van a hacer uso de la VTC.

Tras implementar toda la configuración anterior, a continuación, se muestra lo que sucede con la herramienta Iperf una vez aplicada la política 3M:

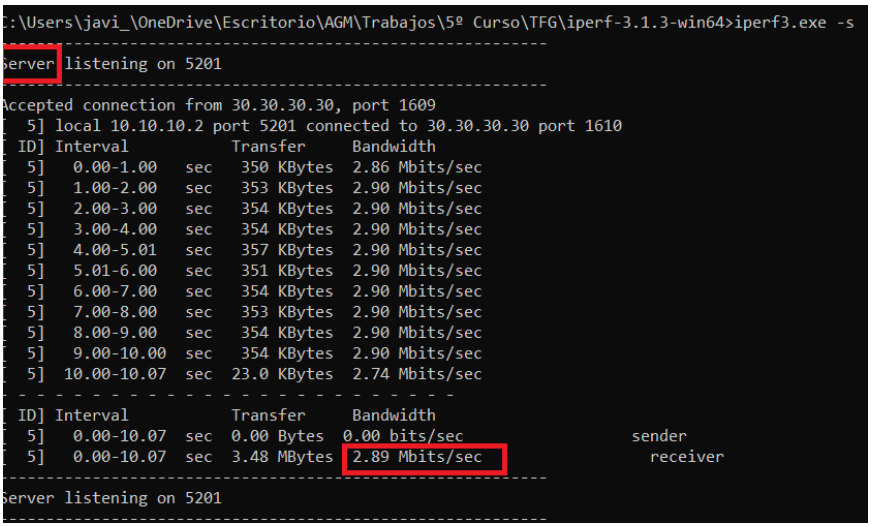

Figura 14 Resultado de Iperf (servidor) tras aplicar QoS

La Figura 14 muestra el ancho de banda medio conseguido en Mb/s en el equipo que trabaja como servidor simulando un equipo conectado a un enlace VTC.

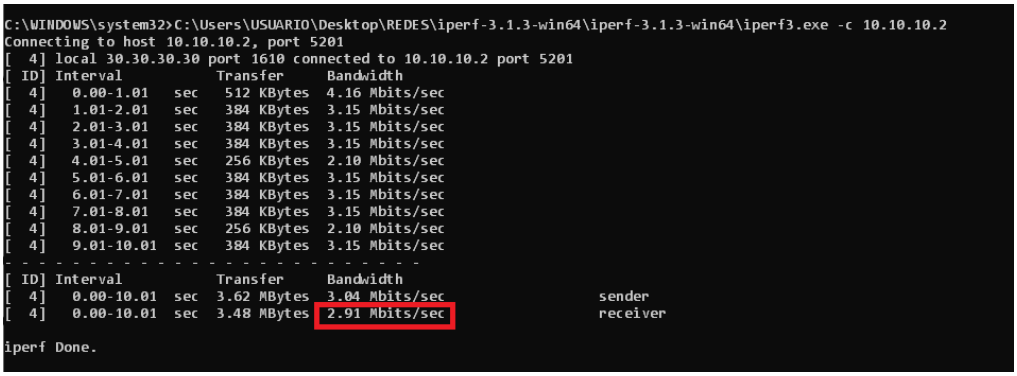

Figura 15 Resultado de Iperf (cliente) tras aplicar QoS

Se puede observar en la Figura 15 la velocidad media obtenida en el equipo que actúa como cliente del enlace VTC.

Analizando ambas figuras, nótese que los datos en ambos casos son muy similares y ambos se aproximan a los 3 Mb/s implementados anteriormente. Se demuestra por tanto la efectividad de la implementación de QoS en los enlaces VTC.

Nótese que QoS funciona de forma aproximada, rara vez será posible conseguir la limitación deseada de forma exacta puesto que existen numerosos factores que influyen durante la transmisión de los paquetes como pueden ser la fluctuación, la latencia, la calidad física del enlace, etc.

4.6.2 Implementación de Red Virtual Multipunto Dinámica

De los protocolos seleccionados para implementar en el RT 1, DMVPN aporta la solución más rápida en términos de descongestión del tráfico de paquetes en las redes. Como ya se ha explicado en el apartado 4.5.2, el hecho de que se generen enlaces dinámicos virtuales permitirá que el router superior (el del CT PPAL en este caso) no reciba demasiado tráfico sobre las

comunicaciones entre el resto de los equipos entre sí y pueda centrarse en las conexiones verdaderamente importantes para él.

En términos de implementación, se trata de dotar al router del CT PPAL de un conocimiento sobre su condición: ser el superior jerárquico o central (el *hub* en términos informáticos) mientras que al resto de routers (el del CT TAC y el CT AVA) hay que hacerles saber que ellos dependen jerárquicamente del *hub*. A estos otros routers se les denomina radios o *spokes.* La configuración de una red de este tipo se denomina, de hecho, *"hub and spoke".* Sin embargo, en el caso que se presenta en esta memoria, DMVPN es el siguiente salto lógico en este tipo de configuraciones. DMVPN utiliza la configuración típica de una red *hub and spoke* y la optimiza evitando que el router que actúa como *hub* reciba información excesiva y que no es útil para sus funciones.

En el caso del router del CT PPAL, puesto que actúa como *hub*, se implementará inicialmente la configuración de un túnel GRE en él y se le dotará de las funciones propias de un router *hub* al mismo tiempo que se le asignarán las funciones para actuar también como un mGRE:

```
interface tunnel 100
ip address 30.0.0.1 255.255.255.0
no ip redirects
ip nhrp map multicast dynamic
ip nhrp network-id 1
tunnel source 192.168.1.2
tunnel mode gre multipoint
```

La configuración para el router *hub* se basa en la creación de un nuevo túnel GRE al que se le asigna numeración y dirección IP propias. Se observa la llamada a un protocolo que no se ha utilizado anteriormente, el protocolo de resolución de siguiente salto (NHRP) que es quien permite que se establezca el túnel GRE en su forma dinámica (permitiendo que se generen los enlaces automáticamente). El comando *network-id* identifica la red DMVPN como la red 1. De esta forma, si la id no se corresponde a la red 1 (por ejemplo, red 4), no se generarán los túneles entre los routers. Finalmente, se le asigna al túnel GRE la dirección IP física que tendrá y el modo multipunto para que funcione como mGRE.

Para el caso de los routers que actúan como *spokes*, la configuración tanto para el CT TAC como para el CT AVA es la misma sólo difiriendo en sus respectivas direcciones IP. En el caso del router del CT TAC, la configuración sería:

interface tunnel *100*

ip address *30.0.0.2 255.255.255.0*

no ip redirects

ip nhrp map *30.0.0.1 192.168.1.2*

ip nhrp map multicast *192.168.1.2*

ip nhrp network-id *1*

ip nhrp nhs *30.0.0.1*

tunnel source *192.168.1.6*

tunnel mode gre multipoint

Nótense las diferencias respecto a la configuración del router del CT PPAL. Las dos líneas señaladas en color verde consisten en decirle a los routers *spoke* cuál es su camino para llegar al router *hub*. Por otro lado, la línea señalada en color rojo introduce al servidor del siguiente salto (NHS). La función de esta línea es informar a los *spokes* cuál es el interfaz del túnel por el que se accede al *hub*.

Para el router del CT AVA, la configuración es la misma que para el router del CT TAC, pero modificando los interfaces pertinentes. Para obtener la configuración completa de cada router, consulte el Anexo V.

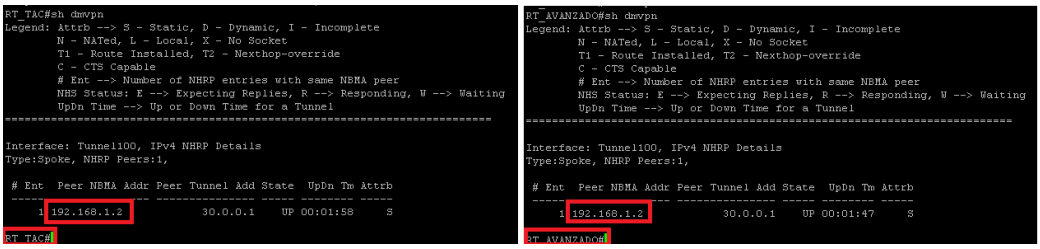

Figura 16 Túneles GRE generados en CT TAC y CT AVA

Se puede observar que la Figura 16 muestra cómo efectivamente los routers del CT TAC y del CT AVA han generado una ruta hacia el router del CT PPAL. Sin embargo, este enlace consiste en un enlace de tipo GRE como el mostrado en la Figura 8a). Es lógico pensar que el camino más corto para llegar del CT TAC al CT AVA es una conexión directa entre ambos sin necesidad de pasar por el CT PPAL (el router *hub*) y esto sólo es posible mediante mGRE.

Para que se genere ese enlace directo, es necesario que ambos routers (CT TAC y CT AVA) se envíen información. Simplemente con ejecutar el comando *ping* en sendos routers para enviar paquetes de comprobación, se generará un nuevo túnel:

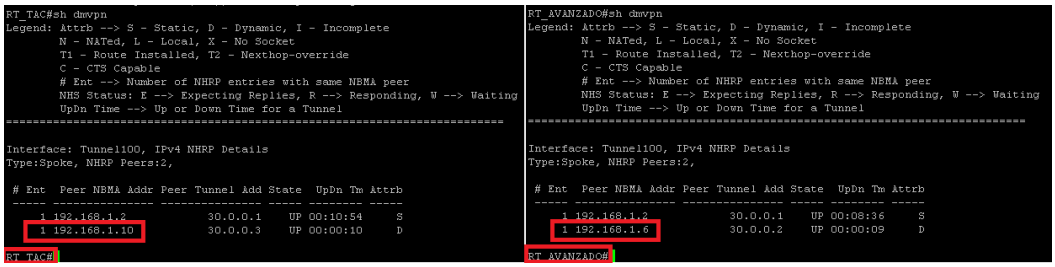

Figura 17 Túneles GRE dinámicos recién generados

Como muestra la Figura 17, en ambos routers se ha generado un enlace directo del uno al otro. Se trata de un túnel que va de un *spoke* a otro *spoke* sin pasar por el *hub*. Nótese además que este enlace posee la letra D como atributo. Esta letra se corresponde a un tipo de enlace que se ha creado dinámicamente. La situación se corresponde por tanto a la mostrada en la Figura 8b), por lo que ya se está haciendo uso de túneles mGRE y, desde este momento, el tráfico de los routers del CT TAC y del CT AVA ya no tienen que pasar por el router del CT PPAL.

Ya se ha mencionado que DMVPN por sí solo no ofrece seguridad. Se considera una buena práctica por tanto implementar el protocolo IPSec (explicado en el capítulo 3 de esta memoria) en estos enlaces para incrementar la robustez general.

Hay que tener en cuenta que, al estar utilizando mGRE en este proyecto, los enlaces que se crean de forma dinámica son escasos debido al tamaño que posee la red con la que se está trabajando. Sin embargo, para la situación en la que existiesen muchísimos más centros a comunicar, si se implementa mGRE se generarían grandes cantidades de enlaces virtuales dinámicos. Por ello, para dotar a la red de una mayor robustez, sería necesario implementar IPSec en todos y cada uno de los enlaces que se generen.

La situación mencionada en el párrafo anterior obviamente no es eficiente. No obstante, nótese que únicamente se ha utilizado un único interfaz túnel (asignado al nº 100 en este proyecto) para la configuración de mGRE. Por tanto, para que el protocolo IPSec funcionase con todos y cada uno de los enlaces que se generen de forma dinámica, basta con implementar IPSec en el interfaz del túnel dentro de todos los routers. De este modo, la cantidad de líneas a implementar se reduce sensiblemente.

Procediendo con la implementación, la configuración para todos los routers (CT PPAL, CT TAC y CT AVA) sería:

crypto isakmp policy *10*

authentication pre-share

crypto isakmp key *cisco123* **address** *192.168.1.0*

crypto ipsec transform-set *set1* **esp-aes** *256* **esp-sha-hmac**

mode *tunnel*

crypto ipsec profile *IPSEC_DMVPN*

set transform-set *set1*

Se crea una política de encriptación a la que se le asigna número, contraseña y dirección IP

a cifrar. Posteriormente se genera un set al que se le asigna un tamaño de encriptación (encriptación de 256 bits en este caso) y se le añade el modo túnel. Finalmente, se crea un perfil al que se le asocia el set creado anteriormente.

Lo último que hay que hacer es entrar en el interfaz del túnel y asignarle la protección:

tunnel protection ipsec profile *IPSEC_DMVPN*

De esta manera, el interfaz túnel nº100 posee el perfil creado con todas las configuraciones anteriores.

```
RT_PPRAL#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.1.2     192.168.1.10    QM_IDLE           1001 ACTIVE
192.168.1.2     192.168.1.6     QM_IDLE           1002 ACTIVE

IPv6 Crypto ISAKMP SA

RT_PPRAL#
```

Figura 18 IPSec activo en el router del CT PPAL

La Figura 18 muestra que el protocolo IPSec efectivamente está activo en los interfaces que viajan del CT PPAL a los otros dos centros. Nótese que el viaje se realiza a través de las direcciones IP reales (las correspondientes a las direcciones 192.168.1.0), no las direcciones IP del túnel (correspondientes a las direcciones 30.0.0.0) ya que estas direcciones no dejan de ser virtuales e interesa que la encriptación suceda en las conexiones reales.

Sin embargo, con la Figura 18 sólo se está comprobando la efectividad de IPSec en un enlace determinado. Lo interesante es que este protocolo puede también actuar en las rutas dinámicas. Obsérvese cómo está actuando el protocolo IPSec en el router del CT TAC:

```
RT_TAC#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.1.2     192.168.1.6     QM_IDLE           1001 ACTIVE
192.168.1.10    192.168.1.6     QM_IDLE           1002 ACTIVE

IPv6 Crypto ISAKMP SA

RT_TAC#
```

Figura 19 IPSec activo en enlaces dinámicos del router del CT TAC

Como muestra la Figura 19, efectivamente el protocolo IPSec está actuando en el enlace virtual directo que se ha generado anteriormente. Hay que destacar que sucede exactamente lo mismo en el router del CT AVA. Por tanto, se demuestra que el protocolo IPSec puede actuar de forma eficaz en DMVPN dotando así a la red de una mayor robustez respecto de la que tenía anteriormente.

4.6.3 Implementación de Acuerdo de Nivel de Servicio IP

Siguiendo la topología de red de este proyecto, se puede observar que es interesante implementar IP SLA en los enlaces hacia los terminales satélites ya que, de esta manera, se podría llevar el monitoreo de éstos. En caso de que un terminal satélite cayese, automáticamente será notificado en pantalla y se podrían llevar a cabo las medidas pertinentes para solucionar el

problema. La gran ventaja radica en el hecho de que ya desde el primer momento se conocería el origen del problema y se podría solucionar directamente evitando contratiempos por no conocer cuál es el terminal satélite que está dando problemas.

Dado que el centro de transmisiones principal (CT PPAL) posee dos enlaces hacia terminales satélites mientras que los centros de transmisiones táctico (CT TAC) y avanzado (CT AVA) poseen un terminal satélite cada uno, la configuración de IP SLA que hay que llevar a cabo es diferente.

Para la topología de red en cuestión, dentro de la configuración del router del CT PPAL habría que introducir los siguientes comandos:

ip sla *1*

icmp-echo *192.168.1.14* **source-ip** *192.168.1.13*

frequency *5*

ip sla schedule *1* **life** *forever* **start-time** *now*

Donde para el enlace con el CT TAC se crea un IP SLA nº1 que enviará paquetes de comprobación desde la dirección IP acabada en .13 hacia la dirección IP acabada en .14 cada 5 segundos. Se le asigna además una configuración cuya duración será para siempre y su inicio será ahora mismo.

ip sla *2*

icmp-echo *192.168.1.18* **source-ip** *192.168.1.17*

frequency *5*

ip sla schedule *2* **life** *forever* **start-time** *now*

Puede observarse que la configuración para el enlace con el CT AVA sólo difiere de la configuración para el enlace con el CT TAC en la numeración inicial (necesaria para indicar que son configuraciones diferentes) y en las direcciones IP correspondientes a sus respectivos enlaces.

Además, IP SLA ofrece una solución en caso de que un enlace caiga. Si esto sucede, los datos son redireccionados por otro camino. Para conseguir que esto suceda, se deben implementar unos elementos denominados *tracks* que se asocian a cada IP SLA configurado y son los encargados de llevar el monitoreo de los enlaces:

track *1* **ip sla** *1* **reachability**

track *2* **ip sla** *2* **reachability**

ip route *20.20.20.0 255.255.255.0 192.168.1.14* **track** *1*

ip route *30.30.30.0 255.255.255.0 192.168.1.18* **track** *2*

La configuración anterior muestra la creación de dos *tracks* y la asociación de éstos a los dos enlaces indicados anteriormente. La Figura 18 muestra el resultado de pedirle a IP SLA un resumen de su configuración:

```
RT_PPRAL#sh ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending

ID           Type        Destination       Stats       Return      Last
                                           (ms)        Code        Run
---------------------------------------------------------------------
*1           icmp-echo   192.168.1.14      RTT=1       OK          2 seconds ago



*2           icmp-echo   192.168.1.18      RTT=1       OK          3 seconds ago



RT_PPRAL#
```

Figura 20 Protocolo IP SLA en correcto funcionamiento

Como se observa en la Figura 20, se han creado dos elementos de IP SLA asociados cada uno a un enlace y están activos (OK).

Para comprobar que efectivamente funciona, se ha provocado la caída de uno de los enlaces y, como se observa en la Figura 21, automáticamente se ha generado un mensaje avisando que uno de los enlaces ya no está disponible:

```
RT_PPRAL#
*Sep 22 12:50:00.018: %TRACK-6-STATE: 1 ip sla 1 reachability Up -> Down
RT_PPRAL#sh ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending

ID           Type        Destination       Stats       Return      Last
                                           (ms)        Code        Run
---------------------------------------------------------------------
*1           icmp-echo   192.168.1.14      -           Timeout     12 seconds ag
                                                                   o


*2           icmp-echo   192.168.1.18      RTT=1       OK          3 seconds ago



RT_PPRAL#
```

Figura 21 Enlace de IP SLA caído

Además, al solicitar un resumen de IP SLA, se observa también que el enlace de la dirección IP acabada en .14 lo señala como caído (*Timeout*).

Al ser IP SLA un protocolo que realiza un monitoreo continuo, también informa cuando un enlace que previamente estaba caído se encuentra disponible de nuevo:

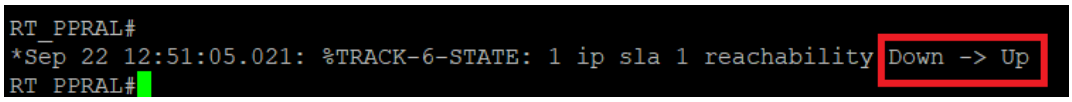

Figura 22 Enlace de IP SLA disponible nuevamente

Como muestra la Figura 22, al volver a conectar el enlace caído, automáticamente IP SLA notifica que el enlace vuelve a estar disponible.

Dado que se ha tenido en cuenta implementar IPSec cuando se ha trabajado con DMVPN, es lógico pensar que IPSec puede ser utilizado en otros enlaces, y así es. Implementar IPSec en los enlaces IP SLA es sencillo de realizar y se consigue una mayor seguridad en los mismos. De este modo, no hace más que seguir beneficiando a la robustez de la red completa. Por ello, en este proyecto también se realizará la implementación de IPSec en los enlaces que posean IP SLA. La diferencia respecto de la implementación de IPSec en DMVPN se centra en señalar los enlaces que correspondan a IP SLA en vez de a los de DMVPN. El resto de las diferencias radican principalmente en la diferencia que existen entre los interfaces dedicados a IP SLA y los interfaces túnel dedicados a DMVPN.

En el caso del router del CT PPAL, la implementación de IPSec para los enlaces de IP SLA sería la que sigue:

```
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 5
lifetime 3600
```

La configuración anterior muestra la creación de una política de encriptación con una descripción numérica sobre la que se implementará lo que se necesite con un algoritmo de encriptación de 256 bits y un tiempo de renovación cada 3600 segundos.

```
crypto isakmp key cisco123 address 192.168.1.14
crypto isakmp key cisco123 address 192.168.1.18

crypto ipsec transform-set set1 esp-aes 256 esp-sha-hmac
mode tunnel

ip access-list extended IPSEC_NUESTRO
permit ip 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255
```

Se puede observar que se han creado claves asociadas a cada dirección IP de los enlaces con IP SLA. Además, se implementa en modo túnel y se limita el número de direcciones IP a un

rango determinado mediante una lista de acceso denominada “IPSEC_NUESTRO”.

crypto map *CMAP_TAC 10* **ipsec-isakmp**

set peer *192.168.1.14*

set transform-set *set1*

match address *IPSEC_NUESTRO*

crypto map *CMAP_AVA 10* **ipsec-isakmp**

set peer *192.168.1.18*

set transform-set *set1*

match address *IPSEC_NUESTRO*

Finalmente, se crea un mapa criptográfico para cada enlace con cada centro de transmisiones al que se le asocia su correspondiente dirección IP, su set en modo túnel y se le incluye dentro de la lista de acceso implementada anteriormente.

Lo último que faltaría sería asociar sendos mapas criptográficos a cada uno de los interfaces físicos conectados al router del CT PPAL:

crypto map *CMAP_TAC* → En el interfaz correspondiente al CT TAC

crypto map *CMAP_AVA* → En el interfaz correspondiente al CT AVA

De este modo, la configuración de IPSec en los enlaces IP SLA ya estaría implementada. La Figura 21 muestra a IPSec en funcionamiento:

```
RT_PPRAL#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.1.14    192.168.1.13    QM_IDLE           1002 ACTIVE
192.168.1.18    192.168.1.17    QM_IDLE           1003 ACTIVE

IPv6 Crypto ISAKMP SA

RT_PPRAL#
```

Figura 23 IPSec activo en los enlaces de IP SLA

Como se puede observar, la Figura 23 muestra que IPSec se encuentra en estado activo en los enlaces utilizados para el monitoreo mediante IP SLA. De este modo, estos enlaces poseen una encriptación y un nivel de seguridad mucho mayor que antes, provocando una gran robustez (en términos de seguridad) en el monitoreo de las redes del regimiento.

Al igual que con los protocolos anteriores, las implementaciones realizadas anteriormente son similares para los routers del CT TAC y del CT AVA y pueden ser consultadas en el Anexo V junto con las implementaciones completas realizadas en el router del CT PPAL.

4.6.4 Implementación de Protocolo de Puerta de Enlace Fronteriza

Ya se ha mencionado anteriormente la importancia del protocolo BGP y la viabilidad de su implementación. Su configuración no se diferencia mucho de la configuración habitual de cualquier otro protocolo de enrutamiento dinámico. Sin embargo, BGP exige un conjunto de direcciones IP sobre las que va a trabajar además de la posibilidad de reforzar la seguridad de las conexiones a través de contraseñas encriptadas.

Nuevamente, la implementación se centrará en la correspondiente al router del CT PPAL puesto que para el resto de routers es similar sólo difiriendo en las direcciones IP correspondientes a cada centro. Se recuerda que en el Anexo V figura la configuración completa de todos los equipos utilizados.

Por tanto, en el router del CT PPAL se comenzaría a configurar el protocolo BGP de la siguiente manera:

router bgp *34001*

bgp log-neighbor-changes

neighbor *192.168.1.6* **remote-as** *34002*

neighbor *192.168.1.6* **description** *ENLACE TAC*

neighbor *192.168.1.6* **password** *cisco123*

neighbor *192.168.1.10* **remote-as** *34003*

neighbor *192.168.1.10* **description** *ENLACE AVA*

neighbor *192.168.1.10* **password** *cisco123*

Se llama al protocolo BGP asignándole un número que será el AS de este centro. Seguidamente, se añaden las direcciones IP físicas de los otros AS (uno por cada centro de transmisiones) a los que se les agrega además una descripción y una contraseña que será cifrada posteriormente.

La siguiente implementación consiste en generar un grupo o familia de direcciones IP ya que este es el lenguaje que utiliza el protocolo BGP para enrutar:

address-family ipv4

network *1.1.1.1* **mask** *255.255.255.255*

aggregate-address *10.10.10.0 255.255.255.0* **summary-only**

redistribute ospf *1*

neighbor *192.168.1.6* **activate**

neighbor *192.168.1.6* **send-community both**

neighbor *192.168.1.6* **soft-reconfiguration inbound**

neighbor *192.168.1.10* **activate**

neighbor *192.168.1.10* **send-community both**

neighbor *192.168.1.10* **soft-reconfiguration inbound**

exit-address-family

Las primeras líneas se centran en las redes que cuelgan directamente del router del CT PPAL como son la red 1.1.1.1 determinada como una red por defecto (*Loopback*) y la red 10.10.10.0 correspondiente a la VTC. Hay que destacar el uso del comando *aggregate-address* para simplificar las direcciones IP que se muestren en pantalla. Si se trata de redes muy grandes, el listado de redes sería de dimensiones desproporcionadas para un análisis eficiente. Con este comando se consigue sólo mostrar las direcciones que interesen como es la dirección de la VTC en el caso que concierne a este proyecto.

Nótese también el comando *summary-only*, el cual resume o agrupa las direcciones IP en su superior correspondiente para simplificar los enlaces activos mostrados en pantalla. El resto de los comandos se centran en introducir las direcciones declaradas en el protocolo BGP dentro de la familia de direcciones para que BGP las trate como direcciones a enrutar.

Lo último que falta por hacer es encriptar las contraseñas utilizadas para que BGP funcione correctamente. Esto se realiza a través de una única línea de configuración:

```
Service password-encryption
```

Con esto, se consigue que las contraseñas queden encriptadas permitiendo que el protocolo BGP funcione correctamente. De hecho, puede observarse como una contraseña de baja seguridad como era “cisco123” ha pasado a transformarse en:

```
neighbor 192.168.1.6 password 7 02050D4808095E731F
neighbor 192.168.1.10 password 7 03189C7756901F634D
```

Se puede observar cómo la información contenida en “cisco123” se ha visto modificada por completo al ser encriptada. Con ello, se mejora la robustez del protocolo cuando entre en funcionamiento.

Tras esto, la implementación el protocolo BGP estaría finalizada en el CT PPAL y en el resto de los centros habría que realizar una implementación similar (tal y como recoge el Anexo V). Si ahora, con todos los equipos implementando BGP de su correspondiente manera, se comprueban las redes de las que tiene información el router del CT PPAL:

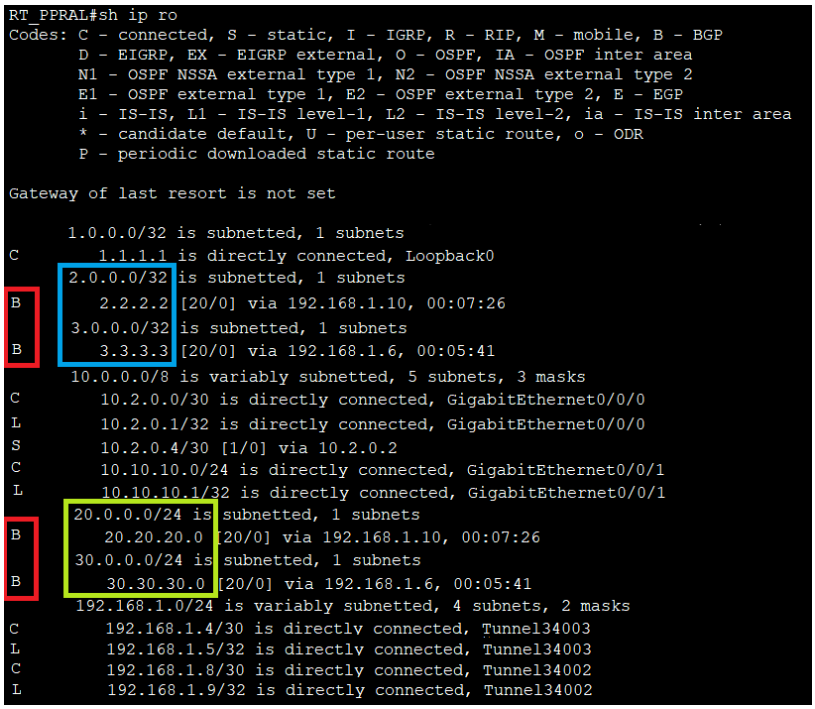

Figura 24 Protocolo BGP funcionando en el router del CT PPAL

Como se observa en la Figura 24, se han generado rutas a las direcciones de los routers pertenecientes a los otros centros de transmisiones indicadas con la letra B haciendo referencia al uso del protocolo BGP para llegar a esa dirección IP. De esta forma se comprueba que el protocolo BGP funciona correctamente.

Nótese también que efectivamente sólo se ha compartido la información correspondiente a la VTC (las direcciones 20.20.20.0 y 30.30.30.0 de los centros TAC y AVA respectivamente, indicadas en amarillo) y a las interfaces por defecto *Loopback* 2.2.2.2 y 3.3.3.3 (indicadas en azul). De no haberlo simplificado y tener una red con muchas más conexiones, en esta pantalla se mostrarían multitud de redes más.

4.7 ANÁLISIS Y RESULTADOS

En este apartado se expone un análisis sobre los resultados obtenidos en las pruebas de implementación de los protocolos de red seleccionados.

Tal y como se ha ido viendo durante el desarrollo de esta memoria, todos los protocolos implementados aportan a las redes del RT 1 una mejora y actualización en múltiples aspectos tales como la calidad, la seguridad, el control, etc.

Teniendo en cuenta que cada protocolo implementado es completamente diferente, no tiene sentido realizar una comparativa entre ellos. Sin embargo, se considera necesario analizar y exponer los resultados en base a una comparativa de redes que no incluyan estos protocolos y redes que sí.

Siguiendo con la idea del párrafo anterior, QoS ha sido el primero de los protocolos seleccionados e implementados. Se ha seleccionado dado su gran abanico de posibilidades y sus múltiples opciones de configuración no sólo en velocidades de transmisión de los datos sino también en priorización de diferentes tipos de datos o servicios.

Como ya ha quedado patente en el apartado 4.6.1 de esta memoria, los resultados de la implementación de QoS en las redes del RT 1 han mostrado que es una gran oportunidad para mejorar las comunicaciones que ofrece y, especialmente, todo lo referente a VTC dada su enorme demanda por parte del personal de los puestos de mando durante misiones y maniobras.

En lo que respecta a la implementación de DMVPN, la descongestión de tráfico que ofrece además de la posibilidad de utilizarlo con redes mucho más grandes ha hecho que sea una buena opción para el RT 1. Además, el poder reforzar la seguridad de estos nuevos enlaces que se generan mediante el protocolo IPSec es otro aliciente para su implementación en el regimiento.

Los resultados observados en el apartado 4.6.2 de esta memoria han demostrado que las rutas virtuales dinámicas que DMVPN genera son automáticas y, además, pueden ser prácticamente ilimitadas (básicamente el tamaño del mGRE queda definido por el tamaño de la máscara de red que se aplique a la dirección IP asignada al mGRE). Por ello, la implementación de IPSec aplicada directamente al entorno entero del mGRE hace que su configuración se simplifique sensiblemente permitiendo que tanto configurar DMVPN como IPSec sea factible y útil para el RT 1. Al ser una unidad de entidad regimiento, el tamaño de las redes que controla e implementa puede variar muchísimo. Así, aplicar DMVPN puede dotar al RT 1 de una mayor versatilidad a nivel de configuración de equipos.

Sobre el protocolo IP SLA, es necesario destacar sobre todo la capacidad de monitoreo que ofrece y la facilidad de implementar y configurar. Tras las pruebas realizadas durante el desarrollo de este proyecto se ha observado cómo este protocolo permite un monitoreo y un control excelentes de una manera bastante sencilla.

Los resultados aplicando IP SLA han sido lo suficientemente satisfactorios como para ser un protocolo para tener muy en cuenta de agregar a las implementaciones normales que suela utilizar el regimiento. Como ya se ha explicado con anterioridad, tener IP SLA funcionando y monitoreando los enlaces desde el CT PPAL sobre el que cuelgan el resto de una manera u otra resulta de una gran opción para mejorar la gestión y control de todo el entorno de red del RT 1. Además, poder implementarle IPSec para aumentar la seguridad permite que este control y monitoreo sea, además, encriptado y seguro para las comunicaciones.

Finalmente, BGP ha sido el último protocolo implementado durante la realización de este trabajo. Su elección proviene de la normalización y homogeneización de redes. Es lógico pensar que cada pequeña o gran red de cada ejército posea sus propias configuraciones e implementaciones que poco o nada tendrán que ver con las configuraciones utilizadas por el ET aquí en España. Por ello, de cara a una unificación de procesos, el protocolo BGP recoge todos ellos y los enruta mediante un lenguaje común y además encriptado para una mayor seguridad.

Los resultados obtenidos han permitido una transferencia de información mediante el protocolo BGP satisfactoria. Hay que destacar lo que se ha indicado en el apartado 4.6.4 de esta memoria: la posibilidad de elegir exactamente qué bloques de direcciones IP mostrar. De este modo, la información que aparece por pantalla se puede observar de manera simplificada haciendo mucho más sencillo su análisis para el administrador encargado de controlar estos enlaces.

4.7.1 Escenarios posibles

Teniendo en cuenta lo expuesto anteriormente y dadas las características y opciones que ofrecen los protocolos implementados, existen una serie de escenarios posibles sobre los que tratar en función de las necesidades que se requieran.

Obviamente, poder tener los cuatro protocolos seleccionados funcionando al mismo tiempo

es la mejor opción, pero no siempre es posible puesto que existen factores que obligan a priorizar unos sobre otros como puede ser la rapidez de implementación, el tiempo disponible para el despliegue y puesta en funcionamiento de los centros de transmisiones, etc.

Teniendo en cuenta lo anterior mencionado, a continuación, se muestran los posibles escenarios planteados acorde al contexto en que se desarrolla este proyecto y teniendo en cuenta el hecho de que no siempre será posible conseguir una red en la que los cuatro protocolos de red estén trabajando simultáneamente:

Tabla 1 Escenarios posibles

Escenarios	Características mejoradas	Protocolos que implementar
Escenario 1	Seguridad	BGP e IPSec
Escenario 2	Monitoreo y control de la red	IP SLA
Escenario 3	Calidad y capacidad de maniobra	QoS y DMVPN

La Tabla 1 muestra, de manera simple y resumida, una serie de escenarios posibles que se desarrollan con mayor detalle a continuación:

- **Escenario 1:** Si lo que se desea es una ampliación general del nivel de seguridad, lo más apropiado sería darle prioridad a la implementación del protocolo BGP para las comunicaciones entre los distintos AS que participen en la maniobra obteniendo esa compatibilidad a nivel OTAN ya mencionada anteriormente. Además, sería muy aconsejable complementar esto con el protocolo IPSec a nivel interno ya visto tanto para IP SLA como para DMVPN.

- **Escenario 2:** Por otro lado, si el requisito indispensable estuviese centrado en el control de la red, el protocolo más apropiado sería IP SLA por su gran control del estado de los enlaces y por su rapidez de implementación. Ello permitiría estar controlando la red desde un tiempo posterior a la instalación de los enlaces muy breve. Además, gracias a la reducción de este tiempo de detección, el problema que se encontrase en el enlace que el protocolo IP SLA detectase también sería solucionado con anterioridad gracias a poder enfocar el problema sólo al área que haya detectado el protocolo.

- **Escenario 3:** Finalmente, otro posible escenario que se plantea tiene como referente la capacidad de maniobra y la calidad de los enlaces. Como ya se ha mencionado anteriormente, en términos de calidad y de personalización, es QoS el más recomendable para ser implementado ya que ofrece multitud de opciones diferentes acordes a las necesidades que demande la maniobra. A éste se le sumaría además DMVPN ya que ofrece una capacidad de maniobra extraordinaria tanto por su generación automática de enlaces dinámicos (evitando preocupaciones en cuando al dimensionamiento de la red) como por su refuerzo en términos de seguridad gracias a complementarlo con el protocolo IPSec.

Se considera necesario destacar que, pese a los posibles escenarios planteados, la solución

óptima radica en implementar todos los protocolos en conjunto y así poder aprovechar las opciones que ofrece cada uno. De esta manera, se dotaría al regimiento de una red totalmente actualizada tanto en términos de seguridad como de personalización como de opciones de control.

Tal y como se menciona en el apartado 2.1 de esta memoria, una red con las características que se han obtenido durante el desarrollo de este proyecto puede llevarse al resto de unidades de transmisiones del ET a fin de unificar características y de actualizar de manera general todo el entorno de red que posee el ejército.

A la vista de lo comentado en los párrafos anteriores, en la Tabla 2 se muestra un breve resumen de lo que se ha comentado en estos a modo de comparativa entre una red a la que se le implementan los protocolos desarrollados y configurados en este proyecto y otra red sin ninguno de estos protocolos añadidos a su configuración:

Tabla 2 Comparativa respecto a la aplicación o no de los protocolos

	Protocolos sin implementar	**Protocolos implementados**
Control y detección de fallos	Siempre con un tiempo de reacción medio alto debido a la falta de opciones de monitoreo	Detección de fallos prácticamente inmediata gracias a IP SLA y notable reducción del tiempo de reacción.
Seguridad	Hacia el exterior: la que ofrezcan los cifradores. A nivel local: la seguridad que ofrece la red por el hecho de ser una red local.	Hacia el exterior: la que ofrecen los cifradores reforzada con una mayor encriptación gracias a BGP A nivel local: notable aumento de la seguridad gracias a la implementación de IPSec a nivel interno.
Grado de personalización	Bajo. Dependiente en todo momento de las características físicas de los medios y escasa probabilidad de modificación.	Total. Selección de necesidades de ancho de banda, priorización de paquetes según el tipo que más se demande, etc. Gracias a la implementación de QoS
Compatibilidad	Se requiere un lenguaje de protocolos totalmente común a todos los equipos para evitar problemas de comunicación.	Unificación en las comunicaciones independientemente de lo que suceda a nivel interno gracias al protocolo BGP.
Tamaño de redes	Necesario conocerlo con precisión. Limitaciones de los equipos por congestión de tráfico de paquetes.	Totalmente moldeable evitando congestión de tráfico de paquetes al implementar DMVPN.

La Tabla 2 analiza de manera breve aspectos clave para tener en cuenta en el momento de decidir implementar los protocolos elegidos o no. Como se puede comprobar, en el ámbito del ET y de los servicios que se suelen demandar, todos ellos se presentan como una gran oportunidad de actualización de las redes del RT 1.

Una vez expuestos los escenarios planteados y los aspectos clave de los protocolos seleccionados, se considera conveniente dedicarle unas líneas a los dos protocolos que finalmente no han sido implementados en el laboratorio de este proyecto: VRF y VTP. A continuación, se mencionan aspectos ventajosos de su implementación si ello sucediera:

- **VRF:** Como ya se ha mencionado, la dimensión de una red que implemente VRF debe ser lo suficientemente grande como para que tenga sentido utilizarlo. De ser este el caso, el protocolo VRF mejoraría la funcionalidad general de la red puesto que simplifica el trabajo de los routers. Esta simplificación la consigue separando el enrutamiento y el tráfico de distintos clientes/usuarios utilizando el mismo router. Sin embargo, las redes que se manejan en el ámbito de este proyecto no son lo suficientemente grandes ya que no se trabaja con una cantidad importante de routers y *switches*.

- **VTP:** Tal y como se ha descrito, este protocolo ya está implementándose en el RT 1. Es por ello por lo que en esta memoria ha sido descartado para su desarrollo. No obstante, las capacidades que ofrece son muy positivas. Lo que ofrece este protocolo es una simplificación a nivel de configuración de equipos. Tomando uno de los *switches* que se utilicen como “maestro” y configurando en este todas las opciones que se demanden, el resto de los *switches*, los “subordinados”, copian automáticamente las configuraciones sin necesidad de introducirlas manualmente en cada uno de ellos. Gracias a ello, VTP consigue que se simplifique bastante la fase de implementación de las redes reduciendo el tiempo necesario hasta conseguir tener la red en pleno funcionamiento.

Tras la mención de estos dos protocolos, se puede observar los beneficios que aportan a los escenarios planteados anteriormente. Principalmente están basados en una simplificación a nivel de configuración y una reducción en el tiempo de trabajo hasta tener la red trabajando como se espera.

CONCLUSIONES

Una vez llevado a cabo todo el desarrollo del presente proyecto y, teniendo en cuenta las propuestas planteadas en esta memoria, se puede concluir que se han alcanzado todos los objetivos establecidos en el apartado 2 de la misma. A la vista de los resultados obtenidos, se puede concluir que todos los protocolos seleccionados son factibles de ser implementados en las redes del RT 1.

La primera conclusión que se puede extraer de este proyecto tiene a QoS como implicado. Se ha observado la gran demanda de ancho de banda que poseen algunos de los servicios que presta el regimiento y es por ello por lo que QoS toma gran protagonismo para la mejora de las redes del RT 1.

Una segunda conclusión se obtiene de la implementación del protocolo IP SLA. Se debe mencionar la sencillez de implementación y funcionamiento que posee y la gran ayuda que ofrece al monitoreo y control de los enlaces.

Otra conclusión que se ha extraído es la importancia de la mejora en la seguridad a nivel local. Por supuesto que gracias a los equipos cifradores, los datos navegan a través de las redes totalmente encriptados y seguros. Aun así, incrementar la robustez a nivel local se ha tenido en cuenta y se ha considerado una buena mejora de las redes del RT 1. Es lógico pensar que cifrar datos que ya poseen un cierto nivel de encriptación gracias a IPSec proporciona una mayor robustez general a todo el entorno.

Respecto a prioridades a la hora de implementar unos protocolos u otros, de ser sólo posible la implementación de uno de ellos, se considera que el más apropiado sería el protocolo IP SLA. Las razones que llevan a esta elección radican en su sencillez a la hora de implementarlo y en las capacidades que ofrece. Hoy en día en el ámbito de las transmisiones del ET, llevar un buen control del estado de los enlaces se considera crucial para que el tiempo sin disponer de un servicio y la reparación de éste sea lo más breve posible.

Finalmente, como se ha mencionado en la introducción de esta memoria, la no utilización de estos protocolos radica en el desconocimiento de los administradores en cuanto al uso de estos. Sin embargo, se considera importante destacar que el hecho de que estos protocolos no se hayan implementado en el RT 1 también tiene que ver con personal del regimiento que evita las actualizaciones de las redes por motivos de costumbre y comodidad.

En cuanto a las posibles líneas futuras de este trabajo, convendría llevar a cabo la implementación de estos protocolos en las redes de otras unidades del ET que no los implementen para una mayor homogeneidad y una mejora general de las redes en el ámbito del arma de transmisiones para todo el ET.

A mayores, sería interesante estudiar más a fondo las capacidades que ofrece el protocolo IP SLA. En los estudios llevados a cabo respecto a los protocolos implementados, se ha observado la posibilidad de conseguir que el protocolo IP SLA no sólo monitorice los enlaces, sino que también redirija la información por otro camino automáticamente si un enlace ha caído. Por ello, de cara a aplicaciones futuras y a una mayor mejora de las redes, explotar IP SLA con mayor efectividad se considera una buena práctica para el futuro.

Se destaca también, una vez mostrada la implementación de estos protocolos, la necesidad de una mayor formación del personal de las unidades de transmisiones para familiarizarse con estos protocolos. Todos tienen un cierto grado de complejidad que hacen necesaria una formación específica sobre los mismos. Por ello, otra posible línea futura sería la realización de un curso sobre la implementación y conocimiento de estos protocolos orientado principalmente

a los administradores de las redes.

Por último, otra posible línea futura a abarcar estaría orientada al estudio de estos protocolos a posteriori de su implementación. La realización de estudios para conocer perfectamente el tiempo necesario para desarrollar estas implementaciones en la red, sus estudios previos, mantenimiento necesario, etc. Todos estos detalles pueden enfocarse como un desarrollo futuro de una posible guía básica de implementación de estos protocolos a fin de unificar y de automatizar métodos y procesos para generar, administrar y mantener las redes.

REFERENCIAS BIBLIOGRÁFICAS

Aguilera, F. (2019) 'Trabajo Fin de Grado: Implementación de calidad de servicio (QoS) en redes tácticas de gran unidad', *Universidad de Zaragoza*, 2021, pp. 0–43. Disponible en: https://zaguan.unizar.es/record/96790?ln=es# (Consultado: 7 September 2021).

Cabello, C. (2015) *Qué es QoS, para qué sirve y cómo configurarlo en la red local*. Disponible en: https://www.nobbot.com/tecnologia/mi-conexion/que-es-el-qos-y-por-que-es-importante-para-tu-red-local/ (Consultado: 7 September 2021).

Cat, B. (2012) *Debian & Comunicacion: Quality of Service: ToS, CoS y otros bits*. Disponible en: http://debian-comunicacion.blogspot.com/2012/03/quality-of-service-tos-cos-y-otros-bits.html (Consultado: 28 September 2021).

Cisco (2009) *Configurar el Dynamic Multipoint VPN (DMVPN) usando el GRE sobre IPSec entre los routeres múltiples - Cisco*. Disponible en: https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/29240-dcmvpn.html (Consultado: 15 September 2021).

Cisco (2018a) *Router de servicios integrados Cisco 4221 - Cisco*. Disponible en: https://www.cisco.com/c/es_mx/support/routers/4351-integrated-services-router/model.html (Consultado: 30 September 2021).

Cisco (2018b) *Switch administrado apilable de 48 puertos Gigabit PoE Cisco SG350X-48P - Cisco*. Disponible en: https://www.cisco.com/c/es_mx/support/switches/sg350x-48p-48-port-gigabit-poe-stackable-managed-switch/model.html (Consultado: 30 September 2021).

Cisco (2020) *What is a Router? - Definition and Uses - Cisco*, *Cisco.com*. Disponible en: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-a-router.html (Consultado: 7 December 2021).

Davila, L. P. (2019) *VRF (Virtual Routing and Forwarding) - Cisco Community*. Disponible en: https://community.cisco.com/t5/documentos-routing-y-switching/vrf-virtual-routing-and-forwarding/ta-p/3406835 (Consultado: 9 September 2021).

eClassVirtual (2020) *Configuración de qos en packet tracer para el CCNA 200-301*. Disponible en: https://eclassvirtual.com/configuracion-de-qos-en-packet-tracer-para-el-ccna-200-301/ (Consultado: 7 September 2021).

Ejército de tierra (2012). Disponible en: https://ejercito.defensa.gob.es/unidades/Melilla/comgemel/Organizacion/index.html (Consultado: 8 September 2021).

Gabriel, E. (2020) *Como configurar IP SLA tracking - Estudia Redes*. Disponible en: https://estudiaredes.com/cisco/como-configurar-ip-sla-tracking/ (Consultado: 6 October 2021).

Gerometta, O. (2019) 'Mis Libros de Networking', pp. 1–6. Disponible en: http://librosnetworking.blogspot.com/2014/11/ruta-estatica-condicionada-por-ip-sla.html (Consultado: 15 September 2021).

González, G. (2017) *Definición de Protocolo de red » Concepto en Definición ABC*. Disponible en: https://www.definicionabc.com/tecnologia/protocolo-red.php (Consultado: 13 September 2021).

Gorgona, L. (2015) *Teoría de Redes de Computadoras*. Disponible en: https://www.oas.org/juridico/spanish/cyber/cyb29_computer_int_sp.pdf (Consultado: 13

September 2021).

Gutierrez, H. T. (2015) *Protocolos, Análisis de Tráfico y Simulaciones de Red - Monografias*. Disponible en: https://www.monografias.com/trabajos93/protocolos-analisis-trafico-y-simulaciones-red/protocolos-analisis-trafico-y-simulaciones-red.shtml (Consultado: 28 September 2021).

IEEE Computer Society (2012) *IEEE 802.3-2018: IEEE Standard for Ethernet*, *IEEE Standard for Ethernet*. Disponible en: https://standards.ieee.org/standard/802_3-2018.html (Consultado: 13 September 2021).

Julieta (2020) *Switch Capa 3 PoE 48 puertos, Allied Telesis AT-x930-52GPX-901 • TLCOM*. Disponible en: https://www.tlcom.mx/switch-industrial-allied-telesis-at-x930-52gpx-901-poe-capa-3/ (Consultado: 30 September 2021).

Lorge, F. *et al.* (2019) 'Calidad de Servicio QoS (Quality of Service) – mundotelematico.com'. Disponible en: https://www.mundotelematico.com/calidad-de-servicio-qos-quality-of-service/ (Consultado: 22 October 2021).

De Luz, S. (2021) *Qué es IPsec, protocolo para VPN con mejor seguridad y cómo funciona*, *Redes zone*. Disponible en: https://www.redeszone.net/tutoriales/vpn/ipsec-que-es-como-funciona/ (Consultado: 7 September 2021).

MediaCloud (2018) *VRF: qué es y las ventajas de un enrutamiento virtual*. Disponible en: https://blog.mdcloud.es/vrf-que-es-y-las-ventajas-de-un-enrutamiento-virtual/ (Consultado: 13 September 2021).

Mocan, T. (2019) *¿Qué es IPSec y cómo funciona?*, *CactusVPN*. Disponible en: https://www.cactusvpn.com/es/la-guia-para-principiantes-de-vpn/que-es-ipsec/ (Consultado: 13 September 2021).

Sobreviela, L. M. and Romero Martínez, J. O. (2017) 'Trabajo Fin de Grado: Calidad de servicio (QoS) con routers Cisco', *Universitat Politècnica de València*. Disponible en: www.etsit.upv.es (Consultado: 7 September 2021).

Sutil Web (2021) *Túnel (Informática) - Sutil Web*. Disponible en: https://sutilweb.com/2021/04/26/tunel-informatica/ (Consultado: 7 December 2021).

Universidad Nacional de La Plata (2018) 'Switch, Routers y Acces Point Conceptos Generales Switch', *Universidad Nacional de La Plata*. Disponible en: http://www.trabajosocial.unlp.edu.ar/uploads/docs/switch__routers_y_acces_point__conceptos_generales.pdf (Consultado: 13 September 2021).

Veato, V. (2016) *7. Protocolo VTP - Redes locales y globales*, *Protocolo VTP*. Disponible en: https://sites.google.com/site/redeslocalesyglobales/4-configuracion-de-red/4-redes-de-area-local-virtuales-vlans/7-protocolo-vtp (Consultado: 13 September 2021).

Walton, A. (2020) 'Túneles GRE: Características y Configuración - CCNA desde Cero'. Disponible en: https://ccnadesdecero.es/tuneles-gre-caracteristicas-y-configuracion/ (Consultado: 7 September 2021).

Watchguard (2018) *Acerca del Border Gateway Protocol (BGP)*. Disponible en: https://www.watchguard.com/help/docs/fireware/12/es-419/Content/es-419/dynamicrouting/bgp_about_c.html (Consultado: 15 September 2021).

ANEXOS

Anexo I. Modelo OSI

Tabla 3 Modelo OSI

N.º	NOMBRE DE LA CAPA	FUNCIÓN
7	*CAPA DE APLICACIÓN*	Interacción entre usuario y máquina
6	*CAPA DE PRESENTACIÓN*	Formato legible y utilizable
5	*CAPA DE SESIÓN*	Control de puertos y sesiones
4	*CAPA DE TRANSPORTE*	Transmisión de datos
3	*CAPA DE RED*	Decisión de la ruta a seguir
2	*CAPA DE ENLACE DE DATOS*	Definición de formato
1	*CAPA FÍSICA*	Flujo de bits a través de medio físico

La Tabla 3 muestra un esquema del modelo OSI. Se trata de un modelo normalizado que permite que distintos sistemas de comunicación se hablen entre si usando protocolos estándar. Básicamente consiste en una estandarización, permitiendo una mayor homogeneidad entre sistemas diferentes facilitando las comunicaciones entre ellos.

Anexo II. Esquema de red

Con el fin de poder implementar los protocolos de red en un contexto realista, se ha llevado a cabo un estudio y análisis de posibles topologías a adoptar para poder implementar los protocolos de manera lógica y útil.

Muchos de los servicios de los que se puede dotar una red militar vienen vía satélite. Además, este elemento es clave también para enlazar a grandes distancias con otros centros de transmisiones que se encuentren en otro lugar. Es por ello por lo que se han tenido en cuenta los enlaces vía satélite que podría llegar a haber.

Como se puede observar en la página siguiente, la Figura 25 muestra un diagrama de red que tiene en cuenta los satélites mencionados. Estos equipos cuentan con sus propios cifradores, por ello el diagrama se centra en el enlace desde el terminal satélite hacia el interior, no en lo que sucede en el enlace entre satélites (se recuerda que una limitación de este proyecto es precisamente la imposibilidad de emplear los cifradores del regimiento). Este tipo de diagrama sería el utilizado en condiciones normales al tener disponible todo tipo de equipos y terminales.

En la práctica, dado que no es posible emplear los cifradores de los terminales satélites, éstos se han simulado con un *switch* al que se le han implementado VLANs por donde iría cada servicio que ofreciese el terminal satélite para aproximarse lo máximo posible a la realidad.

En la siguiente página, la Figura 26 muestra el diagrama de red real que se ha utilizado teniendo en cuenta ya las simulaciones pertinentes. Como ya se ha mencionado, se puede observar que la solución más acorde para la sustitución de los terminales satélites se basa en un *switch* al que se le han implementado VLANs que simulan cada uno de los enlaces vía satélite de los centros de transmisiones. Nótese además la similitud con la Figura 5 de esta memoria, referente al simulador de Cisco Packet Tracer ya que se ha tratado de aproximar la simulación lo máximo posible a la realidad del proyecto.

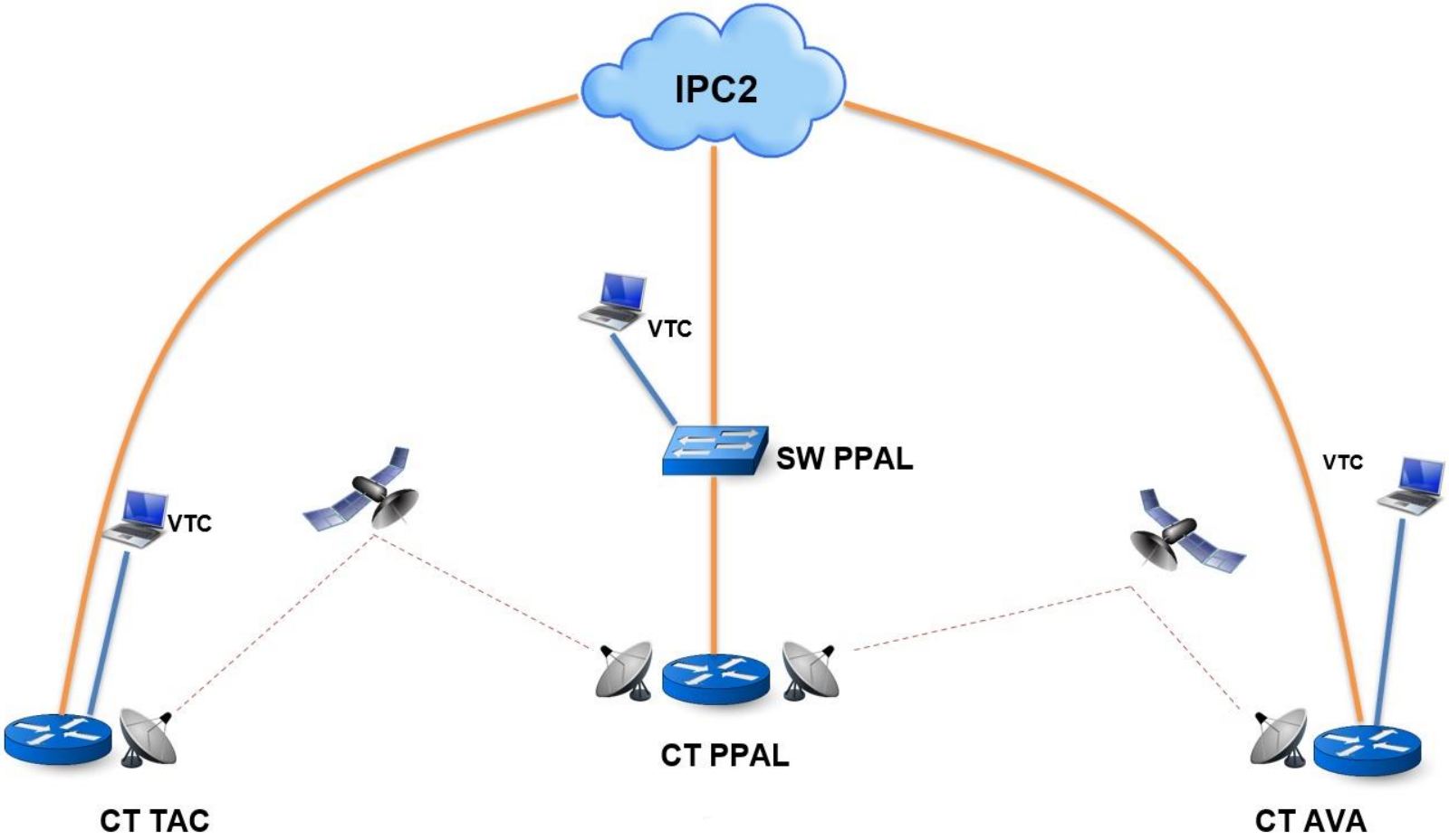

Figura 25 Esquema de red ideal

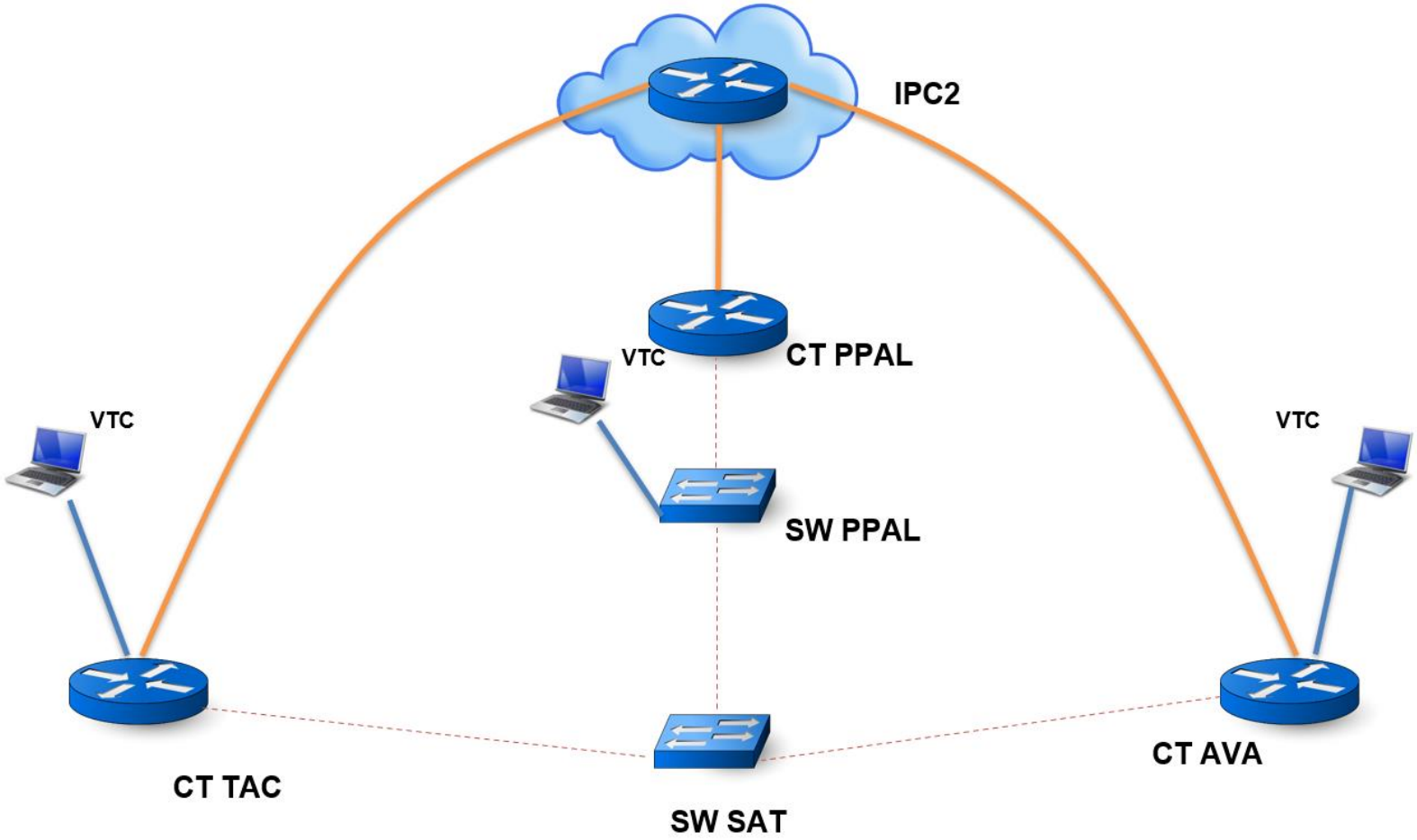

Figura 26 Esquema de red utilizado

Anexo III. Equipos utilizados

Para complementar la información del apartado 4.3 de la memoria, a continuación, se procede a mostrar una serie de ilustraciones mostrando con mayor detalle los equipos utilizados para el diseño del laboratorio utilizado durante este proyecto.

En lo que se refiere al CT PPAL, como ya se ha mencionado, se han dispuesto un router y un *switch*.

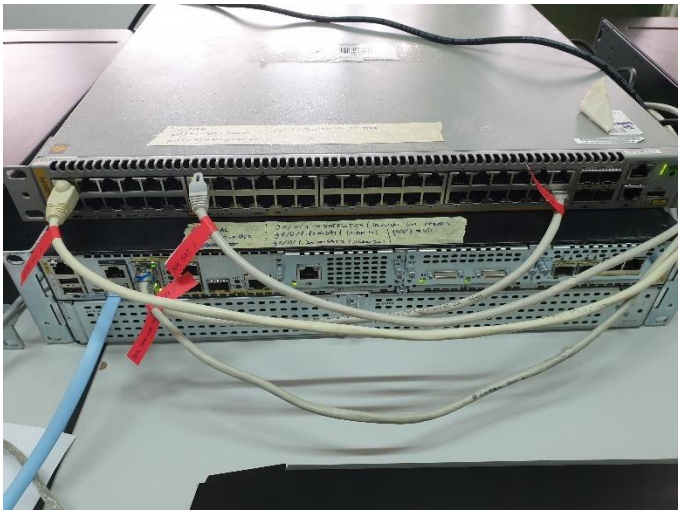

Figura 27 Router y switch del CT PPAL

La Figura 27 ofrece una imagen mostrando tanto el router del CT PPAL (debajo) como el *switch* del CT PPAL (encima) además de las conexiones pertinentes para la posterior implementación de los protocolos elegidos.

Seguidamente, tanto para el CT TAC como para el CT AVA, como ya se ha comentado, se ha dispuesto únicamente de un router para cada centro con el fin de realizar las configuraciones pertinentes y que el desarrollo del trabajo tenga sentido y ofrezca una situación lo más realista posible.

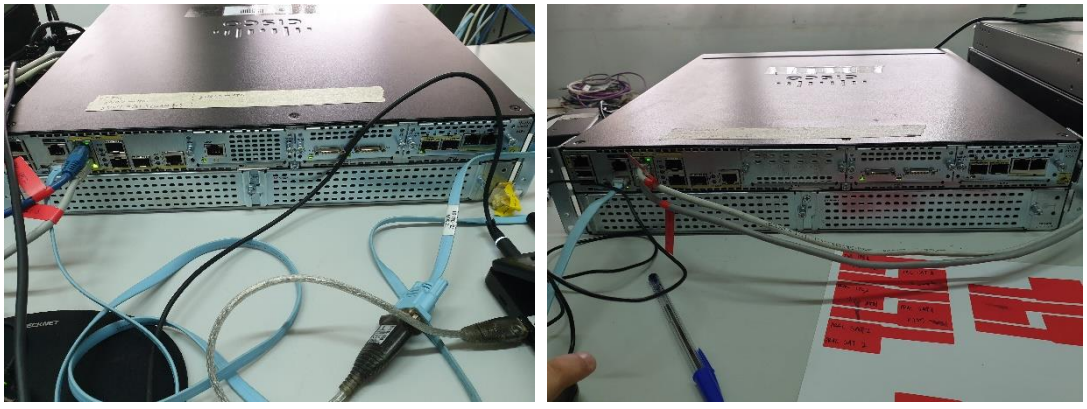

Figura 28 Routers del CT TAC y CT AVA

Como se observa en la Figura 28, ambos routers son idénticos y la diferencia en sus configuraciones radica principalmente en la configuración de sus respectivos interfaces.

Finalmente, para la simulación de la red WAN IPC2 en el desarrollo de este trabajo, se ha dispuesto de un cuarto router que haga las veces de red WAN IPC2. Además, señalar la incorporación de otro *switch* para ofrecer la simulación de los enlaces con los terminales satélite que se utilizarían en un ejercicio real.

Figura 29 Router IPC2 y switch de terminales satélite

Nótese que efectivamente en la Figura 29 se dispone de un cuarto router y de otro *switch* para el correcto desarrollo de este proyecto también con todos los interfaces necesarios ya conectados mediante cables Ethernet.

Finalizado el montaje de todos estos elementos, ya se obtiene lo mostrado en la Figura 4 referente al laboratorio completo utilizado para este trabajo.

Anexo IV. Valores DSCP

Tabla 4 Valores DSCP

DSCP	DECIMAL	COMPORTAMIENTO	VALOR
CS0 (Por defecto)	0x00	Mejor esfuerzo	Mejor esfuerzo
CS1	0x08	AF1	Prioritario
CS2	0x16	AF2	Inmediato
CS3	0x24	AF3	Flash
CS4	0x32	AF4	Anulación de flash
CS5	0x40	EF	Crítico
CS6	0x48	Control de interred	Control de interred
CS7	0x56	Control de red	Control de red

La Tabla 4 muestra los diferentes valores que puede tomar el DSCP, tanto el número que llevaría dentro de la cabecera IP como su comportamiento en función de si es un tipo de paquete u otro.

A su vez, los comportamientos de AF tienen también valores asignados acorde a su probabilidad de que el paquete afectado sea descartado.

Tabla 5 Valores AF

COMPORTAMIENTO	DECIMAL	PROBABILIDAD DE DESCARTE
AF11	0x10	BAJA
AF12	0x12	MEDIA
AF13	0x14	ALTA
AF21	0x18	BAJA
AF22	0x20	MEDIA
AF23	0x22	ALTA
AF31	0x26	BAJA
AF32	0x28	MEDIA
AF33	0x30	ALTA
AF41	0x34	BAJA
AF42	0x36	MEDIA
AF43	0x38	ALTA

La Tabla 5 muestra la probabilidad de que un paquete sea descartado en función del número asignado a cada AF. Nótese que el primer número corresponde a cada uno de los 4 AF de la tabla anterior mientras que el segundo número es asignado al 1, 2 y 3 en función de si su probabilidad de descarte es baja, media o alta respectivamente. Nótese también que la asignación del valor decimal para cada AF está dentro de los valores descritos en la tabla anterior.

Anexo V. Configuración de los routers

A fin de complementar el apartado 4.6 de la memoria, se muestran a continuación las configuraciones completas de los routers correspondientes a cada uno de los centros de transmisiones.

En cuanto a los dos *switches* y al router de la red WAN IPC2, no se considera necesario mostrar su configuración puesto que lo más relevante que tienen es la configuración de los interfaces Ethernet que se han utilizado para el proyecto y se considera algo trivial.

Para obtener la configuración completa de un router, basta con ejecutar el comando *show running-config* desde el perfil de administrador e, inmediatamente, el router muestra todas las configuraciones que se hayan implementado en él.

Es necesario destacar que se trata de configuraciones muy extensas. Por ello, la información más relevante para este trabajo se ha agregado directamente en la memoria mientras que la configuración completa forma parte de este anexo.

A continuación, se muestra la configuración completa de los routers:

- **Router del CT PPAL**

```
RT_PPRAL#sh run
Building configuration...
Current configuration : 4346 bytes
Last configuration change at 13:26:55 CET Mon Sep 27 2021
NVRAM config last updated at 13:27:12 CET Mon Sep 27 2021
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no platform punt-keepalive disable-kernel-core
hostname RT_PPRAL
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
 address-family ipv4
 exit-address-family
 address-family ipv6
 exit-address-family
card type command needed for slot/bay 0/1
no aaa new-model
clock timezone CET 1 0
clock summer-time CET recurring last Sun Mar 2:00 last Sun Oct 2:00
subscriber templating
multilink bundle-name authenticated
license udi pid ISR4351/K9 sn FDO21480LLL
spanning-tree extend system-id
username admin privilege 15 password 7 0822455D0A16544541
redundancy
 mode none
vlan internal allocation policy ascending

track 1 ip sla 1 reachability
track 2 ip sla 2 reachability

class-map match-all VTC_SALIDA
 match ip dscp af41
class-map match-all VTC
```

```
 match access-group name VTC
policy-map VTC
 class VTC
  set ip dscp af41
policy-map 3M
 class VTC_SALIDA
  bandwidth percent 95
 class class-default
  fair-queue
  random-detect
policy-map SHAPE-INTRATEATRO
 class class-default
  shape average 3072000
   service-policy 3M

crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key cisco123 address 192.168.1.0
crypto isakmp key cisco123 address 192.168.1.14
crypto isakmp key cisco123 address 192.168.1.18

crypto ipsec transform-set set1 esp-aes 256 esp-sha-hmac
 mode tunnel
crypto ipsec profile IPSEC_DMVPN
 set transform-set set1
crypto map CMAP_AVA 10 ipsec-isakmp
 set peer 192.168.1.18
 set transform-set set1
 match address IPSEC_NUESTRO
crypto map CMAP_TAC 10 ipsec-isakmp
 set peer 192.168.1.14
 set transform-set set1
 match address IPSEC_NUESTRO

interface Loopback0
 ip address 1.1.1.1 255.255.255.255
interface Tunnel100
 description TUNEL MULTIPUNTO PPRAL
 ip address 30.0.0.1 255.255.255.0
 no ip redirects
 ip nhrp map 30.0.0.2 192.168.1.6
 ip nhrp map 30.0.0.3 192.168.1.10
 ip nhrp map multicast 192.168.1.6
 ip nhrp map multicast 192.168.1.10
 ip nhrp network-id 1
 ip ospf network broadcast
 ip ospf cost 30
 keepalive 10 3
 tunnel source 192.168.1.2
 tunnel mode gre multipoint
 tunnel protection ipsec profile IPSEC_DMVPN
interface Tunnel34003
 description ENLACE A AVA
 ip address 192.168.1.5 255.255.255.252
 ip mtu 1350
 tunnel source 10.2.0.1
 tunnel destination 10.2.0.5
interface GigabitEthernet0/0/0
 description PPRAL_IPC2
```

```
 ip address 192.168.1.2 255.255.255.252
 negotiation auto
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
interface GigabitEthernet0/0/1.10
 description SAT 1
 bandwidth 1000000
 encapsulation dot1Q 10
 ip address 192.168.1.13 255.255.255.252
 crypto map CMAP_TAC
 service-policy output SHAPE-INTRATEATRO
interface GigabitEthernet0/0/1.20
 description SAT 2
 bandwidth 1000000
 encapsulation dot1Q 20
 ip address 192.168.1.17 255.255.255.252
 crypto map CMAP_AVA
 service-policy output SHAPE-INTRATEATRO
interface GigabitEthernet0/0/2
 no ip address
 shutdown
 negotiation auto
interface Serial0/2/0
 no ip address
 shutdown
interface Serial0/2/1
 no ip address
 shutdown
interface GigabitEthernet0/3/0
 description VTC
 ip address 10.10.10.1 255.255.255.0
 negotiation auto
 service-policy input VTC
interface GigabitEthernet0/3/1
 no ip address
 shutdown
 negotiation auto
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
interface Vlan1
 no ip address
 shutdown

router ospf 1
 network 10.10.10.0 0.0.0.255 area 0
 network 30.0.0.0 0.0.0.255 area 0

router bgp 34001
 bgp log-neighbor-changes
 neighbor 192.168.1.6 remote-as 34003
 neighbor 192.168.1.6 description ENLACE AVA
 neighbor 192.168.1.6 password 7 02050D4808095E731F
 neighbor 192.168.1.10 remote-as 34002
 neighbor 192.168.1.10 description ENLACE TAC
 neighbor 192.168.1.10 password 7 03189C7756901F634D

 address-family ipv4
  network 1.1.1.1 mask 255.255.255.255
```

```
  aggregate-address 10.10.10.0 255.255.255.0 summary-only
  redistribute ospf 1
  neighbor 192.168.1.6 activate
  neighbor 192.168.1.6 send-community both
  neighbor 192.168.1.6 soft-reconfiguration inbound
  neighbor 192.168.1.10 activate
  neighbor 192.168.1.10 send-community both
  neighbor 192.168.1.10 soft-reconfiguration inbound
 exit-address-family

ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ip route 10.2.0.4 255.255.255.252 10.2.0.2
ip route 20.20.20.0 255.255.255.0 192.168.1.14 track 1
ip route 30.30.30.0 255.255.255.0 192.168.1.18 track 2
ip route 192.168.1.4 255.255.255.252 192.168.1.1
ip route 192.168.1.8 255.255.255.252 192.168.1.1

ip access-list extended IPSEC_NUESTRO
 permit ip 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255
ip access-list extended VTC
 permit ip 10.10.10.0 0.0.0.255 20.20.20.0 0.0.0.255
 permit ip 10.10.10.0 0.0.0.255 30.30.30.0 0.0.0.255

ip sla 1
 icmp-echo 192.168.1.14 source-ip 192.168.1.13
 frequency 5
ip sla schedule 1 life forever start-time now
ip sla 2
 icmp-echo 192.168.1.18 source-ip 192.168.1.17
 frequency 5
ip sla schedule 2 life forever start-time now
control-plane

line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
ntp master 1
end
```

- **Router del CT TAC**

```
ROUTER_TAC#sh run
Building configuration...
Current configuration : 3581 bytes
!Last configuration change at 11:22:31 UTC Mon Sep 27 2021
 NVRAM config last updated at 10:59:58 UTC Mon Sep 27 2021
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname ROUTER_TAC
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
 address-family ipv4
 exit-address-family
```

```
 address-family ipv6
 exit-address-family
card type command needed for slot/bay 0/1
no aaa new-model
subscriber templating
multilink bundle-name authenticated
license udi pid ISR4351/K9 sn FDO21491CAS
spanning-tree extend system-id
username admin privilege 15 password 2 0861027F0J16582443
redundancy
 mode none
vlan internal allocation policy ascending

track 1 ip sla 1 reachability

class-map match-all VTC_SALIDA
 match ip dscp af41
class-map match-all VTC
 match access-group name VTC
policy-map VTC
 class VTC
  set ip dscp af41
policy-map 3M
 class VTC_SALIDA
  bandwidth percent 95
 class class-default
  fair-queue
  random-detect
policy-map SHAPE-INTRATEATRO
 class class-default
  shape average 3072000
   service-policy 3M

crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key cisco123 address 192.168.1.0
crypto isakmp key cisco123 address 192.168.1.13

crypto ipsec transform-set set1 esp-aes 256 esp-sha-hmac
 mode tunnel
crypto ipsec profile IPSEC_DMVPN
 set transform-set set1
crypto map CMAP_TAC 10 ipsec-isakmp
 set peer 192.168.1.13
 set transform-set set1
 match address IPSEC_NUESTRO

interface Loopback0
 ip address 2.2.2.2 255.255.255.255
interface Tunnel100
 ip address 30.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 30.0.0.1 192.168.1.2
 ip nhrp map multicast 192.168.1.2
 ip nhrp network-id 1
 ip nhrp nhs 30.0.0.1
 tunnel source 192.168.1.6
 tunnel mode gre multipoint
 tunnel protection ipsec profile IPSEC_DMVPN
```

```
interface Tunnel34003
 description ENLACE PPRAL
 ip address 192.168.1.10 255.255.255.252
 ip mtu 1350
 ip pim sparse-mode
 tunnel source 10.2.0.9
 tunnel destination 10.2.0.1
interface GigabitEthernet0/0/0
 description IPC2
 ip address 192.168.1.6 255.255.255.252
 ip ospf cost 1200
 negotiation auto
interface GigabitEthernet0/0/1
 description SAT_TAC
 bandwidth 1024
 ip address 192.168.1.14 255.255.255.252
 ip ospf cost 1300
 negotiation auto
 crypto map CMAP_TAC
 service-policy output SHAPE-INTRATEATRO
interface GigabitEthernet0/0/2
 no ip address
 shutdown
 negotiation auto
interface Serial0/2/0
 no ip address
 shutdown
interface Serial0/2/1
 no ip address
 shutdown
interface GigabitEthernet0/3/0
 description VTC_3
 ip address 20.20.20.1 255.255.255.0
 negotiation auto
 service-policy input VTC
interface GigabitEthernet0/3/1
 no ip address
 shutdown
 negotiation auto
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
interface Vlan1
 no ip address
 shutdown

router ospf 1
 network 20.20.20.0 0.0.0.255 area 0
 network 30.0.0.0 0.0.0.255 area 0

router bgp 34002
 bgp log-neighbor-changes
 neighbor 192.168.1.1 remote-as 34001
 neighbor 192.168.1.1 description ENLACE PPRAL
 neighbor 192.168.1.1 password 9 067914G0589347D064E
 neighbor 192.168.1.10 remote-as 34003
 neighbor 192.168.1.10 description ENLACE AVA
 neighbor 192.168.1.10 password 3 09974A3675410G090B

 address-family ipv4
```

```
  network 2.2.2.2 mask 255.255.255.255
  aggregate-address 20.20.20.0 255.255.255.0 summary-only
  redistribute ospf 1
  neighbor 192.168.1.1 activate
  neighbor 192.168.1.1 send-community both
  neighbor 192.168.1.1 soft-reconfiguration inbound
  neighbor 192.168.1.10 activate
  neighbor 192.168.1.10 send-community both
  neighbor 192.168.1.10 soft-reconfiguration inbound
 exit-address-family

ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ip route 10.2.0.0 255.255.255.252 10.2.0.10
ip route 10.10.10.0 255.255.255.0 192.168.1.13 track 1
ip route 192.168.1.0 255.255.255.252 192.168.1.5
ip route 192.168.1.8 255.255.255.252 192.168.1.5

ip access-list extended IPSEC_NUESTRO
 permit ip 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255
ip access-list extended VTC
 permit ip 20.20.20.0 0.0.0.255 10.10.10.0 0.0.0.255

ip sla 1
 icmp-echo 192.168.1.13 source-ip 192.168.1.14
 frequency 5
ip sla schedule 1 life forever start-time now
control-plane

line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
ntp server 192.168.1.13
end
```

- **Router del CT AVA**

```
RT_AVANZADO#sh run
Building configuration...
Current configuration : 3976 bytes
Last configuration change at 13:07:44 UTC Mon Sep 27 2021
NVRAM config last updated at 13:07:41 UTC Mon Sep 27 2021
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname RT_AVANZADO
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
 address-family ipv4
 exit-address-family
 address-family ipv6
 exit-address-family
no aaa new-model
subscriber templating
multilink bundle-name authenticated
voice-card 0/4
```

```
 no watchdog
license udi pid ISR4351/K9 sn FDO224332CC
spanning-tree extend system-id
username admin privilege 15 password 6 01154F9610034D133E
redundancy
 mode none
vlan internal allocation policy ascending

track 1 ip sla 1 reachability

class-map match-all VTC_SALIDA
 match ip dscp af41
class-map match-all VTC
 match access-group name VTC
policy-map VTC
 class VTC
  set ip dscp af41
policy-map 3M
 class VTC_SALIDA
  bandwidth percent 95
class class-default
  fair-queue
  random-detect
policy-map SHAPE-INTRATEATRO
 class class-default
  shape average 3072000
   service-policy 3M

crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key cisco123 address 192.168.1.0
crypto isakmp key cisco123 address 192.168.1.17

crypto ipsec transform-set set1 esp-aes 256 esp-sha-hmac
 mode tunnel
crypto ipsec profile IPSEC_DMVPN
 set transform-set set1
crypto map CMAP_AVA 10 ipsec-isakmp
 set peer 192.168.1.17
 set transform-set set1
 match address IPSEC_NUESTRO

interface Loopback0
 ip address 3.3.3.3 255.255.255.255
interface Tunnel100
 ip address 30.0.0.3 255.255.255.0
 no ip redirects
 ip nhrp map 30.0.0.1 192.168.1.2
 ip nhrp map multicast 192.168.1.2
 ip nhrp network-id 1
 ip nhrp nhs 30.0.0.1
 tunnel source 192.168.1.10
 tunnel mode gre multipoint
 tunnel protection ipsec profile IPSEC_DMVPN
interface GigabitEthernet0/0/0
 description AVANZADO IPC2
 ip address 192.168.1.10 255.255.255.252
 negotiation auto
interface GigabitEthernet0/0/1
```

```
 description SAT 4
 ip address 192.168.1.18 255.255.255.252
 negotiation auto
 crypto map CMAP_AVA
 service-policy output SHAPE-INTRATEATRO
interface GigabitEthernet0/0/2
 no ip address
 shutdown
 negotiation auto
interface Serial0/2/0
 no ip address
 shutdown
interface Serial0/2/1
 no ip address
 shutdown
interface GigabitEthernet0/3/0
 description VTC
 ip address 30.30.30.1 255.255.255.0
 negotiation auto
interface GigabitEthernet0/3/1
 no ip address
 shutdown
 negotiation auto
interface Service-Engine0/4/0
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
interface Vlan1
 no ip address
 shutdown
router ospf 1
 network 3.3.3.3 0.0.0.0 area 0
 network 30.0.0.0 0.0.0.255 area 0
 network 30.30.30.0 0.0.0.255 area 0

router bgp 34003
 bgp log-neighbor-changes
 neighbor 192.168.1.1 remote-as 34001
 neighbor 192.168.1.1 description ENLACE PPRAL
 neighbor 192.168.1.1 password 3 02254D0389140F449H
 neighbor 192.168.1.2 remote-as 34002
 neighbor 192.168.1.2 description ENLACE TAC
 neighbor 192.168.1.2 password 7 05711D0466371E371J

 address-family ipv4
  network 3.3.3.3 mask 255.255.255.255
  aggregate-address 30.30.30.0 255.255.255.0 summary-only
  redistribute ospf 1
  neighbor 192.168.1.1 activate
  neighbor 192.168.1.1 send-community both
  neighbor 192.168.1.1 soft-reconfiguration inbound
  neighbor 192.168.1.2 activate
  neighbor 192.168.1.2 send-community both
  neighbor 192.168.1.2 soft-reconfiguration inbound
 exit-address-family

ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
```

```
ip route 10.2.0.0 255.255.255.252 10.2.0.6
ip route 10.10.10.0 255.255.255.0 192.168.1.17 track 1
ip route 192.168.1.0 255.255.255.252 192.168.1.9
ip route 192.168.1.4 255.255.255.252 192.168.1.9

ip access-list extended IPSEC_NUESTRO
 permit ip 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255
 permit ip 30.30.30.0 0.0.0.255 10.10.10.0 0.0.0.255
 permit ip 10.10.10.0 0.0.0.255 30.30.30.0 0.0.0.255
ip access-list extended VTC
 permit ip 30.30.30.0 0.0.0.255 any

ip sla 1
 icmp-echo 192.168.1.17 source-ip 192.168.1.18
 frequency 5
ip sla schedule 1 life forever start-time now
control-plane

mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
mgcp profile default

line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
ntp server 192.168.1.17
end
```