

## **ANEXO D. DEMOSTRACIÓN PRÁCTICA DE LA IMPLEMENTACIÓN MULTICAST EN EL EDIFICIO DE INGENIERÍAS Y EL MBONE**

Existen varios conjuntos de herramientas que se pueden utilizar para trabajar con la tecnología multicast y que proveen mecanismos para conocer y anunciar las sesiones creadas en el Mbone y dentro de la red local y de manera transparente al usuario se encargan de los programas necesarios para interpretar el tipo de información que se recibe o que se transmite ya sea voz, video o datos.

Las herramientas utilizadas en este proyecto de grado son: el SDR asociado a las herramientas VIC, RAT, WB y NTE; Mash asociado a las herramientas VIC, VAT, MB y Collaborator y el Cisco IP/TV.

Finalmente se hace un estudio del impacto en el desempeño de la red interna y el enlace hacia Internet causado por el consumo de ancho de banda de las herramientas utilizadas; esto se realizó por medio del software de gestión y monitoreo con los que cuenta la administración de la red de datos de la Universidad.

### **HERRAMIENTAS MULTICAST**

#### **SDR – Directorio de Sesión**

Esta es una herramienta que permite crear y anunciar sesiones para que sean difundidas en diferentes ámbitos: local, regional o mundial. El SDR mantiene un registro de las sesiones que se han creado y las guarda en un archivo cache que utiliza cada vez que es lanzado y mientras se encuentra activo aprende nuevas sesiones y las guarda en este archivo a través de los protocolos SAP y SDP. Estos protocolos contienen información del tipo de sesión, la persona que la creó, su

ubicación, el tiempo de duración y su periodicidad, los medios y formatos que se utilizan en la sesión y si es cifrada, codificada o requiere algún tipo de autenticación.

El SDR escucha los paquetes SAP en la dirección bien conocida 224.2.127.254. Para unirse a una sesión multimedia, se necesita saber que puerto y que dirección de grupo multicast se están utilizando para la sesión, estos parámetros son asignados dinámicamente cuando se crea una sesión.

Esta herramienta es desarrollada por el Grupo de Investigación de Red y Multimedia de la UCL (University College London), que también desarrolla las herramientas de video VIC (Video Conference Tool), de audio RAT (Robust Audio Tool), de datos NTE (Network Text Editor) y WB (White Board); estas herramientas se pueden obtener en la página <http://www-mice.cs.ucl.ac.uk/multimedia/software/>.

Después de haber probado todas las herramientas, el SDR fue la que presentó menos inconvenientes y por lo tanto fue la más utilizada en el proyecto.

En la figura 1 se puede observar la ventana principal del SDR donde se anuncian varias sesiones.

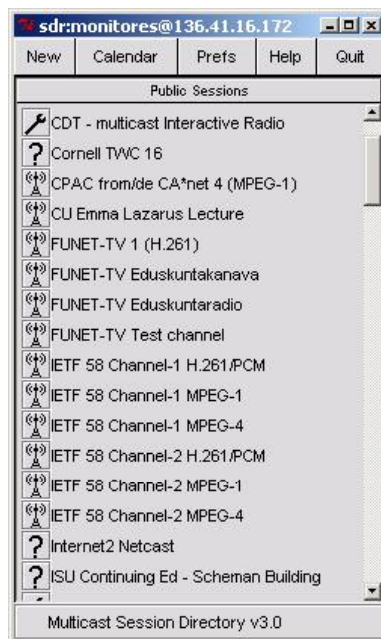


Figura 1. Ventana principal del SDR

## RAT - Robust Audio Tool

El RAT es desarrollado por el mismo grupo de investigación que el SDR; permite transmitir y recibir audio a través de diferentes mecanismos de codificación como PCM, Freeamp MP3 audio, DVI, GSM y LPC. RAT tiene facilidades para monitorear diferentes índices de transmisión y recepción utilizando los protocolos RTP y RTCP.

La ventana principal del RAT se muestra en la figura 2.

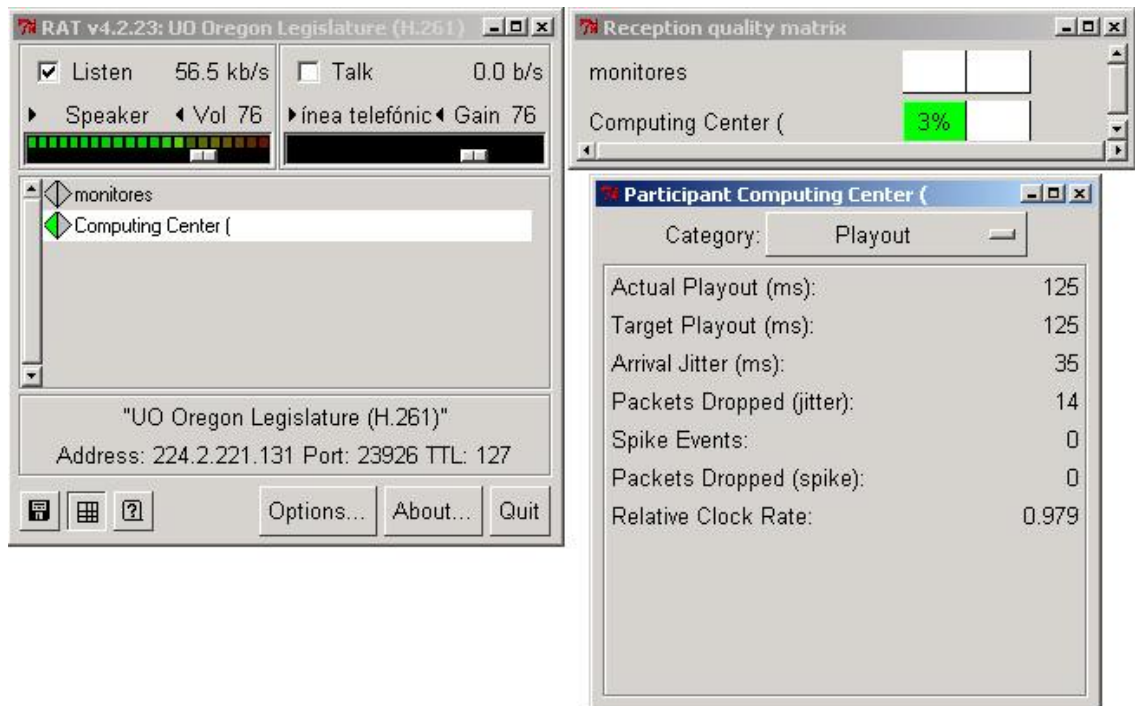


Figura 2. Ventana principal del RAT

## VIC – Video Conference Tool

Al igual que RAT, VIC permite diferentes métodos de codificación como H.261, nv, MJPEG, Cell B y PVH, también se puede configurar el número de tramas por segundo (f.p.s) que se quiere transmitir, la velocidad de transmisión en bits por segundo, la calidad, las dimensiones y las características de decodificación en recepción. VIC también utiliza mecanismos de monitoreo para la calidad de transmisión y recepción.

La ventana principal del VIC se muestra en la figura 3.

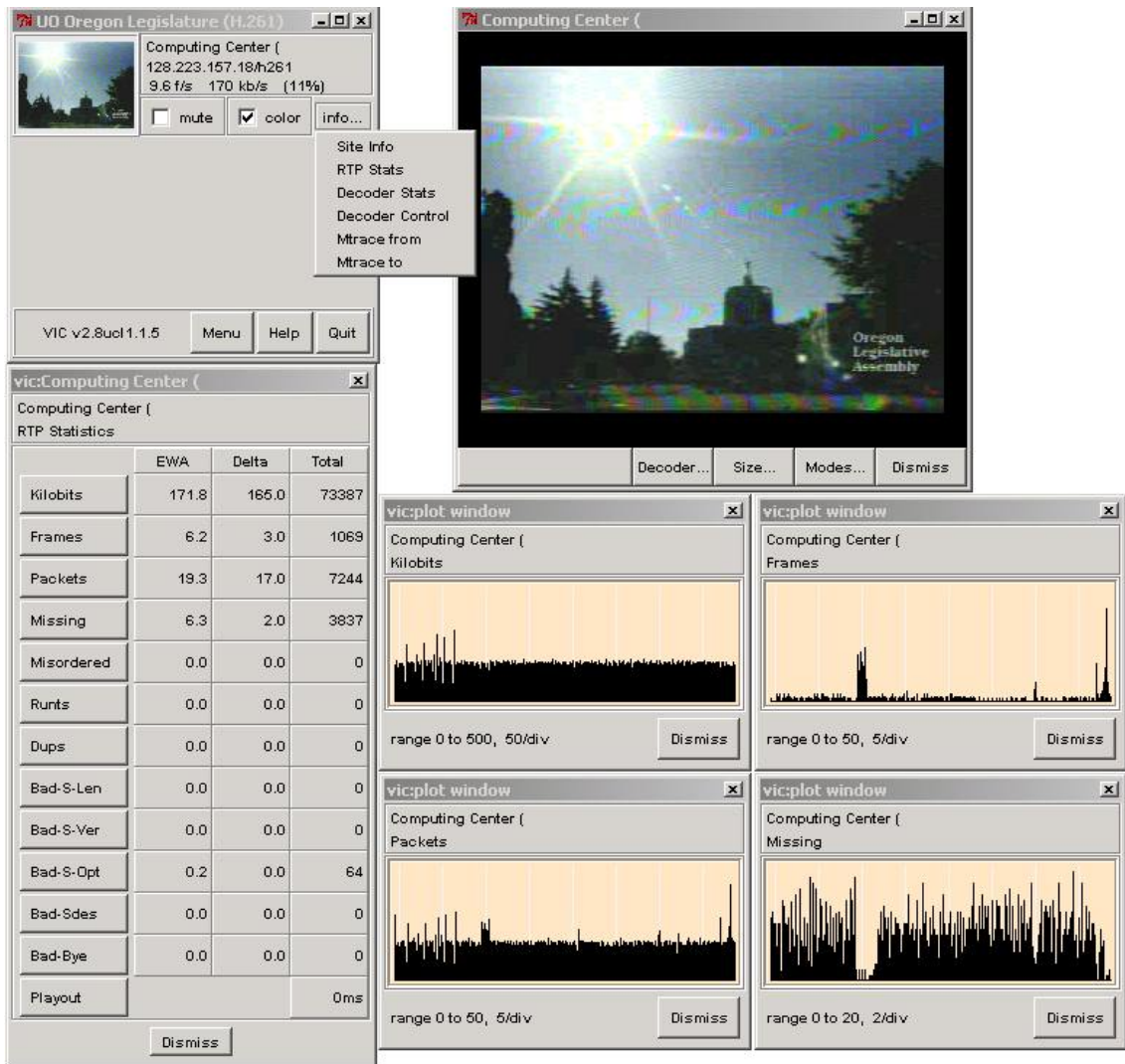
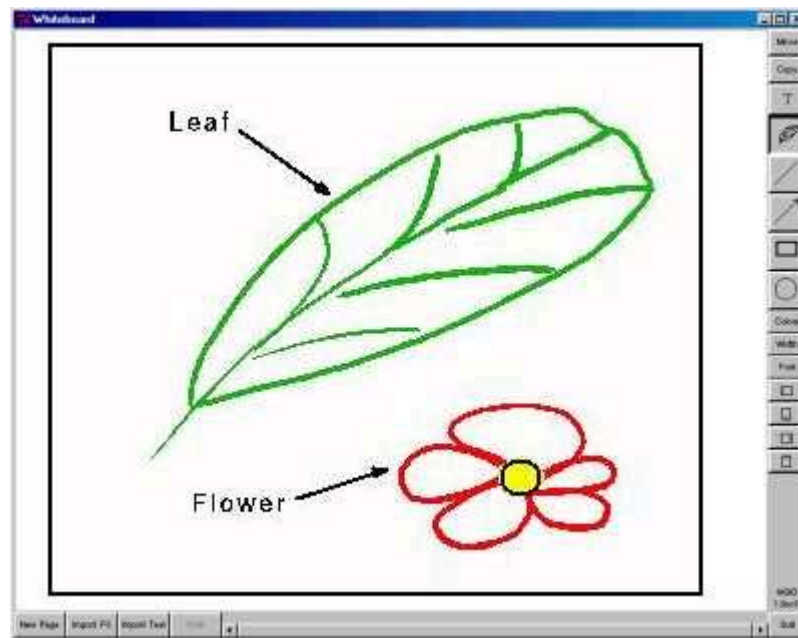


Figura 3. Ventana principal de VIC

### WB – White Board

El white board es una herramienta para la transmisión de datos que permite compartir un tablero electrónico entre los participantes de una sesión. Se pueden crear dibujos sencillos con rectángulos, óvalos, líneas y textos. También permite utilizar diferentes colores para identificar a cada uno de los usuarios e importar archivos postscript y de texto con extensión txt.

La ventana principal del WB se observa en la figura 4.



**Figura 4. Ventana principal de WB**

### **NTE - Network Text Editor**

Esta herramienta permite el intercambio de solo texto entre los participantes de una sesión, identificando a cada uno de ellos con un color y cuenta con más funcionalidades para texto que el whiteboard, como importar texto plano y texto estructurado, guardarlos y editarlos; se pueden utilizar diferentes estilos de fuente.

La ventana principal del NTE se presenta en la figura 5.

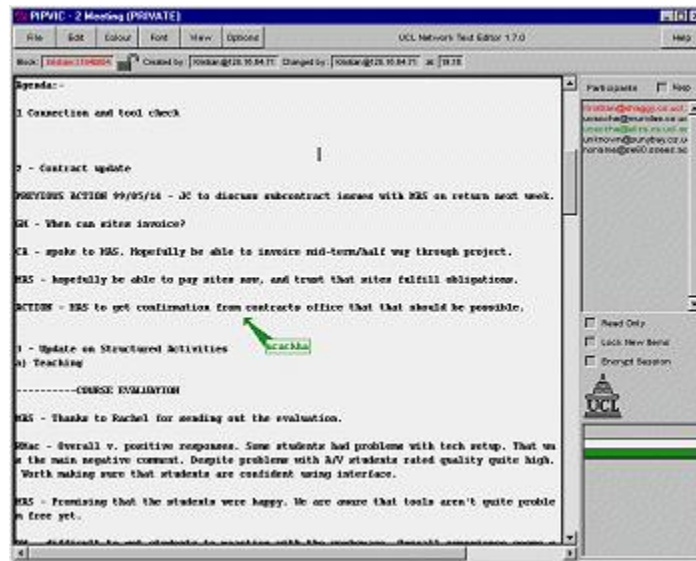


Figura 5. Ventana principal del NTE

Este conjunto de herramientas viene para diferentes arquitecturas y sistemas operativos como Linux, Solaris, Windows, Irix, FreeBSD, SunOS e incluso se pueden bajar las versiones disponibles para multicast IPv6.

## MASH

Mash es un set de herramientas para manejo de flujos multicast desarrollado por la Universidad de Berkeley y consta de utilidades como el NSDR (New session directory tool), el VAT (LBNL Audio Conferencing Tool), el VIC (Video Conference Tool), el MB (media board), Collaborator; existen más herramientas que pueden trabajar con el Mash, pero no fueron probadas.

Mash se puede descargar de la página del grupo de trabajo Open Mash: <http://www.openmash.org/users/tools/index.html> y esta disponible para sistemas operativos como FreeBSD, Linux, Solaris y Windows. Una vista general del Mash utilizando el NSDR, el VIC y el RAT se muestra en la figura 6.

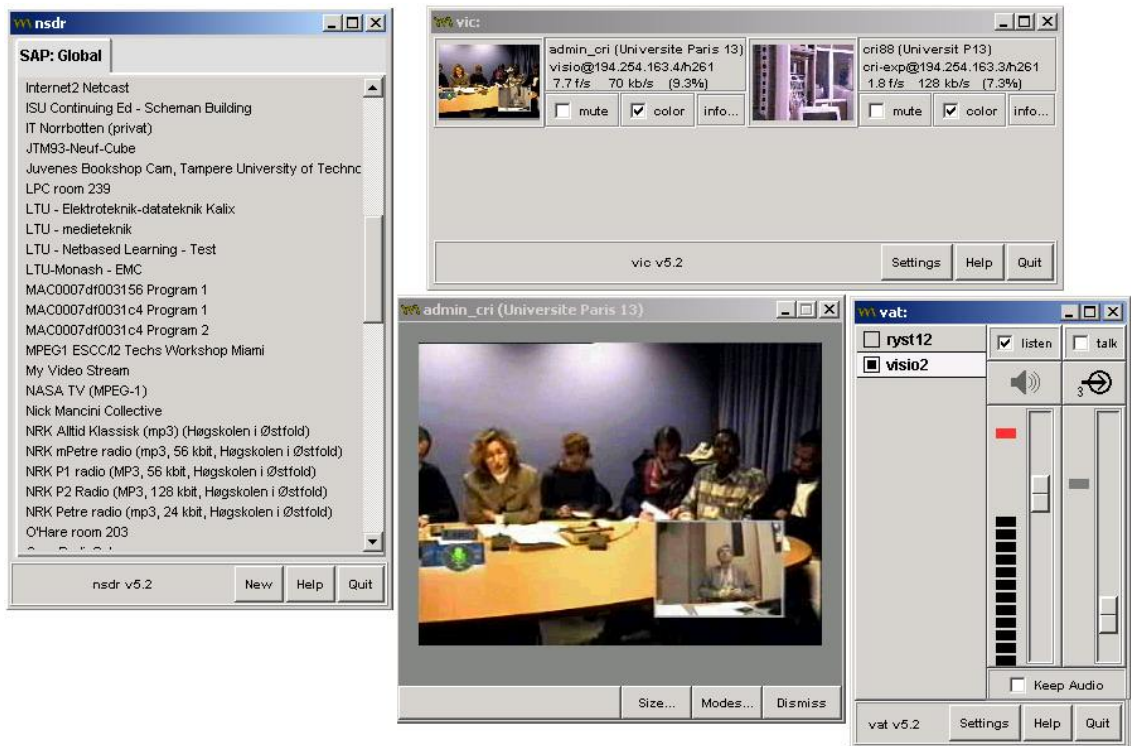


Figura 6. Herramientas del Mash

### Cisco IP/TV

La herramienta IP/TV es desarrollada por la Universidad de Oregon y es un programa que integra las aplicaciones de directorio de sesiones, de video y se audio en una sola interfaz para facilitar su manejo; La aplicación IP/TV está orientada a la comunidad de Internet 2 y esta disponible solamente para el sistema operativo Windows. Esta herramienta se puede descargar de la página [http://videolab.uoregon.edu/iptv\\_license.html](http://videolab.uoregon.edu/iptv_license.html)

La ventana principal se puede observar en la figura 7.

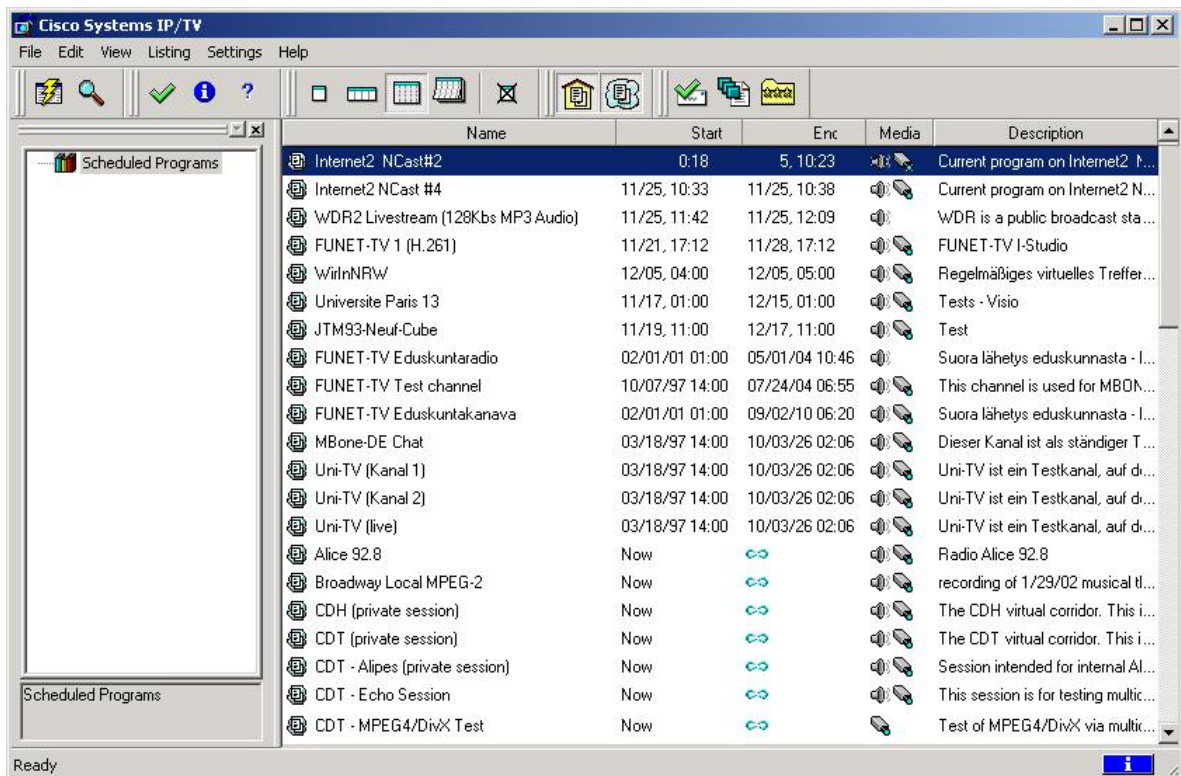


Figura 7. Ventana principal del IP/TV

## PRUEBAS DEL IMPACTO EN EL ANCHO DE BANDA CONSUMIDO POR LAS APLICACIONES MULTICAST

Se llevaron a cabo dos tipos de pruebas para medir el impacto en el ancho de banda consumido por las aplicaciones utilizadas: al interior de la universidad y en el enlace de Orbitel para Internet.

### PRUEBAS DEL DESEMPEÑO DE LOS SWITCHES

#### Prueba 1

En la prueba número uno se trata de observar el impacto del tráfico multicast sobre un switch 3com 3300XM para dar una idea del desempeño de la red de datos de la Universidad frente a este mecanismo de difusión. La LAN de la Universidad es una red conmutada basada en dispositivos de nivel 2, por lo que



es necesario el estudio del comportamiento de un switch frente al tráfico multicast.

Se tiene un switch 3com 3300XM que conecta a través de puertos diferentes a 5 PCs, estos generan tráfico multicast de audio, video y datos al mismo tiempo, todas las máquinas son receptoras y generadoras de información. Se utiliza un PC adicional para recolectar la información de gestión que permite monitorear el ancho de banda utilizada por todo el switch o por un puerto específico. Además se utiliza un hub 3com de 12 puertos que cuelga del switch y es utilizado para medir el impacto alcanzado en un dominio de colisión común.

En la figura 8 se puede ver el ancho de banda consumido por el switch cuando no existe ningún tipo de tráfico, sólo el generado por el equipo monitor.



**Figura 8. Ancho de banda consumido por todo el switch**

Al switch, visto como unidad están entrando 235 bps y sale la misma cantidad, producto del tráfico generado por el equipo monitor.

Ahora se conecta un equipo multicast al puerto 13 del switch; con el programa SDR se crea una sesión y se observa cuál fue el ancho de banda utilizado para esta tarea común.

El tráfico generado por la máquina multicast en el puerto 13 entra al switch y como se puede apreciar en la figura 9 se incrementa el ancho de banda total utilizado a 645 bps.

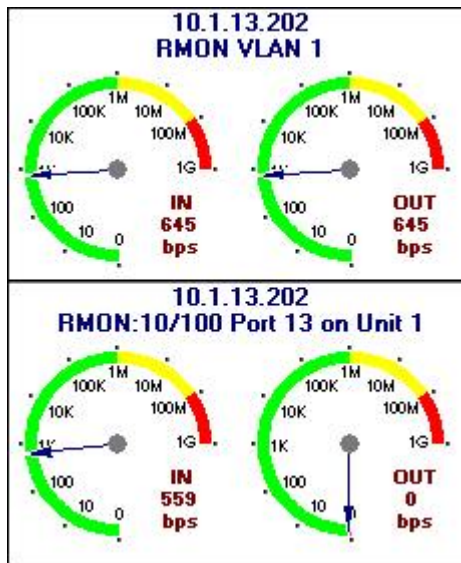


Figura 9. Ancho de banda consumido en la creación de una sesión

Nuevamente se conecta otra máquina al switch, esta vez al puerto 15 y como se muestra en la figura 10, hay un incremento en el tráfico total y en el tráfico del nuevo puerto. Todo esto ocurre cuando el último PC conectado recibe información del anuncio de sesión.

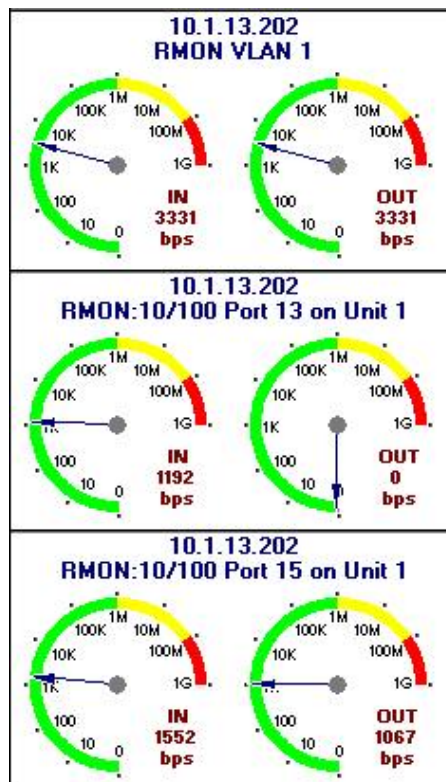
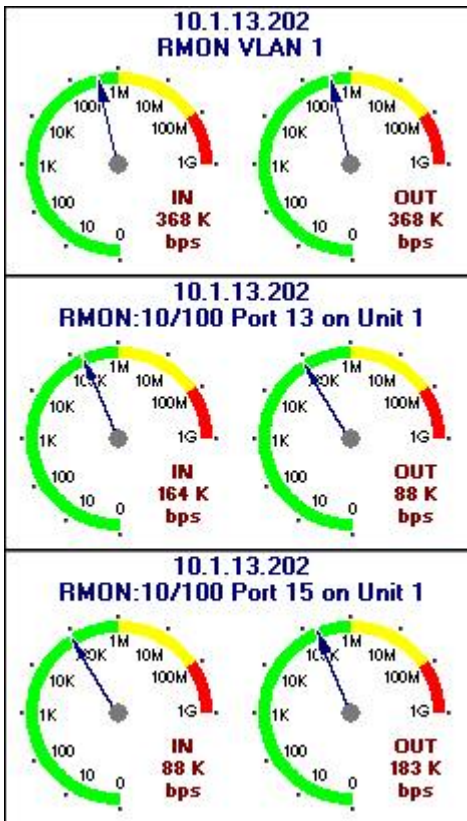


Figura 10. Cambio de ancho de banda al conectar un nuevo PC

En la figura 10 el tráfico del puerto 15 indica que el equipo conectado está recibiendo información acerca de la sesión que esta anunciando el equipo del puerto 13. Hasta ahora los recursos consumidos son mínimos.

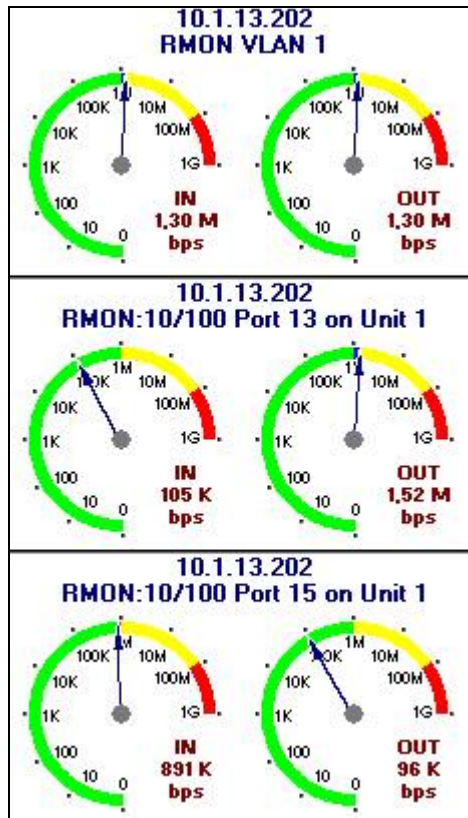
Después de esto, se genera tráfico de audio con el equipo del puerto 13, en la figura 11 se observan los recursos consumidos en los dos puertos.



**Figura 11. Ancho de banda consumido por la aplicación de audio**

Aunque el tráfico es unidireccional, se aprecia que el segundo equipo (puerto 15) también está transmitiendo información que le llega al primer equipo (puerto 13); este comportamiento es debido a la información de control que se genera por la utilización del protocolo RTP.

A continuación se genera audio y video en los dos equipos tratando de consumir la mayor cantidad de ancho de banda posible.



**Figura 12. Ancho de banda consumido por audio y video**

En la figura 12 se observa una concordancia en las magnitudes de los bits de entrada y salida de los puertos 13 y 15.

Ahora se conectan los 5 equipos al switch y se genera audio y video; la figura 13 muestra el comportamiento de entrada y salida en cada uno de los puertos.

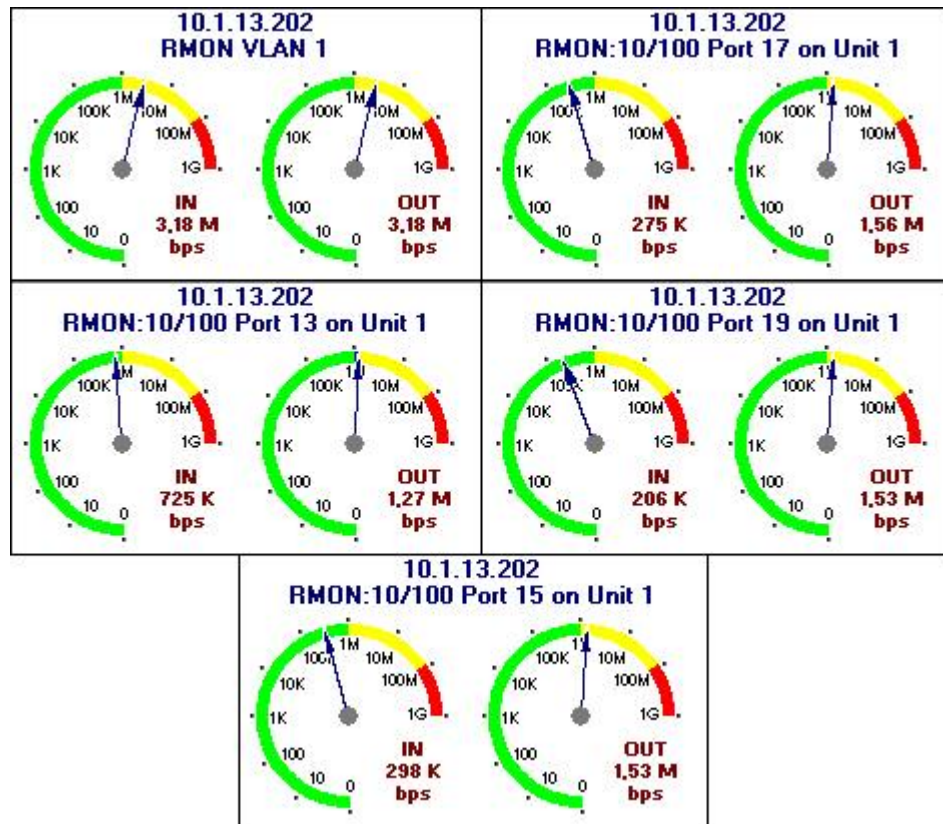


Figura 13. Ancho de banda de entrada y salida de los puertos

En cada puerto llegan entre 200 y 300 Kbps que corresponden a la transmisión de su propia información de audio y video; en cada puerto salen aproximadamente 1.5 Mbps que corresponden al tráfico de todas las demás fuentes de información. La información extra de entrada que se detecta en el puerto 13 se puede justificar por el tráfico extra de control que debe generar la maquina que creo la sesión.

Ahora se conecta el hub al puerto 24 del switch y el PC de control al puerto 1 del hub con la intención de medir el impacto en un puerto del switch en el que no hay una máquina multicast conectada y por lo tanto en todo el hub (el hub es un dominio de colisión común). Esto se puede observar en la figura 14, la gráfica correspondiente a la dirección 10.1.14.3 pertenece al hub y la gráfica de la dirección 10.1.13.202 es la correspondiente al switch.

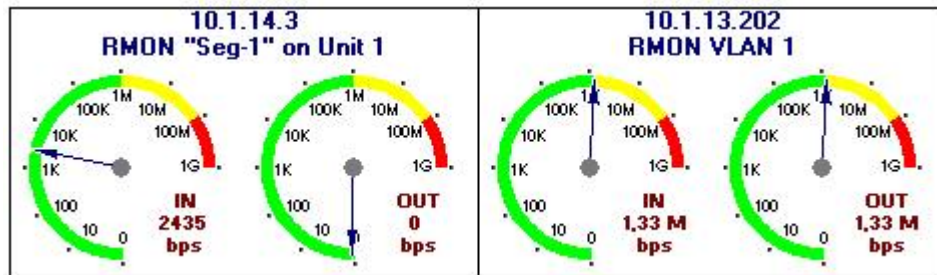


Figura 14. Ancho de banda consumido por el hub y el switch

Mientras que en el switch se está generando un promedio de 1.33 Mbps, en el hub no se nota este flujo de información debido a que el IGMP snooping no permite que este se transmita a otros puertos del switch en donde no se existen miembros multicast.

Si se conectan los 5 equipos al concentrador se observaría el consumo de ancho de banda de la figura 15.

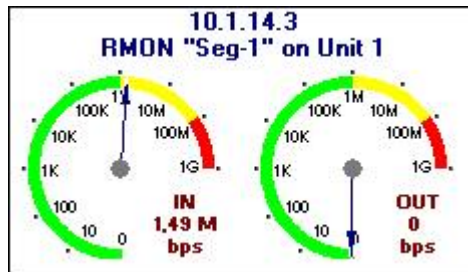
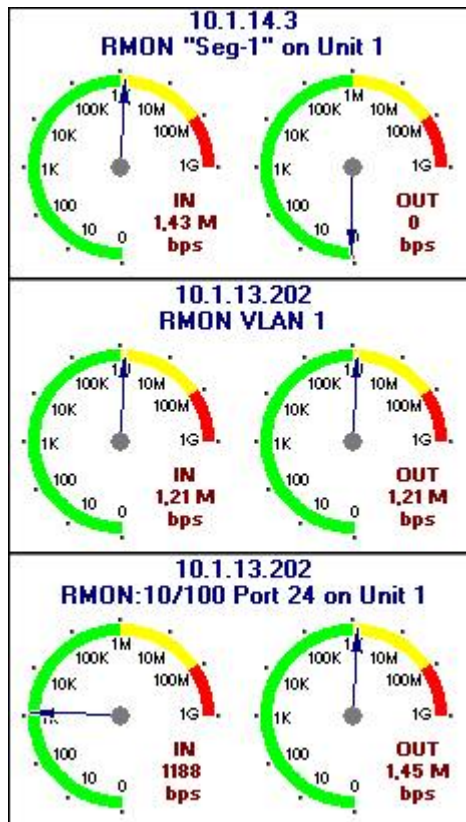


Figura 15. Consumo de ancho de banda del hub con miembros multicast

En la figura 16 se observa la medida que se obtiene en el hub si se deshabilita el IGMP snooping y todos los PCs se conectan al switch.



**Figura 16. Ancho de banda consumido en el hub y en el switch con IGMP Snooping deshabilitado**

Este último comportamiento es el que se quiere evitar ya que por el puerto 24 (donde esta conectado el hub al switch) se está reflejando todo el tráfico multicast que hay en el switch lo que afecta a todo el hub y a los PCs que estuvieran conectados a él.

Comparando las figuras 14 y 16 se puede observar que en el hub (dominio de colisión común) se están ahorrando 1.1 MB de ancho de banda debido al tráfico multicast que están generando los hosts conectados a los puertos 13, 15, 17 y 19.

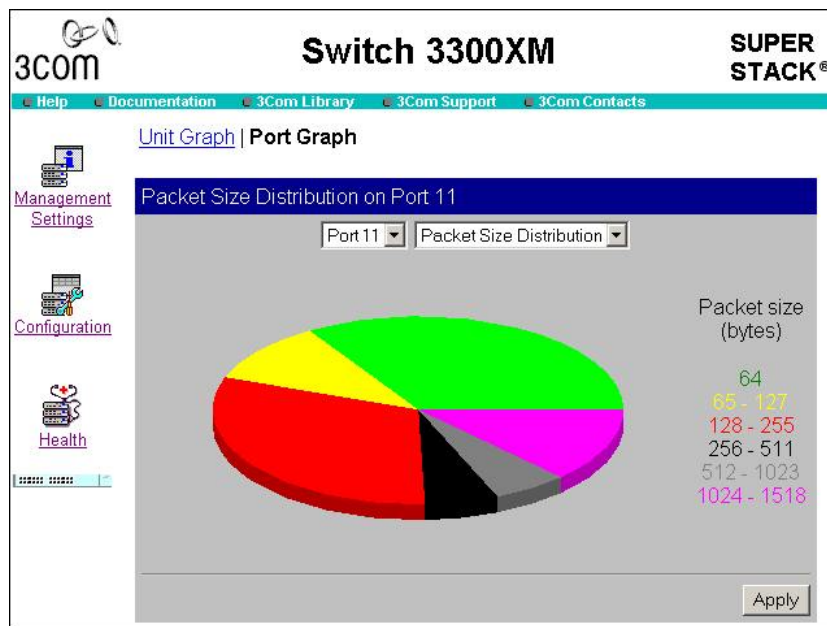
### **Prueba 2**

En esta prueba se trata de medir el desempeño real del switch 3com 3300XM ubicado en CC3 del edificio de Ingenierías.

Se conecta una máquina a un puerto del switch que va a estar unida a una conferencia de audio y video multicast del Mbone. Los paquetes de audio y video

analizados con un sniffer muestran una longitud entre 200 bytes y 1 KB; utilizando el software de gestión del switch se observa la diferencia del tráfico recibido en el puerto donde está conectada la máquina multicast y otro puerto donde no hay miembros activos de este mismo grupo, cuando está habilitado y deshabilitado el mecanismo IGMP Snooping.

En la figura 17 se puede ver una gráfica donde se muestra el porcentaje de paquetes recibidos con diferentes rangos de longitud. Los paquetes multicast hacen parte del porcentaje representado por los colores rojo, gris y negro; en el puerto 11 del switch hay un PC unido a la sesión multicast.



**Figura 17. Puerto "multicast" con IGMP Snooping habilitado**

En la figura 18 se observa la gráfica del puerto 2 en donde los colores rojo, gris y negro se muestran como un porcentaje bajo respecto al que se presenta en el puerto 11, lo que demuestra que no se está enviando tráfico multicast a los puertos donde no haya receptores multicast, esto gracias al funcionamiento de IGMP Snooping.



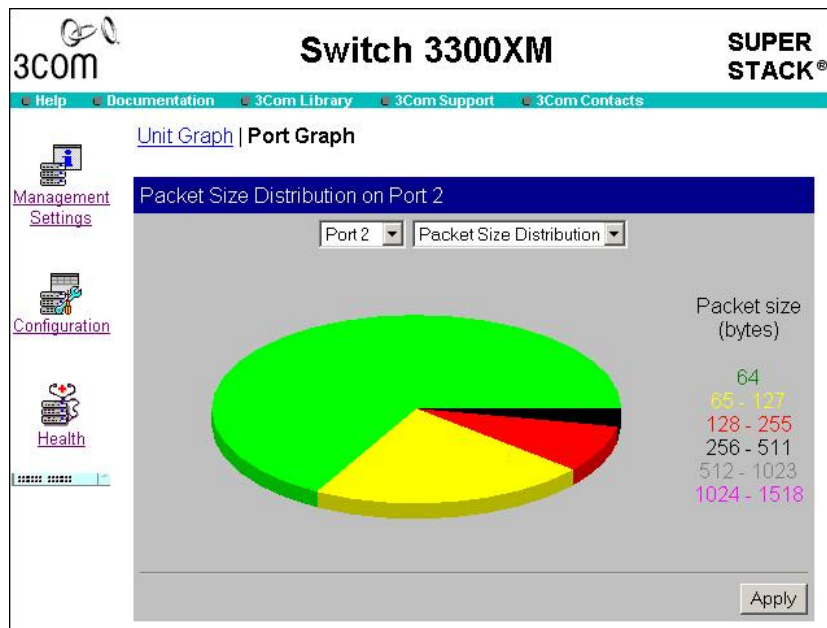


Figura 18. Puerto "no multicast" con IGMP Snooping habilitado

En el siguiente paso se deshabilita IGMP Snooping y se observa el impacto en los mismos puertos. En la figura 19 el puerto 11 no muestra ninguna variación significativa respecto a la figura 17; mientras que en la figura 20 se muestra el puerto 2 que ahora sigue el mismo patrón de comportamiento del puerto 11 en el porcentaje de paquetes del rango multicast.

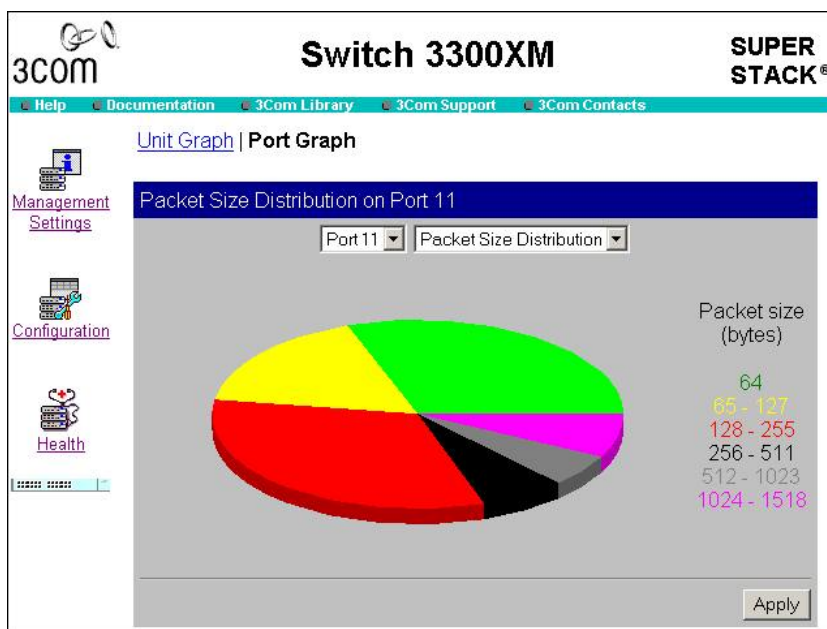
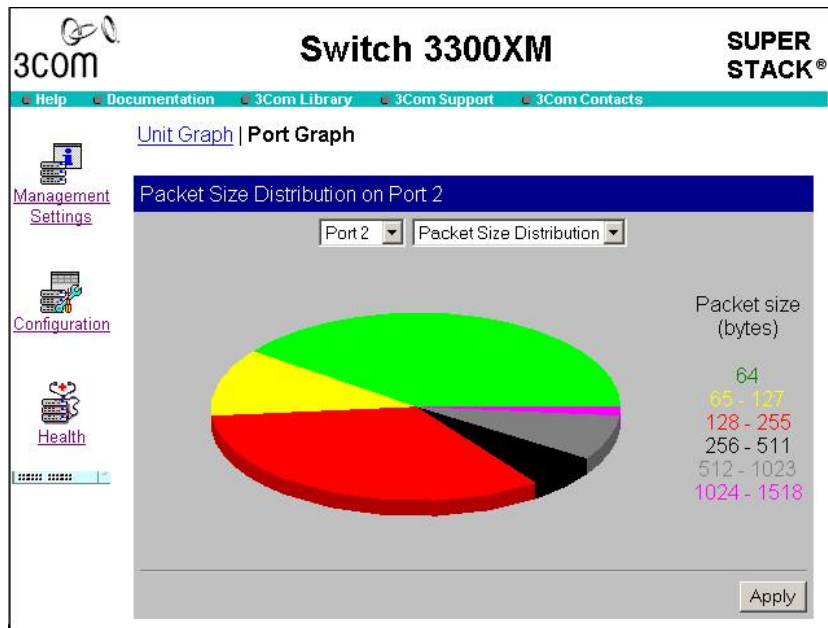


Figura 19. Puerto "multicast" con IGMP Snooping deshabilitado

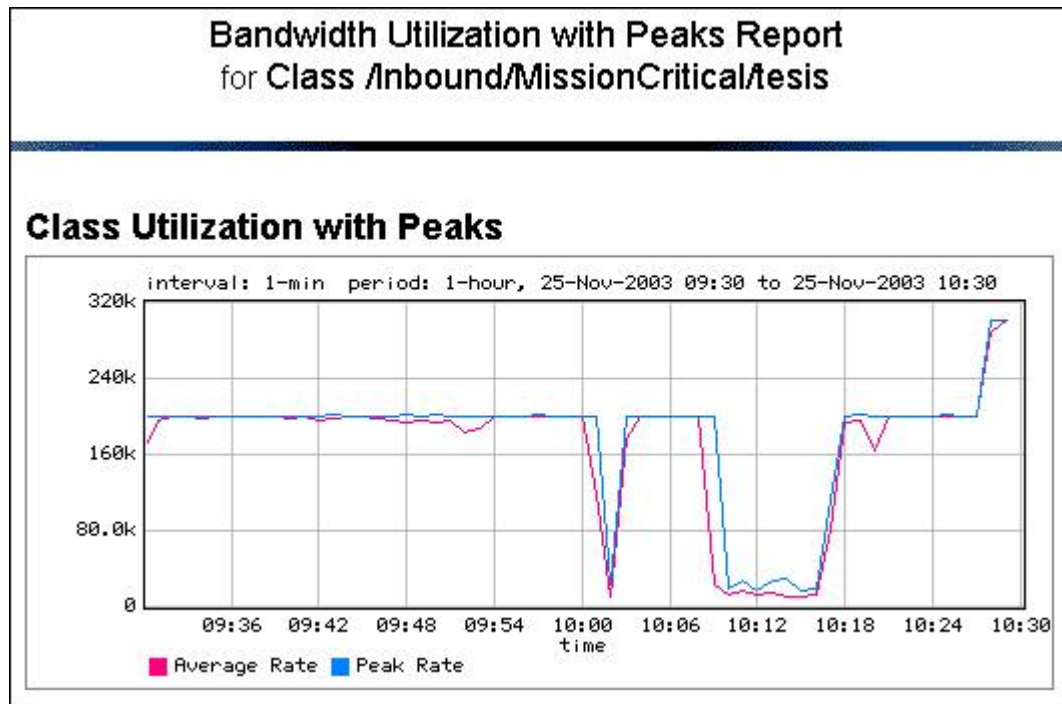


**Figura 20. Puerto "no multicast" con IGMP Snooping deshabilitado**

Con las pruebas 1 y 2 se puede concluir que el mecanismo de IGMP Snooping evita que el tráfico multicast en los dispositivos de nivel 2 actúe como tráfico broadcast, mediante un análisis de la información de los mensajes IGMP que intercambian los enrutadores multicast y los hosts. De esta manera, se evita inundar las redes conmutadas con tráfico multicast indeseado en algunos sectores de la red.

## **PRUEBAS EN EL ENLACE ORBITEL A INTERNET**

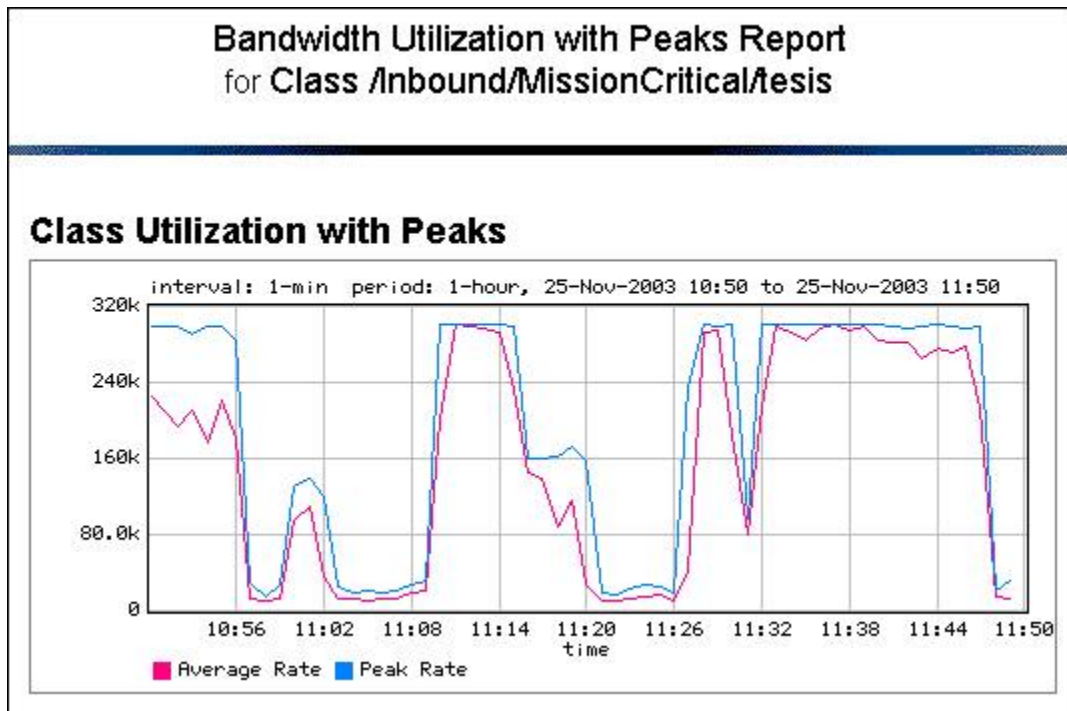
Para el proyecto se ha reservado un ancho de banda de máximo 200 Kbps a través del enlace de Orbitel y gracias al software de gestión del Packetshaper se puede monitorear los recursos consumidos en el túnel creado entre la Universidad del Cauca y la red RETINA. En la figura 21 se muestra la gráfica que indica el ancho de banda consumido al unirse a una sesión de audio y video.



**Figura 21. Ancho de banda consumido entre las 9:30 a.m y las 10:30 a.m**

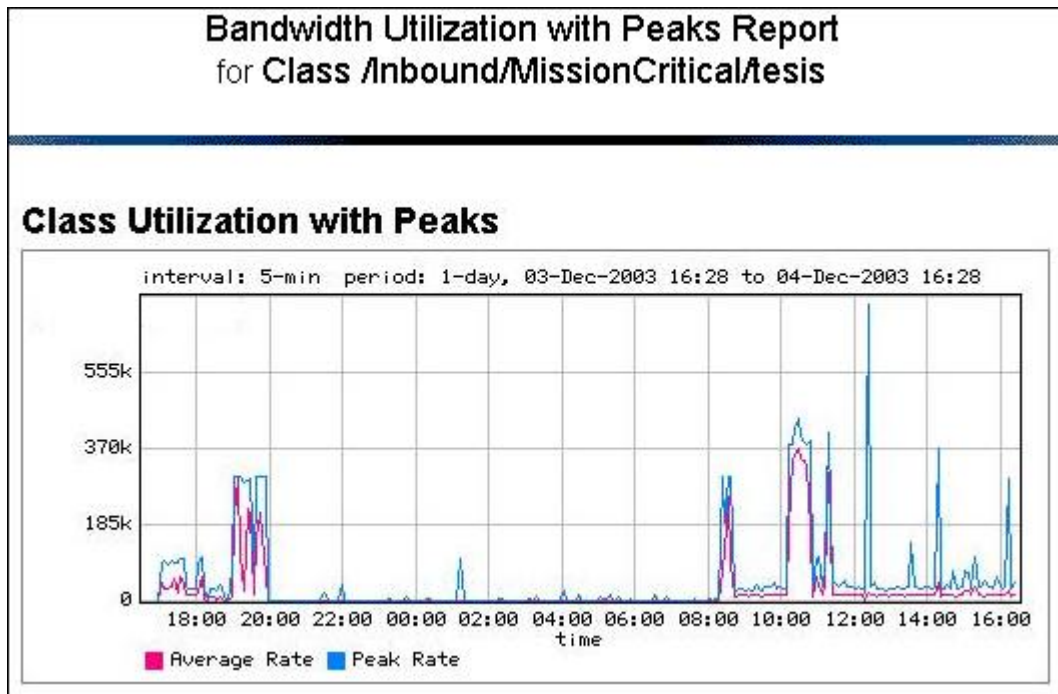
La línea azul muestra el tráfico real utilizado por el enlace, entre las 9:30 y 10:00 de la mañana se utilizaron completamente los 200KB reservados, en este tiempo siempre se mantuvo la unión a la sesión multimedia generada por la Universidad de París. Alrededor de las 10 a.m. se abandonó la sesión por unos minutos y posteriormente se reanudó la recepción del tráfico multicast de la sesión, lo que generó una disminución considerable en el consumo de ancho de banda. Entre las 10:10 a.m. y las 10:15 a.m. aproximadamente se abandonó nuevamente la sesión multimedia; a las 10:18 a.m. se retomó la sesión. El aumento en el consumo de ancho de banda que se ve al final de la gráfica está relacionado con el incremento de ancho de banda reservado para el proyecto, ahora a 300 Kbps, por un período corto de tiempo. Debido a este aumento de ancho de banda disponible la calidad de recepción del audio y video mejoró notablemente.

En la figura 22 se aprecia en mayor detalle la utilización de los 300 Kbps asignados; los cambios en el ancho de banda consumido se deben a la recepción de sólo audio, sólo video, ambos o ninguno de los flujos multimedia.



**Figura 22. Ancho de banda consumido entre las 10:50 a.m y 11:50 a.m**

Finalmente, se hace una prueba aumentando el ancho de banda disponible a 500 Kbps y se observa el comportamiento del túnel Unicauca-Retina en la figura 23.



**Figura 23. Ancho de banda consumido con 500 Kbps de disponibilidad**

Como se aprecia en la figura anterior el máximo ancho de banda consumido es de 400 Kbps aproximadamente en aplicación de voz y video con una calidad de recepción bastante buena.

En las figuras 21 y 22 se observaba que los techos de las gráficas eran constantes lo que insinuaba que el ancho de banda asignado no era suficiente, en contraste con la figura 23, donde se da a entender que este es el ancho de banda máximo (400 Kbps) aproximado que se puede consumir con este tipo de aplicación. Aunque el ancho de banda depende del tipo de codificación utilizado en el flujo de voz y video, de la calidad con la que se transmite y de otros factores que pueden ser configurados en las herramientas VIC y RAT. Por lo tanto se concluye que un ancho de banda de 500 Kbps para este tipo de enlaces es suficiente para obtener una buena calidad en el servicio.