UNIVERSITAT POLITÈCNICA DE VALÈNCIA

_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería de Telecomunicación

Configuración de servicios con QoS en redes IP

Trabajo Fin de Grado

Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación

AUTOR/A: Valero Muñoz, Pablo

Tutor/a: Sempere Paya, Víctor Miguel

CURSO ACADÉMICO: 2022/2023

Agradecimientos

Previamente a la introducción del proyecto, me gustaría dedicar unas palabras de agradecimiento a todas las personas que han hecho posible la realización del mismo.

En primer lugar, me gustaría agradecer a mi tutor Víctor Sempere por ayudarme en todo lo que he necesitado y darme ánimo durante la totalidad del proyecto.

Además, quiero agradecer a José Cano por su ayuda respecto a los conocimientos sobre cisco, y sus consejos y correcciones.

También quiero agradecer a mi familia, que me ha proporcionado un constante apoyo a la hora de realizar este proyecto, y me ha formado como persona.

Por último pero no menos importante, quiero agradecer a los profesores que he tenido a lo largo de la vida y a la universidad, por formarme y proporcionarme todos los recursos necesarios para realizar este proyecto.

Resumen

El objetivo de este proyecto es estudiar y analizar mecanismos de calidad de servicio (QoS) en entornos LAN. Este análisis será utilizado para realizar tres prácticas en la asignatura “Redes Públicas de Acceso”, perteneciente al grado “Grado en Ingeniería de Tecnología y Servicios de Telecomunicación”.

Para cumplir con este objetivo, se han analizado diversas herramientas de calidad de servicio que se pueden encontrar en el switch de cisco 2950 y en el router de cisco 1921. En concreto, se van a analizar las herramientas de calidad de servicio tales como los planificadores de cola disponibles y las funciones policía. En concreto, se han estudiado los planificadores de cola: Priority Queue, Weighted Round Robin, Priority Queue junto a Weighted Round Robin y Class based Weighted Fair Queueing.

Además, para estudiar estas herramientas de calidad de servicio en dispositivos reales se han planteado una serie de diseños de red topológica buscando la minimización de los dispositivos para realizar el estudio de interés, y se ha introducido a programas capaces de generar y capturar tráfico que pueden resultar muy útiles a la hora de estudiar dichos efectos, como son los programas “Iperf3” y “Wireshark”.

Resum

L'objectiu d'aquest projecte és estudiar i analitzar mecanismes de qualitat de servei (QoS) en entorns LAN. Aquesta anàlisi serà utilitzada per a realitzar tres pràctiques en l'assignatura “Xarxes Públiques d'Accés”, pertanyent al grau “Grau en Enginyeria de Tecnologia i Serveis de Telecomunicació”.

Per a complir amb aquest objectiu, s'han analitzat diverses eines de qualitat de servei que es poden trobar en el switch de cisco 2950 i en el router de cisco 1921. En concret, s'analitzaran les eines de qualitat de servei com ara els planificadors de cua disponibles i les funcions policia. En concret, s'han estudiat els planificadors de cua: Priority Queue, Weighted Round Robin, Priority Queue amb Weighted Round Robin i Class based Weighted Fair Queueing.

A més, per a estudiar aquestes eines de qualitat de servei en dispositius reals s'han plantejat una sèrie de dissenys de xarxa topològica buscant la minimització dels dispositius per a realitzar l'estudi d'interés, i s'ha introduït a programes capaços de generar i capturar trànsit que poden resultar molt útils a l'hora d'estudiar aquests efectes, com són els programes “Iperf3” i “Wireshark”.

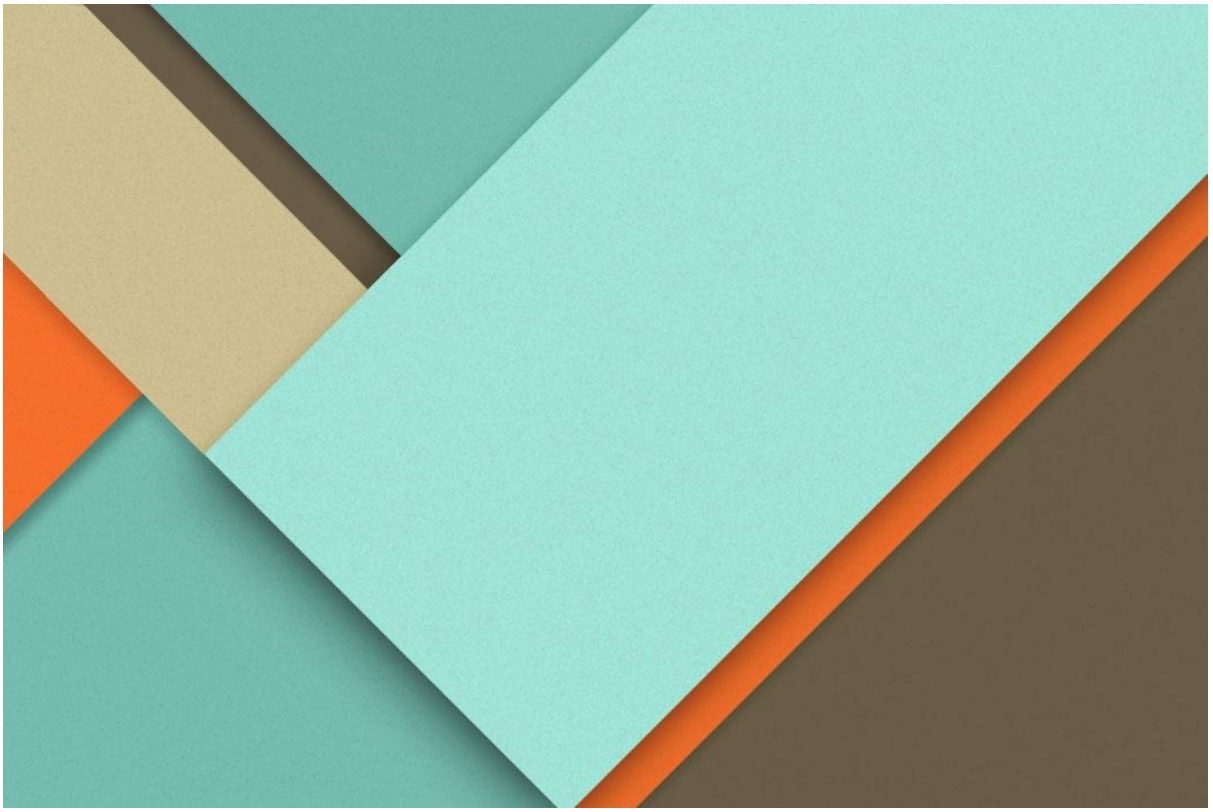
Abstract

The objective of the thesis is studying and analyzing quality of service (QoS) tools mechanisms in LAN environments. Moreover, this analysis will be used to carry out three practices in the subject "Public Access Networks", belonging to the degree "Degree in Telecommunication Technology and Services Engineering".

To meet this objective, various quality of service tools that can be found in the cisco 2950 switch and the cisco 1921 router have been analyzed. Specifically, quality of service tools such as schedulers as well as police functions will be analyzed. Definitely, queue schedulers have been studied: Priority Queue, Weighted Round Robin, Priority Queue together with Weighted Round Robin and Class based Weighted Fair Queuing.

In addition, to study these quality of service tools in real devices, a series of topological network designs have been proposed seeking to minimize the devices to carry out the study of interest, and this thesis has also introduced programs capable of generating and capturing traffic that can be very useful when studying these quality of service tools, such as the programs "Iperf3" and "Wireshark".

Índice



Capítulo 1. Introducción

Capítulo 1. Introducción:

La calidad de servicio o QoS es un mecanismo que permite priorizar distintos tipos de tráfico dentro de una red topológica, con el objetivo de cumplir con unas especificaciones que dependen del tipo de tráfico y la necesidad de la priorización del mismo.

Actualmente, es muy **importante el uso de herramientas de calidad de servicio** debido a que **los recursos** de los que disponemos **son limitados, y se ha de priorizar el tráfico en función de la importancia del mismo**. Cabe destacar que en ese caso, el resto del **tráfico menos prioritario es penalizado.**

A la hora de configurar las herramientas de calidad de servicio, se ha de realizar un **análisis de los distintos flujos que pueden ser transmitidos y su importancia.** A la hora de analizar la importancia de los flujos **se ha de tener en cuenta la necesidad de la correcta transmisión del flujo, y en qué medida es afectado por los distintos parámetros de calidad de servicio:**

- **Tasa de pérdidas:** corresponde a la tasa de paquetes recibidos correctamente respecto a la totalidad de los paquetes que han sido enviados. El valor máximo de la tasa es la unidad, que corresponde a que todos los paquetes enviados han sido recibidos correctamente.
- **Jitter:** diferencia de tiempo entre la recepción de dos paquetes consecutivos.
- **Latencia:** tiempo que tarda un paquete desde que es transmitido en un punto de la red topológica, hasta que es recibido en otro punto de la misma.
- **Throughput:** corresponde con la velocidad a la que un canal transmite datos, en bits por segundo (bps). Es importante conocer cuál es el máximo throughput que puede alcanzar nuestra red topológica.

El **objetivo principal** de este proyecto es **realizar un estudio y analizar mecanismos de calidad de servicio (QoS) en entornos de red de área local (LAN)**, que son redes que interconectan dispositivos (PCs, routers, switches…) a nivel local porque abarcan normalmente poca distancia. Este estudio será **utilizado para la realización de tres prácticas de asignatura para la asignatura "Redes Públicas de Acceso"**, perteneciente al grado "Grado en Ingeniería de Tecnología y Servicios de Telecomunicación", de forma que los **resultados** de las mismas sean **eficaz y eficientemente reproducibles**. Cabe destacar que debido al uso de herramientas software que no se utilizan en el grado, **se ha realizado una introducción a los mismos así como al montaje de redes topológicas, que servirá para realizar una práctica de introducción.**

De esta forma, **los capítulos 2, 3 y 4** de este documento **presentan la información necesaria para realizar las tres prácticas de asignatura.** Cabe destacar que a lo largo de estos capítulos, se han realizado una serie de ejercicios resueltos cuyo objetivo es considerar los conceptos teóricos que se imparten en la asignatura, en el entorno práctico.

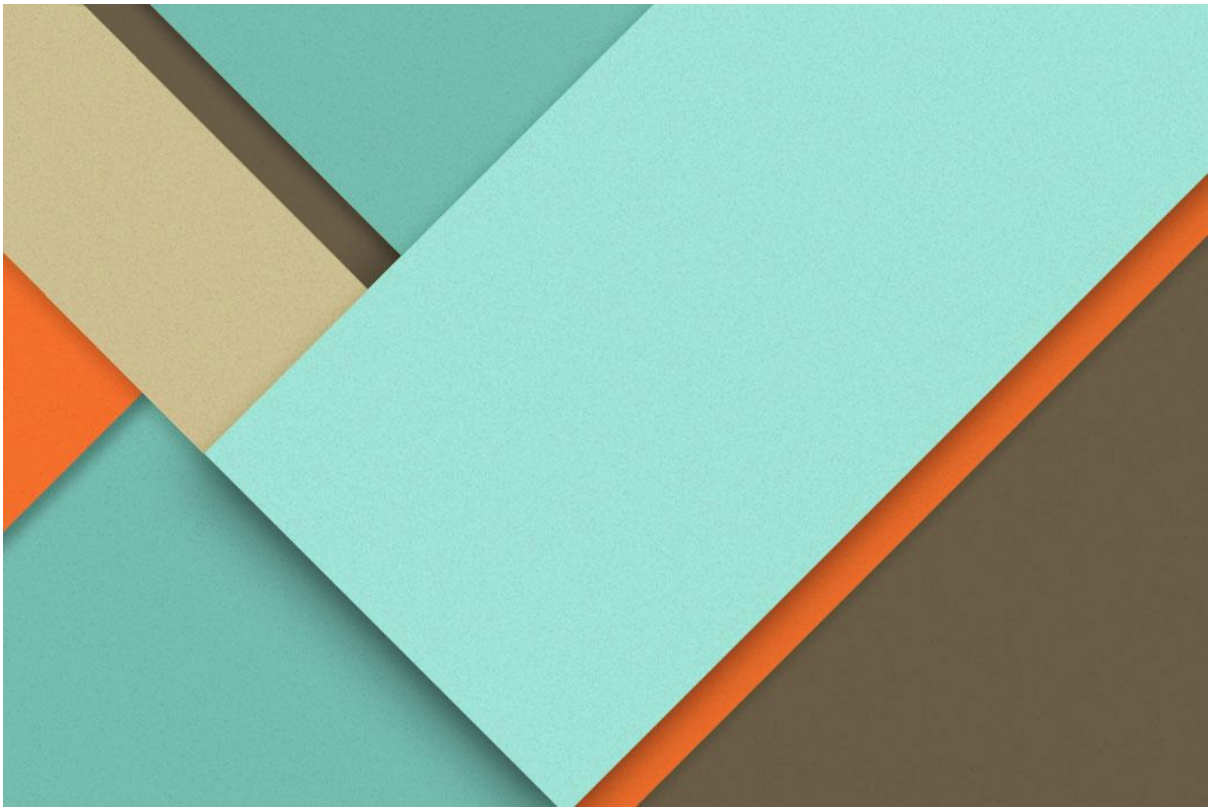
En los capítulos 2, 3 y 4 se han estudiado los siguientes conceptos:

- El capítulo 2 presenta una introducción a los programas Iperf3 y Wireshark, y al montaje de topologías de red.

- El capítulo 3 presenta el uso de las herramientas de calidad de servicio correspondientes con los planificadores de cola en dispositivos CISCO, la clasificación y el marcado a nivel 2 y 3. En concreto, se han estudiado los planificadores de cola: Priority Queue, Weighted Round Robin, Priority Queue junto a Weighted Round Robin y Class based Weighted Fair Queueing.

- El capítulo 4 presenta el uso de las herramientas de calidad de servicio correspondientes con las funciones policía y el marcado DSCP en Routers Cisco.

Finalmente, el capítulo 5 muestra la conclusión del proyecto, así como las posibilidades de expansión que presenta para un futuro proyecto.



Capítulo 2: Introducción a los Programas Utilizados y al Montaje de Topologías de Red

Capítulo 2. Introducción a los programas utilizados y al montaje de topologías de red:

El **objetivo** de este capítulo es la familiarización con el **montaje de topologías de red**, así como de los programas **Iperf 3** y **Wireshark**. Además, a lo largo de este capítulo se observará visualmente la **diferencia entre una red congestionada y una red que no está congestionada**.

Se puede decir que **una red está congestionada cuando dicha red no puede procesar el tráfico generado que debe atravesar la misma, en por lo menos una parte de la topología de red. Esto produce un retraso en la entrega de paquetes e incluso puede hacer que se produzcan pérdidas** en los paquetes enviados.

La congestión puede producirse debido a distintas causas, pero en este proyecto **se va a producir porque la velocidad de un enlace no es suficiente para servir todos los paquetes que le llegan**.

Por ejemplo, si tres ordenadores generan tráfico a una tasa de 10 Mbps con el mismo destino, y todo el tráfico ha de pasar por un enlace en concreto, el sistema no se congestionaría en el caso de que dicho enlace sea igual o superior a 30 Mbps. Sin embargo, si el enlace por el que pasa todo el tráfico funcionara a una velocidad inferior a 30 Mbps el sistema se congestionaría.

Para conseguir que se cumpla el objetivo del primer capítulo se ha planteado un escenario sencillo.

El escenario consiste en el montaje de una topología de red que conecta cuatro PCs mediante el switch de cisco 2950. De esta forma, se han realizado una serie de ejercicios para la familiarización con los programas Iperf 3 y Wireshark.

Tras el montaje de la topología de red, se debe de comprobar la correcta conectividad de los equipos.

2.1 Programa Iperf 3:

Es un programa capaz de **generar tráfico y de comprobar el ancho de banda disponible** entre los distintos elementos que forman la topología de la red en la que se utiliza. Para conseguir este objetivo, **utiliza un modelo de arquitectura cliente servidor** mediante el cual un **cliente se conecta con un servidor y genera tráfico UDP o TCP entre ambos.**

Finalmente, cliente y servidor intercambian mensajes para averiguar el tamaño del **tráfico total que ha sido enviado y recibido**, así como el **ancho de banda** en el caso de que se estén enviando paquetes **TCP**. Para tráfico **UDP** se intercambian mensajes para obtener el **ancho de banda transmitido**, el **tamaño del tráfico total que ha sido enviado**, el **jitter**, el **número de paquetes enviados** y la **tasa de pérdidas.**

2.1 Programa Iperf 3:

Cabe destacar que las instancias cliente y servidor se comunican a nivel IP (capa 3), pero en el primer escenario se utiliza un switch, que funciona a nivel de la capa de enlace (capa 2). Sin embargo, esto no supone ningún problema porque el paquete IP (capa 3) se encapsula en un frame Ethernet (capa 2) que contiene la dirección MAC origen y la dirección MAC destino, para que el switch sea capaz de enviar el frame Ethernet al PC destino correspondiente. Recuerde que a través del protocolo ARP, se averigua la dirección MAC relacionada a una dirección IP.

Para no tener que añadir el iperf3.exe al path simplemente se debe de indicar la ruta de dicho archivo en el CMD. Para ello, **se han seguido los siguientes pasos:**

Paso 1: Buscar "CMD" en el buscador de Windows y hacer click en la aplicación "Símbolo del sistema".
Paso 2: En el cmd, escribir "cd " y pegar la ruta donde se encuentra dicho archivo como se puede apreciar en la figura 1:

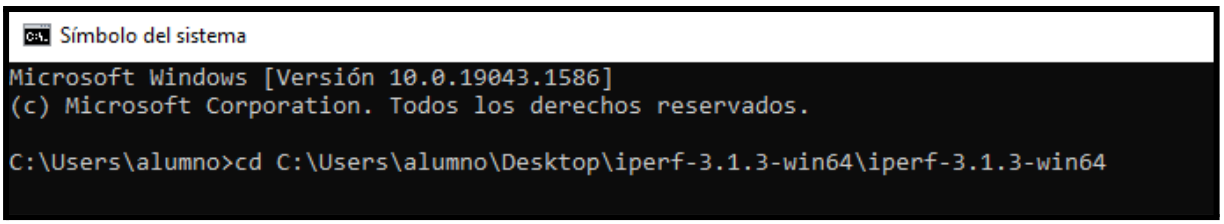


Figura 1. Forma de cambiar la carpeta en el CMD.

Paso 3: Finalmente, el comando "iperf3.exe" debe de mostrar un mensaje de error, y posteriormente todas los comandos posibles a utilizar, en caso de estar en la carpeta correcta. Esto se puede observar en la figura 2:

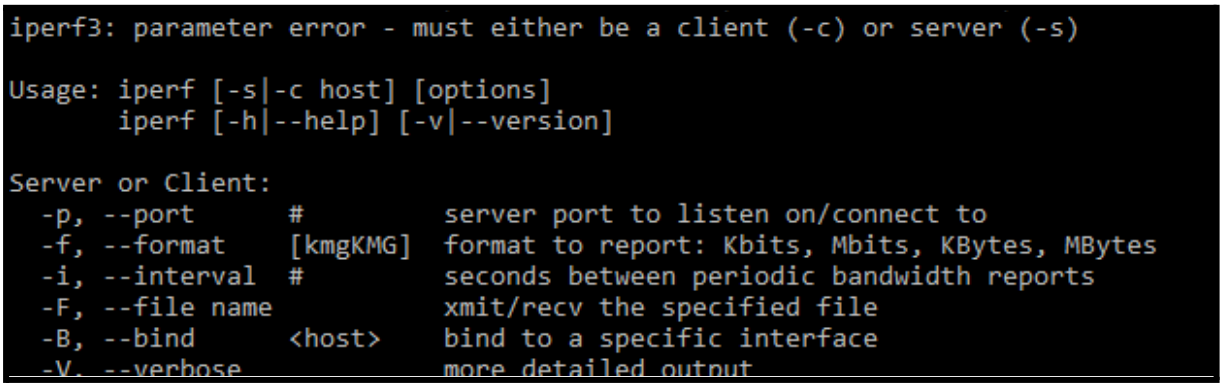


Figura 2. resultado de utilizar ffmpeg.exe.

2.1.2 Generación de paquetes mediante Iperf 3:cd

En este proyecto se va a utilizar el programa **iperf 3 para generar y recibir tráfico UDP**.

2.1 Programa Iperf 3:

1. Para abrir una instancia de servidor se utilizan las siguientes opciones:

-s : Indica que se trata de una instancia servidor
-p : Especifica el puerto que se utilizará para la comunicación entre cliente y servidor.

Ejemplo: Se ha de abrir una instancia servidor en un PC con una dirección IP 10.0.0.4/24 y se va a abrir el puerto 5201 para la conexión.

En el cmd, se debe de escribir el comando:

```
iperf3.exe -s -p 5201
```

Si se desea que el servidor deje de escuchar simplemente hay que pulsar las teclas "Ctrl" y "c" simultáneamente.

2. Para abrir una instancia cliente, se deberán utilizar las siguientes opciones:

-c : Indica la dirección IP del servidor.
-u : Para la generación de tráfico UDP.
-t : Tiempo en segundos de la simulación. Un tiempo de "0" indica que se generan paquetes de forma ilimitada, en este caso se debe de pulsar las teclas "Ctrl" y "c" para finalizar la simulación.
-l : Longitud del tamaño de paquete en bytes. Este tamaño sólo tiene en cuenta el tamaño del payload del paquete
-b : Tasa de envío de paquetes en bits/segundos. Se pueden especificar las unidades añadiendo la letra adecuada al lado del número. Ejemplo: "-b 4M" equivale a 4 Mbps.
-p : Especifica el puerto que se utilizará para la comunicación entre cliente y servidor.

Ejemplo: **Se ha de abrir una instancia cliente que se deba conectar con el servidor anterior. El tráfico generado ha de ser UDP, la tasa de envío de paquetes ha de ser de 100 kbps utilizando un tamaño de paquete de 300 bytes durante una duración de 30 s.**

En otro CMD, se debe de utilizar el comando:

```
iperf3.exe -c 10.0.0.4 -p 5201 -b 100k -l 300 -t 30 -u.
```

En cualquier momento se puede finalizar la generación de paquetes pulsando las teclas "Ctrl" y "c" simultáneamente.

Resultados de la generación de paquetes (figura 3):

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-30.01  sec   366 KBytes  99.8 Kbits/sec  0.054 ms  0/1247 (0%)
[  4] Sent 1247 datagrams

iperf Done.
```

Figura 3. Resultado obtenido mediante Iperf 3.

Como se puede observar en la figura 3, cuando el cliente termina de generar paquetes nos muestra el total de bytes que se han transmitido, el ancho de banda medio, el jitter y la tasa de pérdidas. Como se puede apreciar, el ancho de banda no es exactamente el indicado (100 kbps), pero es un valor muy cercano a este.

2.2 Programa Wireshark:

El programa **wireshark** es utilizado en este proyecto para **capturar el tráfico recibido por PC_4**. Es importante destacar que Wireshark **no captura** los bytes preámbulo + delimitador de comienzo de trama (**8 Bytes**) ni el CRC (**4 Bytes**) **de la cabecera Ethernet**. **Por lo tanto, una cantidad muy alta de paquetes transmitidos puede hacer que disminuya el ancho de banda total que se observa en wireshark.**

Para poder observar el tráfico transmitido desde los distintos PCs se han seguido los siguientes pasos:

Paso 1. En PC4, seleccionar la interfaz "Ethernet" que se puede apreciar en la figura 4, por la que llega el tráfico y pulsar el botón de iniciar captura  . Tras su selección, se empezará a capturar todo el tráfico.

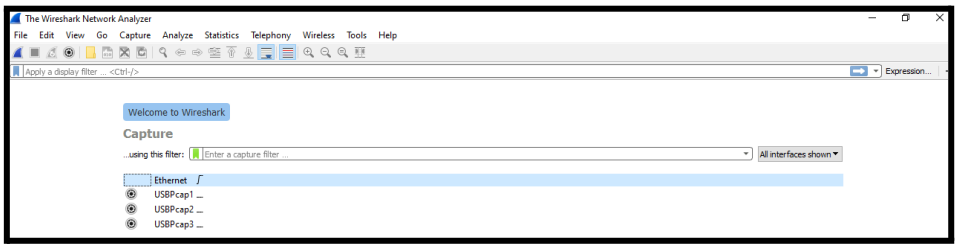


Figura 4. Interfaz inicial de Wireshark.

Paso 2. Parar la captura con el botón de stop  .

Paso 3. En el menú "Estadísticas" hacer clic en la opción "Gráficas de E/S".

Paso 4. Pulsar el icono "+" para crear un nuevo filtro, que se puede apreciar en la figura 5.

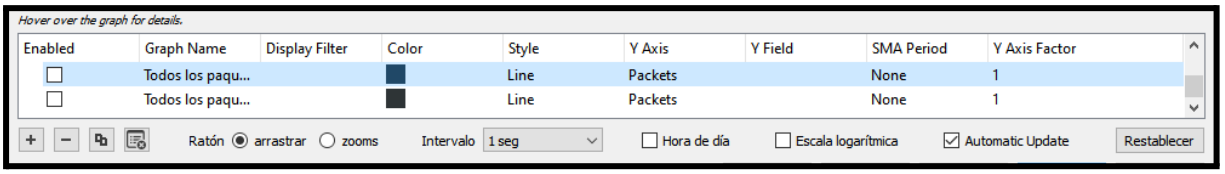


Figura 5. Gráficas E/S.

Paso 5. En la columna de filtro, se debe de indicar "UDP". En la columna de Y Axis se debe indicar la opción de bits/segundo. Finalmente, en la columna SMA Period se le ha de asignar un valor de "100 interval SMA" o superior, para que se haga un promediado y el tráfico recibido sea constante.

Paso 6. Añadir otro filtro al que se le debe de indicar "ip.src == 10.0.0.1 && UDP". En la columna de Y Axis se debe indicar la opción de bits/segundo. Finalmente, en la columna SMA Period se le ha de asignar un valor de "100 interval SMA" o superior.

Paso 7. Repetir el paso 6 para las direcciones IP 10.0.0.2 y 10.0.0.3.

La configuración queda como en la figura 6:

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Fiel	SMA Period
☑	All packets	udp		Line	Bits		100 interval SMA
☑	All packets	ip.src == 10.0.0.2&& udp		Line	Bits		100 interval SMA
☑	All packets	ip.src == 10.0.0.3&& udp		Line	Bits		100 interval SMA
☑	All packets	ip.src == 10.0.0.1&& udp		Line	Bits		100 interval SMA

Figura 6. Filtros de captura de paquetes

2.3 Topología y elementos a utilizar.

El escenario consiste en el montaje de una topología de red que conecta cuatro PCs mediante el switch de cisco 2950. Además, se han elegido una serie de ejercicios para familiarizarse con los programas Iperf 3 y Wireshark.

La red topológica a montar, se muestra en la figura 7.

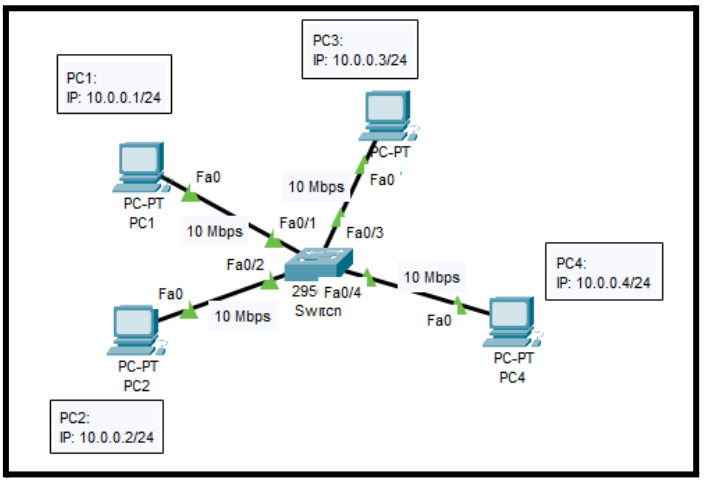


Figura 7. Topología de red.

Los enlaces pertenecientes a las interfaces cuyo rango es Fa0/1-4 deben ser configurados para que trabajen a una **velocidad de 10 Mbps, con el objetivo de que se necesite una menor cantidad de tráfico para congestionar la red.**

Características de los equipos:

- PC_1:
  Software necesario: IPerf3 (generador de tráfico).
- PC_2:
  Software necesario: IPerf3 (generador de tráfico).
- PC_3:
  Software necesario: IPerf3 (generador de tráfico).
- PC_4:
  Software necesario: IPerf3 (generador de tráfico).
  Wireshark (analizador de protocolos).

La configuración de los equipos es la mostrada en la tabla 1:

Equipo.	Interfaz	Dirección IP.	Máscara
PC1	NIC	10.0.0.1	255.255.255.0
PC2	NIC	10.0.0.2	255.255.255.0
PC3	NIC	10.0.0.3	255.255.255.0
PC4	NIC	10.0.0.4	255.255.255.0

Tabla 1. Configuración de los equipos.

En el apartado “Anexo A” se encuentra la forma de configurar la dirección IP de un ordenador.

2.4 Montaje y configuración básica del switch:

El montaje consiste en conectar los PCs con el switch mediante cables de red directos (ethernet). Para mayor claridad, se ha conectado la **interfaz ethernet del PC_x** con la **interfaz fastethernet 0/x del switch**, donde x es el número asignado a cada PC. Además, para realizar la configuración del switch conectamos el **puerto de consola del switch con el puerto COM1 de uno de los cuatro PCs**.

2.4 Montaje y configuración básica del switch:

El montaje queda de la misma forma que se observa en la figura 8.

Figura 8. Montaje de la topología de red.

Una vez se ha realizado el montaje, es necesario hacer **ping entre los distintos PCs** para comprobar la correcta conectividad. Si el ping no funciona, puede ser que el firewall no esté apagado. Para apagar el firewall, se han seguido los pasos indicados por el apartado "Anexo B".

Para la configuración inicial del switch se va a utilizar el programa **putty**. Para comunicarnos con el switch, se ha seleccionado la **opción "serial"** y pulsado **"Open" desde el PC al que ha sido conectado el puerto de consola**, como se puede apreciar en la figura 9.

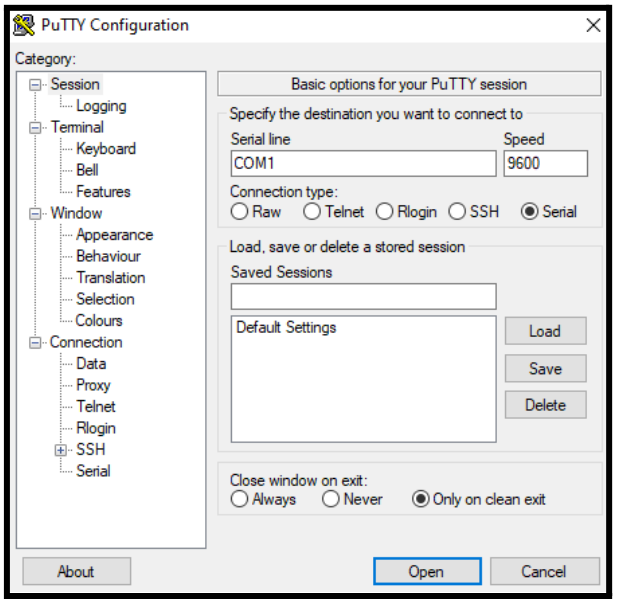


Figura 9. Programa Putty

Una vez se ha accedido a la configuración del switch, se han seguido los siguientes pasos para la configuración inicial del mismo:

Paso 1. Responder "no" ante la siguiente pregunta:

would you like to enter the initial configuration dialog? [yes/no]:

2.4 Montaje y configuración básica del switch:

Paso 2. Entrar en modo privilegiado

```
Switch>enable
```

Paso 3. Borrar la configuración inicial del switch:

```
Switch# erase startup-config
```

Paso 4. Reiniciar el switch:

```
Switch# reload
```

Paso 5. Responder con "no", y pulsar "Enter".

```
System configuration has been modified. Save? [yes/no]
```

Paso 6. Cuando aparezca la siguiente pregunta, se ha de pulsar "Enter".

```
Proceed with reload? [confirm]
```

Paso 7. Cuando aparezca la siguiente pregunta se volverá a responder "no" y a presionar "Enter".

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

Paso 8. Finalmente, se ha de pulsar "Enter" ante la última pregunta:

```
Would you like to terminate autoinstall? [yes]:
```

Paso 9. Entrar en modo de configuración global:

```
Switch# configure terminal
Switch (config)#
```

Paso 10. configurar la velocidad a 10 Mbps en las interfaces fast ethernet:

```
Switch (config)# interface fast ethernet 0/1
Switch (config-if)# speed 10
```

Paso 11. Repetir el paso 10, para las cuatro interfaces a utilizar

Para comprobar la configuración de las interfaces, se ha utilizado el siguiente comando en modo privilegiado:

```
Switch# show run
```

2.5 Ejercicios realizados:

El resultado de utilizar el comando muestra la configuración que presenta la figura 10.

```
interface FastEthernet0/1
 speed 10
!
interface FastEthernet0/2
 speed 10
!
interface FastEthernet0/3
 speed 10
!
interface FastEthernet0/4
 speed 10
!
```

Figura 10. Comando show run.

Nota: Para salir de un modo de configuración a un modo previo se utiliza el comando "exit".

2.4 Ejercicios realizados:

Ejercicio 1: Genere tráfico desde PC_1 con destino PC_4.
Para ello, es necesario que desde PC_4 se abra una instancia servidor utilizando el puerto 5201.

¿Cuál es el tiempo de simulación en segundos, el tamaño medio de paquete en bytes, el número de paquetes generado por segundo en media, y el tiempo entre paquetes en media, por defecto de acuerdo al resultado obtenido?

El flujo a emitir es el indicado en la tabla 2:

Flujo	Protocolo	IP origen	IP destino	Puerto
Best Effort	UDP	10.0.0.1/24	10.0.0.4/24	5201

Tabla 2. Características del flujo a emitir en el primer ejercicio.

Para utilizar el programa abierto, es necesario tener un terminal abierto en la carpeta donde se encuentra el archivo: "Iperf3.exe". Para ello, se han seguido los dos pasos indicados en el apartado 1.2.

Solución:

Desde PC_4 se utiliza el siguiente comando para abrir la instancia servidor:

```
iperf3.exe -s -p 5201
```

2.5 Ejercicios realizados:

Desde PC_1 se utiliza el siguiente comando para generar el flujo indicado:

```
iperf3.exe -c 10.0.0.4 -u -p 5201
```

Para resolver estos ejercicios se ha hecho uso de las siguientes fórmulas:

$$\bar{L}_{paq}(bytes/paquete) = \frac{Tam_{tot}(bytes)}{N_{ptot}(paquetes)} \quad (1)$$

$$\bar{N}_{pasg}(paquetes/s) = \frac{N_{ptot}(paquetes)}{t_{tot}(s)} \quad (2)$$

$$\bar{t}_{paq}(s) = \frac{1(paquete)}{Npasg\ (paquetes/s)} \quad (3)$$

Donde:

$\bar{L}_{paq}$ (bytes/paquete) es el tamaño medio por paquete, en bytes.
Tam_{tot} (bytes) es el tamaño total de tráfico generado, en bytes.
N_{ptot} (Paquetes) es el número total generado de paquetes.
$\bar{N}_{pasg}$ (Paquetes/s) es el número de paquetes generados por segundo, en media.
t_{tot} (s) es el tiempo total de simulación.
$\bar{t}_{paq}$ (s) es el tiempo entre paquetes en media.

```
C:\Users\alumno\Desktop\iperf-3.1.3-win64>iperf3.exe -c 10.0.0.4 -p 5201 -u
Connecting to host 10.0.0.4, port 5201
[  4] local 10.0.0.1 port 62945 connected to 10.0.0.4 port 5201
[ ID] Interval           Transfer     Bandwidth       Total Datagrams
[  4]   0.00-1.01   sec   128 KBytes  1.04 Mbits/sec  16
[  4]   1.01-2.02   sec   136 KBytes  1.11 Mbits/sec  17
[  4]   2.02-3.00   sec   120 KBytes   993 Kbits/sec  15
[  4]   3.00-4.00   sec   128 KBytes  1.05 Mbits/sec  16
[  4]   4.00-5.01   sec   128 KBytes  1.04 Mbits/sec  16
[  4]   5.01-6.01   sec   128 KBytes  1.05 Mbits/sec  16
[  4]   6.01-7.01   sec   128 KBytes  1.05 Mbits/sec  16
[  4]   7.01-8.01   sec   128 KBytes  1.05 Mbits/sec  16
[  4]   8.01-9.01   sec   128 KBytes  1.05 Mbits/sec  16
[  4]   9.01-10.01  sec   128 KBytes  1.05 Mbits/sec  16
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-10.01  sec  1.25 MBytes  1.05 Mbits/sec  4.733 ms  0/159 (0%)
[  4] Sent 159 datagrams

iperf Done.
```

Figura 11. Resultados obtenidos mediante Iperf3 en el primer ejercicio.

Mediante el resultado obtenido con Iperf 3 (figura 11) observamos que el tiempo de simulación por defecto es de 10 segundos aproximadamente. Además, se puede observar que el ancho de banda medio es de 1.05 Mbps y que se han transferido 159 paquetes y un total de 1,25 MBytes.

2.5 Ejercicios realizados:

El tamaño de paquete por defecto se puede calcular de la siguiente forma:

A partir de (1) obtenemos que el tamaño medio por paquete es de:

$$\bar{L}_{paq}\ (\text{bytes/paquete}) = \frac{1{,}25 * 10^{6}}{159} = 7861{,}64\ \text{bytes/paquete}$$

A partir de (2) obtenemos que el número de paquetes generados en media por segundo es de:

$$\bar{N}_{pasg} = \frac{159}{10} = 15{,}9\ \text{paquetes/s.}$$

A partir de (3) obtenemos que el tiempo entre paquetes en media es de:

$$\bar{t}_{paq} = \frac{1}{15{,}9} = 62{,}9\ \text{ms}$$

2.5 Ejercicios realizados:

Ejercicio 2: Genere el siguiente flujo desde PC_1 a PC_4 con el siguiente comando:

```
iperf3.exe -c 10.0.0.4 -u -p 5201 -b 2M
```

¿Qué diferencias se pueden apreciar tras el uso del comando -b 2M? ¿Cuál es el tiempo entre paquetes de acuerdo al resultado obtenido en este caso? ¿Coincide con el obtenido por defecto en el ejercicio 1? ¿Y el tamaño de paquete? Justifique su respuesta:

El flujo a emitir es el indicado en la tabla 3:

Flujo	Protocolo	IP origen	IP destino	Puerto	Bitrate (Mbps)
Best Effort	UDP	10.0.0.1/24	10.0.0.4/24	5201	2

Tabla 3. Características del flujo a emitir en el segundo ejercicio.

Solución:

```
C:\Users\alumno\Desktop\iperf-3.1.3-win64>iperf3.exe -c 10.0.0.4 -u -p 5201 -b 2M
Connecting to host 10.0.0.4, port 5201
[  4] local 10.0.0.1 port 59966 connected to 10.0.0.4 port 5201
[ ID] Interval           Transfer     Bandwidth       Total Datagrams
[  4]   0.00-1.01   sec   232 KBytes  1.88 Mbits/sec  29
[  4]   1.01-2.01   sec   272 KBytes  2.22 Mbits/sec  34
[  4]   2.01-3.01   sec   216 KBytes  1.79 Mbits/sec  27
[  4]   3.01-4.01   sec   256 KBytes  2.09 Mbits/sec  32
[  4]   4.01-5.01   sec   232 KBytes  1.90 Mbits/sec  29
[  4]   5.01-6.01   sec   256 KBytes  2.10 Mbits/sec  32
[  4]   6.01-7.01   sec   232 KBytes  1.90 Mbits/sec  29
[  4]   7.01-8.00   sec   248 KBytes  2.05 Mbits/sec  31
[  4]   8.00-9.00   sec   240 KBytes  1.97 Mbits/sec  30
[  4]   9.00-10.01  sec   248 KBytes  2.02 Mbits/sec  31
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-10.01  sec  2.38 MBytes  1.99 Mbits/sec  8.702 ms  0/303 (0%)
[  4] Sent 303 datagrams

iperf Done.
```

Figura 12. Resultados obtenidos mediante Iperf3 en el segundo ejercicio.

Como se puede observar en la figura 12, el bitrate ha variado aproximadamente al bitrate especificado (2 Mbps). Esto ha hecho que varíe el tiempo de generación entre paquetes, la cantidad de bytes generados y el número de paquetes generados.

En este caso, como el bitrate especificado es mayor que en el ejercicio anterior, el tiempo entre generación de paquetes ha disminuido, generando de esta forma un número mayor de paquetes y un total de bytes transmitidos superior.

A partir de (2) y (3) obtenemos que el tiempo de generación entre paquetes en este caso es de:
10/303 = 33 ms, que es menor al obtenido en el primer ejercicio (62,9 ms).

2.5 Ejercicios realizados:

Ejercicio 3: Genere el siguiente flujo desde PC_1 a PC_4 con el siguiente comando:

```
iperf3.exe -c 10.0.0.4 -u -p 5201 -b 2M -l 1250
```

¿Qué diferencias se pueden apreciar tras el uso del comando -l 1250? ¿Cuál es el tiempo entre paquetes y el número de paquetes en media por segundo de acuerdo al resultado obtenido en este caso? ¿Coincide con lo esperado? Justifique su respuesta:

El flujo a emitir es el indicado en la tabla 4:

Flujo	Protocolo	IP origen	IP destino	Puerto	Bitrate (Mbps)	Tamaño de paquete (Bytes)
Best Effort	UDP	10.0.0.1/24	10.0.0.4/24	5201	2	1250

Tabla 4. Características del flujo a emitir en el tercer ejercicio.

Solución:

```
C:\Users\alumno\Desktop\iperf-3.1.3-win64>iperf3.exe -c 10.0.0.4 -u -p 5201 -b 2M -l 1250
Connecting to host 10.0.0.4, port 5201
[  4] local 10.0.0.1 port 64477 connected to 10.0.0.4 port 5201
[ ID] Interval           Transfer     Bandwidth       Total Datagrams
[  4]   0.00-1.00   sec   223 KBytes  1.83 Mbits/sec  183
[  4]   1.00-2.00   sec   248 KBytes  2.03 Mbits/sec  203
[  4]   2.00-3.00   sec   245 KBytes  2.01 Mbits/sec  201
[  4]   3.00-4.00   sec   245 KBytes  2.01 Mbits/sec  201
[  4]   4.00-5.01   sec   240 KBytes  1.96 Mbits/sec  197
[  4]   5.01-6.01   sec   244 KBytes  2.00 Mbits/sec  200
[  4]   6.01-7.01   sec   244 KBytes  2.00 Mbits/sec  200
[  4]   7.01-8.01   sec   243 KBytes  1.99 Mbits/sec  199
[  4]   8.01-9.00   sec   245 KBytes  2.02 Mbits/sec  201
[  4]   9.00-10.00  sec   244 KBytes  2.00 Mbits/sec  200
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-10.00  sec  2.37 MBytes  1.98 Mbits/sec  2.041 ms  0/1984 (0%)
[  4] Sent 1984 datagrams

iperf Done.
```

Figura 13. Resultados obtenidos mediante Iperf3 en el tercer ejercicio.

En la figura 13 se puede apreciar que principalmente varía el número de paquetes generados, incrementándose en gran medida respecto del ejercicio 2.

Esto se debe a que el tamaño de paquete es mucho menor en este caso: 1250 Bytes respecto de los aproximadamente 7861 Bytes que había en los dos ejercicios anteriores.

Conociendo que el tamaño de paquete es de 1250 Bytes y el bitrate es de 2 Mbps, se puede calcular el número de paquetes generados por segundo de forma ideal mediante la siguiente fórmula:

2.5 Ejercicios realizados:

$\bar{N}_{pasg}(paquetes/s) = \frac{Bitrate\ (bps)}{Lpaq\ (bits/paquetes)}$ (4).

A partir de (4) se obtiene: $\bar{N}_{pasg}(paquetes/s) = \frac{2*10^6}{1250*8} = 200\ paquetes/seg$.

Por lo tanto, a partir de (3) el tiempo de generación entre paquetes ideal es de 1 /200 = 5 ms.

Como se puede observar, el número de paquetes generados es de 1984 paquetes, a partir de (2) calculamos que equivale a una media de 198,4 paquetes/s. Finalmente, a partir de (3) calculamos que el tiempo de generación de paquetes de 1/198,4 (s) = 5,04 ms.

Por lo tanto, el resultado obtenido mediante Iperf 3 no es exactamente ideal, pero se parece considerablemente al ideal.

2.5 Ejercicios realizados:

Ejercicio 4: Genere el siguiente flujo desde PC_1 a PC_4 con el siguiente comando:

```
iperf3.exe -c 10.0.0.4 -u -p 5201 -b 2M -l 1250 -t 20
```

¿Qué diferencias se pueden apreciar tras el uso del comando -t 20?

El flujo a emitir es el indicado en la tabla 5:

Flujo	Protocolo	IP origen	IP destino	Puerto	Bitrate (Mbps)	Tamaño de paquete (Bytes)	Tiempo de generación del flujo (s)
Best Effort	UDP	10.0.0.1/24	10.0.0.4/24	5201	2	1250	20

Tabla 5. Características del flujo a emitir en el cuarto ejercicio.

Solución:

```
C:\Users\alumno\Desktop\iperf-3.1.3-win64>iperf3.exe -c 10.0.0.4 -u -p 5201 -b 2M -l 1250 -t 20
Connecting to host 10.0.0.4, port 5201
[  4] local 10.0.0.1 port 51366 connected to 10.0.0.4 port 5201
[ ID] Interval           Transfer     Bandwidth       Total Datagrams
[  4]   0.00-1.01   sec   225 KBytes  1.81 Mbits/sec  184
[  4]   1.01-2.01   sec   244 KBytes  2.01 Mbits/sec  200
[  4]   2.01-3.00   sec   242 KBytes  1.99 Mbits/sec  198
[  4]   3.00-4.00   sec   247 KBytes  2.01 Mbits/sec  202
[  4]   4.00-5.00   sec   260 KBytes  2.14 Mbits/sec  213
[  4]   5.00-6.00   sec   228 KBytes  1.87 Mbits/sec  187
[  4]   6.00-7.00   sec   244 KBytes  2.00 Mbits/sec  200
[  4]   7.00-8.00   sec   244 KBytes  1.99 Mbits/sec  200
[  4]   8.00-9.00   sec   244 KBytes  2.00 Mbits/sec  200
[  4]   9.00-10.00  sec   244 KBytes  2.00 Mbits/sec  200
[  4]  10.00-11.00  sec   244 KBytes  2.00 Mbits/sec  200
[  4]  11.00-12.00  sec   244 KBytes  2.00 Mbits/sec  200
[  4]  12.00-13.01  sec   242 KBytes  1.97 Mbits/sec  198
[  4]  13.01-14.00  sec   248 KBytes  2.04 Mbits/sec  203
[  4]  14.00-15.00  sec   243 KBytes  1.99 Mbits/sec  199
[  4]  15.00-16.01  sec   243 KBytes  1.98 Mbits/sec  199
[  4]  16.01-17.00  sec   255 KBytes  2.10 Mbits/sec  209
[  4]  17.00-18.00  sec   234 KBytes  1.92 Mbits/sec  192
[  4]  18.00-19.01  sec   265 KBytes  2.15 Mbits/sec  217
[  4]  19.01-20.00  sec   228 KBytes  1.89 Mbits/sec  187
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-20.00  sec  4.75 MBytes  1.99 Mbits/sec  1.868 ms  0/3987 (0%)
[  4] Sent 3987 datagrams

iperf Done.
```

Figura 14. Resultados obtenidos mediante Iperf3 en el cuarto ejercicio.

A partir de la figura 14, se puede apreciar que la duración de la generación de paquetes es de 20 s, como se ha especificado. Esto ha hecho que el total de Bytes y el número de paquetes transmitidos prácticamente se duplique. Pero, el bitrate, el tamaño de paquetes generados en media por segundo y el tiempo de generación entre paquetes se mantiene.

2.5 Ejercicios realizados:

Ejercicio 5: Genere los siguientes flujos especificados en la siguiente tabla.

Nota: es necesario tener abierto 3 instancias servidor en PC_4 utilizando los puertos: 5201, 5202 y 5203.

Además, se ha de capturar el resultado mediante Wireshark (revisar apartado 1.2).

¿Se produce congestión en el sistema?¿En el caso de que se produzca, a qué se debe?¿Cuál es la tasa de pérdidas obtenida para cada uno de los PCs mediante Iperf 3?
Apóyese en el resultado obtenido mediante Wireshark e Iperf 3 para razonar la respuesta.

Los flujos a emitir son los indicados en la tabla 6:

Flujo	Protocolo	IP origen	IP destino	Puerto	Bitrate (Mbps)	Tamaño de paquete (Bytes)	Tiempo de generación del flujo (s)
Best Effort	UDP	10.0.0.1/24	10.0.0.4/24	5201	2	1250	60
Best Effort	UDP	10.0.0.2/24	10.0.0.4/24	5202	2	1250	60
Best Effort	UDP	10.0.0.3/24	10.0.0.4/24	5203	2	1250	60

Tabla 6. Características de los flujos a emitir en el quinto ejercicio.

2.5 Ejercicios realizados:

Solución:

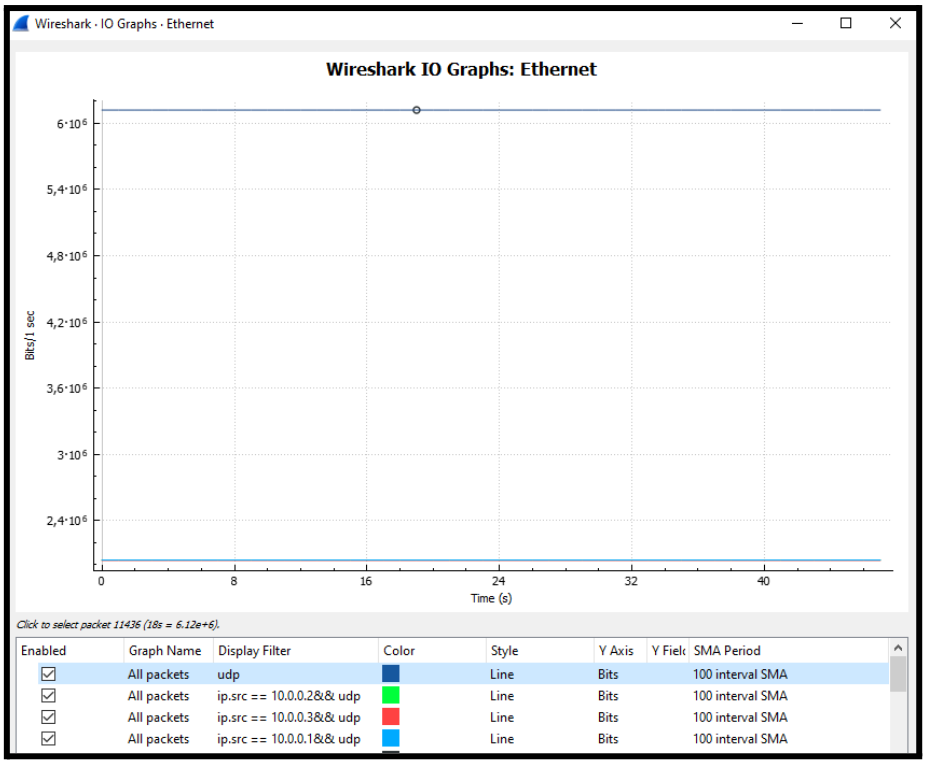


Figura 15. Resultados obtenidos mediante Wireshark en el quinto ejercicio.

En la captura obtenida mediante Wireshark (figura 15), observamos que el ancho de banda ha sido utilizado de la forma (tabla 7):

	Ancho de banda
PC_1	2,041 Mbps
PC_2	2,041 Mbps
PC_3	2,041 Mbps
Total	6,12 Mbps

Tabla 7. Utilización del ancho de banda del canal por cada PC.

Mediante el resultado obtenido, se puede apreciar que no hay congestión porque cada PC ha conseguido transmitir sin problemas todos los paquetes generados. Esto se debe a que el bitrate total de paquetes generados es de 6 Mbps, que es menor al ancho de banda del canal (10 Mbps). Por lo tanto, el Iperf 3 nos debe mostrar que no se han producido pérdidas.

2.5 Ejercicios realizados:

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-60.01  sec  14.3 MBytes  2.00 Mbits/sec  1.273 ms  0/11981 (0%)
[  4] Sent 11981 datagrams
```

Figura 16. Resultados obtenidos mediante Iperf 3 en el quinto ejercicio en PC_1.

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-60.00  sec  14.3 MBytes  2.00 Mbits/sec  2.965 ms  0/11984 (0%)
[  4] Sent 11984 datagrams
```

Figura 17. Resultados obtenidos mediante Iperf 3 en el quinto ejercicio en PC_2.

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-60.01  sec  14.3 MBytes  2.00 Mbits/sec  1.246 ms  0/11981 (0%)
[  4] Sent 11981 datagrams
```

Figura 18. Resultados obtenidos mediante Iperf 3 en el quinto ejercicio en PC_3.

Observando los resultados obtenidos mediante Iperf 3 (figuras 16, 17 y 18) confirmamos que no se han producido pérdidas.

Para resolver este ejercicio, se han utilizado los siguientes comandos desde el servidor:

```
iperf3.exe -s -p 5201
iperf3.exe -s -p 5202
iperf3.exe -s -p 5203
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_1:

```
iperf3.exe -c 10.0.0.4 -u -p 5201 -b 2M -l 1250 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_2:

```
iperf3.exe -c 10.0.0.4 -u -p 5202 -b 2M -l 1250 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_3:

```
iperf3.exe -c 10.0.0.4 -u -p 5203 -b 2M -l 1250 -t 60
```

2.5 Ejercicios realizados:

Ejercicio 6: Genere los siguientes flujos especificados en la siguiente tabla. Además, se ha de capturar el resultado mediante Wireshark.

Los flujos a emitir son los indicados en la tabla 8:

Flujo	Protocolo	IP origen	IP destino	Puerto	Bitrate (Mbps)	Tamaño de paquete (Bytes)	Tiempo de generación del flujo (s)
Best Effort	UDP	10.0.0.1/24	10.0.0.4/24	5201	6	1250	60
Best Effort	UDP	10.0.0.2/24	10.0.0.4/24	5202	6	1250	60
Best Effort	UDP	10.0.0.3/24	10.0.0.4/24	5203	6	1250	60

Tabla 8. Características de los flujos a emitir en el quinto ejercicio.

¿Se produce congestión en el sistema?¿En el caso de que se produzca, a qué se debe?¿Cuál es la tasa de pérdidas obtenida para cada uno de los PCs mediante Iperf 3? Apóyese en el resultado obtenido mediante Wireshark e Iperf 3 para razonar la respuesta.

Copie la gráfica obtenida mediante Wireshark a continuación :

Solución:

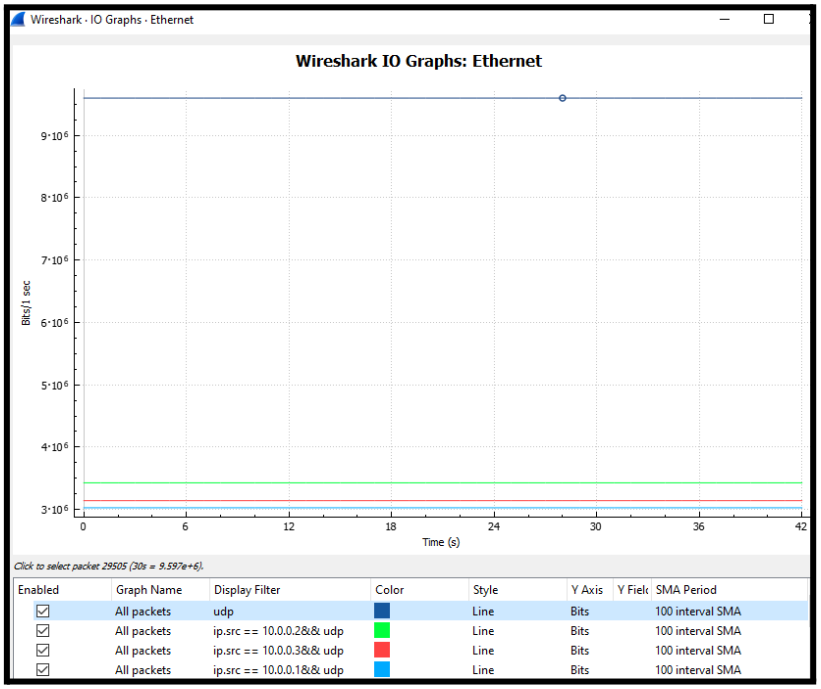


Figura 19. Resultados obtenidos mediante Wireshark en el quinto ejercicio.

2.5 Ejercicios realizados:

En la captura obtenida mediante Wireshark (figura 19), observamos que el ancho de banda ha sido utilizado de la siguiente forma (tabla 9):

	Ancho de banda
PC_1	3,027 Mbps
PC_2	3,427 Mbps
PC_3	3,141 Mbps
Total	9,597 Mbps

Tabla 9. Utilización del ancho de banda del canal por cada PC.

Mediante el resultado obtenido, se puede apreciar que en este caso se produce congestión porque el bitrate total generado es de 18 Mbps y los enlaces son de 10 Mbps. Por lo tanto, el enlace no es capaz de transmitir los paquetes a tiempo y se forma una cola que con el tiempo se llena y se produce una pérdida notable de paquetes.

Las siguientes figuras muestran los resultados obtenidos mediante Iperf 3:

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-60.00  sec  42.9 MBytes  6.00 Mbits/sec  2.136 ms  16550/35981 (46%)
[  4] Sent 35981 datagrams
```

Figura 20. Resultados obtenidos mediante Iperf 3 en el sexto ejercicio en PC_1.

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-60.00  sec  42.9 MBytes  6.00 Mbits/sec  2.682 ms  14486/35995 (40%)
[  4] Sent 35995 datagrams
```

Figura 21. Resultados obtenidos mediante Iperf 3 en el sexto ejercicio en PC_2.

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-60.00  sec  42.9 MBytes  5.99 Mbits/sec  1.255 ms  18303/35945 (51%)
[  4] Sent 35945 datagrams
```

Figura 22. Resultados obtenidos mediante Iperf 3 en el sexto ejercicio en PC_3.

Observando los resultados obtenidos mediante Iperf 3 (figuras 20, 21 y 22) confirmamos que se han producido bastantes pérdidas y por lo tanto, se produce congestión.

Para resolver este ejercicio, se han utilizado los siguientes comandos desde el servidor:

```
iperf3.exe -s -p 5201
iperf3.exe -s -p 5202
iperf3.exe -s -p 5203
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_1:

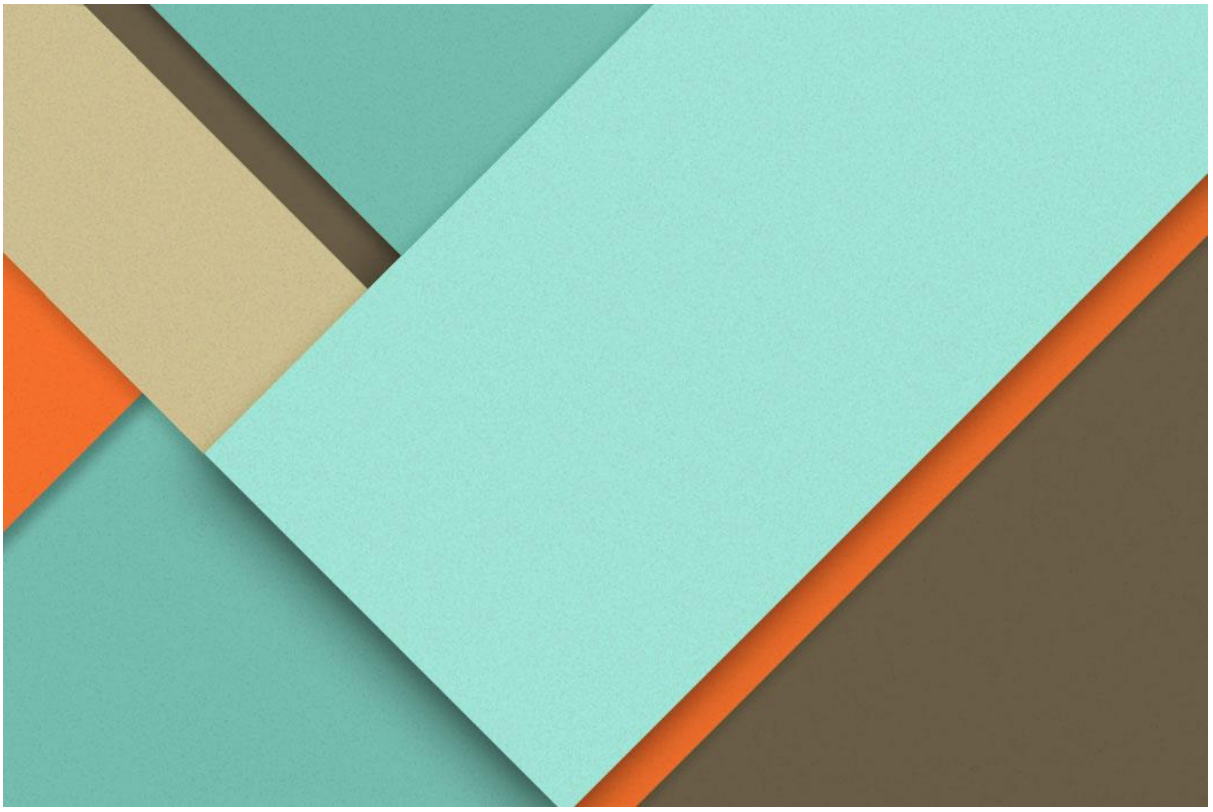
```
iperf3.exe -c 10.0.0.4 -u -p 5201 -b 6M -l 1250 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_2:

```
iperf3.exe -c 10.0.0.4 -u -p 5202 -b 6M -l 1250 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_3:

```
iperf3.exe -c 10.0.0.4 -u -p 5203 -b 6M -l 1250 -t 60
```



Capítulo 3: Planificadores de Cola en Dispositivos CISCO

Capítulo 3. Planificadores de cola en dispositivos CISCO.

El objetivo de este capítulo es poder observar el funcionamiento de los distintos planificadores de cola que poseen algunos dispositivos cisco. En concreto, los planificadores a utilizar son: **Priority Queue (PQ)**, **Weighted Round Robin (WRR)**, **Weighted Round Robin combinado con Priority Queue**, y **Class Based Weighted Fair Queueing (CBWFQ)**. Para apreciar la gestión que realizan los planificadores, se ha implementado en el laboratorio una red congestionada donde se ha podido observar los efectos que presentan en el tráfico al activarlos.

Mediante el **switch cisco catalyst 2950**, vamos a observar las propiedades de los planificadores **Priority Queue (PQ), Weighted Round Robin (WRR), y Weighted Round Robin combinado con Priority Queue.**

Para el caso del planificador **Class Based Weighted Fair Queueing (CBWFQ)**, se utilizará el router cisco 1921.

3.1 Herramientas de QoS a utilizar:

Clasificación y marcado: La clasificación es necesaria para decidir cómo ha de ser tratado el tráfico que cumple unas condiciones específicas. Para clasificar el tráfico es necesario poder diferenciarlo. Hay diversas maneras de **diferenciar el tráfico**: valor de **CoS**, valor del campo **IP precedence**, **DSCP**, interfaz de entrada, interfaz de salida, IP origen, IP destino, dirección IP origen, dirección IP destino, Mac origen, Mac destino etc.

En este capítulo el **tráfico** se **marca** mediante el **valor de CoS**, así como mediante el **valor del campo IP Precedence** dentro del campo TOS (segundo byte de la cabecera IP). La **clasificación** es utilizada para **asignar el tráfico a las distintas colas a utilizar.**

Marcado en el switch: Para poder diferenciar el tráfico se utilizará un **marcado a nivel 2**, utilizando el estándar IEEE 802.1p, a través del protocolo IEEE 802.1Q.

El protocolo IEEE 802.1Q utiliza **tramas ethernet**, a las que les **añade una etiqueta**, denominada **VLAN tag**, con 2 campos (**TPID y TCI**) de **2 bytes de tamaño cada uno**.

3.1 Herramientas de QoS a utilizar:

La figura 23 muestra cómo queda el frame ethernet una vez se le ha añadido la VLAN tag, así como los distintos campos de la etiqueta. Cabe destacar que la figura 23 se ha obtenido del enlace indicado por la referencia [18] de la bibliografía.

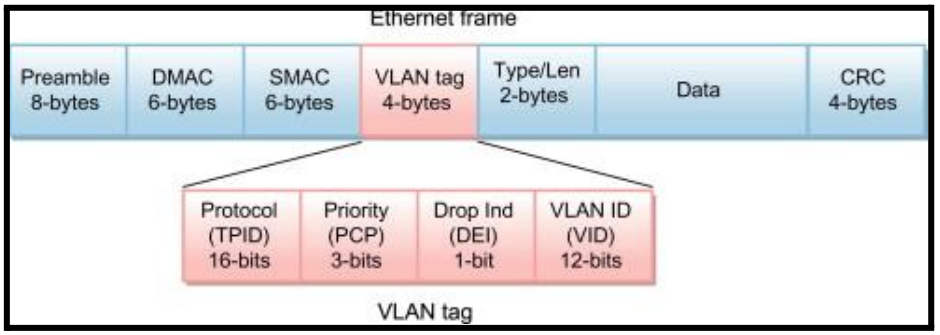


Figura 23. Frame ethernet con la VLAN tag.

El campo **TPID** (Tag Protocol Identifier) indica el protocolo que es utilizado en una VLAN tag. En el caso de IEEE 802.1Q, el valor en hexadecimal del campo TPID será de 0x8100.

El campo **TCI** (Tag Control Information) consta de los campos PCP, DEI y VID.

PCP (Priority Code Point): Campo de **3 bits** que se basa en el estándar IEEE 802.1p, indicando el **nivel de prioridad** de la trama en función del valor asignado.

La figura 24 muestra los distintos valores que puede tener el campo PCP, así como su equivalencia.

PCP	Priority	Acronym	Traffic Types
1	0 (lowest)	BK	Background
0	1	BE	Best Effort
2	2	EE	Excellent Effort
3	3	CA	Critical Applications
4	4	VI	Video, < 100 ms latency and jitter
5	5	VO	Voice, < 10 ms latency and jitter
6	6	IC	Internetwork Control
7	7 (highest)	NC	Network Control

Figura 24. Campo PCP de la VLAN tag.

DEI (Drop Eligible Indicator): campo de **1 bit**, que indica aquellas **tramas que puedan ser descartadas (valor 1), y aquellas que no puedan ser descartadas (valor 0)**, en el caso en que la red está congestionada. Este campo es **utilizado junto al campo PCP**, indicando un nivel de prioridad distinto, entre tramas con el mismo nivel de prioridad PCP.

VID (VLAN Identifier): **campo de 12 bits que indica la VLAN** que le corresponde a la trama ethernet. El valor de este campo puede variar entre los valores decimales 0 a 4095.

3.1 Herramientas de QoS a utilizar:

Tanto el valor 0 como el valor 4095 están reservados. El valor 0 es utilizado para etiquetar una trama que no tiene valor de VLAN ID (Priority tagged frames) y el valor 4095 se reserva para implementación. Además, Cisco también reserva el valor 1, para administración.

Marcado en el router: En el caso del router, el marcado será de nivel 3 mediante el IP precedence dentro del campo DSCP (Diffserv Code Point).

El campo DSCP (figura 25) es una transformación en la estructura del campo ToS (segundo byte de la cabecera IP) que permite diferenciar hasta 64 tipos de tráfico distintos, por lo tanto 64 prioridades distintas. Esto se debe a que el campo DSCP solamente utiliza los 6 primeros bits del segundo byte de la cabecera IP, quedando los 2 bits restantes sin uso actualmente.

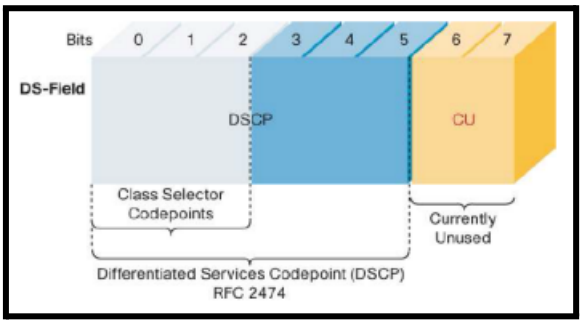


Figura 25. Campo DSCP.

Dependiendo del valor del campo DSCP, los paquetes serán agrupados en distintas clases:

- **Expedited Forwarding (EF):** Corresponde con los paquetes marcados con un valor de 101110 en binario o 46 en decimal. Es la clase con mayor prioridad.

- **Assured Forwarding (AF):** Es la segunda clase con mayor prioridad. Consta de cuatro subclases con tres prioridades distintas de descarte por subclase.

  En la figura 26 se puede observar las distintas subclases que hay en la clase AF, así como las distintas prioridades en función de la probabilidad de descarte de cada subclase. Cabe destacar que la subclase AF4x es la más prioritaria y la AF1x la menos prioritaria.

Prioridad de descarte	*Subclase AF1*	*Subclase AF2*	*Subclase AF3*	*Subclase AF4*
Baja	AF11 (001010) (10)	AF21 (010010) (18)	AF31 (011010) (26)	AF41 (100010) (34)
Media	AF12 (001100) (12)	AF22 (010100) (20)	AF32 (011100) (28)	AF42 (100100) (36)
Alta	AF13 (001110) (14)	AF23 (010110) (22)	AF33 (011110) (30)	AF43 (100110) (38)

Figura 26. Clase AF del campo DSCP.

- **Default Forwarding (DF):** Es la clase menos prioritaria. Corresponde con el valor 0 del campo DSCP, valor que tienen los paquetes en el caso de no haber sido marcados.

- **Class Selector (CS):** Corresponde con las prioridades especificadas por el campo ToS. Por lo tanto, solamente son utilizados los 3 primeros bits del campo DSCP. Se trata de los **valores de IP Precedence**.

La figura 27 muestra los distintos valores que puede tener la clase CS, así como su equivalencia. Cabe destacar que la figura 27 se ha obtenido del enlace indicado por la referencia [20] de la bibliografía.

DSCP Class Selector Names	Binary DSCP Values	IPP Binary Values	IPP Names
Default/CS0*	000000	000	Routine
CS1	001000	001	Priority
CS2	010000	010	Immediate
CS3	011000	011	Flash
CS4	100000	100	Flash Override
CS5	101000	101	Critic/Critical
CS6	110000	110	Internetwork Control
CS7	111000	111	Network Control

Figura 27.Clase CS de DSCP.

Colas: Una vez que el tráfico ha sido marcado, es conveniente que **cada clase de servicio vaya a parar a colas distintas**. Sin embargo, esto no es siempre posible. Por ejemplo, los **switches cisco catalyst 2950** solamente **presentan cuatro colas para ocho clases de servicio**. Debido a esto, por lo menos a una cola le corresponde más de una clase de servicio.

Para poner en práctica la política de servicios de las colas, se utilizarán los planificadores: Priority Queue (PQ), Weighted Round Robin (WRR), Weighted Round Robin combinado con Priority Queue, y Class Based Weighted Fair Queueing (CBWFQ).

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

3.2.1 Introducción:

En esta primera parte vamos a observar cómo actúan los distintos gestores de colas del switch 2950 de cisco. En este escenario, se van a configurar los enlaces que conectan los distintos PCs con el switch a 10 Mbps, para que los enlaces requieran de menos tráfico para su congestión.

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

Los distintos gestores de cola a utilizar en el switch 2950 son los siguientes:

- Priority Queue (PQ).
- Weighted round robin (WRR).
- Weighted round robin combinado con Priority Queue.

El switch 2950 dispone de cuatro colas diferentes que pueden servir frames con los modos indicados previamente.

Priority Queue: Planificador que **sirve todos los frames de las colas más prioritarias antes de servir los frames de las colas que son menos prioritarias**. Es decir, solo se servirán frames de una cola de menor prioridad, cuando la cola de mayor prioridad no tiene frames que servir. En el caso de que 2 o más colas tengan la misma prioridad, los frames se servirán en modo FIFO entre dichas colas.

El **switch 2950 funciona por defecto en modo priority queue** y los frames son llevados a una cola dependiendo del valor de clase de servicio (CoS) con el que han sido marcados. La prioridad de las colas es la siguiente: cola 4 > cola 3 > cola 2 > cola 1.

Por defecto, los valores de CoS se mapean de la forma indicada en la tabla 10, entre las distintas colas:

Valor de CoS	Colas	Prioridad
0, 1	1	-
2, 3	2	
4, 5	3	
6, 7	4	+

Tabla 10. Colas y CoS en los switches 2950.

Weighted round robin (WRR): Cuando el switch funciona en modo WRR, l**os frames se sirven de forma rotatoria, para que no se dé el caso de que una cola se quede sin servir frames**. Las colas que no tengan frames a servir se saltarán y se pasará a la siguiente cola.

En el caso del switch 2950, cada cola sirve una cantidad de frames determinada por el peso asignado a cada una de las colas. Las colas serán servidas de la siguiente forma:

cola 4 -> cola 3 -> cola 2 -> cola 1.

Weighted round robin (WRR) con Priority Queue (PQ): Cuando el switch funciona en modo Weighted Round Robin, pero también se utiliza una cola que funcionan en modo Priority Queue, **en primer lugar** se sirve **la cola que funciona en modo Priority Queue** y **finalmente** se sirven aquellas **colas** que funcionan en modo **Weighted Round Robin**.

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

En este capítulo, la cola utilizada como **cola prioritaria** es la **cola 4**, que corresponde con la cola más prioritaria de entre las cuatro colas del switch.

3.2.2 Topología y elementos a utilizar:

Una solución posible y sencilla para poder comprobar los efectos de los distintos planificadores del switch cisco 2950, es simplemente utilizar dicho switch y 4 ordenadores. De entre estos cuatro ordenadores, 3 ordenadores se dedicarán a emitir tráfico UDP y uno a recibir dicho tráfico UDP.

Para el montaje de dicha topología han sido necesarios los siguientes elementos:

- 1 x Switch Cisco 2950.
- 4 x PC.
- 4x cable de red directo (Ethernet).

Topología a montar (figura 28):

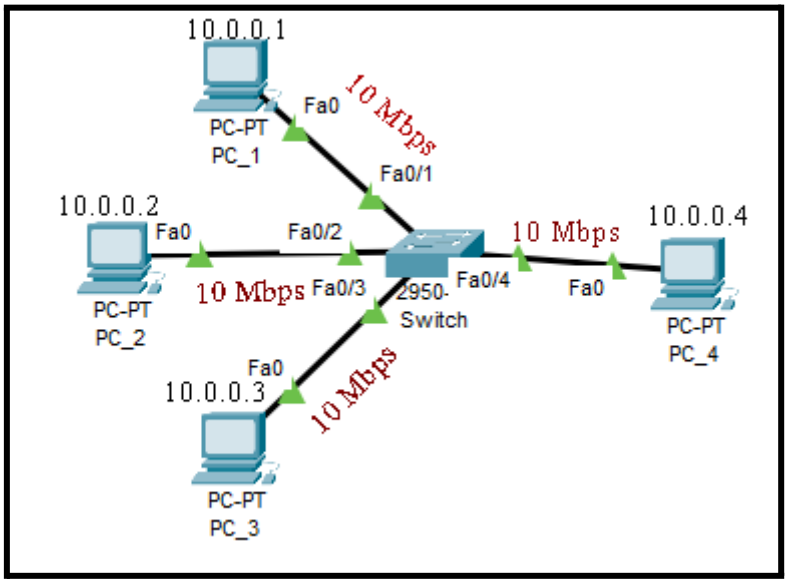


Figura 28. Topología de red del primer escenario

Características de los equipos:

- PC_1:
  Software necesario: IPerf3 (generador de tráfico).
- PC_2:
  Software necesario: IPerf3 (generador de tráfico).
- PC_3:
  Software necesario: IPerf3 (generador de tráfico).

- PC_4:

  Software necesario: IPerf3 (generador de tráfico).
  Wireshark (analizador de protocolos).

Equipo.	Interfaz.	Dirección IP.	Máscara	Gateway
PC_1	NIC	10.0.0.1	255.255.255.0	-
PC_2	NIC	10.0.0.2	255.255.255.0	-
PC_3	NIC	10.0.0.3	255.255.255.0	-
PC_4	NIC	10.0.0.4	255.255.255.0	-

Tabla 11. características de las configuraciones de red de los PCs.

Se han configurado los PCs con las características mostradas en la tabla 11.

3.2.3 Montaje y configuración básica del switch:

El montaje consiste en conectar los PCs con el switch mediante cables de red directos (ethernet). Para mayor claridad, se conectará la **interfaz ethernet del PC_x** con la **interfaz fastethernet 0/x del switch**, donde x es el número asignado a cada PC. Además, para realizar la configuración del switch conectamos el **puerto de consola del switch con el puerto COM1 de uno de los cuatro PCs**.

El montaje se puede observar en la figura 29.

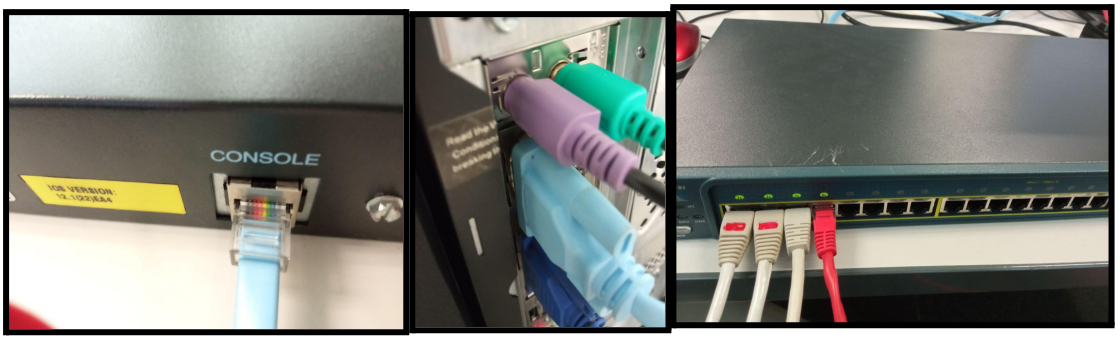


Figura 29. Montaje de la topología de red.

Para la configuración inicial del switch se va a utilizar el programa **putty**. Para comunicarnos con este, debemos seleccionar la **opción "serial"** (figura 30).

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

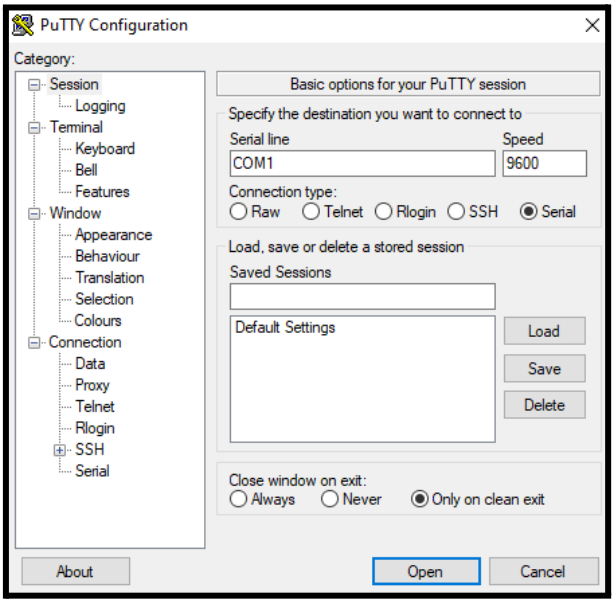


Figura 30. Programa Putty

Una vez se ha accedido a la configuración del switch, se han seguido los siguientes pasos para la configuración inicial del mismo:

Paso 1. Responder "no" ante la siguiente pregunta:

```
would you like to enter the initial configuration dialog? [yes/no]:
```

Paso 2. Entrar en modo privilegiado

```
Switch>enable:
```

Paso 3. Borrar la configuración inicial del switch:

```
Switch> enable
Switch# erase startup-config
```

Paso 4. Reiniciar el switch:

```
Switch# reload
```

Si aparece la siguiente pregunta se debe responder con "no", y pulsar "Enter".

```
System configuration has been modified. Save? [yes/no]
```

Paso 5. Cuando aparezca la siguiente pregunta, se ha de pulsar "Enter".

```
Proceed with reload? [confirm]
```

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

Paso 6. Cuando aparezca la siguiente pregunta se volverá a responder "no" y a presionar "Enter".

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

Paso 7. Finalmente, se ha de pulsar "Enter" ante la última pregunta:

```
Would you like to terminate autoinstall? [yes]:
```

Paso 8. Entrar en modo de configuración global:

```
Switch# configure terminal
Switch (config)#
```

Paso 9. configurar la velocidad a 10 Mbps en las interfaces fast ethernet:

```
Switch (config)# interface fast ethernet 0/1
Switch (config-if)# speed 10
```

Paso 10. Repetir el paso 9, para las cuatro interfaces a utilizar

En el caso de que se desee comprobar la configuración de las interfaces, se puede utilizar el siguiente comando en modo privilegiado:

```
Switch# show run
```

El resultado de utilizar el comando muestra la configuración que presenta la figura 31.

```
interface FastEthernet0/1
 speed 10
!
interface FastEthernet0/2
 speed 10
!
interface FastEthernet0/3
 speed 10
!
interface FastEthernet0/4
 speed 10
!
```

Figura 31. Comando show run.

Nota: Para salir de un modo de configuración a un modo previo se debe de utilizar el comando "exit".

3.2.4 Actividades prácticas:

3.2.4.1 Caso de estudio: Priority Queue

El primer caso de estudio consiste en observar cómo actúa el gestor de cola PQ en un entorno de congestión. En este ejercicio se trabajarán 2 casos en los cuales se podrán comprobar las ventajas y desventajas de dicho gestor de colas. Para ello, se variará el bitrate con el que los PCs generan paquetes.

Estos casos son:

1. **Los 2 PCs más prioritarios serán capaces de transmitir todos los paquetes a costa del menos prioritario.**
2. **El PC más prioritario es capaz de transmitir todos los paquetes a costa de los menos prioritarios, utilizando todo el ancho de banda.**

Herramientas de QoS que se utilizarán:
Marcado:
En este caso el **marcado se hace a nivel 2**, en la capa de enlace. Para ello se asigna el valor del campo pcp, que pertenece al campo TCI de la etiqueta 802.11q (Vlan tag), con un **valor de Cos de entre 0 y 7.**
El marcado a nivel 2 debe de quedar de la forma especificada en la tabla 12.

	Marcado	Equivalencia
pc_1	CoS 1	Best Effort
pc_2	CoS 3	Critical Applications
pc_3	CoS 5	Voz

Tabla 12.Marcado correspondiente a cada PC.

Colas:
Las colas deben ser configuradas de la forma indicada en la tabla 13.

Cola	Marcado Asignado	Modo de funcionamiento	Prioridad
Cola 1	CoS 0,**1**	Priority Queue	-
Cola 2	CoS 2,**3**	Priority Queue	
Cola 3	CoS 4,**5**	Priority Queue	
Cola 4	CoS 6,**7**	Priority Queue	+

Tabla 13. Estado de las colas del switch.

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

Para poder realizar este ejercicio se ha configurado el switch para que sea capaz de marcar el tráfico correctamente. Para ello se han seguido los siguientes pasos:

Paso 1: Entrar en el modo de configuración de la interfaz deseada:

```
Switch (config)# interface fast ethernet 0/1
Switch (config-if)#
```

Paso 2: Asignar el valor de CoS al tráfico entrante a dicha interfaz:

```
Switch (config-if)# mls qos cos 1
Switch (config-if)# mls qos cos override
```

El comando "*Switch (config-if)# mls qos cos valor_de_CoS*" marca los frames que no están marcados, con el valor "CoS *valor_de_CoS"*.

El comando "*Switch (config-if)# mls qos cos override*" hace que se marquen los frames independientemente de si están marcados previamente, o si no lo están, con el valor "CoS *valor_de_CoS"* especificado en el comando anterior.

Paso 3: Repetir el paso 2 para las restantes interfaces a configurar:

Paso 4: Finalmente, en modo privilegiado es necesario utilizar el comando "show run", para poder comprobar la configuración de los interfaces. Los interfaces deben mostrar una configuración como la de la figura 32:

```
Switch# show run
```

```
interface FastEthernet0/1
 speed 10
 duplex full
 mls qos cos 1
 mls qos cos override
!
interface FastEthernet0/2
 speed 10
 duplex full
 mls qos cos 3
 mls qos cos override
!
interface FastEthernet0/3
 speed 10
 duplex full
 mls qos cos 5
 mls qos cos override
!
interface FastEthernet0/4
 speed 10
 duplex full
```

Figura 32. resultado obtenido mediante el comando show run.

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

Además, también es necesario comprobar que el valor de Cos corresponde con un valor adecuado para que el tráfico sea clasificado en colas independientes (Figura 33). Para ello, en modo privilegio se ha utilizado el siguiente comando:

```
Switch# show wrr-queue cos-map
```

```
Switch#sh wr
Switch#sh wrr-queue c
CoS Value      :  0  1  2  3  4  5  6  7

Priority Queue :  1  1  2  2  3  3  4  4
```

Figura 33. resultado obtenido mediante el comando show wrr-queue cos-map.

En el caso de que el resultado obtenido no coincida con la figura 33, se deben utilizar los siguientes comandos en modo configuración:

```
Switch(config)# wrr-queue cos-map 1 0 1
Switch(config)# wrr-queue cos-map 2 2 3
Switch(config)# wrr-queue cos-map 3 4 5
Switch(config)# wrr-queue cos-map 4 6 7
```

Ejercicio 1: Los 2 PCs más prioritarios serán capaces de transmitir todos los paquetes a costa del menos prioritario.

En la figura 34 se puede observar el ancho de banda utilizado por los distintos enlaces.

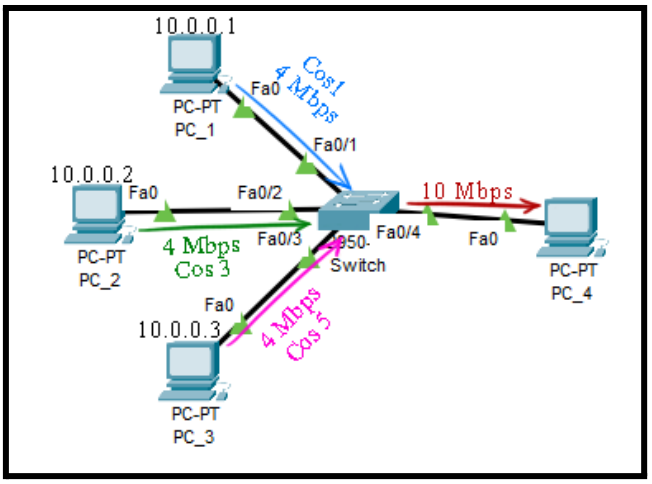


Figura 34. Topología de red del ejercicio 1.

Mediante el Iperf 3, se debe de abrir 3 instancias de servidor en PC_4. Cada instancia debe de ser abierta utilizando un puerto distinto, en concreto se deben utilizar los puertos 520X, en el que X corresponde con el el número del PC (PC_1 -> 5201). Cada puerto es utilizado para la conexión con un cliente.

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

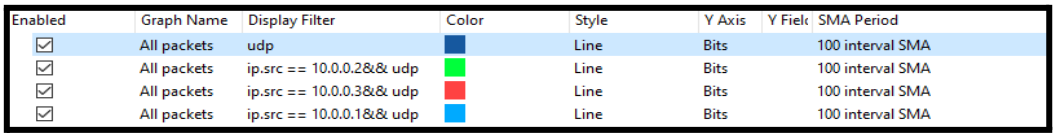
Cada cliente debe generar tráfico con los perfiles especificados en la tabla 14:

Protocolo	IP origen	IP destino	Tamaño de paquete	Bitrate (Mbps)	Tiempo de generación del flujo (s)	Puerto
UDP	10.0.0.1/24	10.0.0.4/24	1000	4	60	5201
UDP	10.0.0.2/24	10.0.0.4/24	1000	4	60	5202
UDP	10.0.0.3/24	10.0.0.4/24	1000	4	60	5203

Tabla 14. características de los flujos.

Una vez se observe que los tres PCs están emitiendo tráfico, se debe de capturar el tráfico recibido por PC_4, en PC_4 mediante wireshark. Para observar un resultado más fiable, se recomienda que se pare la captura antes de que se pare de generar tráfico.

Posteriormente a la captura de tráfico mediante Wireshark, se deben configurar filtros para capturar cada flujo recibido y el total del mismo. La figura 35 muestra un ejemplo de filtros.



Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Fiel	SMA Period
☑	All packets	udp		Line	Bits		100 interval SMA
☑	All packets	ip.src == 10.0.0.2&& udp		Line	Bits		100 interval SMA
☑	All packets	ip.src == 10.0.0.3&& udp		Line	Bits		100 interval SMA
☑	All packets	ip.src == 10.0.0.1&& udp		Line	Bits		100 interval SMA

Figura 35. Filtros de captura de paquetes.

¿Coincide aproximadamente el resultado esperado con el resultado obtenido mediante wireshark?¿Coinciden las tasas de pérdidas obtenidas mediante los clientes del Iperf 3 con lo esperado?

Copiad la gráfica obtenida mediante wireshark a continuación:

Solución:

PC4 debe utilizar los siguientes comandos mediante Iperf 3:

```
iperf3.exe -s -p 5201
iperf3.exe -s -p 5202
iperf3.exe -s -p 5203
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_1:

```
iperf3.exe -c 10.0.0.4 -u -p 5201 -b 4M -l 1000 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_2:

```
iperf3.exe -c 10.0.0.4 -u -p 5202 -b 4M -l 1000 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_3:

```
iperf3.exe -c 10.0.0.4 -u -p 5203 -b 4M -l 1000 -t 60
```

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

La figura 36 muestra la gráfica obtenida mediante Wireshark.

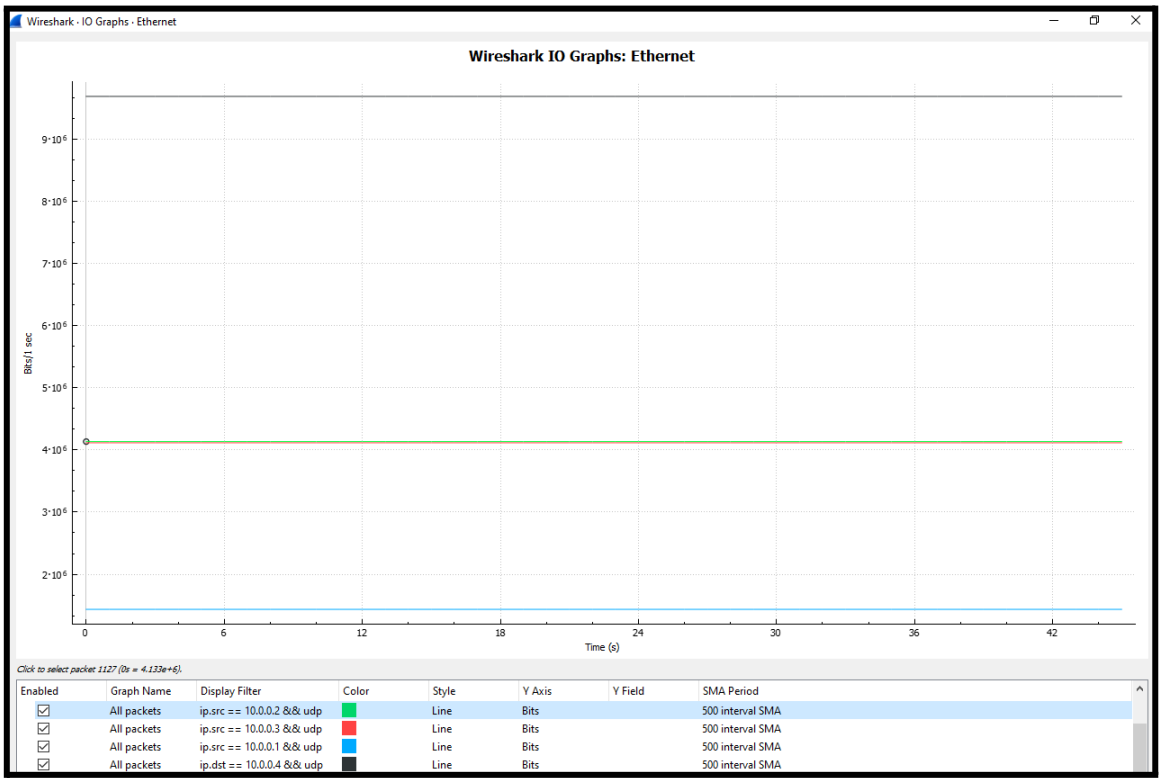


Figura 36. Comportamiento de los flujos obtenidos mediante Wireshark.

En la captura obtenida mediante wireshark, observamos que el ancho de banda se reparte de la forma indicada en la tabla 15:

	Ancho de banda	Prioridad
PC_1	1,436 Mbps	-
PC_2	4,133 Mbps	
PC_3	4,114 Mbps	+
Total	9,682 Mbps	

Tabla 15. Resultados obtenidos mediante Wireshark.

Podemos observar que el ancho de banda utilizado por PC_2 se solapa con el proveniente de PC_3. Esto corresponde con el bitrate que ha sido especificado, que era 4Mbps para todos los flujos. Por lo tanto, para que se consiga transmitir todo el tráfico de las dos colas más prioritarias, se penaliza considerablemente el tráfico correspondiente a la cola menos prioritaria, que consigue transmitir solamente 1,433 Mbps.

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

Además, se observa que el ancho de banda obtenido en los dos PCs más prioritarios (PC_3 y PC_2) es ligeramente superior al que se especificaba mediante Iperf3 (4 Mbps). Esto se debe principalmente a que Iperf3 no genera exactamente tráfico a la tasa especificada y a que el bitrate especificado en Iperf 3 solo tiene en cuenta el tamaño del payload y no las cabeceras IP (20 bytes), UDP (8 bytes) y Ethernet (22 bytes).

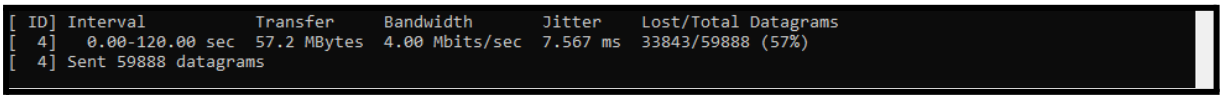


Figura 37. Porcentaje pérdidas PC_1.

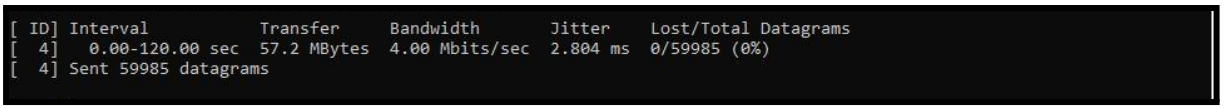


Figura 38. Porcentaje pérdidas PC_2.

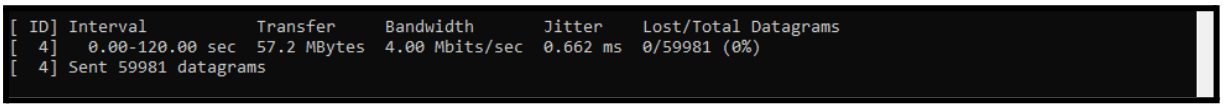


Figura 39. Porcentaje pérdidas PC_3.

Los resultados obtenidos mediante Iperf 3 (figuras 37, 38 y 39) nos permiten comprobar que los dos flujos más prioritarios (PC_3 y PC_2) no presentan pérdidas, y que en el flujo menos prioritario (PC_1) se pierden más de la mitad de los paquetes que se generan (57%).

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

Ejercicio 2: El PC más prioritario es capaz de transmitir todos los paquetes a costa de los menos prioritarios, utilizando todo el ancho de banda.

En la figura 40 se puede observar el ancho de banda utilizado por los distintos enlaces.

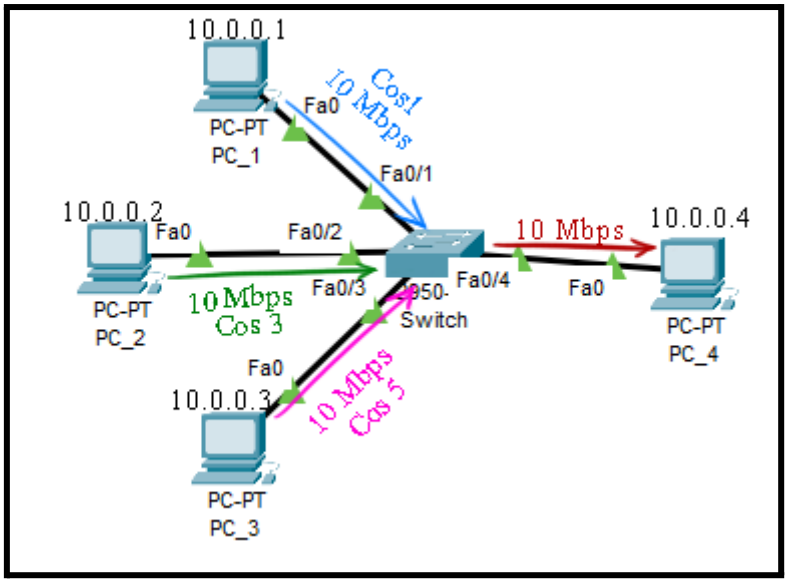


Figura 40. Topología de red del ejercicio 2.

Cada cliente debe generar tráfico con los perfiles especificados por la tabla 16:

Protocolo	IP origen	IP destino	Tamaño de paquete	Bitrate (Mbps)	Tiempo de generación del flujo (s)	Puerto
UDP	10.0.0.1/24	10.0.0.4/24	1000	10	60	5201
UDP	10.0.0.2/24	10.0.0.4/24	1000	10	60	5202
UDP	10.0.0.3/24	10.0.0.4/24	1000	10	60	5203

Tabla 16. características de los flujos.

¿Coincide aproximadamente el resultado esperado con el obtenido mediante wireshark?

Copiad la gráfica obtenida mediante wireshark a continuación:

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

Solución:

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_1:

```
iperf3.exe -c 10.0.0.4 -u -p 5201 -b 10M -l 1000 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_2:

```
iperf3.exe -c 10.0.0.4 -u -p 5202 -b 10M -l 1000 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_3:

```
iperf3.exe -c 10.0.0.4 -u -p 5203 -b 10M -l 1000 -t 60
```

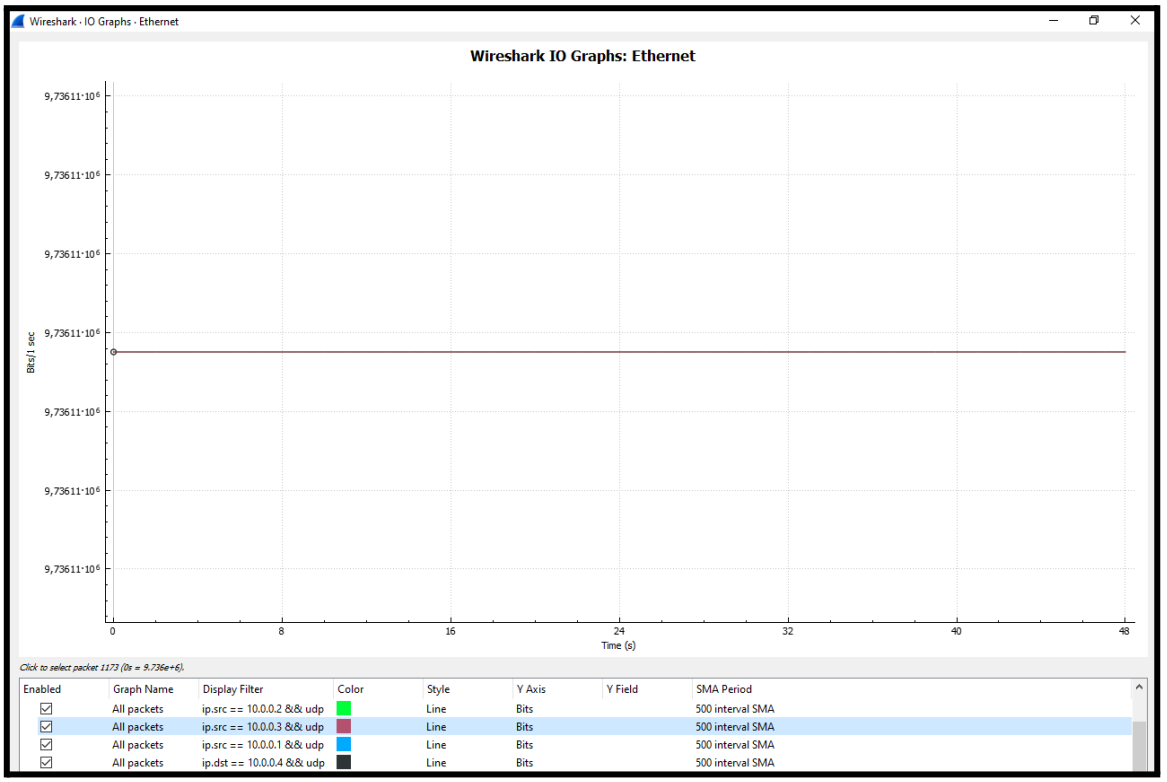


Figura 41.Comportamiento de los flujos obtenidos mediante Wireshark.

En la captura obtenida mediante wireshark (figura 41), observamos que el ancho de banda se reparte de la forma indicada en la tabla 17:

	Ancho de banda	Prioridad
PC_1	0 Mbps	-
PC_2	0 Mbps	
PC_3	9,736 Mbps	+
Total	9,736 Mbps	

Tabla 17. Resultados obtenidos mediante Wireshark.

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

En este caso, el tráfico generado por PC_3 utiliza todo el ancho de banda porque es capaz de congestionar el enlace por sí solo y los paquetes generados van a parar a la cola más prioritaria.

```
iperf3: error - unable to receive control message: Connection reset by peer
```

Figura 42. Porcentaje pérdidas PC_1.

```
iperf3: error - unable to receive control message: Connection reset by peer
```

Figura 43. Porcentaje pérdidas PC_2.

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-90.00  sec   101 MBytes  9.39 Mbits/sec  0.013 ms  0/105629 (0%)
[  4] Sent 105629 datagrams
```

Figura 44. Porcentaje pérdidas PC_3.

Mediante los resultados obtenidos por el Iperf3 (figuras 42,43 y 44), observamos que no se producen pérdidas en los paquetes generados por PC_3. Sin embargo, en el caso de PC_2 y PC_1 se pierde la conexión con el servidor debido a que no son capaces de transmitir paquetes.

Cuando se produce un error como el ocurrido en los PCs 1 y 2, es necesario reiniciar los servidores correspondientes.

3.2.4.2 Caso de estudio: Weighted Round Robin (WRR):

A continuación, se va a comprobar el funcionamiento del gestor de cola WRR en un entorno de congestión. Para ello, se han descrito tres casos mediante los cuales se podrán comprobar las distintas características de WRR.

Estos casos son:

1. **Paquetes con el mismo tamaño en los tres flujos para que WRR proporcione el ancho de banda de forma exacta a cada flujo en función de los pesos de estos.**
2. **Paquetes de tamaño variable entre los tres flujos, favoreciendo de esta forma al flujo con paquetes de mayor tamaño.**
3. **Paquetes de tamaño variable entre los tres flujos en el que uno de ellos genera paquetes a una tasa menor que la que le corresponde, repartiéndose el ancho de banda restante entre los otros dos flujos en función de los pesos y el tamaño de paquete.**

Herramientas de QoS que se utilizarán:

Marcado:

El marcado a nivel 2 debe de quedar de la forma especificada en la tabla 18. Como se puede apreciar, el marcado es igual que en el caso de PQ.

	Marcado	Equivalencia
pc_1	CoS 1	Best Effort
pc_2	CoS 3	Critical Applications
pc_3	CoS 5	Voz

Tabla 18.Marcado correspondiente a cada PC.

Colas:
Las colas deben ser configuradas de la forma indicada en la tabla 19.

Cola	Marcado Asignado	Modo de funcionamiento	Prioridad	Peso
Cola 1	CoS 0,**1**	Weighted Round Robin	-	1
Cola 2	CoS 2,**3**	Weighted Round Robin		2
Cola 3	CoS 4,**5**	Weighted Round Robin		3
Cola 4	CoS 6,**7**	Priority Queue	+	0

Tabla 19. Estado de las colas del switch.

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

Para poder realizar este ejercicio se ha de configurar el switch para que funcione en modo WRR. Para ello en modo configuración global se asigna un peso a cada cola del switch de la siguiente forma:

```
Switch (config)#wrr-queue bandwidth 1 2 3 0
```

Este comando asigna el peso 1 a la cola 1, el peso 2 a la cola 2, el peso 3 a la cola 3 y el peso 0 a la cola 4. En este caso solamente se hace uso de las tres primeras colas.

En modo privilegiado comprobamos que la asignación de pesos es correcta mediante el comando:

```
Switch#show wrr-queue Bandwidth
```

La figura 45 nos muestra la correcta configuración de WRR.

```
Switch#sh wrr-queue Bandwidth
WRR Queue   :   1   2   3   4

Bandwidth   :   1   2   3   0
```

Figura 45. resultado obtenido mediante el comando show wrr-queue Bandwidth.

Ejercicio 3: Paquetes con el mismo tamaño en los tres flujos para que WRR proporcione el ancho de banda de forma exacta a cada flujo en función de los pesos de estos.

En la figura 46 se puede observar el ancho de banda utilizado por los distintos enlaces.

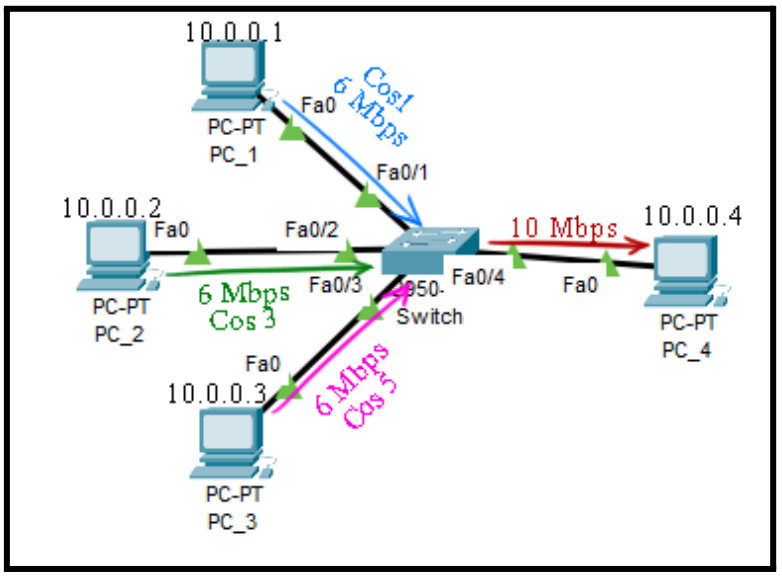


Figura 46. Topología de red del ejercicio 3.

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

Cada cliente debe generar tráfico con los perfiles especificados en la tabla 20:

Protocolo	IP origen	IP destino	Tamaño de paquete	Bitrate (Mbps)	Tiempo de generación del flujo (s)	Puerto
UDP	10.0.0.1/24	10.0.0.4/24	300	6	60	5201
UDP	10.0.0.2/24	10.0.0.4/24	300	6	60	5202
UDP	10.0.0.3/24	10.0.0.4/24	300	6	60	5203

Tabla 20. características de los flujos.

¿Cómo se reparte el ancho de banda?¿Cómo influye el tamaño de los paquetes en el reparto del ancho de banda? ¿Coinciden las tasas de pérdidas obtenidas mediante los clientes del Iperf 3 con lo esperado?

Calcule como debería quedar repartido teóricamente a partir del ancho de banda total obtenido mediante wireshark y compruebe si los resultados obtenidos son los esperados:

Para calcular el ancho de banda teórico de los PCs se utilizan las siguiente fórmulas:

$$\text{Ancho de banda PC\_1} = \text{Ancho de banda total} * \frac{[tam1] * [W1]}{[tam1] * [W1] + [tam2] * [W2] + [tam3] * [W3]} \quad (5)$$

$$\text{Ancho de banda PC\_2} = \text{Ancho de banda total} * \frac{[tam2] * [W2]}{[tam1] * [W1] + [tam2] * [W2] + [tam3] * [W3]} \quad (6)$$

$$\text{Ancho de banda PC\_3} = \text{Ancho de banda total} * \frac{[tam3] * [W3]}{[tam1] * [W1] + [tam2] * [W2] + [tam3] * [W3]} \quad (7)$$

El **ancho de banda total** es el obtenido mediante wireshark (captura de todos los paquetes UDP).

tamx equivale al tamaño de paquete correspondiente a la generación del flujo de PC_x.
tam1 se calcularía de la siguiente forma:

tam1 = 300 + [bytes cabecera IP] +[bytes cabecera ethernet] + [bytes cabecera UDP] =
= 300 + 20 + 22 + 8 = 350.

Wx es el peso asignado a la cola que recibe el tráfico generado por PC_x.

La figura 47 muestra el tamaño de los paquetes que hay en cada cola cuando se produce congestión, así como el peso de cada cola.

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

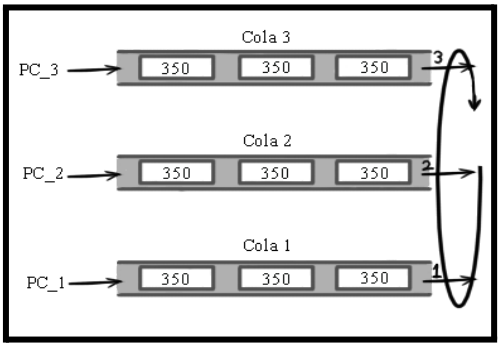


Figura 47. Resumen visual del ejercicio 3.

Copiad la gráfica obtenida mediante wireshark a continuación:

Solución:

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_1:

```
iperf3.exe -c 10.0.0.4 -u -p 5201 -b 6M -l 300 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_2:

```
iperf3.exe -c 10.0.0.4 -u -p 5202 -b 6M -l 300 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_3:

```
iperf3.exe -c 10.0.0.4 -u -p 5203 -b 6M -l 300 -t 60
```

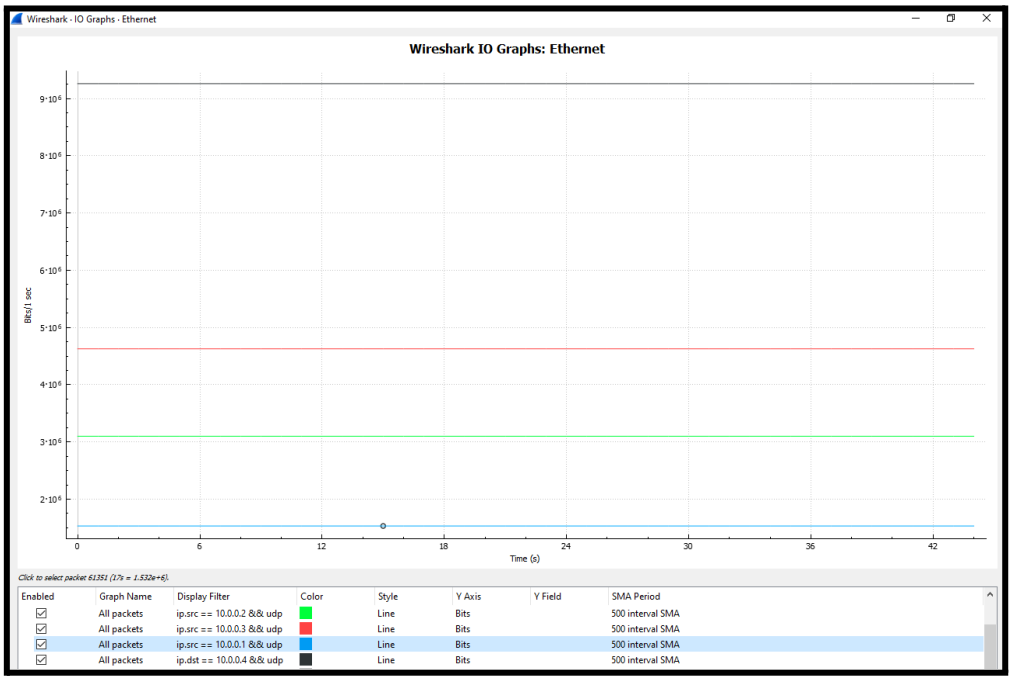


Figura 48.Comportamiento de los flujos obtenidos mediante Wireshark.

En la captura obtenida mediante wireshark (figura 48), observamos que el ancho de banda se reparte de la forma indicada por la tabla 21:

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

	Ancho de banda	Peso
PC_1	1,532 Mbps	1
PC_2	3,1 Mbps	2
PC_3	4,627 Mbps	3
Total	9,259 Mbps	

Tabla 21. Resultados obtenidos mediante Wireshark.

Calculamos el ancho de banda teórico en este caso a partir de (5), (6) y (7):

Ancho de banda PC_1 = Ancho de banda total* $\frac{1*350}{1*350+2*350+3*350}$ =

= Ancho de banda total * $\frac{1}{1+2+3}$ = 9,259/6 = 1,543 Mbps.

Ancho de banda PC_2 = Ancho de banda total* $\frac{2}{1+2+3}$ = 3,086 Mbps.

Ancho de banda PC_3 = Ancho de banda total* $\frac{3}{1+2+3}$ = 4,6295 Mbps.

Podemos observar que hay poca variación entre el resultado teórico y el observado mediante wireshark. Por lo tanto, cuando el tamaño de paquetes no es variable el ancho de banda se reparte exáctamente en función de los pesos.

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-120.00 sec  85.8 MBytes  6.00 Mbits/sec  0.614 ms  216040/299819 (72%)
[  4] Sent 299819 datagrams
```

Figura 49. Porcentaje pérdidas PC_1.

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-120.00 sec  85.8 MBytes  6.00 Mbits/sec  0.210 ms  157811/299857 (53%)
[  4] Sent 299857 datagrams
```

Figura 50. Porcentaje pérdidas PC_2.

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-120.00 sec  85.8 MBytes  6.00 Mbits/sec  1.218 ms  90190/299795 (30%)
[  4] Sent 299795 datagrams
```

Figura 51. Porcentaje pérdidas PC_3.

Como podemos observar (figuras 49, 50 y 51), el porcentaje de paquetes perdidos es del 72% en la cola menos prioritaria respecto del 52% de la segunda cola más prioritaria y del 30% en la cola más prioritaria. Es lógico que en unas condiciones similares, el porcentaje de paquetes que se pierdan sea mayor cuanto menor prioritaria sea la cola.

Además, se puede comprobar que el porcentaje de pérdidas es el esperado, porque la diferencia de los porcentajes de PC_1 y PC_ 2 (19%) es parecida a la diferencia de los porcentajes de PC_2 y PC_3 (23%). Lógicamente, la diferencia debería ser la misma, porque en ambos casos coincide la diferencia entre los pesos. La diferencia se debe principalmente a que no es posible que las tres fuentes generen paquetes al mismo tiempo, alterando ligeramente el resultado.

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

Ejercicio 4: Paquetes de tamaño variable entre los tres flujos, favoreciendo de esta forma al flujo con paquetes de mayor tamaño.

En la figura 52 se puede observar el ancho de banda utilizado por los distintos enlaces.

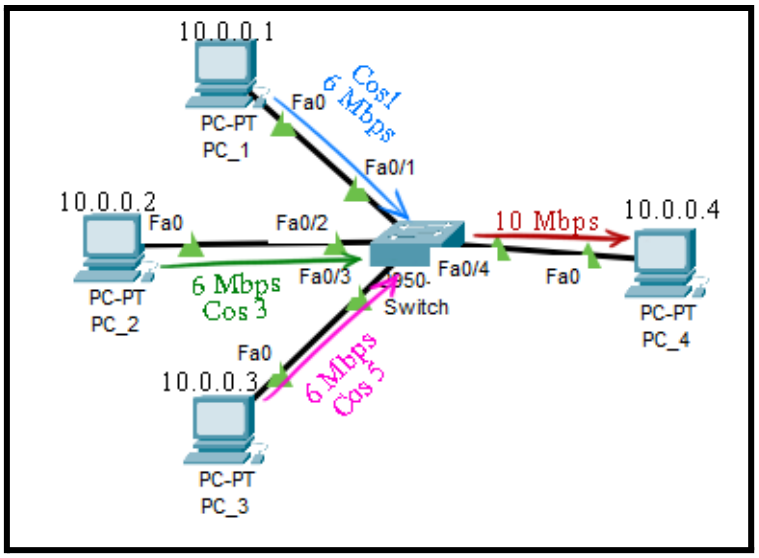


Figura 52. Topología de red del ejercicio 4.

Cada cliente debe generar tráfico con los perfiles especificados en la tabla 22:

Protocolo	IP origen	IP destino	Tamaño de paquete	Bitrate (Mbps)	Tiempo de generación del flujo (s)	Puerto
UDP	10.0.0.1/24	10.0.0.4/24	1300	6	60	5201
UDP	10.0.0.2/24	10.0.0.4/24	700	6	60	5202
UDP	10.0.0.3/24	10.0.0.4/24	300	6	60	5203

Tabla 22. características de los flujos.

El tráfico debe de ser capturado por PC_4 mediante wireshark.

¿Cómo se reparte el ancho de banda?¿Cómo influye el tamaño de los paquetes en el reparto del ancho de banda?¿Qué valor deberían tener los pesos para que se reparta el ancho de banda de la forma deseada?¿Coinciden las tasas de pérdidas obtenidas mediante los clientes del Iperf3 con lo esperado?
Calcule como debería quedar repartido teóricamente a partir del ancho de banda total obtenido mediante wireshark y compruebe si los resultados obtenidos son los esperados:

La figura 53 muestra el tamaño de los paquetes que hay en cada cola cuando se produce congestión, así como el peso de cada cola.

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

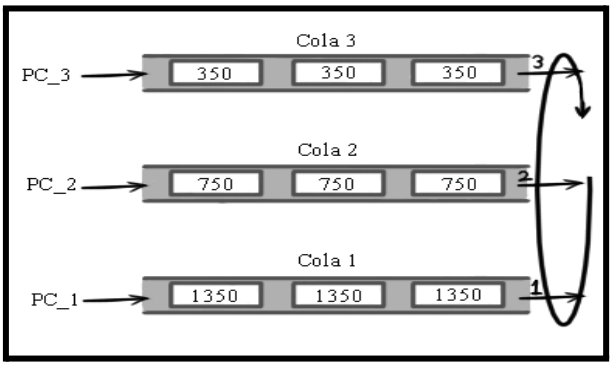


Figura 53. Resumen visual del ejercicio 4.

Copiad la gráfica obtenida mediante wireshark a continuación:
Solución:

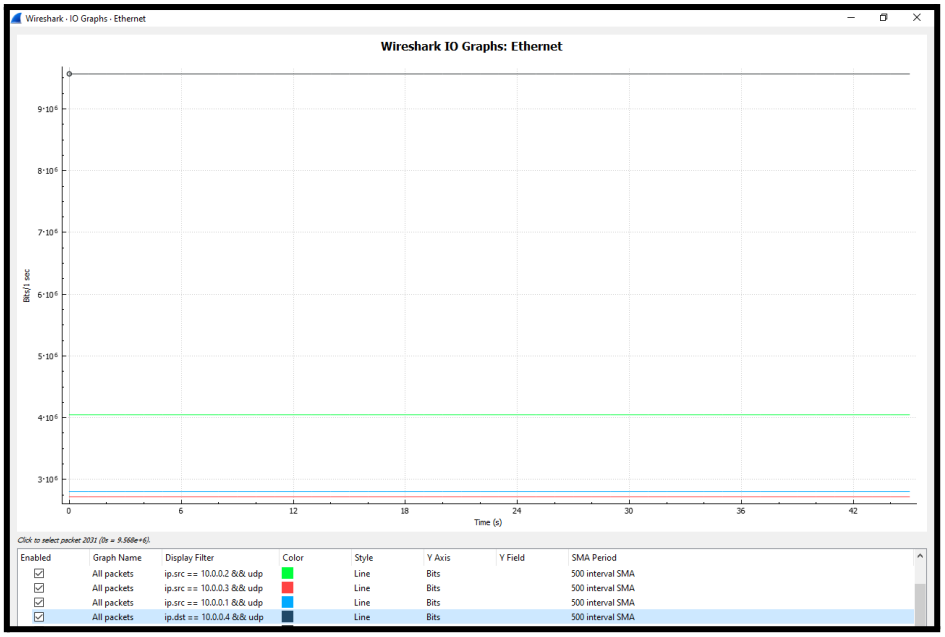


Figura 54.Comportamiento de los flujos obtenidos mediante Wireshark.

En la captura obtenida mediante wireshark (figura 54), observamos que **el ancho de banda se reparte de la forma indicada por la tabla 23:**

	Ancho de banda	Peso
PC_1	3,301 Mbps	1
PC_2	3,699 Mbps	2
PC_3	2,547 Mbps	3
Total	9,546 Mbps	

Tabla 23. Resultados obtenidos mediante Wireshark.

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

En este caso, observamos que pese a que los tres flujos generan paquetes a una tasa parecida (6 Mbps), el flujo con mayor peso (PC_3) utiliza una menor cantidad del ancho de banda total.

En el caso de que WRR funcionara correctamente, el ancho de banda debería repartirse solamente en función de los pesos asignados. Por lo tanto, debería corresponder 1/6 del total al flujo de PC1, 2/6 al flujo de PC2 y 3/6 al de PC3.

Sin embargo, en este ejercicio se observa que el tamaño de paquete influye en la forma de repartir el ancho de banda, beneficiando al flujo con un tamaño de paquete mayor. De esta forma, el flujo que se ve más favorecido por tamaños de paquete variable es el generado por PC1.

Los pesos necesarios para obtener el resultado deseado se pueden calcular de la siguiente forma:

Peso PC3 = 3/350 = 85,7 x $^{-4}$ → Peso PC1 = 857 (857 x 350 = 299950 Bytes).
Peso PC2 = 2/750 = 26,7 x 10^{-4} → Peso PC2 = 267 (267 x 750 = 200250 Bytes).
Peso PC1 = 1/1350 = 7,4 x 10^{-4} → Peso PC1 = 74 (74 x 1350 = 99900 Bytes).

Calculamos el ancho de banda teórico para comprobar que los resultados obtenidos mediante wireshark son correctos a partir de **(5), (6) y (7):**

Al tamaño de paquete especificado hay que añadirle 20 bytes de la cabecera IP, 22 Bytes de la cabecera ethernet y 8 Bytes de la cabecera UDP, quedando: 350 B, 750 B y 1350 B.

Ancho de banda PC_1 = $9{,}546 * \frac{1*1350}{1*1350+2*750+3*350} = 3{,}304$ Mbps

Ancho de banda PC_2 = $9{,}546 * \frac{2*750}{1*1350+2*750+3*350} = 3{,}67$ Mbps.

Ancho de banda PC_3 = $9{,}546 * \frac{3*350}{1*1350+2*750+3*350} = 2{,}57$ Mbps.

Podemos observar que hay poca variación entre el resultado teórico y el observado mediante wireshark.

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-60.01  sec  42.8 MBytes  5.99 Mbits/sec  1.069 ms  15054/34561 (44%)
[  4] Sent 34561 datagrams
```

Figura 55. Porcentaje pérdidas PC_1.

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-60.00  sec  42.9 MBytes  5.99 Mbits/sec  5.051 ms  25307/64211 (39%)
[  4] Sent 64211 datagrams
```

Figura 56. Porcentaje pérdidas PC_2.

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-60.00  sec  42.9 MBytes  5.99 Mbits/sec  2.066 ms  89227/149800 (60%)
[  4] Sent 149800 datagrams
```

Figura 57. Porcentaje pérdidas PC_3.

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

A partir de los resultados obtenidos por Iperf3 (figuras 55, 56 y 57) observamos que el porcentaje de pérdidas es menor en el tráfico generado por PC_2. Esto se debe principalmente a que dicho tráfico queda favorecido debido a que el tamaño de paquete es superior al generado por PC_3, y que a pesar

de tener un tamaño de paquete menor al de PC_1, la diferencia de tamaño tiene menor influencia que el peso entre ambos.

Además, observamos como el porcentaje de pérdidas de la cola menos prioritaria es menor al de la cola más prioritaria, porque el tamaño de paquete es tan grande que tiene más influencia que la diferencia de peso.

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_1:

```
iperf3.exe -c 10.0.0.4 -u -p 5201 -b 6M -l 1300 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_2:

```
iperf3.exe -c 10.0.0.4 -u -p 5202 -b 6M -l 700 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_3:

```
iperf3.exe -c 10.0.0.4 -u -p 5203 -b 6M -l 300 -t 60
```

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

Ejercicio 5: Paquetes de tamaño variable entre los tres flujos en el que uno de ellos genera paquetes a una tasa menor que la que le corresponde, repartiéndose el ancho de banda restante entre los otros dos flujos en función de los pesos y el tamaño de paquete.

En la figura 58 se puede observar el ancho de banda utilizado por los distintos enlaces.

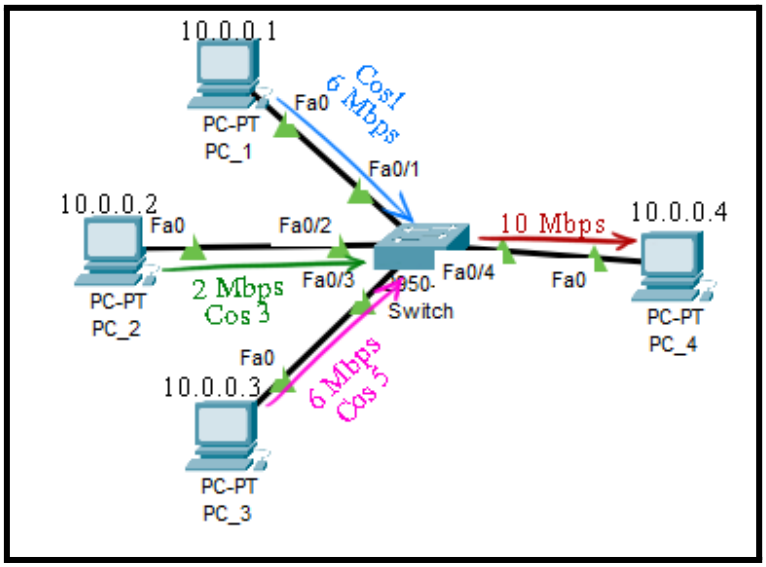


Figura 58. Topología de red del ejercicio 5.

Cada cliente debe generar tráfico con los perfiles especificados en la tabla 24:

Protocolo	IP origen	IP destino	Tamaño de paquete	Bitrate (Mbps)	Tiempo de generación del flujo (s)	Puerto
UDP	10.0.0.1/24	10.0.0.4/24	500	6	60	5201
UDP	10.0.0.2/24	10.0.0.4/24	700	2	60	5202
UDP	10.0.0.3/24	10.0.0.4/24	300	6	60	5203

Tabla 24. características de los flujos.

El tráfico debe de ser capturado por PC_4 mediante wireshark.

¿Cómo se reparte el ancho de banda?¿Cómo influye el tamaño de los paquetes en el reparto del ancho de banda?¿Qué ocurre con el ancho de banda de PC_2?¿Coinciden las tasas de pérdidas obtenidas mediante los clientes del Iperf3 con lo esperado?

Calcule como debería quedar repartido teóricamente a partir del ancho de banda total obtenido mediante wireshark y compruebe si los resultados obtenidos son los esperados:

La figura 59 muestra el tamaño de los paquetes que hay en cada cola cuando se produce congestión, así como el peso de cada cola.

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

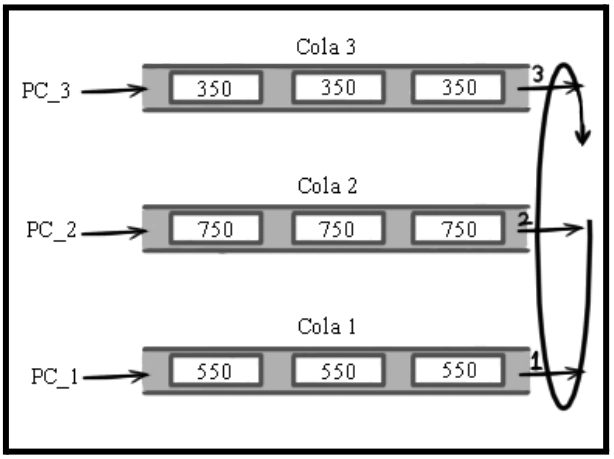


Figura 59. Resumen visual del ejercicio 6.

Copiad la gráfica obtenida mediante wireshark a continuación:

Solución:

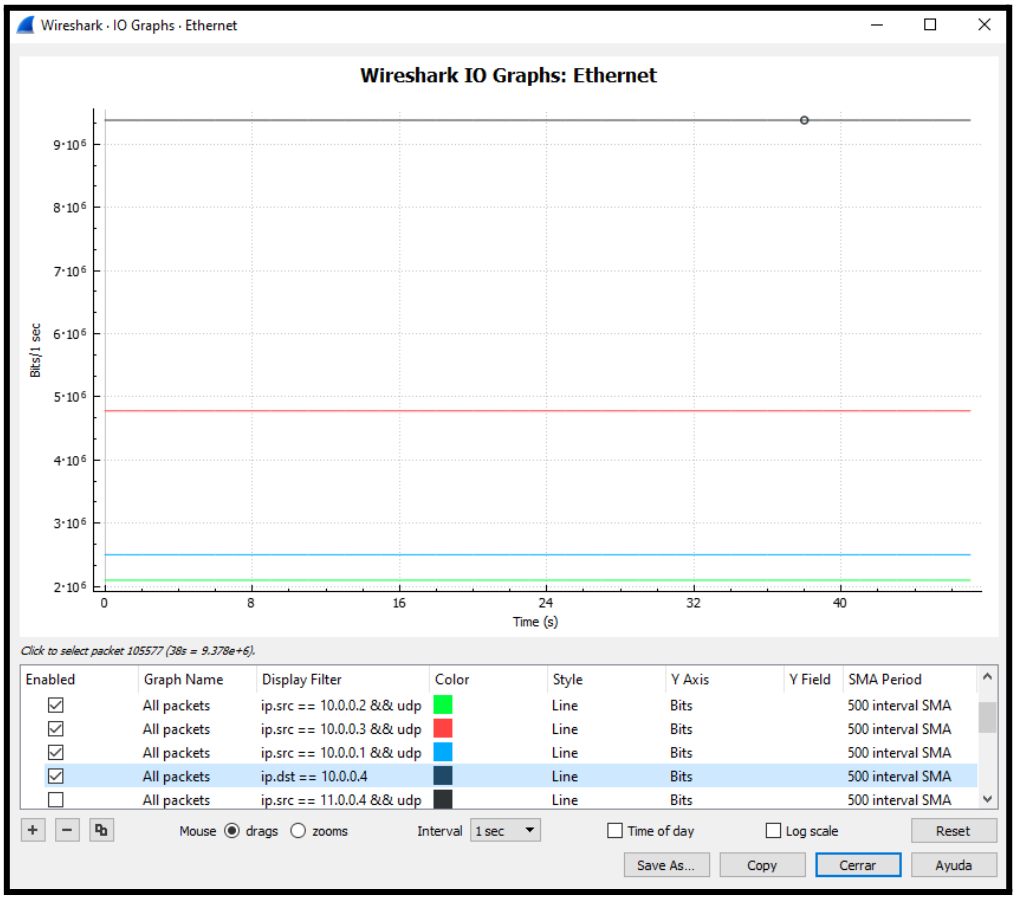


Figura 60.Comportamiento de los flujos obtenidos mediante Wireshark.

En la captura obtenida mediante wireshark (figura 60), observamos que el ancho de banda se reparte de la forma indicada por la tabla 25:

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

	Ancho de banda	Peso
PC_1	2,502 Mbps	1
PC_2	2,098 Mbps	2
PC_3	4,778 Mbps	3
Total	9,378 Mbps	

Tabla 25. Resultados obtenidos mediante Wireshark.

Calculamos el ancho de banda teórico en este caso a partir de (5), (6) y (7):

Al tamaño de paquete especificado hay que añadirle 20 bytes de la cabecera IP, 22 Bytes de la cabecera ethernet y 8 bytes de la cabecera UDP, quedando: 350 B, 750 B y 550 B.

Ancho de banda PC_1 = $9{,}378 * \frac{1*550}{1*550+2*750+3*350} = 1{,}664$ Mbps

Ancho de banda PC_2 = $9{,}378 * \frac{2*750}{1*550+2*750+3*350} = 4{,}538$ Mbps.

Ancho de banda PC_3 = $9{,}378 * \frac{3*350}{1*550+2*750+3*350} = 3{,}176$ Mbps.

PC_2 envía paquetes a una tasa de 2,098 Mbps, que es menor a los 4,538 Mbps que le corresponden teóricamente.

4,538 -2,098 = 2,44

Por lo tanto, 2,44 Mbps quedarán repartidos entre PC_1 y PC_3.

Ancho de banda PC_1 = $1{,}664 + 2{,}44 * \frac{1*550}{1*550+3*350} = 2{,}502$ Mbps.

Ancho de banda PC_3 = $3{,}176 + 2{,}44 * \frac{3*350}{1*550+3*350} = 4{,}777$ Mbps.

Ancho de banda PC_2 = 2,098 Mbps.

Los resultados teóricos coinciden prácticamente con los resultados obtenidos mediante wireshark. Por lo tanto, el ancho de banda sobrante de PC_2 ha quedado repartido correctamente.

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-60.01  sec  42.9 MBytes  5.99 Mbits/sec  0.310 ms  51439/89900 (57%)
[  4] Sent 89900 datagrams
```

Figura 61. Porcentaje pérdidas PC_1.

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-60.00  sec  14.3 MBytes  2.00 Mbits/sec  1.629 ms  0/21400 (0%)
[  4] Sent 21400 datagrams
```

Figura 62. Porcentaje pérdidas PC_2.

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-60.01  sec  42.9 MBytes  5.99 Mbits/sec  5.091 ms  41085/149832 (27%)
[  4] Sent 149832 datagrams
```

Figura 63. Porcentaje pérdidas PC_3.

A partir de los resultados obtenidos con Iperf3 (figuras 61, 62 y 63), observamos que PC_2 no presenta pérdidas porque el ancho de banda total que le corresponde es mayor que su tasa de envío de paquetes.

Además, observamos que el tráfico generado por PC_3 presenta menos pérdidas que el generado por PC_1. Esto se debe a que el tamaño de paquete del flujo generado por PC_1 no es suficientemente grande como para compensar la diferencia de prioridad.

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_1:

```
iperf3.exe -c 10.0.0.4 -u -p 5201 -b 6M -l 500-t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_2:

```
iperf3.exe -c 10.0.0.4 -u -p 5202 -b 2M -l 700 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_3:

```
iperf3.exe -c 10.0.0.4 -u -p 5203 -b 6M -l 300 -t 60
```

3.2.4.3 Caso de estudio: Weighted Round Robin (WRR) + Priority Queue (PQ):

Finalmente, se va a analizar el funcionamiento de WRR combinado con PQ mediante dos casos distintos.

Estos casos son:

1. **Paquetes con el mismo tamaño en los tres flujos para que WRR proporcione el ancho de banda de forma exacta a cada flujo en función de los pesos de estos, respecto del ancho de banda que no es utilizado en la cola que sirve frames en modo PQ.**
2. **La cola que funciona en PQ es capaz de congestionar la red por sí sola.**

Herramientas de QoS que se utilizarán:

- **Marcado:**

El marcado a nivel 2 debe de quedar de la forma especificada en la tabla 26. En este caso, **el marcado en PC_3 es distinto al que se le había asignado en los ejercicios anteriores.**

	Marcado	Equivalencia
pc_1	CoS 1	Best Effort
pc_2	CoS 3	Critical Applications
pc_3	**CoS 7**	Network Control

Tabla 26. Marcado correspondiente a cada PC.

- **Colas:**

Las colas deben ser configuradas de la forma indicada en la tabla 27.

Cola	Marcado Asignado	Modo de funcionamiento	Prioridad	Peso
Cola 1	CoS 0,**1**	Weighted Round Robin	-	1
Cola 2	CoS 2,**3**	Weighted Round Robin		2
Cola 3	CoS 4,**5**	Weighted Round Robin		3
Cola 4	CoS 6,**7**	Priority Queue	+	0

Tabla 27. Estado de las colas del switch.

Para que la cuarta cola funcione en modo PQ se le debe de asignar un peso de 0, valor que ha sido asignado a la hora de configurar WRR. Por lo tanto, hay que configurar el router para que los paquetes que entran desde PC_3 se marquen con un valor de CoS que vaya a parar a la cola 4, como por ejemplo CoS 7. Para ello, en la interfaz fast ethernet 0/3 se deben usar los siguientes comandos:

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

```
Switch (config-if)#mls qos cos 7
Switch (config-if)#mls qos cos override
```

Ejercicio 6: Paquetes con el mismo tamaño en los tres flujos para que WRR proporcione el ancho de banda de forma exacta a cada flujo en función de los pesos de estos, respecto del ancho de banda que no es utilizado en la cola que sirve frames en modo PQ.

En la figura 64 se puede observar el ancho de banda utilizado por los distintos enlaces.

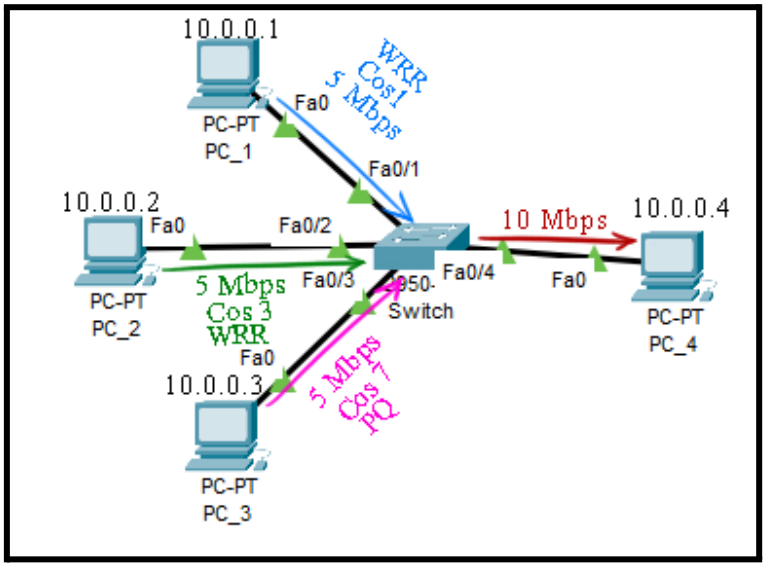


Figura 64. Topología de red del ejercicio 6.

Cada cliente debe generar tráfico con los perfiles especificados en la tabla 28:

Protocolo	IP origen	IP destino	Tamaño de paquete	Bitrate (Mbps)	Tiempo de generación del flujo (s)	Puerto
UDP	10.0.0.1/24	10.0.0.4/24	500	5	60	5201
UDP	10.0.0.2/24	10.0.0.4/24	500	5	60	5202
UDP	10.0.0.3/24	10.0.0.4/24	500	5	60	5203

Tabla 28. características de los flujos.

¿Cómo se reparte el ancho de banda?¿Cómo influye el tamaño de los paquetes en el reparto del ancho de banda?¿Qué ocurre con el porcentaje de paquetes perdidos?

Calcule como debería quedar repartido teóricamente a partir del ancho de banda total obtenido mediante wireshark y compruebe si los resultados obtenidos son los esperados:

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

La figura 65 muestra el tamaño de los paquetes que hay en cada cola cuando se produce congestión, así como el peso de cada cola.

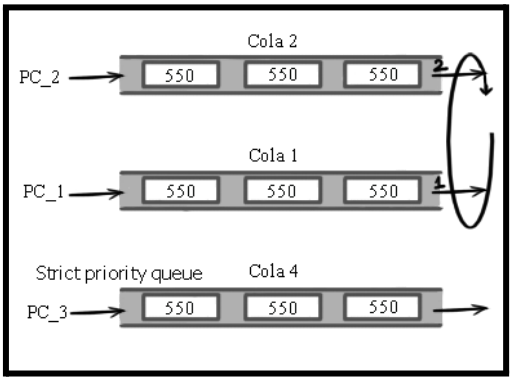


Figura 65. Resumen visual del ejercicio 6.

Copiad la gráfica obtenida mediante wireshark a continuación:

Solución:

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_1:

```
iperf3.exe -c 10.0.0.4 -u -p 5201 -b 5M -l 500 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_2:

```
iperf3.exe -c 10.0.0.4 -u -p 5202 -b 5M -l 500 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_3:

```
iperf3.exe -c 10.0.0.4 -u -p 5203 -b 5M -l 500 -t 60
```

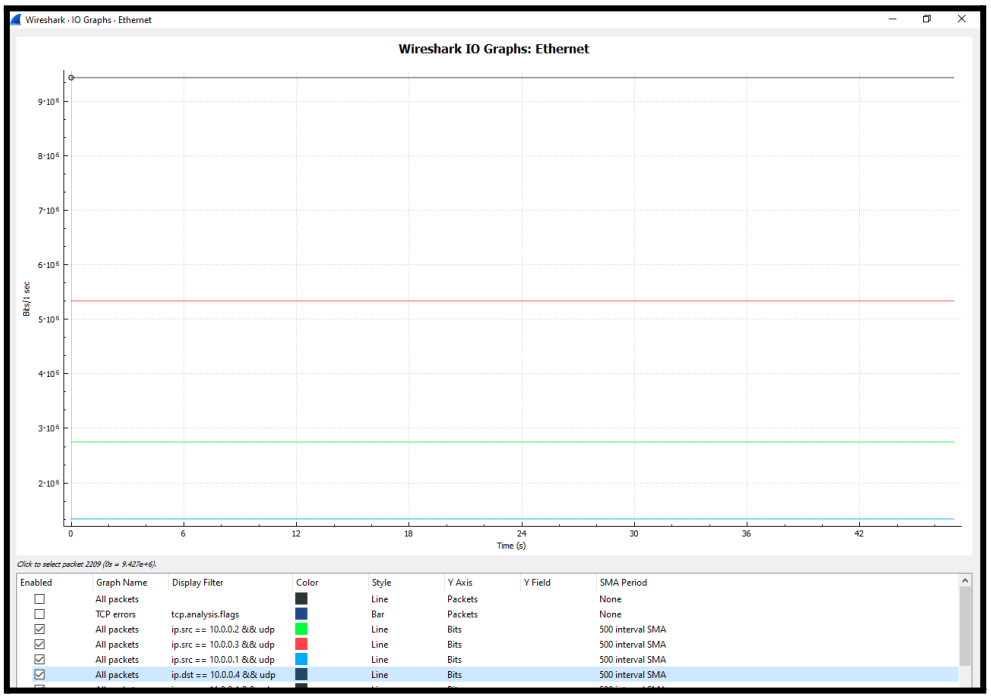


Figura 66.Comportamiento de los flujos obtenidos mediante Wireshark.

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

En la captura obtenida mediante wireshark (figura 66), observamos que el ancho de banda se reparte de la de la forma indicada por la tabla 29:

	Ancho de banda	Peso	Prioridad
PC_1	1,34 Mbps	1	-
PC_2	2,751 Mbps	2	
PC_3	5,337 Mbps	0	+
Total	9,427 Mbps		

Tabla 29. Resultados obtenidos mediante Wireshark.

Calculamos el ancho de banda teórico en este caso a partir de (5) y (6):

Al tamaño de paquete especificado hay que añadirle 20 bytes de la cabecera IP, 22 bytes de la cabecera ethernet y 8 bytes de la cabecera UDP, quedando: 550 B.

Ancho de banda PC_3 = 5,337 Mbps.
Ancho de banda WRR = 9,427 Mbps - 5,337 Mbps = 4,09 Mbps.
Ancho de banda PC_1 = $4{,}09 * \frac{1*550}{1*550+2*550} = 4{,}09 * \frac{1}{1+2} = 1{,}36$ Mbps
Ancho de banda PC_2 = $4{,}09 * \frac{2*550}{1*550+2*550} = 4{,}09 * \frac{2}{1+2} = 2{,}73$ Mbps.

Por lo tanto, observamos que PC_3 que funciona con PQ transmite todos los paquetes y el ancho de banda restante se distribuye entre las colas que funcionan con WRR exactamente en función de sus pesos, porque el tamaño de paquete de las colas que funcionan en modo WRR es el mismo. Por lo tanto, concuerda con el resultado esperado.

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-60.01  sec  35.7 MBytes  4.99 Mbits/sec  0.302 ms  52727/74901 (70%)
[  4] Sent 74901 datagrams
```

Figura 67. Porcentaje pérdidas PC_1.

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-60.00  sec  35.7 MBytes  4.99 Mbits/sec  2.360 ms  33866/74883 (45%)
[  4] Sent 74883 datagrams
```

Figura 68. Porcentaje pérdidas PC_2.

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-60.01  sec  35.7 MBytes  4.99 Mbits/sec  2.309 ms  0/74902 (0%)
[  4] Sent 74902 datagrams
```

Figura 69. Porcentaje pérdidas PC_3.

A partir de las figuras 67, 68 y 69 podemos observar que la cola que funciona con PQ no presenta pérdidas a diferencia de las colas que funcionan en modo WRR, de entre las que observamos que el flujo de tráfico proveniente de PC_2 presenta menos pérdidas, porque se le ha asignado un peso mayor “2” respecto del asignado al flujo de PC1 “1”.

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

Ejercicio 7: La cola que funciona en PQ es capaz de congestionar la red por sí sola.

En la figura 70 se puede observar el ancho de banda utilizado por los distintos enlaces.

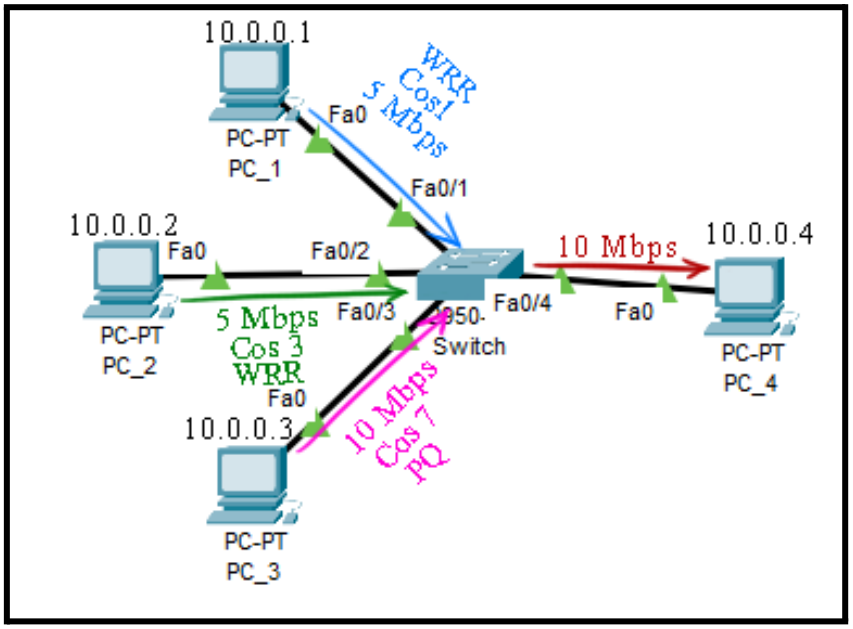


Figura 70 Topología de red del ejercicio 7.

Cada cliente debe generar tráfico con los perfiles especificados en la tabla 30:

Protocolo	IP origen	IP destino	Tamaño de paquete	Bitrate (Mbps)	Tiempo de generación del flujo (s)	Puerto
UDP	10.0.0.1/24	10.0.0.4/24	300	5	60	5201
UDP	10.0.0.2/24	10.0.0.4/24	700	5	60	5202
UDP	10.0.0.3/24	10.0.0.4/24	500	10	60	5203

Tabla 30. características de los flujos.

El tráfico debe de ser capturado por PC_4 mediante wireshark.

¿Qué ocurre con el ancho de banda disponible? ¿A qué se debe?

La figura 71 muestra el tamaño de los paquetes que hay en cada cola cuando se produce congestión, así como el peso de cada cola.

3.2 Escenario 1: Calidad de servicio (QoS) mediante el switch de cisco 2950.

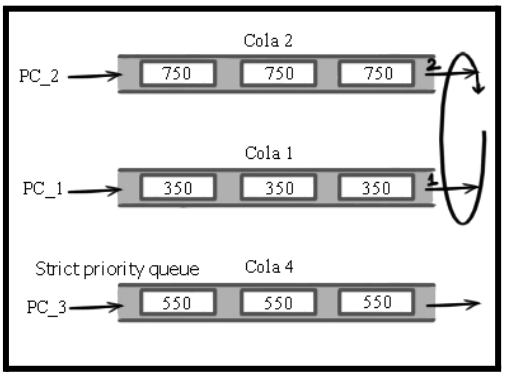


Figura 71. Resumen visual del ejercicio 7.

Copiad la gráfica obtenida mediante wireshark a continuación:

Solución:

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_1:

```
iperf3.exe -c 10.0.0.4 -u -p 5201 -b 5M -l 300 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_2:

```
iperf3.exe -c 10.0.0.4 -u -p 5202 -b 5M -l 700 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_3:

```
iperf3.exe -c 10.0.0.4 -u -p 5203 -b 5M -l 500 -t 60
```

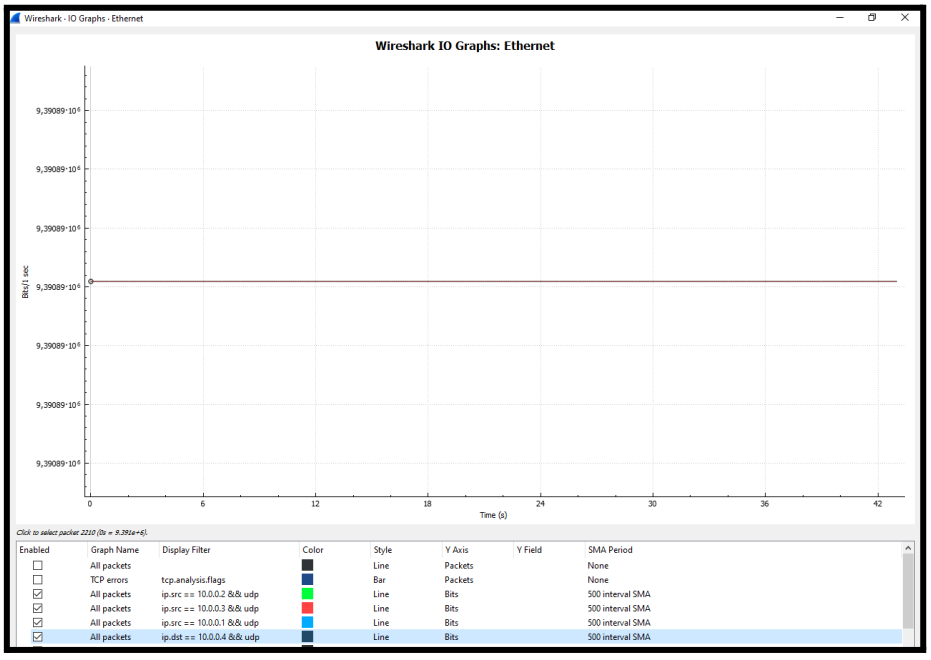


Figura 72.Comportamiento de los flujos obtenidos mediante Wireshark.

Como podemos observar en la captura (figura 72), prácticamente el flujo más prioritario es el único que transmite paquetes, ya que mientras tenga paquetes en cola no dejará servir paquetes de las colas que sirven paquetes en modo WRR.

3.3 Escenario 2: Calidad de servicio (QoS) mediante el router de cisco 1921.

3.3.1 Introducción:

En esta segunda parte vamos a observar cómo actúa el **planificador Class Based Weighted Fair Queueing (CBWFQ) del router 1921 de cisco**.

El planificador **WFQ** funciona como el planificador WRR pero a nivel de bit en lugar de paquetes. Por lo tanto, este planificador es **capaz de calcular correctamente el ancho de banda que le corresponde a cada flujo en función de los pesos asignados a todos los flujos**, independientemente de si los paquetes tienen un tamaño variable o no.

A pesar de que no es posible implementar el planificador WFQ actualmente, se han realizado implementaciones que no funcionan exactamente igual que el planificador WFQ.

El planificador CBWFQ es una implementación de WFQ que funciona de la misma forma que WFQ, pero teniendo en cuenta que en este caso el peso no es asignado a los distintos flujos de forma individual. En este caso, los flujos deben ser clasificados, y en función de la clase a la que pertenecen irán a parar a una cola a la que se le asigna un peso correspondiente a esa clase.

En este caso, se utilizan **tres colas diferentes, una para cada perfil de tráfico distinto**. De esta forma, se utiliza **una cola** para los paquetes marcados con el **valor Precedence 1**, **otra** para aquellos marcados con el **valor Precedence 3** y **la última** para aquellos paquetes marcados con **Precedence 7.**

A la hora de configurar **CBWFQ** se ha de indicar el **mínimo ancho de banda que en caso de congestión se debe de garantizar para cada tipo de clase.** Cabe destacar, que es necesario que se le asigne por lo menos un 1% del ancho de banda, a la clase por defecto.

CBWFQ ha sido configurado de la forma indicada en la tabla 31:

Cola	Marcado Asignado	Peso
Cola 1	Precedence 1	1
Cola 2	Precedence 3	2
Cola 3	Precedence 7	3

Tabla 31. Marcado correspondiente a cada PC.

3.3 Escenario 2: Calidad de servicio (QoS) mediante el router de cisco 1921.

3.3.2 Topología y elementos a utilizar:

Para comprobar los efectos de CBWFQ se ha diseñado la siguiente topología que consta de los siguientes elementos:

- 1 x Switch Cisco 2950.
- 1 x Router 1921.
- 4 x PC.
- 5x cable de red (Ethernet).

Topología a montar:

La figura 73 muestra la topología de red que se deberá montar.

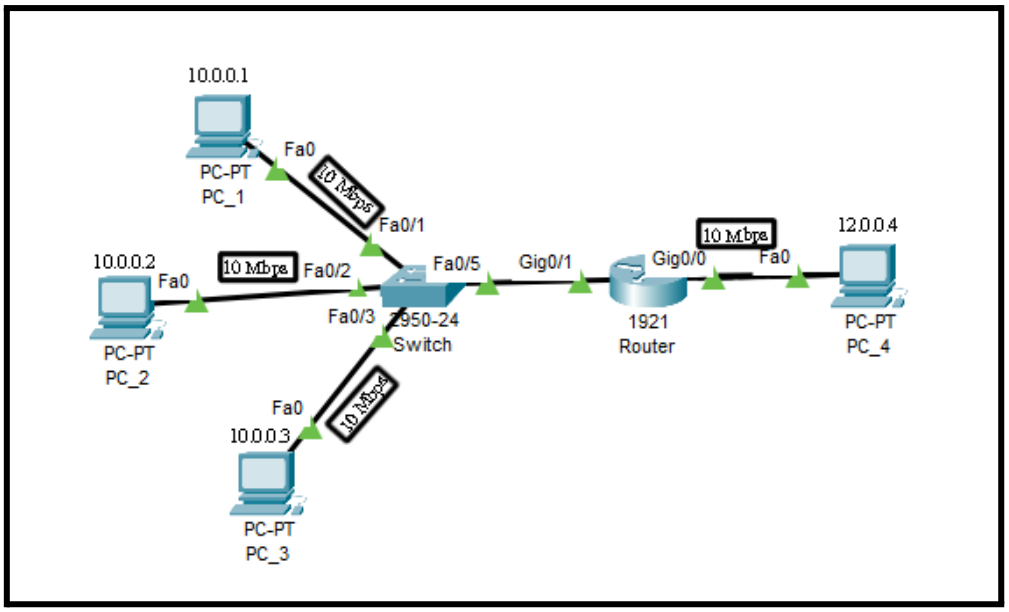


Figura 73. Topología de red del segundo escenario

La tabla 32 indica las características de red de los PCs:

Equipo.	Interfaz.	Dirección IP.	Máscara	Gateway
PC_1	NIC	10.0.0.1	255.255.255.0	10.0.0.10
PC_2	NIC	10.0.0.2	255.255.255.0	10.0.0.10
PC_3	NIC	10.0.0.3	255.255.255.0	10.0.0.10
PC_4	NIC	12.0.0.4	255.255.255.0	12.0.0.12

Tabla 32. características de las configuraciones de red de los PCs.

Se han configurado los PCs de la forma indicada en la tabla 32.

3.3.3 Montaje y configuración de la red:

A partir del montaje del primer escenario, se ha **desconectado el cable que conecta el puerto fastethernet 0/4 del switch con el PC4** y se ha conectado **PC4 con el puerto gigabitethernet 0/0 del router.** Además, **se ha conectado el puerto fastethernet 0/5 con el puerto gigabitethernet 0/1 del router.**

El montaje debe quedar de la forma indicada por la figura 74:

Figura 74. Montaje de la topología de red.

La configuración del router presenta las direcciones IP para que haya conectividad, la configuración del planificador CBWFQ, que se ha configurado en la salida de la interfaz gigabit ethernet 0/0, y finalmente la configuración para que el enlace gigabit ethernet 0/0 funcione a 10 Mbps. Dicha configuración se encuentra en el apartado “Anexo C”.

3.3.4 Actividades prácticas:

Caso de estudio: Class Based Weighted Fair Queueing (CBWFQ).

El caso a estudiar en el router consiste en observar cómo actúa el gestor de cola CBWFQ en un entorno de congestión. En este ejercicio se han trabajado 2 casos en los cuales se podrán comprobar las propiedades de dicho gestor de colas.

Estos casos son:

1. **Paquetes con el mismo tamaño en los tres flujos.**
2. **Paquetes con distinto tamaño en los tres flujos.**

3.3 Escenario 2: Calidad de servicio (QoS) mediante el router de cisco 1921.

Herramientas de QoS que se utilizarán:

Marcado:

En este caso el marcado se hace en el **switch a nivel 2**, en la capa de enlace. Para ello se asigna el valor del campo pcp, que pertenece al campo TCI de la etiqueta 802.11q (Vlan tag), con un valor de Cos de entre 0 y 7.

Este valor de CoS asignado se mapeará al campo IP Precedence dentro del byte ToS, obteniendo un valor de precedence equivalente al de CoS marcado en el switch. Esto se debe a que el switch de cisco 2950 es capaz de entender el byte ToS de la cabecera IP, ya que en el caso que no entendiera el campo ToS, el marcado se perdería una vez el frame Ethernet saliera del switch.

El marcado utilizado en el switch, se dejará de la misma forma que en el ejercicio anterior (CoS 1, CoS 3 y CoS 7), dando lugar al marcado en el router indicado en la tabla 33.

	Marcado	Equivalencia
pc_1	Precedence 1	Priority
pc_2	Precedence 3	Flash
pc_3	Precedence 7	Network Control

Tabla 33. Marcado correspondiente a cada PC.

Colas:

En este caso, el tráfico es asignado a diferentes colas en función del valor de IP Precedence del campo IP.

La tabla 34 muestra la configuración de las colas.

Cola	Marcado Asignado	Modo de funcionamiento	Peso
Cola 1	Precedence 1	CBWFQ	1
Cola 2	Precedence 3	CBWFQ	2
Cola 3	Precedence 7	CBWFQ	3

Tabla 34. Estado de las colas del switch.

3.3 Escenario 2: Calidad de servicio (QoS) mediante el router de cisco 1921.

Ejercicio 8: Paquetes con el mismo tamaño en los tres flujos.

En la figura 75 se puede observar el ancho de banda utilizado por los distintos enlaces.

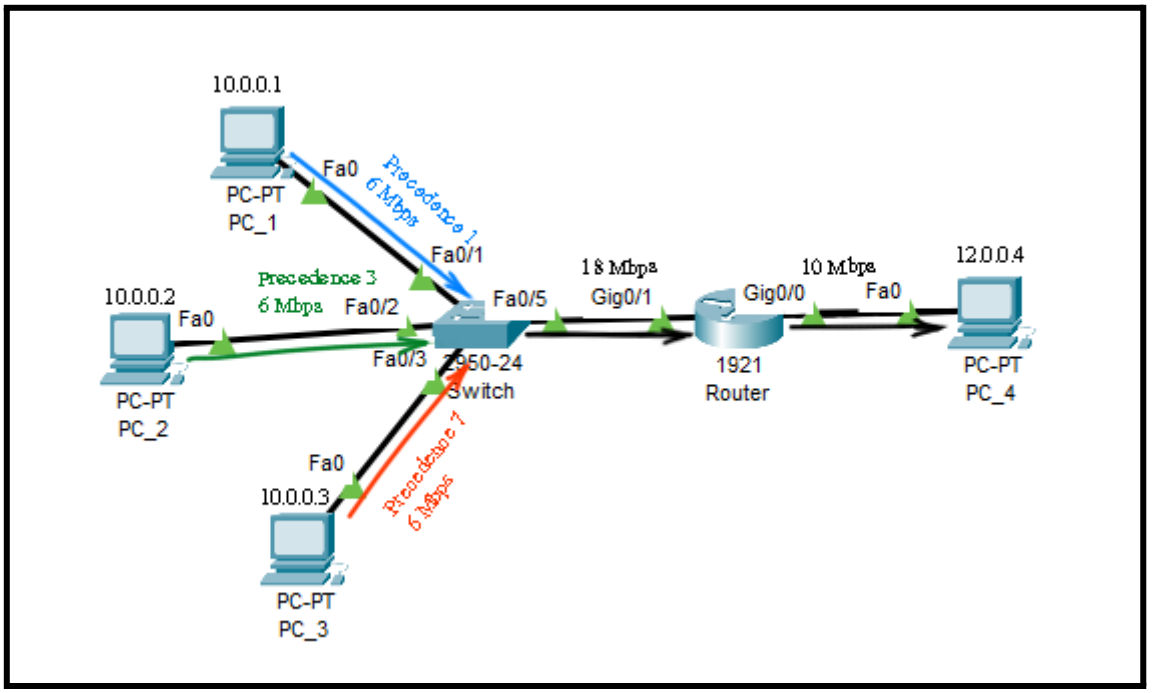


Figura 75. Topología de red del ejercicio 8.

Cada cliente debe generar tráfico con los perfiles indicados en la tabla 35:

Protocolo	IP origen	IP destino	Tamaño de paquete	Bitrate (Mbps)	Tiempo de generación del flujo (s)	Puerto
UDP	10.0.0.1/24	12.0.0.4/24	300	6	60	5201
UDP	10.0.0.2/24	12.0.0.4/24	300	6	60	5202
UDP	10.0.0.3/24	12.0.0.4/24	300	6	60	5203

Tabla 35. características de los flujos.

Una vez se observe que los tres PCs están emitiendo tráfico, se debe de capturar el tráfico recibido por PC_4, en PC_4 mediante wireshark. Para ello, se ha añadido el filtro: ip.dst == 12.0.0.4.

¿Coinciden las tasas de pérdidas obtenidas mediante los clientes del Iperf 3 con lo esperado? Explica los resultados obtenidos mediante wireshark:

Copiad la gráfica obtenida mediante wireshark a continuación:

3.3 Escenario 2: Calidad de servicio (QoS) mediante el router de cisco 1921.

Solución:

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_1:

```
iperf3.exe -c 12.0.0.4 -u -p 5201 -b 6M -l 300 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_2:

```
iperf3.exe -c 12.0.0.4 -u -p 5202 -b 6M -l 300 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_3:

```
iperf3.exe -c 12.0.0.4 -u -p 5203 -b 6M -l 300 -t 60
```

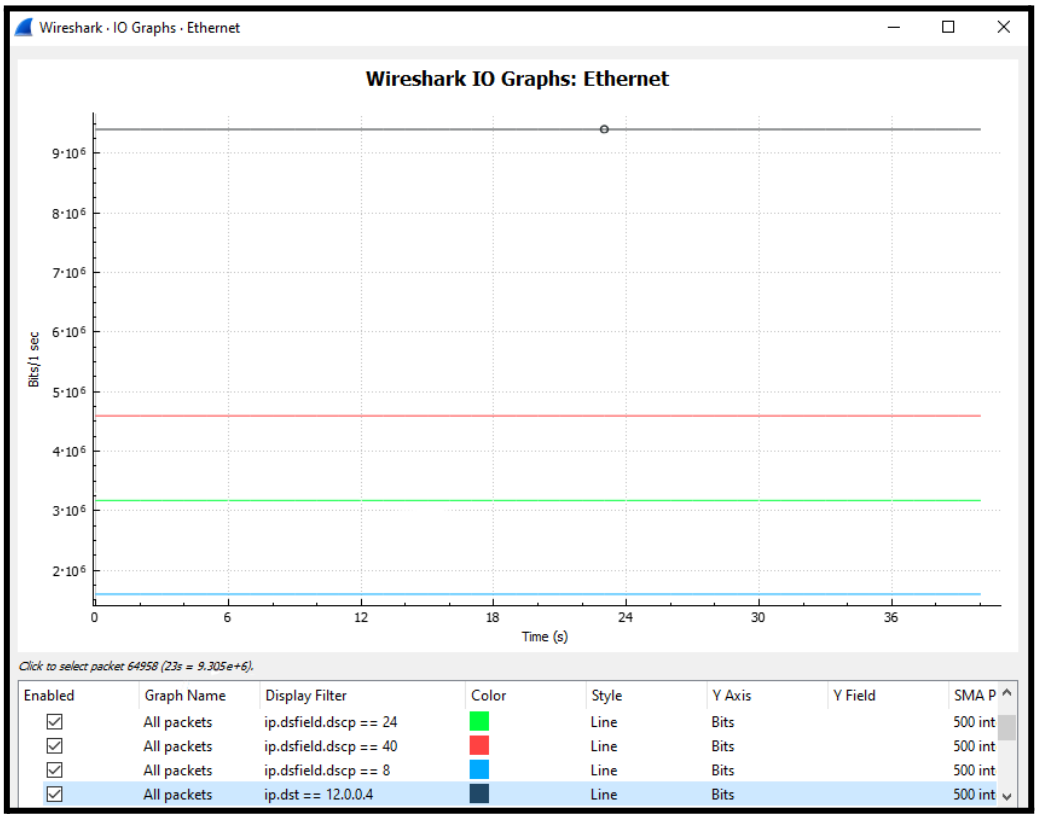


Figura 76. Comportamiento de los flujos obtenidos mediante Wireshark.

En la captura obtenida mediante wireshark (figura 76), observamos que el ancho de banda se reparte de la forma indicada en la tabla 36.

	Ancho de banda	Peso
PC_1	1,576 Mbps	1
PC_2	3,192 Mbps	2
PC_3	4,537 Mbps	3
Total	9,305 Mbps	

Tabla 36 Resultados obtenidos mediante Wireshark.

3.3 Escenario 2: Calidad de servicio (QoS) mediante el router de cisco 1921.

Calculamos el ancho de banda teórico en este caso a partir de (5), (6) y (7) sin tener en cuenta el tamaño de paquete de los flujos:

Ancho de banda PC_1 = 9,305* $\frac{1}{1+2}$ = 1,55 Mbps

Ancho de banda PC_2 = 9,305* $\frac{2}{1+2+3}$ = 3,1 Mbps.

Ancho de banda PC_2 = 9,305* $\frac{3}{1+2+3}$ = 4,65 Mbps.

Como podemos observar, los resultados varían ligeramente con los obtenidos teóricamente. Esto puede deberse a que a medida que se envían más paquetes, hay más bytes que no se capturan y a que el planificador no funciona con total exactitud.

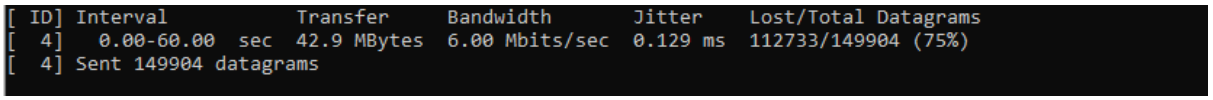


Figura 77. Porcentaje pérdidas PC_1.

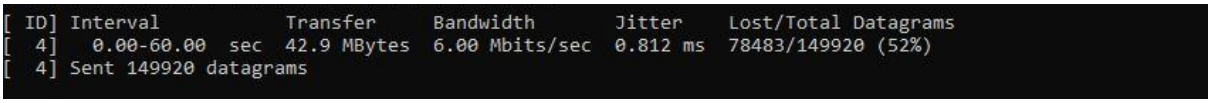


Figura 78. Porcentaje pérdidas PC_2.

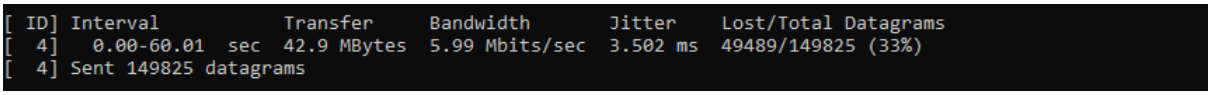


Figura 79. Porcentaje pérdidas PC_3.

Mediante Iperf 3 (figuras 77, 78 y 79), se puede comprobar que el porcentaje de pérdidas es el esperado, porque la diferencia de los porcentajes de PC_1 y PC_ 2 (23%) es parecida a la diferencia de los porcentajes de PC_2 y PC_3 (19%). Lógicamente, la diferencia debería ser la misma, porque en ambos casos coincide la diferencia entre los pesos. La diferencia se debe principalmente a que no es posible que las tres fuentes generen paquetes al mismo tiempo, alterando ligeramente el resultado porque uno de los PCs comienza a emitir antes de que se produzca congestión.

3.3 Escenario 2: Calidad de servicio (QoS) mediante el router de cisco 1921.

Ejercicio 9: Paquetes con distinto tamaño en los tres flujos.

En la figura 80 se puede observar el ancho de banda utilizado por los distintos enlaces.

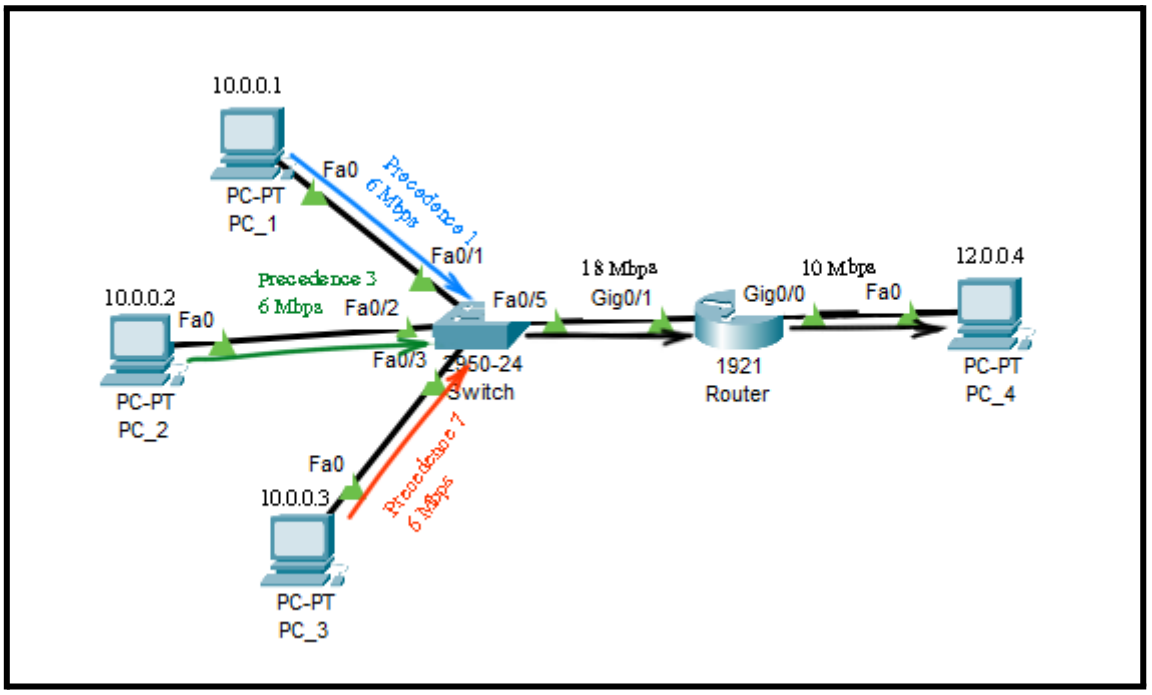


Figura 80. Topología de red del ejercicio 9.

Cada cliente debe generar tráfico con los perfiles especificados en la tabla 37:

Protocolo	IP origen	IP destino	Tamaño de paquete	Bitrate (Mbps)	Tiempo de generación del flujo (s)	Puerto
UDP	10.0.0.1/24	12.0.0.4/24	1300	6	60	5201
UDP	10.0.0.2/24	12.0.0.4/24	700	6	60	5202
UDP	10.0.0.3/24	12.0.0.4/24	300	6	60	5203

Tabla 37. características de los flujos.

Una vez se observe que los tres PCs están emitiendo tráfico, se debe de capturar el tráfico recibido por PC_4 mediante wireshark.

¿Coinciden las tasas de pérdidas obtenidas mediante los clientes del Iperf 3 con lo esperado? Explica los resultados obtenidos mediante wireshark:

Copiad la gráfica obtenida mediante wireshark a continuación:

3.3 Escenario 2: Calidad de servicio (QoS) mediante el router de cisco 1921.

Solución:

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_1:

```
iperf3.exe -c 12.0.0.4 -u -p 5201 -b 6M -l 1300 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_2:

```
iperf3.exe -c 12.0.0.4 -u -p 5202 -b 6M -l 700 -t 60
```

Para resolver este ejercicio, se ha utilizado el siguiente comando desde PC_3:

```
iperf3.exe -c 12.0.0.4 -u -p 5203 -b 6M -l 300 -t 60
```

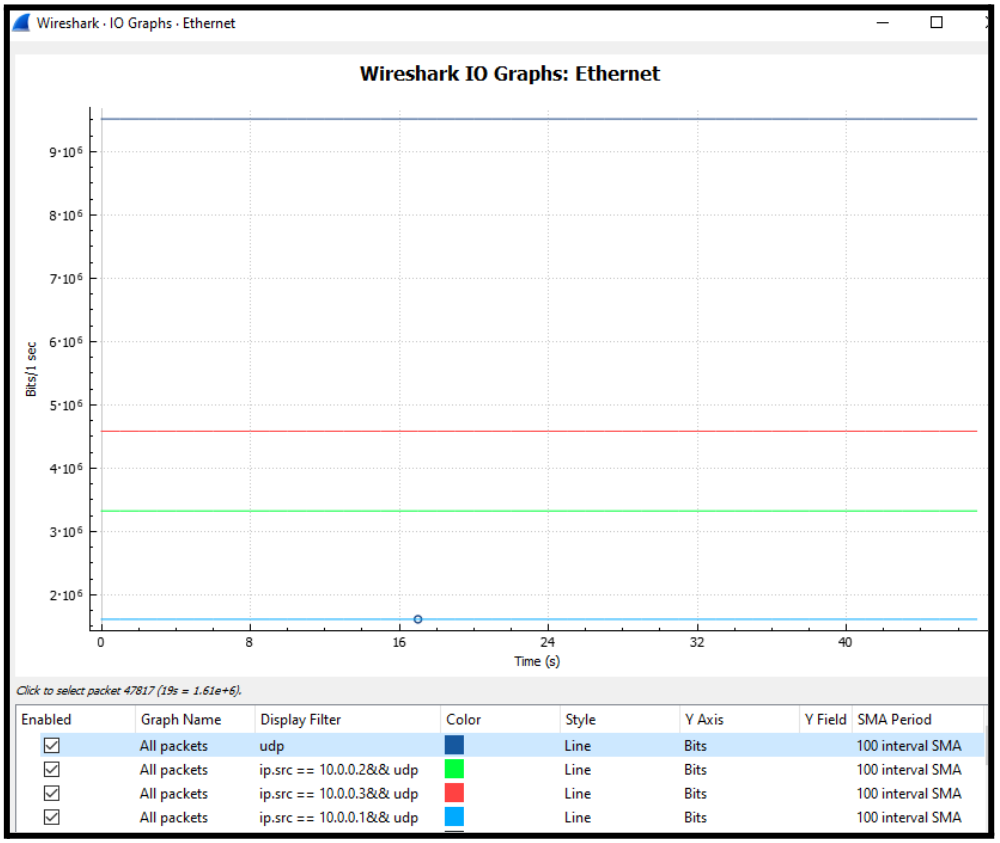


Figura 81.Comportamiento de los flujos obtenidos mediante Wireshark.

En la captura obtenida mediante wireshark (figura 81), observamos que el ancho de banda se reparte de la forma indicada en la tabla 38:

	Ancho de banda	Peso
PC_1	1,61 Mbps	1
PC_2	3,322 Mbps	2
PC_3	4,582 Mbps	3
Total	9,516 Mbps	

Tabla 38. Resultados obtenidos mediante Wireshark.

3.3 Escenario 2: Calidad de servicio (QoS) mediante el router de cisco 1921.

Como podemos observar, la forma en la que se reparte el ancho de banda ha variado poco respecto del ejercicio anterior. Por lo tanto, podemos asegurar que el tamaño de paquete no tiene influencia en el caso de CBWFQ.

Calculamos el ancho de banda teórico en este caso:Calculamos el ancho de banda teórico en este caso a partir de (5), (6) y (7) sin tener en cuenta el tamaño de paquete de los flujos:

Ancho de banda PC_1 = 9,516* $\frac{1}{1+2+3}$ = 1,586 Mbps

Ancho de banda PC_2 = 9,516* $\frac{2}{1+2+3}$ = 3,172 Mbps.

Ancho de banda PC_2 = 9,516* $\frac{3}{1+2+3}$ = 4,758 Mbps.

Observamos que los resultados teóricos se acercan mucho al resultado obtenido mediante Wireshark. La diferencia se debe a los bytes que Wireshark no puede capturar.

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-60.00  sec  42.9 MBytes  6.00 Mbits/sec  8.858 ms  24829/34613 (72%)
[  4] Sent 34613 datagrams
```

Figura 82. Porcentaje pérdidas PC_1.

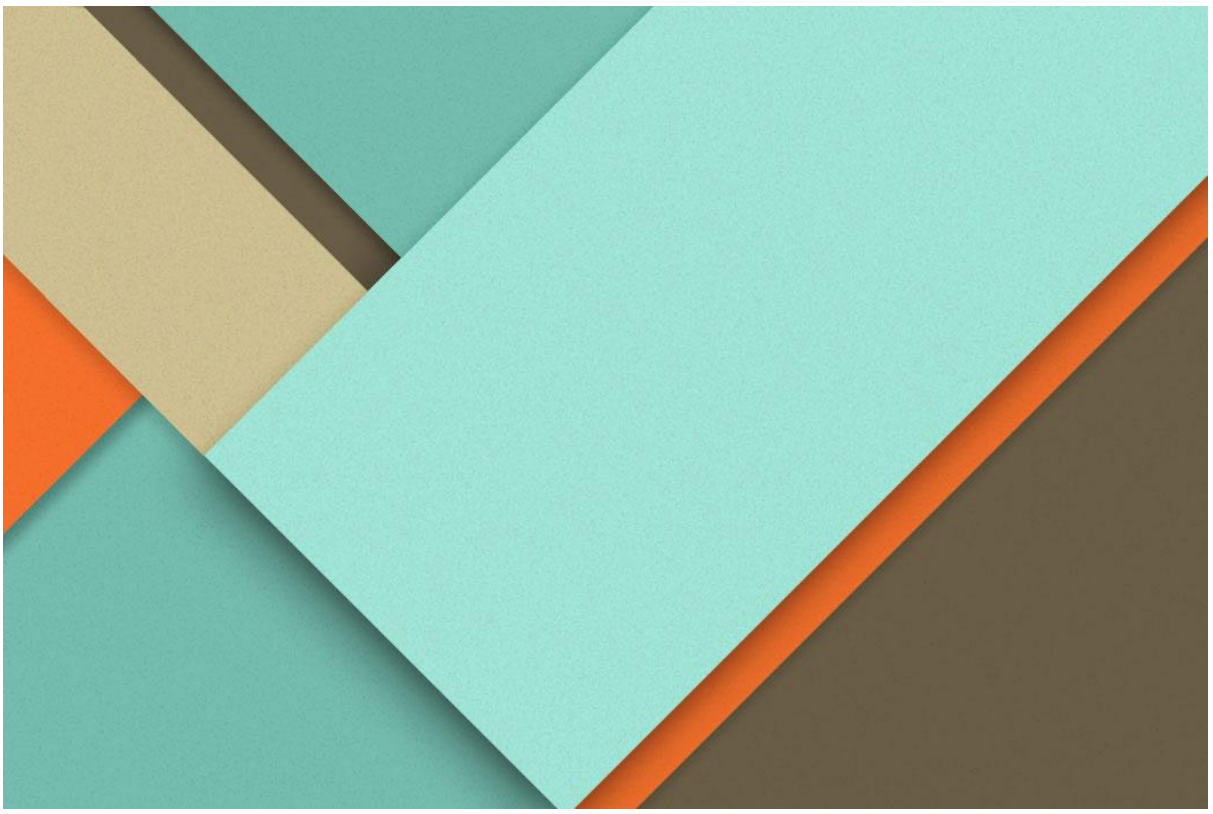
```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-60.01  sec  42.9 MBytes  5.99 Mbits/sec  6.392 ms  29792/64197 (46%)
[  4] Sent 64197 datagrams
```

Figura 83. Porcentaje pérdidas PC_2.

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-60.00  sec  42.9 MBytes  6.00 Mbits/sec  0.192 ms  47971/149899 (32%)
[  4] Sent 149899 datagrams
```

Figura 84. Porcentaje pérdidas PC_3.

Mediante Iperf 3 (figuras 82, 83 y 84), se puede comprobar que el porcentaje de pérdidas ha variado un poco, porque la diferencia de los porcentajes de PC_1 y PC_ 2 (25%) es algo mayor a la diferencia de los porcentajes de PC_2 y PC_3 (15%). La diferencia debería ser la misma, pero hay un incremento del error, puesto que ahora es del 10% respecto del 4% del ejercicio anterior. Esto se debe principalmente a que no es posible que las tres fuentes generen paquetes al mismo tiempo, alterando el resultado porque uno de los PCs comienza a emitir antes de que se produzca congestión.



Capítulo 4: Funciones Policía y Marcado DSCP en Routers CISCO

Capítulo 4. Funciones policía y marcado DSCP en Routers Cisco.

En este capítulo se va a observar la **degradación en la transmisión de un fichero de audio y un fichero de vídeo con audio a causa de la congestión en la red, así como, la mejora que se obtiene al utilizar funciones policía adecuadamente bajo las mismas condiciones**.

Para lograr estos objetivos se han preparado **dos escenarios** distintos:

El primer escenario consiste en la degradación de un fichero de audio codificado en G.711. En este caso, **se ha reducido el ancho de banda de los enlaces en los que se desea producir congestión a 128 kbps, debido al bajo bitrate que presenta el fichero de audio.**

El **segundo escenario** consiste en la **degradación de un fichero que contiene vídeo y audio.** Dicho fichero utiliza una cantidad del ancho de banda muy superior al del primer escenario. En este caso se ha **limitado el ancho de banda de los enlaces en los que se produce congestión a 10 Mbps.**

En ambos casos, la topología de red se mantiene, y solamente se ha de modificar la configuración de los routers.

Para el montaje de dicha topología, se han utilizado los siguientes elementos:

- 3 x Router Cisco 1921.
- 3 x PC.
- 6x cable de red (Ethernet).
- 3 x módulo HWIC-4ESW.

Estos elementos se han conectado como indica la figura 85:

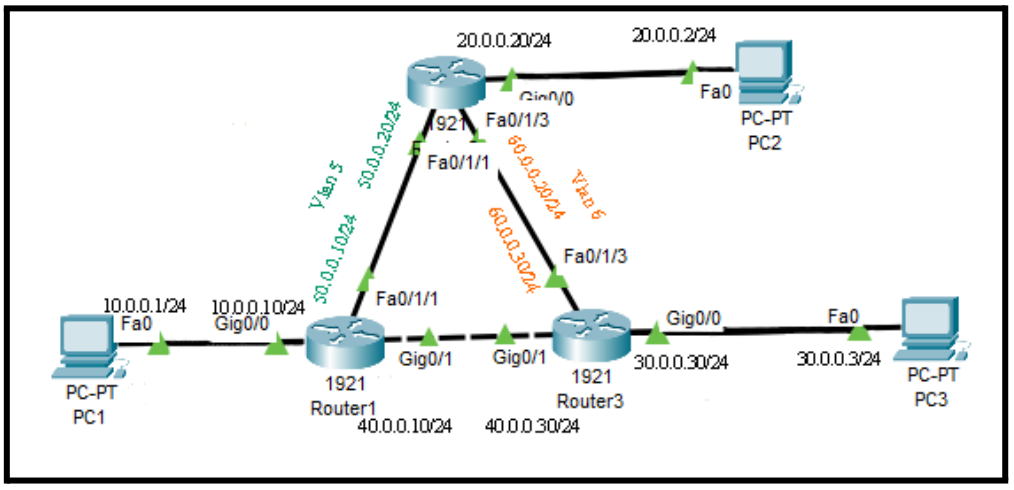


Figura 85. Topología de red.

4.1 Configuración de los equipos:

La tabla 39 muestra la configuración que deben tener los equipos para una correcta conectividad entre los mismos.

Equipo.	Interfaz.	Dirección IP.	Vlan	Máscara	Gateway
Router1	Gig0/0	10.0.0.10	-	255.255.255.0	-
	Gig0/1	40.0.0.10	-	255.255.255.0	-
	Fa0/1/1	50.0.0.10	Vlan 5	255.255.255.0	-
Router2	Gig0/0	20.0.0.20	-	255.255.255.0	-
	Fa0/1/1	50.0.0.20	Vlan 5	255.255.255.0	-
	Fa0/1/3	60.0.0.20	Vlan 6	255.255.255.0	-
Router3	Gig0/0	30.0.0.30	-	255.255.255.0	-
	Gig0/1	40.0.0.30	-	255.255.255.0	-
	Fa0/1/3	60.0.0.30	Vlan 6	255.255.255.0	-
PC1	NIC	10.0.0.1	-	255.255.255.0	10.0.0.10
PC2	NIC	20.0.0.2	-	255.255.255.0	20.0.0.20
PC3	NIC	30.0.0.3	-	255.255.255.0	30.0.0.30

Tabla 39. características de las configuraciones de los equipos.

Las interfaces fast ethernet que proporcionan los módulos HWIC-4ESW son interfaces de capa 2, por lo que no es posible asignarle una dirección IP.

Una posibilidad para poder enrutar los paquetes que provienen de PC2 a PC1 o PC3 es asignar una dirección IP estática a la VLAN a la que pertenece el puerto de switch. De esa forma, el router será capaz de encaminar el tráfico por los interfaces de capa 2.

4.1 Configuración de los equipos:

- PC1:
  Sistema Operativo: Windows 10.
  Software necesario: Wireshark (analizador de tráfico).
  IPerf3 (generador de tráfico).
  Ffmpeg (codificador y decodificador de audio).
  VLC (receptor de audio)
- PC2:
  Sistema Operativo: Windows 10.
  Software necesario: IPerf3 (generador de tráfico).

4.1 Configuración de los equipos:

- PC3:

  Sistema Operativo: Windows 10.
  Software necesario: Wireshark (analizador de tráfico).
  IPerf3 (generador de tráfico).
  Ffmpeg (codificador y decodificador de audio).
  VLC (receptor de audio)

4.1.1 Configuración de los PCs:

Finalmente, se deben **configurar los PCs con las direcciones IP de la forma indicada en la tabla 40:**

Equipo.	Interfaz.	Dirección IP.	Máscara	Gateway
PC1	NIC (Network Interface Card)	10.0.0.1	255.255.255.0	10.0.0.10
PC2	NIC (Network Interface Card)	20.0.0.2	255.255.255.0	20.0.0.20
PC3	NIC (Network Interface Card)	30.0.0.3	255.255.255.0	30.0.0.30

Tabla 40. características de las configuraciones de red de los PCs.

4.1.2 Montaje y configuración de la red:

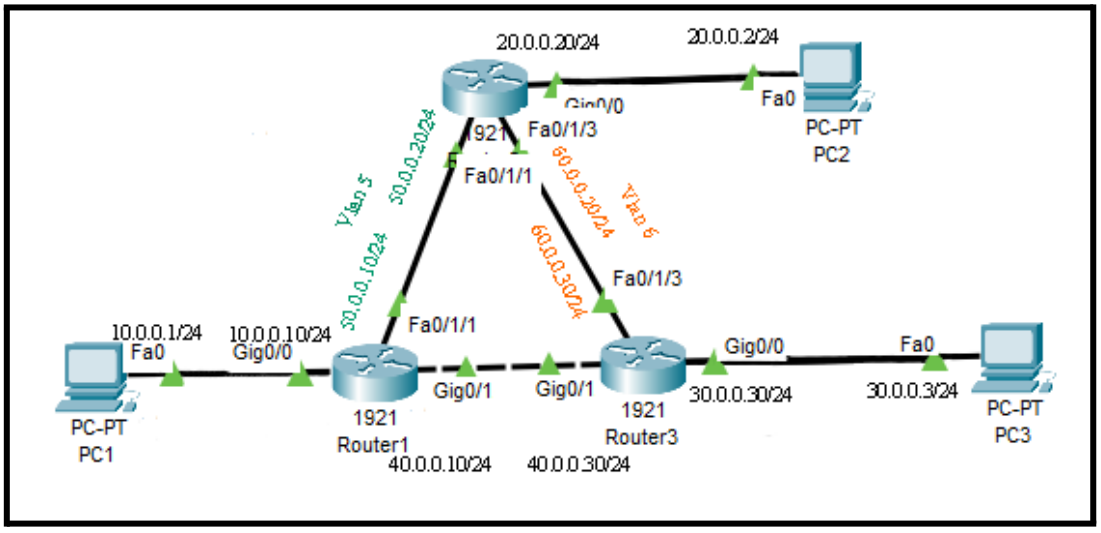


Figura 86. Topología de red.

Tras configurar los PCs se ha de conectar los distintos elementos que forman la topología de red (figura 86).

La figura 87 muestra la forma en que debe quedar el montaje:

4.2 Escenario 1: Degradación de un fichero de audio codificado en G.711.

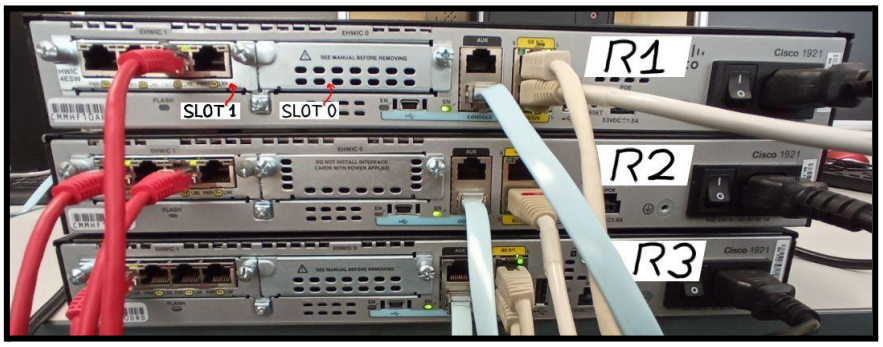


Figura 87. Montaje de la topología de red.

La figura 88 muestra las interfaces correspondientes al módulo de capa 2:

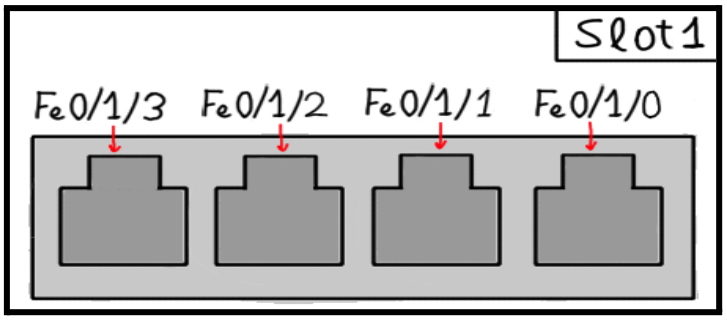


Figura 88. Interfaces correspondientes al módulo de capa 2..

Una vez montada la topología de red se han configurado los routers para aplicar las funciones policía que se detallarán en los apartados 3.2 y 3.3. La configuración de los routers se puede encontrar con sus respectivos comentarios en el apartado "ANEXO D".

4.2 Escenario 1: Degradación de un fichero de audio codificado en G.711.

En el primer escenario se va a poder observar cómo se **degrada un fichero de audio codificado en G.711 en una situación de congestión, en el caso de que no se utilice QoS para garantizar dicha transmisión de audio. Además, se observará la forma en que se comportan los flujos transmitidos en condiciones similares, en el caso de que se utilice QoS.**

Para poder apreciar estos efectos con mayor facilidad, se han **configurado los routers para estrechar el ancho de banda de los enlaces en los que se produce congestión a 128 kbps**.

El escenario queda de la siguiente forma (figura 89):

4.2 Escenario 1: Degradación de un fichero de audio codificado en G.711.

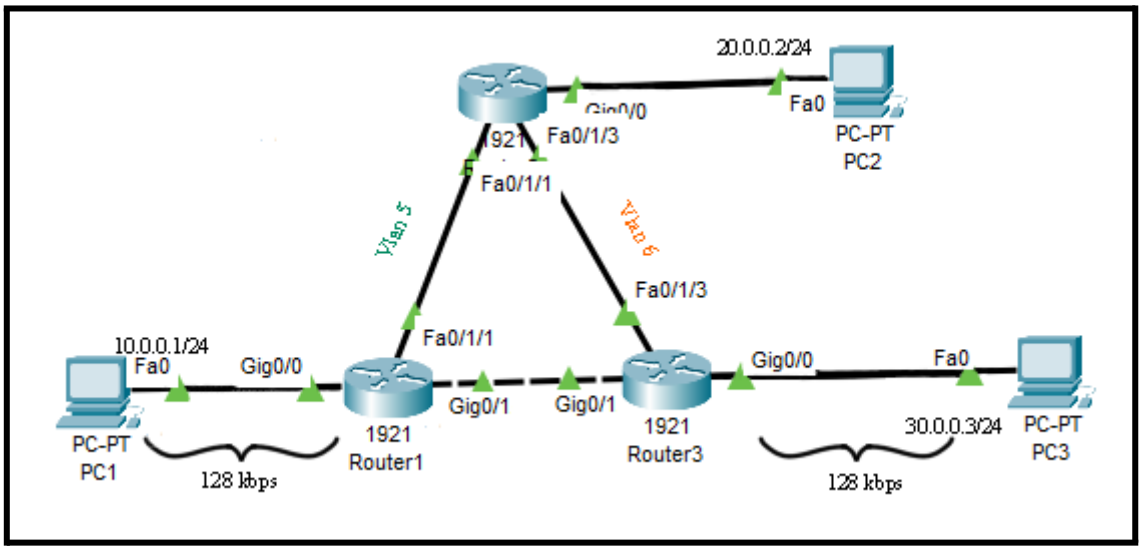


Figura 89. Topología de red del primer escenario.

4.2.1 Herramientas de QoS utilizadas en los routers:

Marcado: Hay diversas maneras de **diferenciar el tráfico**: valor de **CoS**, valor del campo **IP precedence**, **DSCP**, interfaz de entrada, interfaz de salida, IP origen, IP destino, dirección IP origen, dirección IP destino, Mac origen, Mac destino etc.

En este capítulo se va a realizar un **marcado a nivel 3, mediante el campo DSCP de la cabecera IP.** En concreto, **Router 3 marca los paquetes RTP/RTCP entrantes por la interfaz Gi0/0 con DSCP 46 (EF). Además, el resto de paquetes UDP y TCP provenientes de PC3 cuyo destino es PC1 se marcan con el valor DSCP 10 (AF11).**

Función policía:

Una función policía es una **herramienta de calidad de servicio capaz de controlar el tráfico que pasa a través de ella, ajustando dicho tráfico a una tasa deseada.**

Se puede distinguir entre hard policing y soft policing:

Hard policing consiste en descartar todo el tráfico que no se ajuste al perfil asignado.

Soft policing consiste en disminuir la prioridad del tráfico que no se ajuste al perfil asignado.

En este capítulo solamente se utiliza hard policing.

En el caso de los routers cisco 1921, las funciones policía utilizan el algoritmo “two rate Three Color Marker" (trTCM). Por lo tanto se debe indicar el CIR, CBS, PIR y PBS.

CIR: (Committed Information Rate): Tasa de tráfico que se garantiza para un flujo, en bits por segundo.

CBS: (Committed Burst Size): Tamaño máximo que debe tener una ráfaga de paquetes para que se ajuste al CIR, en bytes. El bucket se rellena en un cierto tiempo dependiendo del tamaño máximo de ráfaga especificado, como indica la siguiente expresión:

$$t_{rellena}(s) = \frac{CBS\ (Bytes)*8}{CIR(bps)} \quad (8)$$

PIR: (Peak Information Rate): Tasa de tráfico máxima permitida en un flujo, en bits por segundo. Por lo tanto, si un flujo supera dicha tasa de tráfico, los paquetes comenzarán a descartarse. El PIR debe de ser mayor o igual al CIR.

El PIR está formado por la tasa de tráfico que se garantiza (CIR) y la tasa de tráfico excedente no garantizada. De esta forma, la función policía puede ser configurada para tratar de distinta forma el tráfico garantizado, el excedente y el que no cumple con el PIR.

PBS: (Peak Burst Size): Tamaño máximo que debe tener una ráfaga de paquetes para que se ajuste al PIR, en bytes. El PBS debe de ser mayor o igual al CBS. El bucket se rellena en un cierto tiempo dependiendo del tamaño máximo de ráfaga especificado, como indica la siguiente expresión:

$$t_{rellena}(s) = \frac{PBS\ (Bytes)*8}{PIR(bps)} \quad (9)$$

En este proyecto el valor del PIR equivale al valor del CIR. Por lo tanto, si la tasa de tráfico emitida es superior a la que indica el CIR, se eliminará todo el tráfico que exceda la tasa indicada por el CIR.

Las funciones policía se pueden utilizar en la entrada y en la salida de una interfaz.

Cuando se utiliza una función policía en la **entrada** de una interfaz, afecta al tráfico que proviene **de otro equipo distinto (PC,router,switch…) hacia al propio router.**

Cuando se utiliza una función policía en la **salida** de una interfaz, afecta al tráfico que el propio **router transmite a otro equipo distinto (PC,router,switch…).**

La figura 90 muestra de una forma visual cuál debería ser el sentido del flujo, para que le afecte una función policía dependiendo de si esta se sitúa a la entrada o a la salida de una interfaz.

4.2 Escenario 1: Degradación de un fichero de audio codificado en G.711.

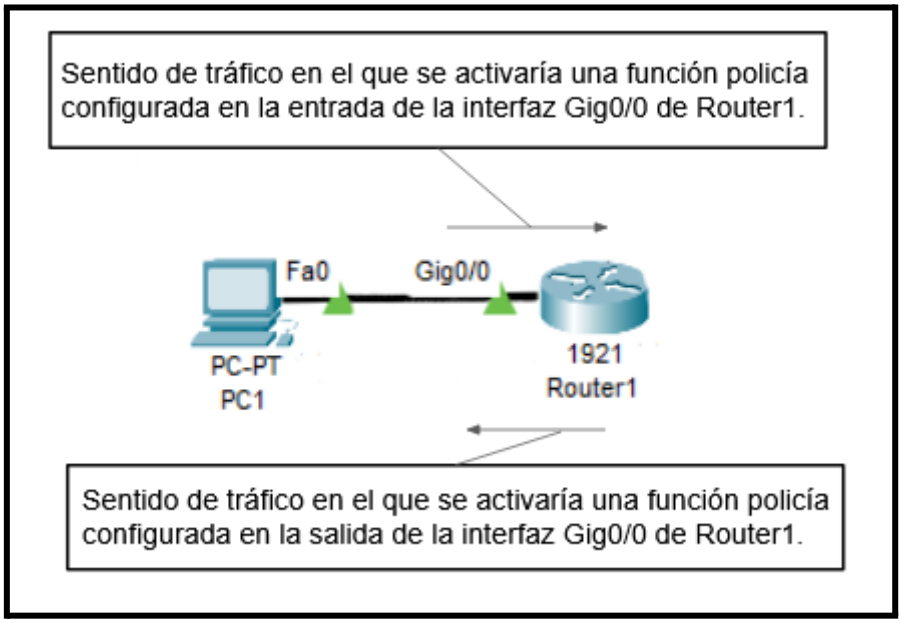


Figura 90. Funciones policía en interfaces.

Las funciones policía utilizadas son las indicadas en la tabla 41:

Router	Interfaz:	Entrada/Salida	Función
Router3	Gig0/0	Entrada	- Garantizar, marcar con DSCP EF y limitar a 88 kbps el tráfico RTP/RTCP/SIP proveniente de PC3. - Garantizar, marcar con DSCP AF11 y limitar a 12 kbps el restante tráfico UDP y TCP proveniente de PC3. - Garantizar y limitar a 28 kbps el resto del tráfico.
	Gig0/0	Salida	- Estrechar el ancho de banda a 128 kbps.
Router1	Gig0/0	Entrada	- Estrechar el ancho de banda a 128 kbps
	Gig0/0	Salida	- Garantizar y limitar a 100 kbps el tráfico proveniente de PC3. - Garantizar y limitar a 28 kbps el tráfico proveniente de PC2.

Tabla 41.Funciones policía configuradas en los equipos.

Las funciones policía son utilizadas para estrechar el ancho de banda a 128 kbps, ya que las interfaces Gigabit Ethernet presentan un ancho de banda mucho mayor (1 Gbps). Sin embargo, **partiendo de** que se consigue estrechar el ancho de banda a **128 kbps**, **las funciones policía son utilizadas para observar qué ocurre al priorizar los flujos de interés frente a cuando no se prioriza ningún flujo.** De esta forma, las funciones policía a considerar son las que se muestran en la figura 91.

4.2 Escenario 1: Degradación de un fichero de audio codificado en G.711.

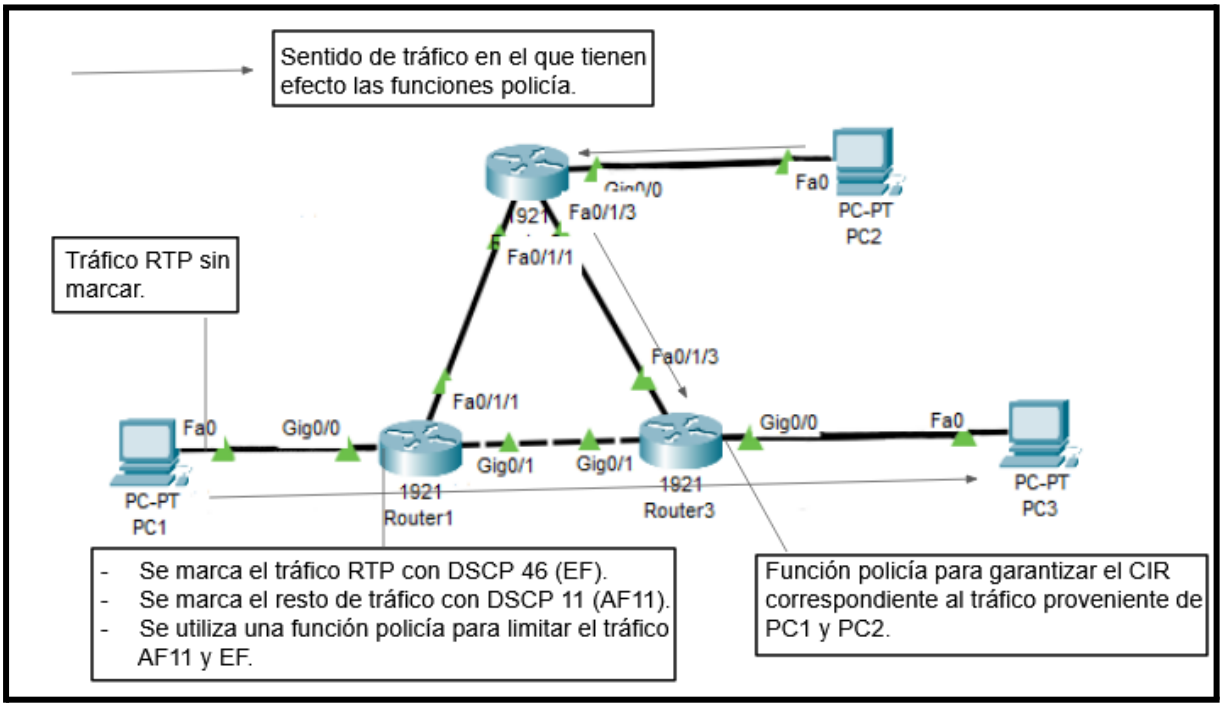


Figura 91. Sentido de tráfico en el que se aplica QoS para mejorar la calidad de experiencia de los usuarios.

La figura 92 muestra cómo quedan repartidos los flujos de acuerdo a las funciones policía.

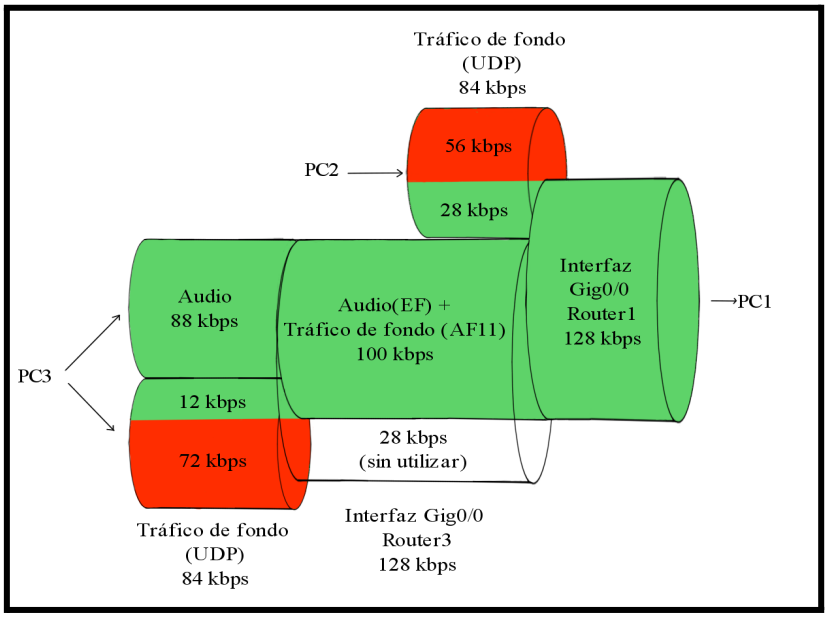


Figura 92. Comportamiento de los flujos de acuerdo a las funciones policía.

De acuerdo con la figura 92 distinguimos hasta tres flujos distintos.

1. **Flujos provenientes de PC3 con destino PC1:**

- Un flujo corresponde con el **fichero de audio codificado en G.711**. Dicho flujo llega **sin pérdidas a PC1 y es marcado con DSCP EF** en la entrada de la interfaz Gig0/0 de Router3.
- Otro flujo corresponde con el **tráfico de fondo (UDP)**. Dicho flujo solo es capaz de transmitir un máximo de **12 kbps** hacia PC3, esto se debe a que el resto del tráfico es descartado en la entrada de la interfaz Gig0/0 de Router3. El tráfico que se consigue transmitir queda **marcado con el valor DSCP AF11.**

2. **Flujo proveniente de PC2 con destino PC1:**

- Este flujo sólo es capaz de transmitir **28 kbps** a PC1, porque la interfaz Gig0/0 de Router1 limita este flujo a 28 kbps, descartando el tráfico restante.

4.2.2 Interacción entre equipos:

PC1: Emite un fichero de audio codificado en G.711 hacia PC3. Además, genera tráfico UDP con destino PC3, con la finalidad de saturar la red.

PC2: Genera tráfico UDP best effort con destino PC1 y PC3 con el objetivo de saturar la red.

PC3: Emite un fichero de audio codificado en G.711 hacia PC1. Además, genera tráfico UDP hacia PC1 para saturar la red.

Router3: En la entrada de la interfaz Gigabit Ethernet 0/0 marca el tráfico RTP/RTCP/SIP con el valor 46 del campo DSCP (EF) y el tráfico UDP y TCP restante con el valor 10 (AF11). Además, garantiza y limita el ancho de banda del tráfico RTP/RTCP a 88 kbps y del tráfico marcado con AF11 a 12 kbps. Finalmente, en la salida de la interfaz Gigabit Ethernet 0/0 limita todo el tráfico a 128 kbps.

Router2: Encamina el tráfico generado por PC2 a PC1 y a PC3. No utiliza QoS.

Router1: En la salida de la interfaz Gigabit Ethernet 0/0 garantiza y limita el ancho de banda recibido por PC3 a 100kbps y por PC2 a 28 kbps. Finalmente, en la entrada de la interfaz Gigabit Ethernet 0/0 limita todo el tráfico a 128 kbps.

4.2.3 Actividades Prácticas:

Para observar los efectos de la calidad de servicio (QoS) en la transmisión de un fichero de audio, se han realizado tres casos de estudio en los que se puede comprobar de forma gradual las mejoras que conllevan el uso de herramientas de QoS, frente a no utilizar dichas herramientas de QoS.

Estos casos de estudio son:

1. Comprobación de conectividad.
2. Congestión de la red tras añadir dos fuentes de tráfico externas (sin QoS).
3. Congestión de la red tras añadir dos fuentes de tráfico externas (con QoS).

4.2.3.1 Comprobación de conectividad:

Este primer caso de estudio consiste en la comprobación de que **los PCs y los routers se han conectado adecuadamente, transmitiendo el audio correctamente, sin pérdidas**. Además, se **observa** el teórico transmitido gráficamente **mediante Wireshark.**

La figura 93 muestra la ruta que seguirán los flujos emitidos.

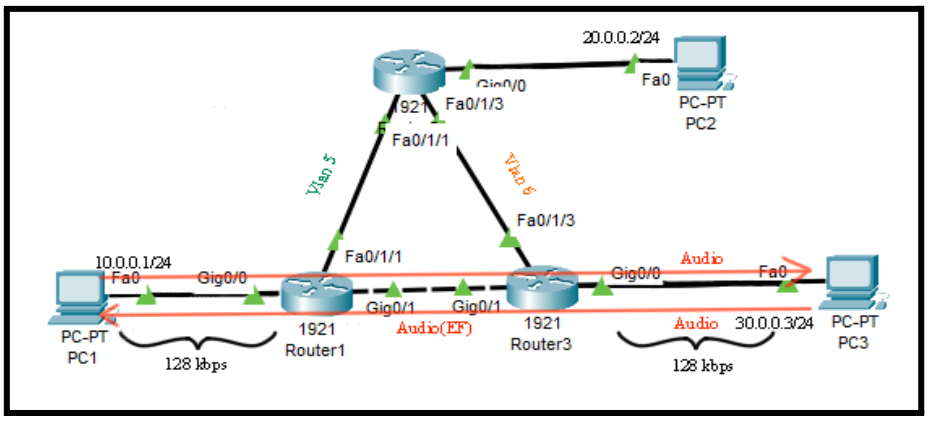


Figura 93. Topología de red y flujos a emitir.

Interacción entre equipos:

PC1: Emite un fichero de audio codificado en G.711 hacia PC3.

PC3: Emite un fichero de audio codificado en G.711 hacia PC1.

Router3: En la entrada de la interfaz Gigabit Ethernet 0/0 marca el tráfico RTP/RTCP/SIP con el valor 46 del campo DSCP (EF).

Router1: En este ejercicio simplemente encamina los paquetes que recibe.

4.2 Escenario 1: Degradación de un fichero de audio codificado en G.711.

Se emitirán dos flujos con las características indicadas en la tabla 42:

Flujo	Protocolo	IP origen	IP destino	Tamaño de paquete	Tiempo entre paquetes (ms)	Tiempo de generación del flujo (s)	Puerto
Audio	RTP	10.0.0.1/24	30.0.0.3/24	160	20	-	5005
Audio	RTP	30.0.0.3/24	10.0.0.1/24	160	20	-	5004

Tabla 42.Características de los flujos.

Para realizar este caso de estudio se debe de **generar el flujo de audio mediante ffmpeg, recibir el stream de audio mediante VLC y capturar el tráfico mediante Wireshark.**

1. **Para generar el flujo de audio mediante ffmpeg se han seguido los siguientes pasos:**

Paso 1. Abrir la aplicación "símbolo del sistema" (CMD).
Paso 2. El CMD se debe situar en la carpeta donde se encuentra el archivo ffmpeg.exe.

Para ello se debe utilizar el comando cd, seguido de la ruta donde se encuentra el archivo:

```
cd ruta-donde-se-encuentra-ffmpeg.exe
```

Paso 3. Se debe utilizar el siguiente comando (en el caso de que PC3 transmita, PC3→PC1):

```
ffmpeg.exe -re -stream_loop -1 -i audio.wav -f rtp -packetsize 172 "rtp://10.0.0.1:5004"
```

El comando **-re** transmite el fichero a la vez que se está reproduciendo.

El comando **-stream_loop -1** es utilizado para que el audio se vuelva a reproducir una vez se haya finalizado de forma ilimitada.

El comando **-i audio.wav** selecciona como input el fichero de audio.

El comando **-f rtp** indica que se va a utilizar el protocolo RTP.

El comando **-packetsize 172** indica el valor del tamaño del paquete (160 payload + 12 RTP)

El comando **"rtp://10.0.0.1:5004"** transmite el archivo a la dirección IP especificada, utilizando el puerto especificado.

Paso 4. Se debe utilizar el siguiente comando (en el caso de que PC1 transmita, PC1→PC3):

```
ffmpeg.exe -re -stream_loop -1 -i audio.wav -f rtp -packetsize 172 "rtp://30.0.0.3:5005"
```

4.2 Escenario 1: Degradación de un fichero de audio codificado en G.711.

2. **Para recibir el flujo de audio mediante VLC se han seguido los siguientes pasos:**

Paso 1. En la barra de menús de VLC, hacer clic en: Medio -- > Abrir ubicación de red, como indica la figura 94:

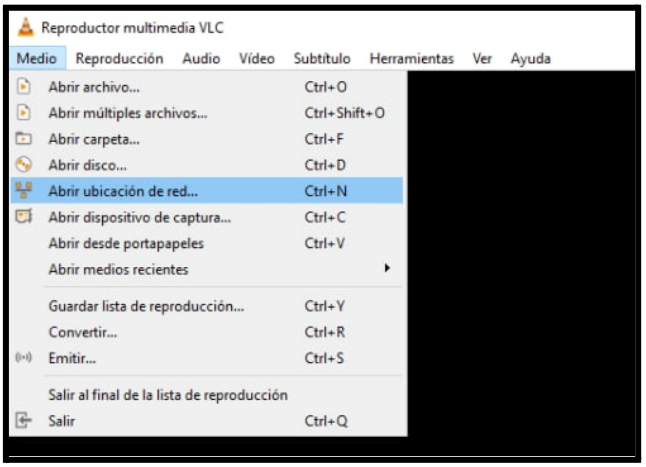


Figura 94. recibir un stream de audio mediante VLC parte 1.

Paso 2. En la ventana red, se debe introducir la URL de recepción del audio y pulsar "Reproducir".

Desde el PC que está recibiendo la transmisión de audio, se debe de introducir la URL para reproducir el audio*: rtp://IP_que_está_recibiendo_el_stream:puerto.*

La figura 95 muestra cómo PC3 cuya IP es 30.0.0.3/24 ha de introducir la URL para recibir la transmisión de PC1.

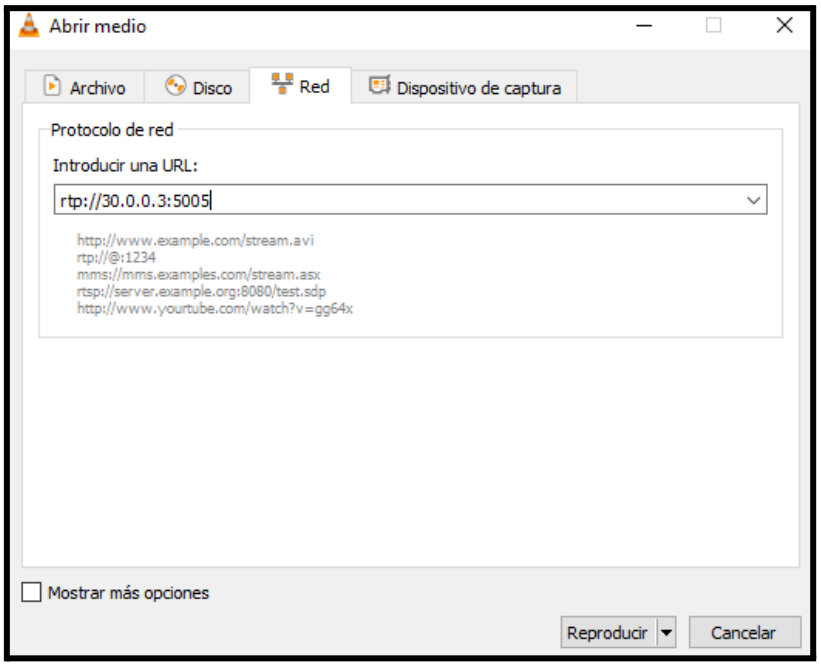


Figura 95. recibir un stream de audio mediante VLC parte 2.

Paso 3. Repetir los dos primeros pasos, para recibir el stream de audio en el sentido opuesto (Utilizando la IP y el puerto correspondiente).

3. **<u>Para capturar el flujo de audio mediante Wireshark se han seguido los siguientes pasos:</u>**

Paso 1. Una vez se ha terminado de capturar el tráfico de la interfaz ethernet, hacer clic en la opción "Gráficas de E/S" dentro del menú "Estadísticas".

Paso 2. Pulsar el icono "+" para crear un nuevo filtro.

Paso 3. Se debe capturar el tráfico proveniente desde PC1, en PC3. Para ello, en PC3 se debe utilizar el siguiente filtro:"ip.src == 10.0.0.1 && UDP.port == 5005". En la columna de Y Axis se debe indicar la opción de bits/segundo. Finalmente, en la columna SMA Period se le ha de asignar un valor de "500 interval SMA", para que se haga un promediado y el tráfico recibido sea una constante.

El filtro debe quedar como en la figura 96:

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Fiel	SMA Period	Y Axis Factor
☑	Todos los paqu...	ip.src == 10.0.0.1 && udp.port == 5005		Line	Bits		500 interval SMA	1

Figura 96. Filtro de captura de paquetes cuyo destino es PC3.

Paso 4. Repetir estos pasos para capturar el tráfico en PC1. Se puede utilizar el filtro ("ip.src == 30.0.0.3&& UDP.port == 5004").

<u>Ejercicio 1:</u> Calcule la tasa de transmisión del fichero de audio conociendo que está codificado con G.711 (paquetes de tamaño 160 Bytes, y el tiempo entre paquetes es equivalente a 20 ms). ¿Coincide aproximadamente con el resultado obtenido mediante wireshark, conociendo que Wireshark no captura los campos de preámbulo + delimitador de comienzo de trama ni el CRC de la cabecera ethernet?

Solución:

Tamaño de trama:

160 Bytes + 12 Bytes (RTP) + 8 Bytes(UDP) + 20 Bytes(IP) + 22 Bytes (Ethernet) =
= 222 Bytes
Intervalo entre tramas: 20 milisegundos
TASA: (222 Bytes * 8) bits / (20*10^-3) segundos = 88,8 kbps

4.2 Escenario 1: Degradación de un fichero de audio codificado en G.711.

Por lo tanto, mediante wireshark se debe poder observar un bitrate cercano a 88,8 kbps.

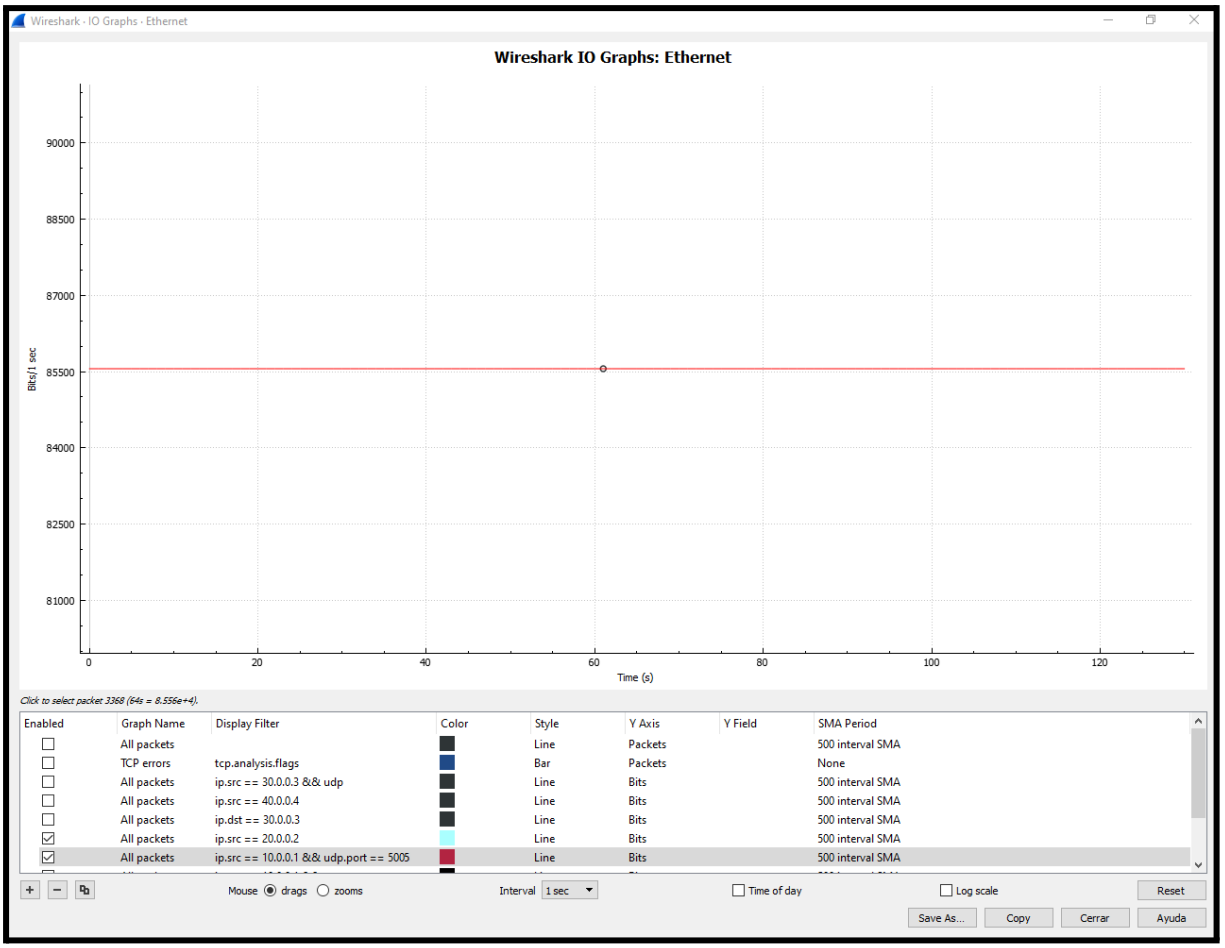


Figura 97.Captura del ancho de banda total utilizado.

Como se puede observar en la captura de Wireshark (figura 97), el promedio del ancho de banda utilizado por el stream de audio es de 85660 bps. Este resultado corresponde a lo esperado puesto que es un valor cercano a 88,8 kbps y ligeramente inferior a este, porque wireshark no captura los bytes de CRC (4 bytes) ni los bytes de preámbulo y delimitador de comienzo de trama (8 bytes), de la cabecera ethernet de cada paquete.

4.2.3.2 Congestión de la red tras añadir dos fuentes de tráfico externas (sin QoS):

Este caso de estudio consiste en observar **qué ocurre con el ancho de banda cuando no se aplica QoS, en un entorno de alta congestión producida mediante la transmisión de tres flujos en la red**. La transmisión del conjunto de estos flujos produce **congestión a la salida de la interfaz Gig0/0 de Router3 y a la entrada de la interfaz Gig0/0 de Router1**.

La figura 98 muestra la ruta que seguirán los flujos emitidos.

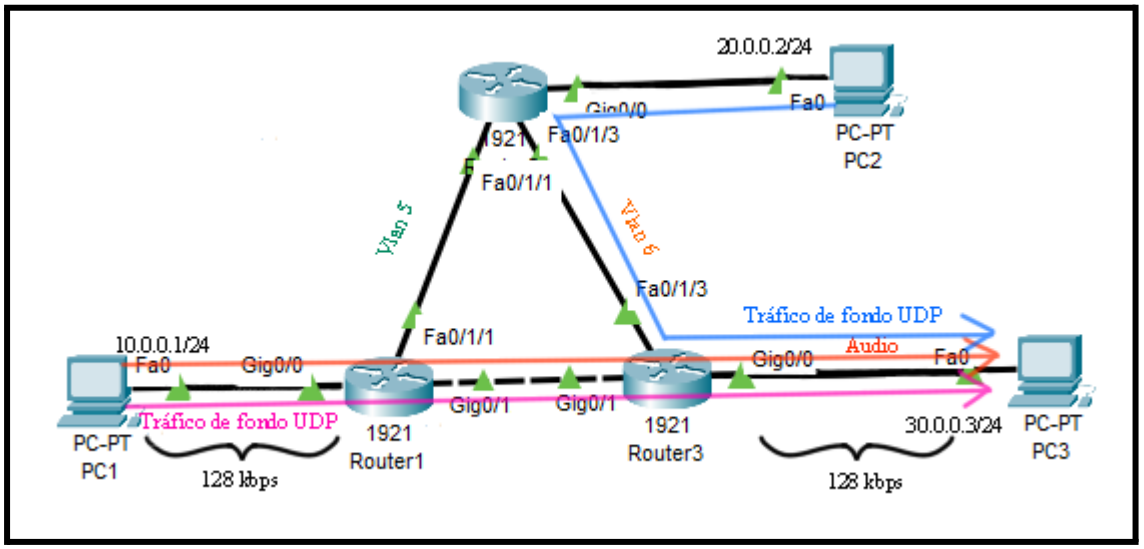


Figura 98. Topología de red y flujos a emitir.

Interacción entre equipos:

PC1: Emite un fichero de audio codificado en G.711 hacia PC3. Además, genera tráfico UDP best effort con la finalidad de saturar la red.

PC2: Genera tráfico UDP best effort con destino PC3 para saturar más la red.

Router3: En la salida de la interfaz Gigabit Ethernet 0/0 limita todo el tráfico a 128 kbps.

Router2: Encamina el tráfico generado por PC2 a PC3.

Router1: En la entrada de la interfaz Gigabit Ethernet 0/0 limita todo el tráfico a 128 kbps.

4.2 Escenario 1: Degradación de un fichero de audio codificado en G.711.

Se emitirán tres flujos con las características indicadas en la tabla 43:

Flujo	Protocolo	IP origen	IP destino	Tamaño de paquete	Tiempo entre paquetes (ms)	Tiempo de generación del flujo (s)	Puerto
Audio	RTP	10.0.0.1/24	30.0.0.3/24	160	20	-	5005
Best Effort	UDP	10.0.0.1/24	30.0.0.3/24	1000	100	0	5203
Best Effort	UDP	20.0.0.2/24	30.0.0.3/24	1000	100	0	5202

Tabla 43.Características de los flujos.

La figura 99 muestra la forma en que se comportan los flujos aproximadamente.

En dicha figura se puede apreciar que se descarta parte de los dos flujos provenientes de PC1 en la entrada de la interfaz Gig0/0 de Router1, y se vuelve a descartar parte de ambos flujos en la entrada de la interfaz Gig0/0 de Router3.

Sin embargo, respecto del flujo proveniente de PC2 solamente se descarta parte del flujo en la entrada de la interfaz Gig0/0 de Router3.

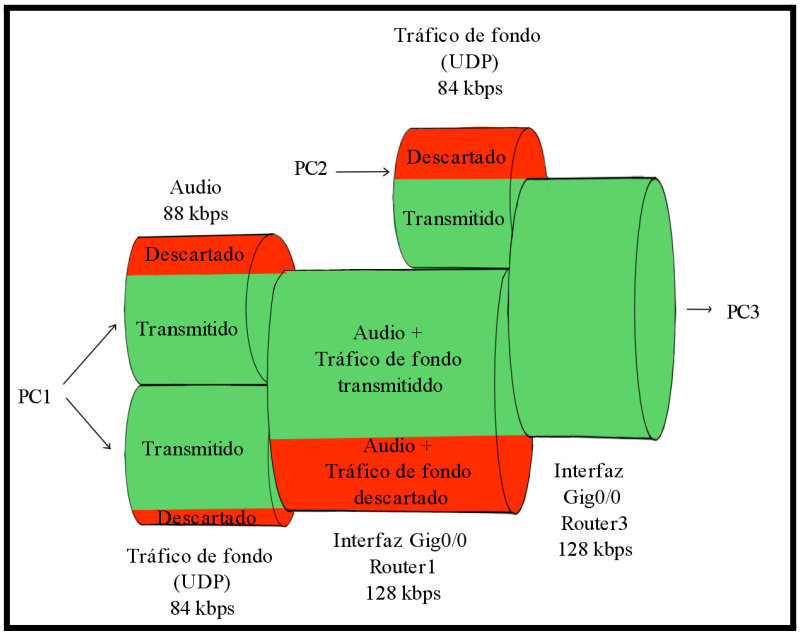


Figura 99. Comportamiento de los flujos en este caso de estudio.

4.2 Escenario 1: Degradación de un fichero de audio codificado en G.711.

En este caso, el flujo de audio generado desde PC1 (PC1 → PC3) ya está activo y no es necesario volver a generarlo. Solamente se han de generar los flujos de tráfico Best Effort desde PC1 a PC3 y desde PC2 a PC3 mediante Iperf 3 con el perfil especificado en la tabla. Además, se debe parar la generación del flujo de audio generado desde PC3 (PC3 → PC1) pulsando las teclas "Ctrl" + "c" en la aplicación símbolo del sistema (CMD/terminal) correspondiente.

Ejercicio 2: Calcule la tasa de generación y transmisión del tráfico de fondo, conociendo que el payload es de 1000 bytes y el tiempo entre paquetes es aproximadamente de 100 ms.

Solución:

Tasa de generación del tráfico de fondo:

*TASA: (1000 Bytes * 8) bits / (100*10^-3) segundos = 80 kbps*

Tasa de transmisión del tráfico de fondo:

Tamaño de trama:

1000 Bytes + 8 Bytes(UDP) + 20 Bytes(IP) + 22 Bytes (Ethernet) =
= 1050 Bytes
Intervalo entre tramas: 100 milisegundos
*TASA: (1050 Bytes * 8) bits / (100*10^-3) segundos = 84 kbps*

1. **Generación de tráfico mediante Iperf 3.**

Ejercicio 3: Genere tráfico UDP desde PC1 con destino a PC3 (IP = 30.0.0.3) un tamaño de payload de 1000 bytes, un tiempo entre paquetes de 100 ms, tiempo de simulación de 0s y utilizando el puerto 5202.

Recuerde que los comandos a utilizar para abrir una instancia servidor son los siguientes:

-s: comando principal para abrir una instancia servidor
-p: puerto de la conexión entre cliente y servidor

Además, recuerde que los comandos a utilizar en el cliente son los siguientes:

-c: IP del pc que ha abierto la instancia servidor
-p: puerto de la conexión entre cliente y servidor
-b: Tasa de generación del tráfico de fondo calculada en el ejercicio anterior.
-l: payload de cada paquete.
-t: tiempo de simulación. Un tiempo de simulación de 0 equivale a generar paquetes de forma infinita.
-u: UDP

4.2 Escenario 1: Degradación de un fichero de audio codificado en G.711.

Solución:

Los flujos se generan mediante los siguientes comandos:

Desde PC3:

```
iperf3.exe -s -p 5203
iperf3.exe -s -p 5202
```

Desde PC1:

```
iperf3.exe -c 30.0.0.3 -p 5203 -u -b 80000 -l 1000 -t 0
```

Desde PC2:

```
iperf3.exe -c 30.0.0.3 -p 5202 -u -b 80000 -l 1000 -t 0
```

2. **Captura de tráfico mediante Wireshark.**

Posteriormente a la generación de tráfico, se ha de capturar el tráfico mediante Wireshark, en PC3. Para ello, se han de añadir los siguientes filtros:

1. Un filtro para observar el combinado de los flujos ("IP.dst == 30.0.0.3 && UDP").
2. Un filtro para observar el flujo de audio ("IP.src == 10.0.0.1&&UDP.src == 5005").
3. Un filtro para observar el flujo Best Effort proveniente de PC2 ("IP.src == 20.0.0.2").
4. Un filtro para observar el flujo Best Effort proveniente de PC1 ("IP.src == 10.0.0.1&&UDP.src == 5203").
5. Un filtro para observar el conjunto de los flujos provenientes de PC1 ("IP.src == 10.0.0.1&&UDP").

Los filtros deben quedar como en la figura 100:

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Fiel	SMA Period	Y Axis Factor
☑	Todos los paqu...	ip.src == 10.0.0.1 && udp.port == 5005		Line	Bits		500 interval SMA	1
☑	Todos los paqu...	ip.src == 20.0.0.2		Line	Bits		500 interval SMA	1
☑	Todos los paqu...	ip.src == 10.0.0.1 && udp.port == 5203		Line	Bits		500 interval SMA	1
☑	Todos los paqu...	ip.src == 10.0.0.1 && udp		Line	Bits		500 interval SMA	1
☑	Todos los paqu...	ip.dst == 30.0.0.3 && udp		Line	Bits		500 interval SMA	1

Figura 100. Filtro de captura de paquetes cuyo destino es PC3.

Ejercicio 4: ¿Cómo se escucha el audio transmitido una vez se están transmitiendo todos los flujos? ¿Se llega a producir congestión?¿A qué se debe?¿En qué interfaces se produce congestión? Apóyese en el resultado obtenido mediante Wireshark:

Copia la gráfica obtenida mediante Wireshark a continuación:

4.2 Escenario 1: Degradación de un fichero de audio codificado en G.711.

Solución:

Mediante wireshark se obtiene el siguiente resultado (figura 101):

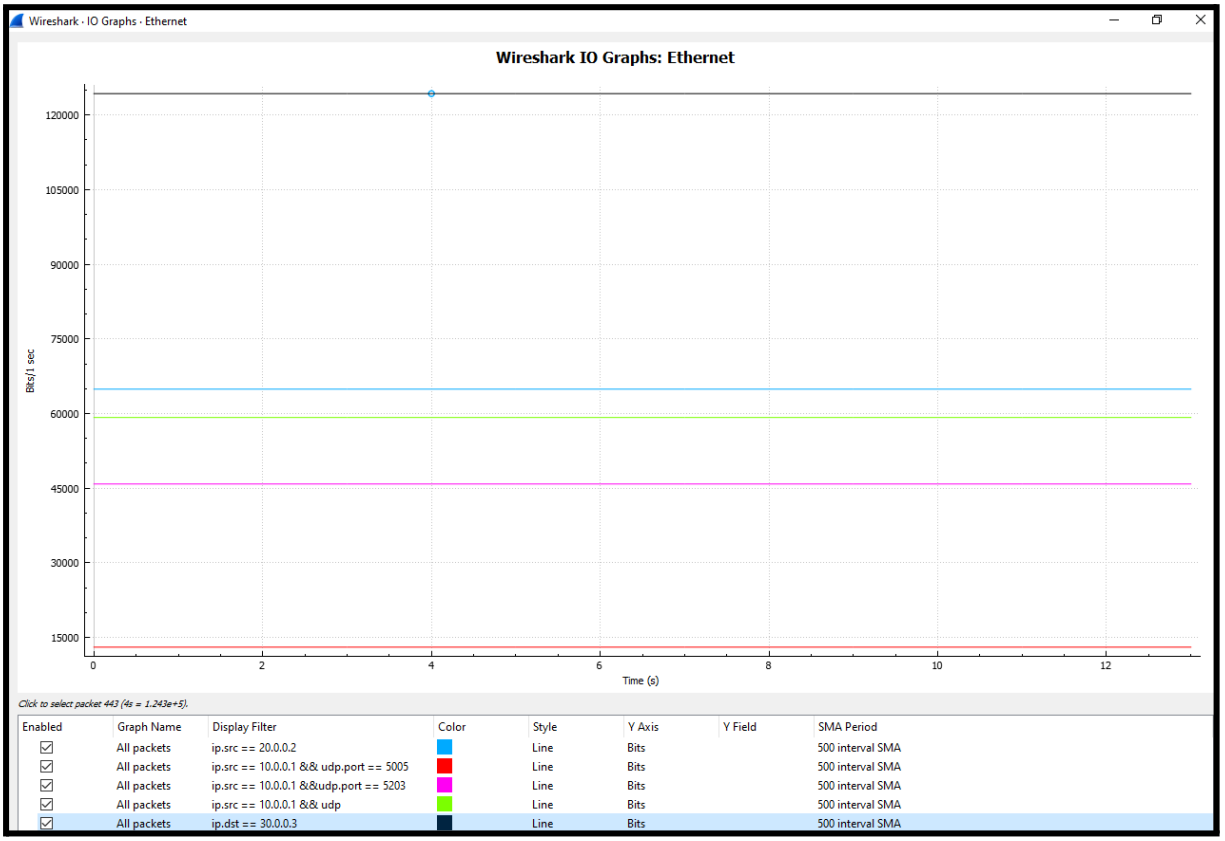


Figura 101.Comportamiento de los flujos obtenido mediante Wireshark.

Tras el comienzo de la contínua transmisión de los tres flujos, se escucha que el audio se entrecorta con mucha frecuencia.

En la captura anterior observamos que el ancho de banda queda repartido de la siguiente forma:

- Ancho de banda **total**: **124300 bps.**
- Ancho de banda que utiliza el fichero de **audio**: **13070 bps.**
- Ancho de banda que utiliza el **flujo** generado por **Iperf3** desde **PC1**: **46140 bps.**
- Ancho de banda que utiliza **PC1** en **total**: **59210 bps.**
- Ancho de banda que utiliza **PC2**: **64900 bps.**

Por lo tanto, podemos observar que el tráfico de audio es el que queda más penalizado con bastante diferencia puesto que es reducido a la entrada de la interfaz Gig0/0 de Router1, así como a la salida de la interfaz Gig0/0 de Router3. Además, como se ha podido observar en el caso anterior, el flujo de audio queda más penalizado que los flujos de tráfico UDP generados mediante el Iperf3. Por lo tanto, se produce congestión.

4.2 Escenario 1: Degradación de un fichero de audio codificado en G.711.

Sin embargo, estos resultados pueden variar, como se puede apreciar en la siguiente imagen:

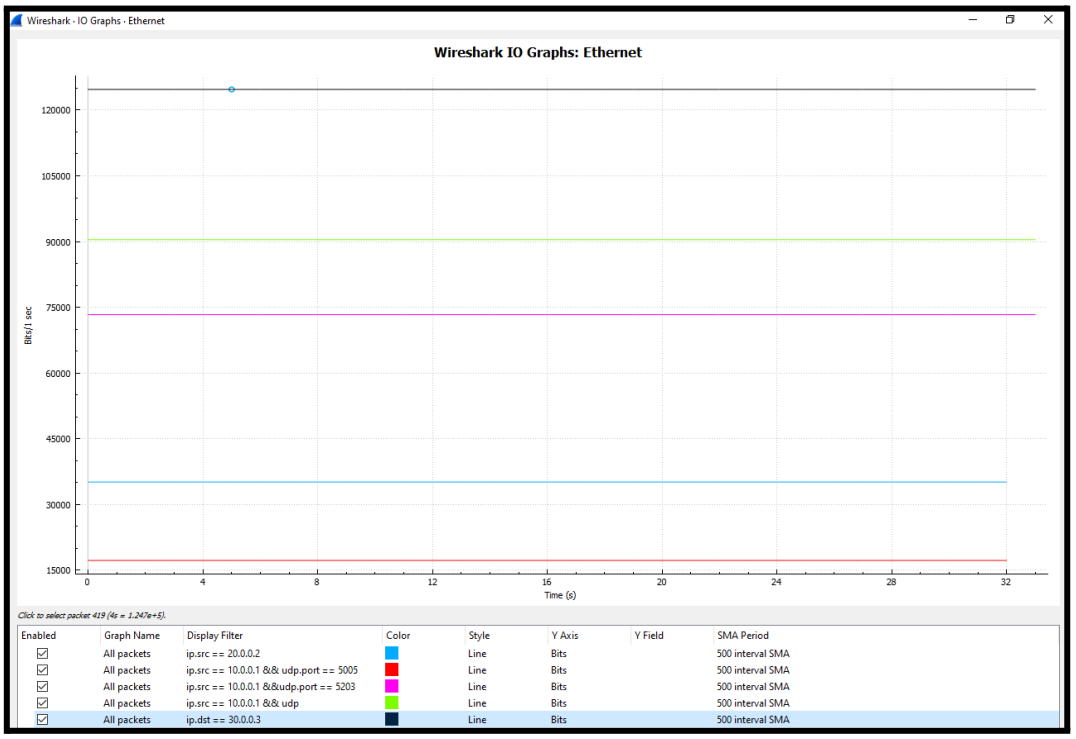
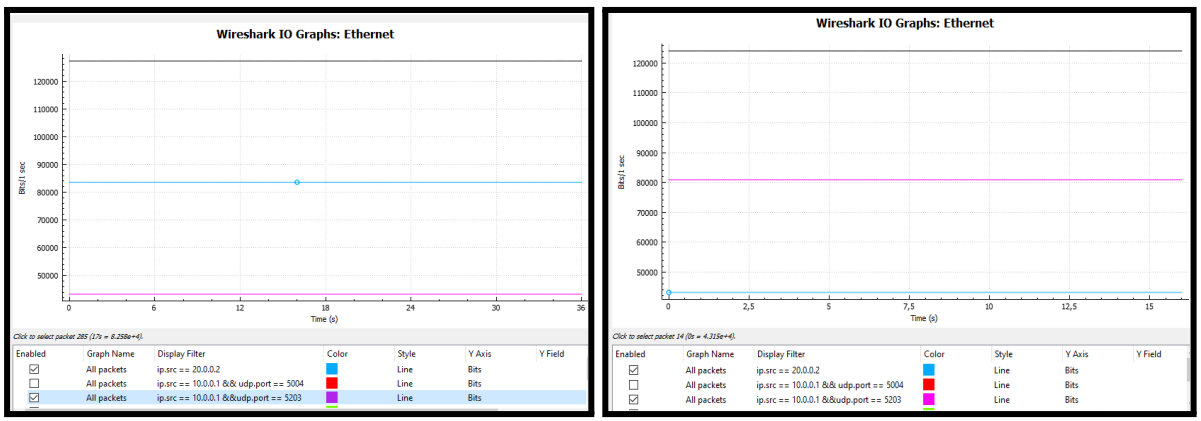


Figura 102.Comportamiento de los flujos obtenido mediante Wireshark.

En esta imagen (figura 102) observamos que el ancho de banda recibido del stream de audio es similar al de la captura anterior. Sin embargo, se observa que en este caso el flujo de tráfico UDP generado por PC2 ha quedado más penalizado que el generado por PC1.

Esta diversidad en los resultados se debe a que cuando se transmiten dos flujos UDP utilizando el Iperf3 uno queda más penalizado que el otro, siendo aleatorio el que queda más penalizado en el caso de recortar el ancho de banda a 128 kbps con una función policía. Esto se puede observar en las figuras 103 y 104.



Figuras 103 y 104.Comportamiento de los flujos Iperf 3.

Por lo tanto, dependiendo de cual sea el flujo generado desde el Iperf3 que queda más penalizado, obtenemos un resultado parecido a una de las dos posibles soluciones de este ejercicio. Sin embargo, como se ha podido comprobar previamente, esto no tiene prácticamente efecto en el ancho de banda recibido del stream de audio.

4.2.3.3 Congestión de la red tras añadir dos fuentes de tráfico externas (cos QoS):

La figura 105 muestra la ruta que seguirán los flujos emitidos.

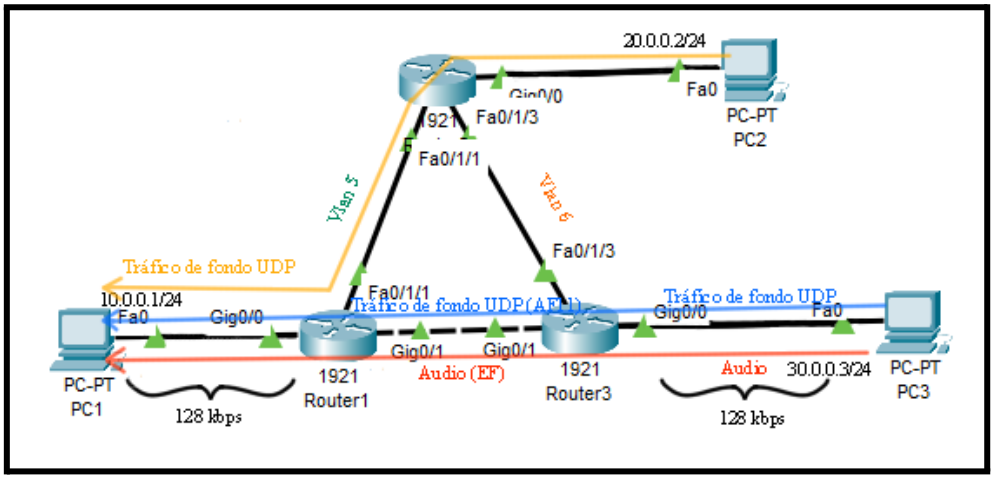


Figura 105. Topología de red y flujos a emitir.

Este caso de estudio consiste en **observar qué ocurre con el ancho de banda cuando se aplica QoS en un entorno de alta congestión producida mediante la transmisión de tres flujos en la red.**

Interacción entre equipos:

PC2: Genera tráfico UDP best effort con destino PC1.

PC3: Emite un fichero de audio codificado en G.711 hacia PC1. Además, genera tráfico UDP hacia PC1 para saturar la red.

Router3: En la entrada de la interfaz Gigabit Ethernet 0/0 marca el tráfico RTP/RTCP/SIP con el valor 46 del campo DSCP (EF) y el tráfico UDP y TCP restante con el valor 10 (AF11). Además, garantiza y limita el ancho de banda del tráfico RTP/RTCP a 88 kbps y del tráfico marcado con AF11 a 12 kbps.

Router2: Encamina el tráfico generado por PC2 a PC1.

Router1: En la salida de la interfaz Gigabit Ethernet 0/0 garantiza y limita el ancho de banda recibido por PC3 a 100kbps y por PC2 a 28 kbps.

4.2 Escenario 1: Degradación de un fichero de audio codificado en G.711.

Se emitirán tres flujos con las características indicadas por la tabla 44:

Flujo	Protocolo	IP origen	IP destino	Tamaño de paquete	Tiempo entre paquetes (ms)	Tiempo de generación del flujo (s)	Puerto
Audio	RTP	30.0.0.3/24	10.0.0.1/24	160	20	-	5004
Best Effort	UDP	30.0.0.3/24	10.0.0.1/24	1000	100	0	5203
Best Effort	UDP	20.0.0.2/24	10.0.0.1/24	1000	100	0	5202

Tabla 44. Características de los flujos.

Las funciones policía que se activan en este caso son las que se muestran en la figura 106.

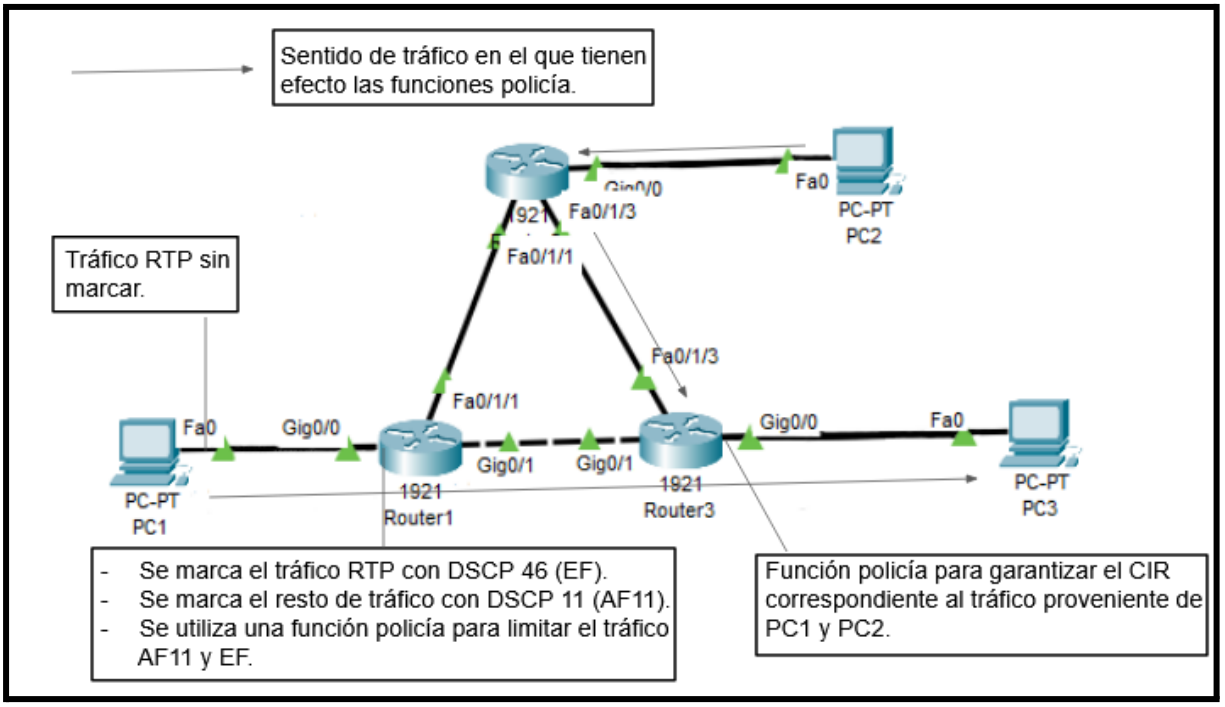


Figura 106. Sentido de tráfico en el que se aplica QoS para mejorar la calidad de experiencia de los usuarios.

4.2 Escenario 1: Degradación de un fichero de audio codificado en G.711.

La figura 107 muestra el comportamiento de los flujos de acuerdo a las funciones policía utilizadas:

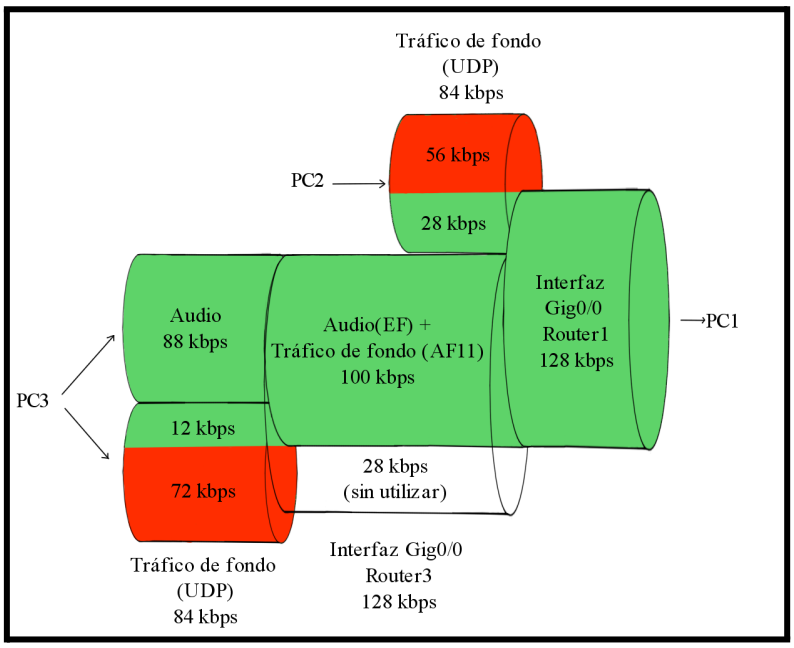


Figura 107. Comportamiento de los flujos de acuerdo a las funciones policía.

1. **Generación de tráfico.**

Ejercicio 5: Genere tráfico de fondo desde PC3 a PC1, que es marcado con el valor AF11 por el router, tráfico de fondo desde PC2 a PC1 y vuelva a generar el flujo de audio. El tráfico de fondo debe tener el perfil especificado en la tabla 45:

Flujo	Protocolo	IP origen	IP destino	Tamaño de paquete	Tiempo entre paquetes (ms)	Tiempo de generación del flujo (s)	Puerto
Best Effort	UDP	30.0.0.3/24	10.0.0.1/24	1000	100	0	5203
Best Effort	UDP	20.0.0.2/24	10.0.0.1/24	1000	100	0	5202
Audio	RTP	30.0.0.3/24	10.0.0.1/24	160	20	-	5004

Tabla 45. Características de los flujos a emitir.

4.2 Escenario 1: Degradación de un fichero de audio codificado en G.711.

Solución:

Los flujos se generan mediante los siguientes comandos:

Desde PC1: iperf3.exe -s -p 5202
Desde PC2: iperf3.exe -c 10.0.0.1 -p 5202 -u -b 80000 -l 1000 -t 0

Desde PC1: iperf3.exe -s -p 5203
Desde PC3: iperf3.exe -c 10.0.0.1 -p 5203 -u -b 80000 -l 1000 -t 0

Desde PC3: ffmpeg.exe -re -stream_loop -1 -i audio.wav -f rtp -packetsize 172 "rtp://10.0.0.1:5004"

2. Captura de tráfico en la interfaz ethernet mediante Wireshark.

Posteriormente, se ha de capturar el tráfico mediante Wireshark y añadir 4 nuevos filtros en PC1 para observar cómo queda repartido el ancho de banda.

En total, deben de estar creados los siguientes filtros:

1. Un filtro que muestre la totalidad del ancho de banda utilizado ("ip.dst == 10.0.0.1&& udp")
2. Un filtro para observar el tráfico marcado con el valor EF del campo DSCP, correspondiente al audio ("ip.dsfield.dscp == 46").
3. Un filtro para observar el tráfico marcado con el valor AF11 del campo DSCP ("ip.dsfield.dscp == 10").
4. Un filtro para observar la totalidad del ancho de banda utilizado por PC3 ("ip.src == 30.0.0.3 && udp").
5. Un filtro para observar la totalidad del ancho de banda utilizado por PC2 ("ip.src == 20.0.0.2 && udp")

Los filtros deben quedar como en la figura 108:

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Fiel	SMA Period	Y Axis Factor
☑	Todos los paqu...	ip.dst == 10.0.0.1 && udp		Line	Bits		500 interval SMA	1
☑	Todos los paqu...	ip.dsfield.dscp == 10		Line	Bits		500 interval SMA	1
☑	Todos los paqu...	ip.dsfield.dscp == 46		Line	Bits		500 interval SMA	1
☑	Todos los paqu...	ip.src == 30.0.0.3 && udp		Line	Bits		500 interval SMA	1
☑	Todos los paqu...	ip.src == 20.0.0.2 && udp		Line	Bits		500 interval SMA	1

Figura 108. Filtros de captura necesarios en Wireshark.

4.2 Escenario 1: Degradación de un fichero de audio codificado en G.711.

<u>Ejercicio 6:</u> ¿Cómo se escucha el audio transmitido una vez se están transmitiendo todos los flujos? ¿Cómo se reparte el ancho de banda?¿A qué se debe? Apóyese en el resultado obtenido mediante Wireshark:

Copia la gráfica obtenida mediante Wireshark a continuación:

Solución:

Mediante wireshark se obtiene el siguiente resultado (figura 109):

Figura 109.Comportamiento de los flujos obtenido mediante Wireshark.

Una vez se estén transmitiendo los tres flujos se escucha como si no hubiera congestión, pese a que el bitrate total generado es de aproximadamente 256 kbps que corresponde con el doble de la capacidad de los enlaces.

Mediante la gráfica obtenida con Wireshark, podemos comprobar que el ancho de banda se adapta al tráfico garantizado indicado en las función policía de Router1 y de Router 3. De esta forma, se debe de observar que el ancho de banda total es de 128 kbps aproximadamente, 12 kbps corresponden al tráfico marcado con AF11, 88 kbps al flujo de audio y 28 kbps corresponden al tráfico generado por PC2.

Estos resultados se obtienen debido a que las funciones policía limitan y garantizan el tráfico de los tres flujos. En concreto, la función policía a la entrada de la interfaz Gig0/0 de Router3 limita y garantiza el flujo de audio a 88 kbps y el tráfico que el router marca como AF11 a 12 kbps.

Finalmente, en la salida de la interfaz Gig0/0 de Router1 la función policía garantiza 100 kbps de tráfico proveniente de PC3 y 28 kbps de tráfico proveniente de PC2.

En este caso observamos que se utiliza la totalidad del ancho de banda del canal, pero observamos que el ancho de banda utilizado por el fichero de audio es el mismo que en el caso en el que se transmitía sin congestión. De esta forma, para que se transmita el audio sin pérdidas se ha sacrificado gran parte del tráfico generado mediante el Iperf3 desde PC1 y PC2.

4.3 Escenario 2: Degradación de un fichero de vídeo con audio.

En el segundo escenario se va a poder observar cómo se **degrada un fichero de vídeo con audio en un entorno de congestión, en el caso de que no se utilice QoS para garantizar la transmisión de dicho fichero. Además, se observará la forma en que se comportan los flujos transmitidos en condiciones similares, en el caso de que se utilice QoS.**

Para poder apreciar estos efectos con mayor facilidad, se han **configurado los routers para estrechar el ancho de banda de los enlaces en los que se produce congestión a 10 Mbps**.

Sin embargo, se deben asignar las funciones policía correspondientes a esta segunda parte. Para ello, utilizando el programa Putty se deben **configurar los routers 1 y 3.**

Configuración de Router1:

en modo configuración global, se utilizan los siguientes comandos:

```
interface GigabitEthernet0/0
no service-policy input bw_recortado_128
no service-policy output policia_128
service-policy output policia_10M
```

Configuración de Router3:

en modo configuración global, se utilizan los siguientes comandos:

```
interface GigabitEthernet0/0
no service-policy output bw_recortado_128
no service-policy input pc3_pc1_128
service-policy input pc3_pc1_10M
```

4.3 Escenario 2: Degradación de un fichero de vídeo con audio.

El escenario queda de la siguiente forma (figura 110):

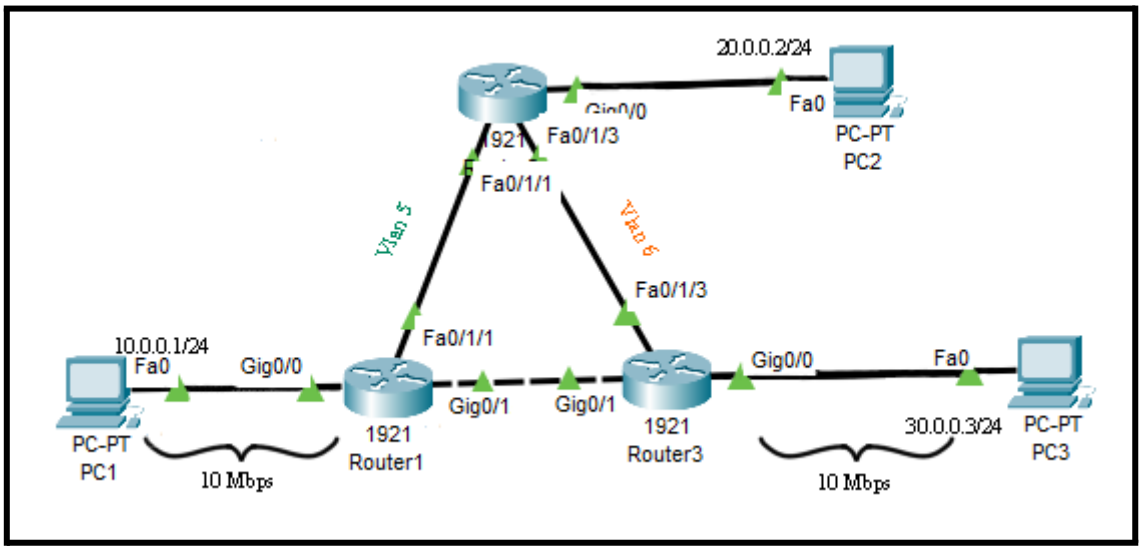


Figura 110. Topología de red del escenario 2.

4.3.1 Herramientas de QoS utilizadas en los routers:

Marcado: El marcado en este escenario se realiza de la misma forma que en el primer escenario

Por lo tanto, se va a realizar un **marcado a nivel 3, mediante el campo DSCP de la cabecera IP.** En concreto, **Router 3 marca los paquetes RTP/RTCP entrantes por la interfaz Gi0/0 con DSCP 46 (EF). Además, el resto de paquetes UDP y TCP provenientes de PC3 cuyo destino es PC1 se marcan con el valor DSCP 10 (AF11).**

Función policía:

Las funciones policía a utilizar son las indicadas por la tabla 46:

Router	Interfaz:	Entrada/Salida	Función
Router3	Gig0/0	Entrada	- Garantizar, marcar con DSCP EF y limitar a 2,2 Mbps el tráfico RTP/RTCP/SIP. - Garantizar, marcar con DSCP AF11 y limitar a 1,8 Mbps el restante tráfico UDP y TCP con destino a PC1.
Router1	Gig0/0	Salida	- Garantizar y limitar a 5 Mbps el tráfico proveniente de PC1. - Garantizar y limitar a 5 Mbps el tráfico proveniente de PC2.

Tabla 46.Funciones policía utilizadas en el segundo escenario.

4.3 Escenario 2: Degradación de un fichero de vídeo con audio.

Las funciones policía que se activan en este caso son las que se muestran en la figura 111.

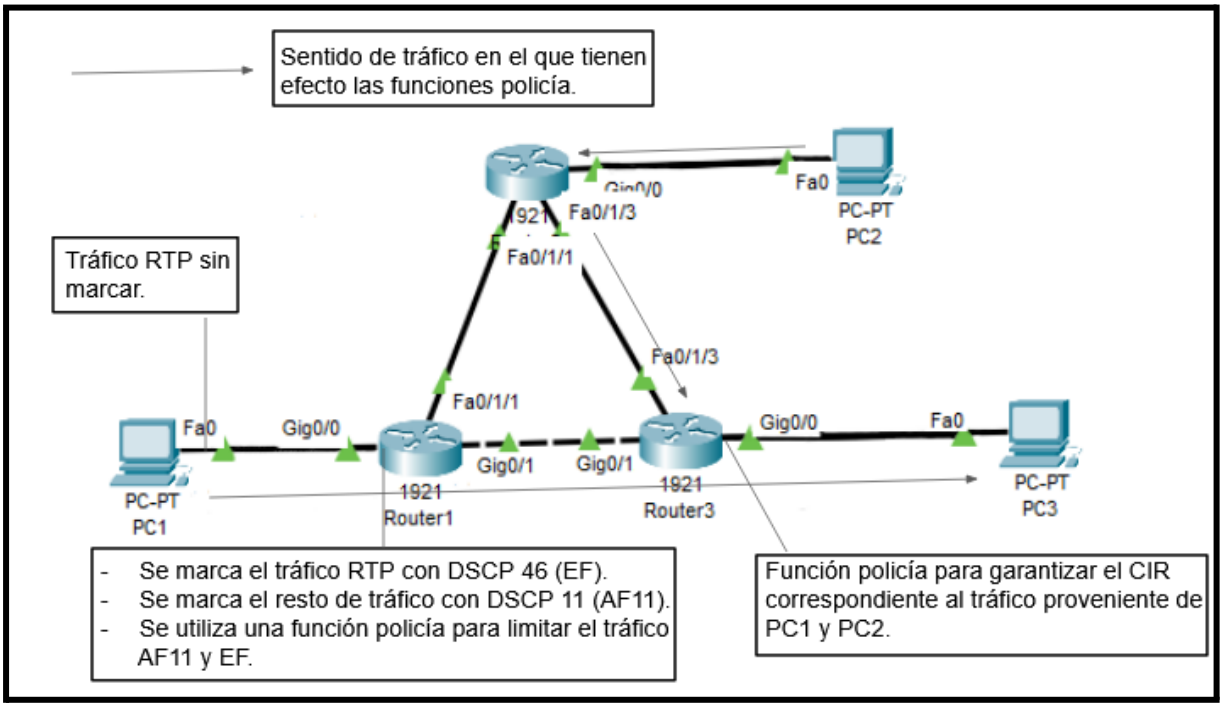


Figura 111. Sentido de tráfico en el que se aplica QoS para mejorar la calidad de experiencia de los usuarios.

La figura 112 muestra cómo quedan repartidos los flujos de acuerdo a las funciones policía.

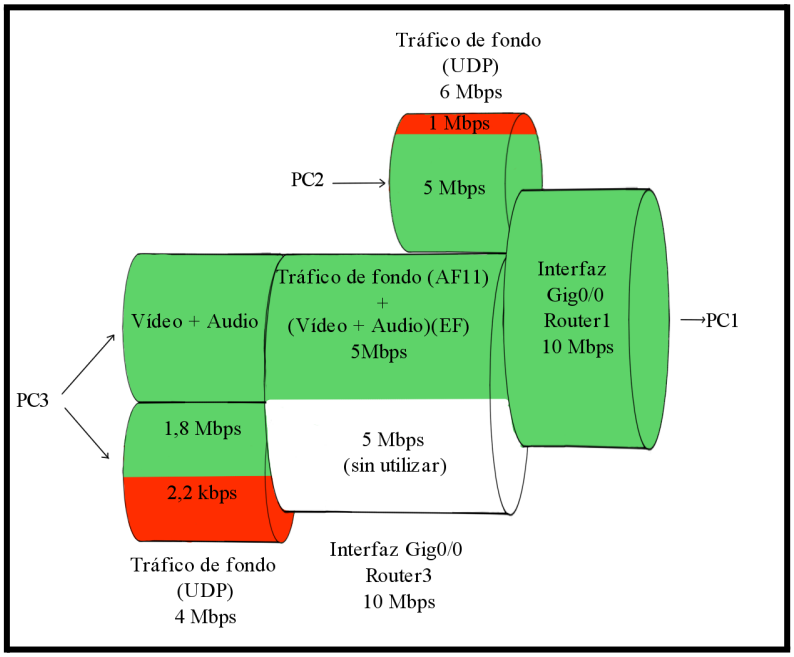


Figura 112. Comportamiento de los flujos de acuerdo a las funciones policía.

4.3.2 Interacción entre equipos:

PC1: Emite un fichero de vídeo con audio hacia PC3. Además, genera tráfico UDP con la finalidad de saturar la red.

PC2: Genera tráfico UDP best effort con destino a PC1 y a PC3 con el objetivo de saturar la red.

PC3: Emite un fichero de vídeo con audio hacia PC1. Además, genera tráfico UDP que será marcado por el router con el valor 10 del campo DSCP (AF11) para saturar la red.

Router3: En la entrada de la interfaz Gigabit Ethernet 0/0 marca el tráfico RTP/RTCP/SIP con el valor 46 del campo DSCP (EF), y el tráfico UDP y TCP restante con el valor 10 (AF11). Además, garantiza y limita el ancho de banda del tráfico RTP/RTCP a 2,2 Mbps y del tráfico marcado con AF11 a 1,8 Mbps.

Router2: Encamina el tráfico generado por PC2 a PC1 y a PC3. No utiliza QoS.

Router1: En la salida de la interfaz Gigabit Ethernet 0/0 garantiza y limita el ancho de banda recibido por PC3 y PC2 a 5 Mbps cada uno.

4.3.3 Actividades Prácticas:

Para observar los efectos de la calidad de servicio (QoS) en la transmisión de un fichero de vídeo con audio se han realizado tres casos de estudio en los que se puede comprobar de forma gradual los efectos que conllevan utilizar herramientas de calidad de servicio frente a no utilizarlas.

Estos casos de estudio son:

1. Transmisión de vídeo con audio sin congestión de red.
2. Transmisión de vídeo con audio con congestión de red (sin QoS).
3. Transmisión de vídeo con audio con congestión de red (con QoS).

4.3 Escenario 2: Degradación de un fichero de vídeo con audio.

4.3.3.1 Transmisión de vídeo con audio sin congestión de red.

Este primer caso de estudio consiste en observar que se puede **visualizar correctamente el flujo de vídeo con audio así como estudiar el comportamiento de dicho flujo**. Para ello, ha de ser capturado mediante Wireshark.

La figura 113 muestra la ruta que seguirán los flujos a emitir.

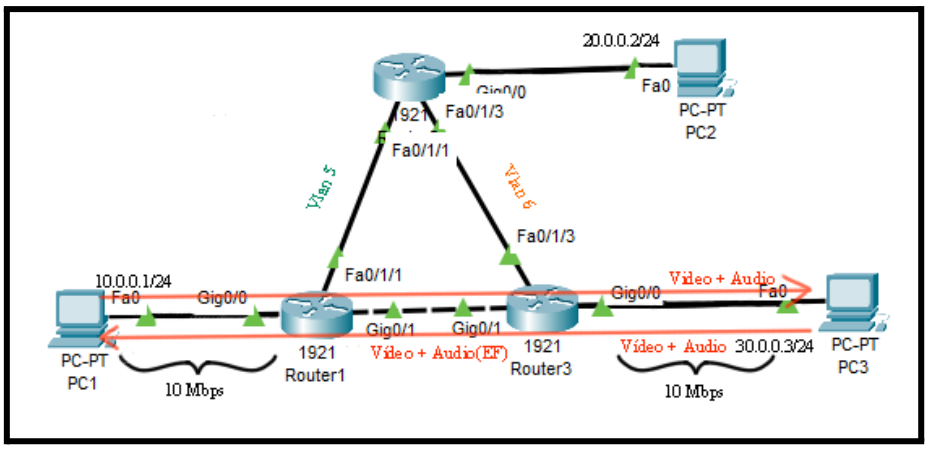


Figura 113. Topología de red y flujos a emitir.

Interacción entre equipos:

PC1: Emite un fichero de vídeo con audio hacia PC3.

PC3: Emite un fichero de vídeo con audio hacia PC1.

Router3: En la entrada de la interfaz Gigabit Ethernet 0/0 marca el tráfico RTP/RTCP/SIP con el valor 46 del campo DSCP (EF).

Router1: Simplemente encamina paquetes entrantes.

Se emitirán dos flujos con las características indicadas por la tabla 47:

Flujo	Protocolo	IP origen	IP destino	Tiempo de generación del flujo (s)	Puerto
Vídeo + Audio	RTP	10.0.0.1/24	30.0.0.3/24	231	5005
Vídeo + Audio	RTP	30.0.0.3/24	10.0.0.1/24	231	5004

Tabla 47.Características de los flujos.

4.3 Escenario 2: Degradación de un fichero de vídeo con audio.

Para resolver este caso de estudio se debe de **generar el flujo de audio mediante VLC, recibir el stream de audio mediante VLC y capturar el tráfico mediante Wireshark.**

1. **<u>Para generar el flujo de audio mediante VLC se han seguido los siguientes pasos:</u>**

Paso 1. En la barra de menús de VLC seleccionar "Medio → Emitir…", como se puede apreciar en la figura 114.

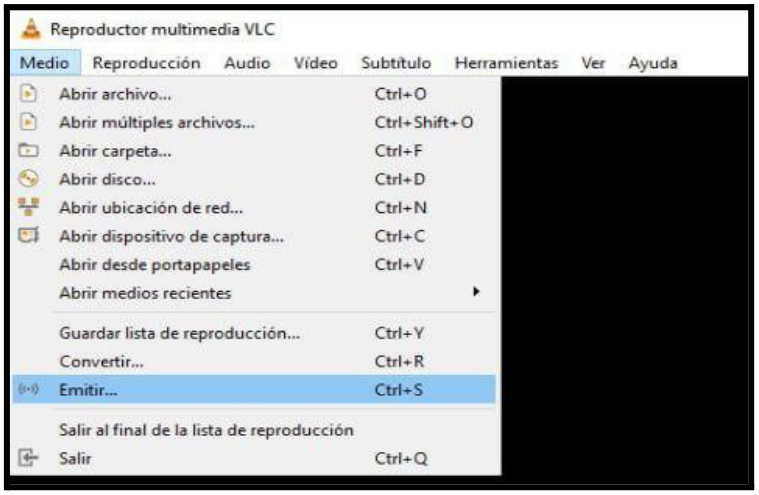


Figura 114. Generación del flujo de audio y vídeo mediante VLC en Wireshark, paso 1.

Paso 2. Cuando se abra la siguiente ventana se debe hacer clic en "Añadir" y seleccionar el archivo de vídeo. Posteriormente se debe hacer clic en "Emitir", como se puede apreciar en la figura 115.

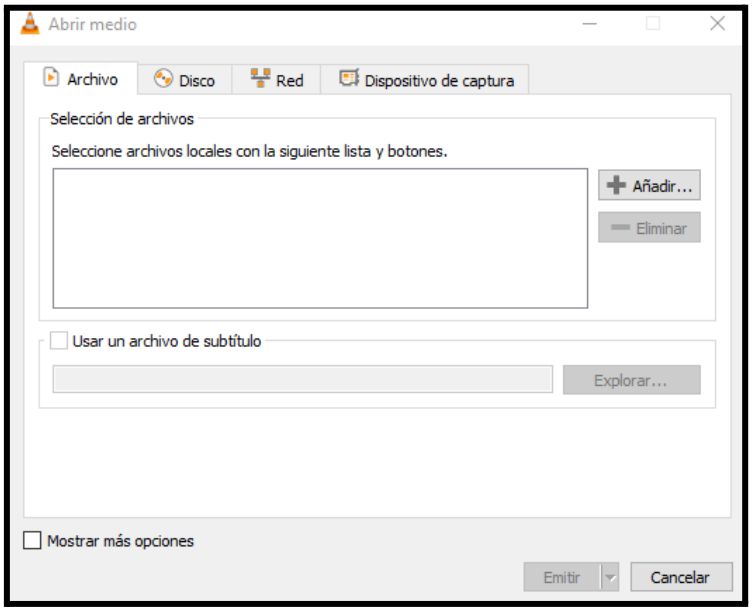


Figura 115. Generación del flujo de audio y vídeo mediante VLC en Wireshark, paso 2.

4.3 Escenario 2: Degradación de un fichero de vídeo con audio.

Paso 3. Se debe seleccionar RTP/MPEG Transport Stream y posteriormente, el botón "Añadir", como se puede apreciar en la figura 116.

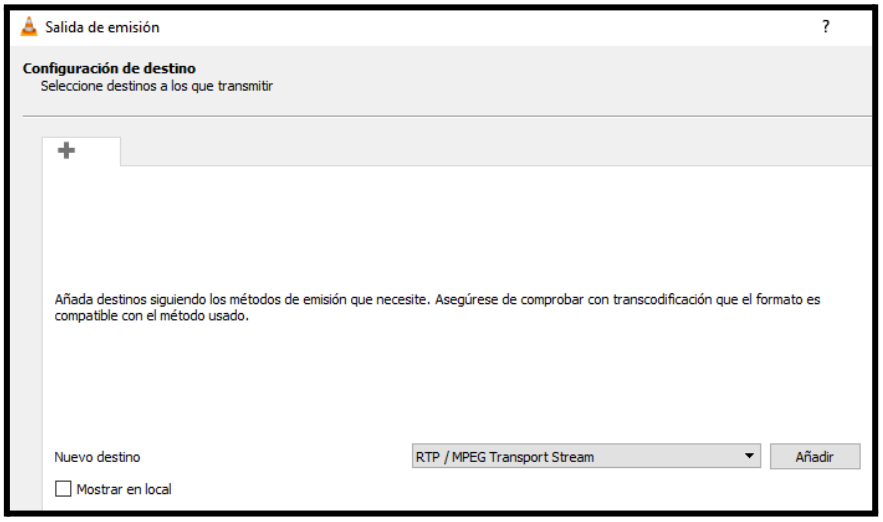


Figura 116. Generación del flujo de audio y vídeo mediante VLC en Wireshark, paso 3.

Paso 4. En "Dirección" se debe escribir la dirección IP de destino, y en "Puerto Base" el puerto indicado para la conexión. Posteriormente se debe hacer clic en "Siguiente". La figura 117 corresponde a la configuración que se debe utilizar cuando el flujo se emite desde PC1 con destino PC3.

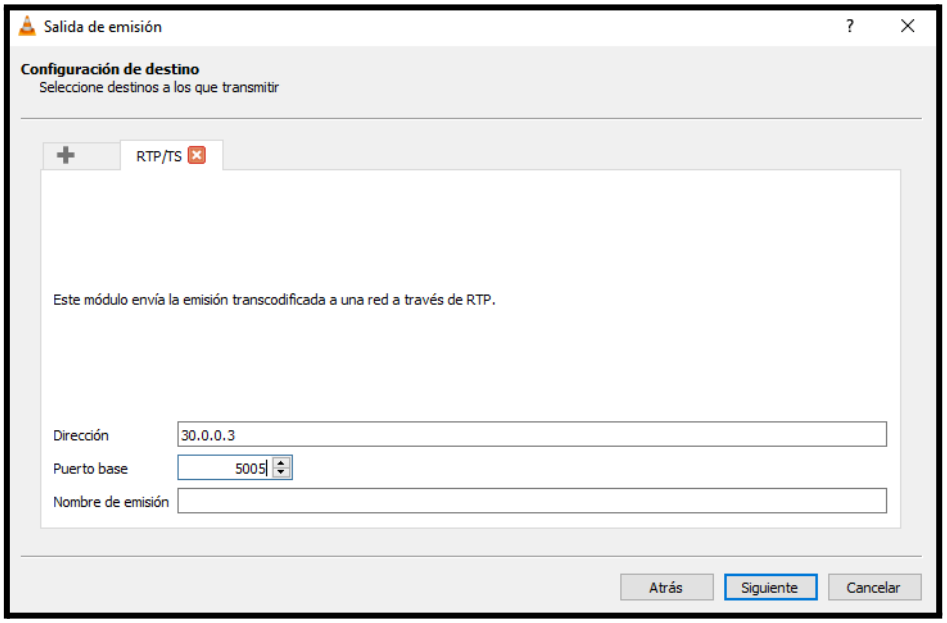


Figura 117. Generación del flujo de audio y vídeo mediante VLC en Wireshark, paso 4.

4.3 Escenario 2: Degradación de un fichero de vídeo con audio.

Paso 5. Cuando aparezca la siguiente imagen (figura 118) se debe deseleccionar la opción "Habilitar transcodificar", seleccionar "vídeo -H.264 +MP3 (MP4)" en el menú desplegable y pulsar el botón con el icono de herramienta.

Figura 118. Generación del flujo de audio y vídeo mediante VLC en Wireshark, paso 5.

Paso 6. Tanto en la pestaña de "Códec de vídeo" como en la de "Códec de audio" se debe seleccionar "Mantener pista de vídeo original", como se puede apreciar en la figura 119. Finalmente, se debe pulsar el botón "Guardar".

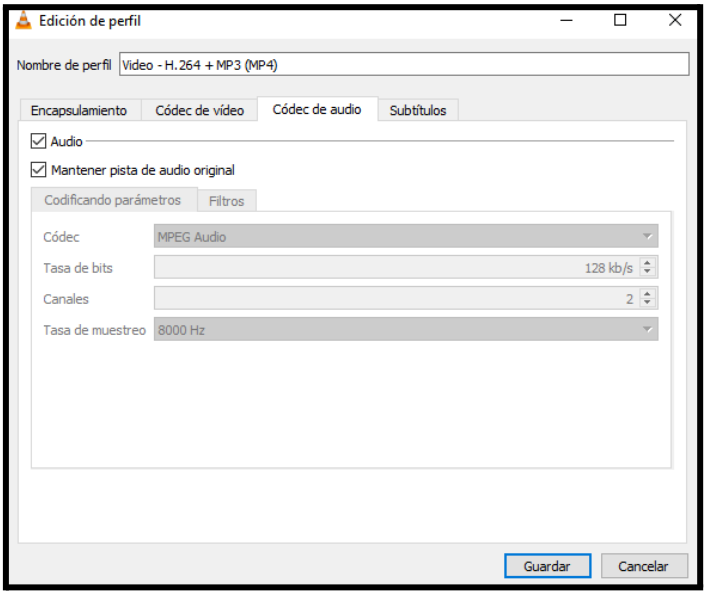


Figura 119 Generación del flujo de audio y vídeo mediante VLC en Wireshark, paso 6.

Paso 7. Una vez se muestre la siguiente imagen (figura 120), se debe pulsar el botón "Emitir".

4.3 Escenario 2: Degradación de un fichero de vídeo con audio.

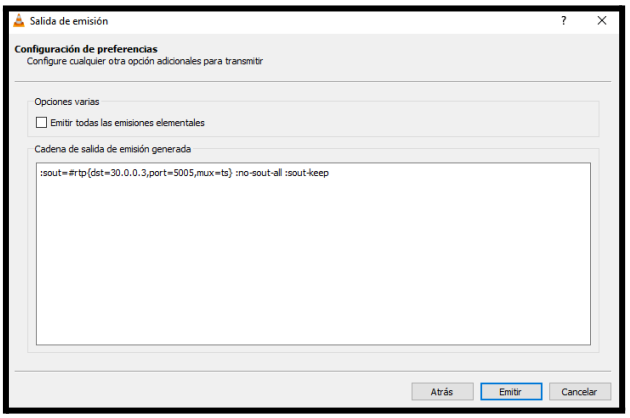


Figura 120. Generación del flujo de audio y vídeo mediante VLC en Wireshark, paso 7.

2. Recepción del flujo mediante VLC y Captura de tráfico mediante Wireshark

Una vez se pueda apreciar la captura del flujo de vídeo + audio, se ha de capturar mediante Wireshark. En este caso no es necesario volver a crear los filtros de Wireshark porque ya han sido creados en el primer escenario. Además, tampoco será necesario volver a realizar los pasos para la captura del vídeo con VLC, porque ya se ha hecho en el primer escenario.

Ejercicio 7: Apunte el bitrate medio del flujo obtenido mediante Wireshark.

Solución:

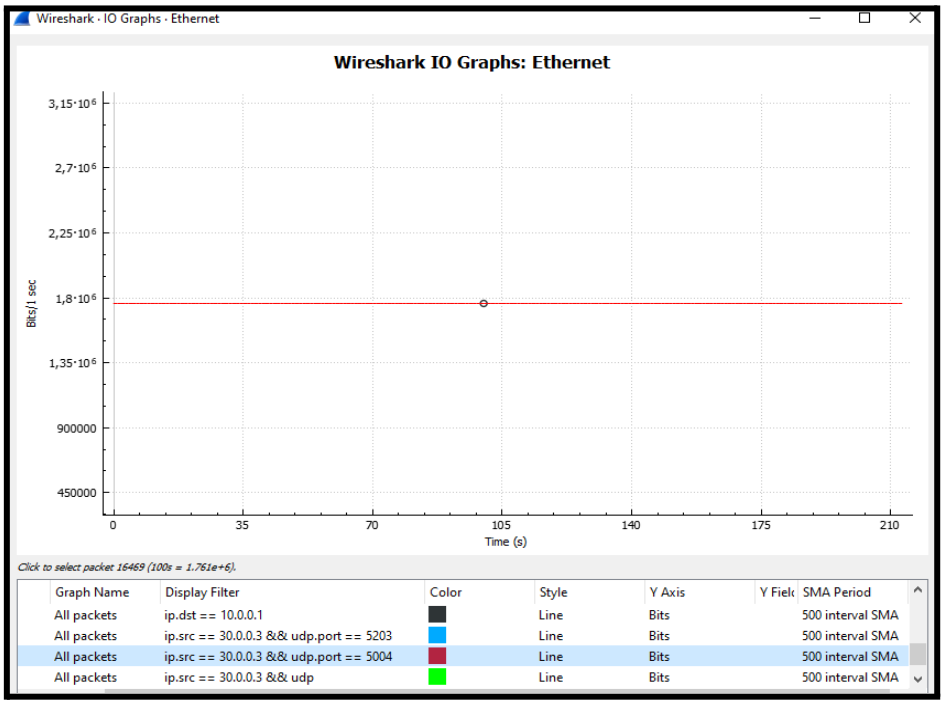


Figura 121.Ancho de banda utilizado obtenido mediante Wireshark.

Mediante Wireshark (figura 121) obtenemos que en media, el bitrate del vídeo es de 1,761 Mbps.

4.3 Escenario 2: Degradación de un fichero de vídeo con audio.

4.3.3.2 Transmisión de vídeo con audio con congestión de red (sin QoS).

Este segundo caso de estudio consiste en observar cómo queda afectado el flujo de vídeo con audio en el caso que se produzca congestión en la red tras la emisión de tres flujos.

La figura 122 muestra la ruta que seguirán los flujos a emitir.

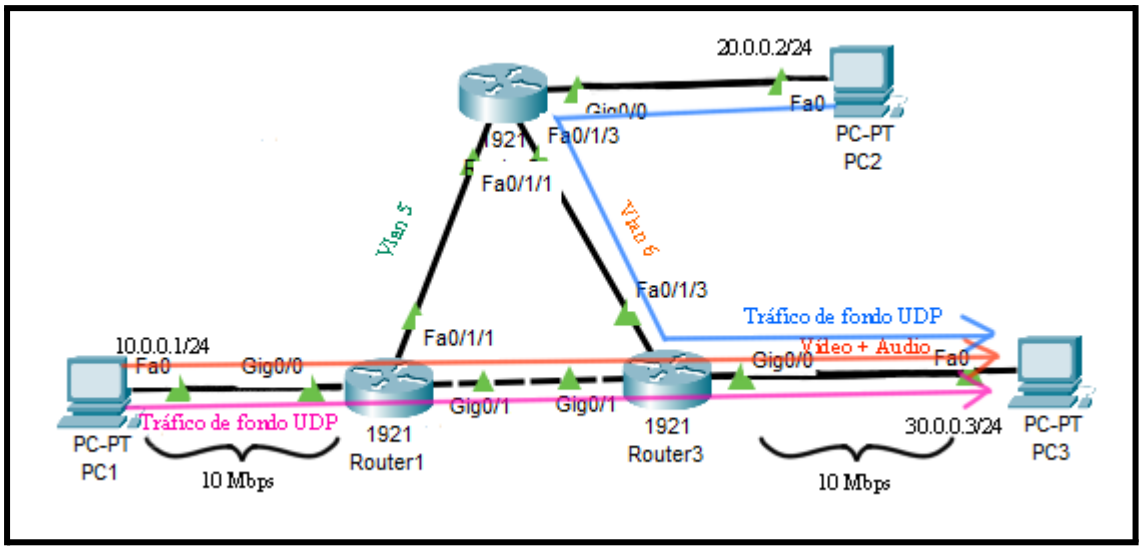


Figura 122. Topología de red y flujos a emitir.

Interacción entre equipos:

PC1: Emite un fichero de vídeo con audio hacia PC3. Además, genera tráfico UDP con la finalidad de saturar la red.

PC2: Genera tráfico UDP best effort con destino PC3 con el objetivo de saturar la red.

Router3: En la salida de la interfaz Gigabit Ethernet 0/0 limita el tráfico a 10 Mbps.

Router2: Encamina el tráfico generado por PC2 con destino PC3. No utiliza QoS.

Router1: Encamina los paquetes entrantes.

4.3 Escenario 2: Degradación de un fichero de vídeo con audio.

Los flujos a emitir son los indicados en la tabla 48:

Flujo	Protocolo	IP origen	IP destino	Tamaño de paquete	bitrate (bps)	Tiempo de generación del flujo (s)	Puerto
Vídeo + Audio	RTP	10.0.0.1/24	30.0.0.3/24	-	-	-	5005
Best Effort	UDP	10.0.0.1/24	30.0.0.3/24	1000	4000000	0	5203
Best Effort	UDP	20.0.0.2/24	30.0.0.3/24	1000	6000000	0	5202

Tabla 48.Características de los flujos.

La figura 123 muestra la forma en que se comportan los flujos aproximadamente.

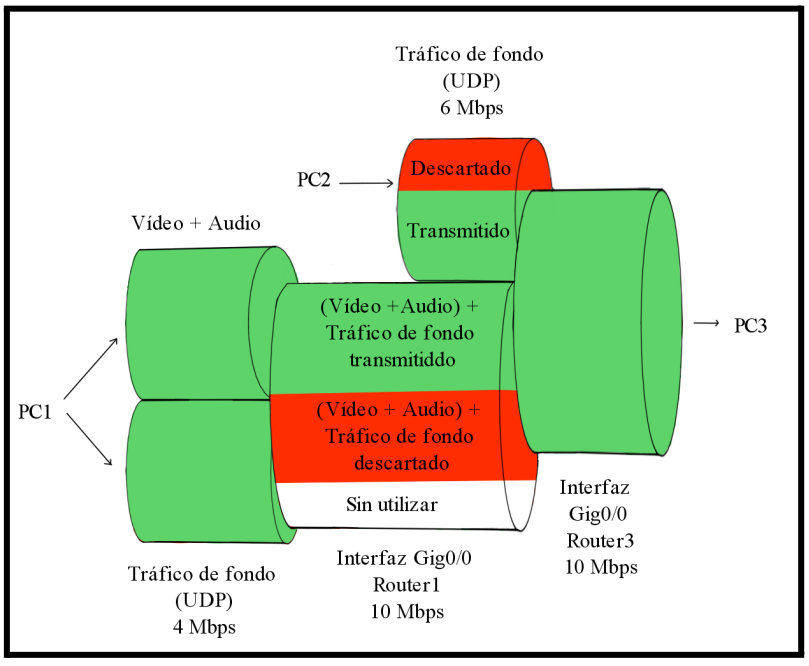


Figura 123. Comportamiento de los flujos en este caso de estudio.

Para realizar este caso de estudio se ha **generado el flujo de audio mediante VLC, recibido el stream de audio mediante VLC, generado tráfico de fondo mediante Iperf 3 y capturado el tráfico mediante Wireshark.**

4.3 Escenario 2: Degradación de un fichero de vídeo con audio.

Ejercicio 8: Genere tres flujos con las características especificadas en la tabla anterior y capture el tráfico mediante Wireshark. ¿Cómo se escucha el audio transmitido una vez se están transmitiendo todos los flujos?¿Cómo se ve el vídeo? ¿Se llega a producir congestión?¿A qué se debe?¿En qué interfaces se produce congestión? Apóyese en el resultado obtenido mediante Wireshark:

Solución:

El flujo se genera mediante los siguientes comandos:

Desde PC3: iperf3.exe -s -p 5203
Desde PC1: iperf3.exe -c 30.0.0.3 -p 5203 -u -b 4M -l 1000 -t 0

Desde PC3: iperf3.exe -s -p 5202
Desde PC2: iperf3.exe -c 30.0.0.3 -p 5202 -u -b 6M -l 1000 -t 0

Una vez los tres flujos están siendo emitidos simultáneamente, se puede apreciar que el vídeo se queda congelado la mayor parte del tiempo. Sin embargo, el audio se escucha de forma fluida con pocos cortes de poca duración. Esto se debe a que se produce congestión en la salida de la interfaz Gigabit Ethernet 0/0, porque el enlace es de 10 Mbps y el total de los flujos utiliza un ancho de banda de aproximadamente 12 Mbps.

Figura 124.Comportamiento de los flujos obtenido mediante Wireshark.

4.3 Escenario 2: Degradación de un fichero de vídeo con audio.

Mediante Wireshark (figura 124) se obtiene que el ancho de banda queda repartido de la siguiente forma:

Ancho de banda **total**: **9,771 Mbps.**
Ancho de banda utilizado por el flujo de **Video + Audio**: **1,695 Mbps.**
Ancho de banda utilizado por el **tráfico de fondo (PC1): 3,831 Mbps.**
Ancho de banda **total utilizado por pc1: 5,527 Mbps.**
Ancho de banda utilizado por **PC2: 4,244 Mbps.**

Como se puede apreciar, el flujo más penalizado en este caso es el de tráfico de fondo generado por PC2, puesto que no consiguen transmitir aproximadamente 2 Mbps. En todas las pruebas realizadas, los flujos se han comportado de una forma similar.

Cabe destacar que se han producido muy pocas pérdidas en promedio del vídeo transmitido, puesto que en media el bitrate es de 1,695 Mbps, respecto de los 1,761 Mbps obtenidos en el ejercicio anterior. Sin embargo, pese a las pocas pérdidas producidas, el vídeo se queda congelado la mayor parte del tiempo.

Esto se debe principalmente al delay que sufre el vídeo. Pese a que no se producen muchas pérdidas, los paquetes llegan con suficiente delay como para disminuir notablemente la calidad del vídeo.

4.3.3.3 Transmisión de vídeo con audio con congestión de red (con QoS).

Finalmente, se va a estudiar cómo queda afectado el flujo de vídeo con audio en unas condiciones similares al ejercicio anterior, pero utilizando QoS.

La figura 125 muestra la ruta que seguirán los flujos a emitir.

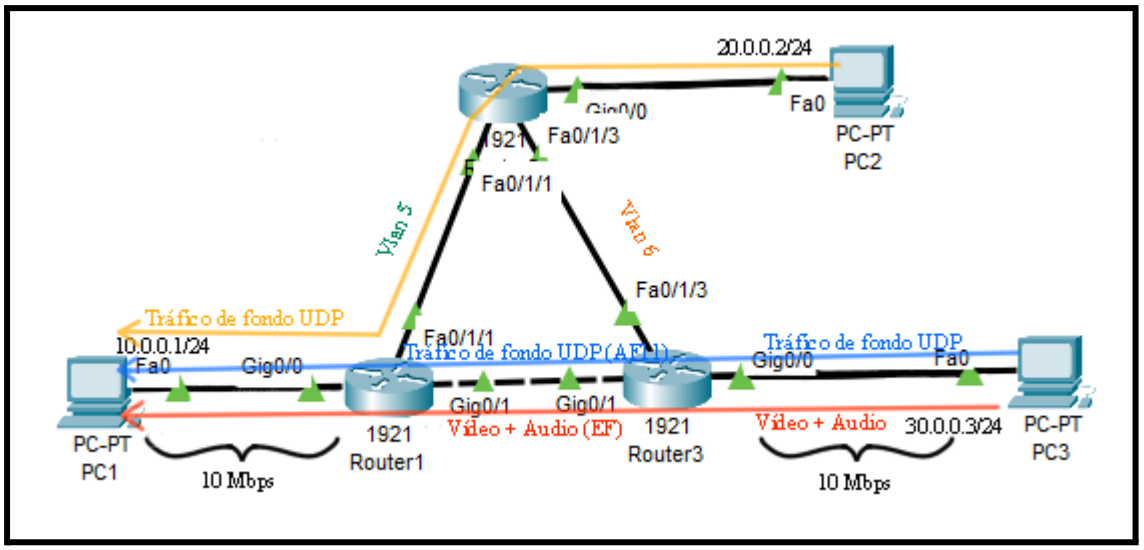


Figura 125. Topología de red y flujos a emitir.

Interacción entre equipos:

PC2: Genera tráfico UDP best effort con destino a PC1 y a PC3 con el objetivo de saturar la red.

PC3: Emite un fichero de vídeo con audio hacia PC1. Además, genera tráfico UDP que será marcado por el router con el valor 10 del campo DSCP (AF11) para saturar la red.

Router3: En la entrada de la interfaz Gigabit Ethernet 0/0 marca el tráfico RTP/RTCP/SIP con el valor 46 del campo DSCP (EF), y el tráfico UDP y TCP restante con el valor 10 (AF11). Además, garantiza y limita el ancho de banda del tráfico RTP/RTCP a 2,2 Mbps y del tráfico marcado con AF11 a 1,8 Mbps.

Router2: Encamina el tráfico generado por PC2 a PC1. No utiliza QoS.

Router1: En la salida de la interfaz Gigabit Ethernet 0/0 garantiza y limita el ancho de banda recibido por PC3 y PC2 a 5 Mbps cada uno.

4.3 Escenario 2: Degradación de un fichero de vídeo con audio.

Los flujos a emitir son los indicados por la tabla 49:

Flujo	Protocolo	IP origen	IP destino	Tamaño de paquete	bitrate (bps)	Tiempo de generación del flujo (s)	Puerto
Vídeo + Audio	RTP	30.0.0.3/24	10.0.0.1/24	-	-	-	5004
Best Effort	UDP	30.0.0.3/24	10.0.0.1/24	1000	4000000	0	5203
Best Effort	UDP	20.0.0.2/24	10.0.0.1/24	1000	6000000	0	5202

Tabla 49.Características de los flujos.

Las funciones policía que se activan en este caso son las que se muestran en la figura 126.

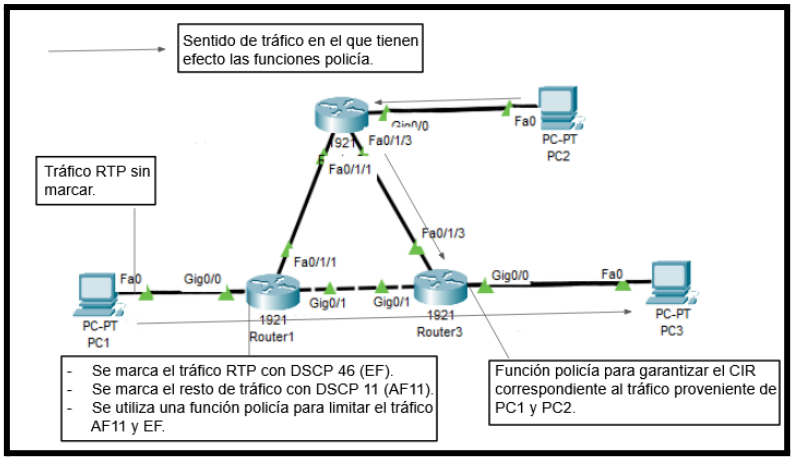


Figura 126. Sentido de tráfico en el que se aplica QoS para mejorar la calidad de experiencia de los usuarios.

La figura 127 muestra cómo quedan repartidos los flujos de acuerdo a las funciones policía.

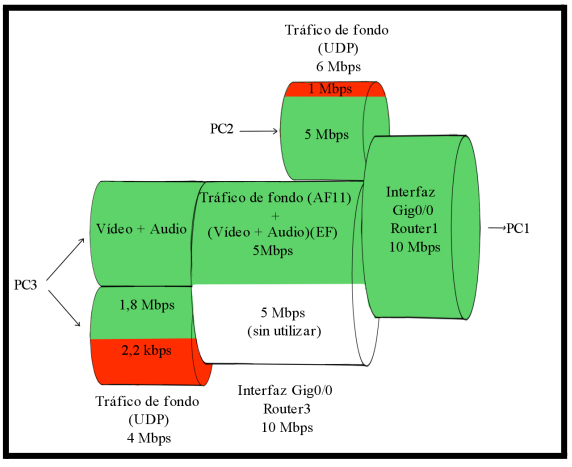


Figura 127. Comportamiento de los flujos de acuerdo a las funciones policía.

4.3 Escenario 2: Degradación de un fichero de vídeo con audio.

Para Realizar este caso de estudio se ha **generado el flujo de audio mediante VLC, recibido el stream de audio mediante VLC, generado tráfico de fondo mediante Iperf 3 y capturado el tráfico mediante Wireshark.**

Ejercicio 9: Genere tres flujos con las características especificadas en la tabla anterior y capture el tráfico mediante Wireshark. ¿Cómo se escucha el audio transmitido una vez se están transmitiendo todos los flujos?¿Cómo se ve el vídeo? ¿Cómo queda repartido el ancho de banda?¿Considera que reservar 5 Mbps para PC3 y PC2 ha sido una decisión apropiada en el caso de querer garantizar el flujo de vídeo?

Para contestar las preguntas anteriores es recomendable obtener los siguientes valores mediante la gráfica de Wireshark: ancho de banda medio y máximo del vídeo, ancho de banda medio y máximo total, ancho de banda utilizado por PC2, ancho de banda medio y máximo utilizado por PC3.

Nota: Para obtener el ancho de banda máximo utilizado por un flujo, se ha de desactivar el promediado utilizado en el filtro de Wireshark, como en la figura 128:

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
☑	Todos los paqu...	ip.dst == 30.0.0.3&& udp		Line	Bits		None	1

Figura 128. Modificación del filtro de captura de Wireshark.

Solución:

Los flujos se generan mediante los siguientes comandos de Iperf 3:

Desde PC1: iperf3.exe -s -p 5203
Desde PC3: iperf3.exe -c 10.0.0.1 -p 5203 -u -b 4M -l 1000 -t 0

Desde PC1: iperf3.exe -s -p 5202
Desde PC2: iperf3.exe -c 10.0.0.1 -p 5202 -u -b 6M -l 1000 -t 0

Una vez los tres flujos están siendo emitidos simultáneamente, se puede apreciar que tanto el vídeo como el audio se escuchan igual de bien que cuando se transmitían en una red sin congestión. Esto se debe a que se ha conseguido asegurar el flujo de vídeo con audio correctamente.

4.3 Escenario 2: Degradación de un fichero de vídeo con audio.

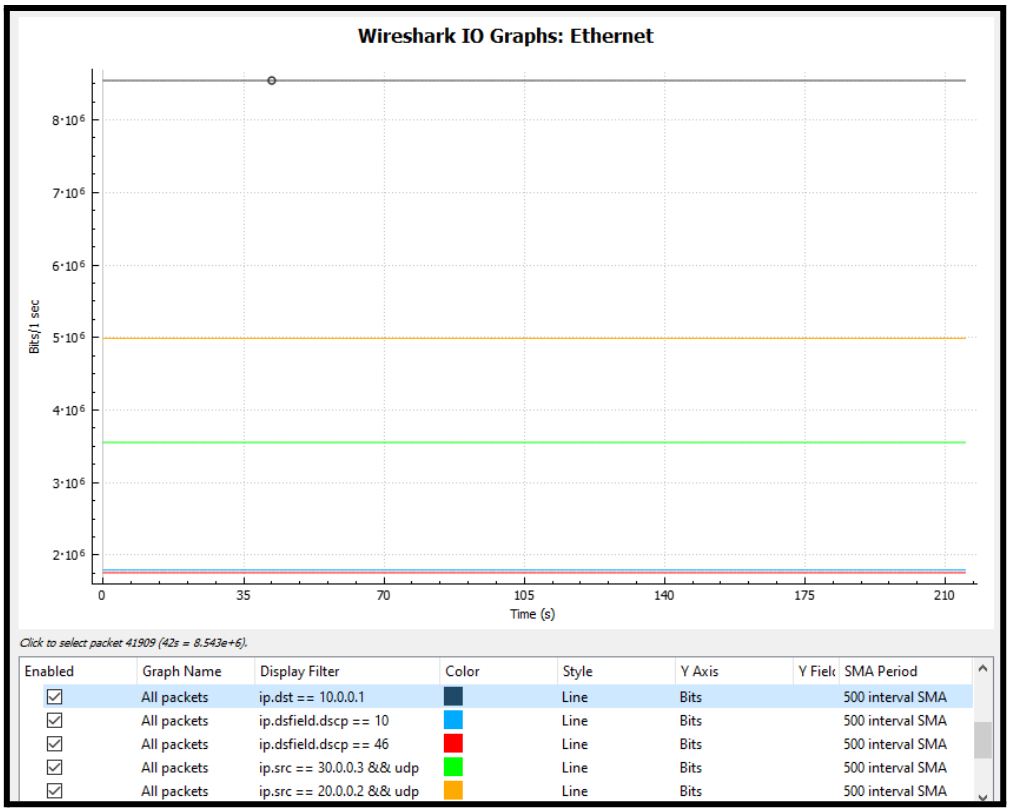


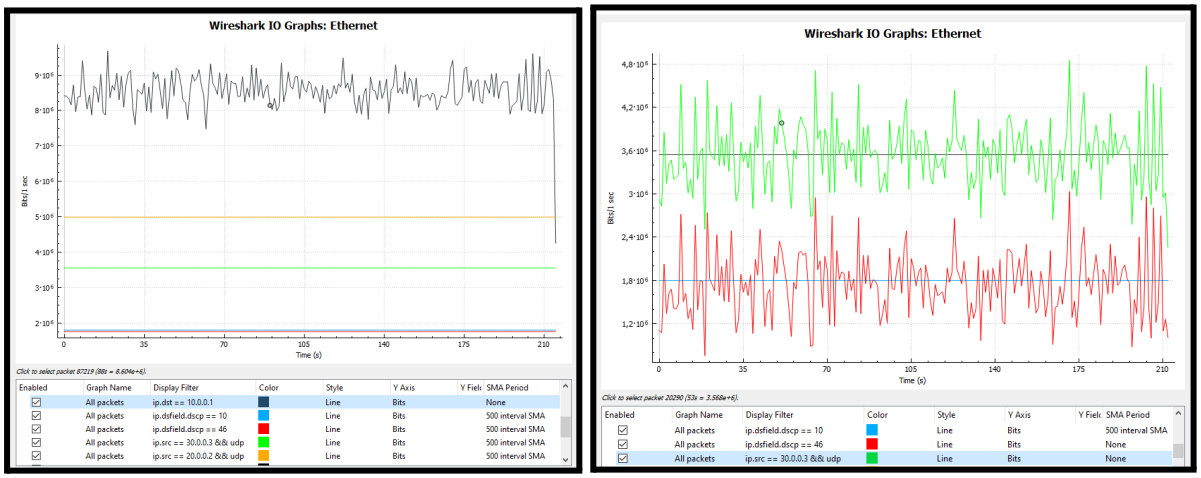
Figura 129.Comportamiento de los flujos obtenido mediante Wireshark.

Mediante esta gráfica (figura 129) se obtienen los siguientes resultados:

Ancho de banda medio **total: 8,543 Mbps.**
Ancho de banda medio utilizado por el tráfico marcado con **AF11: 1,796 Mbps.**
Ancho de banda medio del vídeo **(EF): 1,758 Mbps.**
Ancho de banda medio utilizado por **PC3: 3,554 Mbps.**
Ancho de banda medio utilizado por **PC2: 4,989 Mbps.**

Observando esta gráfica podría llegarse a pensar que el ancho de banda no está siendo utilizado adecuadamente, pues el ancho de banda total en promedio es menor a 9 Mbps.

4.3 Escenario 2: Degradación de un fichero de vídeo con audio.



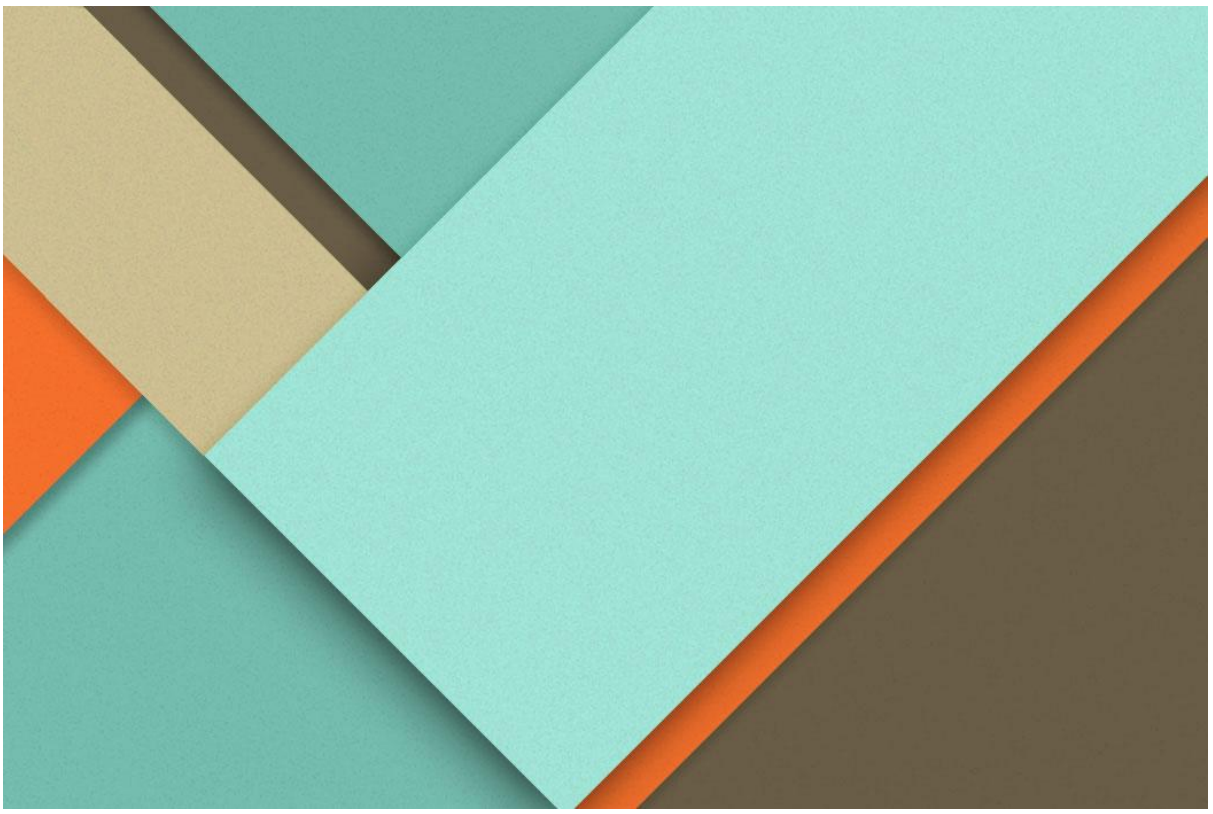
Figuras 130 y 131.Comportamiento de los flujos obtenido mediante Wireshark.

Sin embargo, analizando bien la gráfica obtenida mediante Wireshark (figuras 130 y 131), se pueden obtener los siguientes resultados:

Ancho de banda total utilizado por PC3: 4,854 Mbps
Ancho de banda máximo del vídeo (EF): 3.047 Mbps
Ancho de banda máximo: 9,683 Mbps

A pesar que el ancho de banda total en media no llegue ni siquiera a 9 Mbps, hay muchos picos de ancho de banda que superan esos 9 Mbps. Además, se observa que el ancho de banda utilizado por PC3 se acerca en varias ocasiones a 5 Mbps, siendo el pico máximo de 4,854 Mbps.

Por lo tanto, repartir el ancho de banda en 5 Mbps ha sido una decisión aceptable puesto que se han considerado los momentos de mayor bitrate del vídeo, dejando un poco de margen para que el vídeo no llegue a perder calidad.



Capítulo 5: Conclusión y Líneas Futuras

Capítulo 5. Conclusión y líneas futuras:

Como conclusión, podemos indicar que **el estudio realizado sobre las herramientas de calidad de servicio utilizadas ha sido satisfactorio,** debido a que **se han podido comprobar los efectos de las mismas mediante el uso de dispositivos reales, con poco margen de error respecto a los valores teóricos esperados.** Además, tras numerosas pruebas realizadas de los distintos ejercicios realizados a lo largo del proyecto, se ha concluido que **los ejercicios cumplen con el criterio de repetibilidad** que es uno de los principales objetivos del proyecto a cumplir, ya que debe servir como material para realizar prácticas para la asignatura **"Redes Públicas de Acceso"**.

Inicialmente, en el capítulo 2 se ha realizado una introducción a los programas utilizados para generación y captura de tráfico, que es necesaria puesto que sin dichas herramientas software no se podrían comprobar los efectos de las herramientas de calidad de servicio estudiadas. En este proyecto se ha realizado una introducción básica a los programas **Iperf3** en el caso de software para la generación de tráfico y **Wireshark** para la captura del mismo. Cabe destacar que es posible utilizar otras herramientas que realicen una función similar. Sin embargo, en este proyecto se han utilizado los programas Iperf3 y Wireshark porque son programas free open source sencillos de utilizar.

Uno de los inconvenientes de utilizar Iperf3 en el caso de los capítulos 2 y 3 es que se necesitan hasta tres procesos cliente-servidor distintos, esto quiere decir que **hay un cierto error que no se puede calcular en las medidas obtenidas respecto de los parámetros de calidad de servicio que calcula Iperf3, puesto que dichos procesos no se ejecutan al mismo tiempo**, sino que unos procesos se ejecutan antes que los otros, y **pueden transcurrir segundos desde que se ejecuta el primer proceso hasta que se ejecuta el siguiente proceso**. Cabe destacar que en ese intervalo de tiempo, el flujo de datos comienza su transmisión antes de que el sistema se presente en las condiciones de congestión deseadas, afectando a las medidas deseadas. A pesar de que los parámetros de calidad de servicio no han sido alterados en gran medida, **se podría mejorar el proyecto añadiendo un servidor externo que gestione las conexiones entre cliente y servidor de los distintos procesos, para que dichos procesos se ejecuten de forma simultánea.**

En el **capítulo 3** se ha estudiado el uso de las herramientas de calidad de servicio correspondientes con los **planificadores de cola en dispositivos CISCO**. **Para poder configurar dichos planificadores correctamente se han estudiado las herramientas de calidad de servicio de clasificación y marcado** (tanto a nivel 2, como a nivel 3).

En concreto, se han estudiado los planificadores de cola: **Priority Queue, Weighted Round Robin, Priority Queue junto a Weighted Round Robin y Class based Weighted Fair Queueing**, que corresponden con los planificadores que se estudian de forma teórica en la asignatura "Redes Públicas de Acceso". Además, se han realizado una serie de casos de estudio de cada planificador, para **determinar las características de cada uno de los diferentes planificadores de forma que se puedan apreciar las ventajas y desventajas que presentan unos planificadores respecto de otros.**

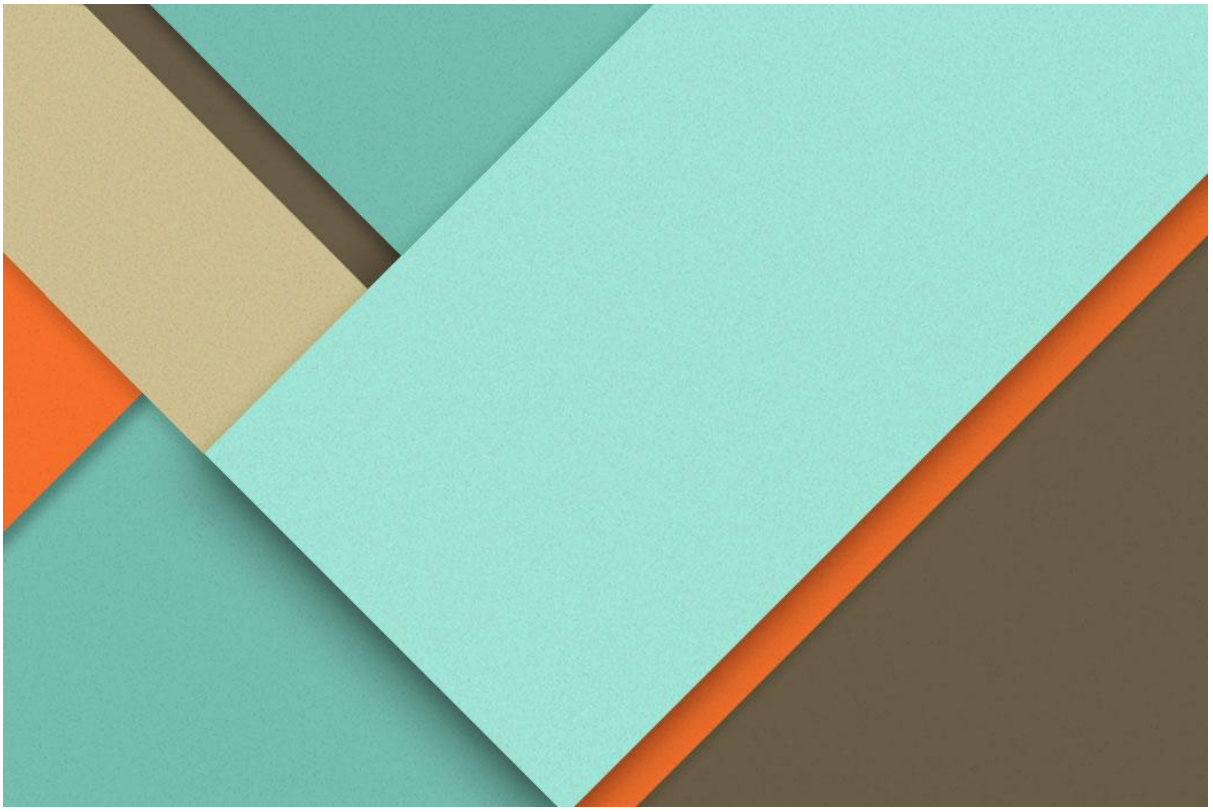
En este proyecto **se ha concluido que el planificador cuyos resultados son mejores respecto de los planificadores estudiados es el Class based Weighted Fair Queueing**, puesto que se le puede **asignar el ancho de banda deseado indicando directamente el porcentaje correspondiente a cada flujo** y los resultados muestran que **a pesar de que varíe el tamaño de los paquetes de los distintos flujos, no tiene mucha influencia en el resultado obtenido, a diferencia del planificador Weighted Round Robin** en el que la variación entre el tamaño de los paquetes de los distintos flujos sí influye en gran medida.

Una de las posibles mejoras de este proyecto es el **uso de otro tipo de tráfico distinto al tráfico Best Effort utilizado, como podría ser la transmisión de vídeo**, de forma que se pudiera **comprobar** visualmente **como quedaría afectada la calidad del vídeo en función de los pesos y prioridades** asignadas a dicho flujo de vídeo **para los distintos planificadores utilizados.**

Finalmente, en el **capítulo 4 se han estudiado el uso de las herramientas de calidad de servicio correspondientes a las funciones policía, y al marcado DSCP**.

El marcado DSCP ha sido utilizado para diferenciar el tráfico con el objetivo de que la función policía garantice un ancho de banda deseado en función del marcado del mismo. Como resultado, hemos podido observar que **utilizando las funciones policía y el marcado correctamente, se ha conseguido priorizar el tráfico de interés**, que en este caso es un fichero de audio y un fichero de audio y vídeo, **de forma que a pesar de que el sistema esté muy congestionado dicho tráfico de interés se haya conseguido transmitir sin pérdidas.** Cabe destacar que para conseguir que el tráfico de interés no presente pérdidas, **se penaliza notablemente el resto del tráfico.**

Finalmente, una posible ampliación a realizar sobre este proyecto es conseguir unos resultados similares utilizando el programa GNS3, que es capaz de emular los dispositivos de cisco, para poder estudiar los efectos que se muestran en este proyecto sin necesidad de disponer del laboratorio de prácticas.



Anexos

Anexos:

ANEXO A: configuración de red de los ordenadores:

Para poder observar los efectos de los distintos planificadores del switch es necesario configurar los distintos PCs de forma que sea posible una comunicación entre ellos.

De esta forma, se ha de configurar cada ordenador con una IP distinta, una máscara y una puerta de enlace o gateway.

Para llevar a cabo esta tarea se deben de seguir los siguientes pasos:

1. En el buscador de windows se debe de buscar "panel de control" y hacer click en la aplicación "Panel de control".

2. Dentro del panel de control se debe seleccionar la opción "Redes e Internet", como se puede apreciar en la figura 132.

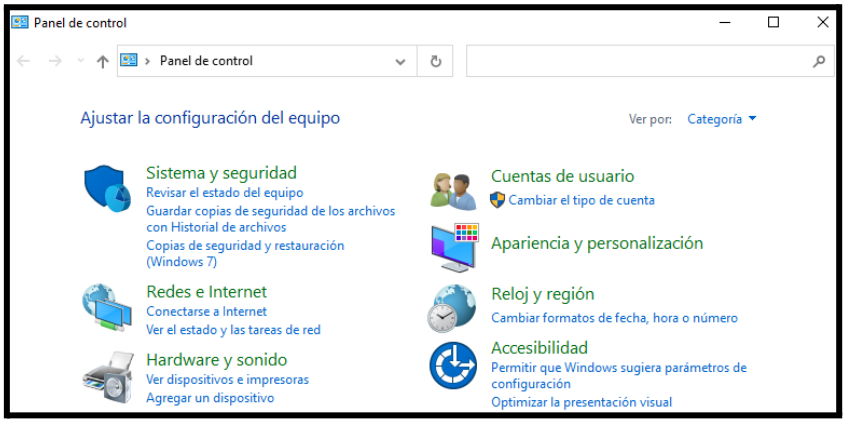


Figura 132. Configuración de red de los PCs, paso 2.

3. Se debe hacer clic en "Centro de redes y recursos compartidos", como se puede apreciar en la figura 133.

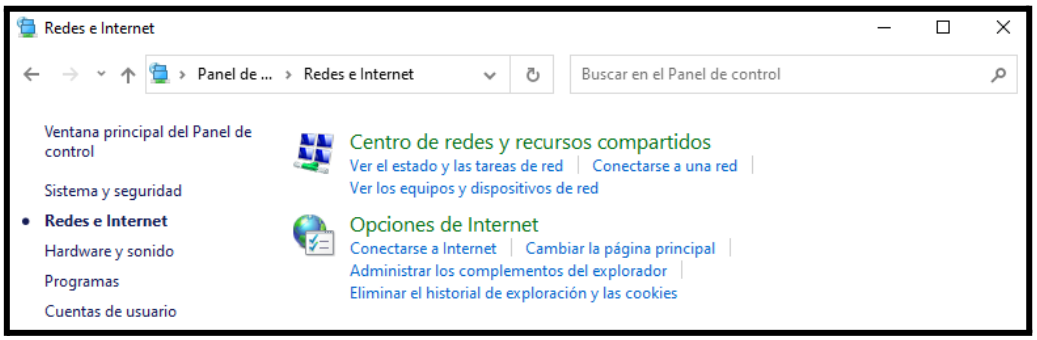


Figura 133. Configuración de red de los PCs, paso 3.

4. Dentro de "Centro de redes y recursos compartidos" se debe de hacer clic en "Ethernet", como se puede apreciar en la figura 134.

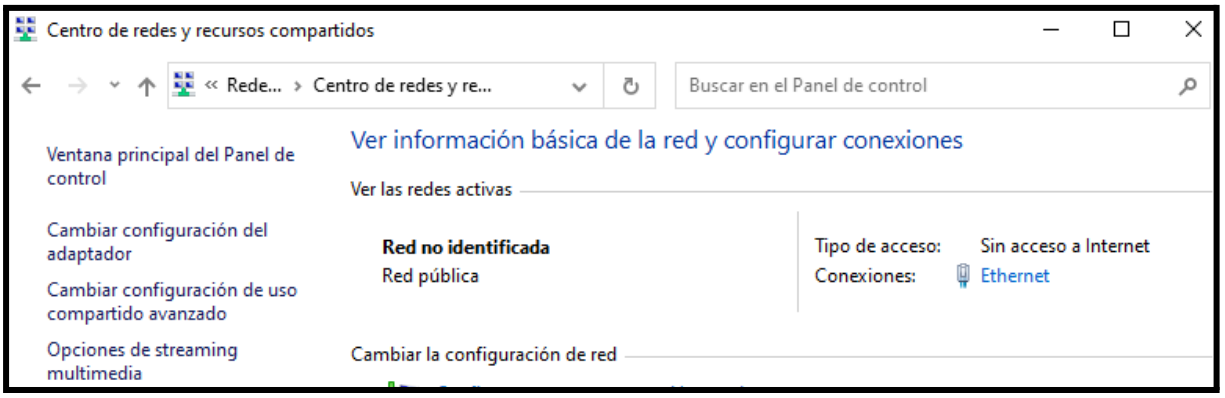


Figura 134. Configuración de red de los PCs, paso 4.

5. Una vez ha aparecido el siguiente menú (figura 135), se ha de pulsar "Propiedades".

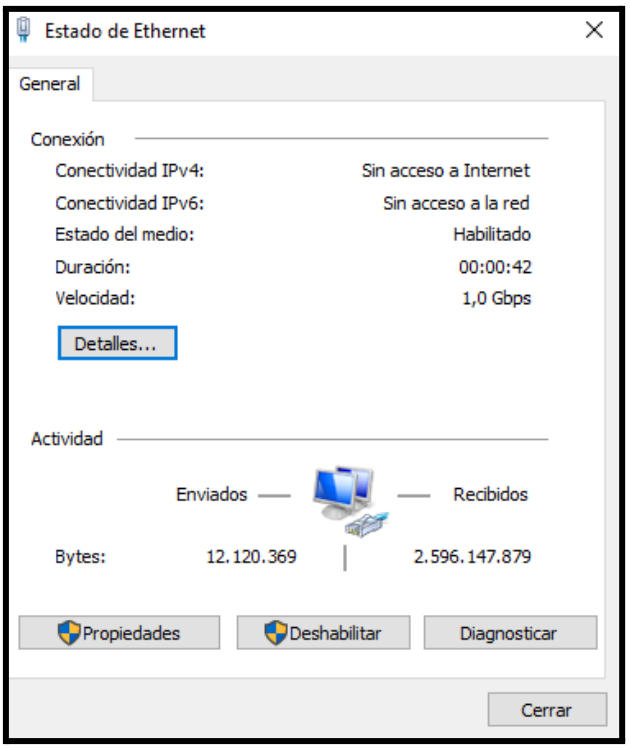


Figura 135. Configuración de red de los PCs, paso 5.

6. Tras la aparición del siguiente menú (figura 136) es necesario hacer click en "Protocolo de internet versión 4 (TCP/IPv4)" y posteriormente en "Propiedades".

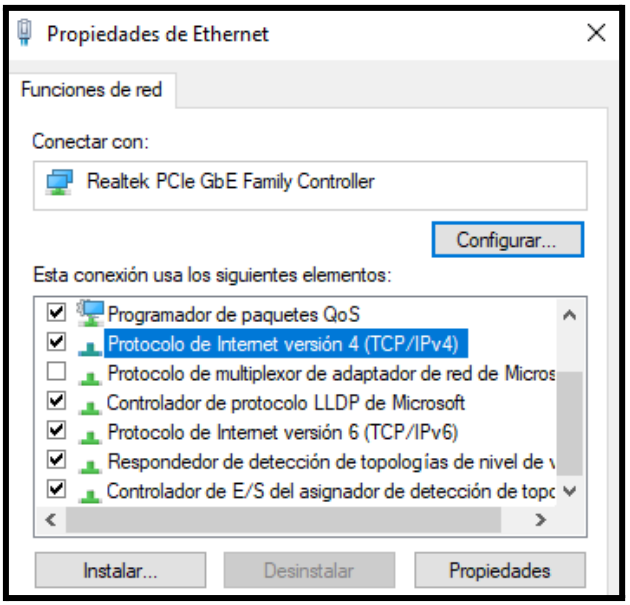


Figura 136. Configuración de red de los PCs, paso 6.

7. Finalmente, se deberá de configurar todos los PCs con la dirección ip y máscara especificada. La figura 137 muestra la forma en la que debe de ser configurado PC_4. Finalmente, se debe de pulsar "Aceptar".

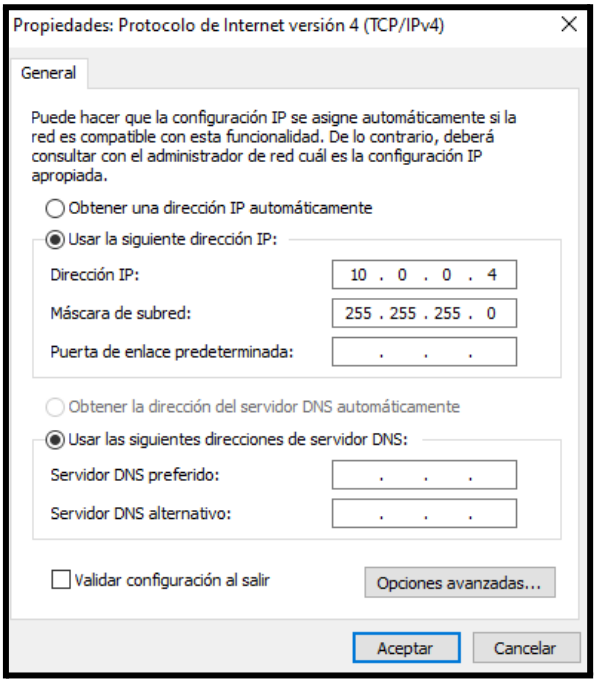


Figura 137. Configuración de red de los PCs, paso 7.

ANEXO B: Desactivación del Firewall de Windows:

Previamente a realizar el montaje de la red es recomendable comprobar que el Firewall de Windows esté desactivado.

Para desactivar el Firewall se deben de seguir los siguientes pasos:

1. Dentro del panel de control se debe seleccionar la opción "Sistema y seguridad".
2. En el siguiente menú (figura 138) se debe seleccionar "Firewall de Windows Defender".

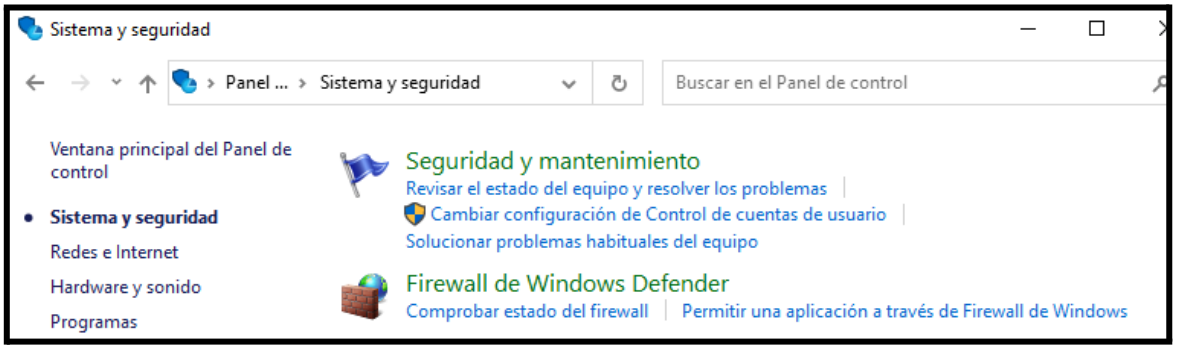


Figura 138. Desactivación del Firewall, paso 2.

3. En este caso (figura 139) podemos observar que el firewall está activo. Para desactivarlo se ha de hacer click en "Activar o desactivar el Firewall de Windows Defender".

Figura 139. Desactivación del Firewall, paso 3.

4. Finalmente, se debe desactivar el firewall y pulsar "Aceptar", como se puede apreciar en la figura 140.

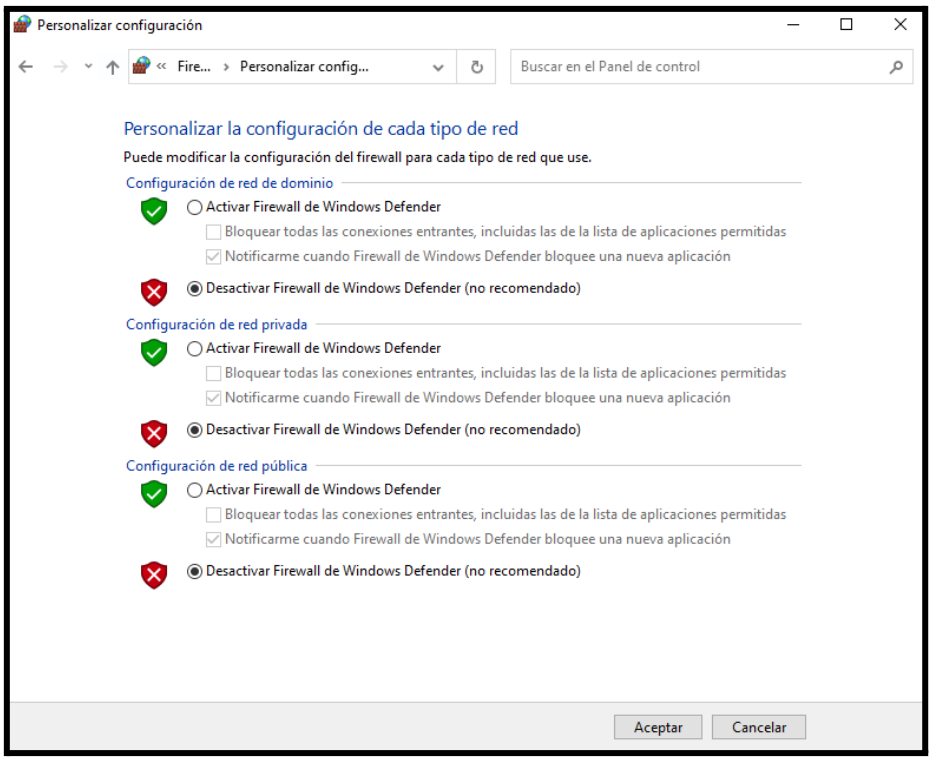


Figura 140. Desactivación del Firewall, paso 4.

ANEXO C: Archivo de configuración del router utilizado en el capítulo 3:

- **Router:**

```
!
!Configuramos la clase "pc3" de forma que comprenda los paquetes marcados con precedence 7.
class-map match-any pc3
match precedence 7
!
!Configuramos la clase "pc2" de forma que comprenda los paquetes marcados con precedence 3.
class-map match-any pc2
match precedence 3
!
!Configuramos la clase "pc1" de forma que comprenda los paquetes marcados con precedence 1.
class-map match-any pc1
match precedence 1
!Configuramos el planificador CBWFQ de forma que le corresponda un 16% del ancho de banda a la
!clase "pc1", un 33% del ancho de banda a la clase "pc2", un 50% del ancho de banda a
!la clase "pc3", y un 1% al resto de tráfico.
policy-map cbwfq
class pc1
bandwidth percent 16
class pc2
bandwidth percent 33
class pc3
bandwidth percent 50
class class-default
bandwidth percent 1
!
!Configuramos la interfaz GigabitEthernet0/1. Se configura la dirección IP y se asigna el planificador
!CBWFQ a la salida de la interfaz..
interface GigabitEthernet0/0
ip address 12.0.0.12 255.255.255.0
no shutdown
duplex auto
speed 10
service-policy output cbwfq
!
!Configuramos la interfaz GigabitEthernet0/1. Solamente se configura la dirección IP.
interface GigabitEthernet0/1
ip address 10.0.0.10 255.255.255.0
duplex auto
speed auto
```

ANEXO D: Archivos de configuración de los routers utilizados en el capítulo 4:

- **Router 1:**

```
hostname Router_1
!
!Configuramos la clase "pc2_pc1" de acuerdo a la ACL 102. De esta forma, los paquetes que cumplen
!con la ACL 102 forman esta clase.
class-map match-any pc2_pc1
 match access-group 102
!
!Configuramos la clase "pc3_pc1" de acuerdo a la ACL 103. De esta forma, los paquetes que cumplen
!con la ACL 103 forman esta clase.
class-map match-any pc3_pc1
 match access-group 103
!
!Configuramos la función policía "policia_10M" para garantizar una tasa de tráfico correspondiente
!a las clases "pc2_pc1" y "pc3_pc1" de 5 Mbps con un bc de 625 kbytes. Si el tráfico supera
!su tasa correspondiente, es descartado.
policy-map policia_10M
 class pc2_pc1
  police cir 5000000 bc 625000
   conform-action transmit
   exceed-action drop
 class pc3_pc1
  police cir 5000000 bc 625000
   conform-action transmit
   exceed-action drop
!Configuramos la función policía "policia_128" para garantizar una tasa de tráfico correspondiente
!a la clase "pc2_pc1" de 28 kbps con un bc de 3,5 kbytes, y una tasa de 100 kbps de tráfico
!correspondiente a la clase "pc3_pc1". Si el tráfico supera su tasa correspondiente, es descartado.
policy-map policia_128
 class pc2_pc1
  police cir 28000 bc 3500
   conform-action transmit
   exceed-action drop
 class pc3_pc1
  police cir 100000 bc 12500
   conform-action transmit
   exceed-action drop
```

ANEXO D: Archivos de configuración de los routers utilizados en el capítulo 4:

```
!Configuramos la función policía "bw_recortado_128" para que garantice una tasa de tráfico de
!128000 bps con un bc de 16000 bytes. Además, si el tráfico excede esa tasa, será descartado.
policy-map bw_recortado_128
 class class-default
  police cir 128000 bc 16000
   conform-action transmit
   exceed-action drop
!
!Configuramos la interfaz GigabitEthernet0/0. Se configura la dirección IP, la función policía
! "bw_recortado_128" a la entrada de la interfaz y la función policía "policia_128" a la salida
!de la misma.
interface GigabitEthernet0/0
 ip address 10.0.0.10 255.255.255.0
 no shutdown
 duplex auto
 speed 10
 service-policy input bw_recortado_128
 service-policy output policia_128
!
!Configuramos la interfaz GigabitEthernet0/1. Solamente se configura la dirección IP.
interface GigabitEthernet0/1
 ip address 40.0.0.10 255.255.255.0
 no shutdown
 duplex auto
 speed auto
!
!Configuramos la interfaz FastEthernet0/1/1. Se le asigna la Vlan 5.
interface FastEthernet0/1/1
 switchport access vlan 5
 no ip address
!
!Configuramos la interfaz Vlan5. Se le asigna la dirección IP correspondiente.
interface Vlan5
 ip address 50.0.0.10 255.255.255.0
!
!Configuramos el protocolo de encaminamiento RIP, para que el router pueda encaminar paquetes a
!redes que no sean locales respecto del router.
router rip
 network 10.0.0.0
 network 40.0.0.0
 network 50.0.0.0
!
!Configuramos la ACL 102 para permitir el tráfico UDP, TCP e ICMP proveniente de PC2 con
!destino PC1.
access-list 102 permit udp host 20.0.0.2 host 10.0.0.1
```

```
access-list 102 permit tcp host 20.0.0.2 host 10.0.0.1
access-list 102 permit icmp host 20.0.0.2 host 10.0.0.1
!Configuramos la ACL 103 para permitir el tráfico UDP, TCP e ICMP proveniente de PC3 con
!destino PC1.
access-list 103 permit udp host 30.0.0.3 host 10.0.0.1
access-list 103 permit tcp host 30.0.0.3 host 10.0.0.1
access-list 103 permit icmp host 30.0.0.3 host 10.0.0.1
end
```

- **Router 2:**

```
hostname Router_2
!Configuramos la interfaz GigabitEthernet0/0. Solamente se configura la dirección IP.
interface GigabitEthernet0/0
 ip address 20.0.0.20 255.255.255.0
 no shutdown
 duplex auto
 speed auto
!Configuramos la interfaz FastEthernet0/1/1. Se le asigna la Vlan 5.
interface FastEthernet0/1/1
 switchport access vlan 5
 no ip address
!
!Configuramos la interfaz FastEthernet0/1/3. Se le asigna la Vlan 6.
interface FastEthernet0/1/3
 switchport access vlan 6
 no ip address
!
!Configuramos la interfaz Vlan5. Se le asigna la dirección IP correspondiente.
interface Vlan5
 ip address 50.0.0.20 255.255.255.0
!
!Configuramos la interfaz Vlan6. Se le asigna la dirección IP correspondiente.
interface Vlan6
 ip address 60.0.0.20 255.255.255.0
!
!Configuramos el protocolo de encaminamiento RIP, para que el router pueda encaminar paquetes a
!redes que no sean locales respecto del router.
router rip
 network 20.0.0.0
 network 50.0.0.0
 network 60.0.0.0

!
end
```

- **Router 3:**

```
hostname Router_3
!
!Configuramos la clase "pc3_pc1" de acuerdo a la ACL 100. De esta forma, los paquetes que cumplen
!con la ACL 100 forman esta clase.
class-map match-any pc3_pc1
 match access-group 100
!
!Configuramos la clase "audio" de forma que los paquetes sip, rtp y rtcp forman esta clase.
class-map match-any audio
 match protocol rtp
 match protocol rtcp
 match protocol sip
!
!Configuramos la función policía "pc3_pc1_10M" para marcar los paquetes de la clase "audio" con el
!valor DSCP EF y los paquetes de la clase "pc3_pc1" con valor AF11. Además, garantiza una tasa de
!tráfico correspondiente a la clase "audio" de 2,2 Mbps con un bc de 262.5 kbytes y una tasa de
!1,8 Mbps con un bc de 225 kbytes, en el caso de tráfico correspondiente a la clase "pc3_pc1".
!Si el tráfico supera su tasa correspondiente es descartado.
policy-map pc3_pc1_10M
 class audio
  set dscp ef
   police cir 2200000 bc 262500
     conform-action transmit
     exceed-action drop
 class pc3_pc1
  set dscp af11
   police cir 1800000 bc 225000
     conform-action transmit
     exceed-action drop
!
!Configuramos la función policía "bw_recortado_128" para que garantice una tasa de tráfico de
!128000 bps con un bc de 16000 bytes. Además, si el tráfico excede esa tasa, será descartado.
policy-map bw_recortado_128
 class class-default
   police cir 128000 bc 16000
     conform-action transmit
     exceed-action drop
```

```
!
!Configuramos la función policía "pc3_pc1_128" para marcar los paquetes de la clase "audio" con el
!valor DSCP EF y los paquetes de la clase "pc3_pc1" con valor AF11. Además, garantiza una tasa de
!tráfico correspondiente a la clase "audio" de 88 kbps con un bc de 11000 bytes, una tasa de 12 kbps
!con un bc de 1500 bytes, en el caso de tráfico correspondiente a la clase "pc3_pc1", y una tasa de
!28 kbps con un bc de .3500 bytes. Si el tráfico supera su tasa correspondiente es descartado.
policy-map pc3_pc1_128
 class audio
  set dscp ef
   police cir 88000 bc 11000
     conform-action transmit
     exceed-action drop
 class pc3_pc1
  set dscp af11
   police cir 12000 bc 1500
     conform-action transmit
     exceed-action drop
 class class-default
   police cir 28000 bc 3500
     conform-action transmit
     exceed-action drop
!
!Configuramos la interfaz GigabitEthernet0/1. Se configura la dirección IP, la función policía
!"pc3_pc1_128" a la entrada de la interfaz y la función policía "bw_recortado_128" a la salida
!de la misma.
interface GigabitEthernet0/0
 ip address 30.0.0.30 255.255.255.0
 no shutdown
 duplex auto
 speed 10
 service-policy input pc3_pc1_128
 service-policy output bw_recortado_128
!
!Configuramos la interfaz GigabitEthernet0/1. Solamente se configura la dirección IP.
interface GigabitEthernet0/1
 ip address 40.0.0.30 255.255.255.0
 no shutdown
 duplex auto
 speed auto
!
!Configuramos la interfaz FastEthernet0/1/3. Se le asigna la Vlan 6.
interface FastEthernet0/1/3
 switchport access vlan 6
```

ANEXO D: Archivos de configuración de los routers utilizados en el capítulo 4:

```
!
!Configuramos la interfaz Vlan6. Se le asigna la dirección IP correspondiente.
interface Vlan6
 ip address 60.0.0.30 255.255.255.0
!
!Configuramos el protocolo de encaminamiento RIP, para que el router pueda encaminar paquetes a
!redes que no sean locales respecto del router.
router rip
 network 30.0.0.0
 network 60.0.0.0
 network 40.0.0.0
!
!Configuramos la ACL 100 para permitir el tráfico proveniente de PC3 con destino PC1,
!teniendo en cuenta que no se permiten los paquetes UDP que utilizan el puerto 5004, puesto que
!este es utilizado para la transmisión de los ficheros de audio y audio+vídeo.
access-list 100 deny   udp host 30.0.0.3 host 10.0.0.1 eq 5004
access-list 100 permit udp host 30.0.0.3 host 10.0.0.1
access-list 100 permit tcp host 30.0.0.3 host 10.0.0.1
!
en
```

Bibliografía:

[1] Barreiros, M.; Lundqvist, P. "QOS-Enabled Networks Tools and Foundations" *John Wiley & Sons*, United Kingdom, 2016.

[2] Balchunas, A. "QoS and Queuing v1.31", https://www.routeralley.com/guides/qos_queuing.pdf, 2010. El documento es accesible a fecha 22-02-2023.

[3] Cisco,"Configuring VLANs",

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_40_se/configuration/guide/scg/swvlan.pdf . El documento es accesible a fecha 22-02-2023.

[4] bobkirby;manjur, "Implementing 802.1q VLANs on a Cisco ICS 7750 Using Version 2.5 or 2.6", https://www.cisco.com/c/en/us/support/docs/voice-unified-communications/ics-7700-series-integrated-communication-systems/41662-vlans-7750-25.html, December 13, 2005. El documento es accesible a fecha 22-02-2023.

[5] aryoba, "QoS Basic and Implementation", https://www.dslreports.com/faq/14597, 20-09-2017. El documento es accesible a fecha 22-02-2023.

[6] Cisco,"Configuring Policy Maps",

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5600/sw/qos/7x/b_5600_QoS_Config_7x/configuring_policy_maps.pdf. El documento es accesible a fecha 22-02-2023.

[7] Cisco, "qos_queues",

https://www.cisco.com/assets/sol/sb/Switches_Emulators_v2_3_5_xx/help/350_550/index.html#page/tesla_350_550_olh/qos_queues.html. El documento es accesible a fecha 22-02-2023.

[8] Cisco, "Catalyst 2950 and Catalyst 2955 Switch Software Configuration Guide",

https://fulmanski.pl/zajecia/net/zajecia_20132014/cisco_devices/2950SCG.pdf, 2004. El documento es accesible a fecha 22-02-2023.

[9] Stephen J., "A quick look at WRR.", https://ccie-or-null.net/2012/06/07/a-quick-look-at-wrr/, 2012. El enlace es accesible a fecha 22-02-2023.

[10] Cisco, "Catalyst 2950 Series Switches Quality of Service (QoS) FAQ",

https://www.cisco.com/c/en/us/support/docs/lan-switching/lan-quality-of-service/46523-2950qosfaq.html, 2005. El documento es accesible a fecha 22-02-2023.

[11] anónimo,"IEEE 802.1Q", https://hmong.es/wiki/802.1Q_VLAN_tagging, 2019. El enlace es accesible a fecha 22-02-2023.

[12] Cisco Press, "Classification and Marking for Cisco DQOS and QOS Exams", https://www.ciscopress.com/articles/article.asp?p=101170&seqNum=2, 2003. El enlace es accesible a fecha 22-02-2023.

[13] NAVILOR, "How to get a live u-Law WAV stream to Cisco VOIP servers", https://videoblerg.wordpress.com/2016/03/01/how-to-get-a-live-u-law-wav-stream-to-cisco-voip-servers/, 2017. El enlace es accesible a fecha 22-02-2023.

[14] FFmpeg, "Limiting the output bitrate" https://trac.ffmpeg.org/wiki/Limiting%20the%20output%20bitrate , 2018. El enlace es accesible a fecha 22-02-2023.

[15] Wikipedia, "IEEE 802.1Q", https://en.wikipedia.org/wiki/IEEE_802.1Q, 2022 (última actualización). El enlace es accesible a fecha 22-02-2023.

[16] Wikipedia, " IEEE 802.1p", https://es.wikipedia.org/wiki/IEEE_802.1p, 2020 (última actualización). El enlace es accesible a fecha 22-02-2023.

[17] Lee, G., "Virtual Local Area Network Tag" , https://www.sciencedirect.com/topics/computer-science/virtual-local-area-network-tag, 2014. El enlace es accesible a fecha 22-02-2023.

[18] movement3, "QoS basics", https://movement3.wordpress.com/2010/11/03/qos-basics/, 2010. El enlace es accesible a fecha 22-02-2023.

[19] NetFlow Analyzer, "Understanding IP Precedence, ToS, and DSCP", https://blogs.manageengine.com/network/netflowanalyzer/2012/04/24/understanding-ip-precedence-tos-dscp.html, 2012. El enlace es accesible a fecha 22-02-2023.

[20] Tony G., "QoS: Class Selector PHB and DSCP Values", https://bethepacketsite.wordpress.com/2016/09/29/qos-class-selector-phb-and-dscp-values/, 2016. El enlace es accesible a fecha 22-02-2023.