Universidad Nacional Autónoma de México

Facultad de Ingeniería

"Implementación de un enlace WAN con capacidad para transmitir voz, video y datos sobre el protocolo IP, mediante el uso de la tecnología WiMAX"

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN TELECOMUNICACIONES

P R E S E N T A N:

OLIVA ANDON ULISES MAURICIO

SANTILLÁN GUERRERO JOSÉ ANTONIO

ASESOR:
Dr. VÍCTOR RANGEL LICEA

Agradecimientos

A nuestras familias por el apoyo incondicional que siempre nos dieron. Externamos el más sincero y eterno agradecimiento por ese apoyo que perpetuamente nos han brindado y gracias al cual hemos logrado terminar nuestra carrera profesional, que es para nosotros la mejor de las herencias.

A nuestros maestros que día a día forjaron en nosotros las habilidades y actitudes que nos permitieron desarrollar nuestra tesis.

Con un infinitito agradecimiento a nuestra querida UNAM por permitirnos vivir una de nuestras mejores etapas de nuestra vida; con especial agradecimiento a nuestra Facultad de Ingeniería la cual nos ha dado las herramientas que nos servirán tanto en el ámbito profesional como académico.

Reconocimientos

Gracias a la DGAPA-UNAM por el apoyo otorgado para la realización de este trabajo a través del proyecto PAPIIT IN108910 “Diseño de algoritmos de reservación de capa cruzada en redes móviles y mesh de banda ancha”.

Gracias al CONACYT por el apoyo brindado a través del proyecto 105279 “Diseño de técnicas de reservación de capacidad de redes BWA móviles”

ÍNDICE

ÍNDICE DE FIGURAS:

ÍNDICE DE TABLAS:

CAPÍTULO I

Antecedentes

En la actualidad una gran cantidad de empresas utilizan redes de computadoras para la administración de sus recursos y/o actividades, dichas redes deben abarcar áreas geográficas de dimensiones considerables. La arquitectura con la que se implementa dicha red puede entenderse, como se explica en [1], como una especie de islas denominadas LAN[1] (Local Area Network) conectadas a través de puentes, estos se clasifican según la distancia del enlace en redes MAN ó redes WAN.

Existen diversas tecnologías capaces de proveer dicho servicio; Sin embargo todas cuentan con limitaciones. En este capítulo se exponen las características que brindan ventaja a la tecnología basada en el estándar 802.16 (WiMAX) sobre las otras tecnologías así como el contexto.

[1]En la sección de Glosario se encuentra la definición de los acrónimos utilizados

1.1 Introducción

Retomando lo mencionado en [1], los usuarios domésticos usamos la red que soporta el INTERNET como enlace MAN/WAN debido a su bajo costo, por lo mismo esta se encuentra constantemente ocupada por las transmisiones de muchos usuarios lo que dificulta la transmisión de determinados tipos de información como son la voz (telefonía) y la información multimedia (videos), además la información corre el riesgo de ser interceptada por terceros. Para fines de una empresa lo anterior no es aceptable, cómo alternativa se implementa un enlace MAN/WAN privado, que ofrece un canal de comunicación exclusivo para los usuarios pertenecientes a la misma.

Existen diferentes tecnologías para implementar los enlaces MAN/WAN; Sin embargo estas opciones requieren de medios guiados para su implementación (par trenzado, cable coaxial, fibra óptica) lo cual es un problema en caso de no existir infraestructura que cubra dicha área geográfica ya que se debe esperar hasta que sea creada, y el costo es elevado.

Las tecnologías de redes inalámbricas de banda ancha, denominadas BWA, como indica su nombre se implementan "sin cables". De las tecnologías BWA existentes, WiMAX representa una buena opción para la implementación del enlace WAN debido a que ofrece completa compatibilidad con el protocolo TCP/IP y puede basar la calidad de servicio en el encabezado del paquete IP.

Más aún, cómo se menciona en [4] WiMAX fue diseñado para ser empleado como competidor de las tecnologías que emplean cables, enfocado en los servicios de telefonía y acceso a INTERNET. Actualmente uno de los mayores potenciales de WIMAX (versión fija) es el poder ofrecer interconexiones a velocidades de transmisión comparables con las conexiones T1/E1.

1.2 Breve historia del desarrollo de las redes de computadoras.

Referente a la importancia de que el estándar 802.16 se base en el protocolo TCP/IP consideramos necesario enumerar los hechos mas relevantes en el desarrollo de redes TCP/IP, basándonos en [3] estos fueron: el desarrollo de la tecnología ARPAnet por parte del Departamento Americano de Defensa en 1969, cuyo objetivo fue conseguir el intercambio de información entre sedes remotas sin importar que parte de la red estuviera destruida. La característica que permitió lograr tal resultado fue segmentar la información en paquetes, añadiendo a cada paquete un encabezado con información de su origen, destino, corrección de errores, etc. De esta manera el paquete no viajaba por una ruta prestablecida a través de la red, en vez de ello cada nodo se encargaba de encaminar el

flujo de paquetes basado en la cabecera de cada paquete, de esta manera si parte de la red era destruida el flujo de paquetes era encaminado hacia una ruta alternativa.

En un inicio ARPAnet fue de uso exclusivo militar y académico, más adelante ARPAnet fue dividido en una versión de uso público y se mantuvo una versión exclusiva para el ejército.

A su vez los desarrollos tecnológicos permitieron a particulares implementar sus propias redes, para garantizar la interconectividad entre equipos creados por diferentes fabricantes en 1974 fue presentado el protocolo TCP/IP (basado en el modelo del mismo nombre). TCP/IP fue adoptado por ARPAnet hacia los ochenta. De la interconexión de pequeñas redes de dominio particular y la versión pública de ARPAnet, ambos operando bajo TCP/IP, surgió INTERNET.

El modelo TCP/IP además de normalizar los equipos brinda la capacidad de ser operable a través de distintos medios de transmisión, actualmente aquellos más empleados son: en primer lugar la tecnología híbrida de fibra óptica y cable coaxial utilizada por las compañías de TV por cable que aprovechan su infraestructura ya desplegada. En segundo lugar, se encuentra la tecnología más común en nuestros días: ADSL, cuyo funcionamiento se basa en la transmisión de señales de información a través del cableado telefónico a frecuencias más altas que las de la voz, utilizando un filtro en el extremo del usuario. Se cuenta también con el acceso por fibra óptica. En general la desventaja de estas tecnologías radica en los costos de instalación cuando no existe infraestructura desplegada. Referente a los sistemas inalámbricos pueden emplearse redes satelitales orientadas al acceso a Internet, cuya desventaja es la distancia que debe recorrer la señal, la cual afecta directamente en el retardo dificultando e incluso impidiendo el despliegue de servicios, por ejemplo VoIP. Y por último, la quinta tecnología: una red BWA, que es fija, baja en costo y extremadamente conveniente en aquellos lugares donde el despliegue de líneas telefónicas o fibra óptica no es rentable o no está planeado aún. Por ejemplo, en lugares montañosos o de difícil acceso técnico.

1.3 Definición del problema

El estándar IEEE 802.16-2004 describe la tecnología WiMAX para enlaces entre terminales fijos, a su vez indica que dichos equipos deben ser capaces de ofrecer calidad de servicio sobre las transmisiones. Por ello se pueden transmitir voz, video y datos sobre dichos enlaces. Otra característica de WiMAX es que es una tecnología de bajo costo, por ello podría utilizarse como una alternativa al enlace MAN en caso de no disponer de infraestructura, además que dicho enlace sería convergente.

Por lo anterior es necesario contar con estudios experimentales para analizar el desempeño de los diversos servicios (voz, video y datos) en enlaces realizados por medio de equipos certificados en esta tecnología. Dichos estudios tienen el fin de demostrar que el enlace es capaz de ofrecer calidad de servicio de extremo a extremo a través de múltiples equipos de red.

La red empleada en esta tesis consiste en dos redes LAN que emplean los componentes básico de una red TCP/IP, es decir un *"router" y* un *"switch"*, el equipo de computo ya sea en función de servidor o de cliente, y el enlace MAN mediante la estación base y la estación suscriptora WiMAX.

Las mediciones se efectúan directamente a partir de funciones en el *"IOS"* del equipo de red y con "*software"* especializado en los extremos del enlace. Estas se realizan bajo determinadas condiciones, por ejemplo con el enlace operando al mínimo de su capacidad, o al máximo, activando o desactivando las políticas de calidad de cierto equipo.

1.4 Objetivos

Éste trabajo tiene como objetivo analizar el desempeño de los servicios ofrecidos en los extremos del enlace MAN, dicho enlace tendrá la capacidad de transmitir voz, video y datos sobre el protocolo IP. También se verifica la interoperabilidad, específicamente con equipos de red de la marca CISCO.

Al final los resultados servirán para comparar cómo la calidad de servicio (QoS) tanto del equipo WiMAX, cómo del equipo de red LAN afectan el desempeño de los servicios (voz, video y datos).

1.5 Método

Se realizarán pruebas con la intención de observar el comportamiento y las prestaciones de una red WiMAX, así como las diferentes calidades de servicio (QoS) implementadas para la transmisión multimedia a través de la red.

Para el estudio instrumental, se utilizarán 1 BS WiMAX, 1 usuario subscriptor, 2 *"routers"* CISCO, 2 *"switches"* y 1 laboratorio de VoIP.

1.5 Estructura de la tesis

El capítulo 1 describe cómo fue el desarrollo de las redes de datos con el fin de recalcar la importancia de la interoperabilidad entre equipos de diferentes fabricantes. También se enumeran las tecnologías actuales que ofrecen el acceso de banda ancha y las desventajas

que presentan al emplear medios de transmisión guiados, se menciona el uso de redes BWA y sus ventajas para cubrir zonas de difícil acceso. Finalmente se exponen las características de la tecnología WiMAX que la convierten en una buena opción como red BWA convergente.

El capítulo 2 se compone de una descripción de los protocolos usados por el equipo de red y por las aplicaciones. Se comienza por explicar el modelo de referencia OSI y el modelo de red TCP/IP. Se describe la evolución del estándar WiMAX, y las especificaciones de la subcapa MAC y la capa física del estándar IEEE 802.16-2004 (WiMAX fijo). Se describen las funciones del protocolo 802.1Q VLAN para ayudar a la implementación del QoS en los extremos de la red. Y por último se enumeran las características de los protocolos usados para el procesamiento de la señal de voz y video G.XX, MPEG-XX.

El capítulo 3 comienza por la descripción de los componentes físicos de la BS WiMAX, su *software* y la administración de la misma. Se continúa por describir las unidades suscriptoras (SS) tanto de interior cómo de exterior, se mencionan características tanto de "*hardware"* cómo de *software* y su administración. Se prosigue por describir los componentes básicos y el mecanismo de operación de los equipos de red (*switch* y *router*). Finalmente se describen las aplicaciones usadas para implementar cada servicio (voz, video, datos).

El capítulo 4 es una descripción de la configuración que implementamos en el cuál presentamos las configuraciones hechas en los equipos de red, cómo las realizadas en las aplicaciones, y el direccionamiento.

El capítulo 5 presenta los resultados y el análisis de los resultados obtenidos de la calidad de las transmisiones recibidas en función de los parámetros de QoS implementados en el la red y de la saturación del sistema.

El capítulo 6 son las conclusiones de las observaciones realizadas en el capítulo 5.

CAPÍTULO II

Estándares y protocolos empleados

Todo sistema de comunicaciones se compone de emisor, receptor, mensaje, canal, y reglas. La función de las reglas es coordinar a los demás componentes para que los mensajes puedan ser enviados y descifrados correctamente. En la práctica dichas reglas reciben el nombre de protocolos y son elaborados por organismos internacionales con el fin de establecer un marco común para que los equipos de distintos fabricantes sean interoperables.

En este capítulo se describen los protocolos empleados por los servicios de voz, video y datos, así como por el radioenlace WiMAX y los equipos de red CISCO.

2.1 Modelos OSI y TCP/IP

Con el fin de facilitar la interoperabilidad entre diferentes protocolos se tienen modelos de referencia sobre los cuáles se desarrollan los protocolos.

En redes de computadoras, los modelos más empleados son: el modelo de referencia OSI y el modelo TCP/IP. En general, como se explica en [2], ambos modelos separan el sistema en capas, donde cada capa es una abstracción de una funcionalidad en particular. Las diferencias entre dichos modelos son, primero, que el modelo OSI fue creado para normalizar los equipos y garantizar la interoperabilidad entre cualquier sistema, mientras que el modelo TCP/IP se publicó para informar cómo debían operar los equipos para conectarse específicamente a INTERNET. Otra diferencia es el número de capas y sus funciones, estás de detallan a continuación.

Capas del modelo OSI:

1. Aplicación, representa la interfaz o "puerta" entre la computadora y la red. Por ejemplo el protocolo HTTP que se encarga de transportar la información entre el explorador "*Web"* y el servidor remoto.
2. Presentación, cómo lo indica su nombre coordina la presentación del tráfico. Por ejemplo, existen diferentes códigos para representar los caracteres (letras), si estos son distintos en los extremos de la comunicación esta capa ajusta el código para que sea útil al receptor.
3. Sesión, dicha capa brinda a un sistema de comunicaciones la capacidad de establecer "sesiones" entre los extremos, define los mecanismos de: control de diálogo, administración de "*token"*, y sincronización. Un ejemplo es la edición remota de un archivo almacenado en un servidor por parte de múltiples personas simultáneamente.
4. Transporte, su principal función es separar el flujo de datos en paquetes, cuando es requerido establece una conexión entre los extremos remotos y administra los mecanismos para compensar errores.
5. Red, esta capa define la administración de los paquetes en equipos intermediarios entre las redes destino. Define el formato de los paquetes, y como debe el equipo procesarlos en función a determinados valores.
6. Enlace de datos, indica cómo transformar los paquetes a una señal adecuada para transmitirse sobre el medio de transmisión. Dicha capa brinda conectividad entre

equipos directamente conectados, y puede brindar mecanismos de corrección de errores.

7. Física, finalmente la capa física se encarga de definir los valores de las variables físicas del canal de transmisión, por ejemplo una diferencia de potencial (voltaje), frecuencia, etc.

Capas del modelo TCP/IP:

- Aplicación, sus funciones engloban las de la capa de aplicación, sesión y transporte del modelo OSI.
- Transporte, en este caso especificada cómo TCP (UDP), define un formato exacto para segmentar el flujo de datos y se basa en el uso de "puertos" para mantener control sobre los segmentos creados.
- Internet, su protocolo se define cómo IP, por un lado define las características de los paquetes en esta capa y por otro los mecanismos para su administración, por ejemplo los protocolos de enrutamiento (ej: OSPF).
- Acceso a la red, este engloba las funciones de la capa de enlace de datos y la capa física del modelo OSI, también brinda la capacidad para adecuar el paquete IP para su transmisión sobre cualquier tipo de medio.

La siguiente figura muestra la comparación entre el modelo OSI y el modelo TCP/IP.

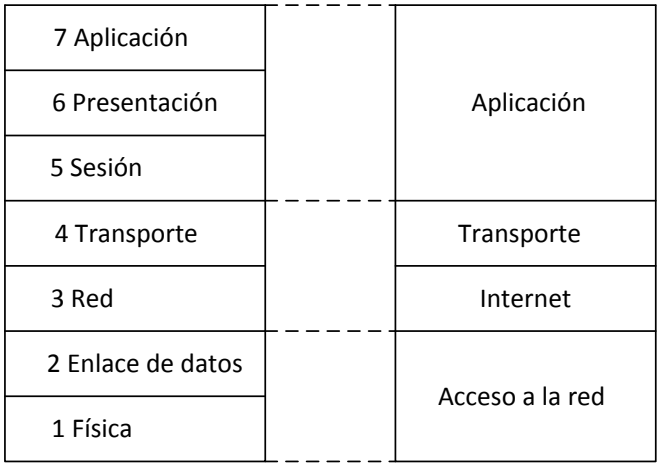


Figura1 Comparación del modelo OSI y el modelo TCP/IP [3]

La interacción entre las capas se basa en "empaquetar" la información conforme se asciende o desciende en las capas. Finalmente es conveniente mencionar los nombres que reciben las unidades de información propias de cada capa, estas son:

Datos para la capa de aplicación, presentación y sesión, segmento para la capa de transporte, paquete para la capa de red, trama para la cada de enlace da datos y bits para la capa física.

2.2 Protocolos TCP (RFC 793) y UDP (RFC 768)

De [18], TCP y UDP son protocolos de la capa de transporte del modelo TCP/IP. La diferencia entre ambos es la cantidad de servicios que ofrecen, la carga que representan para el enlace, el procesamiento y la cantidad de campos en el segmento. A continuación se muestran los segmentos TCP y UDP.

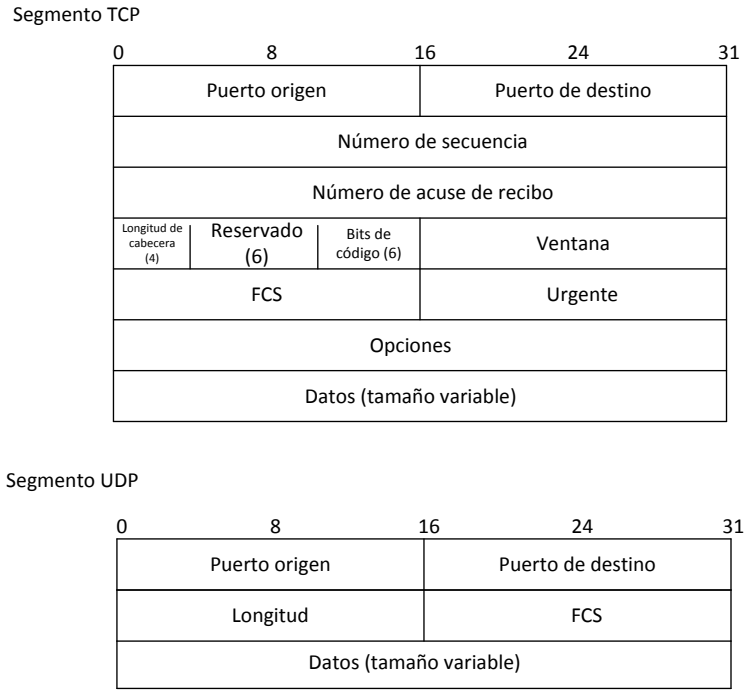


Figura 2 PDUs de TCP y UDP

Como explica [18], comparten un servicio denominado multiplexión (de aplicaciones), para ello se apoyan en los campos "puerto" que asocian el segmento a una aplicación determinada pudiendo transmitir información de más de una aplicación con la seguridad de que el receptor es capaz de extraer dicha información y colocarla en la aplicación correspondiente.

Los servicios adicionales que ofrece TCP se basan en campos de su segmento estos son: número de secuencia, número de acuse de recibo, ventana y bits de código.

El primer servicio es el establecimiento de conexión y terminación, mediante valores determinados del campo bits de código (SYN, ACK, FIN) se instruye a los equipos terminales a iniciar una conexión o finalizarla.

Para el establecimiento se envía el valor de SYN haciendo que el otro equipo sincronice el valor de número de acuse de recibo, el otro extremo responde con SYN y ACK indicando que ha sincronizado su campo número de acuse de recibo y ahora es el turno del equipo local, finalmente el equipo local responde con un ACK indicando que también ha sincronizado su número de acuse de recibo.

Para la finalización un nodo envía el valor FIN, espera a que el otro responda también con FIN y quien inició la terminación envía un ACK final para confirmar la terminación de la conexión.

El servicio de ordenamiento de datos y control de errores, con los campos de número de acuse de recibo y número de secuencia sincronizados TCP ofrece un monitoreo sobre los segmentos siendo capaz de detectar si estos llegan en desorden o si se han perdido. En base a los mismos números puede reordenar los segmentos y/o solicitar la retransmisión de un segmento en particular.

Control de flujo: este campo indica al transmisor cuantos bytes debe enviar en función de la disponibilidad del canal, para ello comienza en un valor pequeño, si no se detectan errores solicita más bytes para la siguiente transmisión. También funciona en sentido inverso, es decir si detecta errores hace decrecer la ventana.

2.2 Protocolo IP (RFC 791)

De [17], el protocolo IP define un formato de paquete en el cual encapsular los segmentos creados en la capa de transporte (en seguida se muestra el formato del paquete IP y se explica cada uno de sus campos). El objetivo de este protocolo es transportar información a redes remotas, para ello se emplea de común acuerdo un esquema de direccionamiento en el que salvo alguna excepciones cada dirección es única e irrepetible. Dicho direccionamiento es repartido por la ICANN (el organismo internacional dedicado a ello) a los RIR (organismos regionales) que finalmente reparten el direccionamiento entre los ISPs. Se reservan rangos de direccionamiento denominados privados para redes no conectadas a INTERNET.

También es importante destacar que IP es un protocolo de mejor esfuerzo no orientado a conexión, es decir que su objetivo es únicamente entregar paquetes, no se encarga de

detectar paquetes faltantes, tampoco de entregar los paquetes en orden ni corregir errores.

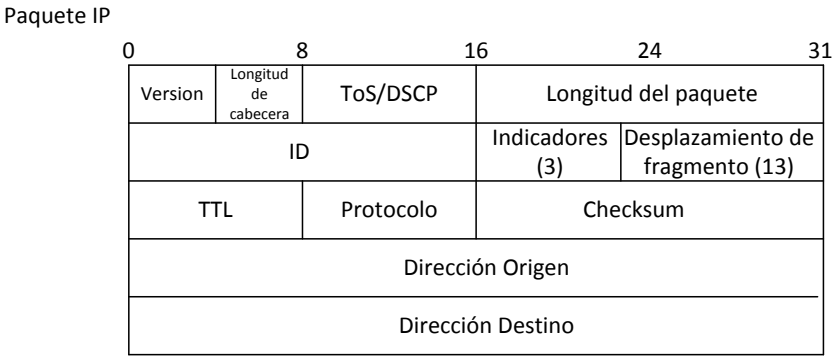


Figura 3 PDU de IP

De [18], el campo de direcciones esta formado por 32 bits. Como se mencionó antes existe una convención para emplear estos valores y es el siguiente:

La notación comprende subdividir en 4 campos de 1 byte, en sistema decimal el rango de cada subcampo toma valores de 0 a 255.

Para crear grupos de direcciones se emplea una herramienta denominada máscara de subred, esta se compone de un conjunto de 32 bits con el valor de unos binarios indicando que bits deben coincidir en las direcciones que conforman el grupo, y ceros para los bits que difieren.

Para tomar la decisión de como enviar los paquetes la computadora analiza las direcciones IP de origen y destino ayudándose de la máscara de subred (operación AND elemento a elemento), si ambas direcciones se encuentran en el mismo grupo entonces los equipos están directamente conectados y se procede a enviar el paquete basado en la dirección de capa dos, si esta se desconoce se emplea ARP (protocolo explicado más adelante en este capítulo). Cuando las direcciones pertenecen a subredes diferentes el paquete se envía a un equipo directamente conectado denominado "puerta de enlace", este tiene la capacidad de manejar el tráfico basado en la dirección IP, conoce redes remotas y reenvía el paquete hacia ellas.

Respecto a las excepciones en el direccionamiento mencionadas anteriormente se tienen grupos de redes que pueden emplearse indiscriminadamente exclusivamente si no tienen conexión hacia INTERNET, por ello empleamos un subgrupo de estas en la implementación.

Las direcciones de redes privadas son: 10.0.0.0 /255.0.0.0, 172.16.0.0 / 255.240.0.0 y 192.168.0.0 / 255.255.0.0.

2.3 IEEE 802.3i ó "*Ethernet*"

Ambas son tecnologías que definen un esquema de comunicación a nivel de capa de enlace de datos y física, difieren sólo en dos campos de sus tramas. Debido a esto se usa indiscriminadamente el término *Ethernet* y el protocolo IEEE 802.3i, incluso estas tecnologías son compatibles entre sí.

Cómo se explica en [2], el acceso al medio se basa en dos técnicas, el CSMA/CD y el "binary exponential backoff", el primero se encarga de censar el medio para detectar la presencia de una transmisión o colisión en base al nivel de tensión (0.85[V] para una transmisión, más de 0.85[V] para una colisión). El segundo mecanismo es posterior la colisión, entonces se asigna de manera local un tiempo de espera antes de reintentar transmitir, teniendo un número de intentos consecutivos máximo de 16. Además la señal se codifica (código Mánchester) para robustecer la señal ante el ruido y facilitar la sincronización en los extremos.

Dichas tecnologías subdividen la capa de enlace de datos en: subcapa MAC y subcapa de enlace de datos.

La subcapa MAC es la más próxima a la capa física, es directamente la responsable de adecuar el paquete IP al medio. Para ello se emplea un formato especial de trama, que es el siguiente:

Trama Ethernet original

Preámbulo	Destino	Origen	Tipo	Datos y relleno	FCS
8	6	6	2	46-1500	4

Trama del 802.3i

Preámbulo + SFD	Destino	Origen	Longitud	Datos y relleno	FCS
8	6	6	2	46-1500	4

Figura 4 PDUs *Ethernet* y 802.3i

El preámbulo se emplea para preparar al receptor para recibir una trama, los campos de direcciones se emplean para identificar las direcciones de capa dos, los campos tipo/longitud pueden emplearse operan dependiendo del valor al comienzo de dicho campo, si este es mayor a 1536 indica el protocolo de la capa superior o alguna función especial en la trama, si es menor a 1536 indica la longitud. El relleno se emplea a fin de introducir un retardo que permita escuchar si la trama colisiona, finalmente el FCS es un

"hash" esto es una especie de huella digital para los bits que componen la trama, el cambió de valor en alguno de ellos modifica el valor del hash y la trama es descartada.

La subcapa de enlace de datos (LLC) está definida por el estándar 802.2, es la más próxima a la capa de red, su función es agregar las capacidades de control de tráfico. Ofrece la opción de tener un servicio confiable orientado a conexión. A su vez provee una interfaz entre la capa de red y la subcapa MAC volviendo la capa de red independiente del medio de transmisión. Esta subcapa también esta presente opera en conjunto tanto con la tecnología *Ethernet* cómo con WiMAX.

2.4 Estándar 802.16-2004, tecnologías WiMAX

WiMAX (versión fija) es una certificación que reciben equipos BWA que cumplen con determinadas funciones y características establecidas por el estándar 802.16-2004; Sin embargo el protocolo se ha modificado varias veces, creándose así diversas versiones del estándar desde su creación, algunas añaden funciones o mejoran las existentes, otras son recopilaciones o correcciones.

En [4] se indica que la versión IEEE 802.16-2004 es la revisión y agrupación (consolidación) de los estándares 802.16-2001, 802.16c-2003, y 802.16a-2002. Posterior a él comenzaron e emitirse nuevos estándares para añadir la función de movilidad (IEEE 802.16e)

Al estar definido por un estándar la gran ventaja de un equipo WiMAX, es la interoperabilidad que significa que este puede comunicarse con cualquier otra tecnología basada en estándares IEEE.

2.4.1 Evolución del estándar IEEE 802.16-2004

El grupo de trabajo IEEE 802.16 sobre Estándares de Acceso Inalámbrico de Banda Ancha (Broadband Wireless Access Standards) fue creado en 1998, con la función principal de desarrollar estándares y prácticas recomendadas que apoyen el despliegue de las Redes Inalámbricas de Área Metropolitana (WMAN).

El estándar 802.16, menciona [4], fue el primero en publicarse, este aportó las técnicas para trabajar con línea de vista (LOS), en el año 2003 se liberó una mejora de dicho estándar, denominado IEEE 802.16 el cual define las características para hacerlo sin línea de vista (NLOS). Otras diferencias de igual importancia son: la banda de frecuencias de operación, para el 802.16 era de 10-66 [GHz] mientras que para el 802.16a era de 2-11

[GHz], siendo esta última la que se adoptó para el 802.16-2004, además la modulación empleada cambió de ser de portadora simple (SC) a OFDM.

Es importante señalar que el estándar no ha dejado de actualizarse, la versión más reciente que encontramos es del año 2011 y se denomina 802.16m; Sin embargo el equipo con el que contamos se encuentra certificado en base al estándar publicado en 2004.

El acceso fijo de banda ancha provisto por WiMAX (versión 2004) es una aplicación en la cual tanto la BS como la SS se encuentran fijas en una posición durante la operación. Este tipo de acceso es común en entornos residenciales, en donde es sencillo fijar la SS, ya sea al interior o al exterior del edificio, con el fin de transmitir hacia la BS. Con ello, servicios como Internet, TV por IP y Video Bajo Demanda (VoD) son ahora capaces de ofrecerse sin la necesidad de utilizar la fibra óptica o el sistema de cable actual.

La siguiente tabla describe algunas versiones del 802.16 que se han publicado:

Versión	Descripción
802.16	Publicado en abril 2002, es el primer conjunto de especificaciones, contiene las referentes para operar en el intervalo de frecuencias de 19 a 66 GHz exclusivamente con línea de vista y en topología PTMP. La máxima velocidad de transmisión es de 134 Mbps en celdas de hasta 5 km.
802.16 a	Publicado en enero de 2003, es una expansión del 802.16 para operar en el intervalo de frecuencias de 2 a 11 GHz, soportar transmisiones LOS y NLOS, así como topologías PTP, PTMP
802.16 c	Publicado en abril de 2003, es una expansión del 802.16 para especificar las operaciones en el intervalo de frecuencias de 10 a 66 GHz
802.16 d	Publicado oficialmente como la versión 802.16-2004. Agrupa la revisión de las versiones anteriores más los perfiles aprobados por WiMAX fórum.
802.16 e	Publicado en diciembre de 2005, extensión de la versión anterior que incluye las especificaciones para los dispositivos móviles.

Tabla 1 Evolución del estándar 802.16 [4]

2.4.2 Subcapa MAC

Los dispositivos basados en el [5] cumplen con una arquitectura de red basada en la subdivisión en capas de acuerdo al modelo de interconexión para sistemas abiertos (OSI), y especifican determinadas características de la subcapa MAC (dentro de la capa de enlace de datos) y la capa física.

De acuerdo a [3], desde la publicación de los estándares IEEE 802.x se dividió la capa de enlace da datos en las subcapas LLC y MAC con la finalidad de tener una interfaz compatible con el protocolo de la capa de red sin importar el medio físico utilizado para la transmisión.

Para explicar cómo se maneja el paquete una vez que es transferido hacia dichas capas es necesario describir los siguientes términos debido a que cuándo un la información se desplaza a través de la torre de protocolos recibe una denominación determinada, estos términos son:

- SDU(Service Data Unit): Se denomina así a la unidad de datos cuando asciende o desciende en la torre de protocolos, dichos protocolos deben ser adyacentes.
- PDU(Protocol Data Unit): Es la unidad de datos intercambiada entre protocolos en la misma altura de la torre de protocolos pero en puntos (ubicaciones) distintos.

Además es conveniente mencionar que son las siguientes definiciones y variables definidas en [5]:

SFID(Service-Flow Identifier): Identificador de SF, es un valor de 32 bits.

CID(Connection Identifier): Es un valor de 16 bits que identifica una conexión unidireccional entre la BS y una SS, a su vez se asocia a un service-flow mediante el mapeo con un SFID.

En general la subcapa MAC del estándar [5] cumple las funciones de:

1. Convertir la SDU recibida de la subcapa LLC a una MAC PDU.
2. Seleccionar el flujo al que corresponde la PDU por medio del CID y del SFID asociado.
3. Brindar calidad de servicio (QoS) a través del mapeo del SFID a determinada “clase de servicio”, este concepto comprende los mecanismos de “*schedulling*”, todo esto se desarrolla a detalle en el capítulo de descripción del equipo.
4. Administrar retransmisiones de PDU’s de ser requeridas.
5. Proporcionar seguridad sobre el canal inalámbrico.

Este estándar, a su vez subdivide la subcapa MAC en tres porciones:

1. Subcapa de convergencia para servicios específicos (ATM o basada en paquetes).
2. Subcapa de parte común.
3. Subcapa de privacidad.

La figura siguiente representa la pila de subcapas que describe el estándar [5]

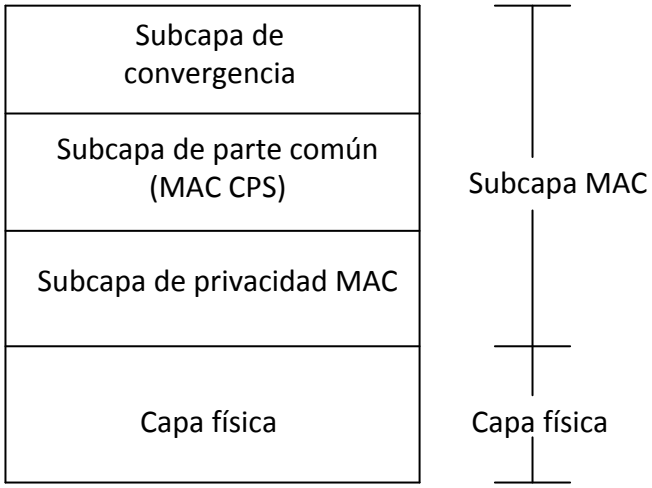


Figura 5 Subcapas del protocolo 802.16-2004 [4]

2.2.2.1 Subcapa de convergencia para servicios específicos CS (ATM o basada en paquetes)

Las especificaciones en [5], se inclinan por el uso del protocolo IP para la administración de las MAC PDU's, para ello la subcapa de convergencia realiza un mapeo entre las direcciones IP de los dispositivos que conforman la red y las direcciones de las conexiones MAC (CID).

La Subcapa de convergencia también cuenta con la capacidad de supresión de cabecera (PHS Protocol Header Supression), esto es suprimir el encabezado de la capa superior, esto resulta útil al momento de enviar la información a través de la interfaz aérea debido a que las direcciones IP origen y destino se encuentran "atadas" a la dirección MAC por medio de dicho mapeo (CID). Al no transmitir los datos de la cabecera se consigue ahorrar ancho de banda del canal.

2.2.2.2 Subcapa de parte común

Esta subcapa es independiente del protocolo de capa superior, realiza sus acciones basado en el CID. Es responsable de administrar el acceso al medio y con ello las políticas de calidad de servicio (QoS).

En el estándar [5] la calidad de servicio se asigna por medio de "plantillas", la plantilla tiene como parámetros determinados valores de campos de la cabecera del paquete IP y un tipo de *schedulling*, esto es un tipo de tráfico determinado. Si los valores del paquete que está siendo procesado coinciden con la plantilla, el paquete se envía a la interfaz aérea respetando las características del tipo de *schedulling* indicado en dicha plantilla. La definición de *schedulling*, los tipos de esté, los campos del encabezado IP así como el proceso para realizar la plantilla se describen más a detalle en el capítulo III Equipo de red y aplicaciones.

La retransmisión de información suele dejarse en responsabilidad de protocolos de las capas superiores; Sin embargo el estándar [5] define mecanismos para que esta subcapa gestione la retransmisión de tramas.

2.2.2.3 Subcapa de Seguridad

En [5], se consideran principalmente dos tipos de amenazas, la primera la violación de privacidad, esto es que alguien logré acceder y utilizar la información de un usuario válido sin su consentimiento, la segunda es el acceso no autorizado a los servicios, esto es que alguien sea capaz de usar los servicios sin autorización del administrador del equipo.

La privacidad se protege a través del cifrado de la comunicación entre la BS y cada SS (AES, 3DES). La llave de encriptación es distribuida sólo por la BS hacia las estaciones suscriptoras registradas (PKM), además se emplean certificados digitales X.509 para garantizar la identidad de las estaciones, de esta manera también se controla el acceso a la red, puesto que sólo las estaciones suscriptoras dadas de alta por el administrador en la BS reciben una llave.

2.4.3 Capa física

La parte del protocolo [5] que corresponde a la capa física (PHY) es la responsable de establecer la conexión a través del medio físico entre los extremos de la conexión.

En general define las características de la interfaz de radio que va a utilizarse. Por ejemplo: el rango de la potencia de la señal, la técnica de modulación y demodulación, el acceso al múltiple, codificación, incluso las características que deben cumplir las antenas tanto de la BS como de las estaciones suscriptoras.

El estándar [5] trabaja bajo la técnica de modulación OFDM; Sin embargo enumera cuatro tipos diferentes de interfaces de radio, esto se debe a la propia evolución del estándar. Las

principales diferencias son la banda de frecuencia en que operan, y el soporte de transmisión sin línea de vista (NLOS) que se debe al tipo de modulación utilizada. Estas variantes son:

Red de Área Metropolitana Inalámbrica con una Sola Portadora (WMAN- SC, Wireless Metropolitan Area Network – Simple Carrier)

Red de Área Metropolitana Inalámbrica con Acceso a una Sola Portadora (WMAN-SCa, Wireless Metropolitan Area Network - Single Carrier access)

Red de Área Metropolitana Inalámbrica con Multiplexaje por División de Frecuencias Ortogonales (WMAN-OFDM Orthogonal Frequency Division Multiplexing)

Red de Área Metropolitana Inalámbrica con Múltiple Acceso por División de Frecuencia Ortogonal (WMAN-OFDMA, Orthogonal Frequency Division Multiple Access)

WMAN-SC es la primera versión, esta se diseñó para operar en el rango de frecuencias de 10 a 66 [GHz], no soporta trasmisiones sin línea de vista. WMAN-SCA es la mejora de la primera versión, esta sí soporta la trasmisión NLOS y opera en la banda de frecuencia debajo de 2 a 11 [GHz]; Sin embargo aún utilizaba la tecnología de una portadora (SC) por lo que no se alcanzaban altas tasas de transmisión. Con WMAN-OFDM se modificó la modulación, la técnica empleada fue OFDM, dicha técnica se describe a detalle a continuación; Sin embargo puede mencionarse que se divide el canal de radio en varios subcanales los cuales poseen las características de: transmitirse sin agregar bandas de guarda entre los subcanales, resistencia al ISI (interferencia entre símbolo), y la respuesta del canal se considera plana en cada subcanal. Esta modificación se definió en el estándar del año 2004 [5], se fijó el número de subcanales en 254 (número de portadoras). Finalmente la última capacidad que se ha agregado en la especificación WMAN-OFDMA es la asignación de un grupo de subcanales a un usuario determinado y se incrementó el número máximo de portadoras a 2048; Sin embargo un número mayor a 254 portadoras se implementa para la versión móvil.

2.4.3.1 OFDM (Orthogonal Frecuency Division Multiplexing)

OFDM es una técnica de multiplexaje (y modulación) multiportadora. Puede verse cómo una adaptación de la modulación en frecuencia que es capaz de transmitir en banda ancha y alcanza altas velocidades de transmisión.

Los sistemas monoportadora fueron los primeros en desarrollarse, incluso siguen empleándose en sistemas como los de AM y FM; Sin embargo por su naturaleza tienen limitaciones significativas.

La principal limitante del ancho de banda en los sistemas que ocupan una sola portadora es la atenuación selectiva en frecuencia. Esto es que determinadas componentes del espectro de la señal son atenuadas al desplazarse en el aire más que otras, se debe principalmente a los componentes químicos del aire que absorben la radiación electromagnética a determinadas frecuencias (puede observarse el comportamiento de la atenuación respecto a la frecuencia en la siguiente figura).

Además los sistemas de una sola portadora necesitan recibir todas las componentes del espectro de la señal para poder leer la información, la interferencia en un conjunto de frecuencias que compongan la señal causa la pérdida completa de la información. La interferencia puede ser originada por la señal consigo misma después de descomponerse al chocar con elementos sólidos y viajar por múltiples trayectorias o por otra señal transmitiendo sobre algunas de sus frecuencias.

Lo anterior limita a que los canales de un sistema monoportadora usen bandas de frecuencias pequeñas y ubicadas a manera de evitar la atenuación selectiva. Además se dejan porciones del espectro radioeléctrico sin utilizar entre los canales con el fin de evitar el traslape con el espectro de la señal de otro canal.

Un ejemplo, tomado de [6], muestra cómo afectan los componentes atmosféricos a las señales, puede apreciarse la atenuación debida a la simple presencia del oxígeno y del vapor de agua:

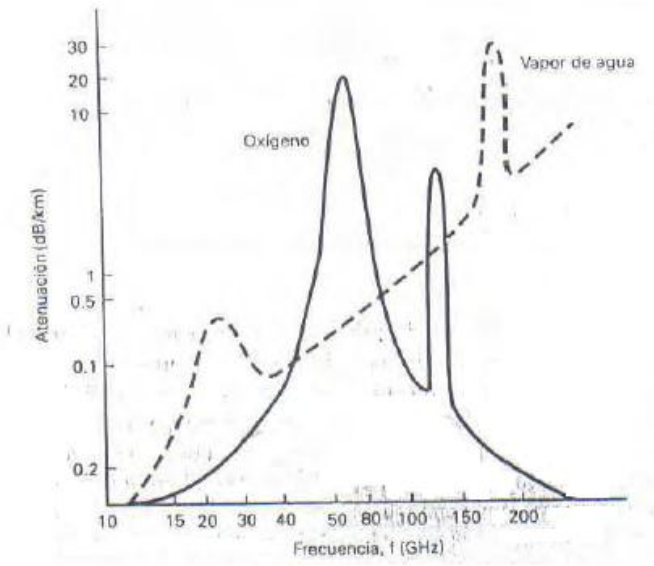


Figura 6 Atenuación de las ondas radioeléctricas debido a la presencia de oxígeno y de vapor de agua [6]

ISI (Inter Simbol Interference)

La tasa de transmisión es una medida de la cantidad de información capaz de enviarse a través del medio por unidad de tiempo, se mide en símbolos por segundo.

El canal inalámbrico presenta una limite en la tasa de transmisión debido principalmente a la interferencia entre símbolos, esta es el traslape de los símbolos (en el dominio del tiempo).

De [5], en sistemas NLOS la señal choca con obstáculos que generan la fragmentación de la señal original, y su desplazamiento a través de diferentes trayectorias genera que los fragmentos de la señal original llegan a su destino con diferentes retardos, así el símbolo original se ve expandido en el tiempo pudiendo traslaparse con el siguiente símbolo en transmitirse.

En [4], se denomina τ como el retardo máximo introducido por el medio de propagación y Ts cómo la duración del símbolo. Si τ es comparable con Ts los símbolos quedan irreconocibles para el sistema, por otra parte en el caso de que $Ts >> \tau$ el sistema es aún capaz de extraer la información gracias a que la duración de la interferencia es despreciable.

En la parte superior de la siguiente ilustración se la señal a la salida de transmisor, y la parte inferior la recibida en el receptor, esta es la señal distorsionada por el ISI

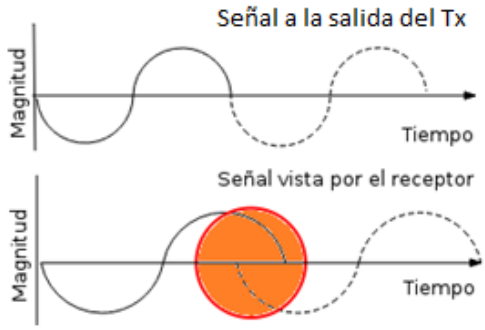


Figura 7 Señal distorsionada por ISI (en el dominio del tiempo)

ICI (Inter Carrier Interference)

Es el traslape del espectro de señales pertenecientes a distintos canales (en el dominio de la frecuencia). Sí al procesar la señal se introducen cambios bruscos en la señal el dominio del tiempo por ejemplo truncamientos, o ISI, se generan componentes de alta frecuencia el espectro de la señal y pueden provocar el traslape con otro canal.

La siguiente ilustración es una representación del espectro de dos señales, en el primer caso estas se consideran ortogonales porque en la componente de la portadora una señal alcanza su máximo valor de potencia mientras que la otra se mantiene en cero. Cuando esto deja de cumplir una canal interfiere con el otro, esto se denomina ICI.

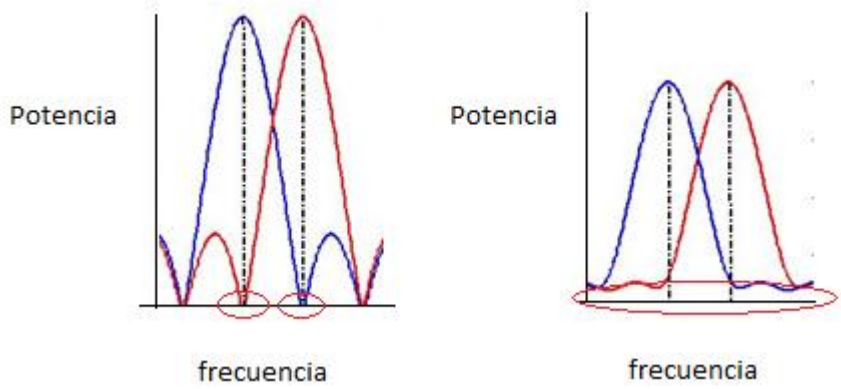


Figura 8 Ejemplo de ICI

La técnica OFDM es capaz de mitigar las atenuaciones selectivas, la ISI e ICI. Su funcionamiento, cómo se plantea en [4] es el siguiente:

1. Toma una alta tasa de transmisión y la divide en N flujos de una menor tasa de transmisión.

La primera etapa se implementa con un convertidor serial a paralelo, el cual divide el flujo principal a los N subcanales. Cada subcanal cuenta con un modulador binario adaptable (hasta 64QAM) el cual reduce aún más la tasa de transmisión de cada subcanal.

Este paso incrementa la duración de Ts haciendo al sistema robusto contra la ISI. Además haciendo uso de diferentes subcanales si se presenta atenuación selectiva sólo algunos subcanales son afectados, los demás pueden seguir transmitiendo sin problemas.

2. "Disfrazar" los símbolos de los subcanales como el espectro de una señal (la moduladora).

Se implementa a través de la IFFT (especificada de 254 puntos para [5]), esta es una transformación del dominio de la frecuencia al dominio del tiempo.

La IFFT (FFT) presenta la ventaja de que el espectro se representa mediante componentes discretas, finitas y equiespaciadas. Al ser discretas y finitas pueden obtenerse a partir de los valores de los símbolos QAM en los subcanales. La separación entre las componentes puede manipularse, esta representa la banda de guarda y puede reducirse al mínimo. Además representados mediante diferentes frecuencias y con el uso de mecanismos de sincronización los canales son ortogonales entre sí.

3. La salida de la IFFT es enviada a un convertidor paralelo-serial, anteriormente le es agregado el prefijo cíclico (*"Cyclic Prefix"*).

La secuencia a la salida del convertidor paralelo a serial es la base del símbolo OFDM. Con el fin de combatir la ISI e ICI parte del comienzo de secuencia es copiada y agregada al final de la secuencia original, dicha copia se denomina prefijo cíclico.

El prefijo cíclico tiene una duración que es usada como tiempo de guarda para contrarrestar el ISI. Si cómo tiempo de guardia se cesa la transmisión se genera un cambio brusco en la secuencia lo cual expande su espectro y genera ICI entre los subcanales, en cambio el prefijo cíclico sigue el mismo comportamiento de la secuencia original por lo que

la modificación del espectro es mínimo o nula y se garantiza la ortogonalidad de los subcanales.

4. La secuencia más el prefijo son convertidos a una señal analógica la cual es modulada y radiada al aire. El proceso de recepción involucra los mismos bloques pero en sentido inverso.

El diagrama siguiente es el diagrama a bloques sobre el cuál se realiza el proceso descrito:

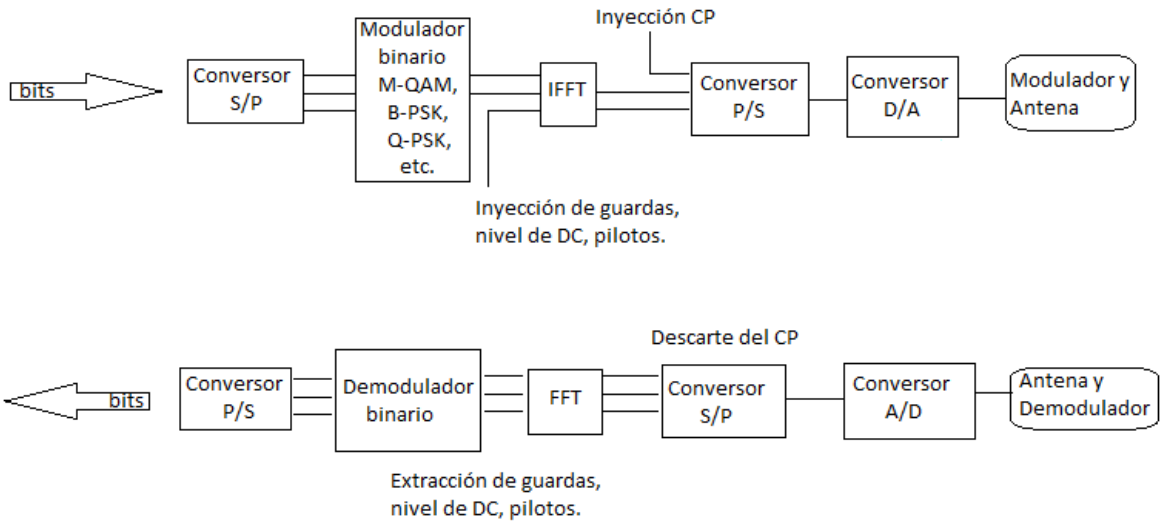


Figura 9 Diagrama a bloques del modulador OFDM [4]

En [4], se describe que puede comprobarse la ortogonalidad mediante las propiedades matemáticas de la transformada rápida de Fourier de la convolución circular.

Cuando la señal atraviesa el aire la secuencia sufre una convolución lineal con la respuesta al impulso del aire; Al agregar el prefijo cíclico la convolución genera una secuencia periódica, los valores de un periodo de dicha secuencia son iguales a los obtenidos mediante la convolución circular de la secuencia original con la respuesta al impulso del aire.

La transformada rápida de Fourier de la convolución circular consta en la multiplicación de la FFT de la secuencia del símbolo con la FFT de la respuesta al impulso del canal. Puede apreciarse que el resultado es el escalamiento del espectro de x[n] más no se agregan, o desplazan sus componentes por lo que se conserva la ortogonalidad.

Las funciones de convolución circular en el tiempo y de producto en el dominio de la frecuencia son:

$$y[n] \equiv f[n] \circledast h[n]$$
$$Y[k] = F[k]H[k]$$

Figura 10 Par de transformadas discretas: Convolución circular - Producto

2.4.3.2 Tipos de modulación soportados por el estándar de WiMAX.

El estándar [5], define la posibilidad de emplear una de las siguientes técnicas de modulación: adaptable, BPSK, QPSK, 16-QAM y 64-QAM, de [6] estas se describen como:

Modulación BPSK (Binary Phase Shift Keying), el símbolo de la modulación π o −π representada un bit.

Modulación QPSK (Quadrature Phase Shift Keying), similar a la modulación BPSK, esta modulación consiste en dos bits para representar cuatro posibles fases con una separación de π/2 entre ellas.

QAM (Quadrature Amplitude Modulation), 16-QAM y 64-QAM. La modulación QAM cambia las amplitudes de dos portadoras sinusoidales dependiendo de la secuencia que deba ser transmitida; las portadoras se encuentran desfasadas entre sí +π/2, esta modulación de amplitud es llamada cuadratura. La modulación 64-QAM es la más eficiente (b/s/Hz) incluida en el estándar 802.16; en ella, se transmiten 6 bits por cada símbolo de la modulación.

Modulación adaptable, Esta es una técnica dinámica, el principio es: cuando se producen condiciones adversas a las ondas de radio, el motor de modulación adaptiva detecta la degradación de la señal y automáticamente cambia el modo de modulación a una tasa inferior, pero más tolerante con el modo de modulación. Es decir, cuando una SS se encuentra cerca de la BS el enlace de radio será mejor, pudiendo ocupar una modulación de mayor orden, lo que se refleja en una mayor tasa de transmisión.

2.4.3.3 Topologías

El estándar [5] define dos topologías para los nodos conectados dentro de una red WiMAX:

- Punto a multipunto (PMP)
- Malla (Mesh). También conocida como Multipunto a multipunto (MP-MP)

La principal diferencia entre estos dos modos es la manera en que se llevan a cabo las conexiones. En el modo PMP, el tráfico puede viajar solamente entre la BS y el suscriptor, y por el contrario, en el modo malla, los nodos están conectados entre sí, de modo que aquellos que estén fuera de la cobertura de la BS, puedan establecer una conexión con algún otro nodo y concretar el envío de información hasta ella.

2.4.3.4 Propagación NLOS y LOS

Se definen dos tipos de propagación para cualquier tecnología inalámbrica de transmisión de información: transmisión en línea de vista (LOS) y transmisión sin línea de vista (NLOS).

El término LOS, cómo se define en [7], se refiere a la propagación de las ondas electromagnéticas viajando con una trayectoria de línea recta, con visibilidad entre el transmisor y el receptor. De acuerdo al estándar, la condición para que una transmisión se considere como LOS, es que el trayecto de la señal esté libre de obstáculos dentro de la primera zona de Fresnel.

Y, por el contrario, la transmisión NLOS es aquella en la que se presentan obstáculos como edificios, árboles, montañas o líneas de alto voltaje entre el transmisor y el receptor. Esto tiene como consecuencia una señal recibida más débil, ocasionando mala calidad, baja tasa de transmisión o incluso, una posible interrupción en la comunicación.

2.5 ARP (RFC 826)

De [2], ARP tiene el objetivo de asociar direcciones IP con direcciones de capa 2, puede verse como una tabla creada y almacenada dinámicamente de manera local en cada computadora.

Se tiene un paquete especial para este protocolo, este es:

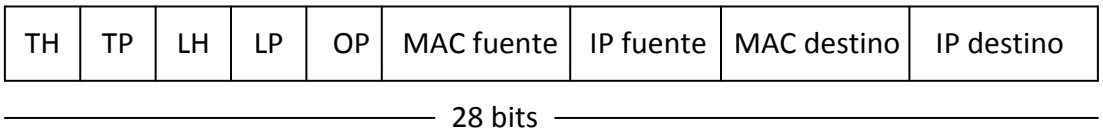


Figura 11 Paquete ARP

Para esta implementación, los campos referentes al hardware (H) se refieren al protocolo de capa dos y su longitud, los campos referentes al protocolo se refieren a IP y su longitud. Y según el campo de operación se tienen diferentes funciones, las más relevantes para nosotros son:

Petición de ARP (ARP request): Es originada por la máquina que desconoce la dirección de capa 2, se envía a todas la máquinas directamente conectadas indicando la dirección IP que se busca esperando que algún destinatario reconozca la dirección IP como propia y proceda a enviar una respuesta de ARP.

Repuesta de ARP (ARP reply): Se origina después recibir una petición de ARP, esta es enviada únicamente a la máquina que la envió y entrega la dirección de capa dos solicitada.

2.6 IEEE 802.1Q

Los *switches* son dispositivos que brindan conectividad de capa 2 en redes de computadoras, es decir conectividad local. Como se describirá posteriormente estos cuentan con un mecanismo para restringir el acceso entre las computadoras por grupos, denominado VLANs.

Los enlaces conectados al *switch* pueden operarse a modo de permitir el paso de información de una VLAN específica o de un conjunto de estas. Cuando permite el paso de varias se denomina un enlace troncal.

Los *switches* de pueden operarse mediante el enlace troncal definido por el protocolo 802.1Q IEEE. Las características de este son: en primer lugar añade una etiqueta sobre la trama *Ethernet* recibida, en esta etiqueta se especifica la VLAN a la que pertenece y cómo se explica posteriormente brinda un campo para definir la QoS. En segundo lugar mantiene una VLAN sin etiqueta, esto para operar con dispositivos incapaces de emplear el 802.1Q.

El proceso con el cual un *switch* asigna una trama a una VLAN es el siguiente:

A la trama recibida por el puerto en modo de acceso con destino a un puerto en modo troncal le es insertada una etiqueta llamada campo información de control de etiqueta, se modifica el valor del campo Tipo/Longitud (antes mencionado) a 0x8100 hexadecimal y se recalcula el valor del FCS. Posteriormente se envía sobre el enlace troncal.

El valor de 0x8100 en el campo Tipo/longitud sirve para indicar que la trama opera bajo el protocolo 802.1Q.

El FCS se emplea para preservar la integridad de la trama, esto es que no sufra modificaciones durante el envío, por ello al modificarla se debe recalcular el FCS puesto que la información ha cambiado y de no hacerlo el receptor lo detectaría como un error.

Finalmente el campo de información de control de etiqueta contiene tres campos:

1. Prioridad del usuario: Aporta la funcionalidad de QoS basado en VLAN (3 bits).
2. Identificador de formato ideal: Es un bit bandera que brinda interoperabilidad con otro protocolo de capa 2 (1 bit).
3. VLAN ID: un número del 1 al 4096 que representa el ID de VLAN (12 bits).

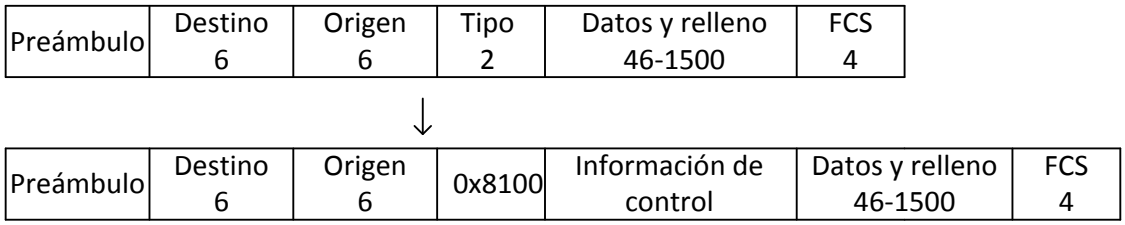


Figura 8 Trama 802.1Q [17]

2.7 DTP

El protocolo de enlace troncal dinámico (DTP) es propietario de CISCO. Su función es simplificar la configuración de un enlace troncal mediante mensajes de negociación entre puertos de *switches* interconectados, dichos mensajes empleados de manera correcta permiten un comportamiento similar al de un maestro/esclavo, en este caso un puerto ordena la formación del troncal y el otro simplemente obedece. De nueva cuenta se recalca el que los *switches* CISCO solo operan con protocolos de VLAN 802.1Q e ISL (casos especiales soportan solo un tipo de estas y en la práctica causan problemas de interconectividad cuanto el otro equipo no puede manejar el mismo protocolo, siendo la única solución cambiar alguno de los equipos).

2.8 Protocolos de VoIP

VoIP (Voice over Internet Protocol) es el servicio de telefonía sobre una red IP. El bajo precio de este servicio es el principal motivo de su desarrollo; Sin embargo es más compleja de transmitir que la telefonía analógica puesto que realizar una llamada requiere de convertir la señal del formato analógico a digital y viceversa, también emplear un sistema de transporte resistente al retardo, el jitter y que tire pocos paquetes. VoIP requiere protocolos que regulen la codificación, la señalización y optimicen el transporte de la señal, estos se describen a continuación. Tiene en común con la telefonía analógica el uso de señalización para el establecimiento de una llamada.

2.8.1 SIP (RFC 3261)

Definido por la IETF, es un protocolo de la capa de aplicación con la capacidad de establecer sesiones telefónicas y de videoconferencia sobre INTERNET. Se encuentra entre los más empleados por que su diseño lo hace compatible con otras aplicaciones de INTERNET, en [2] se menciona el ejemplo de que los número de marcación se representan mediante URLs (ya sea por nombres de dominio, direcciones IPv4 o direcciones IPv6) y la transferencia de mensajes se hace mediante HTTP por lo que puede incrustarse en una página WEB y mediante una aplicación comenzar una conversación de telefonía con dar *click* a un *link*.

Debe mencionarse que este protocolo sólo se encarga de controlar la sesión, delega la responsabilidad del transporte de datos a otro protocolo especializado y el procesamiento de la señal de voz al códec (para esta implementación son el protocolo RTP y G.723 respectivamente).

La desventaja de SIP radica en que es un protocolo distribuido, esto es en el caso de VoIP que todos los teléfonos deben soportar todas las funciones de SIP, y basados en [12], lo que más lo limita es que los teléfonos con los que se desea comunicar deben estar dados de alta de manera local; Sin embargo en [2] se menciona un mecanismo que puede mitigar en cierto grado dicha limitante, este se explica más adelante.

Los mensajes con los que se controla la llamada son:

1. INVITE – Solicita iniciar una sesión.
2. ACK – Confirma el establecimiento de la sesión.
3. BYE – Solicita el fin de una sesión.
4. OPTIONS – Consulta al otro equipo sobre sus capacidades.
5. CANCEL – Niega el establecimiento de una sesión.
6. REGISTER – Informa a un servidor *proxy* la solicitud de una sesión.

Por otra parte los equipos se clasifican de la siguiente manera:

1. Agente de usuario: Los teléfonos son los agentes de usuario, cómo se mencionó antes este es un protocolo distribuido así el equipo que origina la llamada toma la función de cliente, mientras que el equipo que la recibe funge cómo servidor.
2. Servidor proxy y servidor de ubicación: Un servidor *proxy* tiene la función de colocarse entre equipos terminales que establecen una sesión de comunicación, y finge ser uno de los nodos. En el protocolo SIP toma el lugar de ambas terminales ó teléfonos. Por su

parte el servidor de ubicación es una base de datos que contiene todos los teléfonos que componen la infraestructura.

El funcionamiento del servicio se describe en [2] y es el siguiente:

Sin el uso de servidores, el teléfono que desee iniciar la conversación envía una mensaje INVITE al otro extremo informando además las condiciones de la sesión, el otro extremo responde mediante un código especial de HTTP que acepta o rechaza la conexión. Finalmente el equipo que inició la llamada responde con un mensaje ACK.

Con el uso de servidores (el caso de esta tesis), se inicia el establecimiento de la sesión mediante el envió de un mensaje REGISTER hacia él servidor proxy, este se encuentra conectado directamente al servidor de ubicación al cual le redirecciona el paquete recién recibido. El servidor de ubicación busca en su base de datos las direcciones de los teléfonos origen y destino, si encuentra ambas y les está permitido comunicarse entre sí envía un paquete al servidor proxy instruyéndole que envié un mensaje INVITE al teléfono destino, a partir de ese momento se sigue el establecimiento de la sesión mencionado anteriormente entre el servidor proxy y ambos teléfonos, es decir el proxy queda como mediador entre ambos. Este caso mitiga la desventaja de necesitar una base de datos local en cada teléfono; Sin embargo los teléfonos necesitan seguir siendo capaces de soportar tanto las funciones de cliente como de servidor SIP.

Cabe mencionar que el *gateway* de voz empleado en la red tiene integrados tanto un servidor de ubicación cómo un servidor *proxy*.

2.8.2 RTP (RFC 1889)

RTP, expuesto en [2], es un protocolo de transporte implementado en capa de aplicación. Fue diseñado para la transmisión de contenido multimedia (voz, video) en tiempo real. Cómo se explica en el siguiente subtema dicho contenido se compone de más de un flujo de datos, RTP toma estos flujos, los multiplexa y codifica en un solo.

Luego el paquete RTP (con la información multimedia contenida) es enviado a las capas inferiores a través de un flujo único mediante UDP, este puede ser enviado a uno o muchos puntos remotos. La siguiente figura muestra el encapsulado:

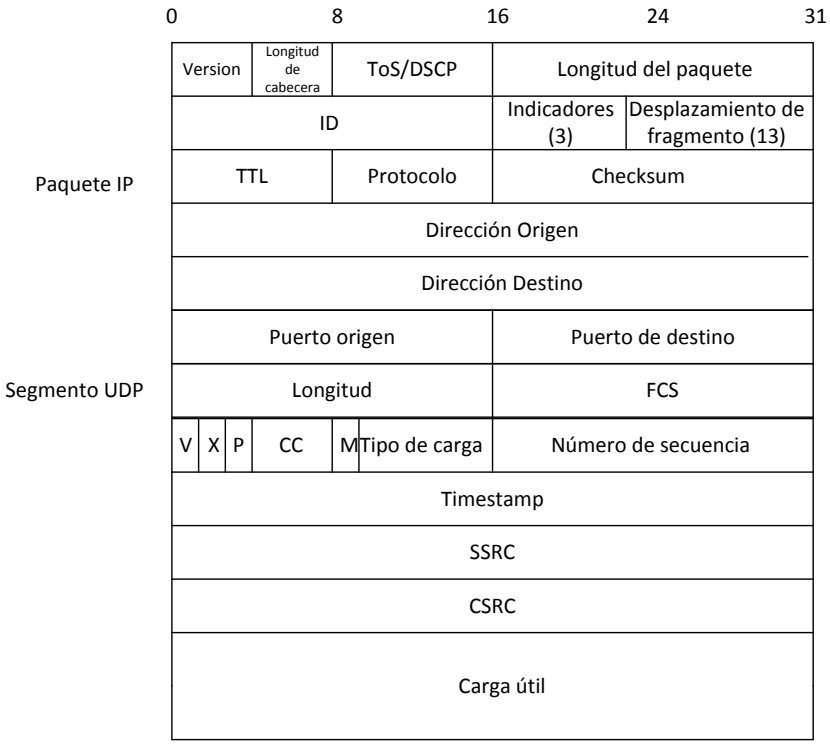


Figura 13 Encabezados de protocolo RTP, UDP e IP

El paquete RTP contiene campos para añadir las funciones de:
Detectar paquetes perdidos y aproximar su valor mediante el campo “número de secuencia”. Anunciar el tipo de códec empleado en su contenido mediante el campo “Tipo de carga”. Anunciar la aplicación que genera el tráfico mediante el campo M. En caso que una aplicación emplease más de un flujo RTP (por ejemplo el sonido estéreo), el campo “timestamp“ sincroniza el inicio de reproducción de dichos flujos. Mientras que el campo “identificador de origen de sincronización” identifica el flujo “padre”.

2.8.3 Códec G.711 (ITU)

De [12], este estándar tiene la función de convertir la señal de voz a un formato digital y viceversa.
El proceso empleado para la conversión analógica a digital consiste en:

- Muestro: captura períodica de fragmentos de voz (8 [kHz]).
- Cuantificación: asignación a un valor normalizado (256 valores).

Codificación y compresión: representar el valor cuantificado mediante una serie de bits (8 bits).
Para convertir la señal digital a analógica se sigue el proceso de:

- De-codificar y de-comprimir: la serie de bits es representada por el valor normalizado.

- Reconstrucción de la señal: consiste en el filtrado selectivo de la serie de valores normalizados. El resultado del proceso anterior es una señal modulada por pulsos, la envolvente de esta es la señal de voz, y para poder escucharla se eliminan las componentes de frecuencia relacionadas a los pulsos (siendo estos de corta duración parecen impulsos así que se relacionan con altas frecuencias) mediante un filtro pasabajas.

Este estándar puede considerarse el códec de voz más simple, basa sus parámetros en las frecuencias promedio de la voz humana y el teorema de Nyquist. No comprime la señal de voz y por ello requiere una tasa de datos de 64 [kbps]. Para fines prácticos este sería uno de los códecs que tratarían de evitarse puesto que consume gran cantidad de canal respecto a otros; Sin embargo el fin de este trabajo es evaluar el enlace operando al máximo de su capacidad.

2.9 Estándares MPEG

La mayor complejidad para transmitir video digital es la gran cantidad que información contenida en una secuencia de imágenes, siendo inviable transmitir sin antes comprimir la información. El archivo de video digital tiene tres componentes básicos:

1. Señal de video (codificada)
2. Señal de audio (codificada)
3. Contenedor (encapsulación)

Definidos para MPEG-1 según [2] cómo: audio, video y sistema.

MPEG (Moving Pictures Experts Group) es un grupo de trabajo de ISO e IEC, este se encarga del desarrollo de estándares de video, es decir de normalizar los códecs y contenedores. Desde su creación ha desarrollado una gran cantidad de códecs como son: MPEG-1, MPEG-2, MPEG-3, MPEG-4, MPEG-7, MPEG-21, MPEG-A, MPEG-B, MPEG-C, MPEG-D, MPEG-E, MPEG-F y MPEG-4AVC. En cuestión de formatos contenedores cuenta actualmente con tres tipos: MP4, MPEG-TS y MPEG-PS, esto se explica brevemente en [8].

El contenedor, envoltura o sistema es la estructura responsable de coordinar la señal de video con la señal de audio, además de proveer funciones extras que ayudan a la reproducción del contenido, dichas funciones van desde agregar subtítulos, hasta corrección de errores en medios con pérdidas (para soportar el "*streaming"*).

La transcodificación, es convertir el archivo multimedia a otro formato, la finalidad puede ser obtener: compatibilidad entre el formato y una aplicación en particular, mayor calidad de video ó como en nuestro caso reducir la tasa de reproducción.

A partir de las opciones de códecs de transcodificación disponibles en nuestro *software* (VLC) y de la calidad de la imagen observada elegimos usar la codificación MPEG 4 AVC y el contenedor tipo MPEG-TS, este último seleccionado por la capacidad de operar con pérdidas de paquetes.

2.10 FTP (File Transfer Protocol)

El tráfico de datos en una red convergente se refiere al flujo de información que contiene por ejemplo: la estructura de una página web, texto, imágenes, etc. Este tipo de información una vez recibida se mantiene estática así que lo importante es recibir todos los datos y sin errores, también debe mencionarse que este tipo de flujo no es afectado por retardos. Por lo anterior la transmisión de datos se realiza bajo conexiones TCP ya que, TCP es capaz de corregir errores y solicitar retransmisiones.

FTP es un servicio (basado en el protocolo del mismo nombre) de transferencia de archivos, forma parte del conjunto de protocolos TCP/IP por lo que garantiza la compatibilidad con el resto de aplicaciones y dispositivos de la red.

En [9] se explica que dicho servicio se basa en el modelo cliente-servidor, el servidor es el encargado de almacenar los archivos a los que se accede de manera remota, también maneja una base de datos con las cuentas de los clientes aceptados y los permisos de estos sobre los archivos. La función del cliente se limita a autentificarse y copiar archivos hacia su ubicación o viceversa (si el servidor lo permite).

El uso de un servidor FTP para simular el tráfico de datos nos ayuda a evaluar el desempeño del enlace, por cumplir con las siguientes características:

1. FTP se basa en conexiones TCP por lo que comprobar la integridad de un archivo descargado a través del enlace nos indicaría sí el enlace soporta tráfico de datos.
2. FTP está diseñado para transmitir a la máxima tasa que le permita el medio de transmisión, esto nos ayuda a evaluar sí las políticas de calidad a partir de la degradación de la calidad en la transmisión de voz y video cada vez que se está descargando un archivo.

CAPÍTULO III

Equipo de red

Para explicar de manera breve la configuración que brinda QoS de extremos a extremo es necesario presentar una breve descripción del equipo empleado y las funciones del mismo.

Este capítulo brinda esa descripción de las capacidades de los equipos de red usados (swithces, *routers*, BS y SS), posteriormente se explica cómo se realiza en general la administración de dichos equipos.

3.1 BS WiMAX Redline 100AN-U

El sistema WiMAX utilizado está compuesto por la BS marca redline modelo 100AN-U, estaciones suscriptoras de uso interior (SUI), y estaciones suscriptoras de uso exterior (SUO).

3.1.1 Características

Según se dice en [7], la BS cumple con la especificación [5], es decir WiMAX fijo. Soporta transmisiones punto a punto, y punto a multipunto ambas NLOS. Está compuesta por la unidad interior (IDU) y la unidad exterior (ODU). La primera se encarga de recibir y procesar el flujo de datos que ingresa por el puerto *Ethernet*, tiene la apariencia de un ruteador sólo que una de sus interfaces permite la conexión de un cable coaxial el cual alimenta la ODU. La ODU contiene el modem y la antena, esta es sectorial de 60 grados con una ganancia de 17 dBi y polarización vertical.

El IDU y ODU aparecen en la siguiente imagen:

Figura 14 BS WiMAX [7]

Soporta un ancho de banda de 3.5 MHz ó 7 MHz (especificación WMAN-OFDM) en la banda de 3.4 a 3.6 GHz. En teoría pueden existir hasta 28 canales de 7 MHz o 57 de 3.5 MHz; Sin embargo se necesita una BS por canal.

El funcionamiento de la BS puede verse como un acces point de kilómetros de cobertura, además analiza el contenido del flujo de datos que recibe y basado en parámetros preconfigurados por el administrador permite y coordina el acceso al canal inalámbrico.

También administra el acceso al medio inalámbrico en las estaciones suscriptoras para que respeten las mismas políticas que la BS.

El sistema soporta transmisiones sin línea de vista (NLOS), con línea de vista (LOS) y con línea de vista óptica (OLOS). El enlace con línea de vista se refiere a una transmisión sin obstáculos en al menos el 60% de la zona de Fresnel. En el enlace OLOS pueden existir obstáculos dentro de esta zona pero aun así existe visibilidad entre la antena de la BS y la SS.

3.1.2 Administración de las políticas de calidad

Service Class (SC):

Cómo se mencionó la subcapa MAC utiliza el mecanismo de *schedulling* o planificación para el manejo y la entrega de las SDU y las MAC PDU con diferentes requerimientos de QoS.

Para elegir el mecaniso de *schedulling* redline definió una plantilla denominada SC. Con dicha plantilla se crean las políticas de calidad que debe cumplir el enlace.

La plantilla de SC necesita que le sea asignado un nombre y un tipo de *schedulling*, estos son los definidos en el estándar [5], explicados en [4] (rTPS, nrTPS, UGS, BE) y se describen a continuación:

Unsolicited Grant Service (UGS)

UGS se diseñó para servicios de tráfico constante, es decir paquetes de datos de tamaño fijo a una tasa constante de bits (CBR). Sirve para ofrecer acceso como lo haría un enlace T1/E1, o la emulación de una línea telefónica privada dedicada. Exige se declare una tasa máxima de transmisión, nivel tolerado de retardo y jitter. La desventaja de esa clase es que “aparta” la tasa que se indica como mínima impidiendo que sea utilizada por otros servicios incluso si está en desuso.

real-time Polling Service (rtPS)

Esta clase está diseñado para soportar flujos tasa variable en tiempo real, tales como videos MPEG, exige se declaren las tasas máximas y mínimas de transmisión, el nivel tolerado de latencia y de jitter; La ventaja sobre UGS es la tasa mínima de transmisión, la cuál indica que cierta porción de la tasa es liberada cuando entra en desuso.

Non-real-time Polling Service (nrtPS)

Este tipo de flujo está diseñado para soportar flujos que requieren un mínimo de tasa de transmisión reservado, pero es tolerante a retrasos y jitter, tales como una descarga de archivos mediante FTP. En nrtPS debe definirse la tasa máxima y mínima de transmisión.

Best Effort (BE)

Esta clase servicio puede considerarse la más baja o de menor cantidad de privilegios, está diseñado para operar con datos robustos ante retraso, jitter, y pérdida de paquetes, estos en su mayoría basados en conexiones TCP que por lo mismo llevan un control en la secuencia de los paquetes y garantizan la retransmisión en caso de ser necesaria, por ejemplo los datos HTML de una página WEB. Los datos son transportados si hay recursos disponibles. Requiere e defina una tasa máxima de transmisión y un nivel de QoS (este último prioriza sólo sobre otros flujos BE)

Extended real-time Polling Service(ertPS)

ertPS no está definido dentro de [5], se diseñó para la versión móvil de WiMAX específicamente para dar soporte a un flujo de datos similar al rTPS.

Una vez asignado el tipo de *schedulling* se activan las siguientes opciones en la plantilla, según se indica en [7]:

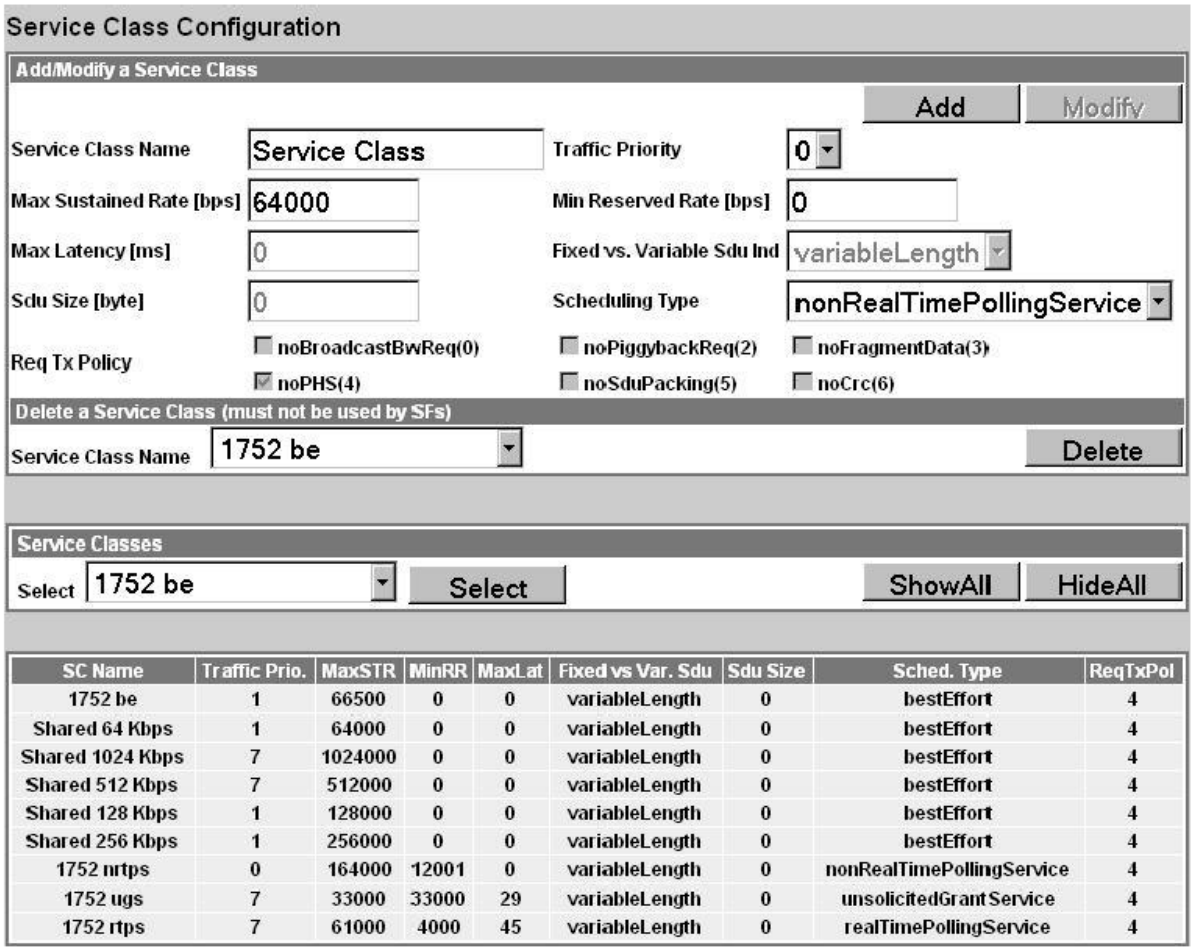
Prioridad (Traffic Priority): Indica la preferencia que tendrá el flujo de datos basado en este tipo de SC sobre otros flujos que utilicen el mismo tipo de *schedulling*. La mayor prioridad está representada por el número siete y la menor por el cero.

Tasa máxima/mínima: (Max/Min Sustained rate): Indica los límites máximo y mínimo en la tasa de transmisión del flujo de datos basado en la SC.

Sdu: Es la opción para elegir en recibir paquetes de longitud varibale en el puerto *Ethernet*. Si se activa la opción debe definirse el tamaño máximo de los paquetes en la casilla del mismo nombre (sdu size).

Req Tx Policy: sirve para elegir cómo se realizarán las peticiones y asginación del canal inalámbrico, es importante señalar que [5] define como obligatorio asignar un valor a dicho parámetro.

La figura siguiente es la captura de pantalla de la interfaz para configurar las SC:



SC Name	Traffic Prio.	MaxSTR	MinRR	MaxLat	Fixed vs Var. Sdu	Sdu Size	Sched. Type	ReqTxPol
1752 be	1	66500	0	0	variableLength	0	bestEffort	4
Shared 64 Kbps	1	64000	0	0	variableLength	0	bestEffort	4
Shared 1024 Kbps	7	1024000	0	0	variableLength	0	bestEffort	4
Shared 512 Kbps	7	512000	0	0	variableLength	0	bestEffort	4
Shared 128 Kbps	1	128000	0	0	variableLength	0	bestEffort	4
Shared 256 Kbps	1	256000	0	0	variableLength	0	bestEffort	4
1752 nrtps	0	164000	12001	0	variableLength	0	nonRealTimePollingService	4
1752 ugs	7	33000	33000	29	variableLength	0	unsolicitedGrantService	4
1752 rtps	7	61000	4000	45	variableLength	0	realTimePollingService	4

Figura 15 Menú de SC [7]

Service Flow (SF)

Con la SC se definen los parámetros que debe cumplir la tasa de transmisión, lo siguiente que debe indicarse es el sentido del flujo y en que campos del paquete deben buscarse las coincidencias para acceder al flujo de datos asociado a la SC. La plantilla que realiza este mapeo se denomina "SF".

La plantilla definida en la BS permite relacionar la SC, con un flujo unidireccional y los campos a analiza en la trama *Ethernet* recibida. Los campos de la plantilla en [7] son:

SFID: número que actúa como la huella digital del "SF", es decir identifica al "SF" y cumple con ser diferente de todas las demás.

SSName: Es la dirección MAC de la SS con la cual se establecerá el enlace.

Dirección: Indica el sentido de la transmisión. "Downstream" se refiere al flujo que va de la BS al suscriptor, y "upstream" identifica el sentido opuesto.

SCName: Es el campo mediante el cual se asocia la SC al "SF", en él se debe seleccionar el nombre de la SC a utilizar.

CSespecification: Indica el campo en el que se debe buscar la coincidencia en el flujo de datos recibido por el puerto *Ethernet*. En esta opción se aprecia la gran compatibilidad de WiMAX con los demás protocolos basados en IP ya que además de admitirse el procesamiento en base al encabezado el paquete IP se puede hacer también respecto al encabezado *Ethernet*, al de VLANs (802.1Q) y combinaciones de estos.

Es importante mencionar la existencia de "default SFs". Los equipos de red intercambian información entre sí para establecer la conexión por ejemplo al mapear direcciones MAC con direcciones IP (ARP). Los paquetes sobre los cuales viajan dicha información tienen un formato que impide que sus campos coincidan con los declarados para acceder a la interfaz aérea. Al no intercambiarse dichos paquetes se pierde la comunicación en capa 3 puesto que no pueden completarse las tablas ARP.

Los "default SFs" son los encargados de transportar dicho tráfico, el "default SFs" de bajada se encuentra siempre activado; Sin embargo el de subida el de subida debe activarse mediante la configuración avanzada del sistema.

La figura siguiente es la captura de pantalla de la interfaz para configurar los SFs:

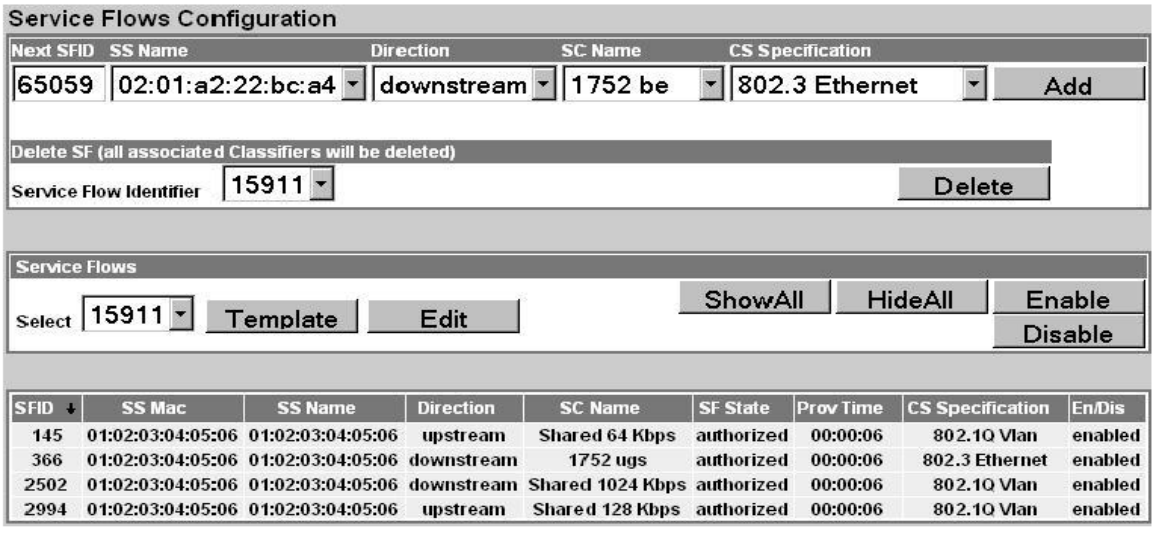


Figura 16 Menú de SFs [7]

“Classifiers”

Los clasificadores se indica en [7] toman un determinado "SF" como argumento de entrada y en base al protocolo de red especificado proporciona una interfaz para ingresar los valores que debe contener el encabezado del paquete. En caso de elegir el protocolo IP pueden ingresarse las direcciones IP origen y destino, sus máscaras de red y el número de puerto.

La BS tiene la capacidad de crear dinámicamente tantos clasificadores como dispositivos finales se posean; Sin embargo su uso limita el uso de las políticas de calidad puesto que estas se asignan al suscriptor impidiendo así especificar el servicio o el usuario al que se desea dar prioridad, además se restringe a usar direcciones IP del mismo segmento.

El proceso para activar esta funcionalidad consiste en crear la SC, mapearla con un SF y finalmente agregar el SF a un clasificador genérico, este es un clasificador con sólo el valor de la prioridad especificada. Además al momento de agregar un suscriptor (el proceso se detalla más adelante) debe activarse la etiqueta MAC *“learning”*.

La figura siguiente es la captura de pantalla de la interfaz para configurar los clasificadores:

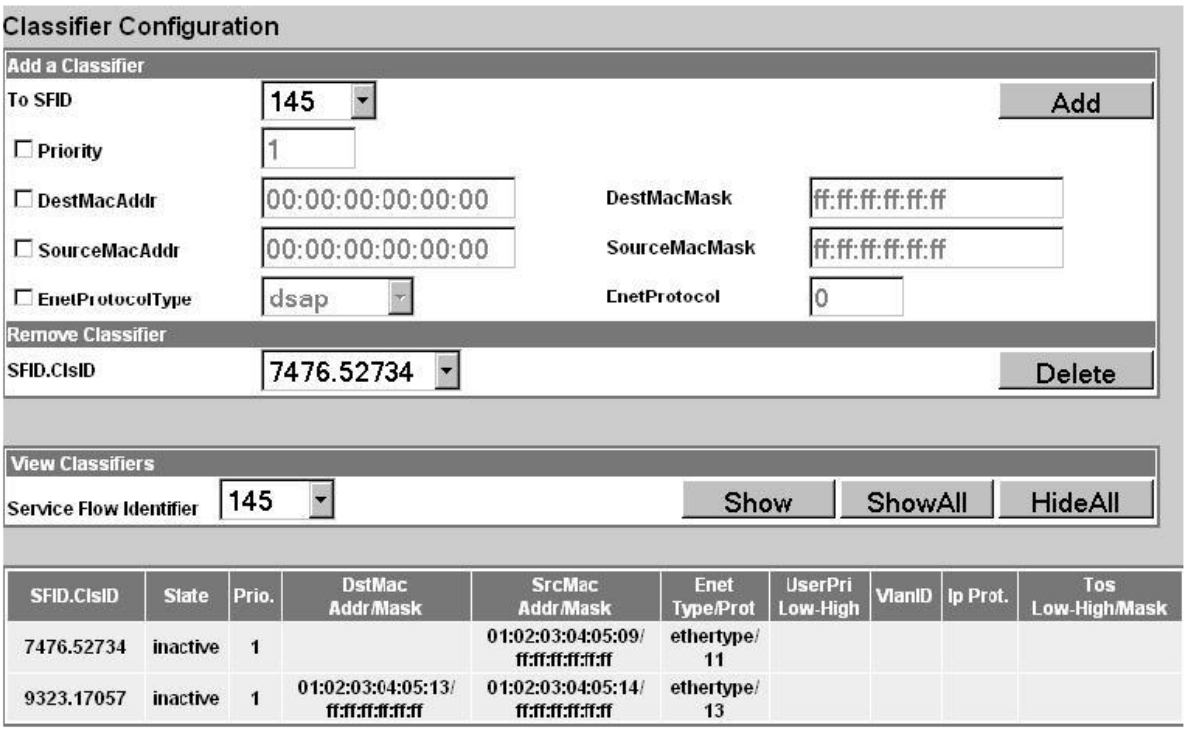


Figura 17 Menú de clasificadores [7]

Resumiendo la BS redline 100AN-U cuenta con las siguientes plantillas para definir la calidad de servicio:

La siguiente tabla resume las características de las plantillas usadas por WiMAX:

SC	Define la tasa de transmisión a la que debe someterse el flujo de datos, así como los valores de retrdo tolerado y la prioridad sobre otros flujos.
SF	Mapea la SC a una SS, indica el sentido del flujo y sobre que encabezado se basa clasificación.
Classifier	Especifica los valores esperados en el encabezado.

Tabla 2 Plantillas de WiMAX

3.1.3 Parámetros de la interfaz aérea

La BS es capaz de operar con canales de 3.5 MHz y de 7 MHz, la selección de dicho parámetro, así como el del prefijo cíclico, y la frecuencia de operación (central) se realiza desde la opción "Wireless Interface Configuration" de la interfaz gráfica (el acceso a la interfaz gráfica se describe más adelante). Además es posible usar el control de potencia y ganancia automático en las estaciones suscriptoras.

Para usar el control automático de potencia (de transmisión) debe activarse la etiqueta con el mismo nombre en la BS e ingresar el nivel de potencia promedio esperado de la señal recibida, los valores sugeridos son de -75 dBm para el canal de 3.5 MHz y -72 dBm para el canal de 7MHz.

Para activar el control automático de ganancia se activan las casillas con este nombre tanto en la BS como en los suscriptores,

3.1.4 Administración del equipo:

El proceso para acceder a la interfaz gráfica, se define en [7], primero se conecta una computadora a la BS mediante un cable de red (directo), luego se asigna una dirección IP del mismo segmento (192.168.182.X/24 por defecto) de la BS a la computadora. Cuando la conexión está lista se abre un navegador web y en el campo de la URL se ingresa la dirección 192.168.182.3 (dirección por defecto de la BS). El navegador pide entonces un nombre de usuario y contraseña, ambos son "admin".

Lo siguiente es agregar un suscriptor, para ello se da *"click"* a la pestaña *"Suscriber"*, al hacerlo se abre una página donde se debe ingresar la dirección MAC del suscriptor que actúa cómo su identificador puesto que es única, además se le da un nombre y de quererse se activa la opción para que el suscriptor aprenda las direcciones MAC de los dispositivos

conectados a él. Cómo el objetivo de nuestro enlace es brindar calidad de servicio basado en la dirección IP no activamos dicha casilla. La siguiente figura muestra el menú descrito:

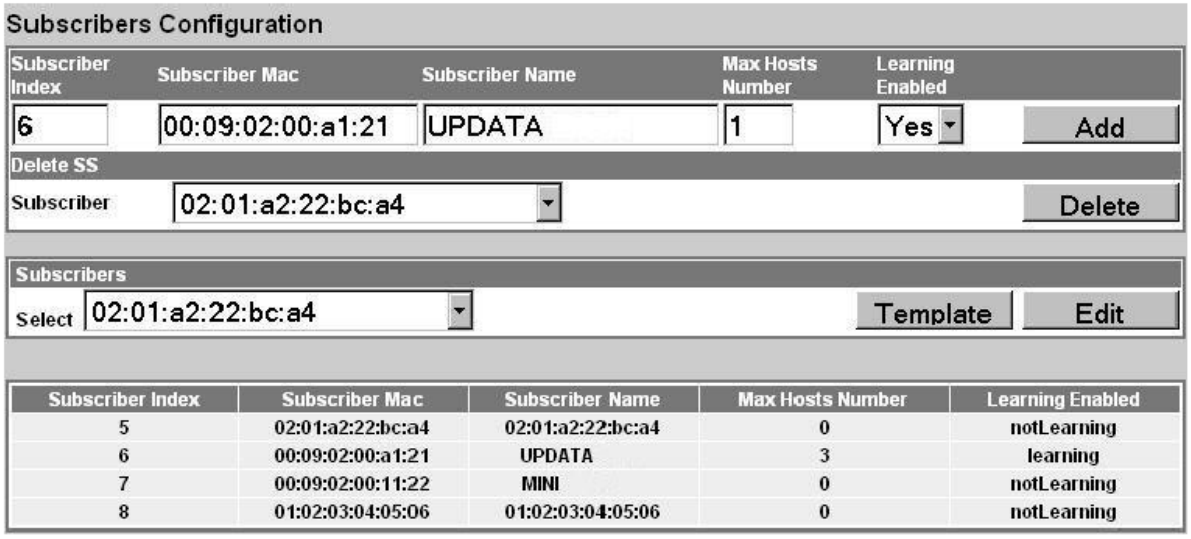


Figura 15 Menú de suscriptores [7]

Después de agregar el suscriptor se sigue el proceso descrito anteriormente, enumerando los pasos tenemos:

1) Crear la SC

2) Mapear en SF la SC, el suscriptor hacia el cual se dirige el flujo, la dirección del flujo y el encabezado en base al que se realiza el filtrado.

3) Se crea un clasificador basado en el SF, en este se especifican los valores del encabezado.

Para activar el *"uplink default SF"* dentro de la interfaz gráfica se ingresa a la pestaña de configuración avanzada, el sistema pide otro nombre de usuario y contraseña que en este caso son: redline y guest respectivamente. Dentro del menú se activa la opción de UL SF default y en la ventana debajo de esta se ingresa la tasa de transmisión de dichos SFs (se crea uno por suscriptor que esté dado de alta). La siguiente figura corresponde al menú para modificar la configuración avanzada:

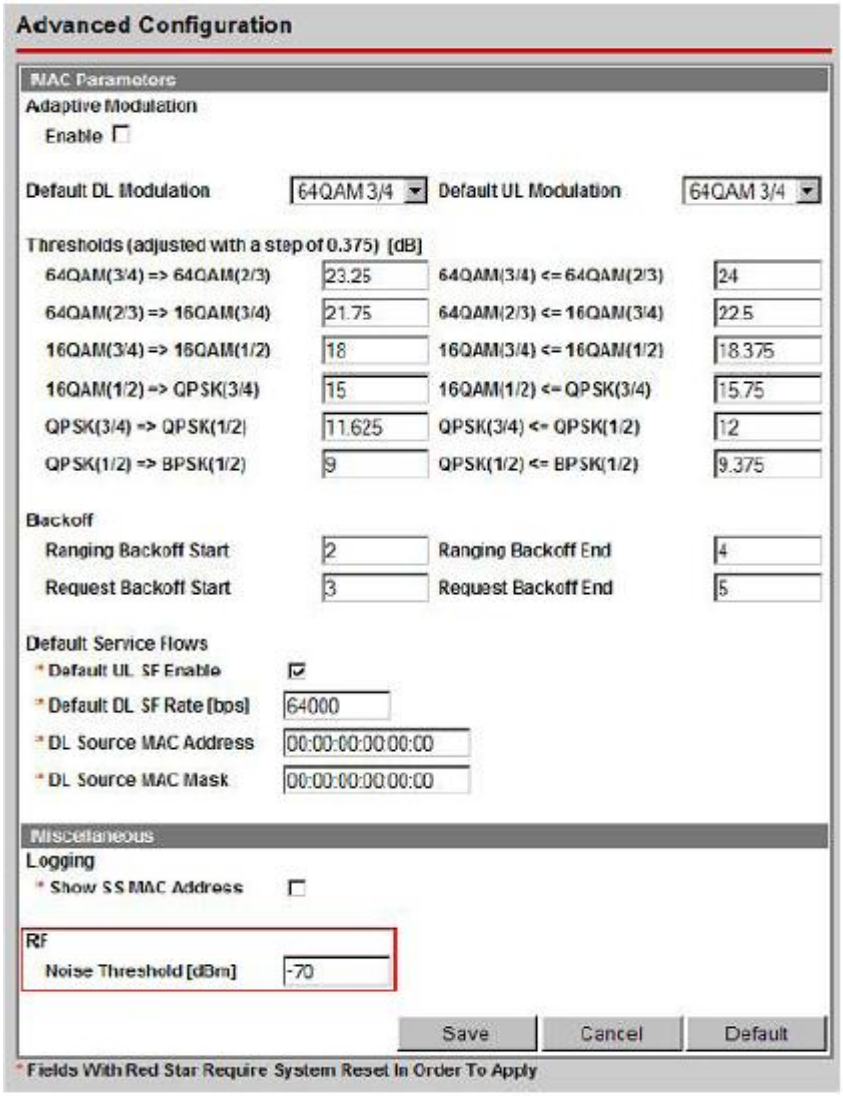


Figura 19 Menú de configuración avanzada [7]

3.2 Estaciones Suscriptoras

Redline fabrica dos tipos de sistemas estaciones suscriptoras, una para uso en el interior de las construcciones (SUI) y otra para su uso fuera de ellas (SUO).

3.2.1 SUI

La antena, el modem y el equipo encargado de procesar las tramas entre la interfaz aérea y el puerto *Ethernet* se encuentran integrados en una sola pieza. Esta se alimenta según [10] mediante un transformador CA-CD a 5 [V]. La antena es sectorial de 80 grados, tiene 10.5

dBi de ganancia, opera de 3.3 a 3.8 GHz y tiene polarización horizontal y vertical. Físicamente el SUI es como se muestra en la siguiente figura:

Figura 17 SUI [10]

3.2.2 SUO

La unidad SUO aparenta ser solamente una antena; Sin embargo también posee la unidad de procesamiento integrada. Está diseñada según [10], para operar a la intemperie por lo que se alimenta por el puerto *Ethernet* a través de PoE (Power over *Ethernet*). Su antena es más robusta siendo de 13.5 grados con una ganancia de 20 dBi, también cuenta con polarización horizontal y vertical.

3.2.3 Administración del equipo:

Los flujos de datos admitidos en el radioenlace así como sus características se configuran automáticamente en las estaciones suscriptoras mediante la descarga de los clasificadores. Siendo así lo único que debe configurarse es la interfaz aérea, y la dirección IP. Opcionalmente pueden activarse el control automático de potencia y el control automático de ganancia.

Establecer la interfaz aérea consta de elegir los valores límites del barrido de frecuencia que realiza el suscriptor para encontrar la banda en la que opera la BS. También se selecciona el ancho de banda del canal (que debe coincidir con el seleccionado en la BS) y la selección de la longitud del prefijo cíclico.

El direccionamiento IP consta de establecer la dirección IP y la máscara de default. Habilitar o deshabilitar la casilla de ethTag para el envío de tramas basadas en VLAN y habilitar o deshabilitar la casilla SSmanaged para la administración del direccionamiento vía IP.

Las unidades suscriptoras tienen la desventaja de no tener interfaz gráfica, deben administrarse vía telnet, el cual es un servicio que de acceso a una línea de comandos para configurar la unidad.

Se accede al servicio de telnet, cómo se describe en [10] conectando el SUI o SUO a una computadora como en el caso de la BS, luego en la computadora se abre una línea de comandos y se ingresa:

>telnet 192.168.101.1

La dirección IP está fijada en el equipo y es una medida de seguridad por sí se olvidara la IP asignada por el administrador.

Habiendo ingresado al sistema hay una interfaz global desde la cual se puede acceder a todos los parámetros. En este caso empezamos por modificar los referentes a la interfaz aérea para ello se ingresa a la carpeta respectiva:

>rfConfig

Dentro de la carpeta se encuentran las variables que definen los límites inferior y superior del barrido en frecuencia, se asignan los valores deseados mediante los comandos:

>set LoRfFreq1 límite_inferior_Hz
>set HiRfFreq1 límite_superior_Hz
Se sale de la carpeta con el comando:

>exit

Luego se ingresa a la carpeta de la capa física, se asigna el valor del ancho de banda y la duración del prefijo cíclico:

>phyConfig
>set cyclicPrefix a
>set bandWith b
>exit

La variable a puede valer 1/4, 1/8, o 1/16, mientras que b puede ser 3500 ó 7000.

Para activar el control automático de ganancia se vuelve a ingresar la carpeta de lainterfaz aérea y se habilita la etiqueta respectiva:

>rfConfig

>set RxAgc 1

Para configurar los parámetros IP se ingresa a la interfaz global, y se asignan los valores de la dirección y la máscara:

>set ipAddress Address a.b.c.d
>set ipAddress Mask e.f.g.h

Finalmente debe desactivarse la administración de tramas VLAN y el dhcp, dichas etiquetas se desactivan desde el modo de configuración global:

>set managedSS 0
>set ethTag 0

3.4 *Switch* CISCO serie Catalyst 2960

Los *switches* son dispositivos que interconectan equipos de manera local (capa dos). Estos se componen de múltiples interfaces ó puertos operando bajo el protocolo 802.3 u 802.1Q, es decir por *Ethernet* o formando enlaces troncales.

La lógica interna, como indica [17], de estos dispositivos permite que analicen las direcciones origen y destino de las tramas recibidas. Estos forman una tabla en memoria (tabla de direcciones MAC) relacionando la dirección origen de la trama al puerto por la que se escucha. La conmutación de paquetes se realiza comparando la dirección destino con la tabla y renviando la trama al puerto correspondiente. La velocidad de renvío depende del equipo, para el modelo empleado es de 32 Gbps.

3.4.3 Teoría de las funciones empleadas en el *switch*

VLAN significa VLAN Virtual, estas son subconjuntos de la conexión LAN provista por el *switch*. En otras palabras forman grupos de puertos existiendo conectividad sólo entre miembros del mismo grupo.

Las razones por las que se implementan, descritas en [17] son seguridad y administración de tráfico. La primera puesto que reduce la cantidad de dispositivos que pueden conectarse entre sí, la segunda porque pueden crearse grupos de usuarios que emplean un servicio en particular (por ejemplo voz, video o datos) y aislar el tráfico de dicho servicio.

Respecto a los puertos cabe recordar que estos pueden operar transportando una VLAN (modo de acceso) o un conjunto de estas (modo troncal).

El *switch* empleado, cómo menciona [12], admite cuatro tipos de VLAN estos son:

1. VLAN de datos: Se emplean para el transporte de datos cómo puede ser un pagína web, una descarga por ftp, etc. Deben ser creadas de manera manual en el equipo y asignárseles también de manera manual los puertos que le pertenezcan.

2. VLAN nativa: Se describió anteriormente pero no se nombró como tal. Como se mencionó el estándar IEEE 802.1Q especifica el uso de una VLAN sin etiqueta para brindar compatibilidad con equipos que no soporten dicho protocolo, esta es dicha VLAN.

3. VLAN de administración: Es una herramienta para la gestión remota del equipo. Existe una interface virtual denominada “Interface VLAN” a la cual se le asigna una dirección IP, esta en conjunto con la asignación de un *gateway* permite que el equipo pueda comunicarse a través de capa tres. A su vez pueden activarse servicios de capa de aplicación en el equipo para acceder al modo de consola.

4. VLAN de voz: Esta opera bajo un puerto en estado troncal. Los teléfonos IP utilizados cuentan con un *switch* interno integrado, este y el *switch* al que se conectan forman un enlace troncal y permiten el paso de esta VLAN y una de datos. Haciendo esto la etiqueta insertada permite priorizar los datos que viajan sobre la VLAN de voz del resto.

3.4.5 Configuración de las funciones empleadas en el *switch*

En general el equipo CISCO, explicado en [17], se opera desde una aplicación denominada CLI (Command Line Interface). Dicha aplicación cuenta con tres modos de operación, estos pueden definirse como cuentas de usuario con permisos para realizar desde funciones de monitoreo hasta configuración en el CLI, estos son:

Exec: Nivel más bajo, prácticamente sólo tiene acceso al monitoreo de interfaces.

Exec Privilegiado: Puede considerarse el nivel intermedio, sigue teniendo sólo la capacidad de monitoreo pero puede acceder a tablas, por ejemplo de direcciones MAC, y en el caso de un *router* a la tabla de enrutamiento.

Configuración: Es el nivel más alto, desde aquí puede configurarse el comportamiento del equipo, cuenta con subdivisiones en función del objeto a configurar por ejemplo: configuración de línea para las interfaces, o configuración de enrutamiento en *routers*.

Los siguiente comandos se emplean desde el modo de configuración global, para crear una VLAN:

#vlan n
#name NOMBRE

El valor “n” es asignado por el administrador y puede tener el valor de 1 hasta 4096. NOMBRE hace referencia la nombre que le asignará el administrador a dicha VLAN

Configuración de puertos, existen dos maneras de configurar el puerto: modo acceso y modo troncal, estas se realizan desde el modo de configuración de línea en la interfaz correspondiente, en seguida se detallan dichas configuraciones:

Modo acceso:

#switchport mode acces
#switchport acces vlan n

El primer comando coloca al puerto en modo de acceso y el segundo lo asigna a la VLAN “n” (la VLAN 1 es creado por defecto y todos los puertos están asignados a ella).

Modo troncal:

#switchport trunk encapsulation dot1q
#switchport mode trunk
#switchport trunk native vlan n

El primer comando es opcional, sirve en equipos que admitan más de un protocolo para formar el troncal, en este caso se elige el estándar 802.1q como base del enlace troncal, el segundo controla la operación de DTP para que forcé el establecimiento de un troncal y el tercero asigna la vlan “n” a la VLAN nativa.

Conexión al teléfono de VoIP:

Como se mencionó el teléfono IP y el *switch* forman un enlace troncal, desde el *switch* se configura la forma en que se administra dicho troncal. Además de esto para activar el manejo de QoS en el *switch*, indicarle cuál será la marca en los paquetes y en que interfaces debe obedecer la marca de los paquetes de entrada. Se ingresa por el CLI, como describe [12], desde el modo de configuración de línea la siguiente secuencia de comandos:

```
mls qos cos 5
mls qos trust device cisco-phone
mls qos trust cos
```

El primer comando marca los bits de CoS (prioridad de VLAN), con el valor de 5, el segundo y tercero indican confiar en la marca CoS si es un teléfono de CISCO el dispositivo conectado a esa interfaz. El enlace troncal se crea mediante DTP entre el *switch* del teléfono y el *switch* de la red.

3.5 *Router* CISCO modelo 2811

El *router* conecta grupos de redes basado en el direccionamiento IP. La comunicación en capa dos (LAN) tiene la característica que todas las computadoras tienen la misma dirección de red. Se emplea el *router* para conectar computadoras pertenecientes a redes distintas, visto de otro modo para conectar LANs.

De manera análoga al *switch*, el *router* emplea una tabla para la decisión de renvío de paquetes denominada en [18] como tabla de enrutamiento. La tabla contiene una combinación de direcciones de red y direcciones IP o interfaces de siguiente salto. La dirección de red indica la subred asociada a una determinada LAN y la dirección IP o interfaz de salida indica a que equipo o por cual interfaz enviar el paquete para alcanzar la subred, esto se denomina ruta.

El *router* modelo CISCO 2811 se clasifica cómo un ISR, esto quiere decir que ofrece servicios extras al enrutamiento. Dichos servicios se refieren principalmente a prestaciones de seguridad y manejo de calidad de servicio.

3.5.3 Teoría de la funciones empleadas en el *router*

Asignación de direccionamiento:

Para establecer comunicación hacia la LAN es necesario asignar una dirección IP de su respectiva subred. Cada interfaz del *router* debe tener asignada una dirección IP y todas deben pertenecer a subredes distintas, de no ser así el *router* simplemente manda un mensaje de error y rechaza el comando.

Rutas estáticas:

Las rutas pueden aprenderse mediante protocolos de ruteo o declarándose directamente en el equipo (rutas estáticas), puesto que la arquitectura de red es pequeña empleamos este último método.

La ruta estática se define indicando la dirección de red destino, la máscara de red y la interfaz o dirección IP de siguiente salto, el comando y la sintaxis se definen más adelante.

Subinterfaces:

Los *routers* en general tienen uno o dos puertos *Ethernet* por lo que llega a haber problemas al momento de interconectarlo hacia la LAN (*switch*).

Cabe mencionar que cada VLAN pertenece a una subred diferente, así que para existir conectividad entre nodos conectados a diferentes VLAN estas deben conectarse a través de un *router*. Si se conectaran a puertos del *switch* en modo de acceso simplemente no sería escalable puesto que se requeriría un puerto *Ethernet* en el *router* por cada VLAN.

Para solventar este problema el *router* cuenta con la capacidad de emplear subinterfaces, estas son divisiones lógicas de la interfaz física, y se comunican hacia el *switch* a través de un enlace troncal.

Las subinterfaces requieren que se les configure una dirección IP, y un valor que indique que VLAN están recibiendo.

ACLs:

Las ACL son un mecanismo de selección de paquetes basada en las direcciones IP de origen y destino de los paquetes que ingresan al *router*. En base a las necesidades de la configuración pueden emplearse para bloquear o permitir tráfico, actualizaciones de protocolos de enrutamiento, selección de paquetes para su renvío y selección de paquetes para determinadas políticas de QoS.

Pueden clasificarse según la información que analizan en estándar y extendidas. Las ACL estándar seleccionan tráfico exclusivamente en función de su dirección IP de origen, mientras que las extendidas pueden hacerlo también por la dirección de destino e incluso por el puerto. Además pueden clasificarse según la forma en que son invocadas en numeradas y extendidas no habiendo mayor diferencia que el empleo de un número o una palabra para emplearlas. Esta tesis comprende únicamente el uso de ACLs numeradas extendidas, la sintaxis y configuración de estas se detallan a continuación.

3.5.5 Configuración de las funciones empleadas en el *router*

Asignación de direccionamiento:

Desde el modo de configuración de interfaz se asigna una dirección IP y se indica su máscara de red:

Router(config-if)#ip address A.B.C.D M.A.S.K
A.B.C.D es una dirección IP válida.
M.A.S.K la máscara asociada a la subred.

Rutas estáticas:

Desde el modo de configuración global se indica la dirección de red remota, su máscara, la dirección de siguiente salto o interface de salida.

Router(config)#ip route A.B.C.D M.A.S.K {dirIP | TipoModNum }
A.B.C.D es una dirección IP válida.
M.A.S.K la máscara asociada a la subred.
dirIP es la dirección IP de siguiente salto y TipoModNum es una abreviación con la que se representa una interface por ejemplo: Gi1/0 (interfaz, modulo, número). La sintaxis indica que es obligatorio el uso de una de ellas.

Subinterfaces:

La subinterfaz se configura accediendo al modo de configuración de línea agregando ".N" al final del número de interfaz, es decir:

Router(config)#interface fa0/0.100
Router(config-if)#ip address A.B.C.D M.A.S.K
Router(config-if)#encapsulation dot1q M

Cómo se mencionó antes la subinterfaz necesita que le sea configurada una dirección IP y el ID de la VLAN de debe recibir (M).

ACLs:

Las ACL se crean desde el modo de configuración global con la siguiente sintaxis:

Router(config)#ip acces-list M permit ip A.B.C.D W.C.M.O E.F.G.H W.C.M.D
A.B.C.D: dirección IP o dirección de red origen.
W.C.M.O: Wild Card Mask de origen.
E.F.G.H: dirección IP o dirección de red destino.
W.C.M.D: Wild Card Mask de destino.

Una wild card mask es una herramienta parecida a la máscara de subred. Esta opera sobre la dirección de red que le antecede, representa con ceros los bits que deben coincidir y con unos aquellos que puedan ser distintos.

QoS:

Para definir la calidad de servicio, como se describe en [13], en el *router* se cuenta con dos entidades denominadas: class-map y policy-map. El modo de emplearlas es el siguiente:

Class-map es la encargada de seleccionar el tráfico, puede hacerlo mediante el comando match que le indica que condición cumple el tráfico que quiere aislar. Puede emplearse más de una sentencia de condición y manipularse la lógica para que acepté el tráfico con que se cumpla una condición o deban cumplirse todas, la sintaxis es la siguiente:

```
class-map NOMBRE_DE_CLASE match {any|all}
match CONDICION1 VALOR
match CONDICION2 VALOR
```

De no especificarse la opción *any* deben coincidir todos los valores descritos por los *match*, el tráfico que no coincida no es descartado, es enviado a la clase default que no coloca ninguna marca sobre el tráfico.

El segundo paso es asignar un valor a las etiquetas, esto se hace mediante la entidad policy-map y el comando set que etiqueta el tráfico aislado por la class-map, además pueden especificarse atributos cómo un ancho de banda mínimo reservado o un descarte preferencial en cola, la sintaxis es:

```
policy-map NOMBRE_DE_POLITICA
class NOMBRE_DE_CLASE
set ip dscp VALOR
ATRIBUTO1 VALOR
ATRIBUTO2 VALOR
```

El último paso es asignar la política a la interfaz que apunta hacia el enlace, esto se hace en modo de configuración de línea con el comando:

```
service-policy output NOMBRE_DE_POLITICA
```

CAPITULO IV

QoS y Aplicaciones de red

Una red basada en la conmutación de paquetes sufre de fenómenos particulares que dificultan el traslado de los paquetes. Las causas de dichos fenómenos se deben principalmente a la congestión de la red, es decir a transmitir datos a una velocidad mayor a la que el canal es capaz de transmitir.

Al emplear servicios de voz, video y datos se espera que la infraestructura de la red llegué a su límite y con ello se degrada la calidad de los servicios. Los fenómenos antes mencionados así como su afectación a los servicios se exponen en este capítulo. Posteriormente se ejemplifica cómo la QoS de CISCO mitiga estos sucesos.

Se explica la configuración de los servicios de video *streaming* y transferencia de datos (FTP).

El “Gateway de voz” representa un caso particular puesto que es un *switch* pero además posee un servidor integrado que regula la comunicación entre los teléfonos IP. Considerando estos últimos cómo el servicio decidimos incluir el “Gateway de voz” en este capítulo.

4.1 Tipos de tráfico y vulnerabilidades

Una red convergente es aquella que transporta flujos de voz, video y datos. El flujo de datos es aquel transportado mediante TCP y es robusto a congestiones en el enlace; Sin embargo los flujos de voz y de video en tiempo real no lo son.

Un enlace saturado intenta transmitir a una tasa de transmisión mayor a la velocidad del enlace. Cuando esto ocurre, describe [12], aparecen los siguientes fenómenos:

1. Pérdida de paquetes: El equipo de red tiene una capacidad finita para el procesamiento y renvío de paquetes que cuando es rebasada por el tráfico ignora el excedente, los paquetes que conforman el tráfico excedente son eliminados y se dice que el equipo ha tirado esos paquetes.

Cuando el tráfico viaja a través de TCP este puede solicitar retransmisiones y reordenar los paquetes recibidos; Sin embargo reduce la ventana con ello reduciendo la velocidad de la transmisión. UDP por el contrario no se percata de dicho suceso y continúa enviado su tráfico sin importar si el tráfico sigue siendo útil o no. Más adelante, durante la descripción de los resultados se aprecia cómo las aplicaciones que emplean UDP acaparan el canal llegando a bloquear por completo al tráfico TCP.

2. Retardo: El retardo de los paquetes puede clasificarse por dos causas. El retardo introducido por el equipo de red y el retardo debido a la propagación en el medio.

El retardo debido a la propagación es el tiempo que tarda la señal en desplazarse por el medio de transmisión, la única manera de controlar este retardo sin cambiar de medio es alinear transmisor y receptor de modo que la distancia entre estos sea mínima. El retardo debido al equipo de red se subdivide en retraso por procesamiento y el retraso de espera en cola.

El equipo de red tiene colas o filas de entrada y de salida, estas son pequeños bloques de memoria en los que se colocan los paquetes en espera de ser procesados. El retardo en cola es el tiempo que permanecen en espera de ser procesados o renviados, El retraso en cola de salida puede controlarse mediante la configuración del equipo.

El retardo de procesamiento es el tiempo que le toma al equipo tomar el paquete que estaba en cola, analizarlo, decidir por donde renviarlo, y ejecutar dicha decisión, el retraso debido al procesamiento se mitiga adquiriendo equipo de mayor capacidad.

El tráfico de datos no es sensible al retardo, los datos son utilizados cuando se descarga el archivo por completo. Las aplicaciones en tiempo real operan con "trozos" del flujo, se apoyan

de una entidad finita de memoria denominada buffer, este extrae la información contenida en los "trozos" del flujo y la facilita a la aplicación. La dimensión del buffer es pequeña puesto que conforme se extrae la información esta es utilizada por la aplicación y ya no se requiere más de ella.

Debido al retardo el buffer se vacía completamente y los servicios de VoIP y video en tiempo real sufren de pausas en el servicio, en telefonía da la sensación que se "corta" la llamada y en el video la imagen se queda congelada.

Puede pensarse que una solución es aumentar el tamaño del buffer pero esto ocasiona dificultades al conversar ya que las personas perciben silencio e intentan hablar siendo que el otro usuario se encuentra hablando. El retardo máximo aceptable en la transmisión de voz es de 200 [ms].

El video puede ser generado en tiempo real o tenerse almacenado. Cuando este se encuentra almacenado puede aumentarse el buffer incluso hasta un tamaño igual al del archivo y transportarse mediante TCP; Sin embargo cuando este es generado en tiempo real no hay tiempo para reordenar paquetes o solicitar retransmisiones así que el tamaño del buffer se mantiene la mínimo posible, la ausencia de paquetes genera pausas y saltos en el video, y los paquetes que llegan tarde se descartan.

3. Jitter: los paquetes transmitidos a una velocidad de transmisión constante no necesariamente se trasladan con el mismo retraso. La diferencia de tiempo entre la llegada de paquetes recibe el nombre de jitter.

La voz y el vídeo en tiempo real sufren de distorsión cuando se presenta el fenómeno de Jitter, este se debe principalmente al tiempo de espera en la cola de salida. Reduciendo el retardo en cola de salida se reduce el jitter y si es lo suficientemente pequeño el buffer puede mitigar sus efectos.

4.2 Definición de Calidad de servicio (QoS) en redes.

Calidad de servicio en redes (QoS por sus siglas en inglés) es el proceso de separar y tratar de manera especializada el tráfico generado por aplicaciones en particular.

Para clasificar el tráfico en una red de computadoras se emplean campos específicos de los PDU, de los segmentos se emplea el puerto, de el paquete IP las direcciones de origen, destino, de la trama del 802.1Q se usan las direcciones MAC origen y destino así como el identificador de VLAN.

4.3 Modelos de QoS

El modelo de QoS se refiere a la manera de asignar recursos por parte del equipo de red, de [12], estos se clasifican en:

Modelo Best-Effort

Este hace referencia a sistemas sin ninguna calidad de servicio configurada. “Best-Effort” significa mejor esfuerzo, quiere decir que el equipo renvía los paquetes haciendo su “mejor esfuerzo” pero no garantiza la entrega. Todos los paquetes son tratados por igual.

Modelo de servicios integrados

El funcionamiento de este modelo crea un canal fijo con prestaciones determinadas, los equipos de red se encargan de negociar y crear el canal, en caso de no poder cumplir las condiciones el canal no es creado.

Un ejemplo es el protocolo RSVP (RFC 2205) para la señalización. Este protocolo envía mensajes a los equipos intermediarios informando y exigiendo los recursos necesarios para establecer el enlace.

Al comienzo de esta tésis se explico que el objetivo de la comunicación IP es tener caminos redundantes hacia el mismo destino, como puede observarse este modelo nos obliga a emplear canales únicos y prestablecidos siendo poco escalable.

El enlace entre la BS y la SS puede considerarse de este tipo, la BS tiene una base de datos de los flujos que debe crear, y esta ordena a los SS que manejen los flujos en base a esas especificaciones.

Modelo de servicios diferenciados

Este modelo busca que cada equipo determine localmente la manera en que debe ser tratado el tráfico.

Para obtener dicho comportamiento es necesario que el tráfico lleve información acerca de la QoS que requiere, esta información se coloca en el campo denominado ToS/DSCP del paquete IP, la trama *Ethernet* representa un caso particular puesto que no tiene un campo para proporcionar este servicio, por ello (cómo se mencionó antes) se emplea un enlace troncal basado en IEEE 802.1Q, este añade 3 bits para priorizar el tráfico.

El paquete IP cuenta con el campo ToS o DSCP, cada uno representa un formato para expresar el valor de preferencia del paquete. ToS resultó poco flexible así que actualmente el marcado se realiza con el formato DSCP.

Con este formato, los *routers* en los extremos del enlace se encargan de asignar el valor de QoS al paquete IP. Como se dijo, ocupa el lugar del byte ToS y su formato es el siguiente:

DS5	DS4	DS3	DS2	DS1	DS0	ECN	ECN

Figura 21 Byte ToS, bits DSCP

Los bits empleados para el control del QoS son los DS5 a DS0, la prioridad de envío esta dada por los bits DS5 a DS3, estos toman valores de 0 a 7 siendo este último la mayor prioridad. Los bits DS2 a DS0 indican la posibilidad de descarte siendo 1 el menor valor y 3 el mayor.

Los niveles de prioridad reciben nombres en específico, estos se muestran en la siguiente tabla:

111110	**Reservado (routing y contol)**	**011110**	**Assured Clase 3 Preced. Alta**
111100	Reservado (routing y contol)	011100	Assured Clase 3 Preced. Media
111010	Reservado (routing y contol)	011010	Assured Clase 3 Preced. Baja
111000	Reservado (routing y contol)	011000	Configurable por el usuario
110110	Reservado (routing y contol)	010110	Assured Clase 2 Preced. Alta
110100	Reservado (routing y contol)	010100	Assured Clase 2 Preced. Media
110010	Reservado (routing y contol)	010010	Assured Clase 2 Preced. Baja
110000	Reservado (routing y contol)	010000	Configurable por el usuario
101110	Expedited (Premium)	001110	Assured Clase 1 Preced. Alta
101100	Configurable por el usuario	001100	Assured Clase 1 Preced. Media
101010	Configurable por el usuario	001010	Assured Clase 1 Preced. Baja
101000	Configurable por el usuario	001000	Configurable por el usuario
100110	Assured Clase 4 Preced. Alta	000110	Configurable por el usuario
100100	Assured Clase 4 Preced. Media	000100	Configurable por el usuario
100010	Assured Clase 4 Preced. Baja	000010	Configurable por el usuario
100000	Configurable por el usuario	000000	Besr Effort (Default)

Tabla 3 Valores estandarizados para DSCP [13]

Valores CoS 802.1Q

Se mencionó antes que al crear un enlace troncal se añaden 3 bits para asignar el QoS, los valores van de 0 a 7, siendo 0 el menor valor, 7 el mayor y 5 lo común para voz.

Los encargados de colocar la marca pueden ser la terminal (teléfono o computadora) siendo este último quien controla esto.

4.4 TelefoníaVoIP

4.4.1 Configuración del Gatekeeper SPA9000

El gatekeeper provee señalización, controla y enruta las llamadas por medio del protocolo SIP, lo que hace más eficiente el tránsito de tráfico de voz, ya que existe una ruta para éste y otra para la señalización.

Para poder acceder a la configuración, se conectó un cable *Ethernet* al puerto *Ethernet* WAN del SPA9000, conectando el otro extremo al puerto *Ethernet* de una computadora. La dirección IP por default del SPA9000 es 192.168.0.1 con máscara de red de 24 bits.

En el navegador web se escribe lo siguiente: 192.168.0.1/admin/voice/advancek, antes de ingresar la dirección, previamente se tiene que configurar una dirección IP en la computadora que será utilizada para administrar el SPA9000, esta dirección tiene que estar en el mismo segmento, es decir, cualquier dirección de 192.168.0.1 a 192.168.0.254, esto con el objeto de que la computadora y el SPA9000 se encuentren en la misma red local.

Una vez que ingresamos al SPA9000 por medio de la Web, saldrá la siguiente pantalla:

Figura 22 Pantalla inicial del SPA900

En la pestaña *Router*, seleccionamos Wan Setup y en esta se configura la IP y el Gateway, los cuales son 192.168.20.100 y 192.168.20.254 respectivamente. La dirección

192.168.20.100 se configuró por el diseño de la red, puesto que este Gateway de Voz esta en el *Switch* del Subscriptor en la VLAN 20.

Figura 23 Configuración de la dirección WAN

4.4.2 Configuración de los temporizadores

Para configurar los temporizadores utilizados por el protocolo SIP, se muestran en la siguiente tabla. Estos se encuentran estipulados y descritos en la RFC 3261.

T1	0.5 s	Cálculo de RTT (Round-trip Time)
T2	4 s	Intervalo máximo de retransmisión para peticiones no INVITE y para respuestas INVITE
T4	5 s	El período de tiempo máximo que un mensaje puede permanecer en la red
Temporizador B	$64 * T1$	Temporizador de tiempo de espera de transacciones INVITE

Temporizador D	> 32 segundos para UDP 0 segundos para TCP y SCTP	Tiempo de espera para retransmisiones de respuestas
Temporizador F	$64 * T1$	Temporizador de tiempo de espera de transacciones no INVITE
Temporizador H	$64 * T1$	Tiempo de espera para la recepción ACK
Temporizador J	$64 * T1$ para UDP 0 segundos para TCP y SCTP	Tiempo de espera para retransmisiones de peticiones no INVITE

Tabla 4 Valores predeterminados de los temporizadores del protocolo SIP [11].

Nota: INVITE Indica que el usuario o servicio está invitado a participar en una sesión.

4.4.3 Parámetros RTP

RTP transmite paquetes que contienen muestras de voz. Por lo cual es necesario configurar algunos parámetros de este para poder asegurar una buena calidad en las llamadas de voz.

RTP Port Min	16384	Es el número de puerto mínimo para transmisiones y recepciones RTP.
RTP Port Max	16482	Es el número de puerto máximo para transmisiones y recepciones RTP.
RTP Packet Size	0.030	Se refiere al tamaño aproximado del paquete de voz RTP en segundos. Puede ser desde 0.01 a 0.16 s, los valores utilizados sólo pueden ser múltiplos de 0.01. El tamaño que se utilizó fue de 0.030 s, debido a qué es un valor típicamente usado por los códecs que maneja el SPA9000.

Tabla 5 Valores predeterminados de los parámetros RTP [11]

La configuración de estos distintos valores se muestra a continuación.

Figura 24 Configuración de los temporizadores SIP y parámetros RTP

4.4.4 Configuración de los teléfonos IP Linksys

Los teléfonos IP Linksys utilizados son los modelos SPA922 y SPA94. Los teléfonos Linksys se registran automáticamente en el SPA9000, aunque su dirección IP y su extensión se configuran en el teléfono.

La configuración de los teléfonos se realizó a través de Web Browser al igual que el SPA9000.

Para poder acceder via web a la administración de los teléfonos, necesitamos conocer la IP que tiene configurada actualmente el teléfono, para poder verificar dicha dirección IP, realizamos lo siguiente:

1.- El teléfono cuenta con un botón de administración, una vez que accedemos al menu, seleccionamos la opcion de network, la cual muestra distintos parametros, entre los cuales se encuentra, la direccion IP, la mascara de red, el Default Gateway, entre otros parametros.

2.- Una vez que conocemos la direccion IP del telefono, la ingresamos en el navegador web, previamente conectamos mediante un cable *Ethernet* nuestra computadora y el telefono asignando una direccion IP del mismo segmento del telefono a la computadora, con el objeto de que se encuentren en la misma red local y estos puedan tener comunicación.

3.- Una vez dentro de la aplicación, seleccionamos la pestaña System y procedemos a configurar la direccion IP, la mascara de red y el Gateway.

La direccion IP asigana fue: 192.168.2.11 la cual esta en el segmento del *Switch* de la BS en la VLAN 2.

La máscara de red asignada fue de 24 bits, es decir, 255.255.255.0

El Gateway configurado fue el 192.168.2.254

La siguiente figura muestra la configuracion.

Figura 25 Configuración del teléfono IP Linksys

La configuración de los temporizadores SIP y de los parámetros RTP fueron los mismos que se configuraron en el SPA9000.

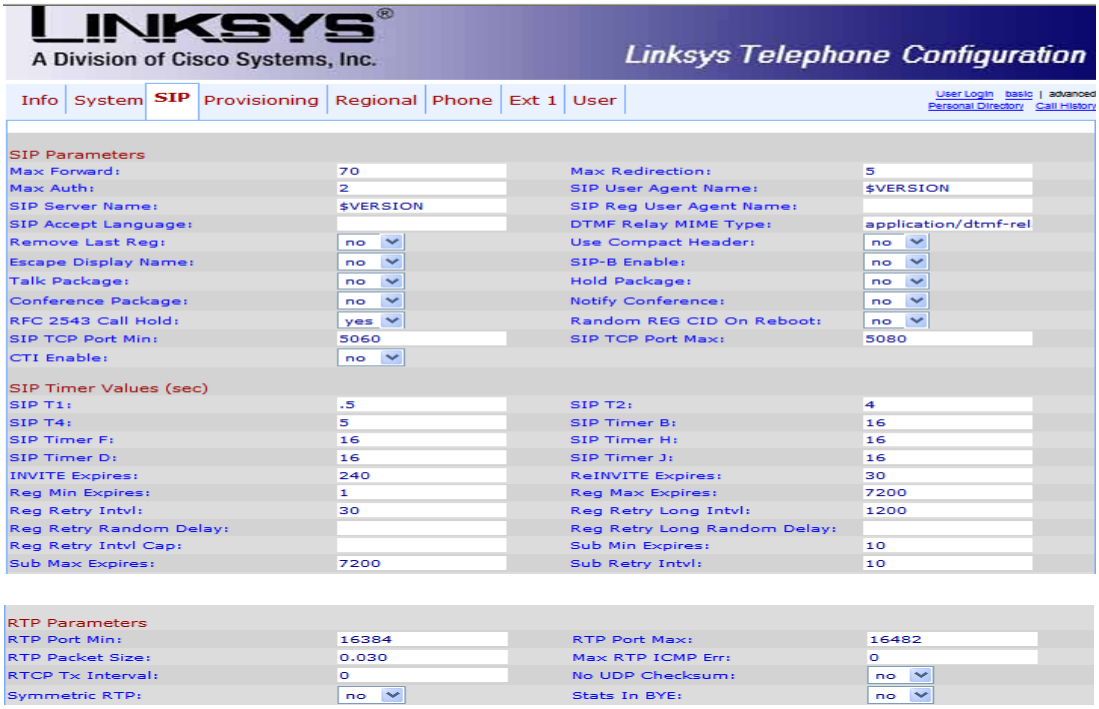


Figura 26 Configuración de los temporizadores SIP y de los parámetros RTP

Para configurar la extensión telefónica así como el nombre, se selecciona la pestaña Phone y la pestaña EXT 1, en estas dos se configuran dichos parámetros.

Figura 27 Configuración del nombre del dispositivo

La siguiente figura, muestra la configuración del número de extensión.

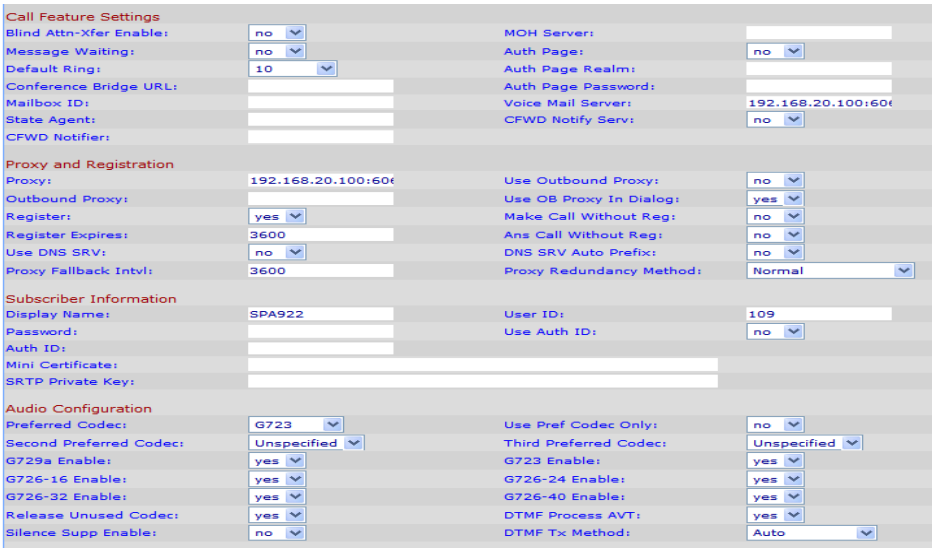


Figura 28 Configuración del número de extensión

La configuración anteriormente mostrada se realizó para el modelo SPA922, la configuración para el modelo SOA941 es la misma.

4.5 VLC Media Player

Para comenzar [8] define este programa como uno de licencia gratuita y código abierto, tiene las capacidades de reproducir contenido multimedia, transcodificar, fungir como servidor de *streaming* a redes tanto locales como remotas a través de varios protocolos cómo FTTP, RTP, UDP y también puede actuar cómo cliente de *streaming*. Además cuenta con el respaldo de una gran comunidad que resulta útil para el uso de las funciones avanzadas.

El proceso para implementar el *streaming* de video a redes remotas requiere que el video sea convertido a un formato que resista la transmisión, este puede realizarse antes de la transmisión o al mismo tiempo. La computadora utilizada para transmitir no soportó la segunda opción por lo que primero convertimos el video en su totalidad a través de la siguiente interfaz gráfica seleccionando medio/convertir:

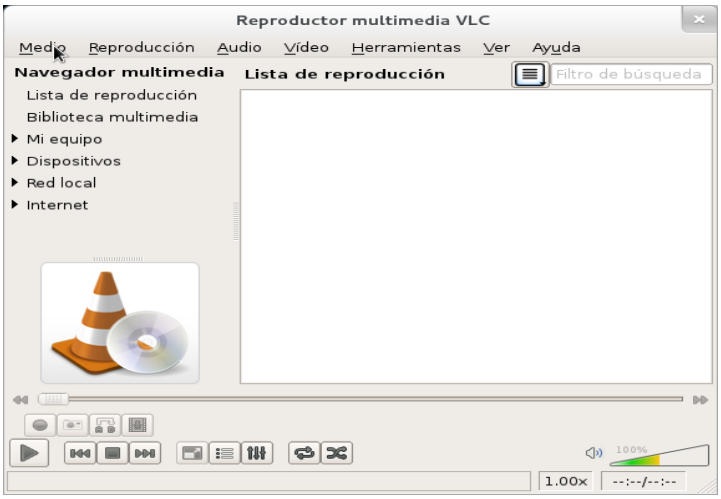


Figura 29 Interfaz gráfica de VLC

Lo anterior abre una ventana para indicar el video origen, el destino y el formato tanto de transcodificación (H264 o MPEG-AVC) cómo el del contenedor (MPEG TS):

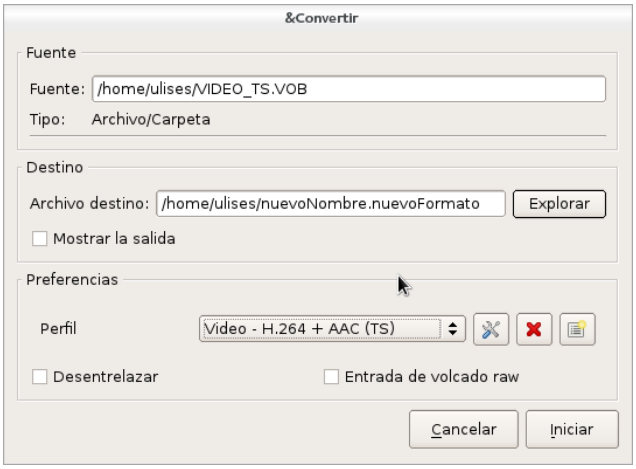


Figura 30 Menú “Convertir”

Para realizar el *streaming* a redes remotas se elige la opción medio/emitir, a lo que el programa desplegará la siguiente ventana:

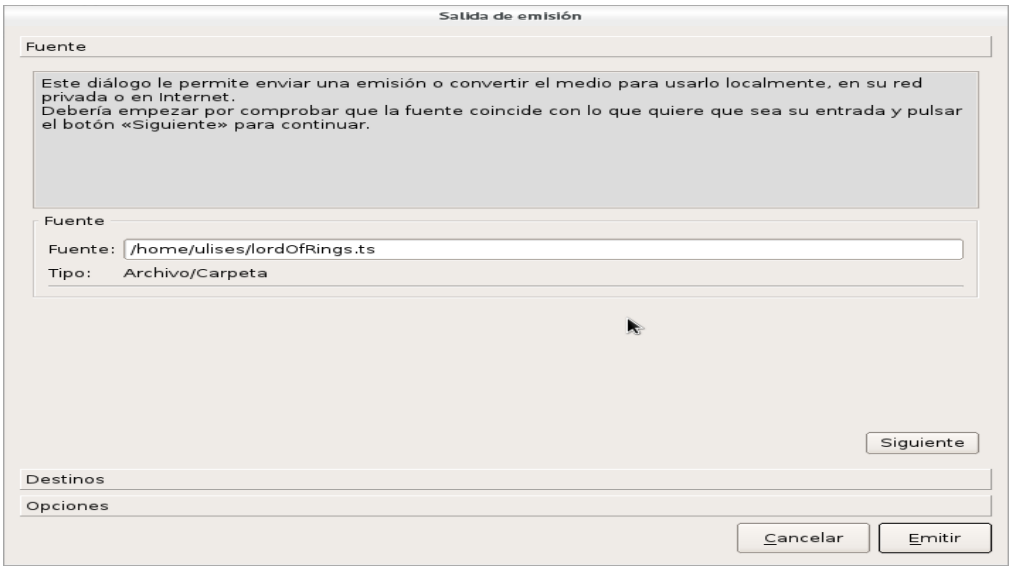


Figura 31 Menú principal de emisión

En dicha ventana se comienza por la selección del video a transmitir, en seguida se elige el protocolo de transporte que en nuestro caso es RTP para MPEG-TS, es importante deshabilitar la transcodificación ya que realizamos esto anteriormente y el video ya se encuentra en el formato deseado.

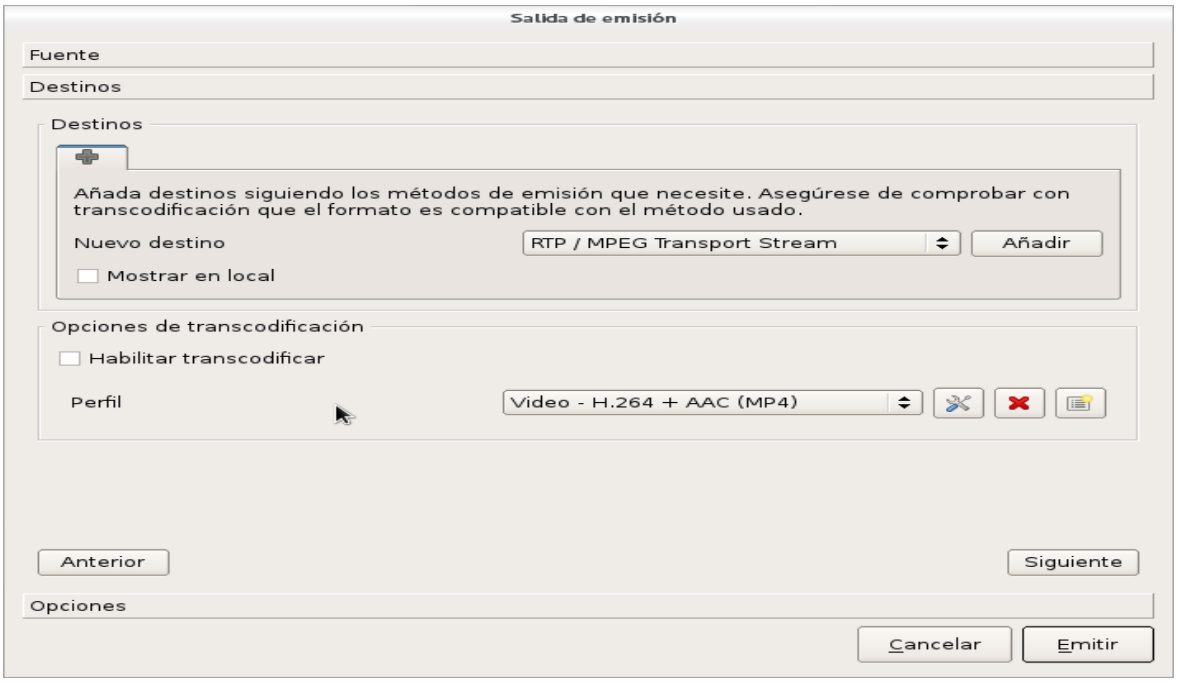


Figura 32 Menú “Protocolo de envío”

La opción mostrar permite observar desde la computadora en modo servidor lo que se está transmitiendo, esto resulta útil para comparar la degradación en la calidad del video.

Al seleccionar el protocolo de transporte se abre una opción para indicar la dirección ip del dispositivo la que será enviada la transmisión:

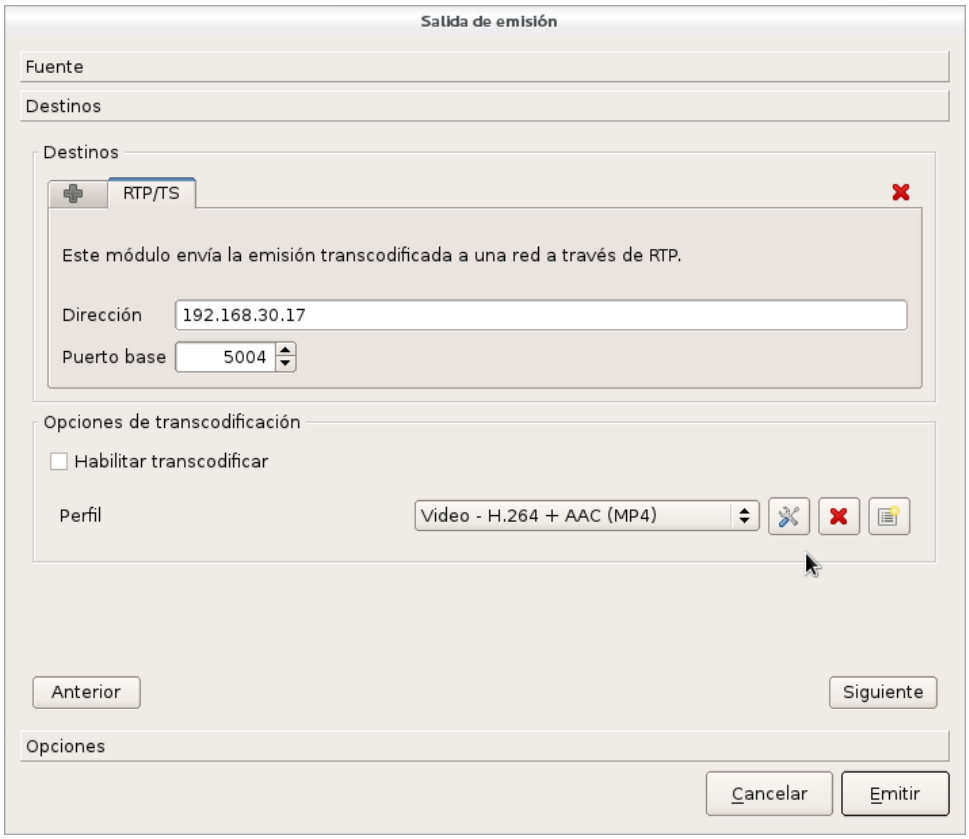


Figura 33 Menú “Destinos”

Finalmente se abre una nueva ventana donde aparece el comando equivalente a lo que se está solicitando hacer a VLC, además aparecen las últimas opciones a activar en la transmisión, de ellas la única relevante es el valor de TTL puesto que por cada *router* que atraviesa el flujo de video el TTL del paquete decrece una unidad y de volverse cero el paquete es descartado.

Cómo en la red ocupamos dos *routers* el TTL debe de establecerse al menos en 3:

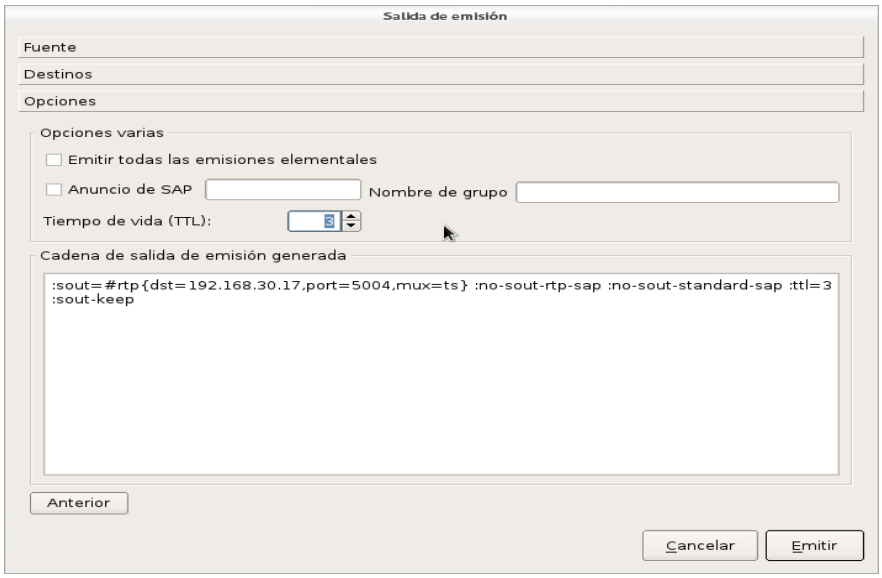


Figura 34 Opciones de red

Para comenzar la reproducción en el lado del cliente también se abre la interfaz gráfica de VLC, se elige la opción medio/Abrir volcado de red lo cual despliega la siguiente ventana, para comenzar a reproducir se indica en la casilla el protocolo de transporte seguido del puerto y finalmente se da *click* en reproducir.

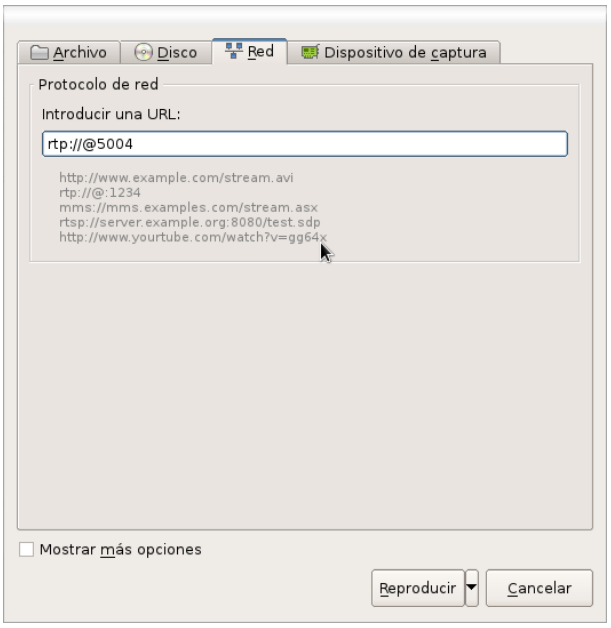


Figura 35 Reproducción de video en el cliente

4.6 VSFTPD

VSFTPD es un servidor de FTP nativo de linux, se configura y opera desde línea de comandos (shell); Sin embargo [14] indica que se encuentra preconfigurado así que para poder utilizarlo sólo hace falta editar los valores de las siguientes variables en el archivo vsftpd.conf, el proceso en general para activar y utilizar el servidor es el siguiente:

Instalar el servidor: Las distribuciones más recientes de linux cuentan con gestores de instalación tanto gráficos cómo desde la línea de comandos, en nuestro caso usamos el sistema operativo fedora 16 por lo que la instalación a través del gestor se ejecutó con el siguiente comando:

```
#yum install -y vsftpd
```

Se edita el archivo vsftpd.conf para permitir la identificación mediante las cuentas de usuario del equipo (servidor) y activamos el usuario anomymus.

```
#vi /etc/vsftpd/vsftpd.conf
listen=YES
anonymus_enable=YES
local_enable=YES
```

Se copian los archivos a descargar mediante el comando:

```
#cp archivo_origen /var/ftp/nombreNuevo
```

Por último se activa el servidor con el comando:

```
#service vsftpd start
```

Desde el equipo del cliente (puede ser cualquier sistema operativo) se ejecutan los siguientes comandos para descargar los archivos:

```
carpeta_actual> ftp ip_servidor
user:
password:
ftp>get nombreArchivo
```

4.7 iPERF

iPERF es una herramienta con la capacidad de inyectar tráfico TCP ó UDP de extremo a extremo de una red y repotar las características de dicho flujo, se emplea mediante linea de comandos y puede especificarse el tipo de tráfico deseado mediante las siguientes banderas:

-s	configura la PC como le servidor de tráfico
-c	configura la PC como el cliente de tráfico
-d	establece el flujo de datos como bidireccional
-l	longitud del buffer de lectura/escritura
-w	tamaño de la ventana TCP
-i	intervalo de tiempo entre reportes
-t	intervalo de tiempo de la simulación total
-P	número de clientes paralelos a simular
-f	formato, reporte en kbps, mbps, Kbps, Mbps

Tabla 14 Banderas del comando iPERF [15]

Hay que destacar, que en [15] se indica que operando bajo la inyección de tráfico tcp iPERF se adapta al canal de tal manera que transmite a la máxima velocidad de transmisión que le permita el enlace.

En sistemas windows no es necesario instalar el programa, sólo se descarga el ejecutable, luego se ingresa al cmd y entra a la dirección de este, finalmente sólo se ingresa el comando requerido.

4.8 nTop

NTOP (Network TOP), de describe en [16] permite monitorizar en tiempo real los usuarios y aplicaciones que están consumiendo recursos de red en un instante concreto. Posee un microservidor web que permite que cualquier usuario, que sepa la clave, pueda ver la salida NTOP de forma remota con cualquier navegador, y además es GNU. El *software* esta desarrollado para platarfomas Unix y Windows.

En Modo Web, actúa como un servidor de Web, volcando en HTML el estado de la red. Viene con un recolector/emisor NetFlow/sFlow, una interfaz de cliente basada en HTTP para crear aplicaciones de monitoreo centradas en top, y RRD para almacenar persistentemente estadísticas de tráfico.

Los protocolos que es capaz de monitorizar son: TCP/UDP/ICMP, (R)ARP, IPX, DLC, Decnet, AppleTalk, Netbios, y ya dentro de TCP/UDP es capaz de agruparlos por FTP, HTTP, DNS, Telnet, SMTP/POP/IMAP, SNMP, NFS, X11.

La instalación en un sistema linux es la siguiente:

1) Se ingresa a una terminal del sistema.

2) Se ejecuta el gestor de paquetes solicitando la instalación de ntop, para fedora es el siguiente comando:

yum install -y ntop

3) se activa el servicio mediante el comando:

ntop -i nombreInterfazMonitoreo

4) Se ingresa al navegador web la dirección 127.0.0.1 y desde allí se pueden ver las estadísticas del tráfico.

CAPITULO V

Estructura de red

En este capítulo se describe cómo fueron realizadas las conexiones físicas y lógicas entres las computadoras clientes y/o servidores y los distintos dispositivos de red. Las conexiones físicas se refieren al cableado entre las distintas interfaces de red y las lógicas a direccionamiento IP implementado.

Además se presentan las configuraciones de equipo en general y de QoS empleadas y cómo fueron usadas para cada caso en particular.

5.1 Estructura

Usamos dos grupos de equipos CISCO interconectados mediante un enlace WiMAX, cada grupo compuesto por un *switch* y un *router*. En el *switch* los puertos se asignan a tres VLAN diferentes para simular redes dedicadas al servicio de voz, video y datos respectivamente.
Se separaron clientes en un extremo del enlace y servidores en otro, se usó una computadora como cliente y una como servidor para realizar las pruebas del servicio de video y de datos, en el caso de telefonía se emplearon teléfonos IP reales y un par de computadoras sólo para poder registrar y comprobar de manera escrita el correcto funcionamientos de dicho canal.
Se reservó un puerto del *switch* para conectarlo hacia el *router*, dicho enlace se empleó cómo troncal y se aprovechó para configurar subinterfaces en el puerto *Ethernet* del *router*.
El otro puerto *Ethernet* del *router* se conectó hacia la BS en el extremo de los servidores y hacia el SUI en el extremo de los clientes.

La siguiente figura es un diagrama de la topología de la red:

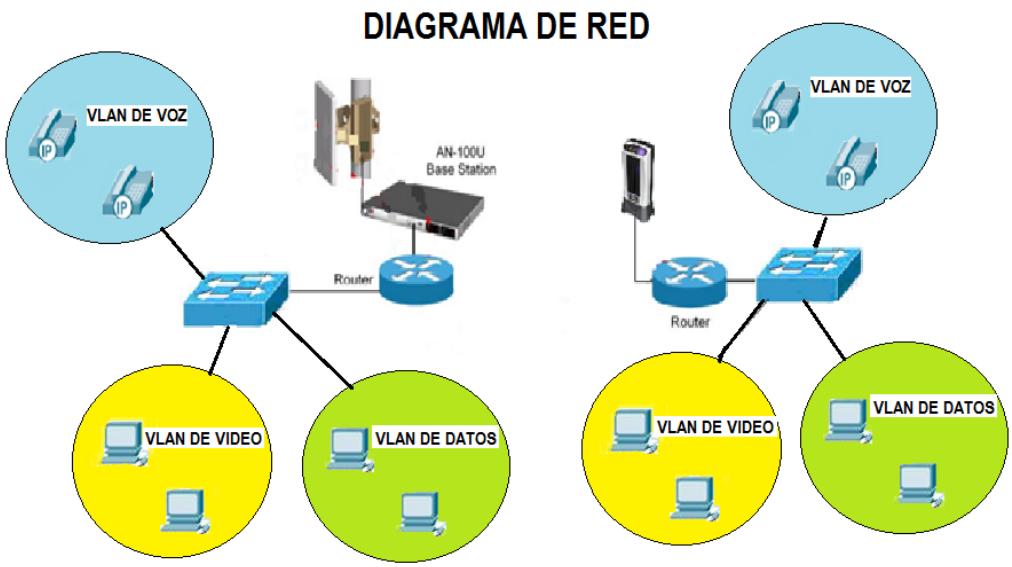


Figura 36 Topología implementada

Y la siguiente tabla describe el direccionamiento IP utilizado:

Dispositivo	Interfaz	IP	Máscara
Teléfono (servidores)	*Ethernet*	192.168.2.11	255.255.255.0
Servidor de video	*Ethernet*	192.168.3.11	255.255.255.0
Servidor de datos	*Ethernet*	192.168.4.11	255.255.255.0
PC (voip)	*Ethernet*	192.168.2.20	255.255.255.0
***Router* (servidores)**	Subinterfaz de voz	192.168.2.254	255.255.255.0
***Router* (servidores)**	Subinterfaz de video	192.168.3.254	255.255.255.0
***Router* (servidores)**	Subinterfaz de datos	192.168.4.254	255.255.255.0
***Router* (servidores)**	*Ethernet* 0/1	192.168.182.37	255.255.255.0
BS	*Ethernet*	192.168.182.3	255.255.255.0
SS	*Ethernet*	192.168.182.40	255.255.255.0
***Router* (clientes)**	*Ethernet* 0/1	192.168.182.111	255.255.255.0
***Router* (clientes)**	Subinterfaz de voz	192.168.20.254	255.255.255.0
***Router* (clientes)**	Subinterfaz de video	192.168.30.254	255.255.255.0
***Router* (clientes)**	Subinterfaz de datos	192.168.40.254	255.255.255.0
Teléfono (clientes)	*Ethernet*	192.168.20.17	255.255.255.0
Cliente de video	*Ethernet*	192.168.30.17	255.255.255.0
Cliente de datos	*Ethernet*	192.168.40.17	255.255.255.0
PC (voip)	*Ethernet*	192.168.20.20	255.255.255.0

Tabla 6 Direccionamiento IP de los dispositivos

5.2 Configuración

La BS cuenta con la opción de deshabilitar flujos de datos sin tener que eliminar los canales, por ello desde un comienzo se crearon todos los flujos a utilizar y estos se activaron o desactivaron en el momento necesario.

Mediante el proceso descrito en el capítulo 3 se configuran los siguientes valores de la interfaz aérea tanto en el suscriptor cómo en la BS:

a) Ancho de banda del canal: 3.5 MHz
b) Frecuencia central de operación: 3478500 Hz
c) Cyclic-Prefix: 1/16

Cómo pasos generales en la BS se desactiva el aprendizaje de MACs para el suscriptor, y en el suscriptor se desactivan los filtrados y el etiquetado de paquetes.

Finalmente se definieron las siguientes clases con sus respectivas características:

Nombre	Tasa reservada	Retardo tolerado	*Schedulling*
VoIP	128 kbps	30 ms	UGS
Datos	100 kbps	NA	BE
DatosFTP	50-100 kbps	NA	nRTPS
***Streaming*Video**	3-3.5 Mbps	50 ms	RTPS
CanalUnico	10 Mbps	NA	BE

Tabla 7 Características de las SC programadas

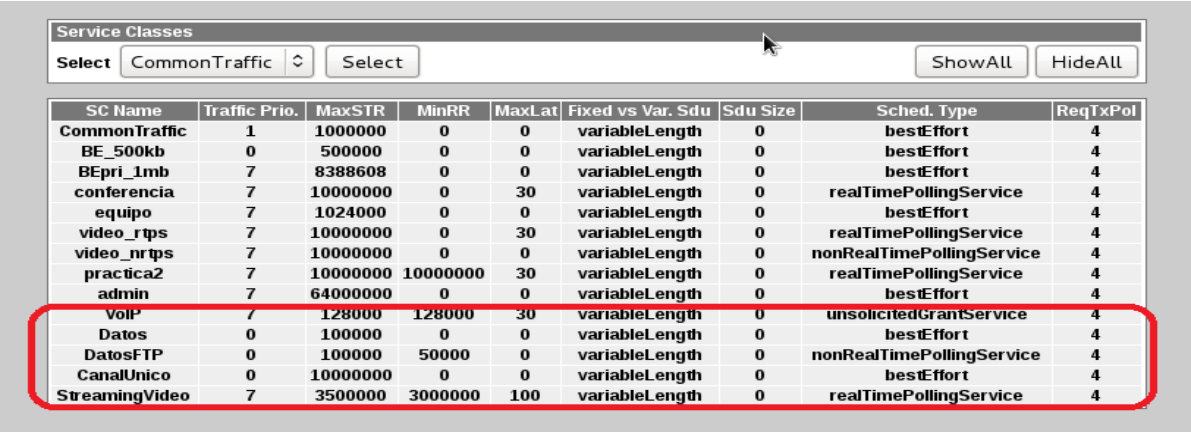
A la voz se le asignó la clase UGS porque esto le garantiza un canal siempre disponible, la desventaja es que esta porción de la tasa de transmisión no está disponible para ningún otro servicio en ningún momento.

Datos es la clase de las peticiones de clientes de video y de datos hacia los servidores, al asignarle la clase BE sí el canal está en desuso puede ser empleado por los otros servicios.

DatosFTP se crea con el tipo nRTPS para que tenga un mínimo de tasa reservado al comenzar la descarga, así el canal aunque se reduzca se mantiene funcionando.

*Streaming*Video opera bajo RTPS, esto asegura que cuando haya transmisión de video ningún otro servicio haga bajar su tasa a menos de 3 Mbps (siendo el promedio para este video de 3.5 Mbps) y sí el canal está en desuso puede ser empleado por otro servicio.

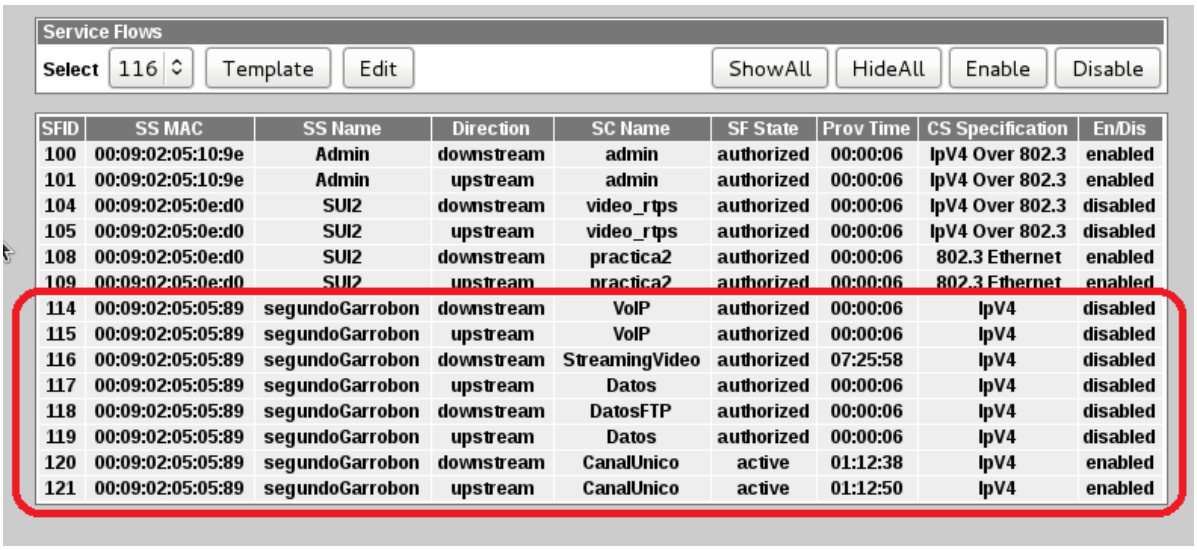
Finalmente CanalUnico se define de 10 Mbps puesto que para el caso en que opera no hay otros flujos activos. La siguiente figura muestra las clases registradas en la BS:



SC Name	Traffic Prio.	MaxSTR	MinRR	MaxLat	Fixed vs Var. Sdu	Sdu Size	Sched. Type	ReqTxPol
CommonTraffic	1	1000000	0	0	variableLength	0	bestEffort	4
BE_500kb	0	500000	0	0	variableLength	0	bestEffort	4
BEpri_1mb	7	8388608	0	0	variableLength	0	bestEffort	4
conferencia	7	10000000	0	30	variableLength	0	realTimePollingService	4
equipo	7	1024000	0	0	variableLength	0	bestEffort	4
video_rtps	7	10000000	0	30	variableLength	0	realTimePollingService	4
video_nrtps	7	10000000	0	0	variableLength	0	nonRealTimePollingService	4
practica2	7	10000000	10000000	30	variableLength	0	realTimePollingService	4
admin	7	64000000	0	0	variableLength	0	bestEffort	4
VoIP	7	128000	128000	30	variableLength	0	unsolicitedGrantService	4
Datos	0	100000	0	0	variableLength	0	bestEffort	4
DatosFTP	0	100000	50000	0	variableLength	0	nonRealTimePollingService	4
CanalUnico	0	10000000	0	0	variableLength	0	bestEffort	4
StreamingVideo	7	3500000	3000000	100	variableLength	0	realTimePollingService	4

Figura 37 SC creadas en la BS

Después de ello se crearon los siguientes SFs:



SFID	SS MAC	SS Name	Direction	SC Name	SF State	Prov Time	CS Specification	En/Dis
100	00:09:02:05:10:9e	Admin	downstream	admin	authorized	00:00:06	IpV4 Over 802.3	enabled
101	00:09:02:05:10:9e	Admin	upstream	admin	authorized	00:00:06	IpV4 Over 802.3	enabled
104	00:09:02:05:0e:d0	SUI2	downstream	video_rtps	authorized	00:00:06	IpV4 Over 802.3	disabled
105	00:09:02:05:0e:d0	SUI2	upstream	video_rtps	authorized	00:00:06	IpV4 Over 802.3	disabled
108	00:09:02:05:0e:d0	SUI2	downstream	practica2	authorized	00:00:06	802.3 Ethernet	enabled
109	00:09:02:05:0e:d0	SUI2	upstream	practica2	authorized	00:00:06	802.3 Ethernet	enabled
114	00:09:02:05:05:89	segundoGarrobon	downstream	VoIP	authorized	00:00:06	IpV4	disabled
115	00:09:02:05:05:89	segundoGarrobon	upstream	VoIP	authorized	00:00:06	IpV4	disabled
116	00:09:02:05:05:89	segundoGarrobon	downstream	StreamingVideo	authorized	07:25:58	IpV4	disabled
117	00:09:02:05:05:89	segundoGarrobon	upstream	Datos	authorized	00:00:06	IpV4	disabled
118	00:09:02:05:05:89	segundoGarrobon	downstream	DatosFTP	authorized	00:00:06	IpV4	disabled
119	00:09:02:05:05:89	segundoGarrobon	upstream	Datos	authorized	00:00:06	IpV4	disabled
120	00:09:02:05:05:89	segundoGarrobon	downstream	CanalUnico	active	01:12:38	IpV4	enabled
121	00:09:02:05:05:89	segundoGarrobon	upstream	CanalUnico	active	01:12:50	IpV4	enabled

Figura 38 SF creados en la BS

Y finalmente los clasificadores:

SFID.ClsID	State	Prio.	Tos Low-High/Mask	Dstlp Addr/Mask	Srclp Addr/Mask	DstPort Start-End	SrcPort Start-End
114.1	inactive	0		192.168.20.0/ 255.255.255.0	192.168.2.0/ 255.255.255.0		
115.1	inactive	0		192.168.2.0/ 255.255.255.0	192.168.20.0/ 255.255.255.0		
116.1	inactive	0		192.168.30.17/ 255.255.255.255	192.168.3.11/ 255.255.255.255		
117.1	inactive	0		192.168.3.11/ 255.255.255.255	192.168.30.17/ 255.255.255.255		
118.1	inactive	0		192.168.40.17/ 255.255.255.255	192.168.4.11/ 255.255.255.255		
119.1	inactive	0		192.168.4.11/ 255.255.255.255	192.168.40.17/ 255.255.255.255		
120.1	active	0					
121.1	active	0					

Figura 39 Clasificadores creados en la BS

5.2.1 Sin QoS

Las configuraciones de equipo CISCO que se mostraran a continuación, son las que se emplearon para todas las pruebas.

5.2.1.1 Configuración del *Router* conectado a la BS

Se configuro la interfaz Fa0/0 con tres subinterfaces, como se muestra a continuación:

A la interfaz fa0/0 se le asocio a una lista de acceso.

```
interface FastEthernet0/0
no ip address
ip access-group 101 in
duplex auto
speed auto
!
interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.2.254 255.255.255.0
!
interface FastEthernet0/0.30
encapsulation dot1Q 30
```

```
ip address 192.168.3.254 255.255.255.0
!
interface FastEthernet0/0.40
encapsulation dot1Q 40
ip address 192.168.4.254 255.255.255.0
```

La interfaz fa0/1 va directamente conectada a la BS, por lo cual se le asignó una IP que perteneciera al mismo segmento.

```
!
interface FastEthernet0/1
description Enlace a BS
ip address 192.168.182.37 255.255.255.0
duplex auto
speed auto
```

También se configuraron rutas estáticas, con las cuales se aseguró comunicación con las redes del otro extremo de la red, las redes que van al subscriptor.

```
ip route 192.168.20.0 255.255.255.0 192.168.182.111
ip route 192.168.30.0 255.255.255.0 192.168.182.111
ip route 192.168.40.0 255.255.255.0 192.168.182.111
```

Finalmente se configuraron listas de acceso, para asegurar comunicación entre VLANs del mismo servicio.

```
access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 101 permit ip 192.168.4.0 0.0.0.255 192.168.40.0 0.0.0.255
```

5.2.1.2 Configuración del *Router* conectado al Subscriptor

Se configuró la interfaz Fa0/0 con tres subinterfaces, como se muestra a continuación:

A la interfaz fa0/0 se le asocio a una lista de acceso.

```
interface FastEthernet0/0
no ip address
ip access-group 100 in
duplex auto
speed auto
```

```
!
interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.254 255.255.255.0
!
interface FastEthernet0/0.30
encapsulation dot1Q 30
ip address 192.168.30.254 255.255.255.0
!
interface FastEthernet0/0.40
encapsulation dot1Q 40
ip address 192.168.40.254 255.255.255.0
```

La interfaz fa0/1 va directamente conectada a la BS, por lo cual se le asigno una IP que perteneciera al mismo segmento.

```
!
interface FastEthernet0/1
description Enlace a subscriptor
ip address 192.168.182.111 255.255.255.0
duplex auto
speed auto
```

También se configuraron rutas estáticas, con las cuales se aseguro comunicación con las redes del otro extremo de la red, las redes que van al subscriptor.

```
ip route 192.168.2.0 255.255.255.0 192.168.182.37
ip route 192.168.3.0 255.255.255.0 192.168.182.37
ip route 192.168.4.0 255.255.255.0 192.168.182.37
```

Finalmente se configuraron listas de acceso, para poder asegurar que solo existiera comunicación entre VLANs del mismo servicio y para la clasificación de tráfico.

```
access-list 100 permit ip 192.168.20.0 0.0.0.255 192.168.2.0 0.0.0.255
access-list 100 permit ip 192.168.30.0 0.0.0.255 192.168.3.0 0.0.0.255
access-list 100 permit ip 192.168.40.0 0.0.0.255 192.168.4.0 0.0.0.255
access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.2.0 0.0.0.255
access-list 102 permit ip 192.168.30.0 0.0.0.255 192.168.3.0 0.0.0.255
access-list 103 permit ip 192.168.40.0 0.0.0.255 192.168.4.0 0.0.0.255
```

5.2.1.3 Configuración del *Switch* conectado a la BS

A las interfaces de la fa0/1 a la fa0/8 se les asigno la VLAN 20 (VLAN de VOZ), y se les configuro en modo de acceso.

```
!
interface FastEthernet0/1
description VLAN_VOZ
switchport access vlan 20
switchport mode access
!
!
interface FastEthernet0/8
description VLAN_VOZ
switchport access vlan 20
switchport mode access
```

Las interfaces de la fa0/9 a la fa0/16 se les asigno la VLAN 30 (VLAN de VIDEO), se les configuro en modo de acceso.

```
interface FastEthernet0/9
description VLAN_VIDEO
switchport access vlan 30
switchport mode access
!
!
interface FastEthernet0/16
description VLAN_VIDEO
switchport access vlan 30
switchport mode access
```

Las interfaces de la fa0/17 a la fa0/23 se les asigno la VLAN 40 (VLAN de DATOS), se les configuro en modo de acceso.

```
interface FastEthernet0/17
description VLAN_DATOS
switchport access vlan 40
switchport mode access
!
!
interface FastEthernet0/23
```

```
description VLAN_DATOS
switchport access vlan 40
switchport mode access
```

La interfaz fa0/24 se configuro como troncal, puesto que esta se conecta como troncal al *Router* BS.

```
interface FastEthernet0/24
description Trunk a R_BS
switchport mode trunk
!
```

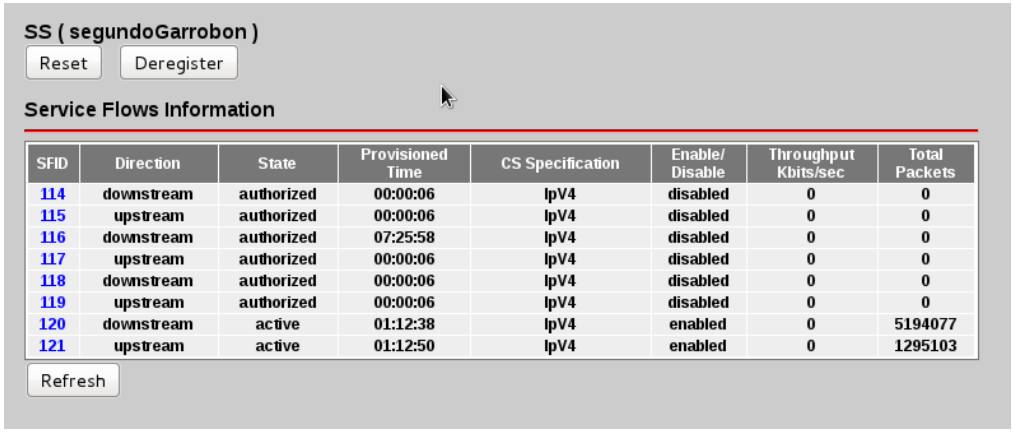
5.2.1.4 Configuración del *Switch* conectado al Subscriptor

La configuración fue exactamente la misma que la mostrada anteriormente.

- Las interfaces de la fa0/1 a la fa0/8 se les asigno la VLAN 20 (VLAN de VOZ) en modo de acceso.
- Las interfaces de la fa0/9 a la fa0/16 se les asigno la VLAN 30 (VLAN de VIDEO), se les configuro en modo de acceso.
- Las interfaces de la fa0/17 a la fa0/23 se les asigno la VLAN 40 (VLAN de DATOS), se les configuro en modo de acceso.
- La interfaz fa0/24 se configuro como troncal, puesto que esta se conecta como troncal al *Router* del Subscriptor.

5.2.1.5 Configuración de flujos en la BS

Para este caso se ingresa a la pestaña de SFs y se desactivan todos los flujos excepto los correspondientes a la clase canal único, para comprobar que sólo dichos canales funcionen se capturó la pantalla correspondiente al número de paquetes enviados a través de cada canal:



SFID	Direction	State	Provisioned Time	CS Specification	Enable/ Disable	Throughput Kbits/sec	Total Packets
114	downstream	authorized	00:00:06	IpV4	disabled	0	0
115	upstream	authorized	00:00:06	IpV4	disabled	0	0
116	downstream	authorized	07:25:58	IpV4	disabled	0	0
117	upstream	authorized	00:00:06	IpV4	disabled	0	0
118	downstream	authorized	00:00:06	IpV4	disabled	0	0
119	upstream	authorized	00:00:06	IpV4	disabled	0	0
120	downstream	active	01:12:38	IpV4	enabled	0	5194077
121	upstream	active	01:12:50	IpV4	enabled	0	1295103

Figura 40 Comprobación del uso del canal “Clase Unica”

5.2.2 Con QoS en el equipo CISCO

5.2.2.1 Configuración del *Router* conectado a la BS

Se crearon tres clases, para cada uno de nuestros servicios (VOZ, VIDEO y DATOS).

A estas clases se les asignaron las listas de acceso previamente configuradas, esto con el objeto de asegurar que las direcciones IP que contienen los distintos paquetes (voz, video y datos) se les asignara la QoS correcta.

```
class-map VoIP
match access-group 101

class-map VIDEO
match access-group 102

class-map DATOS
match access-group 103
```

Posteriormente se crearon políticas, las cuales se les atribuyeron a las diferentes clases.
A la clase de voz, se le marco con DSCP ef, la cual es la óptima para la voz, tiene una prioridad de valor 5, lo cual hace que sea la primera en enviarse.
También se le asigna una cola de prioridad estricta de 256 kbps y un buffer de 6000 bytes, con lo cual aseguramos suficiente ancho de banda para cuatro llamadas.

```
policy-map POLITICAS

class VoIP
set ip dscp ef
priority 256 6000
```

A la clase de video se le etiqueto con un DSCP af43, el cual asegura una prioridad de clase alta, después de la voz, además de que se le reservo un ancho de banda del 60 % de todo el ancho de banda permitido y se activó un mecanismo de descarte inteligente, el cual descarta paquetes con menor valor de DSCP para evitar colisiones, es conocido como WRED(Weighted Random Early Discard).

```
class VIDEO
set ip dscp af43
bandwidth percent 60
```

random-detect dscp-based

A la clase de datos se le etiqueto con un DSCP af11, el cual asegura una prioridad de clase baja, puesto que los datos es lo que tiene prioridad más baja en nuestra red, además se le reservo un ancho de banda del 10 % de todo el ancho de banda permitido y se activó un mecanismo de descarte inteligente, igual que en la política de video.

class DATOS
set ip dscp af11
bandwidth percent 10
random-detect dscp-base

Por último se le asignaron las políticas a la salida de la interfaz fa0/1, la cual está conectada a la BS.

interface fa0/1
service-policy output POLITICAS

5.2.2.2 Configuración del *Router* conectado al Subscriptor

La configuración de QoS debe ser la misma en ambos *Routers*, por lo cual la configuración aplicada en el *Router* de la BS, fue la misma en el *Router* conectado al Subscriptor cambiando al número de ACL a 101.

5.2.2.3 Configuración del *Switch* conectado a la BS

La configuración de QoS a nivel capa 2 solo es necesaria en los puertos que tendrán asignada la VLAN de Voz, en este caso, los puertos Fa0/1 a Fa0/8.

interface range FastEthernet0/1-8
switchport acces vlan 20
mls qos 5
mls qos trust device cisco-phone
mls qos trust cos

Con esta configuración al conectar los teléfonos IP se consigue crear una VLAN entre el *switch* interno del teléfono y el *switch* de la red, las tramas que llegan al *switch* de la red son marcadas con prioridad de 5 (siendo 7 el máximo posible).

5.2.2.4 Configuración del *Switch* conectado al Subscriptor

```
interface  range FastEthernet0/1-8
switchport voice vlan 20
mls qos 5
mls qos trust device cisco-phone
mls qos trust cos
```

La configuración es exactamente igual al *Switch* conectado a la BS.

5.2.3 Con QoS de extremo a extremo

En este caso se activan los SF número 114 hasta 119 correspondientes a los canales separados de voz (VoIP), video (Video*Streaming*), y datos (datosFTP), a la vez se desactivan los SF 120 y 121 correspondientes al canal único.

Sin embargo el proceso mediante el cual *Ethernet* relaciona direcciones de capa 3 con direcciones de capa 2 (ARP) es usado por los *routers* por lo que se requiere activar los canales default (Default serviceflows, mencionados también en el capítulo anterior).

CAPITULO VI

Resultados

Este capítulo comienza por realizar pruebas para determinar la máxima tasa de transmisión disponible en el radioenlace para posteriormente saber con que cantidad de información puede saturarse y comenzar a realizar pruebas sobre la degradación de la calidad de los servicios.

Las primeras pruebas se realizan únicamente con el direccionamiento lógico configurado y de forma gradual hasta hacer fallar a los servicios. En seguida se activa la QoS del equipo CISCO con lo que se comparan las mejoras respecto a la situación anterior. Finalmente también se activa la QoS del equipo WiMAX y se realizan un par de pruebas en primer lugar para verificar el correcto funcionamiento de los servicio y en segundo que se cumplan las limitaciones de velocidad de transferencia para los servicios.

6.1 Sin QoS

El tráfico UDP es el que acapara el medio, este se envía sin importar si su información o la de otros servicios es recibida correctamente, el tráfico UDP de mayor volumen es el de video. Por ello para saturar el canal es utilizaron diversas transmisiones de video de manera simultánea, analizando en cada caso las prestaciones del canal respecto al retardo de paquetes, el porcentaje de paquetes recibidos, y el ancho de banda reservado al canal de video. Lo anterior con el fin de mostrar el comportamiento del flujo de datos respecto a las políticas de QoS tanto del equipo de red cableada, como del equipo WiMAX.

Se saturó exclusivamente el canal de bajada debido a que en el extremo de la BS se ubicaron los servidores y en el extremo del suscriptor se ubicaron los clientes.

El enlace implementado atraviesa dos medios de transmisión, el primero cable de red, y el segundo aire. En las interfaces *Ethernet* se tuvo una velocidad de enlace de 100 Mbps en modo full duplex, mientras que en la interfaz aérea fue de 6.6 Mbps en el canal de bajada y de 4.5 Mbps en el canal de subida. La siguiente figura indica dichos valores:

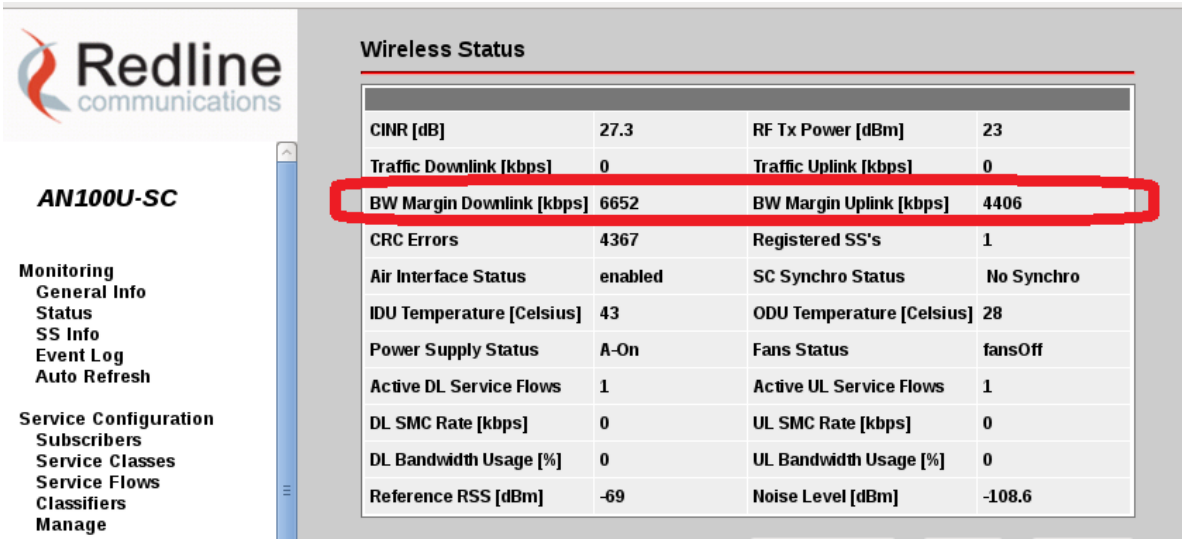


Figura 41 Máxima tasa de transmisión indicada por la BS

Teniendo en cuenta que la velocidad de procesamiento en el equipo de red es mayor a la de sus interfaces, la velocidad de transmisión alcanzada de extremo a extremo está limitada por la velocidad de transmisión de la interfaz aérea. Para comprobar esto se usó un analizador de tráfico.

6.1.1 Velocidad de transmisión máxima del canal de bajada (de extremo a extremo):

El valor de la velocidad de transmisión soportado por la BS fue de 6.6 Mbps, y el valor promedio del video utilizado fue de 2.5 Mbps así que usando sólo las computadoras correspondientes al servicio de video se transmitieron de manera paralela 5 videos, prestando atención a la velocidad de transmisión indicada por el analizador de red en el extremo receptor. Dicho valor es el mostrado en la siguiente figura:

Network Load	Actual	6.1 Mbit/s	581.6 Pkt/s
	Last Minute	6.1 Mbit/s	587.6 Pkt/s
	Last 5 Minutes	5.9 Mbit/s	564.4 Pkt/s
	Peak	6.5 Mbit/s	626.4 Pkt/s
	Average	4.7 Mbit/s	447.3 Pkt/s
Historical Data			[ ]

Global Protocol Distribution

Protocol	Data	Percentage				
IP	969.6 MBytes	100.0%	UDP	968.9 MBytes	99.9%	
			ICMP	740.2 KBytes	0%	

Figura 42 Comprobación de la máxima tasa de transmisión mediante NTOP

6.1.2 Análisis 1 Retardo en el canal de voz sin trafico en los demas segmentos

Para determinar las pérdidas que se presentan de extremo a extremo de nuestra red, se utilizó el comando *"ping"*. Para la primera prueba se hizo *ping* desde el *Router* del Subscriptor hacia una IP del segmento de la VLAN de VOZ, para poder determinar las pérdidas de paquetes y los problemas de latencia; con el objeto de asegurar que los retardos no superen los 126 ms que son los necesarios para una llamada de voz.

Las tres pruebas que se realizaron, fueron las mismas para todos análisis.

Primera prueba:

Ping 192.168.2.11 repeat 1000

El *router* Cisco envía 1000 paquetes tan rápido como se puedan generar, esperando respuestas.

```
R_Subscriptor#ping 192.168.2.11 repeat 1000

Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 192.168.2.11, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (999/1000), round-trip min/avg/max = 28/30/32 ms
```

Figura 43 Respuesta ICMP del *Router* (*ping* repetido 1000)

La figura muestra que los 999 paquetes obtuvieron respuestas, salvo un paquete, con tiempos mínimos de 28ms y máximos de 32ms.

Segunda prueba:

Ping 192.168.2.11 size 1000

Se crea un paquete ICMP de tamaño 1000

```
R_Subscriptor#ping 192.168.2.11 size 1000

Type escape sequence to abort.
Sending 5, 1000-byte ICMP Echos to 192.168.2.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/40 ms
```

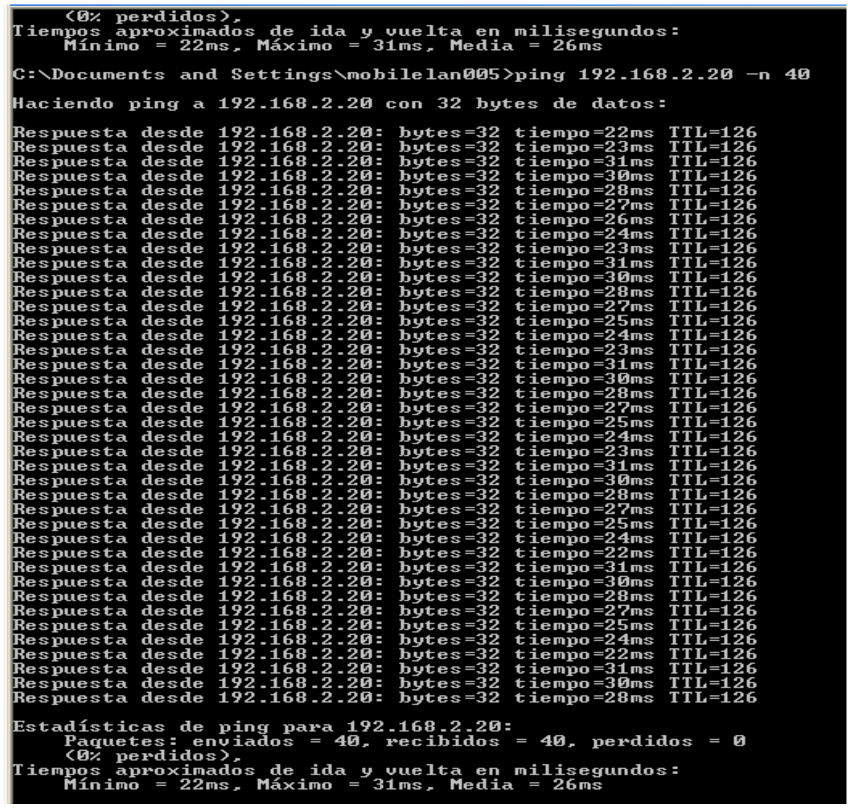
Figura 44 Respuesta ICMP del *Router* (tamaño paquete ICMP 1000)

Se observa que la respuesta de eco fue recibida correctamente, con un mínimo y máximo de 40ms.

Tercera prueba:

Se realizó un *ping* desde una computadora hacia otra computadora.

Se generó un *ping* que se repitió 40 veces.



```
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 22ms, Máximo = 31ms, Media = 26ms

C:\Documents and Settings\mobilelan005>ping 192.168.2.20 -n 40

Haciendo ping a 192.168.2.20 con 32 bytes de datos:

Respuesta desde 192.168.2.20: bytes=32 tiempo=22ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=23ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=31ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=30ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=28ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=27ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=26ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=24ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=23ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=31ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=30ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=28ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=27ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=25ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=24ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=23ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=31ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=30ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=28ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=27ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=25ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=24ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=23ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=31ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=30ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=28ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=27ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=25ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=24ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=22ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=31ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=30ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=28ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=27ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=25ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=24ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=22ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=31ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=30ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=28ms TTL=126

Estadísticas de ping para 192.168.2.20:
    Paquetes: enviados = 40, recibidos = 40, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 22ms, Máximo = 31ms, Media = 26ms
```

Figura 45 Respuesta *ping* de PC de voz

Se puede observar que no hubo pérdidas en los *ping*s, se mandaron 40 *ping*s y se recibieron 40 *ping*s, además se tuvo un mínimo de 22ms y un máximo de 31ms en la respuesta de estos.

La siguiente gráfica muestra los retardos producidos de la anterior prueba.

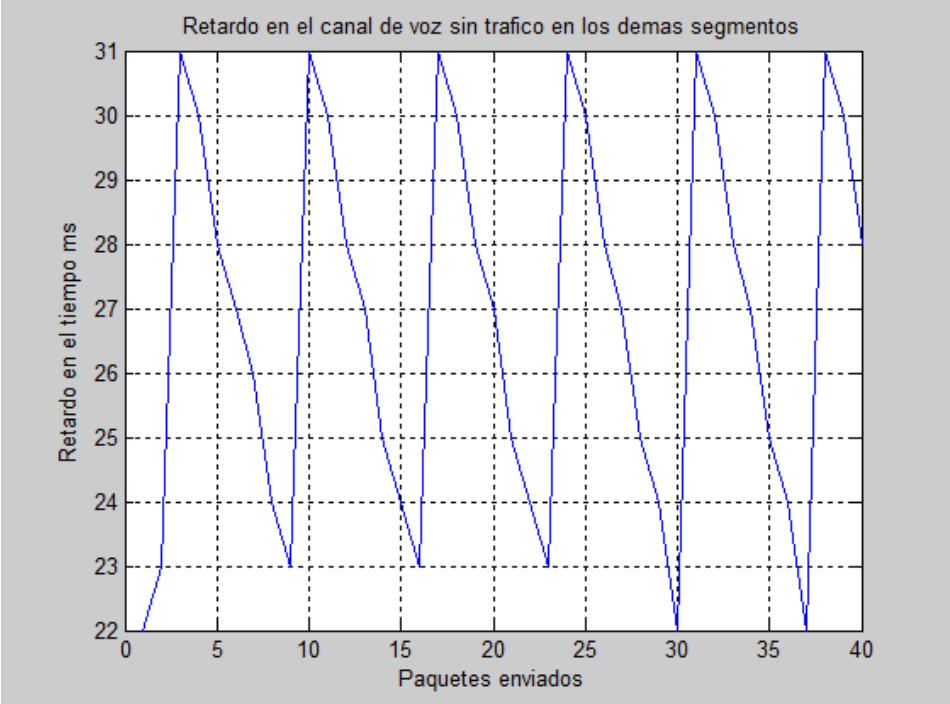


Figura 46 Gráfica de los retardos de los paquetes *ping*

Se observa que los retardos oscilan entre 22ms y 31 ms

6.1.3 Análisis 2. Retardo en el canal de voz inyectando tráfico en el canal de datos mediante el *software* IPERF

Primera prueba:

Ping 192.168.2.11 repeat 1000

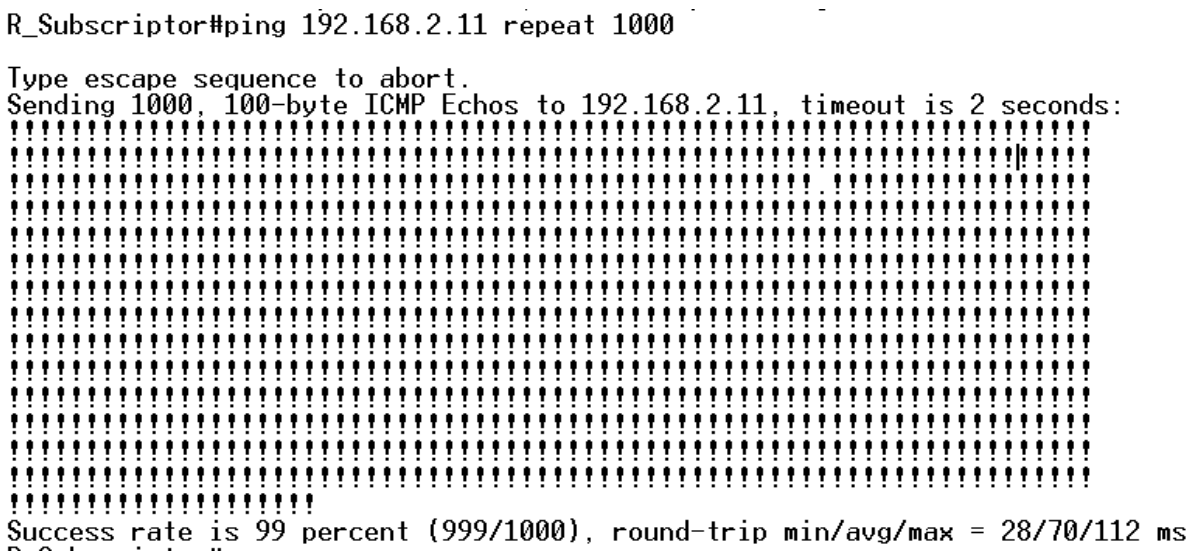


Figura 47 Respuesta ICMP del *Router* (*ping* repetido 1000)

La figura muestra que los 999 paquetes obtuvieron respuestas, salvo un paquete, con tiempos mínimos de 28ms y máximos de 112ms.

Para este caso se puede observar que el tiempo de latencia subió hasta 112ms como máximo, teniendo en cuenta que en la primer análisis sin tráfico agregado fue de 32ms.

Segunda prueba:

Ping 192.168.2.11 size 1000

Se crea un paquete ICMP de tamaño 1000

```
R_Subscriptor#ping 192.168.2.11 size 1000

Type escape sequence to abort.

Sending 5, 1000-byte ICMP Echos to 192.168.2.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/91/120 ms
```

Figura 48 Respuesta ICMP del *Router* (tamaño paquete ICMP 1000)

En este caso la respuesta de eco fue recibida correctamente, con un mínimo de 36 ms y un máximo de 120ms.

Tercera prueba:

Se realizó un *ping* desde una computadora hacia otra computadora.

Se generó un *ping* que se repitió 40 veces.

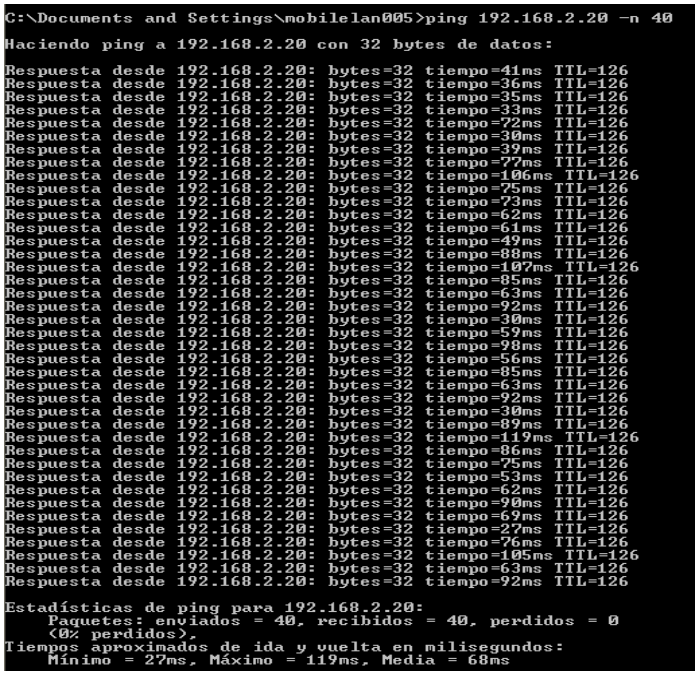


Figura 49 Respuesta *ping* de PC de voz

Tampoco hubo pérdidas en los *ping*s, se mandaron 40 *ping*s y se recibieron 40 *ping*s, pero la latencia está incrementándose, con mínimo de 27ms y máximo de 119ms en la respuesta de estos.

La siguiente gráfica muestra los retardos producidos de la anterior prueba.

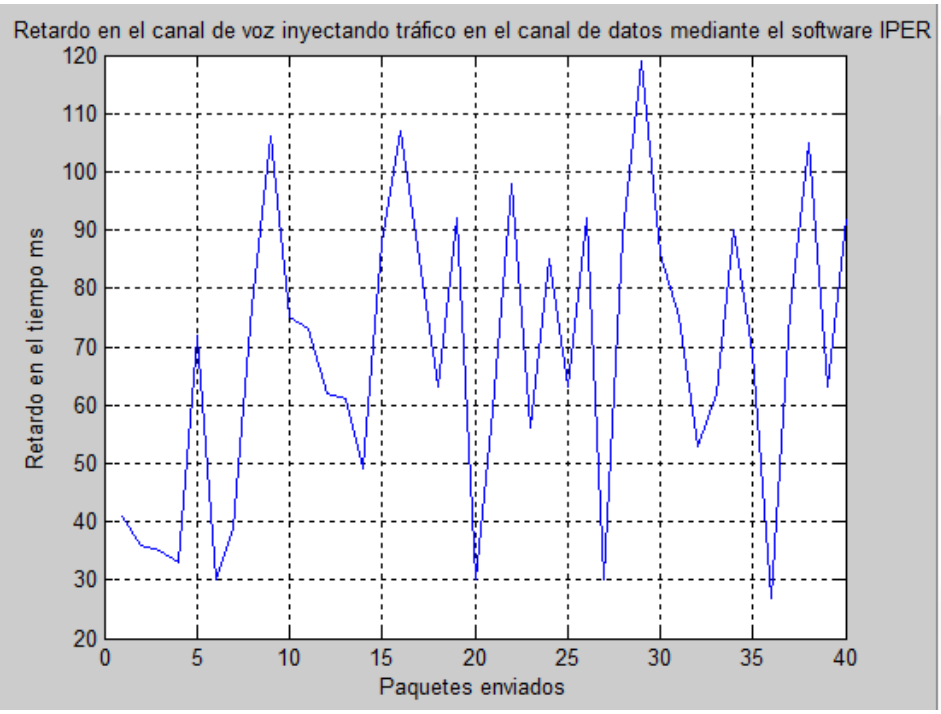


Figura 50 Gráfica de los retardos de los paquetes *ping*

La grafica ilustra la variación del tiempo de respuesta que se da al inyectar tráfico.

6.1.4 Análisis 3. Retardo en el canal de voz inyectando tráfico en el canal de datos mediante el *software* IPERF e inyectando tráfico en el canal de video, mediante la descarga de un video

Primera prueba:

Ping 192.168.2.11 repeat 1000

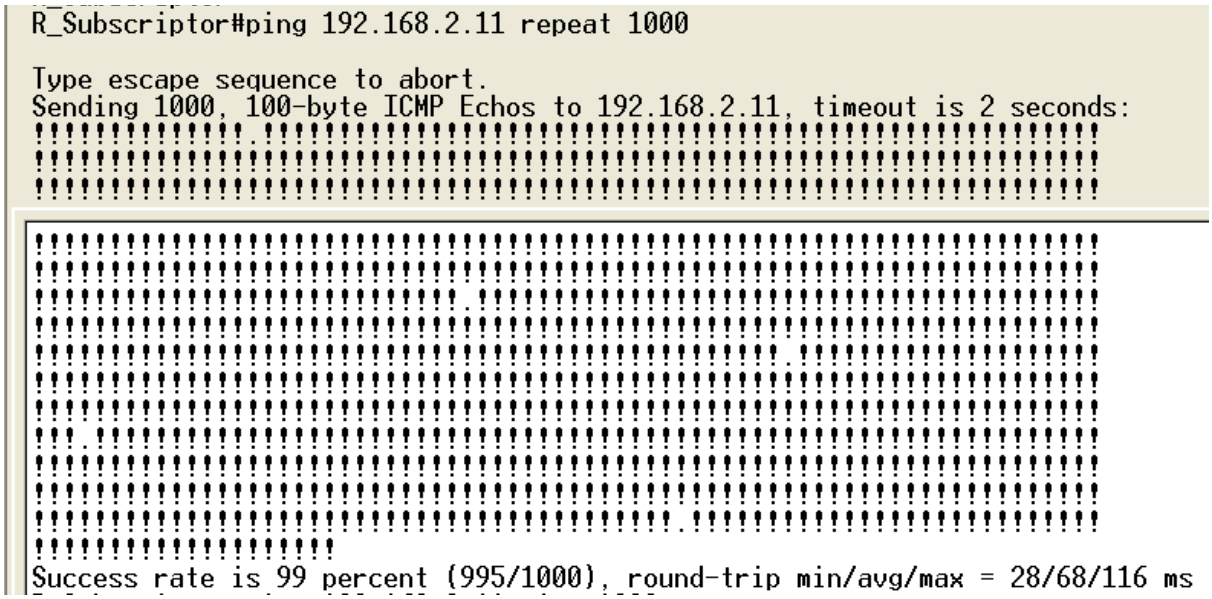


Figura 51 Respuesta ICMP del *Router* (*ping* repetido 1000)

En este caso ya hay un incremento en la perdida de paquetes, 5 en este caso, además de que la latencia sigue incrementándose.

Segunda prueba:

Ping 192.168.2.11 size 1000

Se crea un paquete ICMP de tamaño 1000

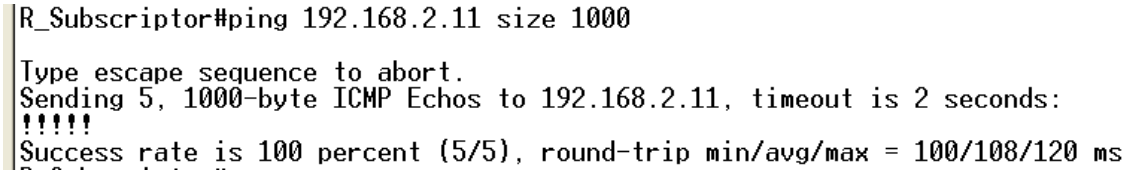


Figura 52 Respuesta ICMP del *Router* (tamaño paquete ICMP 1000)

Las respuestas de eco se siguen recibiendo, pero los tiempos de respuesta ya aumentaron más, puesto que el mínimo se obtuvo en 100ms y el máximo en 120ms.

Tercera prueba:

Se realizó un *ping* desde una computadora hacia otra computadora.

Se generó un *ping* que se repitió 40 veces.

```
C:\Documents and Settings\mobilelan005>ping 192.168.2.20 -n 40

Haciendo ping a 192.168.2.20 con 32 bytes de datos:

Respuesta desde 192.168.2.20: bytes=32 tiempo=105ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=75ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=103ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=72ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=100ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=69ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=107ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=66ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=95ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=63ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=92ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=51ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=89ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=78ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=86ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=95ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=83ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=102ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=80ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=50ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=88ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=116ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=86ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=113ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=72ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=100ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=79ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=107ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=46ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=54ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=93ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=72ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=80ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=109ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=87ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=116ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=75ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=83ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=82ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=60ms TTL=126

Estadísticas de ping para 192.168.2.20:
    Paquetes: enviados = 40, recibidos = 40, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 46ms, Máximo = 116ms, Media = 84ms
```

Figura 53 Respuesta *ping* de PC de voz

Los paquetes ICMP llegaron completos, pero los retardos siguen incrementándose, mínimo de 46 ms y máximo de 116 ms

La siguiente gráfica muestra los retardos producidos de la anterior prueba.

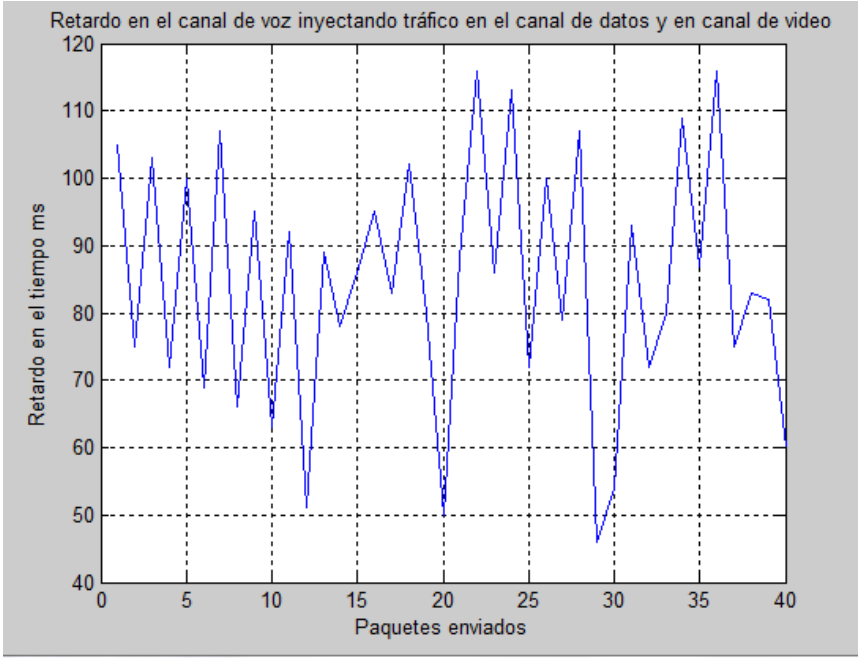


Figura 54 Gráfica de los retardos de los paquetes *ping*

La grafica muestra que los retardos en el tiempo cambian más en comparación con las anteriores.

Por otra parte el video se reprodujo en su mayoría sin pausas ni distorsiones, la siguiente imagen es una captura hecha en el cliente:

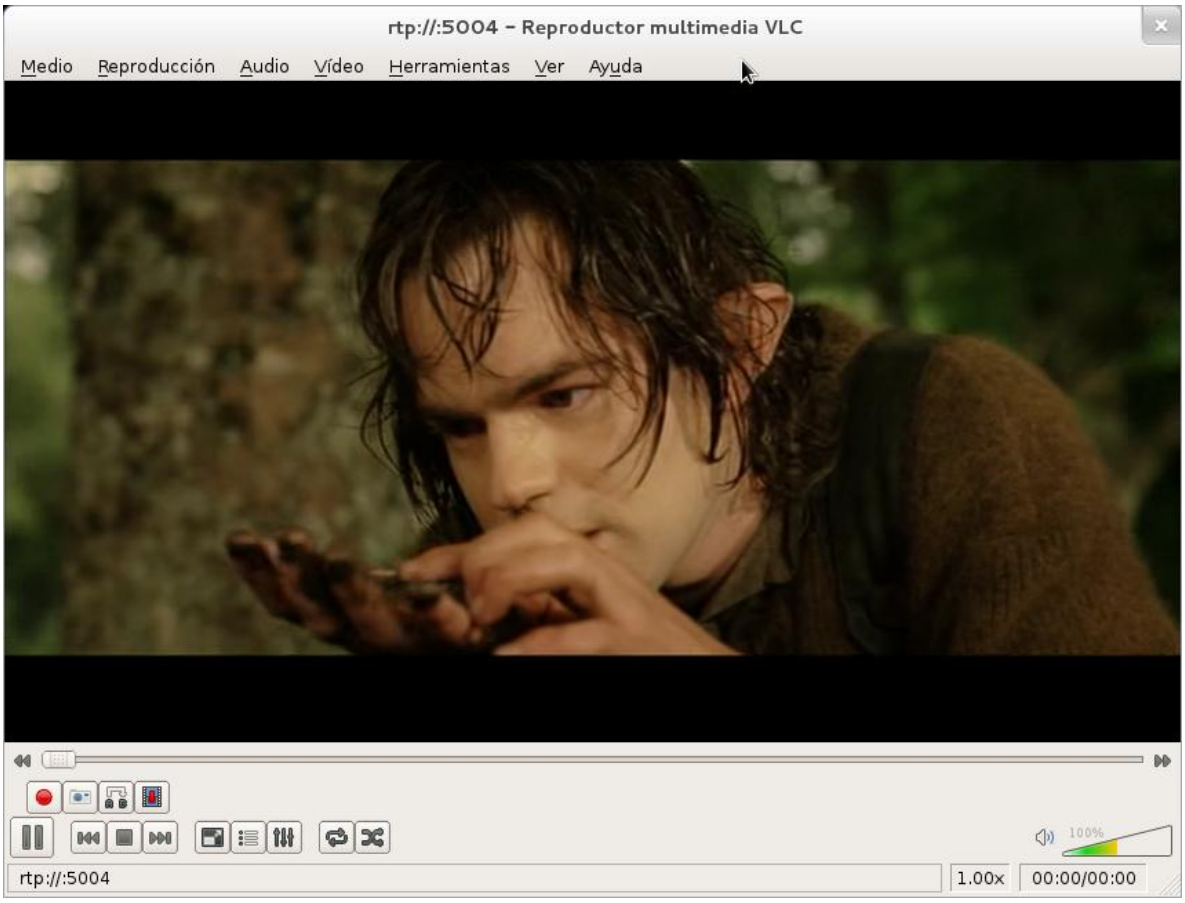


Figura 55 Imagen de un video transmitiéndose

Mediante nTop registramos el siguiente valor de tasa de transmisión en el cliente de video:

Network Load	Actual	2.6 Mbit/s	253.0 Pkt/s
	Last Minute	0.0 bit/s	0.0 Pkt/s
	Last 5 Minutes	0.0 bit/s	0.0 Pkt/s
	Peak	2.6 Mbit/s	253.0 Pkt/s
	Average	2.5 Mbit/s	236.7 Pkt/s
Historical Data			[ ]

Figura 56 Tasa de transmisión para un video

6.1.5 Análisis 4. Retardo en el canal de voz inyectando tráfico en el canal de datos mediante el *software* IPERF he inyectando tráfico en el canal de video, mediante la descarga de 2 videos

Primera prueba:

Ping 192.168.2.11 repeat 1000

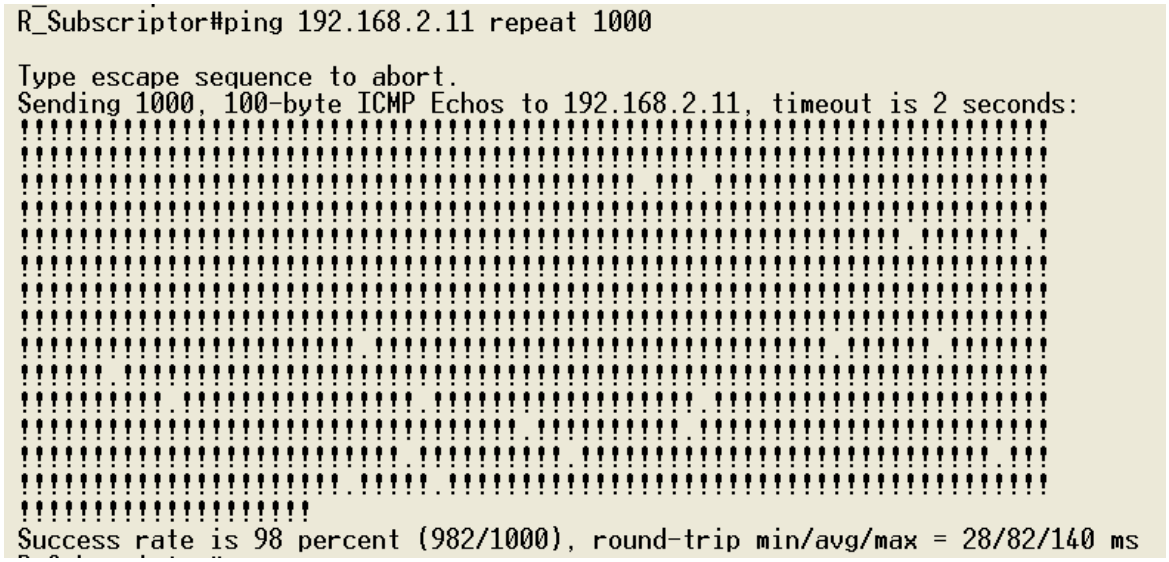


Figura 57 Respuesta ICMP del *Router* (*ping* repetido 1000)

Se observa con mas claridad los paquetes perdidos (18 paquetes), ademas de que la latencia se incremento a 140 ms como maxima.

Segunda prueba:

Ping 192.168.2.11 size 1000

Se crea un paquete ICMP de tamaño 1000

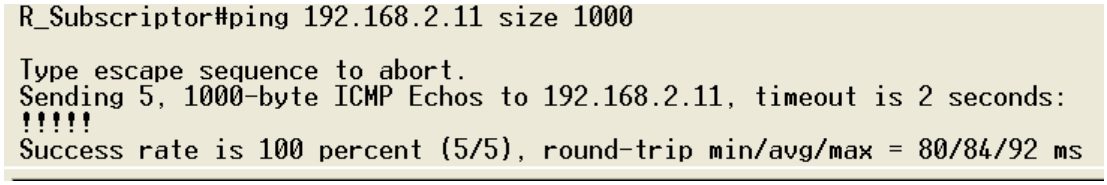


Figura 58 Respuesta ICMP del *Router* (tamaño paquete ICMP 1000)

Los paquetes ICMP llegaron completos, pero el tiempo mínimo de latencia se incremento a 80 ms, y el tiempo máximo bajo a 92 ms, este resultado no se esperaba.

Tercera prueba:

Se realizó un *ping* desde una computadora hacia otra computadora.

Se generó un *ping* que se repitió 60 veces.

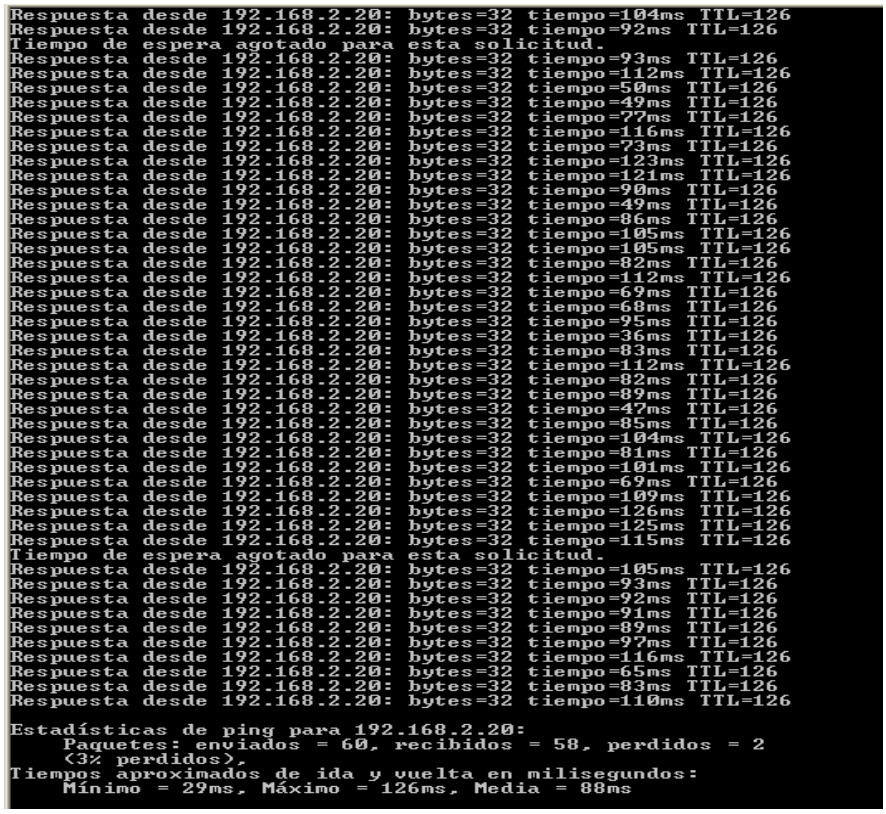


Figura 59 Respuesta *ping* de PC de voz

En esta prueba ya empieza a ver pérdidas de paquetes (2 paquetes).

La siguiente gráfica muestra los retardos producidos de la anterior prueba.

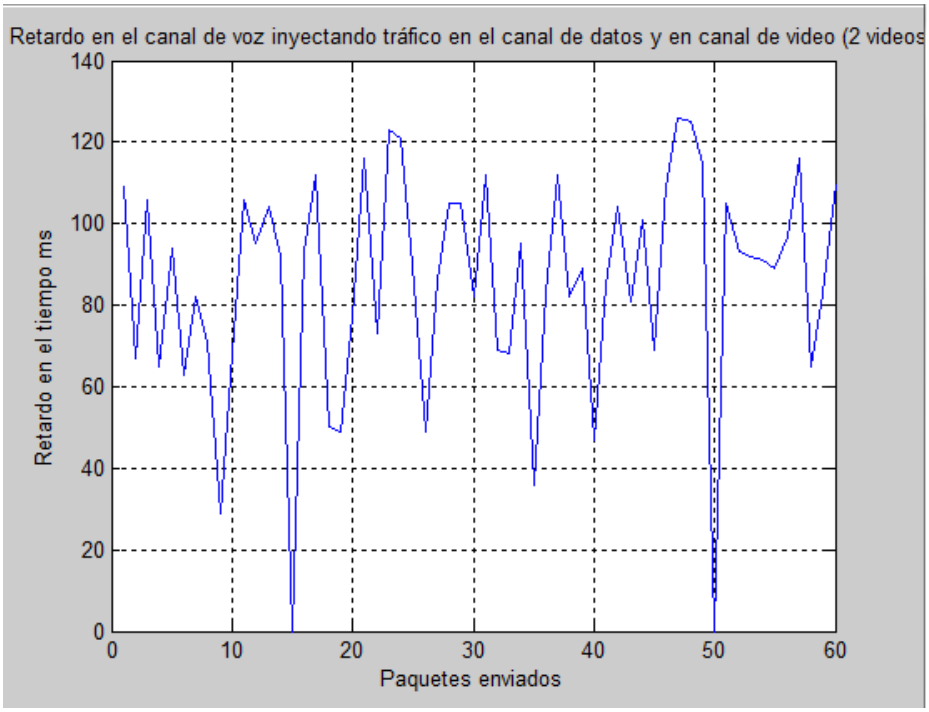


Figura 60 Gráfica de los retardos de los paquetes *ping*

La grafica muestra dos caídas, que significan que los *ping*s no tuvieron respuesta.

El video comenzó a sufrir distorsiones; Sin embargo aún no se producían pausas. La siguiente imagen es una captura de video en el cliente:

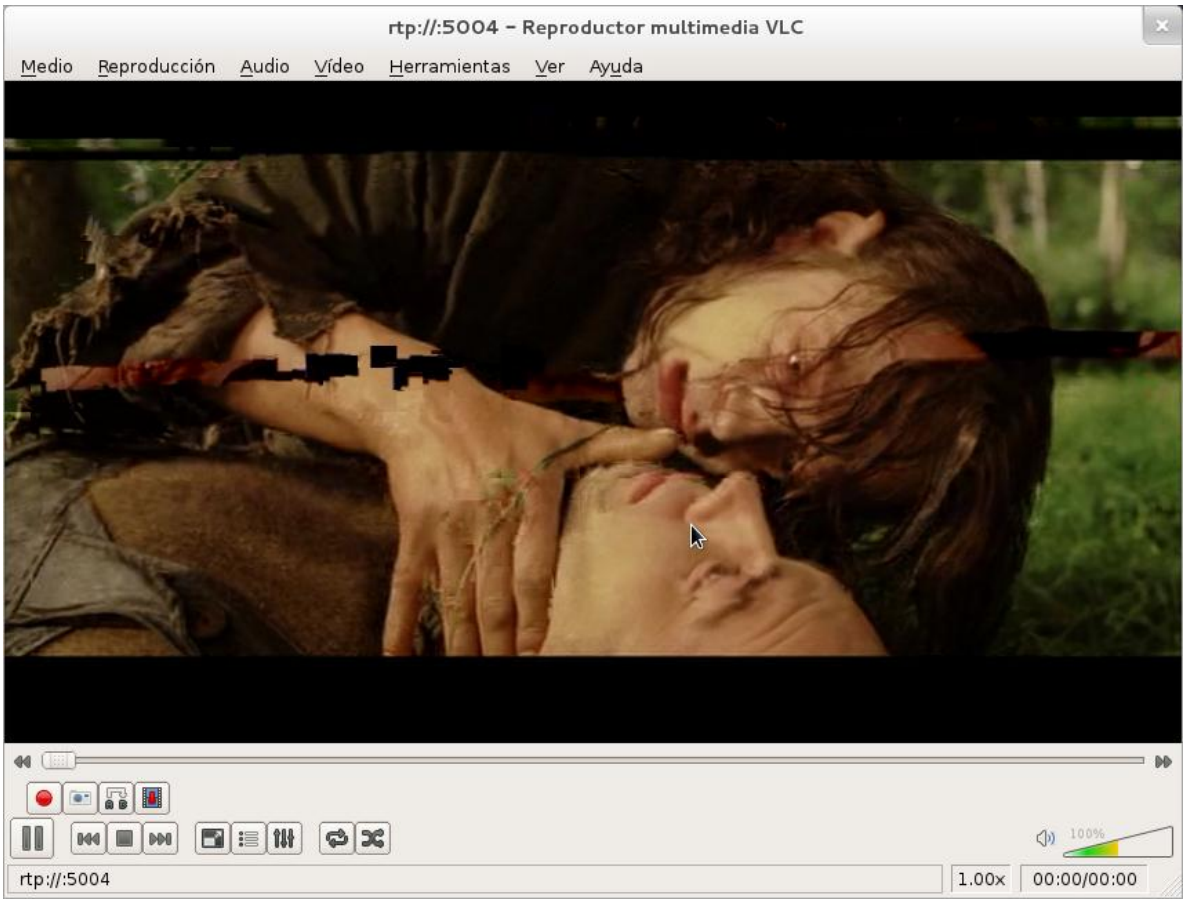


Figura 61 Imagen de dos videos transmitiéndose

De nueva cuenta se analizó nTop y se observó que es este servicio el que acapara el canal:

Network Load	Actual	5.9 Mbit/s	563.6 Pkt/s
	Last Minute	5.5 Mbit/s	531.8 Pkt/s
	Last 5 Minutes	3.8 Mbit/s	368.4 Pkt/s
	Peak	6.2 Mbit/s	593.0 Pkt/s
	Average	3.8 Mbit/s	367.9 Pkt/s
Historical Data			[ ]

Figura 62 Tasa de transmisión para dos videos

6.1.6 Análisis 5. Retardo en el canal de voz inyectando tráfico en el canal de datos mediante el *software* IPERF e inyectando tráfico en el canal de video, mediante la descarga de 3 videos

Primera prueba:

Ping 192.168.2.11 repeat 1000

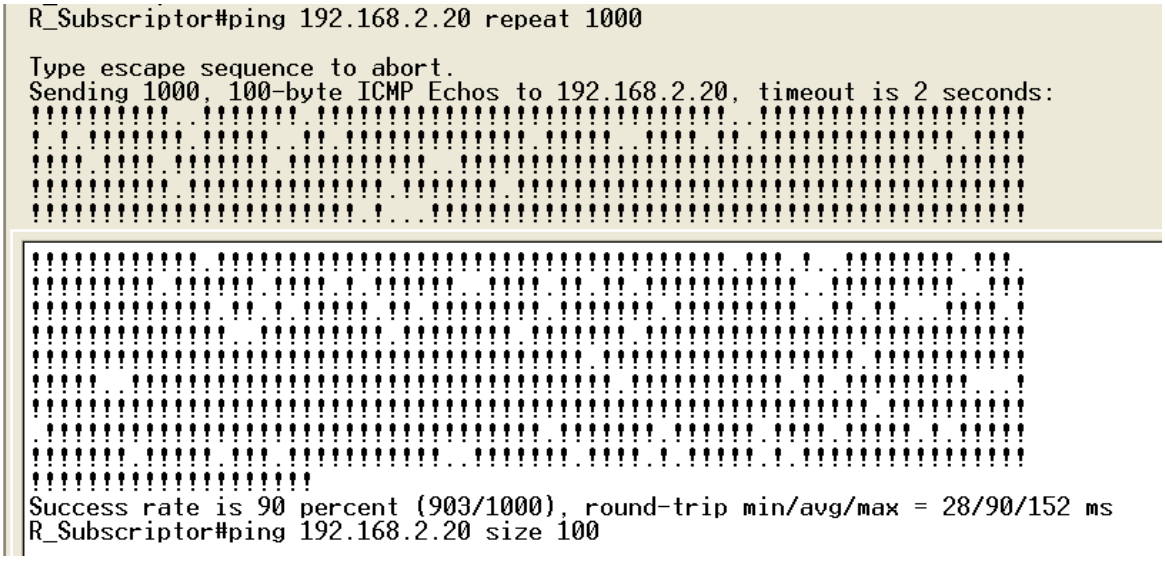


Figura 63 Respuesta ICMP del *Router* (*ping* repetido 1000)

Con tres videos se puede observar quehay mas perdidas de paquetes (97 paquetes), con incrementos de retardos de 152 ms.

Segunda prueba:

Ping 192.168.2.11 size 1000

Se crea un paquete ICMP de tamaño 1000

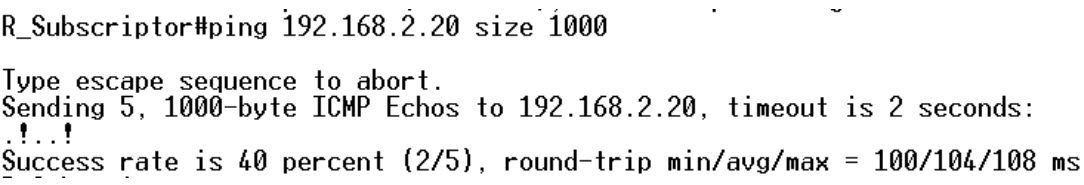


Figura 64 Respuesta ICMP del *Router* (tamaño paquete ICMP 1000)

De 5 paquetes ICMP llegaron solo 3, y los tiempos de latencia son elevados, el mínimo y el máximo son muy parecidos, 100ms y 108 ms respectivamente.

Tercera prueba:

Se realizó un *ping* desde una computadora hacia otra computadora.

Se genero un *ping* que se repitió 40 veces.

Figura 65 Respuesta *ping* de PC de voz

Se muestran mas perdidas de paquetes *ping* (4 paquetes), por otro lado, la latencia sigue respetando el mismo sentido que en la anterior prueba.

La siguiente gráfica muestra los retardos producidos de la anterior prueba.

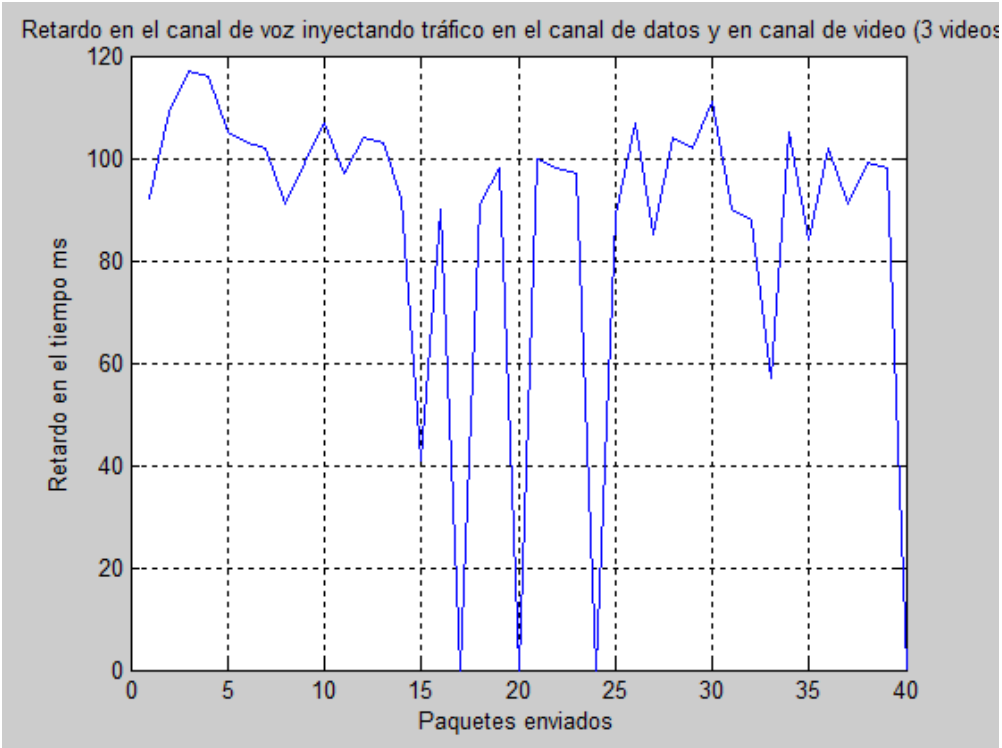


Figura 66 Gráfica de los retardos de los paquetes *ping*

Se muestran 4 caidas, las cuales significan que 4 paquetes ICMP no tuvieron respuesta de eco.

El video comenzó a sufrir pausas además de distorisón, la siguiente imagen es una catura del video en el cliente:

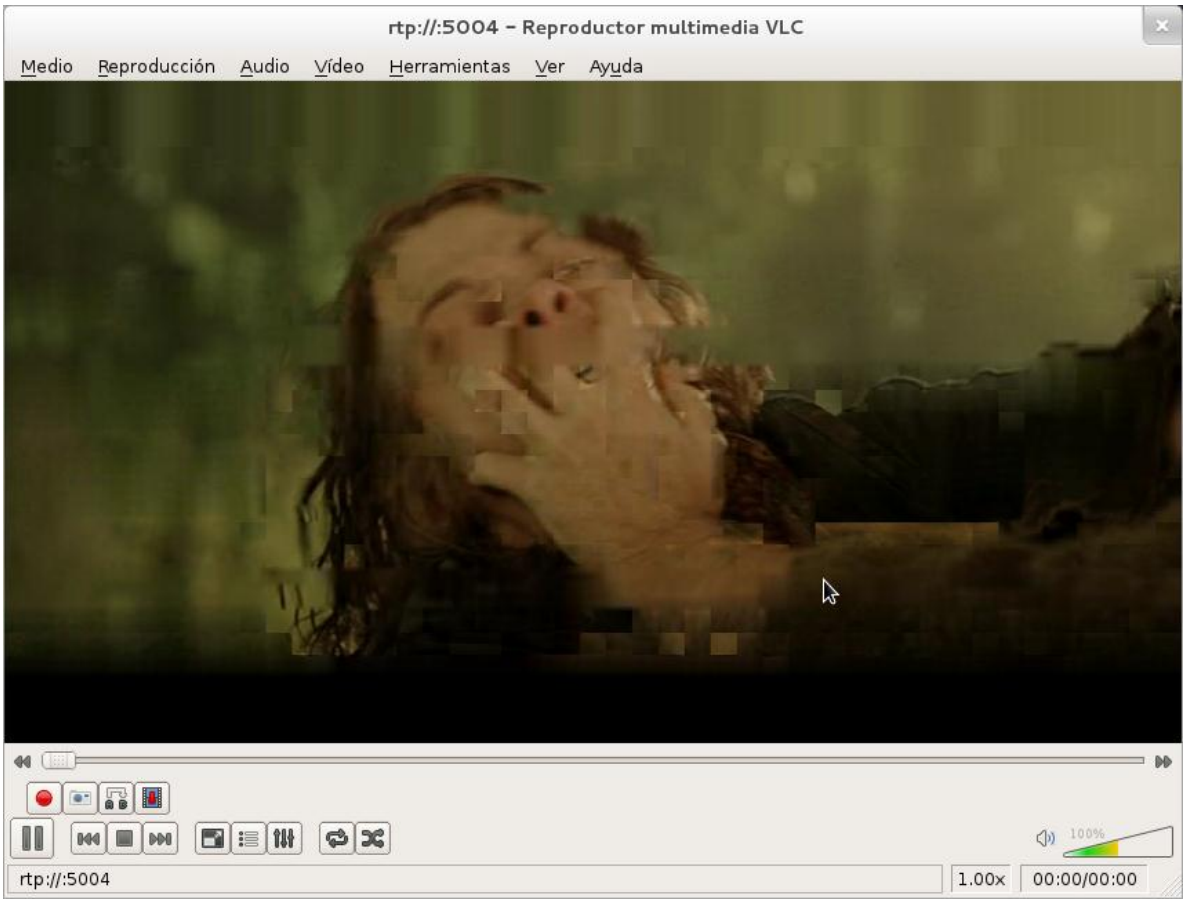


Figura 67 Imagen de tres videos transmitiéndose

Con nTop se observó que a pesar de las distorsiones y pausas aún no se llegaba al límite del enlace:

Network Load	Actual	6.0 Mbit/s	572.0 Pkt/s
	Last Minute	6.3 Mbit/s	602.5 Pkt/s
	Last 5 Minutes	0.0 bit/s	0.0 Pkt/s
	Peak	6.4 Mbit/s	618.0 Pkt/s
	Average	6.1 Mbit/s	589.7 Pkt/s
Historical Data			

Figura 68 Tasa de transmisión para tres videos

6.1.7 Análisis 6. Retardo en el canal de voz inyectando tráfico en el canal de datos mediante el *software* IPERF e inyectando tráfico en el canal de video, mediante la descarga de 4 videos

Primera prueba:

Ping 192.168.2.11 repeat 1000

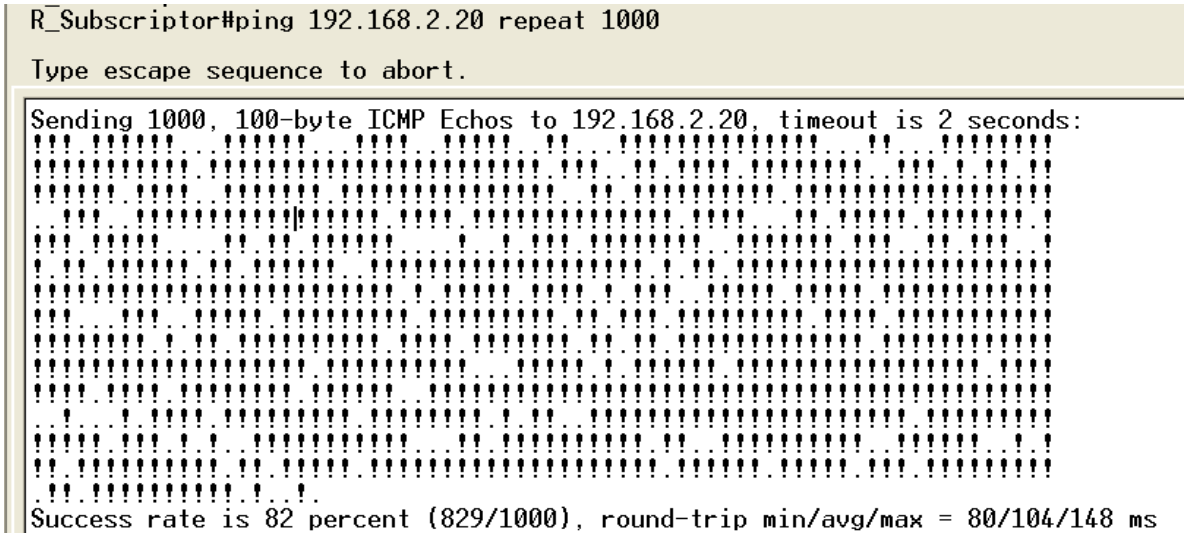


Figura 69 Respuesta ICMP del *Router* (*ping* repetido 1000)

Las perdidas de paquetes ya son muchas (171 paquetes), los retardos son grandes tambien.

Segunda prueba:

Ping 192.168.2.11 size 1000

Se crea un paquete ICMP de tamaño 1000

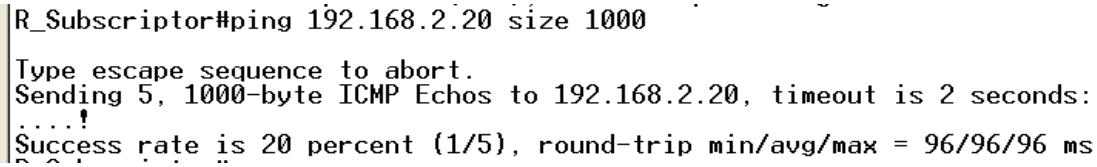


Figura 70 Respuesta ICMP del *Router* (tamaño paquete ICMP 1000)

En este caso solo un paquete llego, y los retardos minimo y maximo son iguales.

Tercera prueba:

Se realizó un *ping* desde una computadora hacia otra computadora.

Se generó un *ping* que se repitió 60 veces.

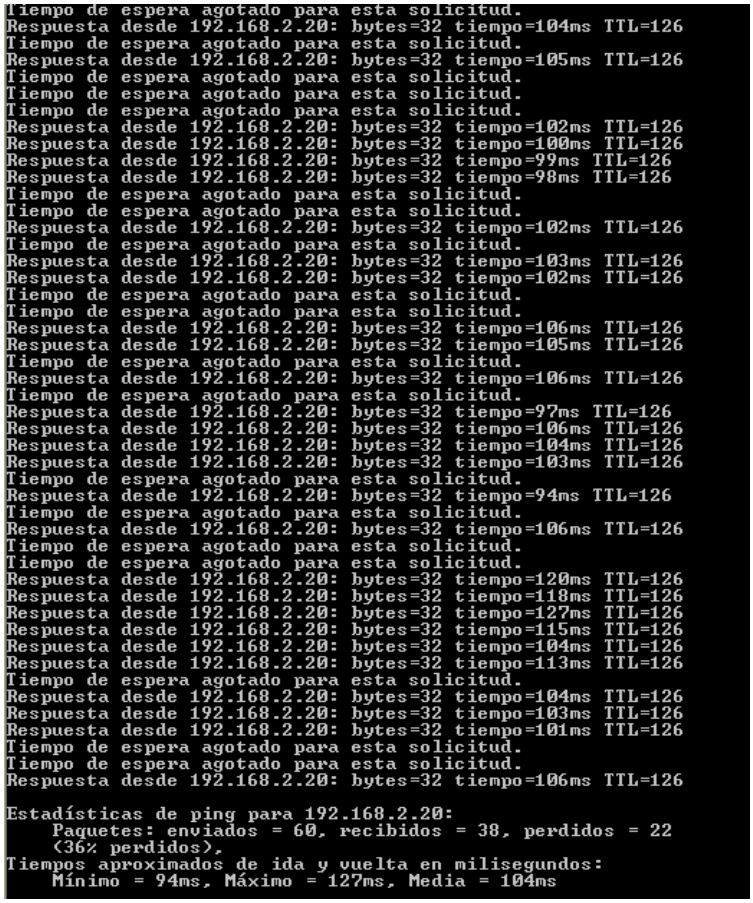


Figura 71 Respuesta *ping* de PC de voz

Se perdieron muchos paquetes *ping* (22 paquetes) de 60 enviados, ademas de que los retardos incrementaron.

La siguiente gráfica muestra los retardos producidos de la anterior prueba.

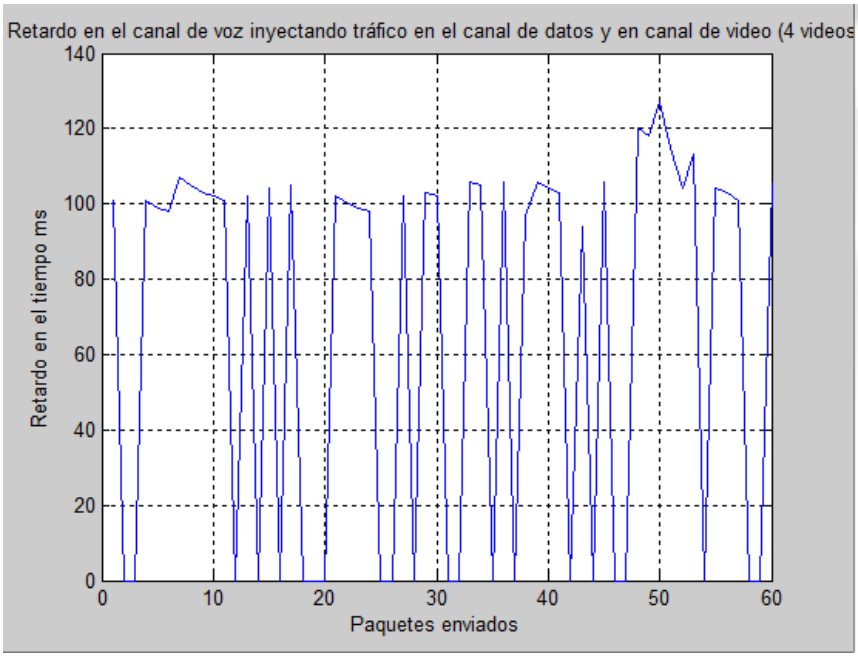


Figura 72 Gráfica de los retardos de los paquetes *ping*

Se observan muchas caidas de mensajes ICMP, ya que estos no tuvieron respuesta de eco.

En este caso el video tanto en audio como en video dejó de ser legible completamente, la siguiente imagen es un captura del video en el cliente:

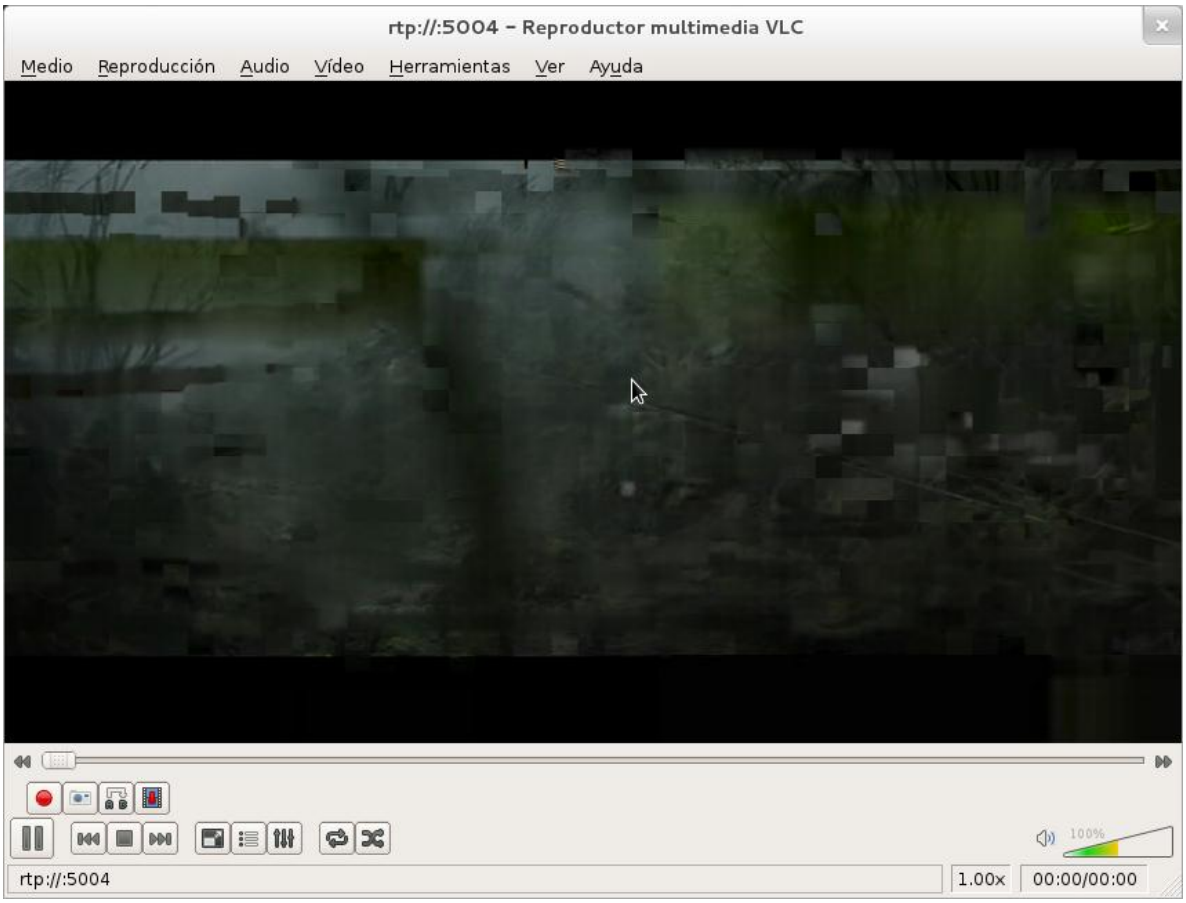


Figura 73 Imagen de cuatro videos transmitiéndose

nTop muestra que se está muy próximo a la saturación del enlace, si no se alcanza es debido a que la tasa de transmisión de los videos es variable y la mayoría de ellos estaba en valores mínimos:

Network Load	Actual	6.4 Mbit/s	615.9 Pkt/s
	Last Minute	6.3 Mbit/s	602.5 Pkt/s
	Last 5 Minutes	0.0 bit/s	0.0 Pkt/s
	Peak	6.4 Mbit/s	618.0 Pkt/s
	Average	6.2 Mbit/s	595.0 Pkt/s
Historical Data			[ ]

Figura 74 Tasa de transmisión para cuatro videos

Cabe destacar que al inyectar tráfico mediante iPERF dicho programa presentó fallas, en repetidas ocasiones no fue capaz de completar la conexión, se capturó la siguiente imagen de dicho evento:

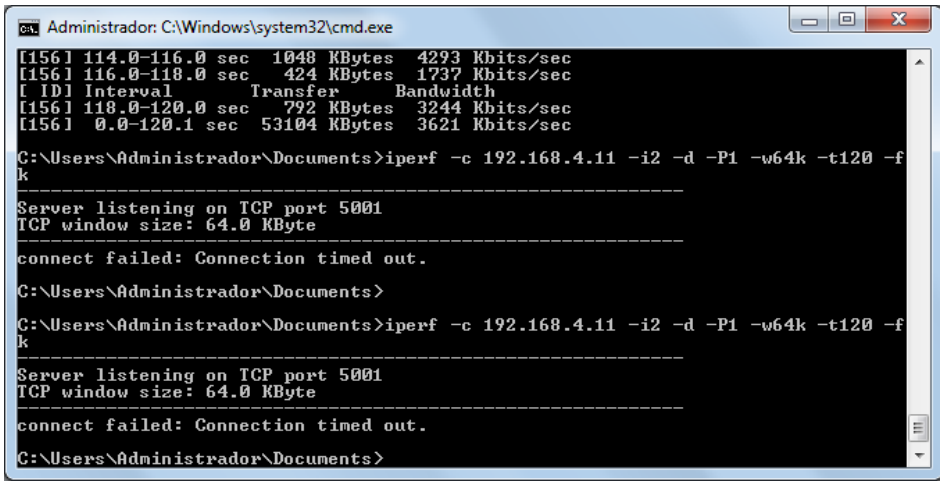


Figura 75 Falló del programa iPERF

6.1.8 Análisis 7. Retardo en el canal de voz inyectando tráfico en el canal de video, mediante la descarga de 5 videos

Una vez comprobado que el tráfico TCP tuvo deificultades de operación se prosiguió por transmitir un video más con el fin de comparar la tasa máxima que podía alcanzar dicho servicio cuando se ocupaban los otros (a pesar de que fallaran).

El video como se esperaba fue completamante distorsionado:

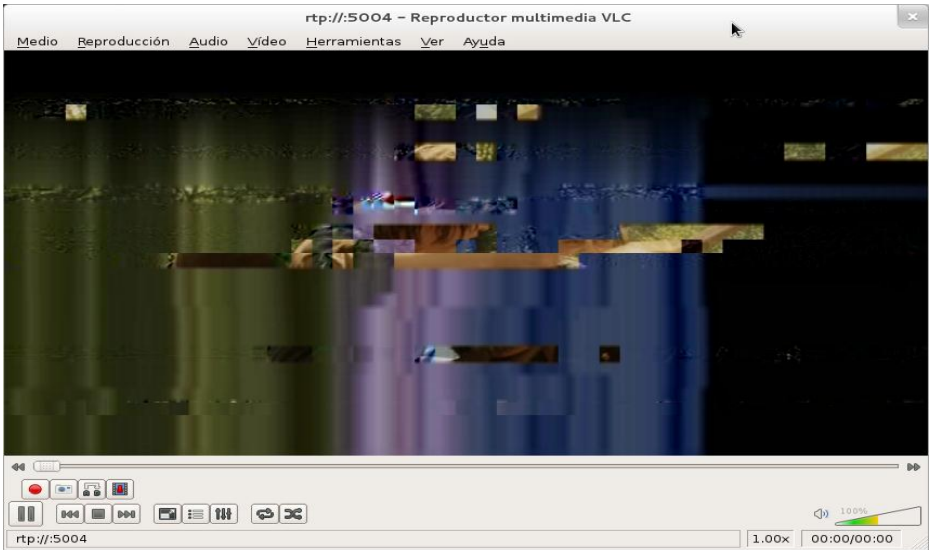


Figura 76 Imagen de cinco videos transmitiéndose

En este caso nTop registró un máximo de 6.4 Mbps en comparación con los 6.5 Mbps alcanzados en un comienzo esto debido al tráfico que se intentó enviar por TCP.

Network Load	Actual	6.3 Mbit/s	605.0 Pkt/s
	Last Minute	6.2 Mbit/s	593.3 Pkt/s
	Last 5 Minutes	0.0 bit/s	0.0 Pkt/s
	Peak	6.4 Mbit/s	618.0 Pkt/s
	Average	6.2 Mbit/s	594.8 Pkt/s
Historical Data			[ ]

Figura 77 Tasa de transmisión para cinco videos

Como observación en todo momento probamos los teléfonos IP a la vez que se probaban los *ping*s, nunca se perdió la comunicación de voz a pesar de la pérdida de paquetes. Lo anterior pudo deberse a la cercanía entre los equipos WiMAX que evitó que se produjera un retraso mayor a 150 ms, por otra parte se comprobó que este servicio es robusto contra la perdida moderada de paquetes.

6.2 Con QoS en el equipo CISCO

Se realizó la simulación únicamente transmitiendo al mismo tiempo 4 videos debido a que en el caso anterior fue con esta cantidad que falló el servicio de tcp (iPerf), además de obtener una velocidad de transmisión constante en el analizador de red que es un indicador de haber saturado el canal.

La imagen de video siguió estando degradada debido a la saturación del enlace; Sin embargo iPerf volvió a funcionar y se presentaron mejoras respecto al retardo y la pérdida de paquetes en el canal de voz. Los resultados se muestran a continuación:

6.2.1 Análisis 1. Retardo en el canal de voz inyectando tráfico en el canal de datos mediante el *software* IPERF e inyectando tráfico en el canal de video, mediante la descarga de 4 videos

Primera prueba:

Ping 192.168.2.11 repeat 1000

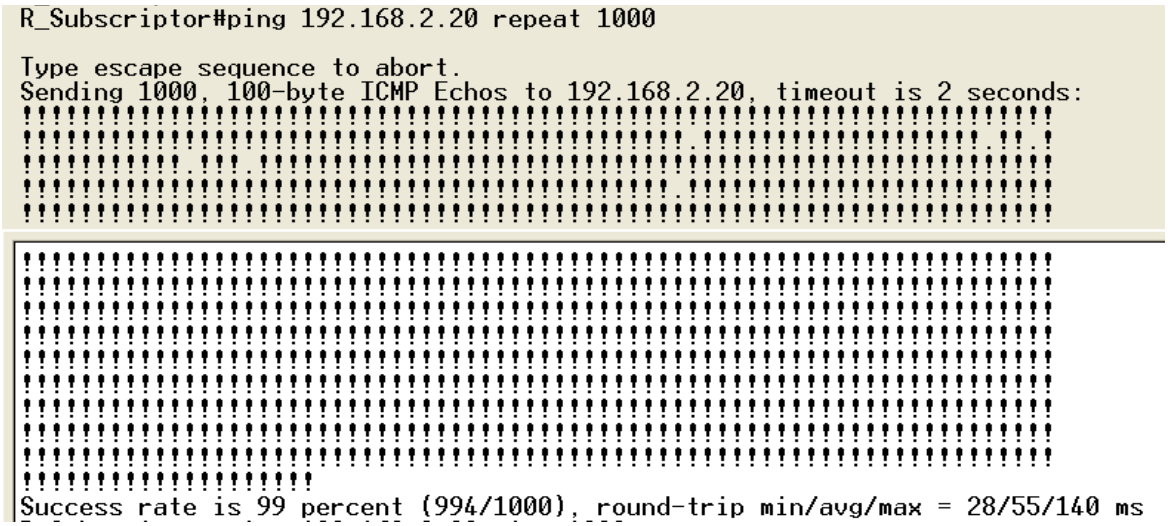


Figura 78 Respuesta ICMP del *Router* (*ping* repetido 1000)

Al comparar esta salida con la mostrada en el análisis 6, se puede observar una gran mejora, solo se pierden 6 paquetes, puesto que la QoS empleada está etiquetando los paquetes, haciendo que se reserve un ancho de banda y una prioridad a cada servicio.

Segunda prueba

Ping 192.168.2.11 size 1000

Se crea un paquete ICMP de tamaño 1000

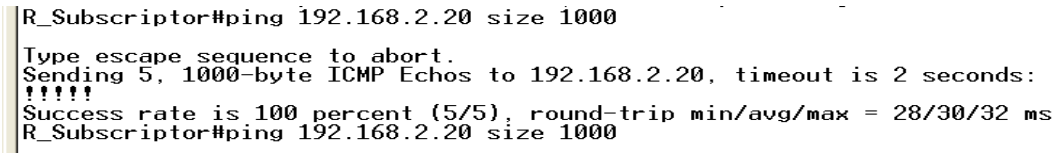


Figura 79 Respuesta ICMP del *Router* (tamaño paquete ICMP 1000)

También esta prueba muestra que ningún paquete ICMP fue perdido, además de que los retrasos de latencia son muy bajos.

Tercera prueba:

Se realizó un *ping* desde una computadora hacia otra computadora.

Se generó un *ping* que se repitió 40 veces.

```
C:\Documents and Settings\mobilelan005>ping 192.168.2.20 -n 40

Haciendo ping a 192.168.2.20 con 32 bytes de datos:

Respuesta desde 192.168.2.20: bytes=32 tiempo=119ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=93ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=92ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=40ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=38ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=97ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=77ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=75ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=123ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=41ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=80ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=90ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=87ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=107ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=74ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=103ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=41ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=30ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=68ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=46ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=85ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=114ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=73ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=101ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=70ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=108ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=68ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=96ms TTL=126
Tiempo de espera agotado para esta solicitud.
Respuesta desde 192.168.2.20: bytes=32 tiempo=87ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=115ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=79ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=73ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=91ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=99ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=119ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=127ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=75ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=114ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=93ms TTL=126

Estadísticas de ping para 192.168.2.20:
    Paquetes: enviados = 40, recibidos = 39, perdidos = 1
    (2% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 30ms, Máximo = 127ms, Media = 84ms
```

Figura 80 Respuesta *ping* de PC de voz

Solo hay un paquete *ping* perdido, los tiempos de latencia siguen en aumento, pero el minino se encuentra en 30ms.

Sin embargo podemos observar a través de nTop que el servicio de video sigue siendo acaparando el canal:

Network Load	**Actual**	5.8 Mbit/s	555.5 Pkt/s
	Last Minute	6.3 Mbit/s	601.7 Pkt/s
	Last 5 Minutes	1.9 Mbit/s	187.3 Pkt/s
	Peak	6.5 Mbit/s	626.4 Pkt/s
	Average	2.6 Mbit/s	249.5 Pkt/s
Historical Data			[ ]

Figura 81 Tasa de transmisión para cuatro videos, con QoS CISCO

6.3 Con QoS de extremo a extremo.

El fin de hacer esta última prueba es por un lado observar que los servicios funcionen de manera correcta y por otro que se respeten las políticas de calidad. Por ello se cambió el uso de iPerf por un servidor de ftp.

El canal de video sólo transmitió un video bajo la limitación de no exceder 3.5 Mbps, el ftp se limitó a una tasa máxima de 100kbps, el canal de voz a 128 kbps, y el resto del canal se dejo libre.

Se capturó una imagen de video correspondiente a este servicio para comprobar su correcto funcionamiento cuando se emite una solo transmisión, posteriormente se intentó volver a saturar el enlace con emisiones paralelas de hasta 3 videos. Operando bajo estas condiciones se analizó la tasa alcanzada por el servicio de video, a su vez se descargó un archivo bajo el servicio de ftp donde el mismo servicio indicó la tasa de la descarga, y finalmente mediante *ping*s se registró el comportamiento de los paquetes en el canal de voz, los resultados son los siguientes:

Imágenes:

Pantalla correspondiente a la emisión de un video:

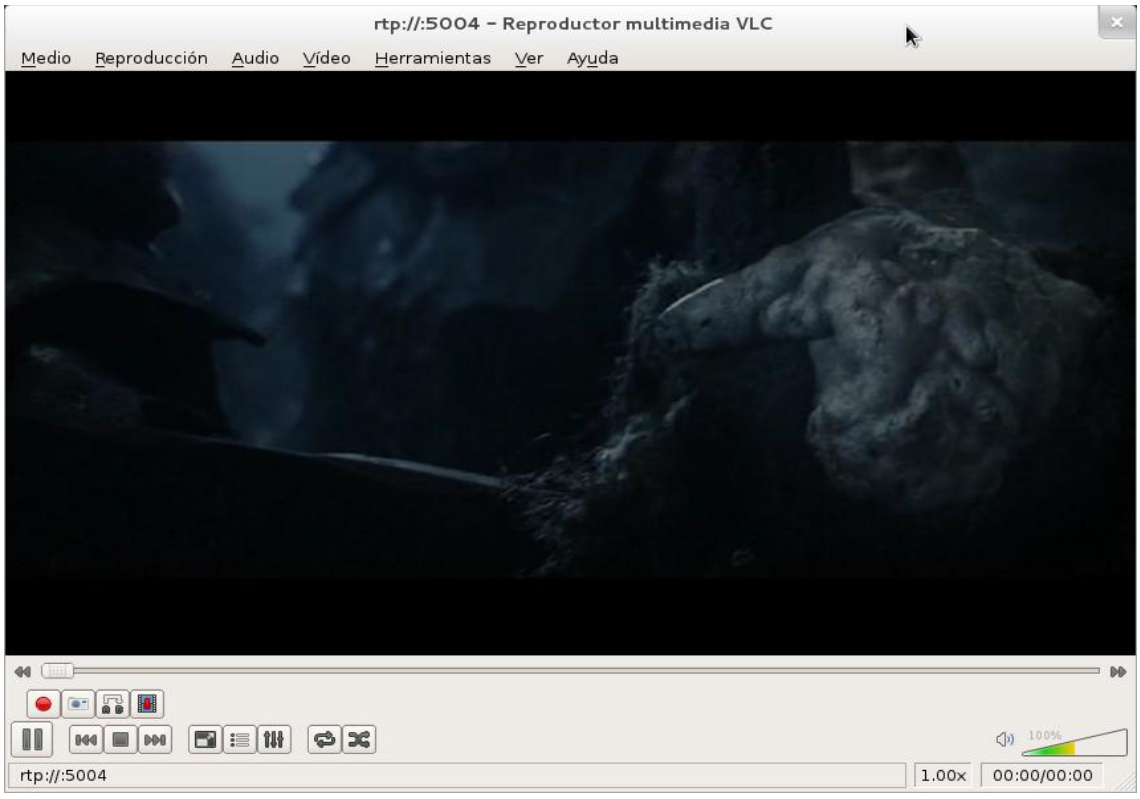


Figura 82 Imagen de un video transmitiéndose con QoS de extremo a extremo

Se prosiguió por emitir un segundo video de manera simultánea, la imagen correspondiente a la emisión de dos videos es:

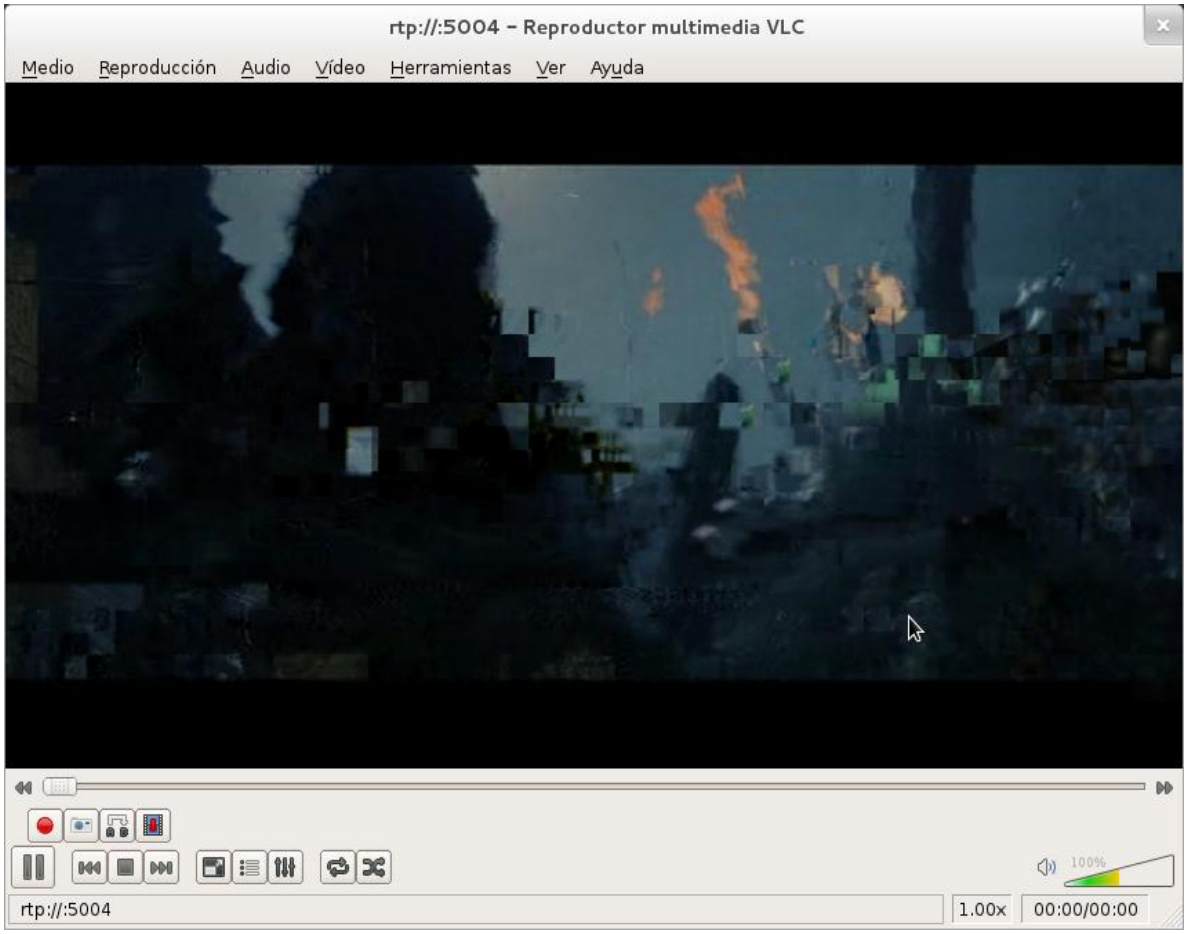


Figura 83 Imagen de dos videos transmitiéndose con QoS de extremo a extremo

Se continuó a emitir un tercer video, la imagen obtenida al hacerlo corresponde a la siguiente figura:

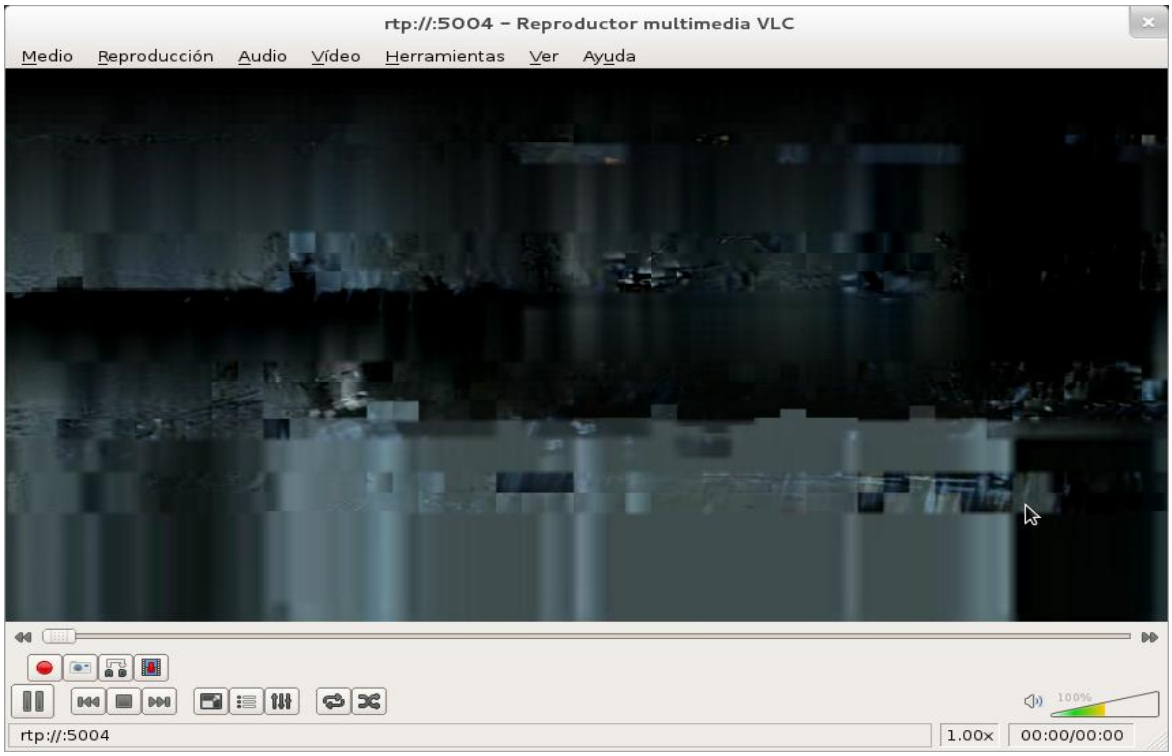


Figura 84 Imagen de tres video transmitiéndose con QoS de extremo a extremo

Antes de activar las políticas de QoS en la BS al transmitir tres videos pudo alcanzarse hasta 6 Mbps en el extremo del cliente de video, ahora los valores registrados para Ntop con tres videos fueron:

Network Load	**Actual**	3.3 Mbit/s	316.5 Pkt/s
	Last Minute	3.3 Mbit/s	317.6 Pkt/s
	Last 5 Minutes	3.3 Mbit/s	317.9 Pkt/s
	Peak	3.4 Mbit/s	324.6 Pkt/s
	Average	3.3 Mbit/s	316.8 Pkt/s
Historical Data			[ ]

Figura 85 Tasa de transmisión para tres videos con QoS de extremo a extremo

El uso de QoS en WiMAX mejoró significativamente el control sobre el tráfico de video.

6.3.1 Análisis 1. Retardo en el canal de voz

Primera prueba:

Ping 192.168.2.11 repeat 1000

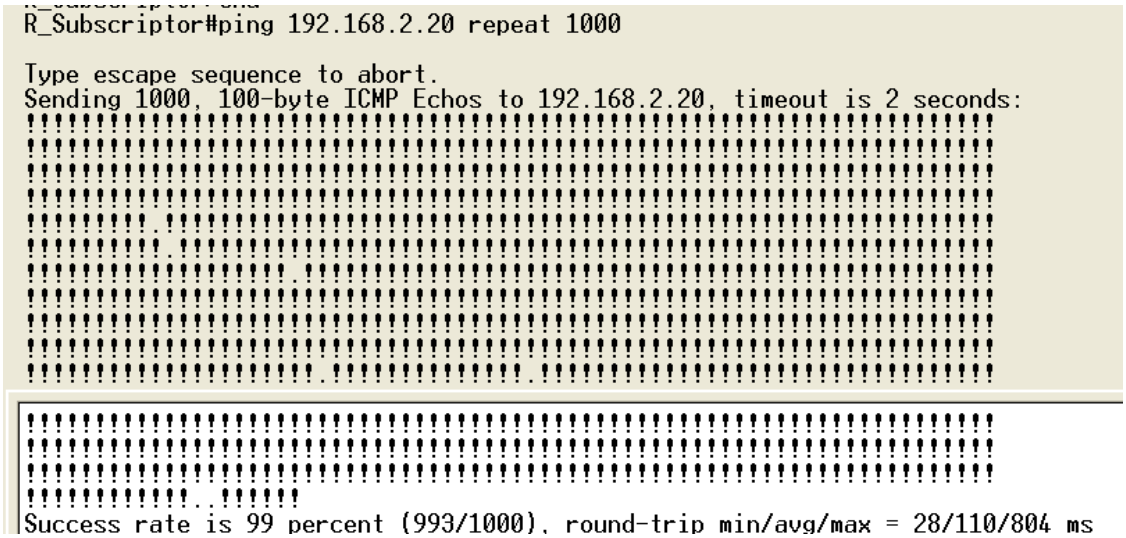


Figura 86 Respuesta ICMP del *Router* (*ping* repetido 1000)

Mejoro notablemente la respuesta de los mensajes ICMP, pero los retardos aumentaron mucho, el máximo estuvo en 804 ms

Segunda prueba

Ping 192.168.2.11 size 1000

Se crea un paquete ICMP de tamaño 1000

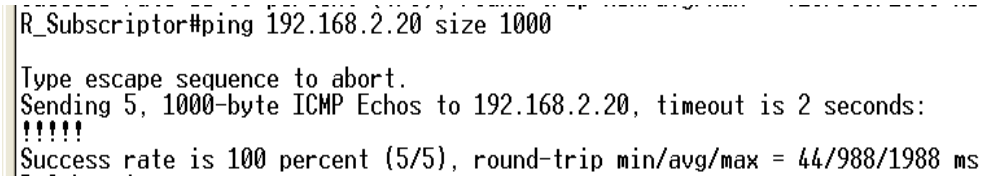


Figura 87 Respuesta ICMP del *Router* (tamaño paquete ICMP 1000)

Los paquetes *ping* fueron respondidos, pero la latencia sigue siendo alta, el máximo esta en 1988 ms.

Tercera prueba:

Se realizó un *ping* desde una computadora hacia otra computadora.

Se generó un *ping* que se repitió 40 veces.

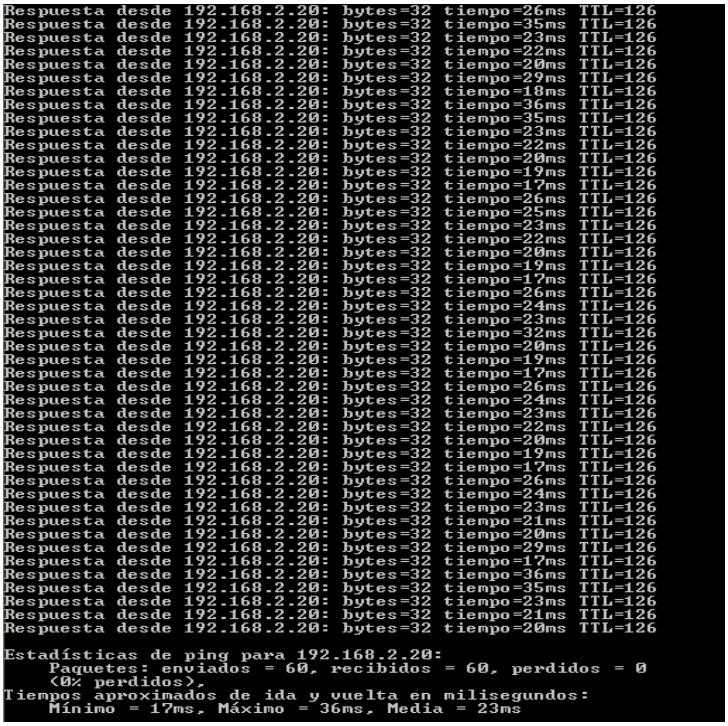


Figura 88 Respuesta *ping* de PC de voz

No hubo pérdidas en los mensajes ICMP, y los retardos fueron bajos, el máximo estuvo en 36 ms.

Respecto al canal de datos se realizó la descarga por ftp, la salida del cliente fue la siguiente:

```
[ulises@localhost ~]$ ftp 192.168.4.11
Connected to 192.168.4.11 (192.168.4.11).
220 (vsFTPd 2.3.4)
Name (192.168.4.11:ulises): ulises
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
227 Entering Passive Mode (192,168,4,11,139,167).
150 Here comes the directory listing.
...
drwxr-xr-x    2 1000     1000         4096 Mar 13 03:46 Documentos
drwxr-xr-x    2 1000     1000         4096 Dec 29 22:58 Escritorio
-rw-rw-r--    1 1000     1000        38720 Mar 09 15:50 FormatosVideo.pdf
drwxr-xr-x    2 1000     1000         4096 Mar 23 02:16 Imágenes
...
226 Directory send OK.
ftp> get FormatosVideo.pdf
local: FormatosVideo.pdf remote: FormatosVideo.pdf
227 Entering Passive Mode (192,168,4,11,180,143).
150 Opening BINARY mode data connection for FormatosVideo.pdf (38720 bytes).
226 Transfer complete.
38720 bytes received in 2.75 secs (14.10 Kbytes/sec)
ftp> close
```

Figura 89 Resultados obtenidos en el cliente ftp

Donde realizando la conversión de la tasa de transmisión en Kbytes a kbits se tiene:

14.10 * 8 = 112 kbps

Comprobándose que FTP (un servicio TCP) pudo operar a una tasa similar a la reservada para su canal a la vez que se intentó saturar el enlace con múltiples videos, además el archivo descargado pudo abrirse sin errores.

CAPITULO VII

Conclusiones

En primer lugar comprobamos la ventaja de trabajar con servicios y equipos certificados bajo estándares de organismos de normalización. Tanto los servicios como los equipos empleados operan bajo el protocolo IP lo cual permitió el intercambio de información entre los hosts y a través de la red. Por otra parte las políticas de QoS se basan en el análisis del encabezado del paquete IP y del encabezado de las tramas MAC, de nueva cuenta estos operan bajo protocolos estandarizados lo que permitió que los equipos procesaran correctamente el flujo de datos.

Respecto a las políticas de QoS comprobamos que un enlace sin ninguna política definida conlleva a la degradación de todos los servicios cuando el canal es saturado. Además de implementarse políticas estas deben existir y coordinarse entre todos los dispositivos de red involucrados en el traslado, por ejemplo en las pruebas realizadas con QoS sólo en el equipo de CISCO se observó una pequeña mejora en el retardo de paquetes en el canal de voz, se redujo la pérdida de paquetes y el tráfico TCP pudo ser transmitido nuevamente; Sin embargo el tráfico UDP seguía consumiendo casi la totalidad del canal. Al usar en conjunto la QoS del equipo WiMAX y del equipo CISCO se obtuvo una mayor mejora en el retardo y la pérdida de paquetes en el canal de voz, la velocidad de descarga en el canal de

datos fue cercana a la deseada y la tasa de transmisión en el canal de video se contuvo exitosamente.

Finalmente comprobamos la importancia de los protocolos de la capa de transporte respecto a la saturación del canal. En principio intentamos saturar el canal mediante tráfico TCP pero este mediante los mecanismo de repuestas ACK y ventanas deslizantes ajustaba su velocidad de transmisión en función de la tasa libre en el canal, incluso disminuyéndola. En cambio UDP envía su información sin importar el estado de la red, ni siquiera el estado de la aplicación receptora.

GLOSARIO:

ADSL Asymmetric digital subscriber line
AM Amplitud Modulada
ARP Address Resolution Protocol

BE Best Effort
BWA Broadband Wireless Access

CID Connection Identifier
CoS Class of Service
CSMA/CD Carrier Sense Multiple Acces Collition Detection

DSCP Differentiated Services Code Point
DTP Dynamic Trunking Protocol

FCS Frame Check Sequence
FFT Fast Fourier Transform
FM Frecuencia Modulada
FTP File Transfer Protocol

HTTP Hypertext Transfer Protocol

ICANN Internet Corporation for Assigned Names and Numbers
ICI Inter Carrier Interference
ICMP Intener Control Message Protocol
ISI Inter Symbol Interference
IEEE Institute of Electrical and Electronics Engineers
IETF Internet Engineering Task Force
IFFT Inverse Fast Fourier Transform
IOS Internetwork operating System
IP Internet Protocol
ISP Internet Service Provider
ITU International Telecommunication Union

LAN Local Area Network
LLC Link Layer Control
LOS Line Of Sight

MAC Media Acces Control
MAN Metropolitan Area Network
MPEG Movie Pictures Expert Group

NLOS Non Line Of Sight
nrTPS non real Time Polling Service

OFDM Ortognal Frequency Division Multiplexing
OSI Open System Interconection
OSPF Open Shortest Path First

PDU Protocol Data Unit
PHS Packet Header Supression
PKM Privacy Key Management

QAM Quadrature Amplitud Modulation
QoS Quality Of Service

RIR Regional Internet Registries
RSVP Resource Reservation Protocol
RTP Real-time Transport Protocol
rTPS real Time Polling Service

SDU Service Data Unit
SFID Service Flow Identifier
SIP Session Initation Protocol
SS Suscriber Station

TCP Transsmision Control Protocol
ToS Type of Service

UDP User Datagram Protocol
URL Uniform Resource Locator

UGS Unsolicited Grant Service

VLAN Virtual LAN
VoIP Voice over IP
VSFTPD Very Secure FTP Daemon

WMAN Wireless Metropolitan Area Network
WAN Wide Area Network
WiMAX Worldwide Interoperability for Microwave Access

REFERENCIAS:

[1] Accesing the WAN, Cisco Networking Academy

[2] Redes de Computadoras, Andrew S Tanenbaum

[3] Network Fundamentals,Cisco Networking Academy

[4] Fundamentals of WiMAX understanding Broadband Wireless Networking

[5] IEEE 802.16-2004

[6] Sistemas de Comunicaciones Electrónicas, Wayne Tomasi

[7] Redline an-100u manual

[8] VLC usage documentation

[9] Redes. Manual de Referencia, Zacker

[10] Redline SUI manual

[11] Data Sheet: Cisco SPA9000 Voice System, Cisco System

[12] Redes Cisco CCNP a Fondo. Guía de estudio para profesionales, ARIGANELLO, ERNESTO / BARRIENTOS SEVILLA, ENRIQUE

[13] Implementing Quality of Service Policies with DSCP, www.cisco.com

[14] Vsftpd --help

[15] Iperf --help

[16] Ntop –help

[17] CCENT/CCNA ICND1 Official Exam Certification Guide 2nd Edition, Wendell Odom

[18] CCENT/CCNA ICND2 Official Exam Certification Guide 2nd Edition, Wendell Odom