Universidad Zaragoza
1542

Trabajo Fin de Grado

Implementación de calidad de servicio (QoS) en redes tácticas de gran unidad

Autor

Francisco Aguilera Pino

Director/es

Director académico: Jorge Ortín Gracia
Director militar: Diego Herrero Tejada

Centro Universitario de la Defensa-Academia General Militar
2019

Resumen

La implementación de la tecnología en el campo militar es un desafío. Esto se debe al hecho que proporciona una gran cantidad de ventajas, pero requiere una atención especial debido a que gran parte de los ejercicios militares nacionales e internacionales que se llevan a cabo actualmente dependen de una gran red IP que debe gestionarse de manera segura y optimizando los recursos disponibles.

En este trabajo, se evalúan las técnicas de calidad de servicio (Quality of Service – QoS) que se pueden aplicar en una red de comunicaciones y se comprueba su correcto funcionamiento en un entorno operativo de gran unidad. En la primera parte del trabajo se realiza un estudio teórico sobre QoS. En primer lugar, se explica qué son las redes convergentes y cómo las utiliza el ejército español. A continuación, se definen los parámetros que tienen una relación directa con la QoS y, posteriormente, se discuten los diferentes mecanismos de aplicación de QoS, enfocando el proyecto en el modelo de servicios diferenciados debido a que es el que se usa actualmente en las unidades del ejército. Para finalizar esta parte, se explica distintas estrategias de gestión de las colas de los routers, ya que son el principal mecanismo para aplicar QoS en enlaces donde puede haber congestión.

En la segunda parte, se detallan las diferentes posibilidades de configurar un router Cisco de acuerdo con el método de QoS que el administrador desea utilizar, siempre dependiendo de las diferentes vicisitudes del ejercicio táctico.

En la tercera parte, se realiza una prueba en un entorno de laboratorio con el fin de implementar QoS y el marcado de paquetes críticos autogenerados, esa prueba se realizó ya que posteriormente se desplegó en un ejercicio real (Trident Jackal 19) en el que se utilizó la metodología obtenida para marcar los paquetes de videollamada con respecto al resto de los paquetes y se estudió como se mejoraba la calidad de la videollamada según se gestionaban mejor los recursos mediante QoS.

La principal conclusión del trabajo es posible implementar QoS en redes tácticas de gran unidad, siendo una herramienta fundamental para poder suministrar adecuadamente servicios de voz y multimedia sobre una red con enlaces de ancho de banda limitado.

Abstract

The implementation of technology in the military field is a challenge. This is due to the fact that it provides a lot of advantages, but requires special attention because a large part of the national and international military exercises that are currently carried out depend on a large IP network, which must be managed safely and optimizing available resources.

In this project, the quality of service techniques (Quality of Service – QoS) that can be applied in a communications network are evaluated and its correct operation is verified in a large unit operating environment. In the first part of the work a theoretical study on QoS is carried out. First, it explains what convergent networks are and how the Spanish army uses them. Next, the parameters that have a direct relationship with the QoS are defined and subsequently, the different mechanisms of QoS application are discussed, focusing the project on the differentiated services model because it is the one currently used in the units from army. To conclude this part, different strategies for managing queues of routers are explained, since they are the main mechanism to apply QoS in links where there may be congestion.

In the second part, the different possibilities of configuring a Cisco router according to the QoS method that the administrator wishes to use are detailed, always depending on the different vicissitudes of the tactical exercise.

In the third part, a test is performed in a laboratory environment in order to implement QoS and the marking of self-generated critical packages, that test was performed since it was subsequently deployed in a real exercise (Trident Jackal 19) in which was used the methodology obtained to mark the video call packages with respect to the rest of the packages and it was studied how the quality of the video call was improved as resources were better managed through QoS.

The main conclusion of the work is possible to implement QoS in large unit networks, being a fundamental tool to be able to adequately provide voice and multimedia services over a network with limited bandwidth links.

Agradecimientos

En primer lugar, quería agradecer la disposición total de los tutores de este trabajo: el profesor D. Jorge Ortín Gracia y el teniente D. Diego Herrero Tejada. Sin su ayuda hubiera sido imposible la realización de este proyecto.

En segundo lugar, dar las gracias al personal del Regimiento de Transmisiones Nº21, en especial al 1ºBatallón el cual me ha acogido como a uno más y me han demostrado porque se auto-denominan con toda la razón los primeros en transmisiones y ejemplo de combatientes.

En tercer lugar, me gustaría agradecer a todos los compañeros de promoción y sin olvidarme de aquellos que ya no están, que han sido indispensables para mi formación como militar y sobre todo como persona.

Por último, dar las gracias a mi familia y a mi pareja porque solo ellos saben lo que se ha pasado para llegar aquí.

Índice

Índice de ilustraciones

Índice de tablas

Lista de acrónimos

Acrónimo	Significado
ACL	*Access Control List*
AF	*Assured Forwarding*
ASA	*Adaptive Server Anywhere*
ATQH	*At the Quick Halt*
CBWFQ	*Class-Based Weighted Fair Queuing*
CGTAD	*Cuartel General Terrestre de Alta Disponibilidad*
CIS	*Communications and Information Systems*
DiffServ	*Differenciated Services*
DSCP	*Differentiated Services Code Point*
EF	*Expedited Forwarding*
FIFO	*First In First Out*
IntServ	*Integrated Services*
IP	*Internet Protocol*
LLQ	*Low Latency Queuing*
MAC	*Media Access Control*
MCU	*Multipoint Control Unit*
MC3	*Modernization, Command, Control and Communication*
MQC	*Modular QoS Command-Line Interface*
OTAN	*Organización del Tratado del Atlántico Norte*
PCMOV	*Puesto de Mando Móvil*
PMCE	*Puesto de Mando de Cuerpo de Ejército*
QoS	*Quality of Service*
RT	*Regimiento de Transmisiones*
TJ19	*Trident jackal 2019*
SOTM	*Satcom Of the Move*
VLAN	*Virtual Local Area Network*
VoIP	*Voz sobre IP*
VTC	*Video Teleconferencing*
WLAN	*Wireless Local Area Network*
WMM	*Wifi Multi-Media*

1. Introducción

La siguiente memoria presenta los resultados del trabajo de fin de grado correspondiente al grado de Ingeniería de Organización Industrial, impartido en el Centro Universitario de la Defensa en Zaragoza. El objetivo del proyecto es la implementación de la calidad de servicio (Quality of Service – QoS) en redes tácticas de gran unidad, comprobando su funcionamiento en un entorno real de una maniobra militar de gran unidad en ambiente OTAN.

1.1. Motivación

Según la arquitectura MC3, marcada por el Ministerio de Defensa, la estructura deseada en vista al futuro de los sistemas CIS (Communications and Information Systems) dentro del Ejército Español será una red con todos sus elementos (datos, voz, VTC (Video Teleconferencing), sistema de mando y control) basados en tecnología IP (Internet Protocol)[1] .

En las redes convergentes en las que se integran distintos servicios sobre una misa red, existen aplicaciones críticas como sería el caso de la VoIP (Voice over Internet Protocol) con requisitos muy estrictos de calidad que comparten la red con otras aplicaciones de datos (navegación web) menos exigentes. Para asegurar que estas aplicaciones críticas reciben los recursos de red necesarios para cumplir con sus requisitos, se necesitan implementar herramientas de QoS que protejan los paquetes prioritarios frente a los flujos de datos convencionales. Este tipo de herramientas darán preferencia a los paquetes de aplicaciones críticas como la voz, que se trasmitirán a través de la red de forma preferente.

En este proyecto se pretende evaluar las técnicas de QoS típicas que se pueden en una red de comunicaciones, de tal modo que se pueda determinar si dichas técnicas son válidas para su uso en las redes que se emplean en una gran unidad.

1.1. **Objetivo**

El principal objetivo de este proyecto es identificar las técnicas de QoS que se pueden aplicar en una red de comunicaciones y comprobar su correcto funcionamiento en un entorno operativo de gran unidad. En concreto, en este TFG se va a comprobar la viabilidad de transmitir videollamadas y conversaciones de voz de modo satisfactorio a través de un enlace de ancho de banda limitado gracias a la aplicación de estas técnicas de QoS en el ejercicio militar realizado (Trident Jackal 2019) con el Regimiento de Transmisiones Nº21.

1.2. **Metodología**

Para la realización del trabajo, se ha realizado en primer lugar un estudio teórico de las principales técnicas de QoS que se pueden implementar en una red. Asimismo, se ha analizado la documentación de los equipos disponibles en la Unidad para comprobar qué técnicas de QoS tiene disponibles y cómo configurarlos. Seguidamente, se ha realizado una prueba de marcado en ambiente laboratorio para observar cómo se pueden marcar los paquetes de cada tipo de servicio o aplicación para poder aplicarles luego las políticas de QoS que se definan. Finalmente, se han aplicado las técnicas de QoS en un caso práctico en ambiente militar OTAN, teniendo en cuenta que OTAN ya marca unas restricciones mínimas a las cuales nos tenemos que ceñir obligatoriamente.

1.3. **Estructura de la memoria**

La memoria está organizada en cinco grandes capítulos, empezando por el presente capítulo introductorio y recogidos en el índice general. El capítulo "Calidad de Servicio en una Red de comunicaciones" contiene la información teórica necesaria para entender la necesidad de aplicar mecanismos de QoS en una red y cuáles son estos mecanismos. Seguidamente, el capítulo "Implementación de QoS en equipos Cisco" explica cómo aplicar los mecanismos presentados en el capítulo anterior en equipos del fabricante Cisco, que los que se emplean en la unidad en la que se realizó este trabajo fin de grado. En el apartado "Resultados de la aplicación de QoS en una red táctica" se encuentra la parte práctica del proyecto, comenzando por una práctica en un entorno controlado y terminando con un ejercicio sobre el terreno con la metodología aprendida anteriormente. Finalmente, se muestran las conclusiones y se exponen las nuevas tendencias en este campo.

1.4. **Planificación del proyecto**

En el Anexo A, se puede contemplar el desglose completo de las actividades realizadas para la consecución del proyecto. Estas tareas han sido clasificadas temporalmente, siendo realizadas en su mayoría durante el periodo de prácticas externas en el Regimiento de Transmisiones Nº21. La organización del trabajo fue planteada para comenzar el 20/07/2019 a través de la planificación de la agenda y terminar en la entrega del trabajo el 04/11/2019.

2. Calidad de Servicio en una Red de Comunicaciones

En el siguiente capítulo se introducirá la estructura de una red táctica utilizada en el Ejército de Tierra, haciendo hincapié en los equipos que la forman. También se explica la necesidad de implementar mecanismos específicos de QoS en una red cuando por ella viaja tráfico de aplicaciones con requisitos de QoS distintos. Seguidamente se explicarán los pasos que se han de seguir para aplicar QoS a una red. Finalmente, se expondrán los principales mecanismos de gestión de la congestión que se pueden aplicar a los routers para garantizar los requisitos de QoS de los distintos tipos de tráfico que viajan por la red.

2.1. Funcionamiento y estructura de una Red de Comunicaciones Táctica

Las redes de telecomunicaciones (como la red telefónica) se implementaban en un principio utilizando tecnologías basadas en técnicas de conmutación de circuitos, las cuales reservan un circuito dedicado para cada comunicación. De este modo se garantizaba un retardo mínimo y fijo en la comunicación, y también se aseguraba que no pudiera existir congestión para las comunicaciones ya establecidas (cualquier intento de conexión se bloqueaba si la red no disponía de recursos suficientes). Por ello, las redes basadas en conmutación de circuitos contaban inherentemente con una QoS alta ya que fueron diseñadas para soportar tráfico sensible a retardos y pérdidas de aplicaciones como voz y video. Por el contrario, estas redes no son adecuadas para el tráfico de datos, ya que las aplicaciones de datos (por ejemplo, la navegación web) no generan tráfico continuamente, por lo que es ineficiente disponer de recursos reservados exclusivamente para cada estas comunicaciones.

La transmisión de datos se realiza habitualmente empleando otra tecnología distinta a la conmutación de circuitos denominada conmutación de paquetes por datagrama. En esta tecnología la información a mandar se divide en pequeños bloques denominados paquetes que se mandan por la red. Cada uno de estos paquetes se trata de modo independiente por los routers de la red y lleva codificado el destinatario del paquete. De este modo, cada vez que un paquete llega a un router, este lee el destinatario y lo manda por la salida más adecuada. En esta tecnología no se reservan recursos previamente, por lo que es mucho más eficiente, pero presenta el problema de que todos los paquetes son tratados por igual y de que no se garantiza ninguna QoS para ellos. El ejemplo más paradigmático de este tipo de redes es Internet.

El hecho de que las redes de conmutación de paquetes como Internet no ofrecieran ningún tipo de QoS, hizo que durante muchos años convivieran estos dos tipos de redes en paralelo, una red de conmutación de circuitos para cursar llamadas telefónicas y otra de conmutación de paquetes para la transmisión de datos. Esta solución no obstante es bastante ineficiente (implica aumentar el número de equipos de red) e implica problemas operativos para entornos móviles como las redes tácticas, en las que es necesario modificar el despliegue de la red conforme se realiza una operación.

Para evitar esta duplicidad en la infraestructura de red, la tendencia actual es hacia las redes convergentes, las cuales cuentan con una única infraestructura de red, basada en conmutación de paquetes, que soporta múltiples servicios (voz, video y datos). Este tipo de redes son la mejor opción hoy en día para los operadores de una red táctica de gran unidad por su versatilidad y eficiencia con respecto a su costo, aunque sea posible que no soporten aplicaciones específicas con la eficacia que lo haría una red construida específicamente para dicha aplicación. Para mitigar este comportamiento, la aplicación de técnicas de QoS pasa a tomar un rol fundamental en redes convergentes, ya que las mismas debe ser flexibles y soportar muchos tipos de aplicaciones y servicios simultáneamente [2].

En la siguiente ilustración, se muestra cómo sería una red de comunicaciones convergente dentro del ejército, que podría dar servicio en un despliegue táctico de gran unidad. La

infraestructura de la red de comunicaciones está formada por 3 routers y 3 switches. En esta red hay 7 redes virtuales de diferentes aplicaciones como VoIP (Voice over IP), VTC-IP (Video Teleconferencing IP) y otras redes de datos que conviven en una sola red de transporte. Estas redes se configuran mediante VLAN (Virtual Local Area Network) configuradas en el switch de cada centro de transmisiones.

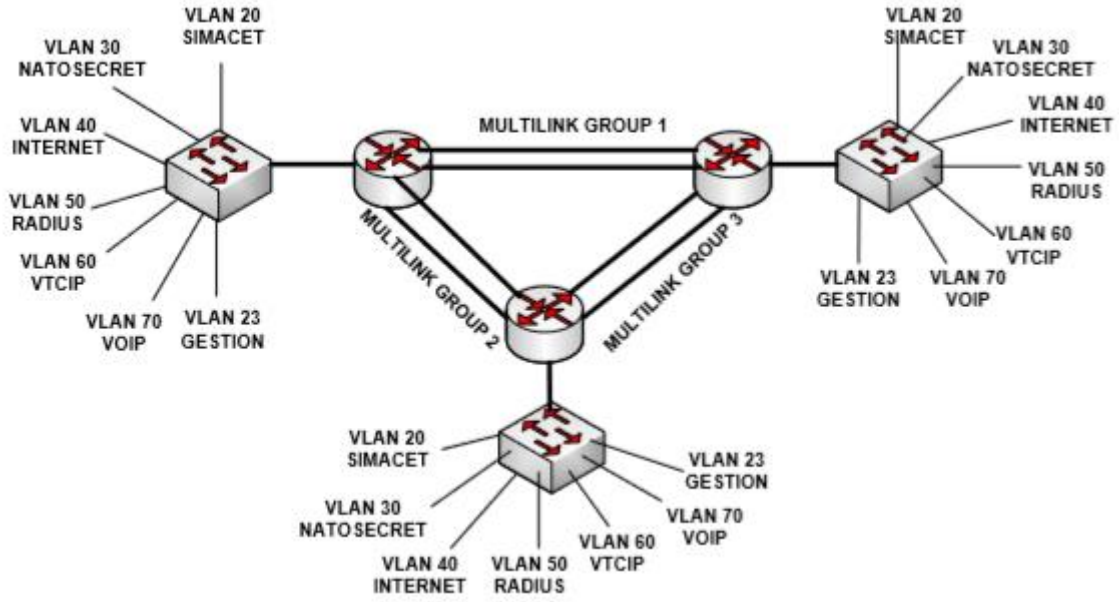

Ilustración 1 Ejemplo de red táctica convergente. Los elementos cuadrados indican los switches y los circulares los routers [3].

Cada VLAN crea su propio tráfico de paquetes que se manda al router más cercano, que se ha de configurar con unos parámetros de QoS para dar prioridad a las redes que necesitan una baja latencia y un jitter (diferencia de latencia de los paquetes) constante como son las de VoIP y VTC-IP. Para asegurar un ancho de banda mínimo a este tipo de redes se le aplica un modelo de calidad de servicio que se le conoce como DiffServ (servicios diferenciados) que se introducirá más adelante.

Los pasos para configurar la QoS en la red son los siguientes:

1. Identificación de los tipos de tráfico y sus necesidades.
2. Clasificación y marcado de los paquetes en función de su tipo de tráfico.
3. Creación de políticas de gestión y evitación de la congestión que prioricen las distintas categorías en cada uno de los equipos de la red.

En cambio, si no se aplica QoS, los routers tratarían a todos los paquetes por igual (independientemente de la VLAN a la que pertenezcan), por lo que no se podría priorizar a unos sobre otros y los requisitos de QoS de las VLAN que se emplean para las aplicaciones más críticas (VoIP, VTC) podrían no cumplirse. Este modo de funcionamiento de la red, en el que no se prioriza el tráfico según su clase, se denomina Best-Effort.

En el Anexo B aparece una entrevista con el Capitán Sergi Heras Lapeña, destinado en el Regimiento de Transmisiones Nº21, sobre la importancia de implementar QoS en las redes tácticas militares.

2.2. **Parámetros de QoS**

Las cuatro parámetros principales de QoS que aparecen en una red convergente son [4]:

- **Ancho de Banda.** El ancho de banda es la cantidad de datos que se pueden transferir entre dos puntos de una red por unidad de tiempo [5]. En una red es un recurso limitado que se tiene que repartir entre todas las aplicaciones que usan la red, ya sean de datos, voz o video.
- **Latencia de extremo a extremo.** La latencia es lo que le cuesta a un paquete llegar de un extremo a otro de la red, esto es, el tiempo que pasa desde que se envía por la fuente hasta que llega al destino. Si bien existen muchos factores que afectan a la latencia extremo a extremo, el principal es el tiempo de espera en las colas (buffers) de los distintos equipos de la red que se atraviesan para llegar al destino [6].
- **Variación de la latencia (Jitter).** El jitter es la variabilidad temporal de la latencia extremo a extremo, ya que no todos los paquetes que viajan por una red experimentan la misma latencia [7], [8]. Igual que la latencia, el principal factor que afecta al jitter es el tiempo de espera en las colas de los equipos de red.
- **Pérdida de paquetes.** Un volumen de tráfico que no sea controlado correctamente puede provocar una saturación de la capacidad de transferencia de datos en una interfaz o en un dispositivo y esto puede provocar que los paquetes se descarten y se pierdan.

Es importante señalar que cada uno de estos parámetros tiene un doble significado. Cuando se refieren a un servicio o aplicación, constituyen los requisitos de QoS de dicho servicio o aplicación. Por el contrario, cuando se refieren a una red, estos parámetros constituyen las prestaciones que se consiguen en esa la red. Estas prestaciones suelen estar interrelacionadas, ya que un bajo ancho de banda disponible tiende a implicar una elevada latencia, jitter y pérdida de paquetes.

Por ejemplo, el servicio de telefonía sobre IP, para funcionar correctamente, requiere que la latencia sea inferior a 150 ms[1], mientras que la latencia que se obtiene en una red táctica suele ser superior a este valor, debido al limitado ancho de banda del que se dispone. Además, el jitter, que indica la variación de la latencia con la que llegan los paquetes de VoIP a su destino, debe estar limitado y controlado, para que los búferes en el receptor no sufran una saturación, ni al contrario se vacíen al completo, causando un decremento en la calidad de la conversación de voz [3], [9].

Por el contrario, una aplicación de datos tiene unos requisitos sobre la latencia y el jitter mucho menos severos (pueden ser de segundos y la experiencia de usuario no se vería mermada). Cuando coinciden comunicaciones de VoIP junto a las aplicaciones de datos, no tiene sentido que todas se traten por igual y deberán utilizarse mecanismos específicos de QoS que prioricen a las aplicaciones críticas con unos requisitos de QoS más estrictos. De este modo es posible conseguir que convivan una gran cantidad de aplicaciones con requisitos diversos (por ejemplo, voz y datos) sobre una red, priorizando unas sobre otras según sus necesidades [10].

2.3. **Mecanismos de QoS**

Para garantizar los requisitos de QoS de las aplicaciones que emplean una red se han propuesto un conjunto de estándares y mecanismos específicos. Mediante el uso de estos

1 Valor recomendado por Cisco para una muy buena calidad de voz, no obstante, otros fabricantes aseguran que se pueden obtener valores de hasta 400ms para alcanzar un nivel óptimo, siendo de esta manera la única posibilidad de lograr comunicaciones satélites de VOIP [12] [13].

mecanismos, los administradores de red pueden usar los recursos existentes de manera eficiente y garantizar el nivel de servicio requerido sin expandir de forma reactiva ni aprovisionar en exceso o sobredimensionar sus redes [11].

Como se ha comentado antes, las redes convergentes soportan distintos servicios y aplicaciones y por lo tanto necesitan implementar procedimientos que regulen los flujos de tráfico de los servicios y aplicaciones según sus prioridades o necesidades. A modo de ejemplo, los servicios de telefonía IP o videoconferencia son prioritarios. La pérdida de paquetes de estas aplicaciones provocaría una total perdida de la comunicación. Por el contrario, servicios como el correo electrónico necesitan menos requisitos de prioridad, por lo que los mecanismos de QoS deberían asignar más recursos para la telefonía IP que para el correo electrónico [9].

Es importante señalar que los mecanismos de QoS no solucionan los problemas de congestión que puede haber en una red (la congestión aparece cuando el tráfico que entra a la misma es superior al que puede soportar). Sin embargo, sí que van a conseguir que en estas situaciones las aplicaciones más críticas funcionen mejor que las que no lo son.

Para implementar estos mecanismos y proporcionar garantías de QoS en las redes IP convergentes se pueden emplear dos modelos de QoS distintos, los cuales son [3], [4]:

Servicios Integrados o IntServ: Proporciona a ciertas aplicaciones un nivel de servicio garantizado mediante la reserva de recursos en los dispositivos de la red y la aplicación de mecanismos de control de admisión (solo se acepta un nuevo flujo si se asegura que se puede cumplir con sus requisitos de QoS y con el de todos los flujos que ya están en la red). Se garantiza las características de cada flujo, tales como el ancho de banda, latencia y las tasas de pérdida de paquetes, de extremo a extremo. El modelo IntServ no es escalable para grandes redes.

Servicios Diferenciados o DiffServ: Este modelo incluye un conjunto de herramientas de clasificación y marcado, además de mecanismos de gestión de colas, que permiten priorizar determinados protocolos o aplicaciones. Para ello, el tráfico de la red se puede clasificar en función de la dirección de red, protocolos, puertos, interfaces de entradas y ACL (Access Lists). Sus beneficios son que es altamente escalable y que ofrece diferentes niveles de QoS en función de la clasificación que se haga del tráfico.

2.4. **Implementación de QoS mediante DiffServ**

Para poder implementar QoS mediante DiffServ se debe identificar los tipos de tráfico y sus necesidades, clasificar el tráfico basada en las necesidades detectadas y por último definir las políticas de red o de calidad de servicio para cada clase de tráfico.

2.4.1. Identificación de los tipos de tráfico y sus necesidades

Para identificar los tipos de tráfico y sus necesidades se recomienda realizar una auditoría de red que observe el comportamiento de la red y las aplicaciones que en ella se utilizan. Mediante este estudio se identifican las necesidades de tráfico de cada sistema, el ancho de banda mínimo garantizado que necesita cada aplicación, la pérdida de paquetes dependiendo de las horas punta de utilización de cada sistema y la latencia de los paquetes.

2.4.2. Clasificación de tráfico

Después de la auditoria, se realiza una clasificación del tráfico. A continuación y a modo de ejemplo, se describe una de las más aplicadas (las clases aparecen por orden de prioridad de más alta a más baja) [10]:

- **Clase de Voz (VoIP)**: Más alta prioridad y categoría. Necesita un ancho de banda limitado y constante. Requiere muy baja pérdida de paquetes y una latencia por debajo de 150 ms.
- **Clase de Misión Crítica**: Aplicaciones como la VTC-IP.
- **Clase de aplicaciones transaccionales**: Aplicaciones de base de datos e interactivas.
- **Clase de Señalización**: Es el tráfico que corresponde al establecimiento de la llamada de voz, la configuración, y el cierre. A menudo este tipo de tráfico se suele poner en una clase separada al tráfico propio de la conversación de VoIP, debido a que esta clase tiene un ancho de banda limitado.
- **Clase Best-Effort**: Tráfico que no se clasifica en ninguna de las otras clases. Se le permite emplear el ancho de banda sobrante.
- **Clase Basura (Scavenger):** Aplicaciones no esenciales como aplicaciones Peer-to-Peer.

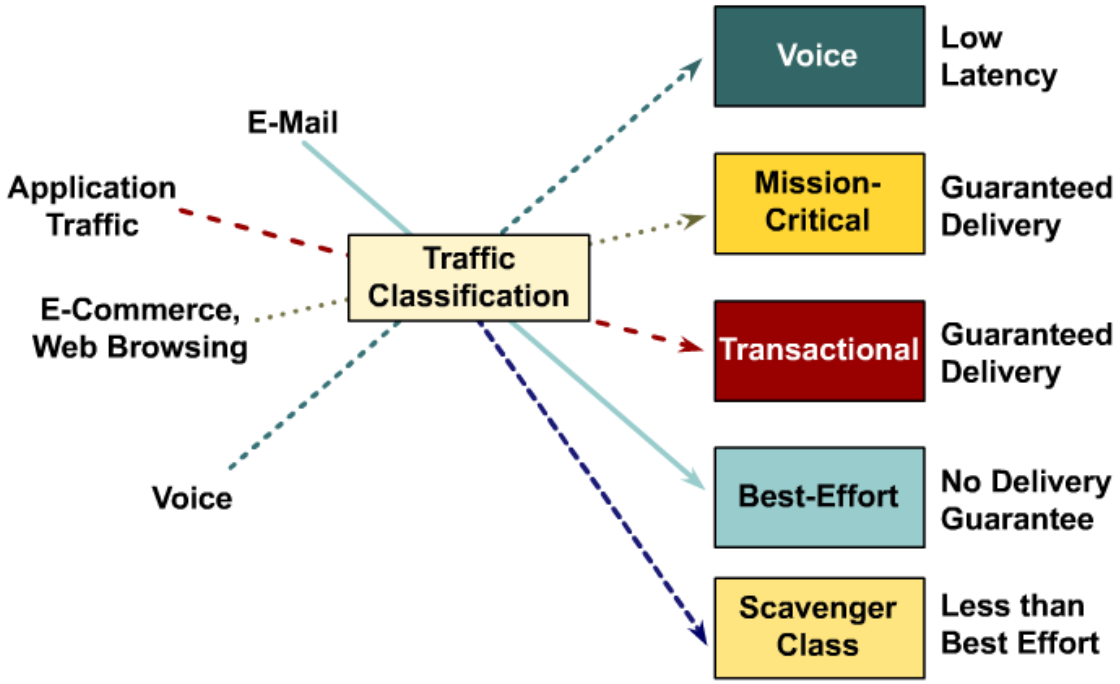

Ilustración 2 Ejemplo de clasificación del tráfico basada en las necesidades detectadas [2].

Como se puede observar en la *Ilustración 2*, el tráfico de las distintas aplicaciones y servicios (e-mail, navegación web, voz) se clasifica en las distintas clases definidas anteriormente.

2.4.3. Definición de políticas para cada clase de tráfico

Por último, se define una política de QoS que establece para cada clase. Esta política incluye para cada clase: i) límite máximo de ancho de banda que va a usar, ii) ancho de banda mínimo garantizado, iii) nivel de prioridad respecto al resto de clases, iv) mecanismos de gestión de la congestión que se le van a aplicar (gestión de las colas que se emplean en los routers y los switches y otros mecanismos adicionales que se explican en el siguiente apartado). En la siguiente tabla aparece esta política para las distintas clases definidas en el apartado anterior.

Clase	Prioridad	Tipo de Cola	Min/Max Ancho de Banda	Tecnologías QoS adicionales
Voz	5	Prioritaria	1 Mbps Min 1 Mbps Max	Cola Prioritaria
Misión Crítica	4	CBWFQ	1 Mbps Min	CBWFQ
Señalización	3	CBWFQ	400 Kbps Min	CBWFQ
Transacional	2	CBWFQ	1 Mbps Min	CBWFQ
Best-Effort	1	CBWFQ	500 Kbps Max	CBWFQ CB-Policing
Tráfico Basura	0	CBWFQ	Max 100 Kbps	CBWFQ CB-Policing WRED

Tabla 1 Definición de políticas para cada clase de tráfico [2].

2.5. **Mecanismos de gestión de la congestión**

La congestión puede ocurrir en cualquier lugar dentro de una red donde la velocidad no sea la adecuada, bien por qué no hay coincidencia de ancho de banda con otros componentes de la red o por qué se produce la agregación de varios enlaces (ver *Ilustración 3*).

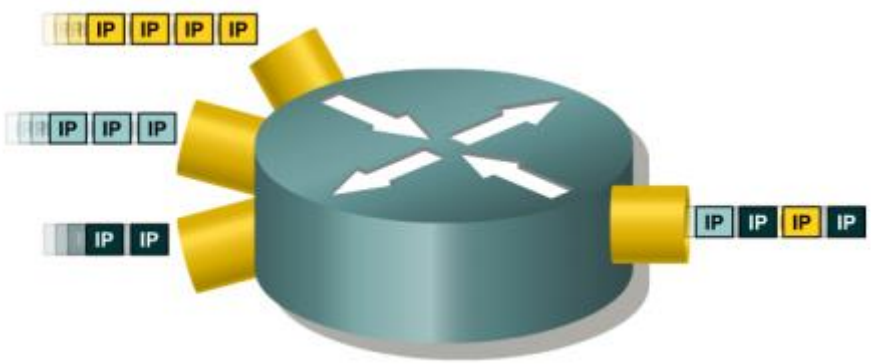

Ilustración 3 Ejemplo de agregación de varios enlaces [2]

En estos casos será necesario habilitar herramientas de gestión de la congestión que la controlen cuando se produzca. Una manera en que los elementos de la red (routers fundamentalmente) manejan el desbordamiento ocasionado por la llegada de tráfico excesivo es almacenarlo en sus colas[2] y, a continuación, utilizar métodos que den prioridad a algunos paquetes hacia el enlace de salida.

En función del método que se emplee para elegir qué paquete se transmite en cada momento de todos los que están esperando en las colas (el cual dependerá de las prioridades asignadas a los paquetes), se tendrán distintas estrategias de encolado (queueing) que ayudarán a garantizar los requisitos QoS de los distintos tráficos que hay en la red.

[2] Las colas de los equipos de red son buffers en el que se almacenan los paquetes antes de ser transmitidos por un enlace cuando en ese momento se está transmitiendo otro paquete por el enlace.

En un sistema sin QoS, cada router emplea una única cola en la que se van almacenando todos los paquetes que se quieren transmitir por un enlace. La transmisión de los paquetes se produce posteriormente por su orden de llegada a la cola (los primeros en llegar son los primeros en ser transmitidos). Este tipo de estrategia se denomina FIFO (First In, First Out). Este tipo de solución con una única cola FIFO no garantiza los requisitos de QoS de los distintos tráficos que hay en la red, por lo que no se debe usar si se quiere emplear QoS en la red.

Por el contrario, si se quiere aplicar QoS en la red, la solución habitual es emplear una cola distinta para cada tipo de tráfico, de tal modo que los paquetes esperan en una cola u otra en función de su clase, que se ha definido previamente. Posteriormente, el router determina el orden de transmisión de los paquetes que hay esperando en cada cola, en función de los recursos asignados a cada clase de tráfico.

Los métodos más utilizados para la gestión de colas en redes convergentes y que se emplean también en los ejercicios militares tácticos son el *Class-Based Weighted Fair Queuing* (CBWFQ) y el *Low Latency Queuing* (LLQ), los cuales se explican a continuación.

2.5.1. Class-Based Weighted Fair Queuing (CBWFQ)

Con CBWFQ se tiene una cola FIFO distinta para cada una de las distintas clases de tráfico que se han definido, de modo que el tráfico que pertenece a una clase es enviado a la cola de esa clase.

Después de definir los criterios para aceptar paquetes en una clase, se asigna a cada clase los recursos necesarios para garantizar sus requisitos de QoS. En concreto a cada clase se le asigna un ancho de banda y un límite máximo de paquetes que pueden ser almacenados en su cola correspondiente. El ancho de banda asignado a una clase se corresponde con el mínimo ancho de banda garantizado para dicha clase en periodos de congestión. El tamaño máximo de la cola de esa clase determina el número máximo de paquetes que se permite almacenar en la cola de la clase. Cuando una cola ha llegado a su límite de capacidad, los paquetes adicionales serán descartados. Este mecanismo garantiza a cada cola (y por tanto a cada clase) un ancho de banda mínimo, pero también permitiría el acceso a más ancho de banda en el caso de que estuviera disponible, por ejemplo, porque el resto de las colas no están haciendo uso de su ancho de banda asignado. En un router Cisco se pueden configurar hasta un máximo de sesenta y cuatro clases independientes cuando se emplea CBWFQ. La siguiente figura explica gráficamente el método CBWFQ.

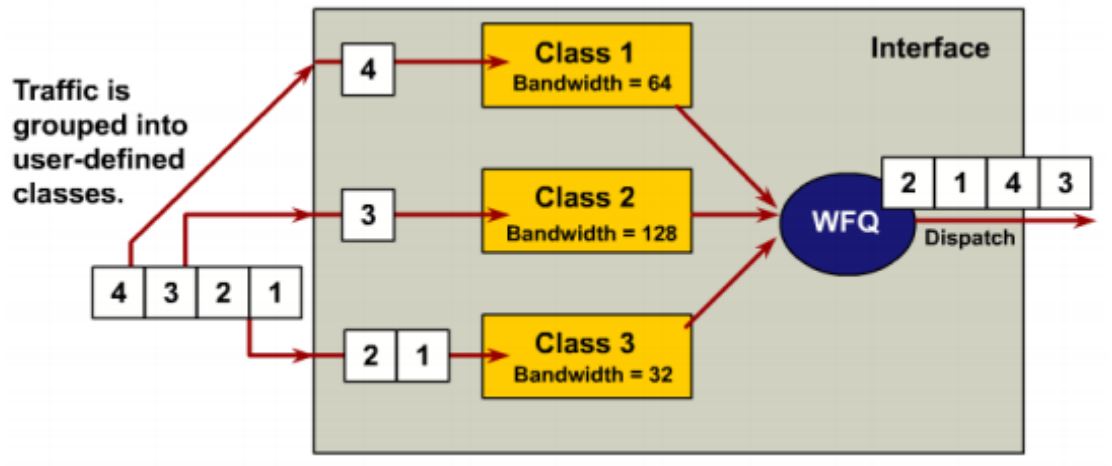

Ilustración 4 Arquitectura CBWFQ

El inconveniente que presenta CBWFQ es que el tráfico que requiere un retardo mínimo, como la voz, todavía puede sufrir latencias inaceptables cuando se utiliza CBWFQ como único mecanismo de cola. Esto se debe a que CBWFQ proporciona un sistema de colas ponderado en función del ancho de banda definido para cada clase (ver *Ilustración 4*), pero sin asegurar una prioridad estricta para el tráfico de ninguna clase. Este inconveniente se soluciona con la introducción de LLQ, como se verá en el siguiente apartado.

2.5.2.Low Latency Queuing

El método Low Latency Queuing (LLQ) es una combinación de un sistema de colas CBWFQ, en las cuales se asigna pesos a la cola de cada clase de acuerdo con el ancho de banda que necesita la clase, y un sistema de colas basado en prioridades (ver *Ilustración 5*). En LLQ se puede forzar que los paquetes correspondientes al tráfico de una o varias clases se almacenen en una cola de prioridad estricta (priority queue), que tiene prioridad absoluta respecto al resto de colas. La cola con prioridad estricta permite enviar siempre en primer lugar los datos sensibles a la latencia (como por ejemplo la voz). De este modo, los paquetes de voz que entran en el sistema LLQ se envían a la cola con prioridad, donde tienen una asignación fija de ancho de banda y se sirven en primer lugar (pero limitándose al ancho de banda fijo asignado a la clase para no canibalizar al resto). Los paquetes de datos que no pertenecen a clases prioritarias entran en el sistema de colas CBWFQ donde los achos de banda asignados a cada cola determinarán la forma en que los paquetes serán tratados. La siguiente figura muestra el esquema de un sistema LLQ.

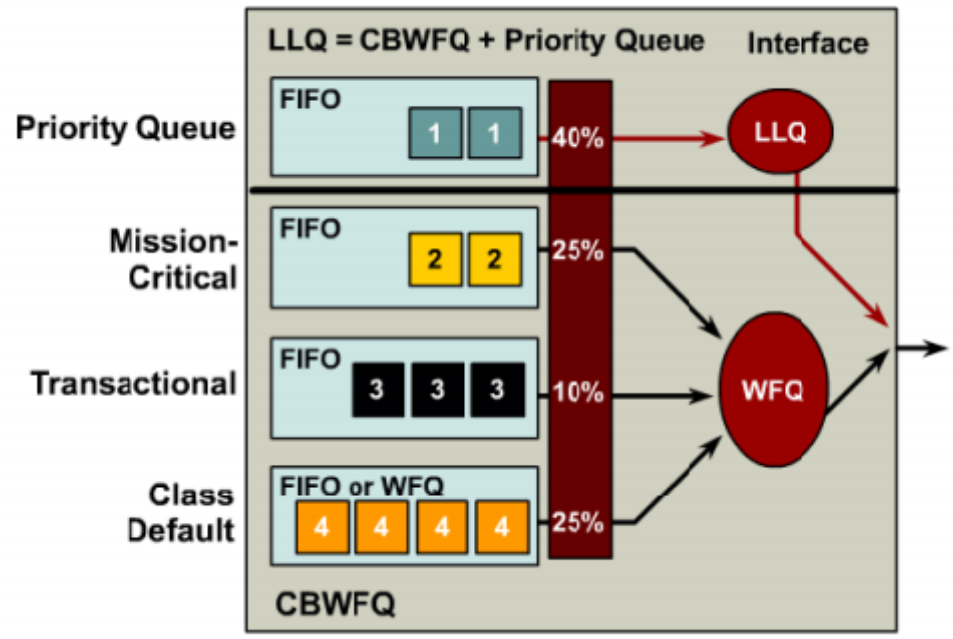

Ilustración 5 Arquitectura LLQ

2.5.3.Traffic Shaping y Traffic Policing

Finalmente, se describen dos mecanismos de gestión de la congestión adicionales que se pueden emplear en paralelo a las estrategias de queueing descritas anteriormente y que son el conformado de tráfico (traffic shaping) y la política de tráfico (traffic policing).

El traffic shaping se utiliza para conseguir que el tráfico de una clase cuya tasa de transferencia no es constante se uniformice (sin superar el ancho de banda máximo asignado a la clase). Para ello se emplea una cola en la que se almacena todo el tráfico recibido en periodos en los que la tasa de transferencia puntual es superior al ancho de banda máximo asignado a la clase, y se transmiten cuando la tasa de transferencia puntual es inferior.

Por el contrario, el traffic policing aplica una política mucho más agresiva que el traffic shaping. En el traffic policing se descarta todo el tráfico que supera el ancho de banda máximo asignado a la clase (en vez de almacenarse). En las siguientes figuras se puede ver el comportamiento de ambos mecanismos frente al mismo tráfico de entrada.

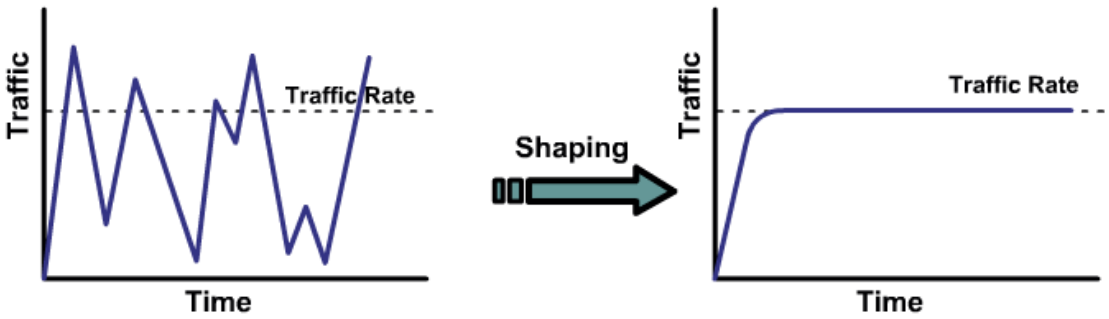

Ilustración 6 Con Shaping el flujo de tráfico se acomoda al ancho de banda de los enlaces para evitar el desbordamiento de los buffers de salida [1].

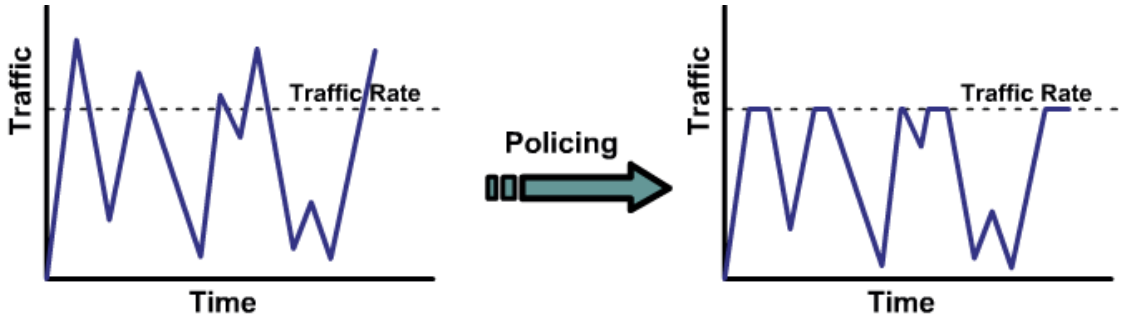

Ilustración 7 Con Policing se descartan los paquetes que superan un límite predefinido en lugar de almacenarse para su posterior reenvío [2].

Tanto traffic policing como traffic shaping son mecanismos que se utilizan en una red para controlar la tasa de transferencia, acondicionando el tráfico en función de sus características y las del enlace. Para ello, ambos mecanismos miden en tiempo real la tasa de transferencia de las distintas clases y la comparan con el ancho de banda asignado a cada clase, intentando hacer coincidir ambos.

La principal diferencia entre traffic policing y traffic shaping tiene que ver con la acción resultante después de comparar la tasa de transferencia real de una clase con el valor de ancho de banda máximo asignado a la clase. Mientras que traffic policing elimina el exceso de tráfico para poder controlar el flujo y mantenerlo dentro de los límites fijados, traffic shaping intenta transmitirlo con posterioridad. Desde el punto de vista de los paquetes transmitidos en la red, traffic shaping perderá menos paquetes, a costa de una mayor latencia, mientras que traffic tolicing tendrá menores latencias (al no almacenar paquetes), pero un mayor número de paquetes perdidos. El uso de una estrategia u otra dependerá de cada clase, de sus requisitos de QoS y de su estadística de tráfico. Si la clase requiere una latencia baja y su tasa de transmisión es constante, interesa usar traffic policing. Por el contrario, si la latencia no es tan importante y la tasa de transmisión es variable, interesa usar traffic shaping para perder menos paquetes y aumentar la eficiencia del enlace.

3. Implementación de QoS en equipos Cisco

En este capítulo se explica cómo se aplica las técnicas de QoS vistas en el capítulo anterior en equipos Cisco, que son los empleados comúnmente en el Ejército. Cisco permite implementar la QoS mediante un método denominado *Modular QoS Command-Line interface* (MQC), el cual consta de 3 pasos que corresponden a grandes rasgos con los definidos en la sección 2.4:

1) Definir clases de tráfico, haciendo uso de las sentencias 'class-map'
2) Marcar y establecer políticas para cada clase, haciendo uso de las sentencias 'policy-map'
3) Aplicar las políticas anteriores, con el comando 'service-policy output' aplicado a interfaces.

Además de este método MQC, Cisco dispone del método *AutoQoS*, el cual permite que la configuración de QoS de los equipos se haga sola. No obstante, este método es relativamente nuevo y no está desarrollado por completo. Por tanto, el método que se va a utilizar en este TFG será el MQC [12]. A continuación, se expondrá a grandes rasgos cómo se aplicaría el método MQC.

3.1.1. Definición de clases de tráfico (Class-map)

La definición de clases de tráfico se realiza con el comando class-map y se puede realizar de dos maneras:

ROUTER(config)#class-map match-all VOIP

ROUTER(config)#class-map match-any VOIP

Cuando usamos el primer comando, significa que para clasificar un paquete como de VoIP, sus características deberán coincidir con todas las líneas del class-map posteriores. Por ejemplo:

ROUTER(config)#class-map match-all VOIP
ROUTER(config-cmap)#match access-group 10
ROUTER(config-cmap)#match access-group 20

Siendo access-group 10 una lista de direcciones IP de origen y access-group 20 una lista de direcciones IP de destino predefinidas. Por tanto, para que un paquete sea clasificado como VOIP debe tener una dirección de origen y destino que corresponda con sus respectivos access-group.

Para el comando any, sería suficiente con que la dirección IP origen o la dirección IP destino coincidieran con alguna de las correspondientes direcciones que están en los access-group. Por ejemplo:

ROUTER(config)#class-map match-any VOIP
ROUTER(config-cmap)#match access-group 10
ROUTER(config-cmap)#match access-group 20

Mediante este sistema, se pueden crear todos los class-map que sean necesarios, pudiendo matchear por ejemplo:

- IP de origen
- IP de destino

- Marca de paquete
- Access-group
- Interfaz de entrada
- Interfaz de salida

3.1.2.Policy-map

Seguidamente se crearán los policy-map donde se marcarán los paquetes y se aplicarán las políticas de gestión de la congestión. En primer lugar, se asocian las clases definidas anteriormente con el comando class-map a las distintas políticas y se marcan con uno de los tipos de marcado posibles. Estas marcas se codifican en un subconjunto de bits de la cabecera IP de los paquetes (en el Anexo C se explica con más detalle el mecanismo que se emplea para marcar los paquetes en DiffServ), de tal modo que cualquier equipo en la red podría emplear estas marcas posteriormente como criterio para aplicar sus políticas de gestión de la QoS:

- **Mediante IP precedence (3 bits de la cabecera IP):**

ROUTER (config)#policy-map MARCADOMS
(Nombre del policy-map)

ROUTER(config-pmap)#class VOIP
(Aquí se define el class-map que se quiere marcar)

ROUTER(config-pmap-c)#set precedence flash
(Aquí se marca el campo IP precedence de la cabecera IP de cada paquete con el valor 'flash')

- **Por DSCP (7 bits de la cabecera IP):**

ROUTER(config)#policy-map MARCADOMS
(Nombre del policy-map)

ROUTER(config-pmap)#class VOIP
(Aquí se define el class-map que se quiere marcar)

ROUTER (config-pmap-c)#set ip dscp cs4
(Aquí se marca el campo DSCP de la cabecera IP de cada paquete con el valor cs4)

En el caso de tener interfaces hacia otros centros, se tienen que aplicar políticas de gestión de colas que garanticen la QoS en esos interfaces. El mecanismo de gestión de colas utilizado por los administradores del Regimiento de Transmisiones Nº21 es el Class-Based Weighted Fair Queuing (CBWFQ), pero dependiendo de la situación también puede llegar a usarse el Low-latency queuing (LLQ).

En primer lugar, se expondrá la configuración del modelo CBWFQ. Para ello se emplea en primer lugar los comandos:

ROUTER (config)#policy-map *MARCADOMS*
(Nombre del policy-map)

ROUTER (config-pmap)#class *VOIP*
(Aquí se pondrá la clase a la que se quiere asignar un ancho de banda)

Seguidamente, hay tres métodos de asignar el ancho de banda a una clase mediante el comando bandwidth:

1. El primer método especifica la asignación del ancho de banda en velocidad de bits por segundo (bps).

   ROUTER (config-pmap-c)#bandwidth (kbps)

2. El segundo método especifica la asignación de ancho de banda como un porcentaje de la velocidad del interfaz.

   ROUTER (config-pmap-c)# bandwidth (percent)

3. El tercer método especifica la asignación del ancho de banda un como porcentaje del ancho de banda que queda disponible, por ejemplo, si un interfaz tiene cogido un 30% de ese interfaz, con el comando remaining se reparte el 70% que queda de ese ancho de banda del interfaz.

   ROUTER (config-pmap-c)# bandwidth (remaining percent)

En caso de querer aplicar LLQ, la configuración es idéntica a la realizada con CBWFQ, con la diferencia de que la clase en la cual se requiere prioridad estricta debe ser configurada de la siguiente forma:

> ***ROUTER (config)#***policy-map *MARCADOMS*
> *(Nombre del policy-map)*
>
> ***ROUTER (config-pmap)#***class *VIDEO*
> *(Aquí se pondrá la clase que se quiere mandar a la cola de alta prioridad)*
>
> ***ROUTER (config-pmap-c)#***priority (kilobits)
> ***ROUTER (config-pmap-c)#*** priority (percent)
> *(se le asigna un ancho de banda a la clase con el comando priority, de uso similar al comando bandwidth)*

Esto es, para enviar tráfico de tiempo real a una cola con prioridad estricta, se emplea el comando ***priority*** dentro de la configuración de dicha clase dentro de la política (en lugar de utilizar el comando ***bandwitdh*** para, simplemente, asignar ancho de banda, que se utilizará en el resto de clases CBWFQ).

Las clases a las que se les aplica el comando ***priority*** se consideran clases prioritarias. Dentro de una política, puede haber una o más clases prioritarias. Cuando varias clases dentro de una única política se configuran como clases prioritarias, todo el tráfico de estas clases es enviado a la misma (y única) cola de prioridad estricta.

3.1.3. Implementación de Traffic Shaping

El conformado de tráfico (traffic shaping) se utiliza normalmente cuando hace falta prevenir la congestión en redes donde se tienen equipos conectados a enlaces con valores de ancho de banda muy distintos, como es habitual en el caso del Ejercito. En concreto, el ejército cuenta con dispositivos que tienen mayor ancho de banda, como sería el caso del Pentatrama, que sería

capaz de proporcionar cinco tramas de 10 Mbps, y otros con menor ancho de banda, como sería el SOTM (Satcom Of The Move) que solo puede proporcionar una trama de 256 Kbps. Por ello, es necesario implementar conformado de tráfico, que en el caso de equipos Cisco se denomina *Class-Based-Shaping.*

El *Class-Based-Shaping* se usa en una configuración basada en MQC y puede utilizarse en combinación con CBWFQ y LLQ, configurándose de la siguiente manera:

ROUTER(config)#policy-map *QOSSAT8M*
(Nombre del policy-map)

ROUTER(config-pmap)#class ANY
(Aquí se debe poner el class-map ANY que se tiene configurado previamente. ANY quiere decir que es para todo el tráfico)

ROUTER(config-pmap-c)#shape average 1000000000 *1 Gbps

El conformado de tráfico trabaja con las colas, y lo que hace es retrasar la transmisión de los paquetes para que estos no superen el límite permitido. El inconveniente de este mecanismo es que cuando se tiene mucho flujo de tráfico, es posible que los retardos que sufren los paquetes sean elevados debido a que muchos paquetes se van almacenando en las colas para no superar la tasa de transmisión promedio configurada en el conformado de tráfico [13]. Por ello, cuando este mecanismo se usa en combinación con CBWFQ, es recomendable anidar una política a la otra de manera jerárquica como se mostrará en el siguiente ejemplo:

ROUTER(config)#policy-map QOSSAT8M
ROUTER(config-pmap)#class TrafA
ROUTER(config-pmap-c)#bandwitdh percent 60
ROUTER(config-pmap)#class TrafB
ROUTER(config-pmap-c)#bandwitdh percent 20
ROUTER(config-pmap)#class TrafC
ROUTER(config-pmap-c)#bandwitdh percent 15
ROUTER(config)#policy-map SHAPE
ROUTER(config-pmap)#class TrafT
ROUTER(config-pmap-c)#shape average 256000
ROUTER(config)#service-policy BW

La finalidad de utilizar el comando ‘shape’ es repartir manualmente el ancho de banda y además limitarlo a 256000 para la clase de tráfico TrafT.

4. Resultados de la aplicación de QoS en una red táctica

A continuación, se exponen los resultados obtenidos tras la implementación de la calidad de servicio en distintos ejercicios realizados durante la estancia en el Regimiento de Transmisiones Nº21. En el primer punto se realizará un ensayo en un entorno controlado, cuya finalidad será ver cómo se puede marcar el tráfico al gusto del usuario. Se marcará el tráfico como de videollamada debido a que el ejercicio sobre el terreno se centrará en la videollamada y la gestión del ancho de banda aplicando QoS para obtener una mejoría de la calidad de imagen.

4.1. Marcado de paquetes de videollamada generados en un ambiente controlado

A continuación, se va a mostrar cómo se monitoriza el tráfico generado con la herramienta *QoS Traffic*, la cual permite generar un tráfico específico de datos durante un tiempo delimitado. Esta herramienta permite que un mismo equipo pueda generar tráfico y a la vez estudiar y capturar la información al mismo tiempo mediante *Wireshark*, siendo dicho programa un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones. El objetivo de esta prueba será comprobar que verdaderamente dicho tráfico generado se está marcando con el valor DSCP deseado [14], [15].

Para ello, en primer lugar, se dejará capturando el *Wireshark* (ver *Ilustración 9*).

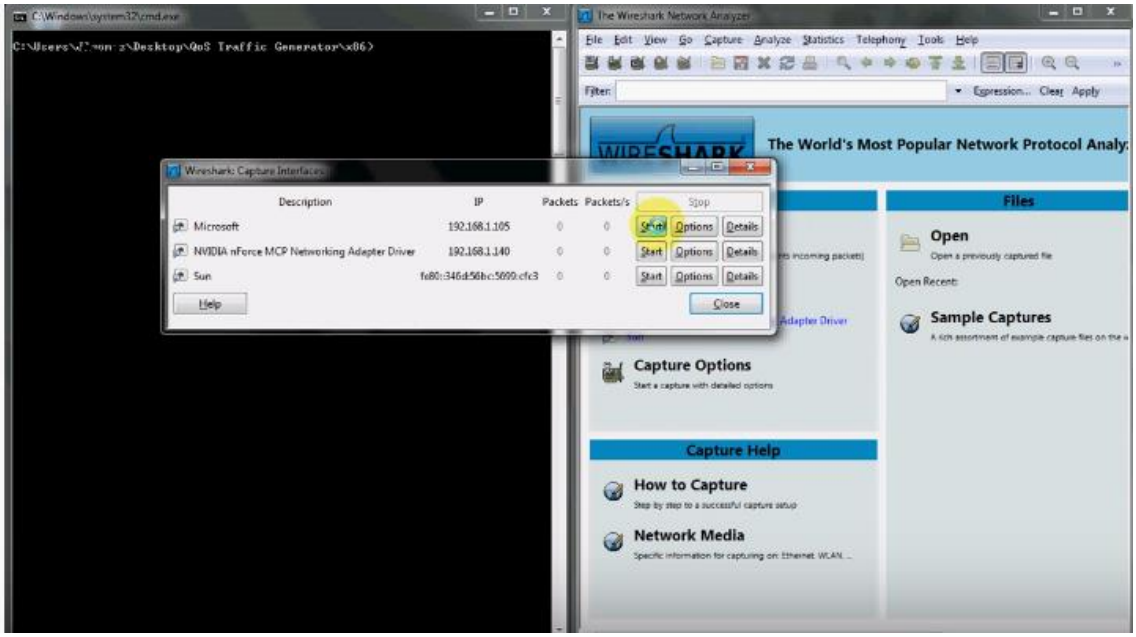

Ilustración 8 Interfaz de captura del Wireshark

Una vez Wireshark está funcionando y capturando el tráfico, se usará la consola de comandos de Windows (cmd) para utilizar la herramienta de *QoS Traffic*. En esta herramienta se introducirán los siguientes parámetros: modo de trabajo, tipo de tráfico, destino del tráfico, tamaño del tráfico enviado, tiempo durante el que se enviará el tráfico, valor DSCP y el valor IEEE 802.1p[3]. Para ello, se emplean las siguientes opciones (ver *Ilustración 10*):

1. source (modo servidor)
2. –udp (user datagram protocol) (tipo de tráfico enviado)
3. –dest 192.160.1.1 (destino)
4. –throttle 1000 (1 Kilobit)

3 "**IEEE 802.1p** es un estándar que proporciona priorización de tráfico y filtrado multicast dinámico. Esencialmente, proporciona un mecanismo para implementar Calidad de Servicio (QoS) a nivel de MAC (Media Access Control)" [19][20].

5. –duration 2 (tiempo en segundos durante el que se mandará tráfico)
6. –tc 40 (valor DSCP prioritario)
7. 4 (valor IEEE 802.1p usado para video, explicado en el Anexo D)

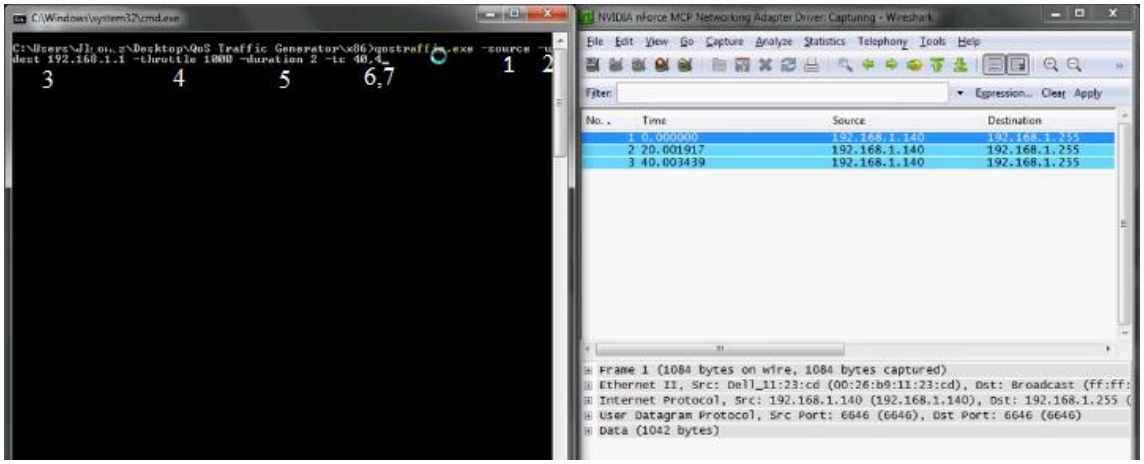

Ilustración 9 Comando introducido en la cmd de Windows

Una vez se ha introducido dicho comando, se procederá a su ejecución. Se puede observar mediante la aplicación de *Wireshark* todo el tráfico que se ha generado durante dos segundos.

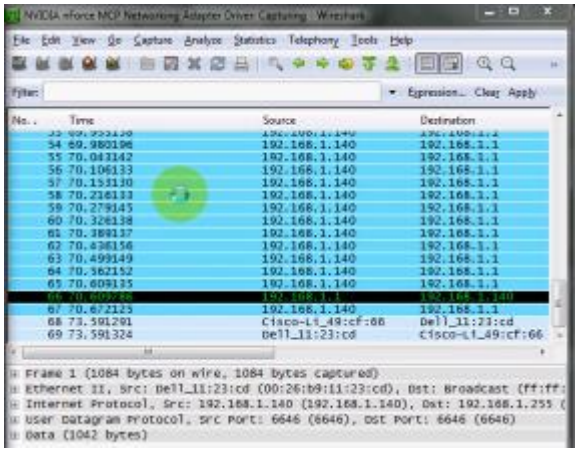

Ilustración 10 Tráfico capturado Wireshark

Para comprobar el marcado se abre uno de los paquetes capturados y se accede al protocolo de Internet. Una vez seleccionado se puede verificar que el valor de DSCP del paquete es 0x28 (ver Anexo C para los distintos valores del código DSCP).

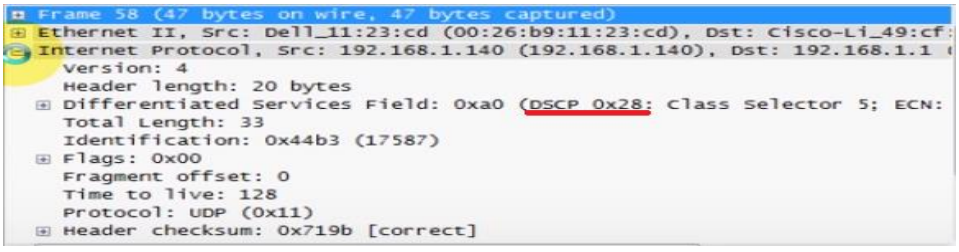

Ilustración 11 Valor DSCP, protocolo Internet capa 3

Para comprobar que también se puede mandar tráfico sin marcar, ejecutaremos la siguiente línea de comando, donde no aparecerá ni el valor del DSCP ni el del IEE 802.1P.

```
C:\Users\JL\Desktop\QoS Traffic Generator\x86>qostraffic.exe -source -u
dest 192.168.1.1 -throttle 1000 -duration 2
```

Ilustración 12 Comando de paquetes sin marcar

En la siguiente ilustración se muestra como los paquetes generados ya no están marcados.

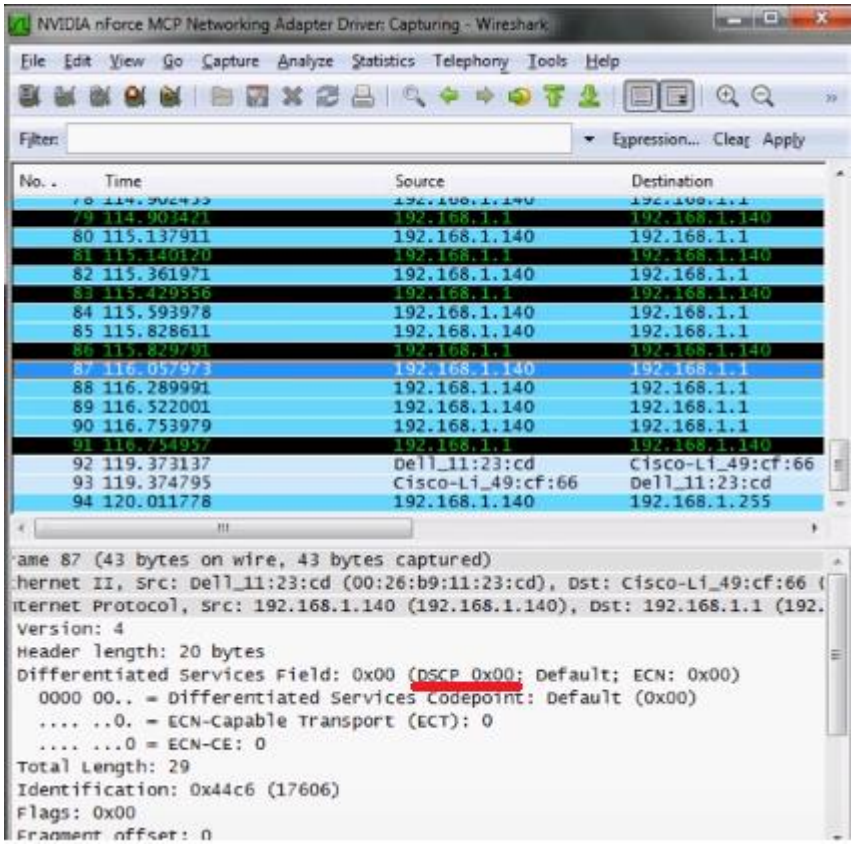

Ilustración 13 Paquetes sin marcar capturados por Wireshark

De este modo se puede generar tráfico y comprobar que los paquetes marcados en la red se transmiten adecuadamente.

4.2. **Aplicación de la calidad de servicio para un caso práctico en ambiente militar OTAN**

La aplicación de las técnicas de QoS en un ejercicio táctico en ambiente militar OTAN, se realizó a través del SOTM (Satcom of the Move), vehículo militar que cuenta con un enlace vía satélite capaz de proporcionar una trama de 256 Kbps. Para la gestión del ancho de banda disponible se ha considerado una situación en la cual se iban a utilizar cuatro clases de tráfico: videollamada, señalización, telefonía IP y otros servicios como podría ser el correo electrónico. Dicho ejercicio consistió en hacer un reconocimiento por la isla de Menorca, realizando pruebas de enlaces con el Puesto de Mando de Cuerpo de Ejército (PMCE) que se encontraba en la Base San Isidro. Las pruebas de enlace consistieron en hacer video llamadas y llamadas mediante telefonía IP. Como los SOTM no cuentan con router, toda la configuración de QoS se realizó en un Adaptive Server Anywhere (ASA) que es un sistema administrador de bases de datos relacionales de alto rendimiento, que dentro de su funcionalidad incluye gestión de transacciones,

integridad referencial, procedimientos almacenados Java y SQL, triggers, bloqueo a nivel de registro, programación de eventos y recuperación automática [16]. En el Anexo E se explica en detalle la topología de red completa del ejercicio OTAN, las pruebas realizadas en este apartado se efectuaron sobre dicha red.

Los paquetes de videollamada y de telefonía IP se configuraron mediante el mecanismo LLQ debido a que eran paquetes prioritarios. En cambio, el resto de los paquetes de datos que no pertenecen a las clases prioritarias (señalización y el resto de servicios) entran en el sistema de colas CBWFQ.

Ilustración 14 SOTM

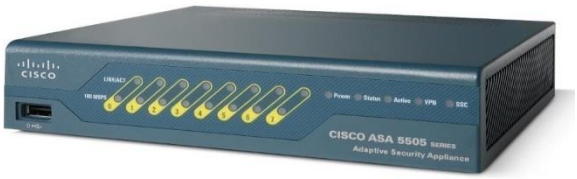

Ilustración 15 ASA

Ilustración 16 Ruta de reconocimiento con el SOTM

En la ilustración de la ruta realizada se pueden apreciar cuatro puntos señalizados: Puerto de Mahón, Villacarlos, Trepucó y una rotonda en la carretera Me-1. El SOTM al ser un sistema satélite no le afecta realmente la posición, dichas ubicaciones marcan los puntos donde se reconfiguró el ASA con diferentes parámetros de QoS.

En primer lugar, el ASA se configuró con una QoS en el Puerto de Mahón con la siguiente configuración:

- 64 Kbps para videollamada
- 64 Kbps para llamadas IP
- 64 Kbps para señalización (para establecer enlace)
- 64 Kbps para el resto de servicios

Con dicha configuración se obtuvo una mala calidad en la videollamada debido a que la asignación del ancho de banda para este servicio no era suficiente, en cambio la llamada con telefonía IP funcionaba correctamente.

Ilustración 17 Prueba videollamada a 64Kbps

En la Ilustración 12 se puede apreciar que el administrador del satélite no se ve claramente y que la imagen está claramente pixelada, demostrando la baja calidad de la videollamada. Esta baja calidad se debe a la gran cantidad de paquetes perdidos como se ve en la siguiente tabla.

Participante	Nombre del canal	Paquetes perdidos	Pérdida paquetes %
Local	Audio Tx	353	22
Local	People Tx	1117	50
1002	Audio Rx	81	22
1002	People Rx	203	62

Tabla 2 Pérdida de paquetes en el Puerto de Mahón

A continuación, se describe cada una de las entradas de esta tabla:

- Local Audio Tx, es el audio que se emite desde el SOTM durante la video llamada, en la tabla se puede observar cómo se pierde un 22%
- Local People Tx es el video que se emite desde el SOTM durante la video llamada, en la tabla se puede observar que se pierde un 50%
- 1002 Audio Rx es el audio que recibe el SOTM por parte del centro durante la video llamada, en la tabla se puede observar que se pierde el 22%
- 1002 People Tx es el video que recibe el SOTM por parte del centro durante la video llamada, en la tabla se puede observar que se pierde el 62%

Analizando los datos, se observa que la cantidad de información que se pierde por el audio no es excesiva, en cambio el video se puede observar cómo el 50% de los paquetes se pierden por parte del SOTM y el 62% por parte del centro. Estos parámetros muestran claramente que los parámetros de QoS elegidos (el reparto del ancho de banda entre las distintas clases) no son buenos y por tanto hay una mala gestión de los recursos de transmisión.

Con los resultados obtenidos, se reconfiguró la ASA con una QoS diferente en Villacarlos con los siguientes parámetros:

- 96 Kbps para video llamada
- 64 Kbps para llamadas IP
- 64 Kbps para señalización (para establecer enlace)
- 32 Kbps para el resto de servicios

Con dicha configuración se obtuvo una pequeña mejora de la calidad en la videollamada debido a que la distribución del ancho de banda para este servicio se aumentó en 32Kbps. La llamada con telefonía IP seguía funcionando correctamente.

Ilustración 18 Prueba videollamada a 92Kbps

En la ilustración anterior se puede apreciar que el administrador del satélite se empieza poco a poco a ver claramente, aunque la imagen sigue estando pixelada. En el lado izquierdo se ve difuminada a causa del movimiento y a que todavía era necesario asignar un mayor ancho de banda a la videollamada.

Participante	Nombre del canal	Paquetes perdidos	Perdida paquetes %
Local	Audio Tx	349	22
Local	People Tx	1854	52
1002	Audio Rx	694	18
1002	People Rx	2141	51

Tabla 3 Pérdida de paquetes en Villacarlos

- Local Audio Tx, en la *Tabla 3* se puede observar cómo se pierde un 22%
- Local People Tx en la *Tabla 3* se puede observar que se pierde un 52%
- 1002 Audio Rx en la *Tabla 3* se puede observar que se pierde el 18%
- 1002 People en la *Tabla 3* se puede observar que se pierde el 51%

Analizando los datos, se observa que la cantidad de información que se pierde por el audio es la misma que con 64Kbps, en video se puede señalar un pequeño empeoramiento, perdiendo un 52% de los paquetes que transmite el SOTM. En cambio, hay una notable mejoría a la hora de la recepción de paquetes de audio con un 4% menos y un 11% menos en video que en la prueba anterior.

Con los resultados obtenidos, se reconfiguró la ASA con una QoS diferente en Trepucó con los siguientes parámetros:

- 128 Kbps para video llamada
- 64 Kbps para llamadas IP
- 64 Kbps para señalización (para establecer enlace)

Con dicha configuración se empezó a notar claramente la mejora de calidad en la videollamada debido a que la distribución del ancho de banda se estaba distribuyendo exclusivamente para este servicio. La telefonía IP seguía funcionando correctamente.

Ilustración 19 Prueba de video llamada a 128 Kbps

En dicho fotograma se puede apreciar que el administrador del satélite se empieza a ver claramente y en general toda la imagen tiene una buena calidad.

Participante	Nombre del canal	Paquetes perdidos	Perdida paquetes %
Local	Audio Tx	48	24
Local	People Tx	32	31
1002	Audio Rx	34	25
1002	People Rx	18	23

Tabla 4 Pérdida de paquetes en Trepucó

- Local Audio Tx en la *Tabla 4* se puede observar cómo se pierde un 24%
- Local People en la *Tabla 4* se puede observar que se pierde un 31%
- 1002 Audio Rx en la *Tabla 4* se puede observar que se pierde el 25%
- 1002 People Tx en la *Tabla 4* se puede observar que se pierde el 23%

Analizando los datos, se observa que la perdida de paquetes es mucho más equilibrada. Aunque los valores de voz tienen pequeñas subidas tanto en transmisión como recepción, se puede observar como la pérdida de paquetes en video baja drásticamente en ambos casos.

Con los resultados obtenidos, se reconfiguró la ASA con una QoS diferente en la rotonda de la carretera Me-1 con los siguientes parámetros:

- 192 Kbps para video llamada
- 64 Kbps para señalización (para establecer enlace)

Con dicha configuración se buscó tener la mejor calidad posible en una videollamada que un SOTM puede ofrecer con 256 Kbps y se consiguió.

Ilustración 20 Prueba de video llamada a 192 Kbps

En la ilustración anterior se ve la excelente calidad de la imagen, pudiendo apreciar todos los detalles posibles. La telefonía IP dejó de funcionar ya que el ancho de banda asignado era cero.

Participante	Nombre del canal	Paquetes perdidos	Perdida paquetes %
Local	Audio Tx	201	28
Local	People Tx	0	0
1002	Audio Rx	195	18
1002	People Rx	195	28

Tabla 5 Pérdida de paquetes en Rotonda carretera Me-1

- Local Audio Tx en la *Tabla 5* se puede observar cómo se pierde un 28%
- Local People en la *Tabla 5* se puede observar que se pierde un 0%
- 1002 Audio Rx en la *Tabla 5* se puede observar que se pierde el 18%
- 1002 People Tx en la *Tabla 5* se puede observar que se pierde el 28%

Analizando los datos, llama la atención el 0% de paquetes que se pierde por parte de video transmitido del SOTM, de ahí la calidad del fotograma. Los demás porcentajes varían levemente, sin éxito de que bajaran más de lo ya alcanzado.

5. Conclusión

A lo largo del proyecto se ha realizado el estudio correspondiente de las capacidades y ventajas que proporciona la implementación de QoS en las redes tácticas del ejército. La implementación de estos mecanismos es imprescindible para resolver los graves problemas relacionados con la gestión del ancho de banda en las redes IP que surgen durante los ejercicios tácticos militares. En estos ejercicios, el ancho de banda disponible es muy reducido, con "cuellos de botella" que pueden provocar perdida de información o retardos elevados. Teniendo en cuenta que tanto la información sensible a retardos y pérdidas como la que no lo es comparten el mismo ancho de banda, es necesario realizar una correcta gestión de los recursos con mecanismos de QoS que prioricen la información a transmitir y reserven recursos para los distintos servicios de la red. Sin estos mecanismos, no es viable ofrecer servicios como videoconferencia o telefonía IP en redes tácticas.

De entre las posibles alternativas tecnológicas para implementar QoS, se ha elegido el modelo DiffServ al ser el que mejor escala en una red y ser su configuración más sencilla. Además, se ha decidido implementar en los equipos de red el mecanismo de gestión de colas LLQ, ya que es el que mejor asegura que el tráfico de elevada prioridad se transmita de modo preferente. Con esta configuración, se han realizado distintos análisis durante el ejercicio Trident Jackal 2019, donde hubo un despliegue internacional con un flujo constante de información que permitió su realización. En concreto, se determinó el ancho de banda mínimo necesario que es necesario reservar para el correcto funcionamiento de una videoconferencia, consiguiendo una red táctica robusta y totalmente operativa para la transmisión de distintos servicios.

La realización de esta práctica, así como el estudio de los distintos manuales de equipos, permite también concluir la importancia de la formación del personal para que tengan conocimiento sobre los mecanismos de QoS, debido a que hay numerosos métodos y protocolos que se pueden aplicar según las circunstancias y capacidades del ejercicio.

5.1. Líneas futuras de trabajo

Todo el trabajo expuesto asume que la red sobre la que se transmite el tráfico es cableada. Sin embargo, en la actualidad, se está tendiendo a las redes inalámbricas como WiFi. La implementación de QoS en redes de este tipo se definió en el estándar 802.11e[4], el cual incluyen mecanismos específicos de priorización del tráfico, prevención de colisiones de paquetes y minimización de las latencias para mejorar el rendimiento en las aplicaciones de vídeo y voz.

En una red inalámbrica, los usuarios finales acceden a un punto de acceso inalámbrico, el cual se conecta mediante de modo cableado al Wireless LAN Controller y este a su vez a un switch. De cara a implementar QoS en una red de este tipo, es necesario analizar los distintos mecanismos que se pueden aplicar a cada uno de estos dispositivos, así como la configuración conjunta que se ha de aplicar para que funcionen correctamente.

No obstante, hay que tener en cuenta que actualmente OTAN no acepta ningún tipo de red inalámbrica ya que no cumple con los estándares de seguridad impuestos. Por ello, antes de implementar mecanismos de QoS en redes inalámbricas, sería necesario esperar a que se definieran las guías de seguridad por parte del centro criptológico nacional para el uso de estos dispositivos para que se pudieran emplear en un entorno OTAN.

4 IEE 80.2.11e-2005 define un conjunto de mejoras de calidad de servicio (QoS) para aplicaciones LAN inalámbricas a través de modificaciones en la capa de control de acceso a medios (MAC) [20][21]

6. Bibliografía

[1] "Plan MC3 Ejército de Tierra."

[2] "Calidad de Servicio (QoS)." [Online]. Available: http://www.auben.net/index.php/tecnologias/calidad-de-servicio-qos. [Accessed: 17-Sep-2019].

[3] Alexis Pinos, "Curse of QoS." Marines, Valencia, 2014.

[4] C. Introducción, C. De Servicio, and I. Qos, "Capítulo 1. Introducción a la Calidad de Servicio (QOS) 1.1.," pp. 1–153.

[5] "Ancho de banda: definición y detalles." [Online]. Available: https://www.es.paessler.com/it-explained/bandwidth. [Accessed: 14-Sep-2019].

[6] "Latencia - Wikipedia, la enciclopedia libre." [Online]. Available: https://es.wikipedia.org/wiki/Latencia. [Accessed: 14-Sep-2019].

[7] D. Derickson and M. Muller, *Digital communications test and measurement : high-speed physical layer characterization*. Prentice Hall, 2008.

[8] *Hoja de datos de osciladores HO-22 y HO-25´*. .

[9] J. J. Herranz, "Estudio de la variación de QoE en Televisión IP cuando varían los parámetros de QoS," *2014*. 2014.

[10] R. Transmisiones, "INSTRUCCIÓN TÉCNICA 04 / 11 QoS : CALIDAD DE SERVICIO," 2011.

[11] M. Betegón García, "Estudio de técnicas de Ingeniería de Tráfico basadas en SDN," 2018.

[12] "Configuración y manejo de calidad de servicio en enrutadores Cisco Configuración de calidad de servicio (QoS) en enrutadores Cisco."

[13] "Solucionado: duda sobre policy map shape average - Cisco Community." [Online]. Available: https://community.cisco.com/t5/discusiones-seguridad/duda-sobre-policy-map-shape-average/td-p/3098074. [Accessed: 19-Sep-2019].

[14] "Q&A with the founder of Wireshark and Ethereal," *Interview with Gerald Combs*.

[15] eWEEK Labs and eWEEK Labs, "Wireshark," *Most Important Open-Source Apps All Time*, 2012.

[16] "Adaptive Server Anywhere - Wikipedia, la enciclopedia libre." [Online]. Available: https://es.wikipedia.org/wiki/Adaptive_Server_Anywhere. [Accessed: 20-Sep-2019].

[17] "Manipulación de los bits de TOS." [Online]. Available: http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/x-087-2-firewall.tos.manipulation.html. [Accessed: 18-Sep-2019].

[18] "Differentiated Services Code Point - Wikipedia, la enciclopedia libre." [Online]. Available: https://es.wikipedia.org/wiki/Differentiated_Services_Code_Point. [Accessed: 18-Sep-2019].

[19] "IEEE 802.1Q - Wikipedia, la enciclopedia libre." [Online]. Available: https://es.wikipedia.org/wiki/IEEE_802.1Q. [Accessed: 18-Sep-2019].

[20] "IEEE 802.1p - Wikipedia, la enciclopedia libre." [Online]. Available: https://es.wikipedia.org/wiki/IEEE_802.1p. [Accessed: 15-Oct-2019].

[21] "Tucny." [Online]. Available: https://www.tucny.com/Home/dscp-tos. [Accessed: 15-Oct-2019].

[22] "Cabecera IP - Wikipedia, la enciclopedia libre." [Online]. Available: https://es.wikipedia.org/wiki/Cabecera_IP. [Accessed: 23-Oct-2019].

Anexos

ANEXO A. Planificación del proyecto

En este anexo se puede observar la planificación del proyecto realizada con la herramienta Project Libre. A continuación, se presenta en la *Tabla 6* la estructura que se ha seguido para la consecución del trabajo.

		Nombre	Duracion	Inicio	Terminado	Predecesores
1		1. Project Kick-off	4 days	20/07/19 8:00	25/07/19 17:00	
2		Generar agenda de trabajo	4 days	20/07/19 8:00	25/07/19 17:00	
3		2. Búsqueda de información	19 days	25/07/19 8:00	20/08/19 17:00	
4		Estudio de la situación actual	4 days	26/07/19 8:00	31/07/19 17:00	2
5		Estudio de QoS	1 day	20/08/19 17:00	21/08/19 17:00	3
6		Consulta tutor militar	1 day	18/08/19 8:00	19/08/19 17:00	4
7		Reunión en el RT-21 con lo...	2 days	19/08/19 8:00	20/08/19 17:00	4
8		3. Generar estructura de t...	30 days	21/08/19 8:00	1/10/19 17:00	1
9		Propuesta indice del proye...	3 days	21/08/19 8:00	23/08/19 17:00	6
10		Propuesta ideas principale...	0 days	21/08/19 8:00	21/08/19 8:00	6
11		Propuesta TFG	25 days	2/10/19 8:00	5/11/19 17:00	8;9
12		4. Recopilación de datos p...	1 day	3/09/19 8:00	3/09/19 17:00	10
13		Análisis conceptos previos	1 day	5/11/19 17:00	6/11/19 17:00	11
14		Ejercicio en un entorno co...	2 days	5/09/19 8:00	6/09/19 17:00	12
15		Recopilación de datos y le...	1 day	6/11/19 17:00	7/11/19 17:00	13
16		Ejercicio en una maniobra...	1 day	15/09/19 8:00	16/09/19 17:00	14
17		Recopilación de datos y le...	1 day	7/11/19 17:00	8/11/19 17:00	15
18		Análisis comparativo de a...	3 days	28/09/19 8:00	2/10/19 17:00	16
19		5. Redacción de la memoria	46 days	21/08/19 8:00	23/10/19 17:00	3
20		Redacción introducción	1 day	21/08/19 8:00	21/08/19 17:00	3;4;6
21		Redacción desarrollo	10 days	3/10/19 8:00	16/10/19 17:00	12
22		Redacción conclusiones	4 days	11/11/19 8:00	14/11/19 17:00	17
23		Corrección de errores y fo...	3 days	19/10/19 8:00	23/10/19 17:00	21
24		6. Finalización del proyecto	1 day	15/11/19 8:00	15/11/19 17:00	22
25		Entrega del proyecto	1 day	15/11/19 8:00	15/11/19 17:00	22

Tabla 6 Planificación del proyecto

A continuación, en la ilustración 23 se muestra el diagrama de Gantt donde se representan los datos de la tabla anterior.

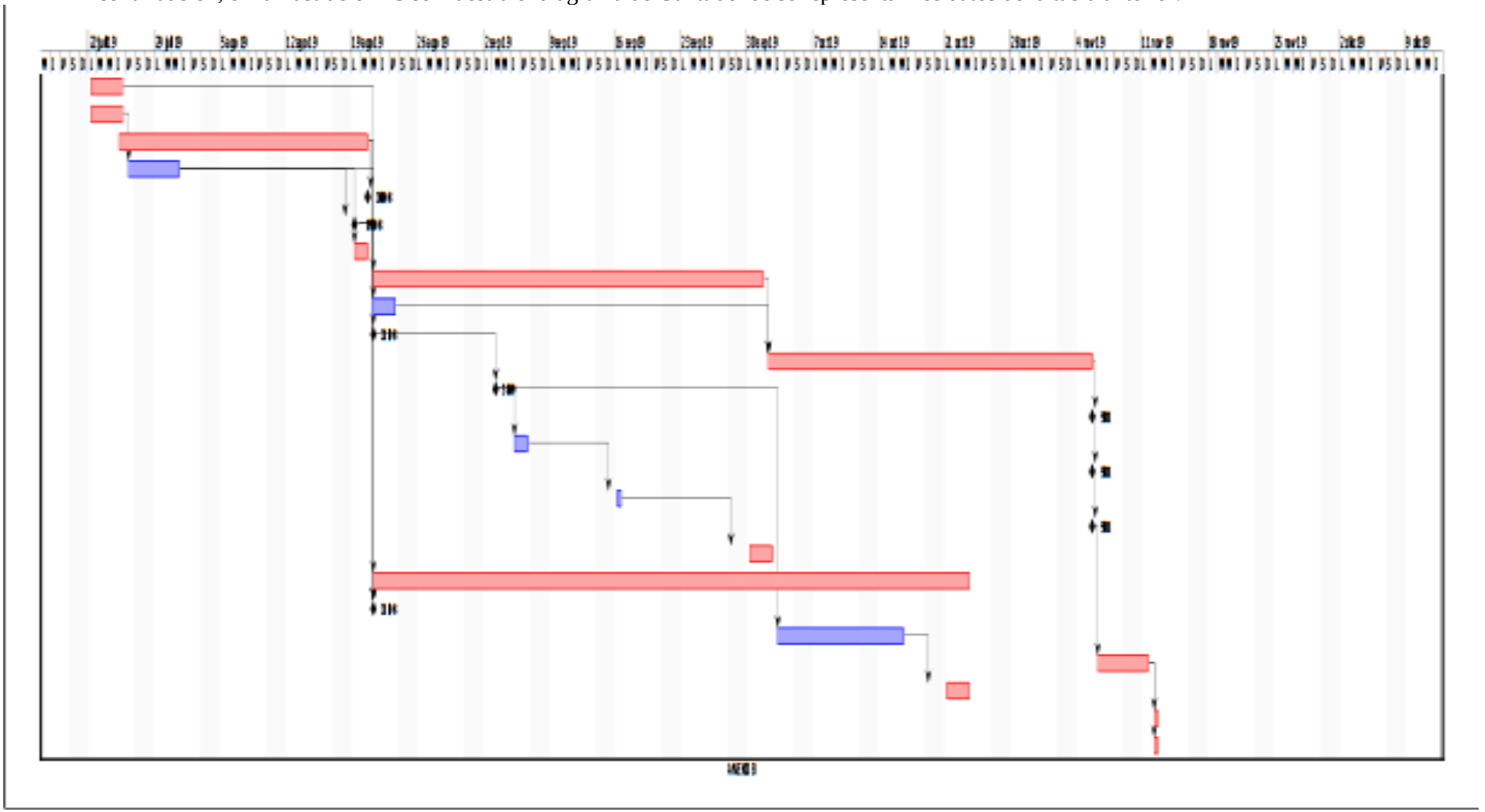

Ilustración 21 Diagrama de Gantt donde se muestra la planificación del proyecto por días

ANEXO B. Entrevista al Cap. D. Sergi Heras Lapeña

A continuación, se expone la entrevista realizada al Cap. D. Sergi Heras Lapeña, destinado en el Regimiento de Transmisiones Nº21, en funciones de jefe de la 12 compañía.

Esta entrevista ha sido realizada a este individuo para conocer su opinión en base a su experiencia sobre QoS.

1º Pregunta: ¿Qué es la calidad de servicio?

1º Respuesta: La calidad de servicio (comúnmente denominada por sus siglas en ingles QoS) es una tecnología que permite en una red priorizar un tipo de tráfico frente a otro (el ejemplo habitual es la priorización del servicio de videoconferencia sobre los servicios de datos ya que es preferible que un correo electrónico tarde 2 segundos más en llegar que se vea degradada la calidad de la videoconferencia.

2º Pregunta: ¿Por qué es importante la calidad de servicio en el ejército?

2º Respuesta: El principal motivo de la aplicación de la calidad de servicio es la limitación de ancho de banda actual en los sistemas militares, concretamente en los enlaces satélite (2-6MB). En grandes puestos de mandos como pueda ser un puesto de mando de entidad cuerpo de ejército o división la aplicación de calidad de servicio es fundamental ya que existe un elevado volumen de tráfico. De hecho, en la arquitectura FMN de OTAN (red federada de misión), que es una estandarización de procedimientos y configuraciones CIS para garantizar la interoperabilidad de los sistemas de los diferentes países miembros de la alianza se especifica y estandariza la calidad de servicio a emplear.

3º Pregunta: ¿En qué se basa la calidad de servicio?

3º Respuesta: La calidad de servicio se basa principalmente en 2 operaciones:
- Marcado y categorización: Para diferenciar un tipo de trafico de otro (videoconferencia, correo, web, etc...) lo primero es necesario categorizarlo, para ello los dispositivos de red con la correcta configuración son capaces de marcar o rellenar unos bits que existen en las cabeceras IP con una numeración especifica que podrá ser utilizada por diferentes dispositivos de red para realizar una priorización. Esto sería como si hubiese una etiquetadora que va marcando por ejemplo los paquetes de voz y video con un código, los de correo con otro, etc.
- Lógica de proceso: Aquí viene la cuestión de fondo, una vez identificado el paquete mediante una etiqueta hay que aplicar una lógica de proceso a los mismos de tal forma que por ejemplo se podría reservar un determinado ancho de banda para los paquetes de videoconferencia en caso de congestión en detrimento de otro servicio.

ANEXO C. Marcado de paquetes en el modelo DiffServ

El modelo DiffServ se basa en marcar paquetes IP mediante un código llamado DSCP (Differentiated Services Code Point) que corresponde a los 6 primeros bits del campo TOS (Type of Service) de la cabecera IP [22]. A continuación se muestra tanto la cabecera IP (ilustración X) como los bits que se emplean del campo TOS para codificar el código DSCP (tabla X).

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

Tabla 7 Formato de la cabecera IP [22]

7	6	5	4	3	2	1	0
DSCP							(0)

Tabla 8 Campo Tipo de Servicio en la cabecera IP (marcado DSCP)

Los routers y switches de la red pueden leer este código DSCP y priorizar el tráfico según su valor mediante técnicas de encolado del tráfico. Este código lo fijan los switches y routers de acceso a la red para clasificar el tráfico de entrada a la red en función de su prioridad. Además, el resto de switches y routers pueden cambiar el código DSCP entrante por otro distinto, alterando el tratamiento de un determinado tipo de tráfico en la red [17],[18].

Los códigos DSCP permiten clasificar el tráfico en 8 clases que van del CS0 al CS7. Algunos CS, denominados *Assured Forwarding* (AF), se subdividen también en varias subclases según su prioridad. A continuación, se mostrará una tabla en la que se muestra esta clasificación:

Tipo de tráfico	**DSCP**	**Comportamiento**	**Prioridad**
Bulk data	CS1	AF11, AF12, AF13	Priority
Networking Data Base	CS2	AF21, AF22, AF23	Immediate
Local Mission Critical	CS3	AF31, AF32, AF33	Flash
Video	CS4	AF41, AF42, AF43	Flash overdrive
Interactive voice	CS5	EF	Critical
Routing	CS6		InternetWork Control
Network Control	CS7		Network Control

Tabla 9 Clasificación del tráfico en el modelo DIffServ

En la tabla anterior, la clase EF (Expedited Forwarding) se utiliza para el servicio de baja latencia y la clase Assured Forwarding (AF) se utiliza para los servicios que necesitan garantizar el ancho de banda. A los CS de tipo AF se les puede definir tres tipos de prioridades de descartes, a modo de ejemplo:

CS1	AF11	Probabilidad de descarte bajo
	AF12	Probabilidad de descarte medio
	AF13	Probabilidad de descarte alto

Tabla 10 Prioridades de descartes del CS1

La siguiente tabla muestra los valores decimales, hexadecimales y binarios para las clases DSCP anteriores [21].

TOS (diciembre)	TOS (Hex)	TOS (Bin)	Precedencia de TOS (Bin)	Precedencia de TOS (diciembre)	Nombre de precedencia de TOS	TOS Delay flag	Indicador de rendimiento de TOS	Bandera de fiabilidad de TOS	DSCP (Bin)	DSCP (Hex)	DSCP (diciembre)	Clase DSCP / PHB
0	0x00	00000000	000	0	Routine	0	0	0	000000	0x00	0	none
4	0x04	00000100	000	0	Routine	0	0	1	000001	0x01	1	none
8	0x08	00001000	000	0	Routine	0	1	0	000010	0x02	2	none
12	0x0C	00001100	000	0	Routine	0	1	1	000011	0x03	3	none
16	0x10	00010000	000	0	Routine	1	0	0	000100	0x04	4	none
32	0x20	00100000	001	1	Priority	0	0	0	001000	0x08	8	cs1
40	0x28	00101000	001	1	Priority	0	1	0	001010	0x0A	10	af11
48	0x30	00110000	001	1	Priority	1	0	0	001100	0x0C	12	af12
56	0x38	00111000	001	1	Priority	1	1	0	001110	0x0E	14	af13
64	0x40	01000000	010	2	Immediate	0	0	0	010000	0x10	16	cs2
72	0x48	01001000	010	2	Immediate	0	1	0	010010	0x12	18	af21
80	0x50	01010000	010	2	Immediate	1	0	0	010100	0x14	20	af22
88	0x58	01011000	010	2	Immediate	1	1	0	010110	0x16	22	af23
96	0x60	01100000	011	3	Flash	0	0	0	011000	0x18	24	cs3
104	0x68	01101000	011	3	Flash	0	1	0	011010	0x1A	26	af31
112	0x70	01110000	011	3	Flash	1	0	0	011100	0x1C	28	af32
120	0x78	01111000	011	3	Flash	1	1	0	011110	0x1E	30	af33
128	0x80	10000000	100	4	FlashOverride	0	0	0	100000	0x20	32	cs4
136	0x88	10001000	100	4	FlashOverride	0	1	0	100010	0x22	34	af41

Tabla 11 Tabla TOS [22]

En la práctica realizada en el entorno controlado se decide escoger el valor 40, con dicho valor se obtiene la clase AF11 que es prioritaria. Este valor fue escogido previendo que los paquetes de la videollamada deberían ser prioritarios sobre los demás.

Finalmente se muestra el marcado por precedence, el cual se empleaba con anterioridad a DiffServ. En este caso, solo utilizan tres bits de la cabecera TOS de IP.

7	6	5	4	3	2	1	0
Precedence			Type os Service			No usados (0)	

Tabla 12 Campo Tipo de Servicio en la cabecera IP (marcado precedence)

ANEXO D. IEE 802.1p

A diferencia del Anexo C que se refiere al marcado de paquetes en la capa de red, este anexo explica el marcado de paquetes en la capa de enlace. En esta capa se definen 8 clases diferentes de servicios, expresados por medio de 3 bits del campo prioridad de usuario (user_priority) de la cabecera IEEE 802.1Q[5] añadida a la trama, asignando a cada paquete un nivel de prioridad entre 0 y 7. No está definida la manera de cómo tratar el tráfico que tiene asignada una determinada clase o prioridad, dejando libertad a las implementaciones. IEEE, sin embargo, ha hecho amplias recomendaciones al respecto [19], [20].

.

Tipo	Prioridad	Tipo de tráfico
1	0 (baja)	Background
0	1 (por defecto)	Best Effort
2	2	Excellent Effort
3	3	Critical Applications
4	4	Video, < 100 ms latencia y fluctuación
5	5	Voz, < 10 ms latencia y fluctuación
6	6	Internetwork Control
7	7 (más alta)	Network Control

Tabla 13 Valores protocolo IEE 802.1p

En la práctica realizada en el entorno controlado, se marca el valor 4 (video) previendo el ejercicio realizado sobre el terreno que consistía en una videollamada.

5 IEEE 802.1Q es un protocolo que permite desarrollar un mecanismo que hace posible que múltiples redes compartan de forma transparente el mismo medio físico, sin problemas de interferencias entre ellas [19].

ANEXO E. Red táctica Trident Jackal 2019

En la ilustración 25 se observa cómo sería una red táctica de gran unidad en un ejercicio militar OTAN. Dicha estructura corresponde al ejercicio realizado este año en Menorca (Trident Jackal 2019) en el cual participó una gran cantidad de países y se establecieron enlaces tanto nacionales como internacionales. El Puesto de Mando de Cuerpo de Ejército localizado en Menorca contaba con dos Pentatramas, uno en constante funcionamiento y otro de reserva que permitían establecer todas las comunicaciones. El Puesto de Mando localizado en Stavanger contaba con un ATQH (At The Quick Halt) para establecer los enlaces, al igual que en el Puesto de Mando localizado en Bétera. El Puesto de Mando Móvil localizado en un SOTM en Menorca cuenta con su propio satélite para establecer las comunicaciones.

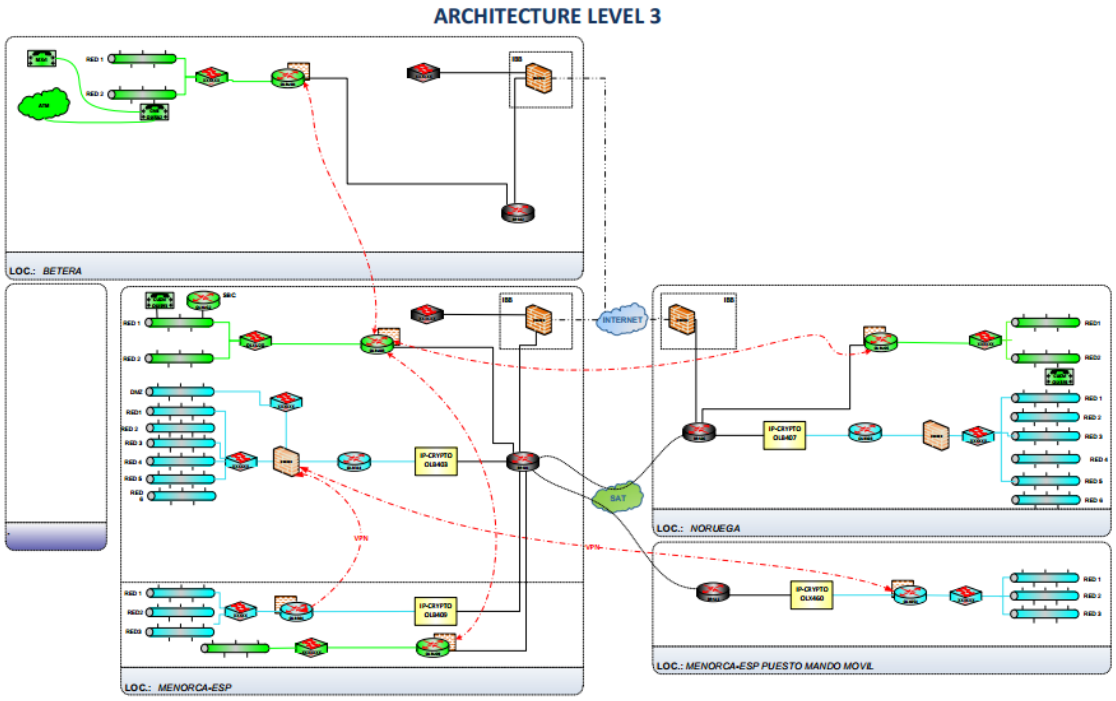

Ilustración 22 Esquema de red Trident Jackal 2019

En el modelo de servicios diferenciados hay diferentes distinciones entre los dos tipos de routers: internos (rojos) y de frontera (negros). La nomenclatura de rojos o negros depende de si la información está cifrada o no. En el caso de los routers rojos o internos, la información todavía no ha pasado por el cifrador y los datos que contienen son transparentes para el administrador.

En cambio, en los router negros o frontera, los datos han sido cifrados previamente, provocando que los datos sean invisibles para cualquier usuario. Los mecanismos de gestión de la congestión se aplican en los routers negros, ya que son los que tienen un enlace de ancho de banda reducido y por tanto son los que necesitan priorizar el tráfico en función de su clase. Este tipo de sistema se utiliza dentro de las Fuerzas Armadas, en el ámbito civil es más civil encontrar cifradores entre routers.

Como se puede observar en la ilustración toda la información que se transmite entre los diferentes puestos de mando está cifrada dos veces. La primera vez mediante el cifrador localizado entre los routers rojo y negro y la segunda vez mediante los satélites, que tienen de serie un cifrador siempre, es decir, el cifrador del satélite se encarga de cifrar lo cifrado haciendo todavía más segura la transmisión de información entre dos puntos.