UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

PROGRAMA DE MAESTRÍA Y DOCTORADO EN INGENIERÍA
INGENIERÍA ELÉCTRICA – TELECOMUNICACIONES

EVALUACIÓN DE VoIP EN REDES MESH PARCIALES

TESIS
QUE PARA OPTAR POR EL GRADO DE:
MAESTRO EN INGENIERÍA

PRESENTA:
TANIA BERENICE AGUIRRE ENCISO

TUTOR PRINCIPAL:

DR. VICTOR RANGEL LICEA
Facultad de Ingeniería

MÉXICO D.F. AGOSTO 2014

JURADO ASIGNADO:

Presidente: DR. JAVIER GÓMEZ CASTELLANOS

Secretario: DR. RAMÓN GUTIÉRREZ CASTREJÓN

Vocal: DR. VÍCTOR RANGEL LICEA

1er. Suplente: DR. MIGUEL MOCTEZUMA FLORES

2do. Suplente: DR. VÍCTOR GARCÍA GARDUÑO

Lugar donde se realizó la tesis: Ciudad Universitaria, México, D.F.

TUTOR DE TESIS:

DR. VICTOR RANGEL LICEA

_____

FIRMA

DEDICATORIAS

A mis padres Dolores Enciso Murillo y Robertino Aguirre Rodríguez por su cariño, dedicación y entrega, por apoyarme física y moralmente en mi educación, formación todos estos años. Por mostrarme el buen camino a seguir en todos los aspectos.

A mi hijo Diego Emiliano Arteaga Aguirre, por llegar a mi vida y ser mi fuente de inspiración por obtener lo que uno desea y quiere.

A mi hermano Gandhi Aguirre Enciso por su apoyo y nobleza.

A Gabriel Arteaga Hernández, a mis familiares y amigos por todo el apoyo incondicional que me brindaron en todas las etapas de mi vida.

AGRADECIMIENTOS

A la Universidad Nacional Autónoma de México por abrirme las puertas y brindarme el apoyo en la formación tanto profesional como humana, para la realización de mis estudios de posgrado.

Gracias Dr. Víctor Rangel Licea por su comprensión, paciencia y dedicación, pero sobre todo por ser mi guía en la realización de este trabajo.

Al profesor Dr. Zbynek Kocur por brindarme herramientas y conocimientos para desarrollar pruebas.

A la Universidad Técnica Checa en Praga, por darme un espacio de trabajo dentro de sus aulas.

A DGAPA-UNAM por brindar el apoyo para la realización de esta tesis a través del proyecto PAPIIT IN114713 “Diseño y análisis de algoritmos de calendarización en redes LTE y WiMAX”.

A CONACYT por brindar el apoyo para la realización de este trabajo a través del proyecto 105279 “Diseño de técnicas de reservación de capacidad de redes BWA móviles.

A la CEP por el apoyo económico brindado, para la realización de una estancia académica.

RESUMEN

En esta tesis se explica un bosquejo general del estándar 802.11, lo que son las redes ***mesh***, sus dos clasificaciones, así como su estándar 802.11s. Se describe lo que es la VoIP y la implementación de este tipo de servicio.

Esta tesis muestra el estudio de una implementación de red ***mesh*** parcial con diferentes escenarios, basados en VLAN's y sin éstas, siendo importante evaluar si se tienen beneficios o no con este tipo de redes virtuales.

La tolerancia a fallos y recuperación de este tipo de sistemas, son también enfoque de esta tesis para poder realizar la evaluación de la red propuesta.

ÍNDICE

ÍNDICE DE FIGURAS

Capítulo 2

Capítulo 3

Capítulo 4

Capítulo 5

ÍNDICE DE TABLAS

Capítulo 2

Capítulo 4

Capítulo 5

CAPÍTULO 1

Introducción

1.1. Antecedentes

El servicio de Voz sobre el Protocolo Internet (VoIP)[1] está rápidamente trasformando el camino que nosotros usamos para las comunicaciones de voz, siendo una aplicación muy popular e importante sobre Internet por sus características de bajo costo y conveniencia.

VoIP es usado bastantemente por una gran variedad de tipos de consumidores, que obtienen gratuitamente llamadas de largas distancias sobre Internet para soluciones empresariales a gran escala. El objetivo de la gran mayoría de las empresas es reemplazar completamente la inherente infraestructura de la telefonía analógica y así reducir los costos de comunicación significantemente.

Conseguir llamadas con calidad comparables a la Red Telefónica Pública Conmutada (PSTN) es el reto de esta tecnología, por lo que el despliegue de VoIP requiere de cuidadosos análisis de los requerimientos de la red.

Las redes de computadoras están evolucionando y hoy en día se tiene un gran impacto en el mundo, debido a que por medio de éstas nos es posible el intercambio de información. La demanda de usuarios en las redes es grande y la gran mayoría busca rapidez y calidad en el envío de su información, así como un bajo costo por los servicios brindados.

Por otro lado, implementar una red inalámbrica muchas veces puede salir muy costoso si no se tiene una buena planeación para su construcción. En el caso donde las redes alámbricas no son fáciles de instalar o el despliegue de éstas son muy costosas, las redes inalámbricas ***mesh*** *(malla)* pueden ser un camino atractivo para estos factores o simplemente para extender las coberturas de red en zonas de difícil acceso.

1.2. Justificación

A través de las redes ***mesh*** se puede aumentar la cobertura sin incrementar el costo de éstas. Se puede tener comunicación en zonas con acceso difícil, es decir, en la industria existen zonas las cuales han sido aisladas debido a cuestiones de seguridad, en donde es de vital importancia tener comunicación hacia el exterior y por el escaso número de usuarios que requieren de los servicios. Por consiguiente, las redes inalámbricas ***mesh*** son una excelente opción tanto en entornos exteriores como interiores.

[1] La lista de términos se encuentra en el glosario de la página 116.

1.3. Objetivos

Evaluar parámetros del rendimiento de una red de VoIP ***mesh*** parcial, implementada con equipos *RouterBoard* con el sistema operativo *RouterOS* de la compañía *MikroTik*, configurada de tal forma que pueda soportar, la transmisión y recepción de VoIP, video y datos, haciendo uso de redes virtuales (VLAN's) para la separación de tráfico en la red.

1.4. Contribuciones

Esta tesis muestra un estudio del comportamiento dinámico de VoIP, en una red ***mesh*** parcial que soporta datos y video a la vez. Contiene además conceptos necesarios para la comprensión del funcionamiento, transmisión y evaluación de VoIP. Así como características importantes de las redes Wireless Distribution System (WDS) ***mesh*** parciales.

Se pretende proponer un marco de referencia para la implementación, estudio y evaluación de futuros proyectos que permitan analizar a fondo el comportamiento de las redes de VoIP tipo ***mesh.***

1.5. Estudios Relacionados

Entre algunas publicaciones de la IEEE que implementan de alguna forma VoIP en redes inalámbricas ***mesh*** son:

En el estudio "Infrastructure Dependent Wireless Multicast Over 802.11n WLAN" [1], se implementan 3 nodos para la realización de las pruebas, los cuales utilizan tarjetas inalámbricas 802.11n, uno de los nodos posee el sistema operativo *RouterOS* en una computadora de escritorio, por la flexibilidad que este sistema ofrece con respecto al encendido y apagado de ciertas antenas que utilizan. Además tienen la habilidad de cambiar el esquema de modulación y codificación (MCS, por sus siglas en ingles), usado para transmitir datos *multicast* de forma que el rango de datos en la capa física (PHY), pueda satisfacer las necesidades de los peores receptores y pueda cubrir grandes rangos.

MCS nos permite manipular fácilmente parámetros como: tipo de modulación, rango de código y rango de datos. Sin embargo, si un rango de datos PHY es usado, el Packet Error Rate (PER) aumenta. En este estudio se presenta la medición del PER con la trasmisión de video *multicast*.

Este estudio se enfoca en dividir el área de cobertura a la mitad, a través de dos antenas conectadas a la misma tarjeta inalámbrica transmitiendo la misma información resultando en un bajo PER. Por consiguiente, este estudio concluye que dentro de su investigación empírica, se muestra que la disposición de la infraestructura puede ser la responsable del suministro de una mejor calidad del canal para los receptores.

El estudio también destaca una ventaja que en diferentes situaciones puede ser todo lo contrario, los adaptadores de red inalámbricos pueden diferir de sus capacidades llegando a ser quasi-confiables, como se indica en el artículo [2] "Quasi-reliable *multicast*". Por tanto, entre los nodos la confiabilidad puede verse afectada, sin embargo, en este estudio se obtuvo una buena calidad en el canal.

Aunque el enfoque de esta tesis no es la parte de modulación o codificación, en el estudio llevado a cabo en [1], se dió a conocer la importancia del PER dentro de este tipo de redes. El estudio muestra que no siempre influye la separación que existe entre los nodos, o que las tarjetas inalámbricas en el mismo estándar asegura la confiabilidad en la red entre los nodos vecinos, ocurriendo alteraciones dentro del PER que en ocasiones pueden ser buenas o todo lo contrario.

Tomando en consideración el uso de tarjetas inalámbricas del mismo tipo, en el estándar 802.11, (con el mismo chipset), se implementó dentro de la presente tesis las mismas características de tarjeta de red inalámbrica 802.11g, para tener un comportamiento en cuanto a confiabilidad de los nodos homogéneos. Y de esta forma poder realizar una evaluación dinámica solamente de los parámetros deseados.

En el siguiente estudio, "Simulative Analysis of the Hybrid Wireless Mesh Protocol (HWMP)" [3], se detalla una evaluación simulada de los modos permitidos del protocolo HWMP (reactivo, proactivo y proactivo forzado) para la obtención de conclusiones acerca de su comportamiento dinámico y conveniencia para ambientes específicos. Se realizó la simulación de este protocolo HWMP y sus diferentes modos a través del simulador NS-2 v2.9 mostrando sus ventajas y desventajas.

La conclusión a la cual llega este artículo, es que el modo reactivo es una buena y razonable opción para un escenario con patrones de tráfico arbitrarios, o con una fracción pequeña de tráfico del nodo raíz. Mientras éste puede ser usado en cualquier otro escenario, incluso con tráfico del nodo raíz al 100%, los modos proactivo HWMP muestra sus ventajas más con respecto a la relación de entrega de paquetes y ruta optima en escenarios con un incremento de tráfico del nodo raíz.

Si la mitad del tráfico es proveniente de la raíz, el modo proactivo simple es recomendado o si más de la mitad del tráfico es del nodo raíz, se recomienda modo proactivo forzado. Sin embargo, la red tiene que ser capaz de llevar un alto rango de selección de rutas si se utiliza modo proactivo.

La tesis propuesta aquí da un bosquejo del comportamiento de VoIP utilizando métrica como entrega de paquetes, pérdida de paquetes, entre otros. Este tipo de protocolo es utilizado en redes tipo ***mesh*** totales, en donde se utiliza la interface inalámbrica ***mesh*** ya sea de tipo reactiva o proactiva. Sin embargo, la red propuesta en esta tesis se enfoca a utilizar interface inalámbrica puente (bridge), en conjunto con la tecnología WDS entre sus AP's, lo cual define la innovación la presente tesis.

1.6. Estructura de la Tesis

Capítulo 2

Este capítulo describe los conceptos básicos para poder entender el estándar 802.11, se desarrolla una explicación de lo que es el estándar de redes ***mesh*** 802.11s, la estructura del *frame* y el control de acceso al medio. En la segunda parte de este capítulo se describe la tecnología de VoIP, componentes, ventajas, códecs y protocolos que interactúan de forma directa con el estándar 802.11s.

Capítulo 3

En este capítulo se explica lo que son las redes ***mesh***, los dispositivos o componentes que lo forman y sus ventajas. Además se explican los conceptos de redes ***mesh*** totales y redes ***mesh*** parciales. Por otro lado, se desarrolla lo que es WDS y la utilización de redes WDS con interface ***mesh*** y con interface puente. Se explica lo que es el protocolo Hybrid Wireless Mesh Protocol (HWMP) tanto estandarizado como propietario, así como el Protocolo de Tiempo Real (RTP, Real Time Protocol) o Protocolo de Trasporte de Tiempo Real (SRTP, Real Time Transport Protocol).

Capítulo 4

En este capítulo se desarrolla la propuesta de la infraestructura, detalla los componentes o dispositivos necesarios para implementar la red inalámbrica ***mesh*** parcial, así como las configuraciones en los equipos *RouterBoards*, servidor *Asterisk* y servidor de video.

También se muestra un estudio realizado en el entorno donde se implementó la red inalámbrica, usando un analizador de espectros para tener una evaluación lo más acercada a lo ideal.

Capítulo 5

Muestra los resultados obtenidos del análisis de VoIP en la red ***mesh*** parcial con todos los escenarios implementados, esquemas y diagramas (con y sin utilizar VLAN´s). Dentro de los parámetros obtenidos fueron: *jitter*, *delta*, total de paquetes RTP transmitidos y/o recibidos, utilización de los enlaces inalámbricos WDS o utilización en VLAN's, paquetes perdidos y desfasados por errores de secuencias, tiempo de inestabilidad de la red debido a errores de secuencia, etc.

CAPÍTULO 2

Conceptos Básicos

La utilización hoy en día de Wireless Local Area Network (WLAN) es de uso más frecuente y cada vez más veloz, eficaz y seguro. El funcionamiento de WLAN es similar en muchos aspectos al de Local Area Network (LAN) tradicionales. Una gran variedad de aplicaciones son posibles gracias a estos tipo redes como son: voz, video, datos.

El estándar que rige a las redes WLAN es el IEEE 802.11 y describe cómo es que los dispositivos inalámbricos pueden comunicarse. En este capítulo se da un bosquejo general del protocolo, su diseño y sus versiones que han surgido a / b / g. Así como la estandarización ***mesh*** para el protocolo 802.11. El cuál es el denominado IEEE 802.11s.

En la segunda parte de este capítulo se explica lo que es VoIP, como funciona, los tipos de códec de audio que existen, así como los parámetros que afectan a la VoIP en las redes.

2.1. Estandarización del Protocolo IEEE 802.11

2.1.1. Definición del protocolo

La arquitectura de la norma IEEE 802.11x se centra en definir los niveles más bajos del modelo OSI, la capa física y la subcapa de Control de Acceso al Medio (MAC). En junio de 1997 fue ratificado el estandar IEEE 802.11, el cual alcanzaba una velocidad de 2Mbps. En el año 2007 se tuvo la última publicacion del estandar.

2.1.2. Descripción Breve

Dentro de la capa física en el estándar IEEE 802.11 se encuentra la luz infrarroja y el Espectro Disperso (SS, Spread-Spectrum), que es definido por la distribución de la potencia de la señal sobre una banda de frecuencias. Espectro disperso posee dos técnicas que utilizan la banda de 2.4GHz y son: Espectro Disperso por Secuencia Directa (DSSS, por sus siglas en ingles), aunque también contempla la opción de Espectro Expandido por Salto de Frecuencia (FHSS, por sus siglas en ingles).

Dentro del DSSS el transmisor utiliza la función XOR, para la multiplicación de cada bit de información por una cadena o código de 11 chips.

El código se envía al receptor para que pueda decodificar correctamente, al recibir la secuencia el receptor hace uso de la función XOR para multiplicar por el código de 11 chips y así descifrar la información que fue enviada.

En el FHSS la portadora es invocada a saltar de frecuencia de acuerdo a una secuencia pseudoaleatoria, se hace que la portadora se transmita en una frecuencia durante un intervalo establecido, y después la frecuencia es cambiada siguiendo el mismo patrón de transmisión, durante el tiempo de operación.

El SS es resistente a las intercepciones (sin código el mensaje no puede ser decodificado) e interferencias (si la señal llego al receptor sin ser multiplicada por el código de 11 chips este es eliminado).

El estándar 802.11 define dos mecanismos de acceso al medio, los cuales son:

El método MAC es mediante escucha pero con prevención de colisión, CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

Para que varios usuarios tengan disponibilidad en un canal de comunicación de forma simultánea en la WLAN, es utilizado el Acceso al Medio por División de Código (CDMA) y el Multiplexaje por División de Frecuencias Ortogonales (OFDM).

En CDMA, esta técnica de acceso múltiple los usuarios utilizan la totalidad del espectro disponible durante todo el tiempo, gracias a la ortogonalidad de los códigos. En la figura 2.1 se muestra la caracterización de Acceso Múltiple por División de Código.

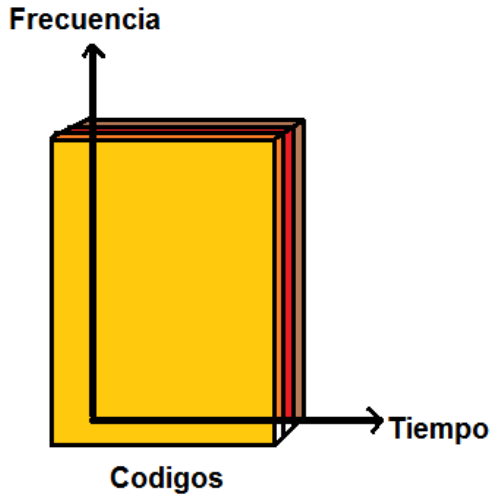


Figura 2.1. Acceso Múltiple por División de Código (CDMA).

En OFDM cada uno de los usuarios transmite su información segmentada, a través de un conjunto de portadoras o canales y la cantidad de portadoras que se le asignan, es proporcional a la cantidad de información que envía. En la figura 2.2 se muestra la caracterización de OFDM con subportadoras.

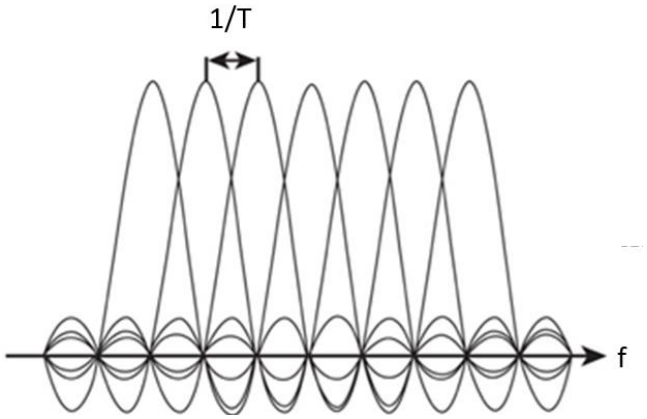


Figura 2.2. Multiplexaje por División de Frecuencia Ortogonal (OFDM).

2.1.3. Diseño de red 802.11

Una estación o STA, es un estándar 802.11 (compatible con la MAC y la capa física), constituye una entidad básica en las redes 802.11. La red más elemental 802.11 es el llamado Conjunto de Servicios Básicos (BSS, por sus siglas en ingles), puede ser formado usando dos estaciones. Si la estación provee el servicio de integración a otras estaciones, ésta es referida como un Punto de Acceso (AP). Si un AP está presente en un BSS, éste es referido como un BSS de infraestructura.

Existen AP que ofrecen acceso al Sistema de Distribución (DS, Distribution System). La DS proporciona servicios que son necesarios para comunicarse con dispositivos fuera de las propias BSS de las estaciones. Los DS permiten a los AP´s unir múltiples BSSs para formar un Conjunto de Servicios Extendido (ESS, Extended Service Set). Dentro de un ESS, las estaciones pueden moverse desde un BSS a otro.

2.1.4. Protocolo de comunicaciones IEEE 802.11a

El IEEE ratificó en julio de 1999 el estándar 802.11a con una modulación QAM-64 y la codificación OFDM, la cual alcanza una velocidad de hasta 54Mbps en la banda de 5GHz, actualmente es la menos congestionada, y por ahora con menos interferencias. Pero tiene un alcance limitado a 50 metros, lo que implica tener que montar más AP's que si utilizáramos el estándar 802.11b para cubrir la misma área, con el coste adicional que implica.

2.1.5. Protocolo de comunicaciones IEEE 802.11b

En el año de 1999 fue aprobado el estándar 802.11b, siendo una extensión del 802.11 para WLAN empresariales, con una velocidad de 11Mbps y un alcance que puede llegar a superar los 100 metros con una potencia de emisión de 100mW, que al igual que Bluetooth y Home RF. También emplea la banda de Instrumental Científico y Médico (ISM) de 2.4GHz, pero en lugar de utilizar FHSS, utiliza DSSS.

El 802.11b permite tener una mayor velocidad, pero con una seguridad menor, y puede llegar a los 100 metros de cobertura, suficientes para un entorno de oficina o residencial.

2.1.6. Protocolo de comunicaciones IEEE 802.11g

La IEEE aprobó en el año 2003 el estándar 802.11g, para competir con los otros estándares, que prometen velocidades mucho más elevadas pero que no son compatibles con los equipos 802.11b ya instalados [4], aunque puede coexistir en el mismo entorno debido a que las bandas de frecuencias que emplean son distintas. Este estándar es el más utilizado hoy en día por los numerosos dispositivos que lo soportan, por la eficiencia que han mostrado en sus implementaciones y la capacidad de alcanzar una velocidad de 54Mbps.

La versión g opera dentro del rango de frecuencias de 2.4 a 2.483 GHz. En la figura 2.3 se puede observar la distribución de los canales del estándar.

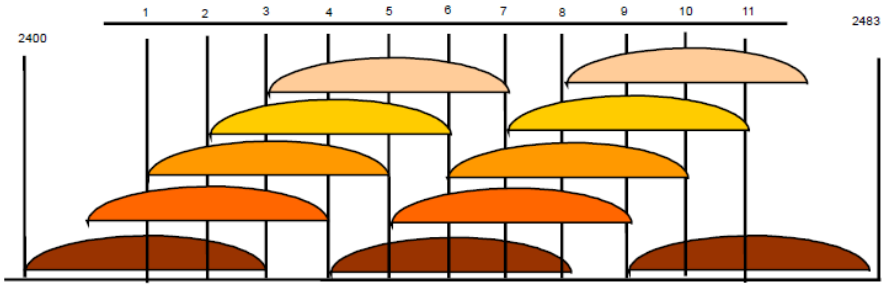


Figura 2.3. Distribución de los canales del 802.11 g [5].

En la tabla 2.1 se muestran algunas de las características de los canales del estándar 802.11g.

Características de los canales del estándar IEEE 802.11 g	
Número total de canales	11 canales
Tamaño de los canales	22MHz
Espacio entre frecuencias centrales	5MHz
Canales no traslapables	3 (1, 6 y 11)

Tabla 2.1. Características de los canales del estándar 802.11g.

En la tabla 2.2 se muestra su distribución de canales.

Distribución de canales		
Canales	**Frecuencia [GHz]**	
CH 1	**2.412**	**No traslapable**
CH 2	2.417	Con interferencia
CH 3	2.422	Con interferencia
CH 4	2.427	Con interferencia
CH 5	2.432	Con interferencia
CH 6	**2.437**	**No traslapable**
CH 7	2.442	Con interferencia
CH 8	2.447	Con interferencia
CH 9	2.452	Con interferencia
CH 10	2.457	Con interferencia
CH 11	**2.462**	**No traslapable**

Tabla 2.2. Distribución de canales del estándar 802.11g.

El tipo de modulación que maneja este estándar es OFDM y DSSS, con un radio de cobertura en interiores de 35m y coberturas exteriores de 140m. Tienen una tasa de transmisión mínima de 11Mbps a 54Mbps como máxima.

2.1.7. Protocolo de comunicaciones IEEE 802.11 s

La implementación de este estándar trabaja con la capa física ya existente en los estándares 802.11 a/b/g/n/e, además de incluir extensiones para la formación de topologías, que hacen posible la autoconfiguración de las redes inalámbricas ***mesh***.

Las redes Inalámbricas ***mesh*** 802.11, facilitan dos niveles de infraestructura: uno donde el nivel más bajo brinda el acceso a los clientes al nivel superior y a la estructura de la red inalámbrica, y el otro es el nivel superior en donde es integrada la red de retorno (*blackhaul*) que facilita las puertas de enlace, como es el caso de Internet u otras redes.

Para superar las limitaciones de comunicación con un solo salto, los paquetes de datos necesitan recorrer la red a través de múltiples saltos y los dispositivos inalámbricos, tienen la funcionalidad de llevarlo a cabo.

Desde el año 2004 el Task Group S ha estado desarrollando una enmienda, para el estándar 802.11 cuyo objetivo es abordar exactamente la necesidad antes mencionada, para la comunicación multisalto. Además de introducir el direccionamiento del *frame* inalámbrico y capacidades de enrutamiento en la capa MAC, la enmienda 802.11s trae nueva interconexión y seguridad.

La selección del camino se utiliza para referirse a la dirección MAC, basada en enrutamiento y para diferenciarlo del ruteo IP convencional.

Dado que el actual estándar [6] no define los procedimientos necesarios para la implementación WDS, muchas implementaciones multisalto 802.11 no interoperan. El estándar 802.11s además de ayudar en la interconexión inalámbrica de BSS's, también permite un nuevo tipo de BSS, la denominada ***mesh*** BSS (MBSS).

2.1.7.1. Estructura del *frame* en el estándar 802.11s

La categorización que se le ha dado a los *frames* en la actual 802.11 son: datos, control y administración tal y como se ha descrito en un estudio del estándar 802.11s denominado "IEEE 802.11s: The WLAN ***mesh*** Standard", [7] del cual se realizara una breve explicación al respecto.

Los dispositivos utilizan administración de *frames* para establecer, organizar y mantener una red WLAN y la conexión local. El protocolo IEEE 802.11s extiende datos y administración de *frames* para un campo adicional de control ***mesh***.

Las *frames* de datos transportan datos de capa superior. Los *frames* de control son usados para confirmaciones (acks) y reservaciones. El campo de control ***mesh*** consiste de un campo ***mesh*** Time To Live (TTL), un número de secuencia ***mesh***, un campo de banderas ***mesh***, y un campo de ampliación posible de la dirección ***mesh***. El TTL y el campo de número de secuencia son utilizados para la prevención de ciclos. Cuando las estaciones ***mesh*** se comunican sobre un solo salto, sus *frames* no poseen campos de control ***mesh***.

El campo de bandera ***mesh*** indica la presencia de una dirección MAC adicional en el campo de control ***mesh***. La extensión de la dirección permite seis campos de direcciones en un *frame* ***mesh***, esto es útil cuando el origen y el destino del *frame* no son parte de la red ***mesh***, pero son próximos por estaciones ***mesh.***

La extensión a seis direcciones permite un enrutamiento proactivo. El enrutamiento proactivo divide un camino en dos rutas distintas, para simplificar la selección del camino. En la extensión de campo de dirección se permite la adición de tres direcciones, en lugar de sólo dos. La razón de esto es que en el estándar los *frames* de administración tienen únicamente tres direcciones. De ahí que, en el caso de *frames* de administración ***mesh*** de múltiples saltos, la dirección 4 está incluida en el campo de control ***mesh*** y no en el encabezado de la trama estándar.

La siguiente figura 2.4 se muestra el formato del *frame* de datos, en el estándar 802.11s y el despliegue del campo de control ***mesh***.

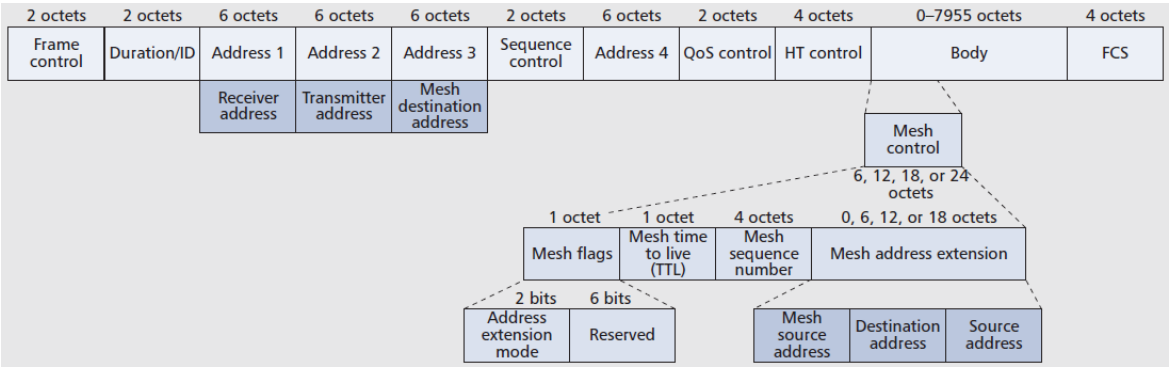


Figura 2.4. Formato del *frame* de datos en el estándar 802.11s y el despliegue del campo de control ***mesh*** [7].

2.1.7.2. Control de acceso al medio

Debido al reenvío multisalto, los flujos equivalentes consumen diferentes cantidades de recursos en las redes de acuerdo con la distancia del nodo portal. Por lo tanto, los recursos disponibles deben estar asignados en la red de una manera que sea eficiente, para un área de cobertura determinada.

En la capa MAC se realizan pruebas de sincronización y la optimización del Acceso al Canal Distribuido Mejorado (EDCA, Enhanced Distributed Channel Access), en donde se asignan los recursos de la red ***mesh*** con respecto a la capacidad y el tiempo.

La sincronización es una característica opcional para los Puntos ***Mesh*** (MPs, Mesh Points), con éste cada MP actualiza sus tiempos con etiquetas de tiempo e información recibida de los *beacons*, y respuestas probadas de otros MPs, manteniendo de este modo un tiempo común ***mesh***.

Para el acceso al medio, las estaciones ***mesh*** implementan la Función de Coordinación ***Mesh*** (MCF, Mesh Coordination Function). MCF consiste de un esquema obligatorio y un esquema optativo. Para la parte obligatoria, MCF depende de un protocolo basado en la contención conocido como EDCA, que en sí es una variante mejorada de la norma 802.11 Función de Coordinación Distribuida (DCF, Distributed Coordination Function). Utilizando DCF, una estación transmite un solo *frame* de longitud arbitraria. Con EDCA, una estación puede transmitir múltiples *frames* cuya duración de transmisión total no puede exceder la llamada “limite de oportunidad de transmisión” o (TXOP limit).

2.2. VoIP

VoIP es la forma de llevar las llamadas de voz sobre una red IP, o en otras palabras es una tecnología que encapsula la voz en paquetes para poder transportarla en una red de datos, siendo parte la digitalización y paquetización de la voz. La telefonía IP utiliza los estándares de VoIP para crear un sistema de telefonía, donde características de nivel superior, tales como enrutamiento avanzado de llamadas, correo de voz, centros de contacto, entre otros, pueden ser utilizados.

2.2.1. Beneficios de VoIP

Entre los que más se destacan son:

- Mejor uso de acho de banda. De forma tradicional la voz requiere un circuito dedicado de 64kbps para cada llamada de voz, sin embargo llamadas de VoIP pueden utilizar menor ancho de banda. Cabe recalcar que el ancho de banda no es consumido cuando una llamada no es realizada.
- Ahorro de costes de integración en la red de datos. Los cargos para la comunicación de voz entre oficinas pueden ser evitados mediante el enrutamiento de voz a través de líneas de datos existentes.
- Integración en dispositivos más allá de teléfonos.

2.2.2. Componentes básicos de VoIP

Dentro de los componentes básicos de una red VoIP existen tres fundamentales:

- Terminales. Son los dispositivos que utilizaran los usuarios para comunicarse, implementado tanto en hardware como en software, realizan las funciones de los teléfonos tradicionales.
- Gateways. De forma transparente se encargan de conectar las redes de VoIP con las redes de telefonía tradicional.
- Gatekeeper. Son el centro decisivo de las redes de VoIP. Se encarga de realizar tareas de autenticación de usuarios, control de admisión, control de ancho de banda, encaminamiento, servicio de facturación y temporización.

2.2.3. Sistema de VoIP

A través de un par de métodos de codificación y decodificación de voz, es posible transmitirla a través del protocolo Internet. En el punto transmisor, un módulo de grabación captura la voz, para después utilizar el método de Modulación por Codificación de Pulsos (PCM, Pulse Code Modulation).

El tráfico de voz es generalmente transportado sobre el Protocolo de Datagramas de Usuario (UDP, User Datagram Protocol). Sin embargo, UDP no soporta secuencias y éstas son muy importantes para el decodificador. Por lo tanto, el protocolo RPT, es utilizado en la parte superior de éste.

En la parte de recepción final, después de despojarse de cabeceras de protocolo, los *frames* de voz son colocados en un *búfer* (espacio de memoria) de *jitter*. El decodificador requiere que los intervalos de los datos que llegaron sean regulares.

No obstante, la red subyacente no puede garantizar su entrega justo a tiempo, por lo tanto el *búfer* del *jitter* juega un rol crucial en VoIP. El decodificador toma ***frames*** de datos de éste y decodifica a PCM para posteriormente ser reproducido.

2.2.4. Paquetización de VoIP

El tráfico de voz debe ser paquetizado a medida que atraviesa la red IP. El sonido es detectado por primera vez utilizando un micrófono en el auricular. Para convertir la voz analógica a un formato digital, se hacen muestras de frecuencia y amplitud de la onda analógica. En el proceso de muestreo se toma un instante de la señal en un punto dado en el tiempo.

A la altura de la amplitud de cada muestra se le asigna un valor numérico, por medio de un proceso llamado cuantificación. Este valor numérico se representa entonces como una secuencia de dígitos binarios (generalmente 8) a través de un proceso llamado codificación.

El teorema de muestreo de Nyquist establece que, la onda analógica debe ser muestreada a un rango del doble de frecuencia del canal:

$$fs = 2 \text{ (rango frecuencia)}$$

Donde:

- fs es la frecuencia del canal.

Una llamada de voz requiere un canal de 4 kHz (4000 Hz), suponiendo una rango de este valor, se tendrá una tasa de 8000 muestras por segundo. A cada muestra se le asigna un valor de 8 bits para representar la altura de amplitud en el momento del muestreo. Por lo tanto, un canal dedicado de 64.000 bits (8-bits x 8000 muestras por segundo) fue tradicionalmente requerido para una llamada de voz (siendo un DS0 de 64kbps).

El proceso de codificación de una señal analógica en formato digital se controla mediante un códec (codificador-decodificador). El códec por lo general proporciona un nivel de compresión.

2.2.5. Códecs

Son utilizados para convertir una senal analogica a digital. Como sabemos la voz provienen de una señal analogica y tiene que llevar un proceso para ser convertida en digital. El códec usualmente provee un nivel de compresion, la eficiencia de la compresion varia con el códec que se utilice. Por otro lado, cuando existe una mayor compresion generalmente la calidad del sonido se degrada. Algunos codecs son:

- G.711 utiliza 64kbps para una llamada de voz.
- G.726 utiliza 32,24, o 16 kbps por una llamada de voz.
- G.728 utiliza 16kbps para una llamada de voz.
- G.729 utiliza 8kbps para una llamada de voz.

2.2.5.1. Códec G.711

El estándar G.711 de la ITU-T [8] se emplea en la codificación de señales PCM (este códec también se conoce como PCM), implementando la ¨ley μ¨ utilizada en los Estados Unidos, Canadá y Japón, la ¨ley A¨ es utilizada en el resto del mundo. Obteniendo una señal digital de 64kbps, donde muestrea la señal de voz a una frecuencia de 8000 muestras por segundo. Esto proporciona una mejor calidad en comparación de la mayoría de los códecs empleados.

Como se había mencionado anteriormente, una llamada telefónica requiere 64kbps en el cable. De acuerdo al teorema de muestreo de Nyquist tendremos 8000 muestras de voz cada segundo. Cada muestra es de 8 bits; por lo que al multiplicar 8000 x 8, obtendremos 64kbps, lo que significa que G.711 no usa compresión y es una alternativa cuando existe suficiente ancho de banda.

2.2.5.2. Códec G.723.1

El estándar de este códec fue desarrollado por la ITU-T [9], éste codifica señales PCM a 6.4kbps o 5.3kbps utilizando ventanas de audio de 30ms.

Para la codificación de 6.4Kbps se utiliza el algoritmo Multi Pulse Maximum Likelihood Quantitation (MPC-MLQ), generando 24 bytes por cada ventana de 30ms. Para la codificación a 5.3kbps se utiliza Algebraic Code Excited Linear Prediction (ACELP), generando 20 bytes por cada ventana de 30ms.

2.2.5.3. Códec G.726

El estándar G.726 de la ITU-T [10] codifica señales PCM, genera señales digitales de entre 16 – 40kbps, y se basa en la tecnología Adaptive Differential Pulse Code Modulation (ADPCM). El modo más utilizado regularmente es de 32kbps, siendo la mitad de la velocidad del G.711, es capaz de aumentar la capacidad de utilización en la red en un 100%.

2.2.5.4. Códec G.729

Este códec al igual que los demás tiene su estandarización de la ITU-T [11], codifica las señales PCM a 8kbps utilizando el método llamado Conjugate Structure Algebraic Code Excited Linear Prediction (CS-ACELP).

En CS-ACELP se fundamenta en el modelo CELP, que no mantiene la estructura de onda sino que codifica el audio en ventanas de 10ms, que equivalen a 80 muestras u 80 bits (recordando que este valor se debe a la frecuencia de muestreo, es de 8000 muestras por segundo).

2.2.6. Protocolo SIP

Protocolo de Iniciación de Sesión (SIP) fue desarrollado por el grupo de trabajo de ingeniería de Internet, su estándar es el Request for Comments (RFC) 3261. Utiliza funciones aportadas por otros protocolos como el Protocolo de Flujo en Tiempo Real (RTSP, Real Time Streamming Protocol) para el control de flujos y sesión, Protocolo de Descripción de Sesión (SDP, Session Description Protocol) para describir flujos, RTP / RTCP para el transporte de datos en tiempo real.

Es un protocolo usado para establecer, mantener y terminar una sesión multimedia. Las sesiones multimedia incluyen telefonía IP, conferencias, y otras aplicaciones similares envolviendo medios tales como: audio, video y datos. Invitaciones SIP son utilizadas para establecer sesiones y transmitir descripciones de sesiones.

SIP soporta sesiones de *unicast* y *multicast*, es decir punto a punto y multipunto. Para establecer y terminar comunicaciones se utilizan las siguientes cinco facetas de SIP: localización de usuario, capacidad de usuario, disponibilidad de usuario, establecimiento de llamada, y gestión de llamadas. [12]

Los dos componentes en un sistema SIP son: agente usuario y servidores de red.

Agente usuario

Los agentes usuario son clientes de aplicaciones de sistemas finales que contienen ambos, un cliente agente usuario y un servidor agente usuario, conocidos como cliente y servidor respectivamente.

- Cliente (UAC): inicia peticiones SIP y actúa como agente de llamadas de usuario.
- Servidor (UAS): Recibe peticiones y regresa respuestas de parte del usuario, actúa como agente usuario llamado.

En la figura 2.5 se puede visualizar un esquema de la comunicación en el protocolo SIP.

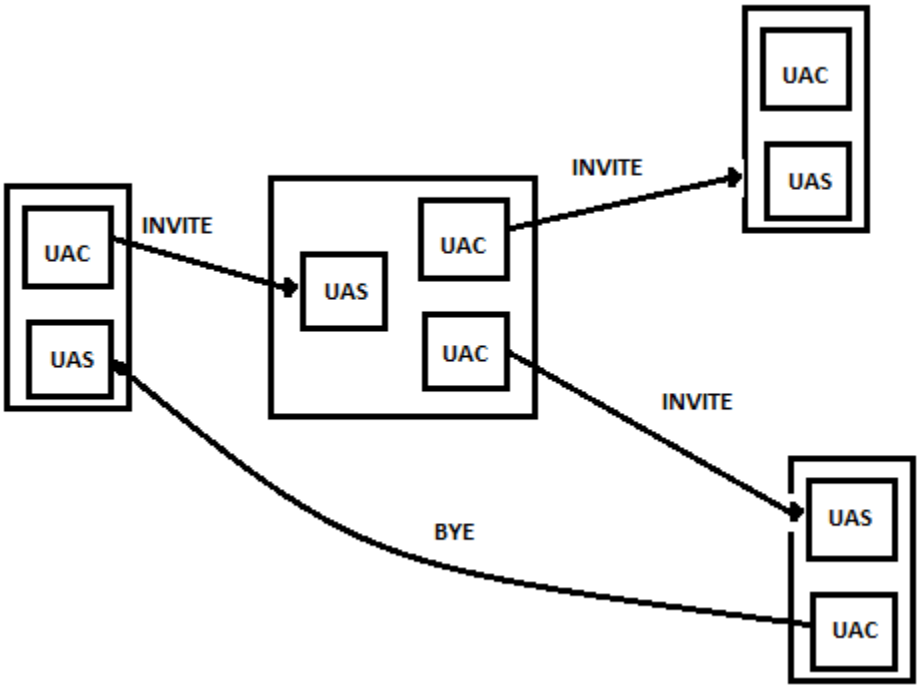


Figura 2.5. Esquema de comunicación del protocolo SIP.

Servidores de red

Existen dos tipos de servidores de red: servidores proxy y servidores que redirigen.

- Servidor proxy: Actúa de parte de otros clientes y contiene ambas funciones, tanto como cliente y servidor. Un servidor proxy interpreta y puede reescribir los encabezados de solicitud, antes de pasarlos sobre otros servidores. Al reescribir los encabezados identifica el proxy como el iniciador de la solicitud y se asegura, de que las respuestas siguen el mismo camino de regreso al proxy en lugar del cliente.
- Servidor que redirige: Acepta peticiones SIP y envía una respuesta de redirección a los clientes, con contenido de la dirección del siguiente servidor. Redirige servidores, no acepta llamadas, ni tampoco procesa solicitudes o envía peticiones SIP.

La figura 2.6 ilustra el establecimiento de una llamada SIP donde:

- Invite.- Es un mensaje de petición. Este método indica que el usuario o servicio es invitado a participar en una sesión, ésta incluye una descripción de sesión y, para las llamadas de dos vías.
- ACK.- Este mensaje representan la confirmación final del sistema y concluye la transacción iniciada por invite.
- Trying, ringing, OK, queued, call I being forwarded, request time out, entre otros, son mensajes de respuesta SIP.

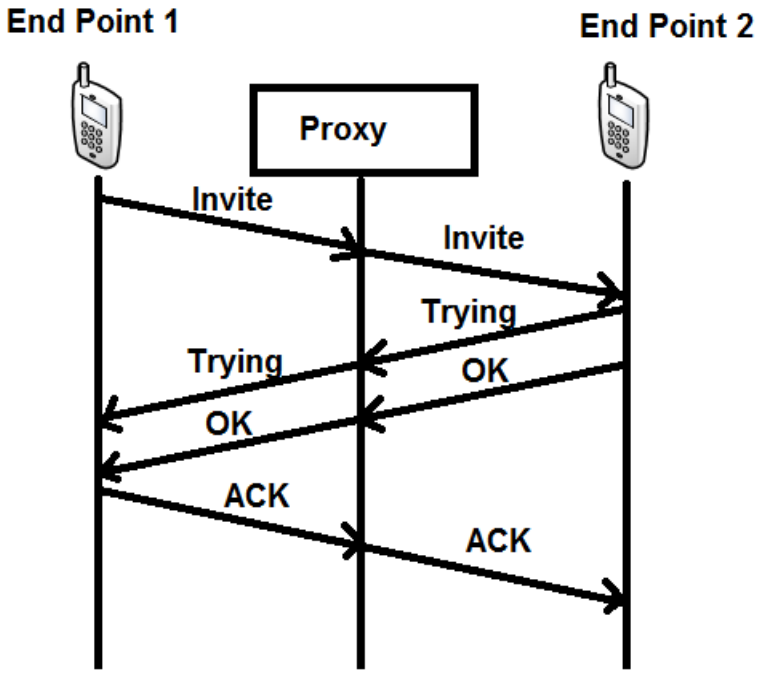


Figura 2.6. Establecimiento de una llamada SIP.

2.2.7. Protocolo RTP

El Protocolo de Tiempo Real (RTP, Real Time Protocol) está basado en el RFC 3550 [13], el cual establece los principios de un protocolo de trasporte sobre redes que no garantizan calidad de servicio para datos de tiempo real, como son: voz y video.

Cada paquetes RTP contien una cabecera y una seccion de datos de voz, la cabecera está compuesta por números de secuencia, marcas de tiempo, y monitoreo de entrega. Las aplicaciones comunmente utilizan RTP sobre protocolos de red “no confiables”, como UDP. Los “bytes” obtenidos de cada conjunto de muestras de voz o video son encapsulados en paquetes RTP, y cada paquete RTP es a su vez encapsulado en segmentos UDP.

RTP soporta transferencia de datos a destinos multiples, usando facilidades de “*multicast*”, si es provisto por la red.

El RFC 3550 también establece el Protocolo de Control de Tiempo Real (RTCP, Real Time Control Protocol), encargado de enviar periodicamente paquetes de control entre los participantes de una sesion.

2.2.8. Parametros del comportamiento dinámico en VoIP

La VoIP es suceptible al retardo, *jitter*, pérdida de paquetes, entre otros, lo cuales pueden degradar las aplicaciones de voz, hasta el punto de ser inaceptables para los usuarios. VoIP acepta retardos menores a 150ms, despues de ese valor la llamada ya no tendrá una buena calidad.

2.2.8.1. *Jitter*

El *jitter* es un problema específico de la calidad de servicio en VoIP que puede afectar la calidad de conversación si ésta se sale de control. Se define como la variacion del retardo sobre el tiempo de un punto a otro.

En el caso de que los paquetes no lleguen con el mismo intervalo de tiempo, el sistema receptor debe ser capaz de ofrecer un búfer de *jitter,* para que no existan pérdidas de paquetes cuando lleguen más juntos de lo debido. Esto es, tener almacenados los suficientes paquetes para soportar una espera mayor, en la recepción del siguiente paquete, cuando este demore su llegada más de lo esperado. De no ser así se producirán errores análogos a los ocurridos por las pérdidas de paquetes, en el caso de que se reciban más paquetes de los que se pueden almacenar hasta que llegue el momento de ser transmitidos. En otras palabras la cantidad de *jitter* tolerable sobre la red se ve afectada por la profundidad del búfer de *jitter* sobre el equipo de la red.

Si la variacion llega a ser tan alta y excede 150ms, los usuarios notaran los retardos, llegando a una conversacion estilo walkie-talkie, por tanto es recomendable que el valor del *jitter* no exceda los 100ms.

2.2.8.2. *Delta* (latencia)

El *delta* es el tiempo tomado de un punto a otro punto en la red, también conocido como latencia o retardo. El *delta* puede ser medido ya sea en un solo sentido o de ida y vuelta. Los cálculos del *delta* unidireccional requieren de prueba sofisticadas, además de estar fuera del presupuesto y la experiencia de la mayoría de los clientes de una empresa. Sin embargo, medir el *delta* de ida y vuelta es más fácil y requiere un equipo menos costoso. Para obtener una medida general del *delta* en un sentido, el *delta* o retardo de ida y vuelta, el resultado simplemente se divide por dos.

Este parámetro es una medida dentro de todo el tipo de redes de telecomunicaciones, no únicamente es para las redes no orientadas a conexión.

Si se comprende todos los factores que causan un retardo en una red, es posible mantener ésta aceptable. La calidad de la voz está en función de muchos factores, entre los más destacados son:

- Los algoritmos de compresión.
- Pérdidas y retransmisiones de tramas.
- La cancelación del eco y los retardos.

Algunos de los factores que contribuyen a que el promedio de retardo sea cambiado son:

- Retardos en el códec.
- Retardos en el hardware.
- Retardos en el procesamiento.
- Retardos en la red física.

Sin embargo varios factores del retardo son variables:

- Retardo en colas.
- Retardo en la propagación de la red.

En el estándar de la ITU G.114 se estipulan los límites de retardo en una red en general. En la tabla 2.3 se visualiza el rango del retardo y descripción según la ITU G.114 [14].

Rango (ms)	Descripción
0-150	Aceptable para las aplicaciones más comunes. Dentro de este rango entra la VoIP.
150-400	Aceptable, teniendo en cuenta que un administrador de red conozca las necesidades del usuario. Dentro de este rango ya se ve la degradación de la VoIP.
Sobre 400	Inaceptable para la mayoría de planeaciones de red, sin embargo, este límite puede ser excedido en algunos casos aislados.

Tabla 2.3. Límites de retardo en una red en general ITU G.114.

2.2.8.3. Secuencias de error y pérdida de paquetes

Paquetes de datos viajan independientemente uno del otro y están sujetos a varios retardos dependiendo sobre la ruta exacta que ellos toman. Los paquetes que están fuera de secuencia no son considerados un problema para la transferencia de datos, debido a que protocolos de trasferencia de datos pueden reordenar los paquetes y reconstruir los datos como se indica en el articulo “Medida de calidad de voz en redes IP” [15].

La pérdida de paquetes es de suma importancia en las redes de comunicaciones, debido a que los errores de transmisión pueden corromper los bits y retardar la transmisión**.**

CAPÍTULO 3

Redes *mesh*

En este capítulo se explica lo que son las redes ***mesh***, su definición, los tipos de redes ***mesh*** total y ***mesh*** parcial. Se describen el protocolo HWMP reactivo y proactivo, así como el protocolo HWMP +, el cual es propietario de *MikroTik*. Se explica el comportamiento que tienen las redes inalámbricas ***mesh*** parciales, las cuales utilizan la interface puente y en conjunto con la tecnología WDS para los AP's, las ventajas que poseen y la posibilidad de implementar todo esto con equipo *MikroTik*, haciendo uso del sistema operativo *RouterOS*.

3.1. Conceptos básicos de redes ***mesh***

Definición

Las redes ***mesh*** se definen como el conjunto de AP's o nodos interconectados que se comunican entre sí, de manera directa, transmitiendo la información de otros nodos hasta su destino final por medio de múltiples saltos. No hay necesidad de una unidad centralizada que los controle, por lo tanto éste es conocido como distribuido. En caso de existir una unidad que administre las condiciones de operación de la red se conoce como centralizado. En cualquier caso, la comunicación se realiza entre los nodos directamente y cada nodo puede ser al mismo tiempo fuente o destino de los datos o un enrutador de la información de otro nodo.

La configuración de los enlaces es dinámica, y basada en un algoritmo de optimización de enrutado. De esta forma la ruta establecida optimiza el tráfico en la mayor medida posible, y se establecen rutas alternativas en caso de fallos entre enlace. El objetivo de las redes ***mesh*** es mejorar o ampliar la cobertura de las redes inalámbricas, cubriendo aquellas zonas en las que no es posible instalar cableado para proporcionar conectividad de red a los puntos de acceso.

Los enlaces inalámbricos entre AP's puede ser un enlace, o puede ser incluso una solución propietaria de éste.

3.1.1. Ventajas de las redes ***mesh***

- Topología de la red dinámica. Los enlaces se configuran de manera automática: un AP en el momento que detecta que no tiene conexión con la red comienza un procedimiento de descubrimiento de los AP's.

- Facilidad de configuración, instalación y escalabilidad de la red. A medida que se incorporen nuevos AP's en la red, los caminos y las rutas se actualizan automáticamente, no es necesaria la re-configuración manual de los equipos.
- Tolerancia a fallos: se realiza un testeo continuo de los enlaces, analizando la eficiencia de las posibles rutas alternativas en caso de caídas de los enlaces.
- Disponibilidad de caminos redundantes alternativos, con la finalidad de determinar cuál es la ruta óptima en cada momento en función de la carga de tráfico, la velocidad del enlace, el nivel de señal, etc.

3.1.2. Dispositivos en redes WLAN ***mesh***

A continuación se describen los dispositivos que interactúan en las redes WLAN ***mesh***.

- Punto ***Mesh*** *(*MP, ***Mesh*** Point*):* Es cualquier nodo que soporte servicios de control ***mesh***, administración y operación dentro de la red ***mesh***. Establece vínculos entre vecinos MP y cuenta con una completa participación en los servicios WLAN ***mesh***.
- ***Mesh*** AP (MAP*)*: Tiene el funcionamiento de un MP colocado con AP, el cual provee servicios al BSS para soportar comunicación con STA's.
- ***Mesh*** Portal (MPP): Conectan el Internet alámbrico, es un punto en el que las unidades de servicios de datos MAC (MSDU's salen y entran en la ***mesh*** WLAN.
- Estación (STA*,* station)*:* Son los nodos o estaciones que se conectan con la red ***mesh*** a través de los ***mesh*** AP (MAP).
- BSS. Conjunto de estaciones (STAs) que se han sincronizado satisfactoriamente, usando la unión de servicios primitivos.

En la figura 3.1 se muestra una configuración de una red ***mesh*** WLAN, así como los dispositivos que intervienen en ella.

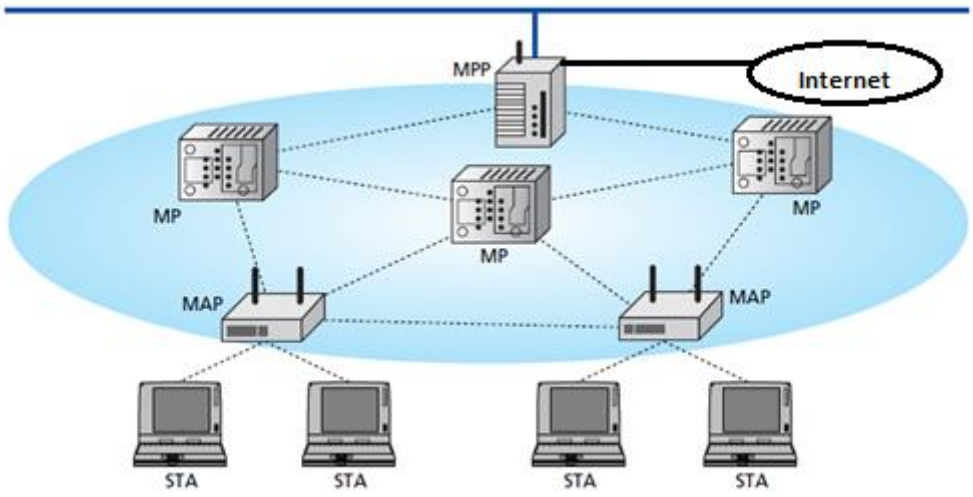


Figura 3.1. Configuración de una red ***mesh*** WLAN.

3.1.3. Topología ***mesh*** total y ***mesh*** parcial

La Topología ***mesh*** total ocurre cuando cada nodo tienen un circuito conectado a cada uno de los otros nodos de la red. Este tipo de topología es muy costoso de implementar si de infraestructura alámbrica se trata, pero posee una grandiosa cantidad de redundancia, entonces sí, en el evento en el cual uno de sus nodos falle, el tráfico de la red puede ser dirigido a cualquiera de los otros nodos. Este tipo de redes usualmente está reservado para redes *backbone*. La topología ***mesh*** parcial posee una menor redundancia en comparación con ***mesh*** total. La topología parcial es comúnmente encontrada en redes periféricas conectadas a un *backbone* ***mesh*** total. [16]

En las figuras 3.2.a y 3.2.b se muestran las topologías de las redes ***mesh*** total y ***mesh*** parcial respectivamente.

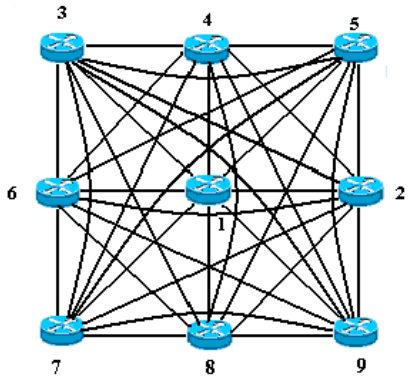


Figura 3.2.a) Topología ***mesh*** total.

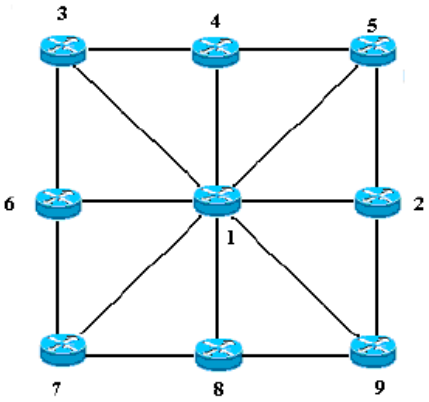


Figura 3.2. b) Topología ***mesh*** parcial.

3.2. Sistema de Distribución Inalámbrica (WDS)

El WDS es utilizado para la comunicación inalámbrica entre dos AP's. Este sistema solo es utilizado para el protocolo 802.11, y para que funcione adecuadamente tienen que estar configuradas o habilitadas las interfaces WDS en los extremos AP's con los que se desee utilizar. Con WDS es posible extender una infraestructura de cableado para puntos donde éste no es posible o es ineficiente de implementar.

En conclusión WDS crea un enlace entre dos AP´s, a través de sus interfaces de radio.

3.2.1. *Frames* WDS

Los sistemas WDS son implementados utilizando un único formato *frame,* para paquetes en los cuales su medio de transmisión es el aire. Los *frames* WDS están definidos en el estándar 802.11 para tener cuatro campos de dirección (en lugar de tres), el estándar define el formato del *frame*, pero cabe recalcar que éste no indica como debe ser utilizado.

3.2.2. WDS estático y WDS dinámicos

Existen dos tipos de configuración WDS, los cuales son implementados dentro de los AP's y estos son los estáticos y los dinámicos.

WDS estático.- Con este tipo de configuración, una serie de enlaces WDS son configurados de forma manual sobre cada AP y registrados en una tabla interna de enlaces WDS (se registran direcciones MAC de otros AP's dentro de su alcance). El tráfico de los clientes que necesitan retransmitir a través de otro AP o puente es reenviado de forma inalámbrica a su destino utilizando *frames* WDS.

WDS dinámico.- En esta configuración un AP aprende automáticamente de otros AP's, esto es hecho mediante el registro de las direcciones de todas las fuentes de tráfico WDS de los alrededores.

3.3. Red ***mesh*** WDS

Es una topología que tiene conectividad completa bidireccional entre sus nodos. En este modo, todos los nodos en la red o AP's no únicamente tienen un camino a otros nodos sino que también, ellos pueden acceder a otras redes por medio de estos AP's.

Mesh tiene algunos modos tales como (***mesh*** total, ***mesh*** parcial o ***mesh*** híbrida.

Las redes ***mesh*** tienen algunas ventajas como: habilidad de roaming, cobertura total, redundancia y tolerancia a fallos entre enlaces, etc. [17]

3.3.1. WDS ***mesh*** inalámbrica con interface ***mesh***

Todos los AP´s tienen conectividad total unos con los otros, en este modo si un enlace falla o se viene abajo entre dos AP's, éstos utilizan otro camino de otros AP's.

En este modelo WDS ***mesh***, se tiene una red ***mesh*** total, ya que al mismo tiempo se tienen algunos caminos a otros AP's.

En este tipo de red una interfaz ***mesh*** debe ser creada para que interactúe con los enlaces WDS. Dentro de la configuración inalámbrica se tiene que agregar un WDS en modo ***mesh*** dinámico o ***mesh*** estático, según sea requiera. Es importante ligar WDS por default con la interfaz ***mesh,*** para así formar la red WDS ***mesh*** inalámbrica con interfaz ***mesh.***

Cabe mencionar que, con este modelo se puede usar el Protocolo ***Mesh*** Inalámbrico Híbrido + (HWMP, Hybrid Wireless ***Mesh*** Protocol +), este protocolo no es un estándar IEEE HWMP, es un protocolo de enrutamiento propietario de *MikroTik* en capa 2.

La figura 3.3 muestra una red ***mesh*** total, la cual es implementada a través de una red WDS ***mesh*** Inalámbrica con interface ***mesh***.

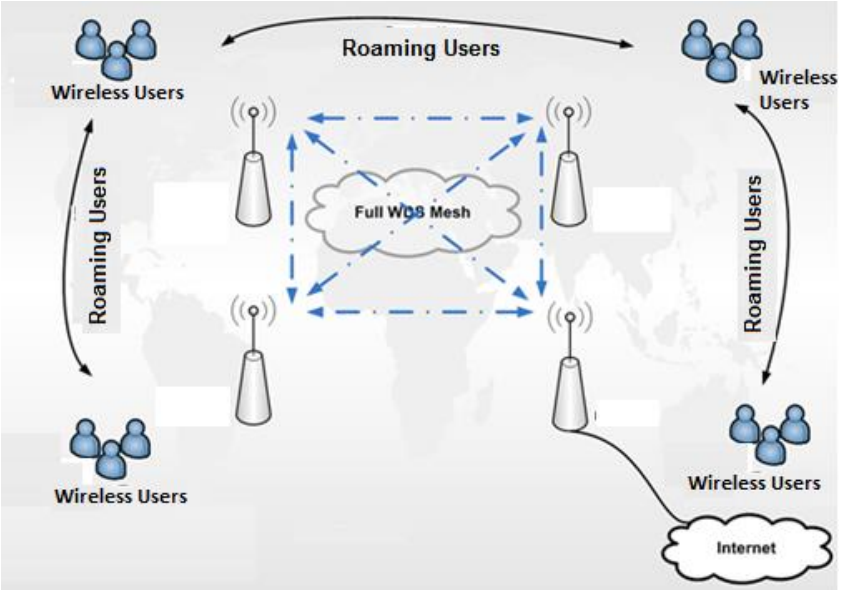


Figura 3.3. WDS ***mesh*** inalámbrico con interface ***mesh.***

3.3.2. WDS ***mesh*** inalámbrico con interfaz puente

Este modo es similar a WDS ***mesh*** total, pero tiene una diferencia y ésta es que utiliza una interface puente en lugar de una interfaz ***mesh***, además de utilizar el Protocolo de Árbol de Extensión (STP, Spanning Tree Protocol) de la familia de protocolos STP, RSTP.

Los protocolos STP y RSTP proveen trayectorias libres de ciclos en la red, además de analizar y monitorear la capa 2 en la red con envío y recepción de Bridge Protocol Data Unit (BPDU). Si la red ve algunos BPDU regresar, éste envía un bloqueo a esos AP's.

En este modo un *RouterBoard* es seleccionado como puente raíz, y administra la red libre de ciclos en capa 2, bloqueando caminos extras si la topología cambia. El puente raíz consigue nuevas estrategias para bloquear y permitir puertos.

En este tipo de red una interfaz *puente* debe ser creada para que interactúe con los enlaces WDS. Dentro de la configuración inalámbrica se tiene que agregar un WDS en modo ***mesh*** dinámico o ***mesh*** estático, según sea requiera. Es importante ligar WDS por default con la interfaz *puente,* para así formar la red WDS ***mesh*** inalámbrica con interfaz *puente.*

La figura 3.4 muestra una red ***mesh*** parcial, la cual es implementada a través de una red WDS ***mesh*** inalámbrica con interface puente. Donde las líneas punteadas permiten puerto (puente raíz), y las líneas continuas: son puertos o interfaces bloqueadas.

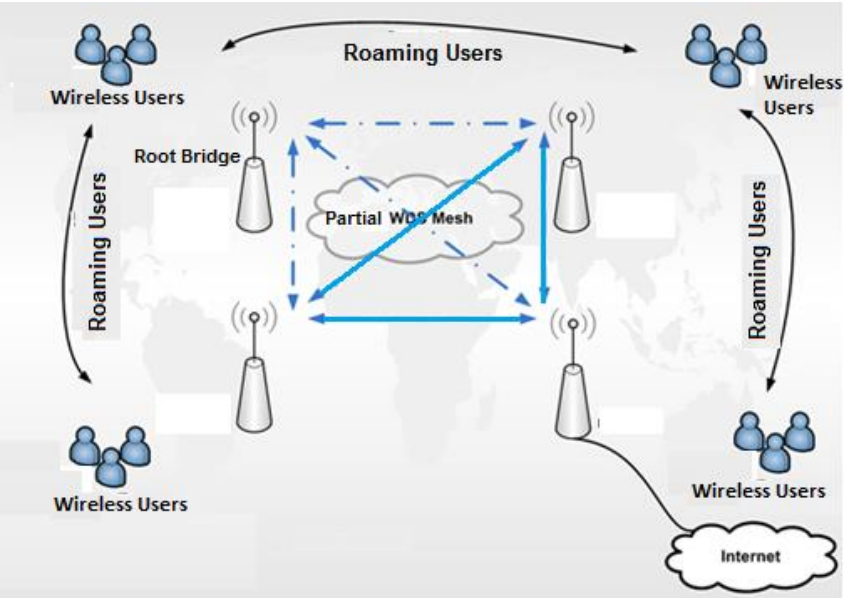


Figura 3.4. WDS ***mesh*** inalámbrico con interface puente.

3.4. Protocolo de Árbol de Expansión (STP)

El Protocolo de Árbol de Expansión (STP) es un protocolo de capa dos, publicado en la especificación del estándar IEEE 802.1d.

El objetivo de STP es mantener una red libre de ciclos. Un camino libre de ciclos se consigue cuando un dispositivo es capaz de reconocer éste en la topología y bloquear uno o más puertos redundantes.

El protocolo STP explora constantemente la red, de forma que cualquier fallo o adición en un enlace es detectado al instante. Cuando cambia la topología de red, el algoritmo de árbol de expansión reconfigura los puertos para evitar una pérdida total de la conectividad.

Los puertos intercambian información *multicast* o bien BPDU cada dos segundos, si se detecta alguna anormalidad en algún puerto STP, cambiará de estado algún puerto automáticamente utilizando algún camino redundante sin que se pierda conectividad en la red.

3.4.1. Proceso STP

STP funciona automáticamente siguiendo los siguientes criterios:

- **Elección de un dispositivo raíz**. En un dominio de difusión solo debería existir un dispositivo raíz. Todos los puertos del dispositivo raíz se encuentran en estado enviando y se denominan puertos designados. Cuando está en este estado, un puerto puede enviar y recibir tráfico.

  La elección de un dispositivo raíz se lleva acabo determinando el dispositivo que posea la menor prioridad. Por ejemplo en un switch (dispositivo de capa 2), este valor es una suma de la prioridad por defecto dentro del rango de 1 a 65536 (20 a 216) y el ID del dispositivo equivalente a la dirección MAC. Por defecto la prioridad es $2^{15} = 32768$ y es un valor configurable. Un administrador puede cambiar la elección del dispositivo raíz por diversos motivos configurando un valor de prioridad menor a 32768.

- **Puerto raíz.** El puerto raíz corresponde a la ruta de menor coste desde el dispositivo no raíz, hasta el dispositivo raíz. Los puertos raíz se encuentran en estado de envío o retransmisión y proporcionan conectividad hacia atrás al dispositivo raíz. La ruta de menor coste al dispositivo raíz se basa en el ancho de banda.

- **Puertos designados**. El puerto designado es el que conecta los segmentos al dispositivo raíz y solo puede haber un puerto designado por segmento. Los puertos designados se encuentran en estado de retransmisión y son los responsables del reenvío de tráfico entre segmentos. Los puertos no designados se encuentran normalmente en estado de bloqueo con el fin de romper la topología de ciclo.

3.4.2. Estado de los puertos STP

Los puertos del dispositivo o interfaces que participan en STP toman diferentes estados según su funcionalidad en la red.

- **Bloqueado.** Inicialmente todos los puertos se encuentran en este estado. Si STP determina que el puerto debe continuar en ese estado, solo escuchará las BPDU pero no las enviará.
- **Escuchando.** En este estado los puertos determinan la mejor topología enviando y recibiendo BPDU.

- **Aprendiendo.** El puerto comienza a completar su tabla MAC, pero aún no envía *frames*. El puerto se prepara para evitar inundaciones innecesarias.
- **Enviando.** El puerto comienza a enviar y recibir *frames.*

En la figura 3.5 se muestra como el protocolo STP bloquea uno de sus puertos o interfaces para prevenir los ciclos.

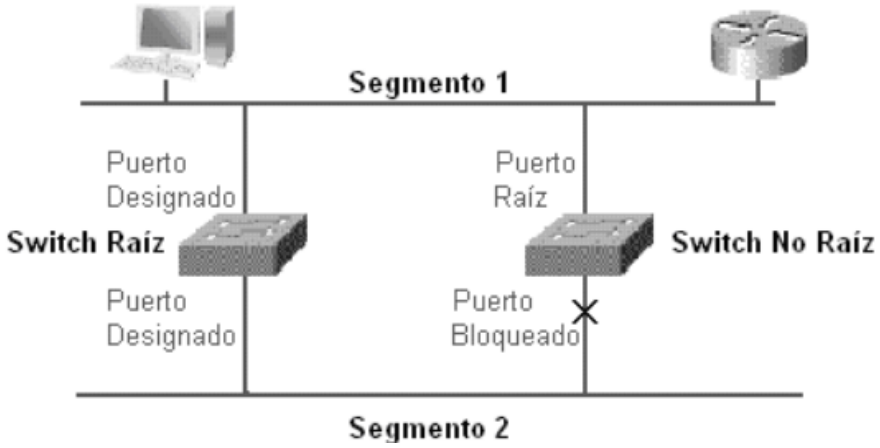


Figura 3.5. Ejemplo donde STP bloquea los puertos para evitar ciclos.

3.5. Protocolo de Árbol de Expansión Rápido (RSTP)

Protocolo de Árbol de Expansión Rápido (RSTP) es la versión mejorada de STP definido por el estándar 802.1w. RSTP funciona con los mismos parámetros básicos que su antecesor.

- Designa el dispositivo raíz con las mismas condiciones que STP.
- Elige el puerto no-raíz o raíz con las mismas reglas.

A pesar de estas similitudes con STP, RSTP mejora la convergencia entre los dispositivo, ya que STP tarda 50 segundos en pasar del estado bloqueado al enviando, mientras que RSTP lo hace prácticamente de inmediato sin necesidad de que los puertos pasen por los otros estados.

3.6. Protocolo ***Mesh*** Inalámbrico Hibrido (HWMP)

El protocolo de enrutamiento para la interoperabilidad es: Protocolo ***Mesh*** Inalámbrico Hibrido (HWMP, Hybrid Wireless ***Mesh*** Protocol).

Combina la flexibilidad de descubrimiento de ruta bajo demanda, con eficiencia enrutamiento proactivo eficiente a un portal ***mesh***.

- El enrutamiento sobre demanda ofrece una gran flexibilidad en ambientes cambiantes.
- Árbol pro-activo basado en enrutamiento es muy eficiente en las implementaciones ***mesh*** fijo.

El protocolo HWMP posee dos tipos de modos: uno es el modo reactivo y el otro es el modo proactivo.

3.6.1. Modo reactivo

Con el protocolo HWMP establece una ruta bajo demanda, cuando una fuente desea enviar datos a un destino por el que no tiene una ruta de acceso aún, éste inicia un descubrimiento de ruta.

El originador o fuente ***mesh*** STA difunde un mensaje de solicitud de ruta (PREQ, Path Request) en la red ***mesh***, preguntando por el objetivo o el destino STA ***mesh***. El objetivo responde a una PREQ recibido con un mensaje de ruta de respuesta (PREP, Path Response), que se envía al originador por *unicast*.

La métrica de trayectoria almacenada en PREQ y PREP determina la mejor ruta, según la métrica de selección de ruta utilizada. El número de secuencia HWMP en los mensajes de selección de ruta impide ciclos, que generalmente son causados por información de selección de ruta obsoleta.

El mecanismo reactivo tiene un tiempo de latencia inicial, debido a que los *frames* de datos sólo se pueden enviar después de que el proceso de descubrimiento de ruta ha terminado. Mientras que la generación del mensaje PREP por el objetivo, asegura que se utilicen los valores más actuales de las métricas del enlace.

La latencia inicial puede ser acortada, si las estaciones ***mesh*** intermedias que tienen un camino al destino se les permite responder a una PREQ. Este comportamiento es controlado mediante la bandera destino único. La bandera responder y enviar determina si el PREQ se propaga más allá del destino, incluso si una estación ***mesh*** intermedia generó una PREP gratuito. De esa manera, rutas de información ligeramente atrasadas de la estación ***mesh*** intermedia, pueden ser utilizadas por un rápido descubrimiento de rutas.

3.6.2. Modo Proactivo

En algunos casos de uso, una única o solamente unas pocas estaciones ***mesh*** son un punto final de la mayoría de las conexiones de datos. Este es el caso, por ejemplo, con *gateways* (puertas de enlace) en una ***mesh*** inalámbrica *backhaul.* Dichas estaciones ***mesh*** se pueden configurar como estaciones ***mesh*** raíz, las cuales utilizarán la selección de rutas proactivas a fin de permitir la transferencia de datos libre de latencia con ellos.

Las estaciones ***mesh*** raíz inician periódicamente la selección de rutas. Una ruta válida y vigente entre las estaciones ***mesh*** y la estación ***mesh*** raíz siempre está disponible. Más adelante, el camino existente se puede usar inmediatamente para transferir *frames* de datos sin ninguna latencia inicial. Sin embargo, la selección del camino proactivo crea una sobrecarga de red adicional. Si la transferencia de datos es entre las estaciones ***mesh*** no raíz, estas estaciones todavía utilizan la selección de rutas reactiva.

La especificación HWMP considera dos enfoques diferentes para la configuración de ruta proactiva, hacia las estaciones ***mesh*** raíz: el mecanismo PREQ proactivo y el mecanismo RANN.

El mecanismo PREQ proactivo utiliza los mismos tipos de mensajes como el mecanismo reactivo descrito anteriormente. El STA ***mesh*** raíz, envía periódicamente difusión de mensajes PREQ en la red ***mesh*** con el destino, siendo la dirección de difusión. Éste crea rutas de todas las estaciones ***mesh*** hacia el STA ***mesh*** raíz. La bandera de ruta de respuesta proactiva, contenida en un PREQ proactivo, determina si un mensaje PREP tiene que ser generado o no en respuesta al PREQ proactivo.

En caso de que la bandera de ruta de respuesta proactiva no se ha colocado, este modo se llama modo proactivo simple. Se espera que este modo sea muy pobre con respecto a la sobrecarga o encabezado de la selección de rutas. Sin embargo, sólo hay rutas unidireccionales de todas las estaciones ***mesh*** a la STA ***mesh*** raíz proactiva disponible. Si se requiere la comunicación de datos bidireccional, la STA ***mesh*** envía un PREP proactivo a la STA ***mesh*** raíz, antes de que comience el envío de *frames* de datos y después de recibir una petición de ruta proactiva, siempre y cuando la comunicación de datos está en curso. Si el STA ***mesh*** raíz necesita una ruta bidireccional a la STA ***mesh***, un descubrimiento de ruta reactiva es iniciada por el STA ***mesh*** raíz.

En el modo proactivo forzado, la bandera de ruta de respuesta proactiva es colocada y requiere cualquier estación ***mesh***, la cual recibe una petición de ruta con la dirección de difusión como dirección destino.

Y de esta forma, enviar un mensaje PREP al STA ***mesh*** raíz originario, para establecer una ruta bidireccional de forma proactiva. Este modo, permite la comunicación bidireccional entre un STA ***mesh*** raíz y cualquier otro STA ***mesh,*** sin caer al establecimiento de trayectoria reactiva. Sin embargo, la sobrecarga de la red para el envío de las respuestas de trayectoria puede ser significativo.

El mecanismo anuncio de RANN (Root Announcement) utiliza la emisión especial de mensajes, que distribuyen información sobre los siguientes saltos adecuados al STA ***mesh*** raíz periódicamente. Los mensajes RANN, sin embargo, no establecen ninguna ruta. La selección de la ruta actual se realiza con *unicast*, basado en la información del siguiente salto.

La mayoría de las investigaciones se enfocan en los mecanismos de modo proactivo PREQ y no tanto en los mecanismos RANN debido a su peculiaridad.

3.7. HWMP +

HWMP + es un protocolo propietario de *MikroTik* el cual provee redes libres de ciclos de capa 2. Actualmente éste provee una red de capa 2 enrutada, escogiendo caminos basados en la mejor métrica disponible. El protocolo de *MikroTik* localizará y solucionará el problema.

Se pueden agregar puentes de forma manual e interactuar con interfaces Ethernet o inalámbricas, dependiendo la necesidad.

MikroTik ofrece el sistema WDS ***mesh*** que funciona como una liga inalámbrica si alguna conexión falla, el sistema te lo hace saber o lo hace de forma dinámica solucionando la falla.

La interface ***mesh*** tiene todas las ventajas del protocolo STP, pero lo más importante es que es inmune a los ataques BDPU.

3.8. *RouterOS MikroTik*

RouterOS es un sistema operativo de la empresa *MikroTik* basado en *Linux*, que permite convertir un equipo x86 común o una placa *RouterBoard* en un router dedicado, con funcionalidades como: administrador de ancho de banda, un dispositivo inalámbrico, administrador Border Gateway Protocol (BGP), o cualquier otra cosa que sea relacionada con las necesidades de interconexión de redes. [18]

El sistema *RouterOS* fue creado por dos estudiantes de Latvia país exintegrante de la Unión Soviética, como tesis universitaria para diseñar un router basado en *Linux* que permita equiparar las funcionalidades de otros routers que se encontraban en el mercado. Con el pasar del tiempo se han integrado varias aplicaciones dentro del sistema, como: soluciones de telefónica IP, administración de protocolo BGP, integración de IPv6, servidor de VPN's, administración de ancho de banda, calidad de servicio (QoS), administración de *hotspots*, puntos de acceso inalámbrico, *backhaul* inalámbrico, etc.

CAPÍTULO 4

PROPUESTA DE INFRAESTRUCTURA

Se realizará una breve descripción de los equipos utilizados, sus configuraciones, así como las herramientas que permitieron la evaluación de VoIP en una red WDS ***mesh*** parcial con equipo *MikroTik*, con la utilización de VLAN's y sin ellas para la separación de tráfico de voz, video y datos.

Material o equipo empleado:

- 1 *RouterBoard MikroTik* B951Ui-2HnD
- 3 *RouterBoards MikroTik* RB951-2n
- 4 laptops
- Cables Ethernet
- Cable USB – serial
- AARONIA AG: SPECTRAN HF-4060
- AARONIA AG: HyperLOGn7060

Software y herramientas empleadas:

- *Winbox*
- *Webfig*
- 4 licencias *RouterOS* nivel 4
- *Wireshark*
- *Zoiper*
- Servidor *Asterisk*
- CMD (símbolo del sistema)
- MCS analizador de espectros en tiempo real

4.1. Propuesta de infraestructura utilizando VLAN's

La figura 4.1 muestra el diagrama de la propuesta general de infraestructura, haciendo uso de la VLAN's.

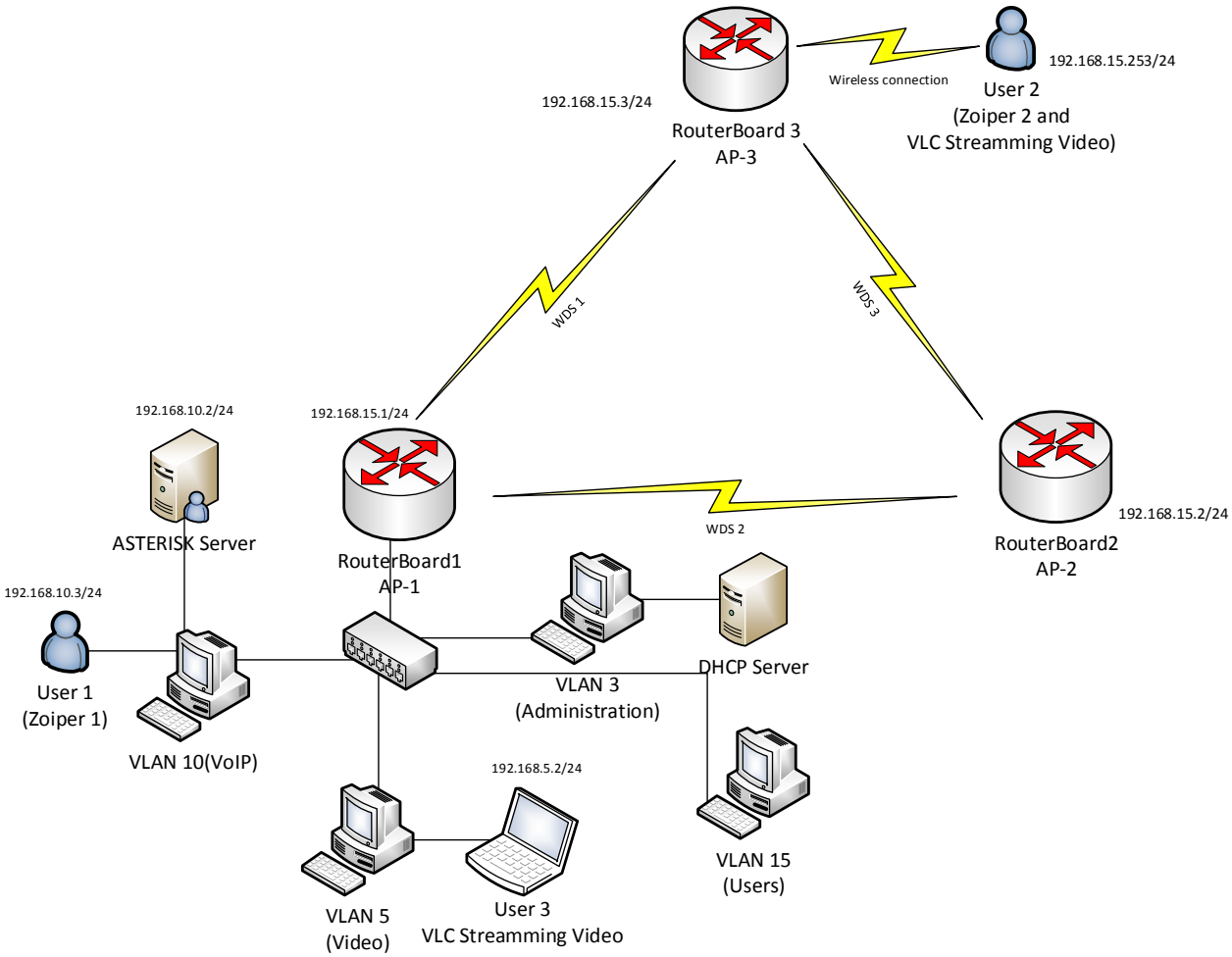


Figura 4.1. Diagrama general de implementación de red inalámbrica ***mesh*** parcial con VLAN's.

4.1.1. Modelo Instrumental

La red consta de cuatro *RouterBoards* con interfaz inalámbrica interna, donde uno de ellos fungirá como *test-switch* para la implementación de un enlace troncal, debido a que se utilizaran VLAN's para la separación del tráfico en la red y el resto de *RouterBoards* se configuraran como AP's de redes WDS ***mesh*** parciales, habilitando sus interfaces inalámbricas wlan.

Se configurará el direccionamiento IP, las interfaces inalámbricas y puentes de los *RouterBoards,* los cuales serán AP's en la red.

En la tabla 4.1 se muestra el direccionamiento IPv4 de todos los elementos que interviene en la propuesta (AP's, VLAN's, interfaces puente, usuarios, servidores, etc.).

Host o Nombre	Dirección IP
AP 1	192.168.15.1 / 24
AP 2	192.168.15.2 / 24
AP 3	192.168.15.3 / 24
VLAN 3 (administración de la red)	192.168.3.0 /24
VLAN 5 (video en ráfaga)	192.168.5.0 /24
VLAN 10 (VoIP)	192.168.10.0 /24
VLAN 15 (usuarios de video, datos, llamadas IP)	192.168.15.0 /24
Servidor *Asterisk*	192.168.10.2 / 24
Usuario 1 (Zoiper 1 ubicado en VLAN VoIP)	192.168.10.3 / 24
Usuario 2 (*Zoiper* 2 ubicado en VLAN usuarios) y servidor de video	192.168.15.253 / 24
Usuario 3 (ubicado en VLAN de video)	192.168.5.2 / 24
Puente_VLAN_3_Servicio	192.168.3.1/24
Vlan5_Switch	192.168.5.1/24
Vlan10_Switch	192.168.10.1/24
Puente_VLAN_15_Usuarios	192.168.15.1/24

Tabla 4.1. Direccionamiento IPv4 (*RouterBoard* 1, 2, 3, servidor *Asterisk*).

Configuración *Test_Switch*

En el *RouterBoard Test_Switch* se configura el direccionamiento IP de las VLAN's para la formación del enlace troncal, como se muestra en la tabla 4.2.

Host o nombre	Dirección IP
VLAN 3 (servicio)	192.168.3.20/24
VLAN 5 (video)	192.168.5.20/24
VLAN 10 (VoIP)	192.168.10.20/24

Tabla 4.2. Direccionamiento IPv4 en *Test_Switch.*

Se configuran las VLAN de servicio, video y VoIP para poderlas incorporar por un enlace troncal con interface Ethernet al AP 1.

- **Configuración inalámbrica**

En las interfaces de red inalámbrica WLAN de los *RouterBoards* 1, 2 y 3 (AP1, AP2 y AP3) se realizará la misma configuración como se muestra en la tabla 4.3:

Parámetros	
Modo	AP - puente
Banda	2Ghz - Only G
Ancho de Banda	20 MHz
SSID	*MikroTik*-Tania
Frecuencia	2437
Perfil de seguridad	Default
Modo WDS	***Mesh*** dinámico
WDS Puente default	Interface-puente
Nombre de radio	AP1 (AP2, AP3)

Tabla 4.3. Configuración inalámbrica.

La figura 4.2 muestra la visualización de la configuración inalámbrica en la interfaz wlan1 de los AP's.

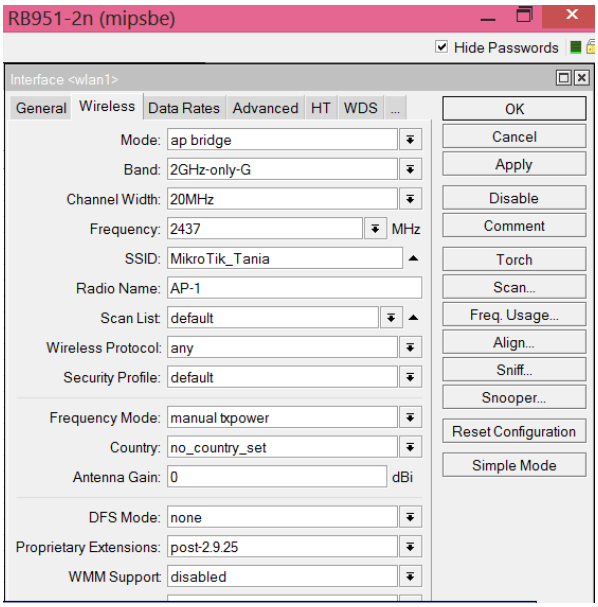


Figura 4.2. Configuración inalámbrica de la interfaz wlan1.

- **Configuración interfaz puente (bridge)**

La tabla 4.4 muestra los parámetros para la configuración de las interface puente dentro de los *RouterBoards* que serán AP's.

Parámetro	Configuración
Nombre	Interface - puente
Puertos puente	Wlan1, Ether1 (utilizando interfaz puente)
Modo protocolo	RSTP

Tabla 4.4. Configuración de parámetros en la interfaz puente.

La figura 4.3 muestra la configuración gráfica:

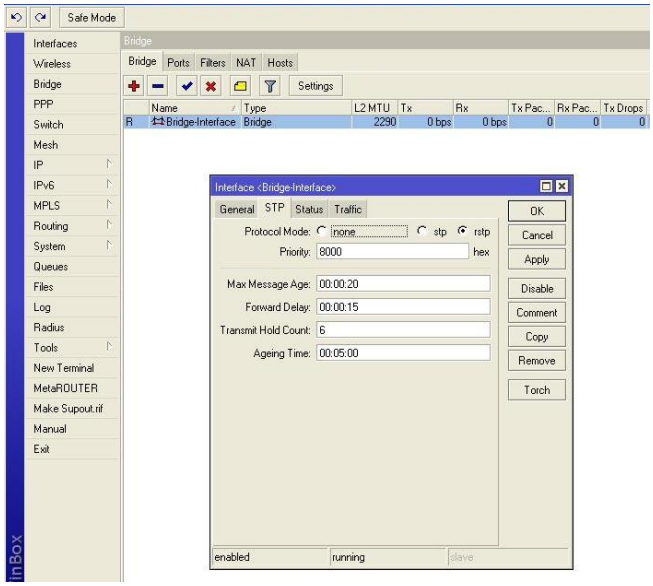


Figura 4.3. Configuración interface puente.

- **Servidor DHCP en AP 1**

Se implementó un servidor DHCP dentro del AP1, para la asignación de direccionamiento IPv4 dinámico en los usuarios. La figura 4.4 muestra el servidor DHCP creado.

Puente_VLAN_15_Usuarios: 192.168.15.2 - 192.168.15.254

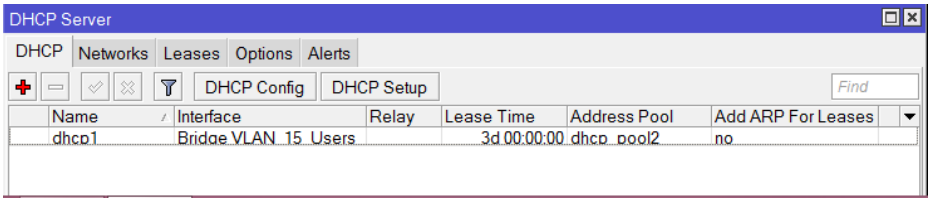


Figura 4.4. Servidor DHCP.

➢ Enrutamiento estático en AP 2 y AP 3

Se aplicará enrutamiento estático en AP 2 y AP 3, como se muestra en la figura 4.5.

- Ruta IP: 0.0.0.0/0
- Gateway: 192.168.3.1

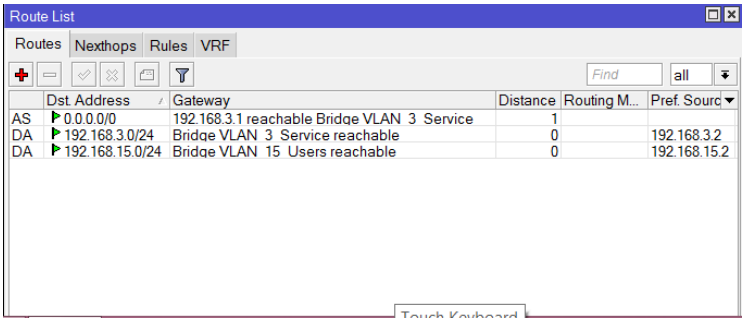


Figura 4.5. Implementación de ruta estática en AP 2 y AP 3.

El laboratorio implementado quedo de la siguiente manera:

La figura 4.6 muestra los cuatro *Routerboards* en donde se utilizaron las VLAN's.

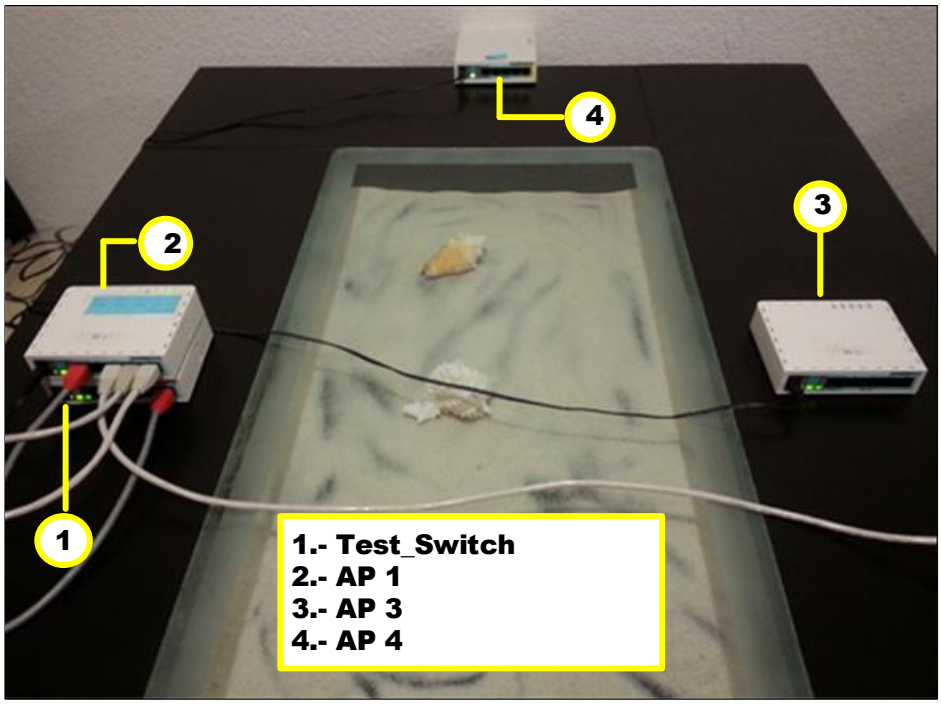


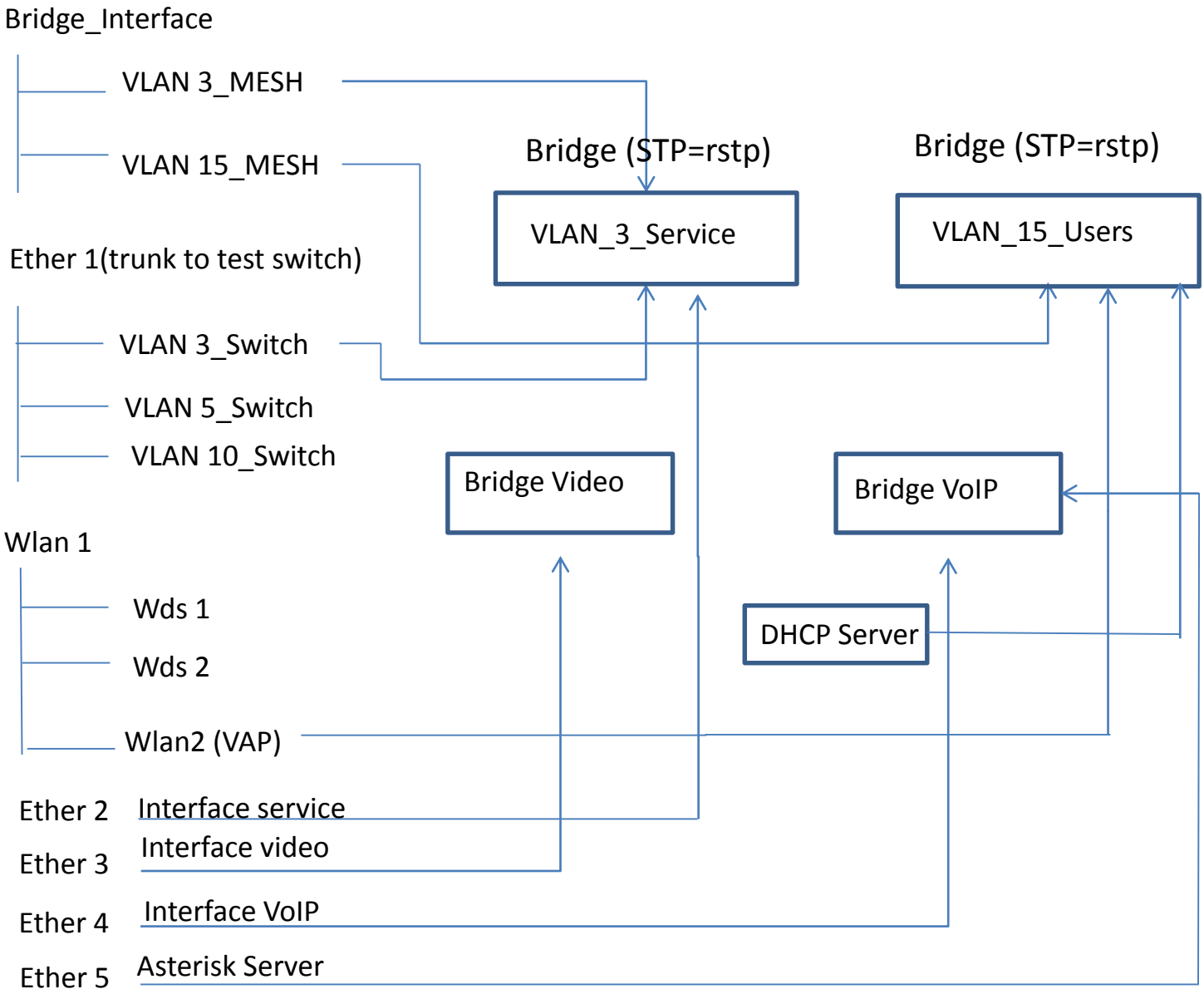
Figura 4.6. Laboratorio físico implementado (vista de *RouterBoards*).

La figura 4.7 muestra el laboratorio completo con los usuarios 1,2 y 3, el servidor *Asterisk* y los *RouterBoards* (*Test_Switch,* AP 1, AP 2 y AP 3):

Figura 4.7. Laboratorio físico de la red inalámbrica ***mesh*** parcial.

En las siguientes dos páginas se presentan los diagramas de las configuraciones realizadas dentro de los *RouterBoards,* para la implementación de AP 1, AP 2 y AP 3.

RouterBoard AP 1



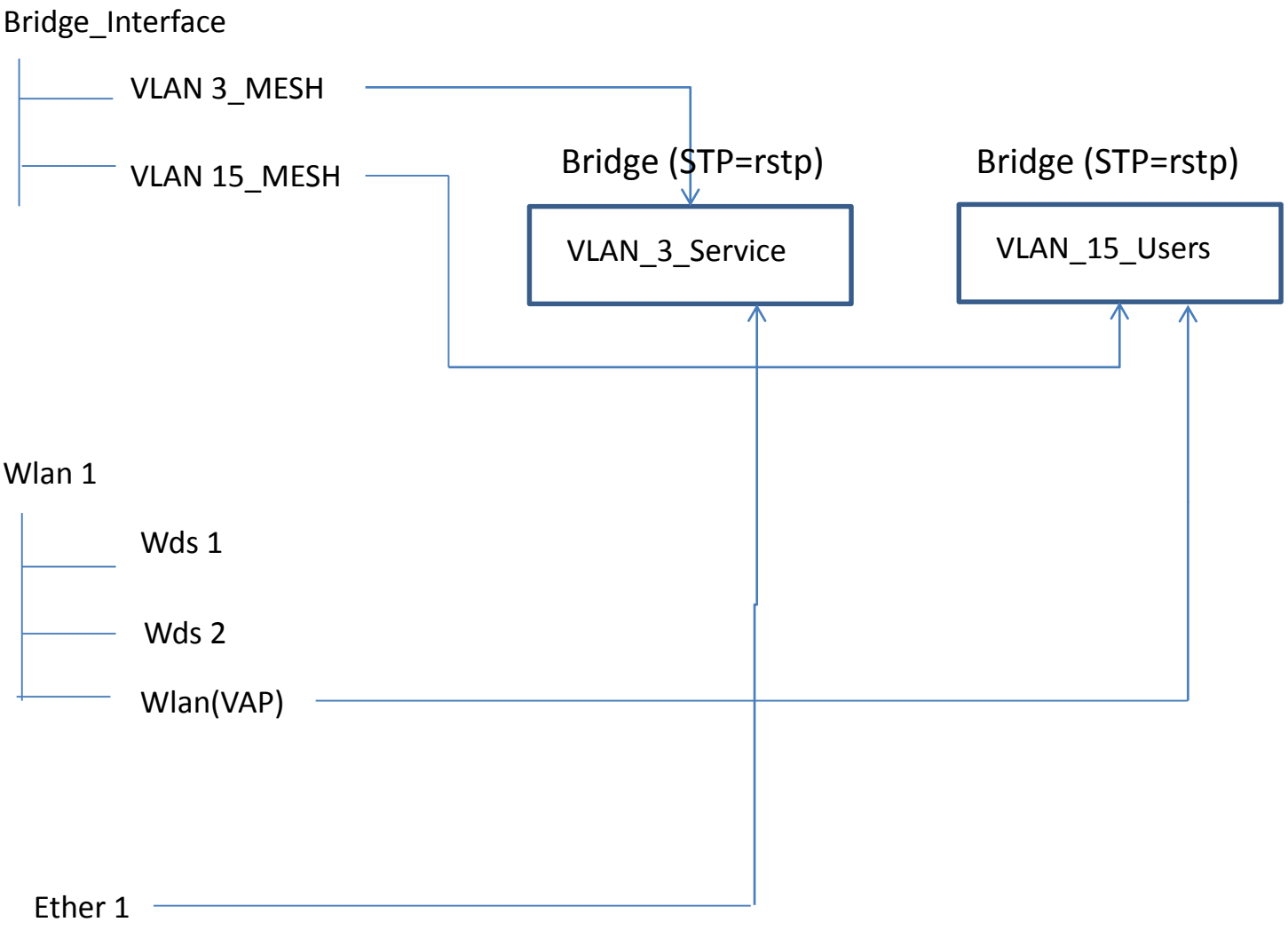
Bridge_VLAN_3_Service: 192.168.3.1/24

Vlan5_Switch: 192.168.5.1/24

Vlan10_Switch: 192.168.10.1/24

Bridge_VLAN_15_Users: 192.168.15.1/2

RouterBoard AP 2 y AP 3



Bridge_VLAN_3 _Service: 192.168.3.2/24

Bridge_VLAN_15 _Users: 192.168.15.2/24

Routing:

IP route: 0.0.0.0/0 Gateway: 192.168.3.1

Servidor *Asterisk*

Para la realización de las llamadas se utilizó un servidor *Asterisk* basado en Linux con la finalidad de establecer llamadas IP. El protocolo implementado en esta tesis para la señalización y sincronización de las llamadas fue el Protocolo de Inicio de Sesión (SIP, Session Initiation Protocol).

A continuación se describen las instrucciones para instalación y configuración del servidor *Asterisk*:

Para la instalación ingresamos la siguiente instrucción en la línea de comandos.

```
$ sudo apt-get install asterisk
```

Es necesario accesar y modificar los archivos sip.conf y extensions.conf, para la configuración de usuarios en base a sus extensiones, ID, nombre, el códec de voz a utilizar, etc.

```
$ gedit sip.conf  / extensions.conf
```

Para acceder al servidor:

```
$ asterisk –r
```

Para guardar modificaciones:

```
Fuera de consola $ sudo / etc / init.d / asterisk restart

Dentro de consola HP*CLI> dialplan reload
```

Para visualizar a los usuarios conectados a nuestro servidor:

```
HP*CLI> sip show peers
```

A continuación se muestran las extensiones utilizadas por los usuarios, así como su número ID.

User 1 (conectado a VLAN de VoIP)

```
Ext: 111------ID: 82
```

User 2 (conectado al AP3 de forma inalámbrica)

```
Ext: 222------ID: 80
```

La figura 4.8 muestra la consola del servidor *Asterisk* en la red ***mesh*** parcial con VLAN’s y dos usuarios *Zoiper* conectados a éste:

```
root@HP: /etc/asterisk
'82' is now Reachable. (1753ms / 2000ms)
HP*CLI> sip show peers
Name/username              Host                                    Dyn Forcerpor
t ACL Port     Status
80/80                      192.168.15.253                           D          5
060     OK (105 ms)
81/81                      (Unspecified)                            D          0
        UNKNOWN
82/82                      192.168.10.3                             D          5
060     OK (1753 ms)
83/83                      (Unspecified)                            D          0
        UNKNOWN
4 sip peers [Monitored: 2 online, 2 offline Unmonitored: 0 online, 0 offline]
HP*CLI> sip show peers
Name/username              Host                                    Dyn Forcerpor
t ACL Port     Status
80/80                      192.168.15.253                           D          5
060     OK (155 ms)
81/81                      (Unspecified)                            D          0
        UNKNOWN
82/82                      192.168.10.3                             D          5
060     OK (1753 ms)
83/83                      (Unspecified)                            D          0
        UNKNOWN
```

Figura 4.8. Consola del servidor *Asterisk* con 2 usuarios *Zoiper* conectados.

Softphone *Zoiper*

Se utilizó el software *Zoiper* para la realización de llamadas, creando cuentas para poder registrarlas en el servidor, configurando parámetros como nombre de cuenta, nombre de usuario y dominio. Estos *Softphones* se encuentran implementados tanto en la VLAN de VoIP y en la VLAN de Usuarios, para establecer las llamadas de VoIP. En la figura 4.9 se muestra una terminal *Zoiper* con una llamada en curso a la extensión 111.

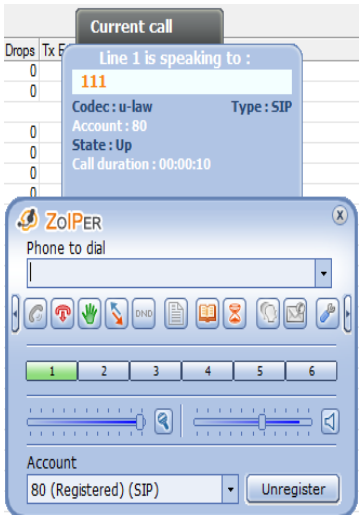


Figura 4.9. Softphone *Zoiper*.

Video en ráfaga

El servidor de video se localiza en el usuario 2 que se encuentra en la VLAN de usuarios, a través de la herramienta *VLC Media Player* para la implementación de ráfaga de video hacia la VLAN 5 de video. Se emitirá un video en ráfaga con formato .wmv. La figura 4.10 muestra la apertura del video para la emisión en la red.

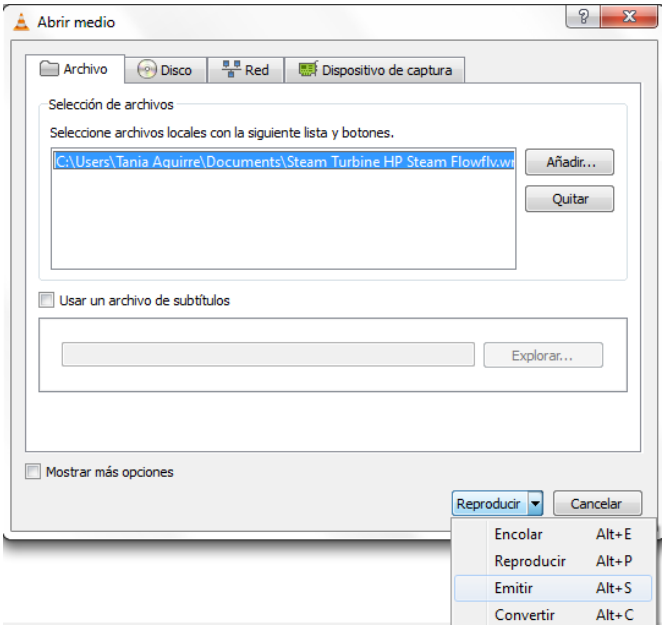


Figura 4.10. Apertura de video para emisión.

La figura 4.11 muestra el archivo .wmv cargado para la salida de emisión.

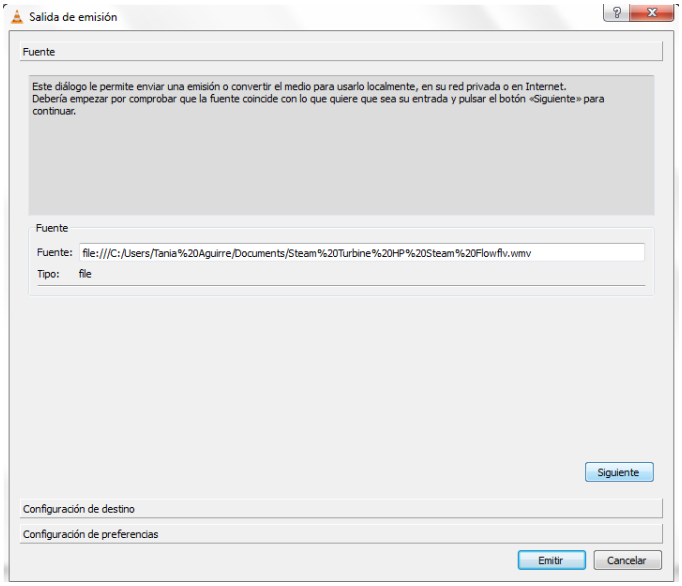


Figura 4.11. Salida de emisión del video.

Se utilizaron los protocolos de emisión RTP / MPEG Transport Stream para poder enviar al destino video, el cual tiene la IP 192.168.5.2 a través del puerto 5004. También se habilitó la opción de transcodificación video WMV + WMA (ASF), para evitar errores en la recepción de éste. En las figuras 4.12 y 4.13 se muestran las configuraciones del destino en ráfaga.

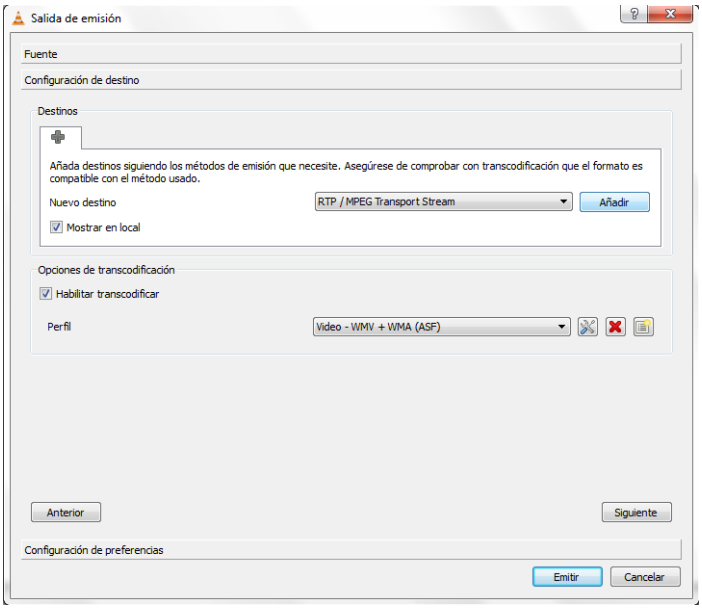


Figura 4.12. Configuración del protocolo de emisión en VLC.

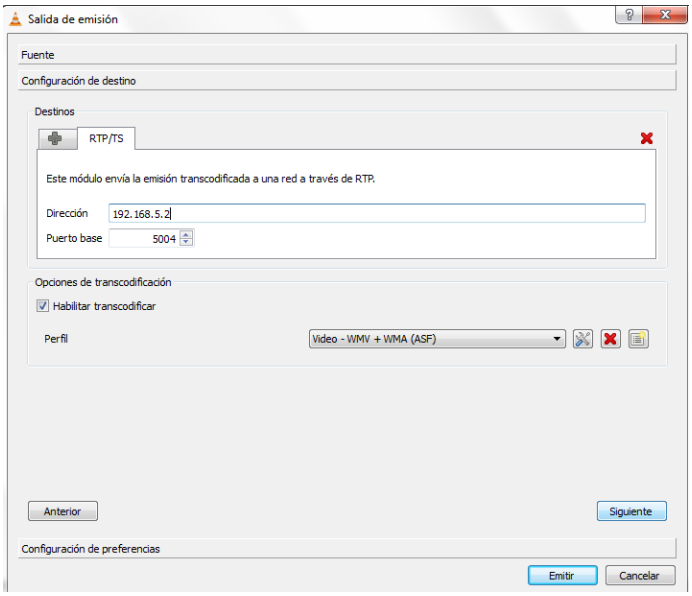


Figura 4.13. Configuración de la dirección destino y puerto en VLC.

Por último en la figura 4.14 se muestra la emisión en tiempo real de video en el servidor de video, el cual se encuentra en el usuario 3.

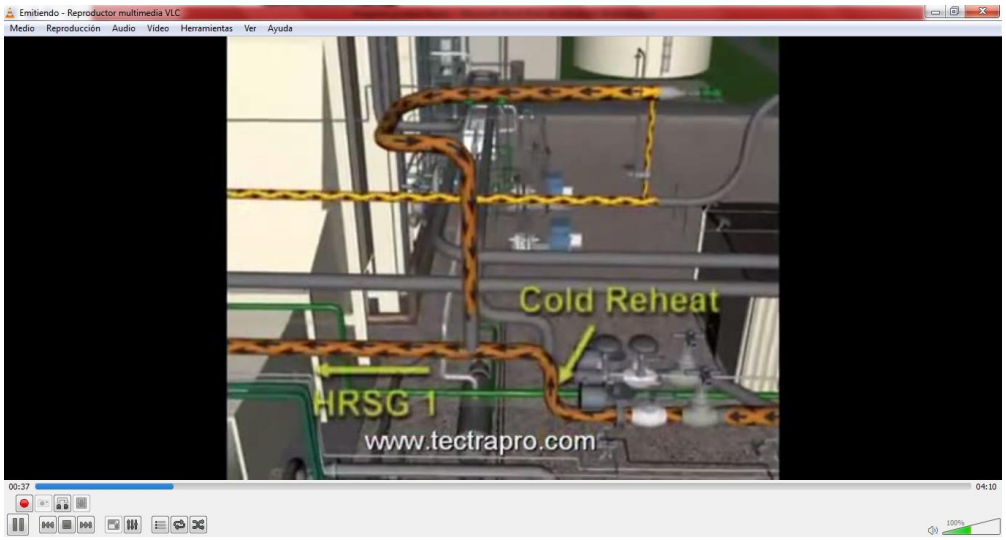


Figura 4.14. Emisión del video en ráfaga.

Propiedades de los video transmitidos

El primer video tiene una duración de 4.10 minutos y tiene un tamaño de 88.5 MB. En el segundo video se tiene una duración de 4.09 minutos con un tamaño de 339 MB, pero en todos los casos se realizó la transmisión en ráfaga después de haber entablado la llamada, siendo la duración de video transmitido menor a los 3 minutos, ya que la duración de las llamadas IP tienen una duración aproximada a los 3 minutos.

En las figuras 4.15 a y 4.15 b se muestran las propiedades de los videos transmitidos:

a) Video con duración de 4.10 min.

Tamaño = 88.5MB = 708Mb

Duración tot. = 4.10min = 246 s.

$Vel.de\ tx = \frac{708Mb}{246s} = 2.878Mbps$

b) Video con duración de 4.09 min.

Tamaño = 339MB = 2712Mb

Duración tot. = 4.09 min = 245.4s

$Vel.de\ tx = \frac{2712Mb}{245.4s} = 11.051Mbps$

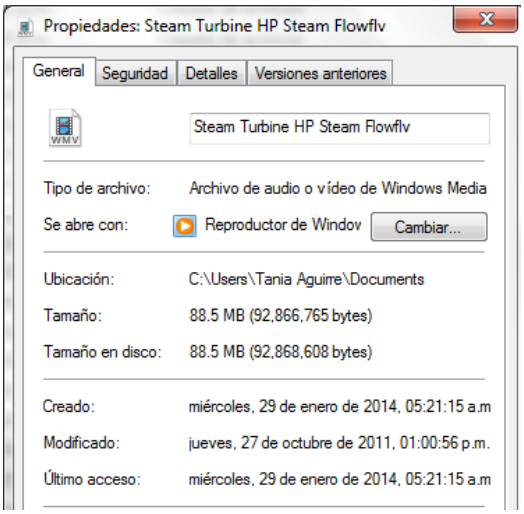


Figura 4.15 a. 1er video transmitido.

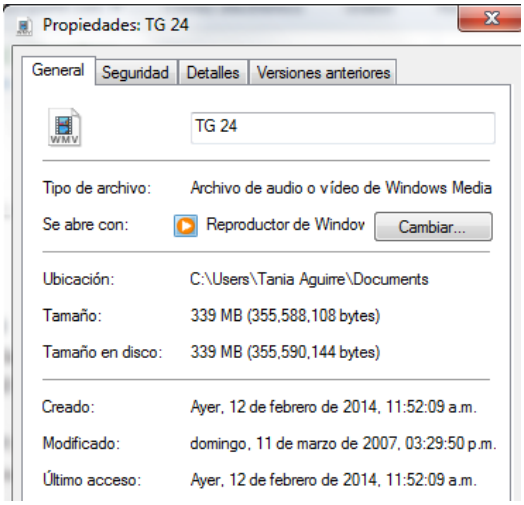


Figura 4.15 b. 2do video transmitido.

4.2. Propuesta de infraestructura sin utilizar VLAN's

La figura 4.15 muestra el diagrama de la propuesta general de infraestructura de la red ***mesh*** parcial sin hacer uso de VLAN's:

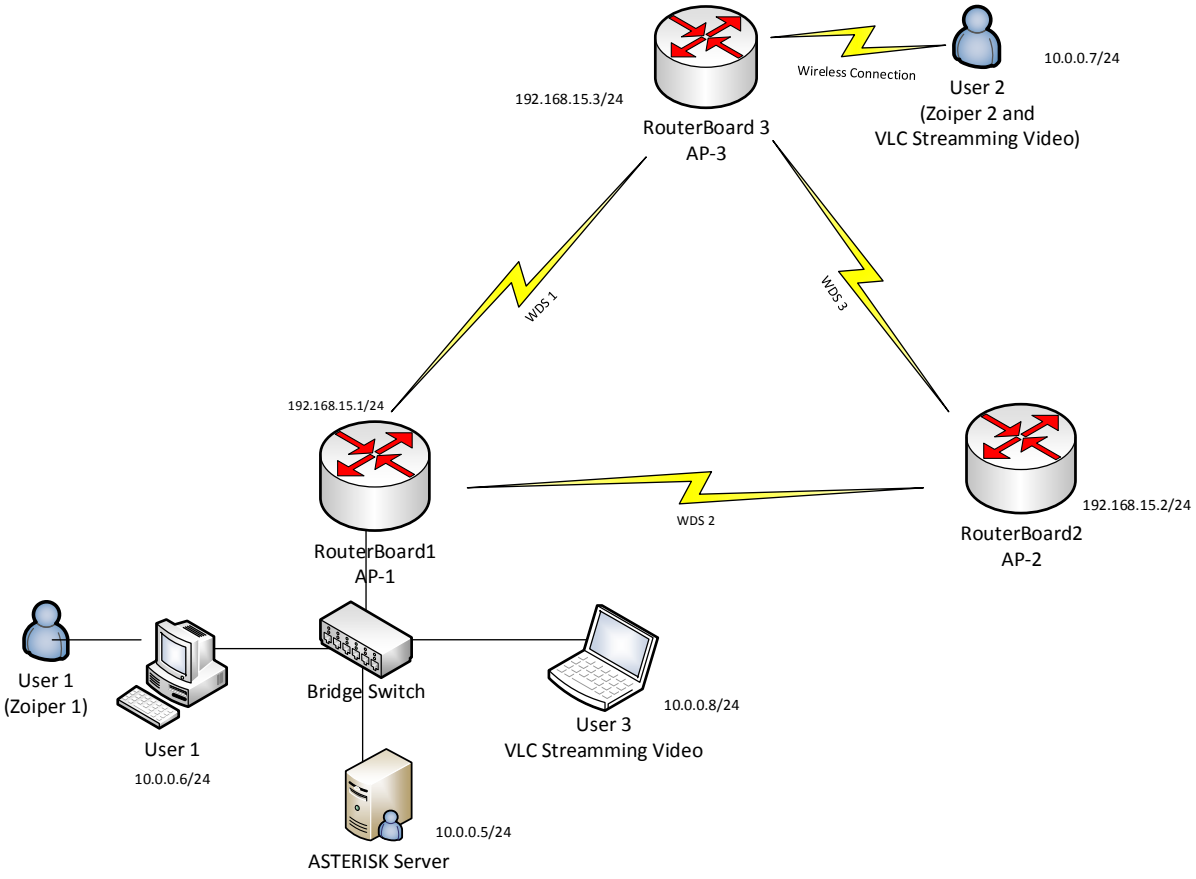


Figura 4.15. Diagrama general de implementación de red inalámbrica ***mesh*** parcial sin VLAN's.

4.2.1. Modelo Instrumental

Las configuraciones en las interfaces inalámbricas son exactamente las mismas que en el caso de VLAN's, así como el seguimiento de las transmisión de VoIP y video. Se debe eliminar todas las VLAN's, modificando el direccionamiento IP como viene indicado en el diagrama principal, así como el *RouterBoard* con la configuración *Test_Switch* de igual forma debe descartarse, quedando así tres AP's para la realización de la prueba.

La tabla 4.5 muestra el direccionamiento IP en esta implementación:

Host o Nombre	Dirección IP
Usuario 1	10.0.0.6 / 24
Usuario 2	10.0.0.7 / 24
Usuario 3	10.0.0.8 / 24
Gateway por default	10.0.0.4
Servidor Asterisk	10.0.0.5 / 24

Tabla 4.5. Direccionamiento IPv4 sin VLAN's.

Se realizó el mismo seguimiento que en el caso con las VLAN's, para registrar a los usuarios *Zoiper*, se modificaron las direcciones IP, dominio, usuarios, los ID, etc.

Servidor *Asterisk* sin VLAN's

La figura 4.16 muestra el registro de los dos usuarios conectados por medio de *Zoiper* al servidor *Asterisk*:

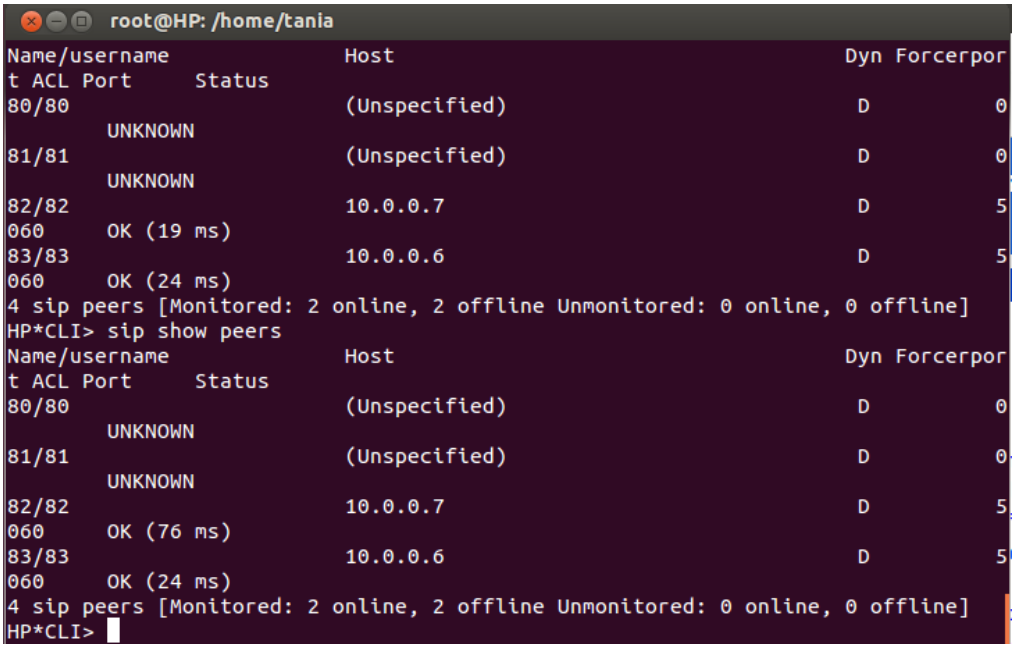


Figura 4.16. Usuarios conectados en la consola del servidor *Asterisk* sin VLAN's.

4.3. Pruebas y configuraciones adicionales

4.3.1. Test de análisis de espectros

Antes de la evaluación de estas pruebas, se hizo un análisis de las trasmisiones inalámbricas en el ambiente donde se realizó, con un analizador de espectros para ver en cual canal existían menos interferencias para poder llevar acabo las pruebas.

En las figuras 4.17 y 4.18 se muestran las pruebas del analizador de espectros utilizado:

Figura 4.17. Analizador de espectros 1.

Figura 4.18. Analizador de espectros 2.

Se pudo observar que el canal más limpio fue el de 2437MHz, en donde las portadoras no llegaban completamente a ocupar el canal, siendo este el canal número 6 dentro del rango de frecuencias del estándar 802.11g.

Cabe mencionar que antes de este análisis se hicieron las pruebas con la frecuencia 2412MHz ya que viene por default en los *RouterBoards*, siendo el canal número 1. El resultado fue que se tenía demasiado ruido y el desempeño de la red era demasiado baja aun sin congestionar de tráfico la red. La siguiente figura 4.19 ilustra la selección de frecuencias dentro de la interfaz inalámbrica.

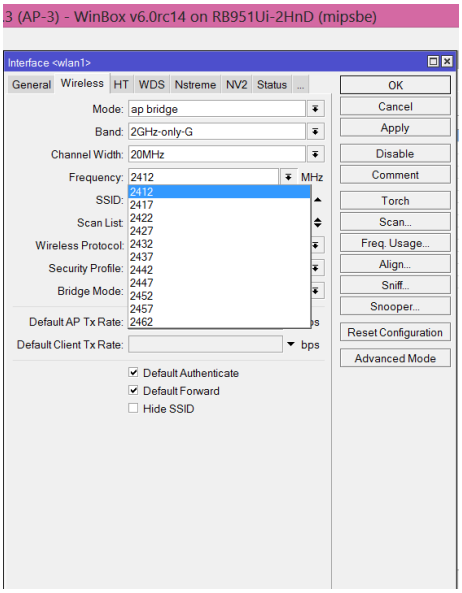


Figura 4.19. Selección de la frecuencia en la interfaz inalámbrica a través de *Winbox*.

La figura 4.20 muestra la prueba físicamente del análisis de espectros, en el entorno donde fue implementada la red inalámbrica ***mesh*** parcial.

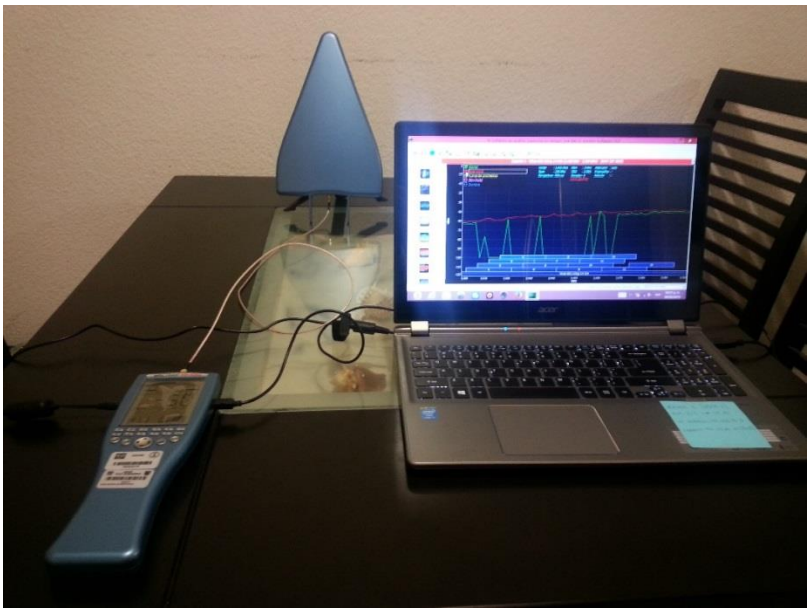


Figura 4.20. Prueba física con el análisis de espectros.

- El analizador de espectro utilizado se muestra en la figura 4.21, siendo el dispositivo AARONIA AG: SPECTRAN HF-4060.
- Y la antena utilizada fue el dispositivo AARONIA AG: HyperLOGn7060, mostrado en la figura 4.22.

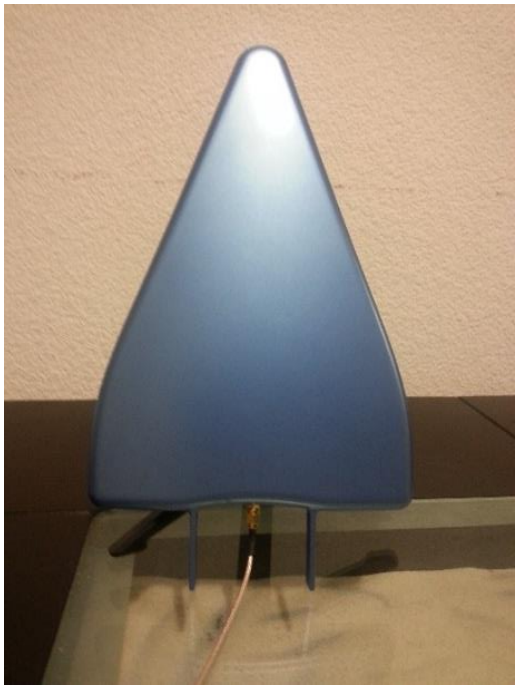


Figura 4.21. Antena para análisis de espectro.

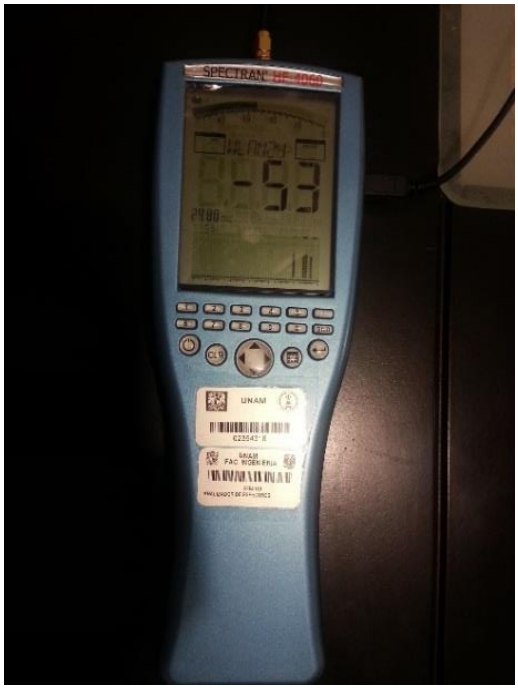


Figura 4.22. Analizador de espectros.

CAPÍTULO 5

RESULTADOS

En este capítulo se muestran los resultados del comportamiento dinámico de los parámetros de VoIP, para la evaluación en la red WDS ***mesh*** parcial, en donde se visualiza si realmente es viable o no la implementación de una red como la propuesta, utilizando VLAN's como separadoras de tráfico de video, voz y datos.

Se estudió el comportamiento dinámico de la red enfocado a VoIP, obteniendo parámetros como *jitter*, *delta* (latencia o retardo end to end), paquetes perdidos, paquetes desfasados, tiempos de inestabilidad y utilización de las llamadas IP en la red ***mesh*** WDS.

Los resultados fueron obtenidos por medio de capturas de tráfico en las interfaces inalámbricas y alámbricas en *Wireshark*, realizando filtrados RTP, UDP y utilizando herramientas muy útiles que permiten la obtención y manipulación del tráfico.

Se tienen seis escenarios a comparar, los cuales se encuentran dentro de dos agrupaciones muy importantes en la evaluación.

a) Comportamiento dinámico de VoIP en redes WDS ***mesh*** parciales con VLAN's.

1. Análisis de VoIP en redes WDS ***mesh*** parciales con VLAN's, y tráfico medio de fondo.
2. Análisis de VoIP en redes WDS ***mesh*** parciales con VLAN's, y tráfico medio de fondo, con un fallo de enlace.
3. Análisis de VoIP en redes WDS ***mesh*** parciales con VLAN's, y tráfico alto de fondo.
4. Análisis de VoIP en redes WDS ***mesh*** parciales con VLAN's, y tráfico alto de fondo, con un fallo de enlace.

b) Comportamiento dinámico de VoIP en redes WDS ***mesh*** parciales, sin VLAN´s.

5. Análisis de VoIP en redes WDS ***mesh*** parciales sin VLAN's, y tráfico alto de fondo.
6. Análisis de VoIP en redes WDS ***mesh*** parciales sin VLAN's, y tráfico alto de fondo, con un fallo de enlace.

5.1. Comportamiento dinámico de VoIP en redes WDS ***mesh*** parciales con VLAN's

5.1.1. Análisis de VoIP en redes WDS ***mesh*** parciales con VLAN's, y tráfico medio de fondo.

La figura 5.1 muestra el diagrama de la ruta del tráfico enviado desde usuario 2, como iniciador de llamada y trasmisor de ráfaga de video, hacia VLAN de VoIP y VLAN de video respectivamente.

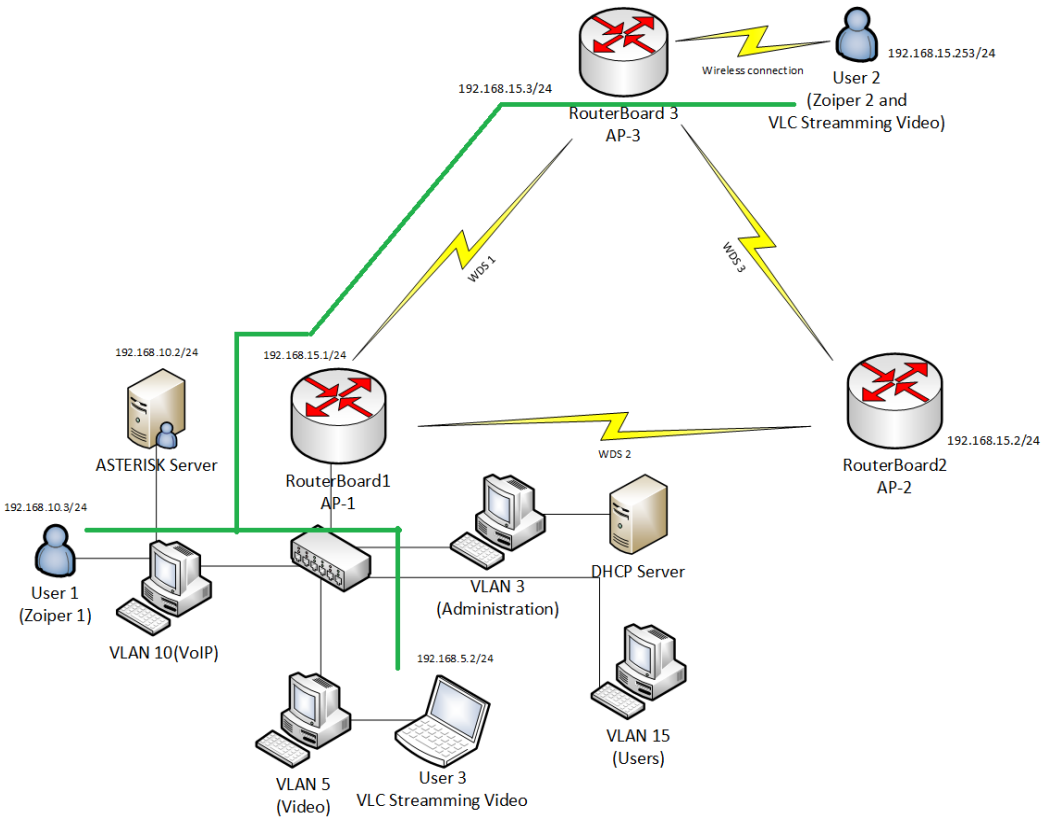


Figura 5.1. Diagrama de la ruta del tráfico en escenario 1 con VLAN's.

- ***Tráfico en VLAN de usuarios***

La figura 5.2 muestra el envío y recepción de tráfico RTP (VoIP) y UDP (ráfaga de video) en la VLAN de usuarios.

El promedio del tráfico UDP en la VLAN de usuarios fue de 2.1258Mbps, siendo éste el tráfico de video.

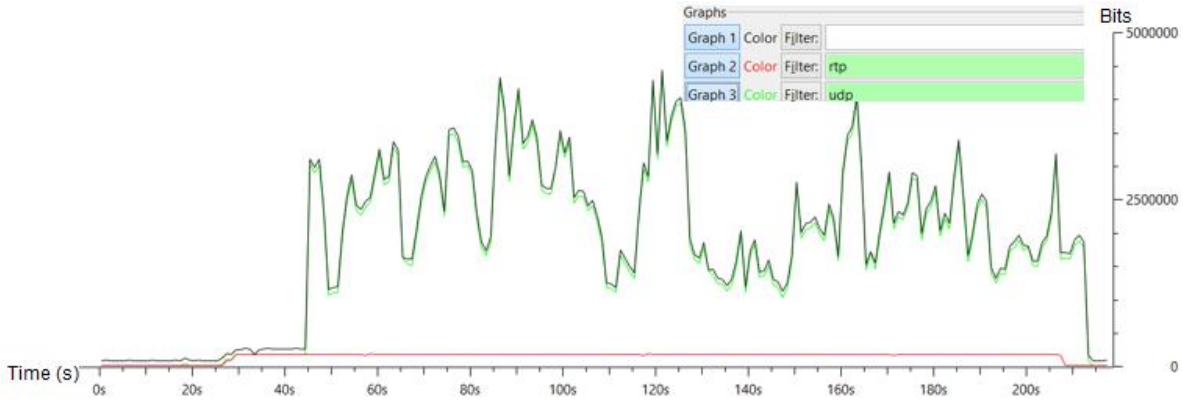


Figura 5.2. Gráfica del tráfico en la VLAN de usuarios en escenario 1 con VLAN´s.

- ***Paquetes que se recibieron y emitieron en la VLAN de VoIP***

En la figura 5.3 se observa que se están emitiendo y recibiendo un total de 100 paquetes por segundo aproximadamente, en la VLAN de VoIP.

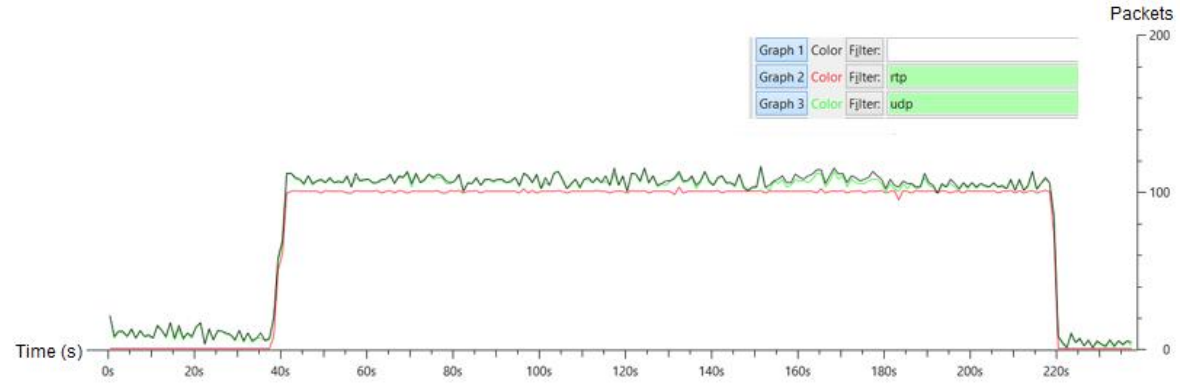


Figura 5.3. Gráfica paquetes que se recibieron y emitieron en VLAN de VoIP en escenario 1.

- ***Utilización en la VLAN de VoIP***

La figura 5.4 muestra la utilización en la VLAN de VoIP de la llamada establecida desde el usuario 2 al usuario 1, la cual fue de 175Kbps aproximadamente.

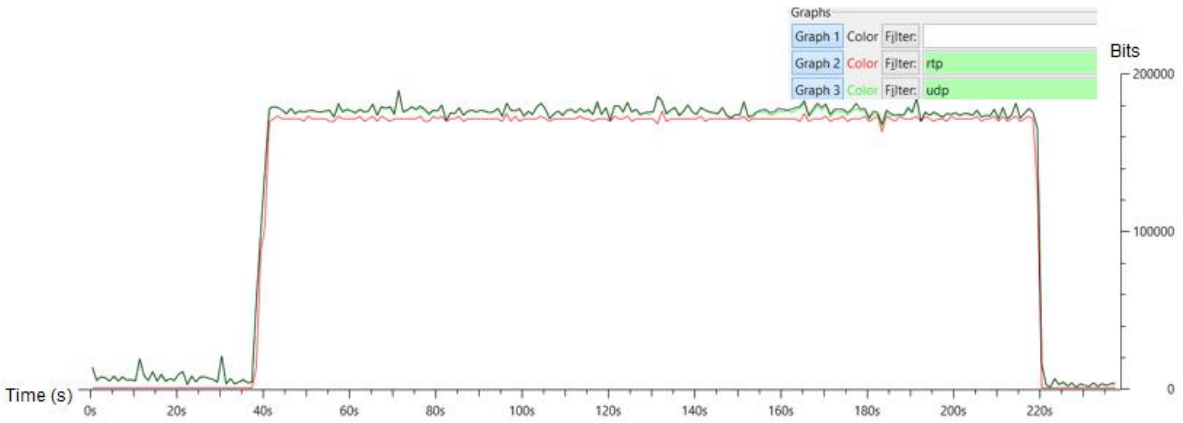


Figura 5.4. Utilización de llamada en VLAN de VoIP en escenario 1.

- ***Jitter***

El *jitter* promedio del envío fue de 6.29ms, de recepción 3.59ms, un máximo de 6.57ms y 14.87ms respectivamente, como puede apreciarse en la figura 5.5.

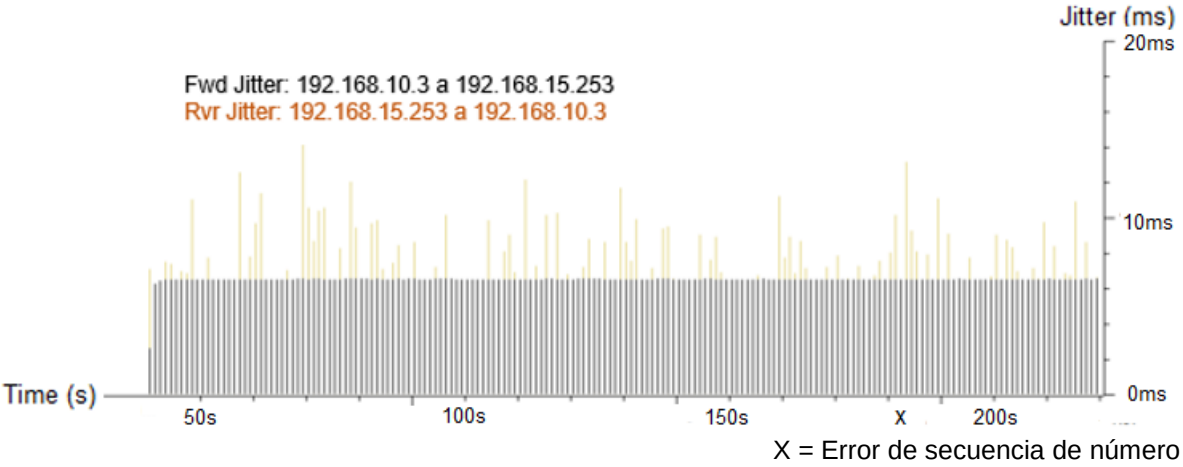


Figura 5.5. *Jitter* en escenario 1 con VLAN's.

- ***Delta***

En el *delta (latencia)* dentro de la dirección de envío, se tiene un promedio de 31.72 ms. *Delta* máximo de 31.76ms en envío y 108.98ms en recepción como se muestra en la figura 5.6.

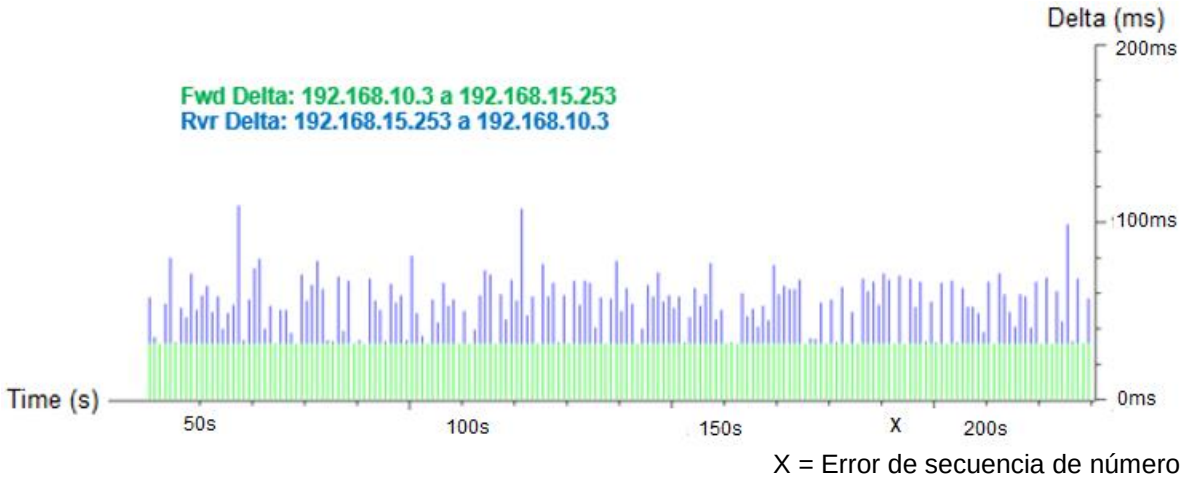


Figura 5.6. *Delta* en escenario 1 con VLAN's.

- ***Delta zoom* en error de secuencia de número ¨X¨**

La figura 5.7 muestra gráficamente la voz transmitida en la VLAN de VoIP, capturando el momento donde ocurre la secuencia de error de número:

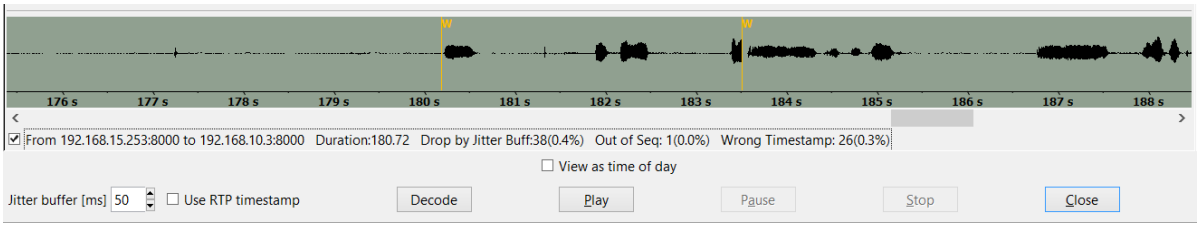
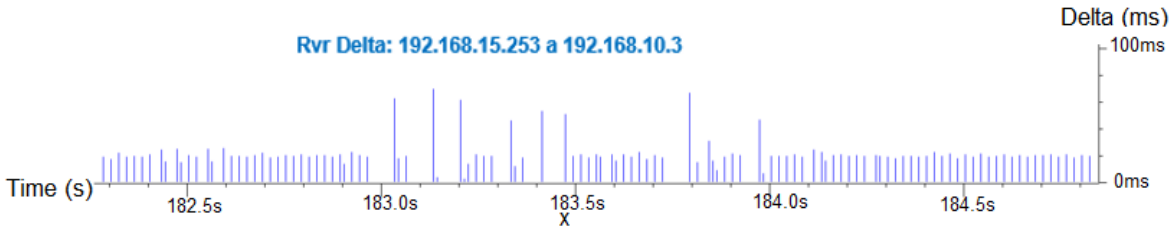


Figura 5.7. Captura de voz en forma gráfica en escenario 1.

El error de secuencia de número se dió en el segundo 183.4 aproximadamente.

Realizando un zoom en un intervalo dentro del cual ocurre la secuencia de error, se puede concluir que se perdieron 9 paquetes en el segundo anterior al fallo y 3 paquetes después de él, teniendo un total de 12 paquete perdidos, a partir del tiempo 182.9s empezaron las pérdidas.

Hasta el segundo 184.0 se estabilizó la voz, enviando 5 paquetes cada décima de segundo, teniendo 1.1 segundos de inestabilidad. La figura 5.8 muestra la gráfica del *delta zoom* cuando ocurre el error de secuencia de número ¨X¨.



X = Error de secuencia de número

Figura 5.8. *Delta zoom* en error de secuencia de número ¨X¨ en escenario 1.

➢ Tráfico en VLAN de video

Se recibió tráfico UDP en la VLAN de video de aproximadamente 2.1256Mbps, como se muestra en la figura 5.9.

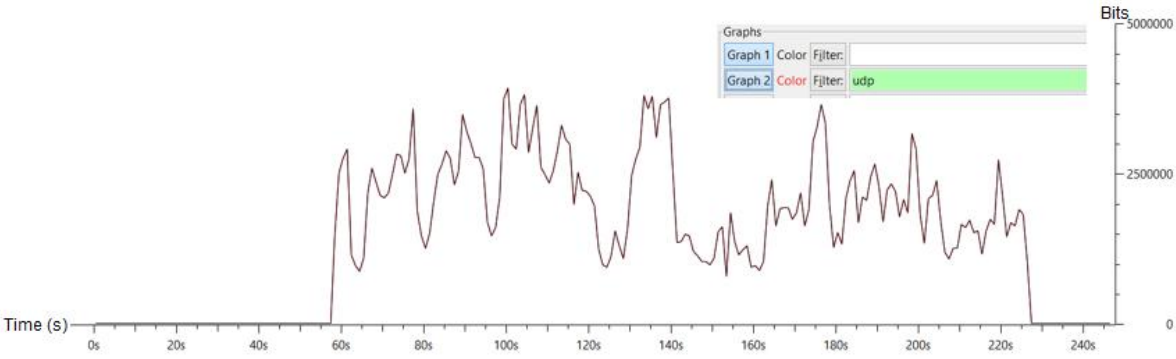


Figura 5.9. Gráfica de tráfico en VLAN de video en escenario 1.

➢ Resumen de resultados

En la tabla 5.1 se muestra el resumen de los resultados del análisis de VoIP obtenidos en este escenario. Recordando que la llamada fue inicializada por el usuario 2 (VLAN de usuarios, AP-3) con dirección IP 192.168.15.253 hacia el usuario 1 (VLAN de VoIP AP-1) con dirección IP 192.168.10.3.

Medición	Resultado
Total de paquetes RTP	9032
Pérdida de paquetes RTP	3 (0.03%)
Secuencias de error	1
Jitter promedio	3.59ms
Máximo *jitter*	14.87ms
Máximo *delta*	108.98ms
Duración	180.72s
Tirados por *buffer jitter*	38(0.4%)
Fuera de secuencia	1(0.0%)
Paquetes perdidos por sec. de error	12 paquetes
Paquetes desfasados por sec. de error	0 paquetes
Tiempo de inestabilidad en sec. de error	1.1s

Tabla 5.1. Análisis de VoIP en redes WDS ***mesh*** parciales con VLAN's, y tráfico medio de fondo.

Como se puede apreciar en la tabla 5.1 las llamadas de voz se pueden llevar acabo, sin problema alguno aún en congestionamiento del enlace con 2.13Mbps, ya que el valor de delta o latencia de la aplicación de VoIP, no supera los 150ms.

La pérdida de paquetes total, considerando los paquetes tirados por buffer y los paquetes perdidos por secuencia de error, no superan el .6%.

$$Pérdida\ de\ paquetes\ total = \left(\frac{38\ + 12 + 3}{9032}\right) = 0.00586 = .59\%$$

Lo cual es un valor muy por debajo del 3% como máximo que puede soportar la aplicación de VoIP para que sea funcional.

Ahora procederemos a realizar el mismo escenario, pero provocando un fallo en uno de los enlaces WDS para ver el tiempo de recuperación, y así determinar si es posible mantener la conexión de la llamada de VoIP.

5.1.2. Análisis de VoIP en redes WDS ***mesh*** parciales con VLAN's, y tráfico medio de fondo, con un fallo de enlace.

La figura 5.10 muestra el diagrama de la ruta del tráfico enviado desde usuario 2 como iniciador de llamada y trasmisor de ráfaga de video, hacia VLAN de VoIP y VLAN de video respectivamente, provocando el fallo en un enlace inalámbrico WDS del AP3, se mostrará el comportamiento de la VLAN de VoIP.

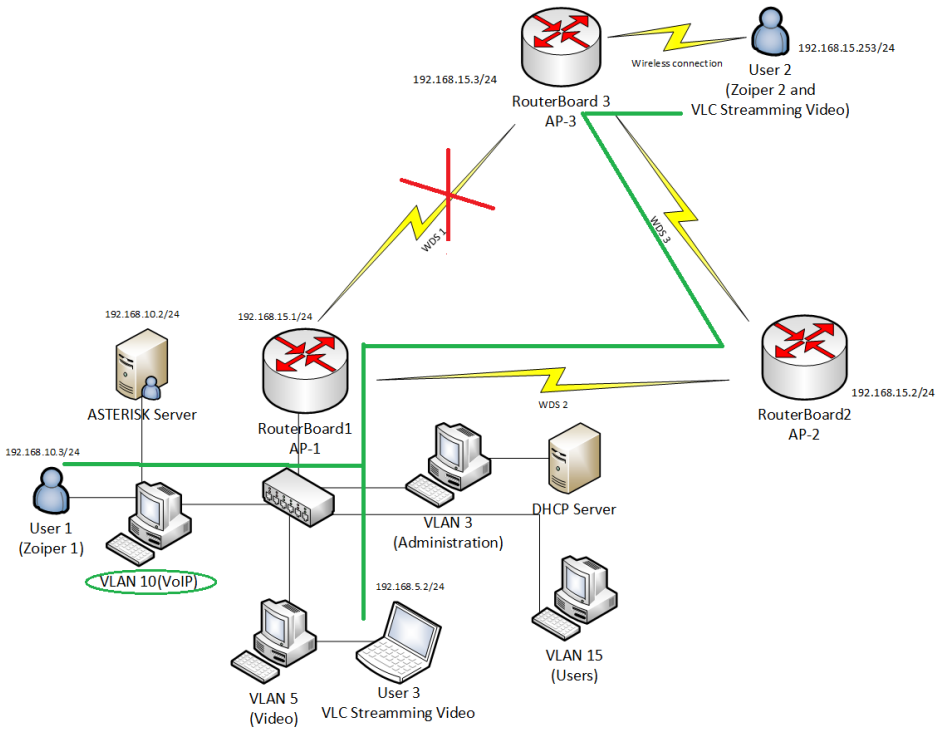


Figura 5.10. Diagrama de la ruta del tráfico en escenario 2 con VLAN´s.

- **Tráfico en VLAN de usuarios**

En la figura 5.11 se puede visualizar el envío y recepción de tráfico RTP (VoIP) y UDP (ráfaga de video) en la VLAN de usuarios

El promedio del tráfico UDP en la VLAN de usuarios fue de 2.1206Mbps, siendo éste el tráfico de video.

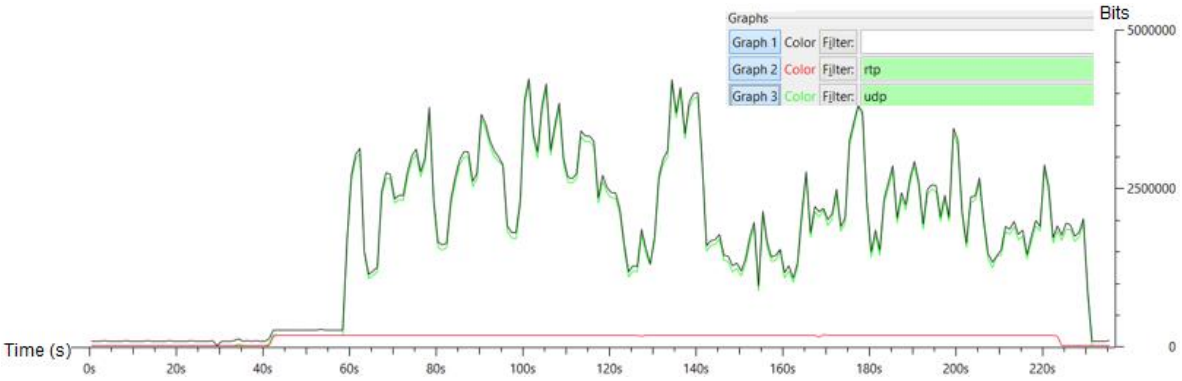


Figura 5.11. Tráfico en la VLAN de usuarios en escenario 2 con VLAN´s.

- ***Paquetes que se recibieron y emitieron en la VLAN de VoIP***

En la figura 5.12 se observa que se están emitiendo y recibiendo un total de 100 paquetes por segundo aproximadamente, en la VLAN de VoIP.

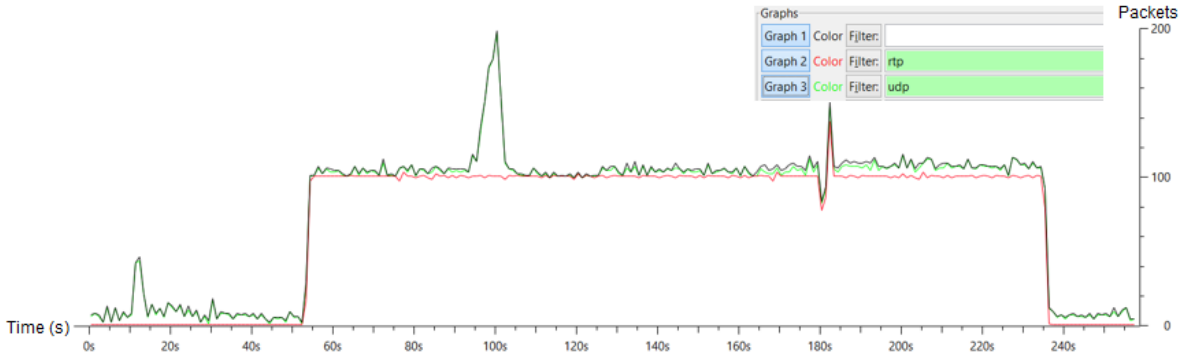


Figura 5.12. Paquetes que se recibieron y emitieron en la VLAN de VoIP en escenario 2.

- ***Utilización en la VLAN de VoIP***

La figura 5.13 muestra la utilización en la VLAN de VoIP de la llamada establecida desde el usuario 2 al usuario 1, la cual fue de 175kbps aproximadamente.

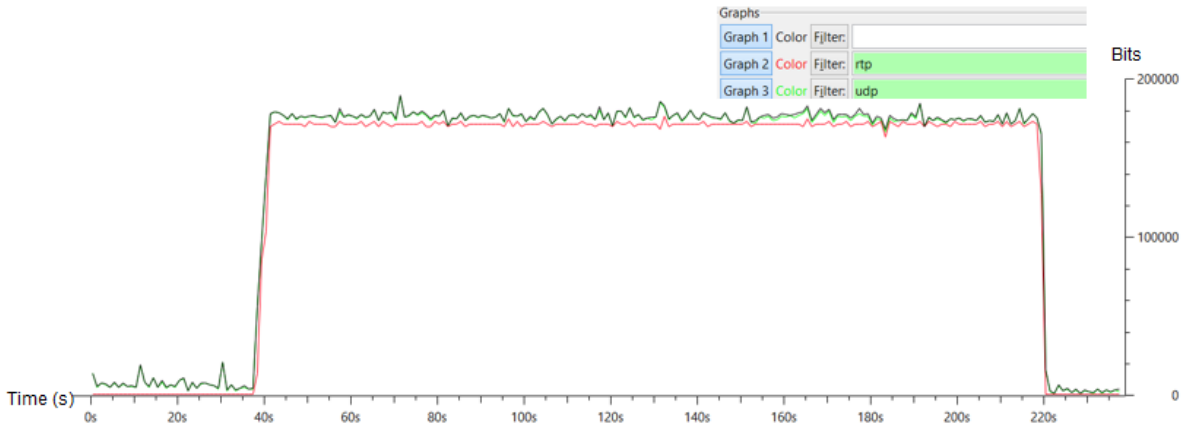


Figura 5.13. Utilización de llamada en la VLAN de VoIP en escenario 2.

- ***Jitter***

El *jitter* promedio del envío fue de 6.32ms y de recepción 3.46ms, un máximo de 6.67ms y 38.62ms respectivamente, como puede apreciarse en la figura 5.14.

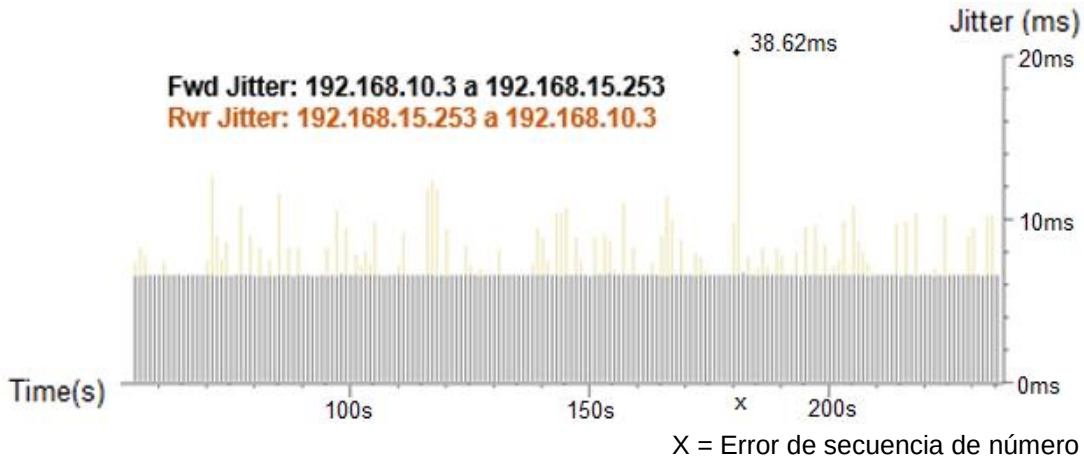
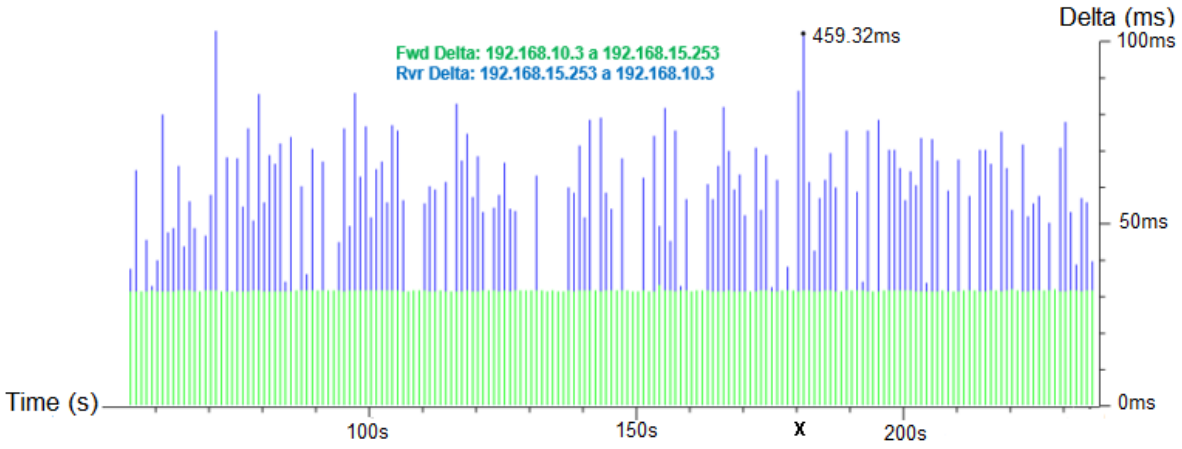


Figura 5.14. *Jitter* en escenario 2 con VLAN's.

- ***Delta***

En el *delta (latencia)* dentro la dirección de envío, se tiene un promedio de 32 ms. *Delta* máximo de 32.96ms en envío y 459.32ms en recepción como se muestra en la figura 5.15:



X = Error de secuencia de número.

Figura 5.15. *Delta* en escenario 2 con VLAN's.

- ***Delta zoom* en error de secuencia de número ¨X¨**

La figura 5.16 muestra gráficamente la voz transmitida en la VLAN de VoIP, capturando el momento donde ocurre el error de secuencia de número*:*

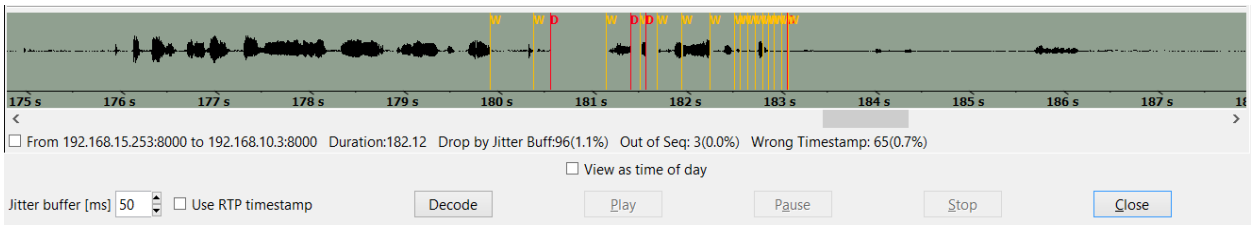


Figura 5.16. Captura de voz en forma gráfica en escenario 2.

El error de secuencia ocurrió aproximadamente en el segundo 180.55.

Realizando un zoom en *delta* en un intervalo dentro del cual ocurre la secuencia de error, se puede concluir que se tuvieron 37 paquetes perdidos y 13 que llegaron desfasados, la inestabilidad fue a partir del segundo 180 al 182.8, siendo 2.8 segundos con inestabilidad.

La figura 5.17 muestra la gráfica del zoom en *delta* cuando ocurre el error de secuencia de número ¨X¨.

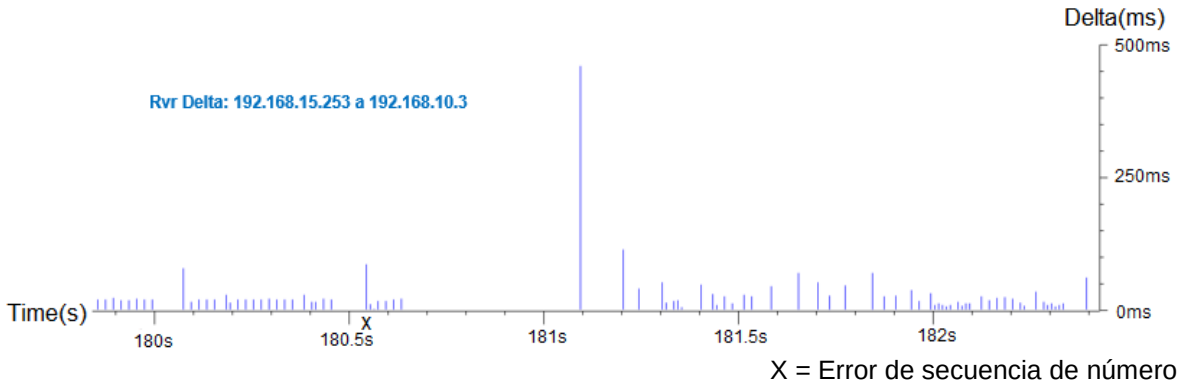


Figura 5.17. *Delta zoom* en error de secuencia de número ¨X¨ en escenario 2.

➢ Tráfico en VLAN de Video

El promedio del tráfico UDP recibido en la VLAN de video fue de 2.1205Mbps, como se muestra en la figura 5.18.

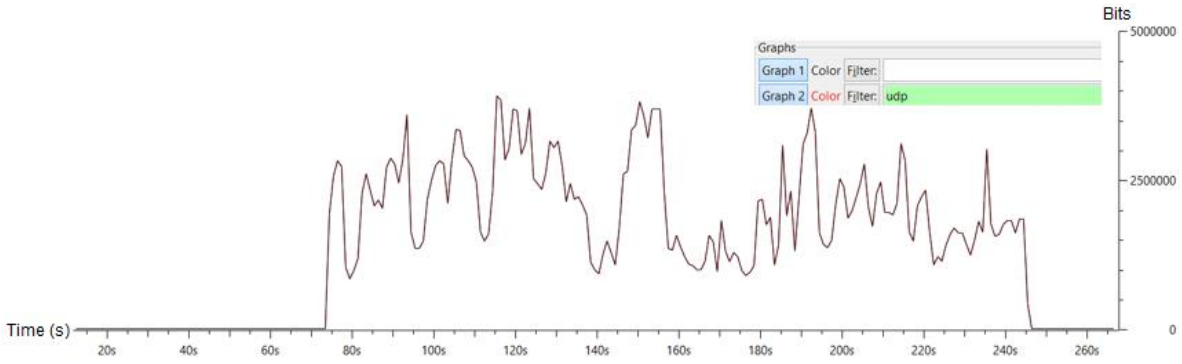


Figura 5.18. Gráfica de tráfico en VLAN de video en escenario 2.

➢ Resumen de resultados

En la tabla 5.2 se muestra el resumen de los resultados del análisis VoIP obtenidos en este escenario. Recordando que la llamada fue inicializada por el usuario 2 (VLAN de usuarios, AP-3) con dirección IP 192.168.15.253 hacia el usuario 1 (VLAN de VoIP AP-1) con dirección IP 192.168.10.3.

Medición	Resultado
Total de paquetes RTP	9083
Pérdida de paquetes RTP	0
Secuencias de error	3
Jitter promedio	3.46ms
Máximo *jitter*	38.62ms
Máximo *delta*	459.32ms
Duración	181.64s
Tirados por *buffer jitter*	96(1.1%)
Fuera de secuencia	3(0.0%)
Paquetes perdidos x sec. de error	37 paquetes
Paquetes desfasados x sec. de error	13 paquetes
Tiempo de inestabilidad en sec. de error	2.8s

Tabla 5.2. Análisis de VoIP en redes WDS ***mesh*** parciales con VLAN's, y tráfico medio de fondo, con un fallo de enlace.

En este escenario, aún cuando se estresó el enlace inalámbrico con tráfico de video, y habiendo provocado la caída de un enlace inalámbrico WDS, el protocolo RSTP tardó aproximadamente 2.8 segundos en restablecer la conectividad. Cabe resaltar que estos 2.8 segundos de reconexión, no provocaron la caída de la llamada VoIP, y la pérdida total de paquetes fue del 1.46%

$$Perdida\ de\ paquetes\ total = \left(\frac{96 + 0 + 37}{9083}\right) = 0.01464 = 1.46\%$$

El cual sigue por debajo del 3% que soporta la aplicación de VoIP.

Ahora procederemos a realizar la misma prueba que en el escenario uno, pero congestionando aún más el enlace, ésto es triplicando el tráfico de fondo y así poder evaluar si la aplicación de VoIP puede ser soportada.

5.1.3. Análisis de VoIP en redes WDS ***mesh*** parciales con VLAN's, y tráfico alto de fondo.

La figura 5.19 muestra el diagrama de la ruta del tráfico enviado desde usuario 2 como iniciador de llamada y trasmisor de ráfaga de video, hacia VLAN de VoIP y VLAN de video respectivamente.

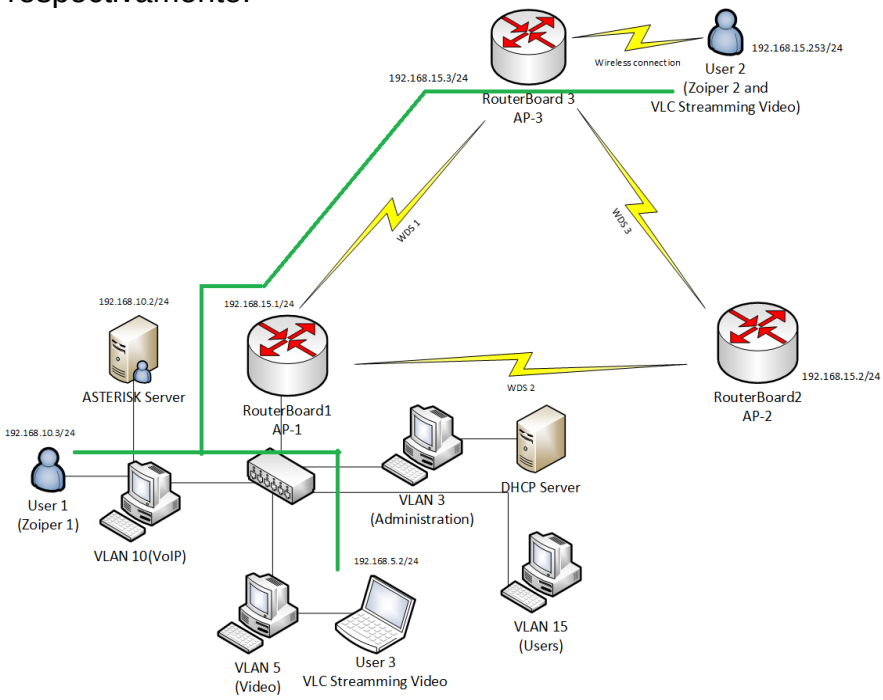


Figura 5.19. Diagrama de la ruta de tráfico en escenario 3 con VLAN's.

- **Tráfico en VLAN de usuarios**

La figura 5.20 muestra el envío y recepción de tráfico RTP (VoIP) y UDP (ráfaga de video) desde la VLAN de usuarios.

El promedio del tráfico UDP en la VLAN de usuarios fue de 6.8914Mbps, siendo éste el tráfico de video.

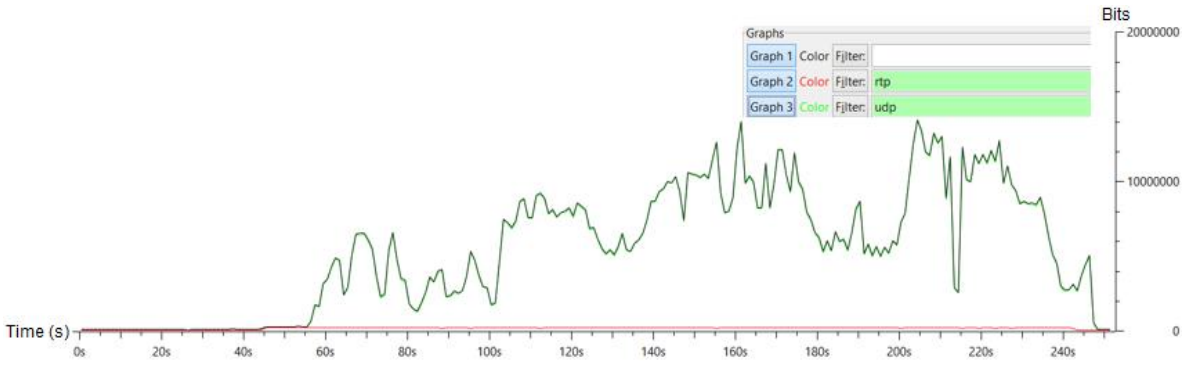


Figura 5.20. Gráfica del tráfico en la VLAN de usuarios en escenario 3 con VLAN's.

- ***Paquetes que se recibieron y emitieron en la VLAN de VoIP***

En la figura 5.21 se observa que se están emitiendo y recibiendo un total de 100 paquetes por segundo aproximadamente, en la VLAN de VoIP.

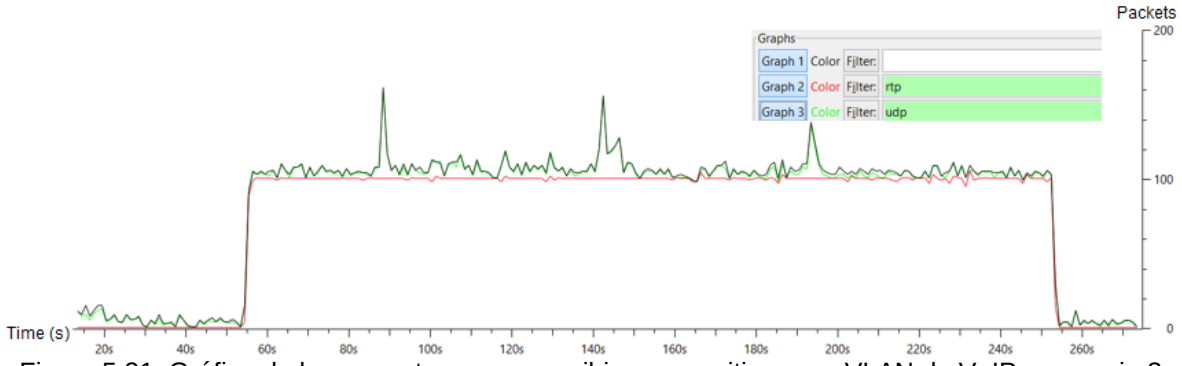


Figura 5.21. Gráfica de los paquetes que se recibieron y emitieron en VLAN de VoIP escenario 3

- ***Utilización en la VLAN de VoIP***

La figura 5.22 muestra la utilización en la VLAN de VoIP de la llamada establecida desde el usuario 2 al usuario 1, la cual fue de 175kbps aproximadamente.

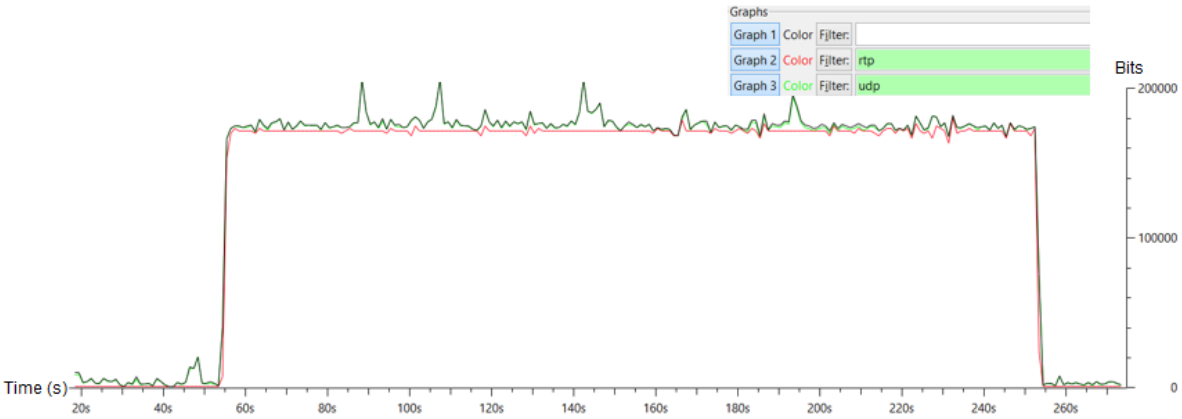
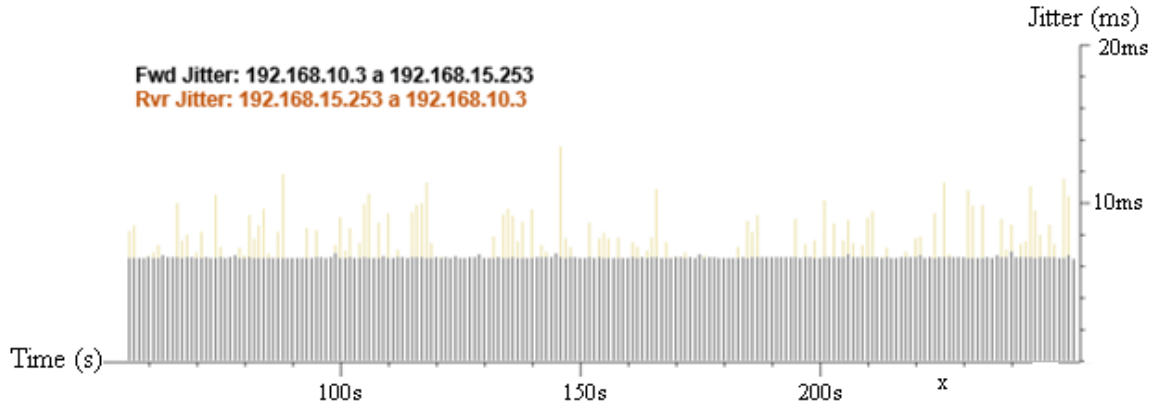


Figura 5.22. Utilización de llamada en VLAN de VoIP en escenario 3.

- ***Jitter***

El *jitter* promedio del envío fue de 6.31ms y de recepción 3.78ms, un máximo de 6.93ms y 13.56ms respectivamente, como puede apreciarse en la figura 5.23.

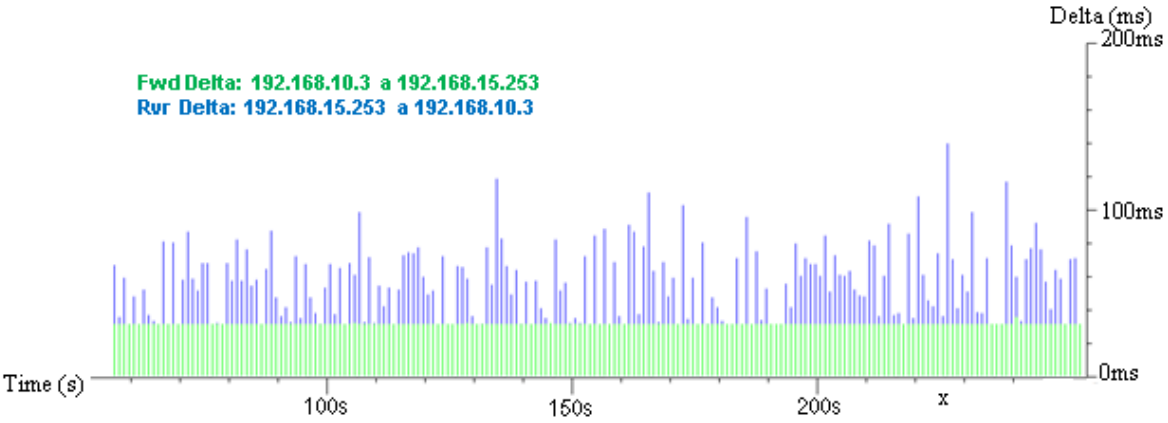


X = Error de secuencia de número

Figura 5.23. *Jitter* en escenario 3 con VLAN's.

- ***Delta***

En *delta (latencia)* en la dirección de envío, se tiene un promedio de 35.54 ms. *Delta* máximo de 35.54ms en envío y 139.92ms en recepción como se muestra en la figura 5.24.



X = Error de secuencia de número.

Figura 5.24. *Delta* en escenario 3 con VLAN's.

- ***Delta zoom* en error de secuencia de número ¨X¨**

La figura 5.24 muestra gráficamente la voz transmitida en la VLAN de VoIP, capturando el momento donde ocurre la secuencia de error de número:

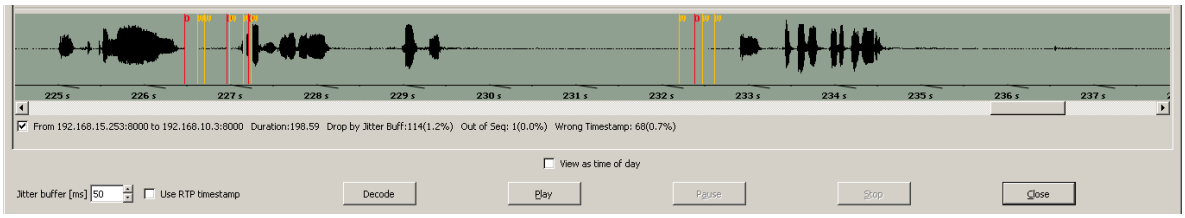


Figura 5.24. Captura de voz en forma gráfica en escenario 3.

El error de secuencia se da en el segundo 225 aproximadamente.

Realizando un *zoom* en un intervalo dentro del cual ocurre la secuencia de error, se puede concluir que se tiene una inestabilidad a partir del segundo 224.3s al 225.8s, con una pérdida de 5 paquetes y 5 paquetes que llegaron desfasados.

Con una duración de la inestabilidad de 1.5s, la figura 5.25 muestra la gráfica del *delta zoom* cuando ocurre el error se secuencia de número ¨X¨.

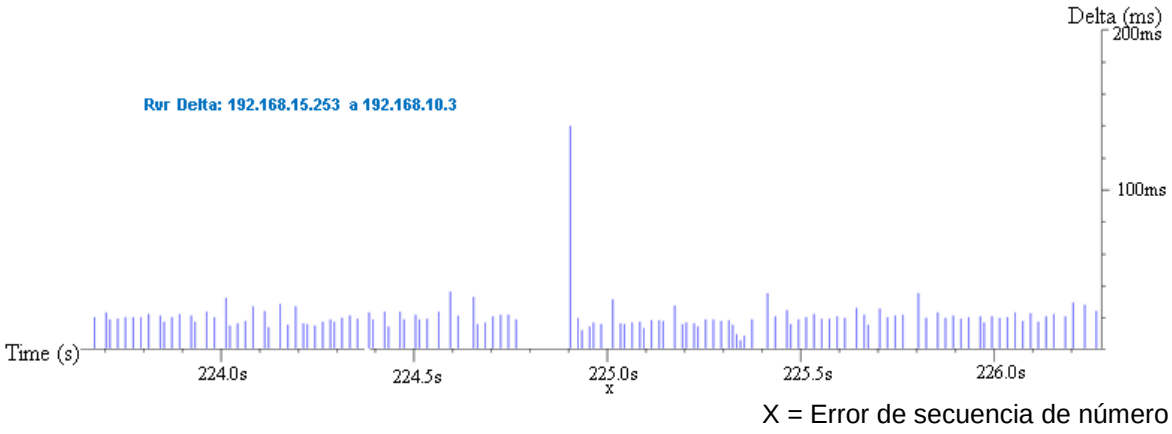


Figura 5.25. *Delta zoom* en error de secuencia de número ¨X¨ en escenario 3.

- **Tráfico en VLAN de video**

  El promedio del tráfico UDP recibido en la VLAN de video fue de 6.8726Mbps, como se muestra en la figura 5.26.

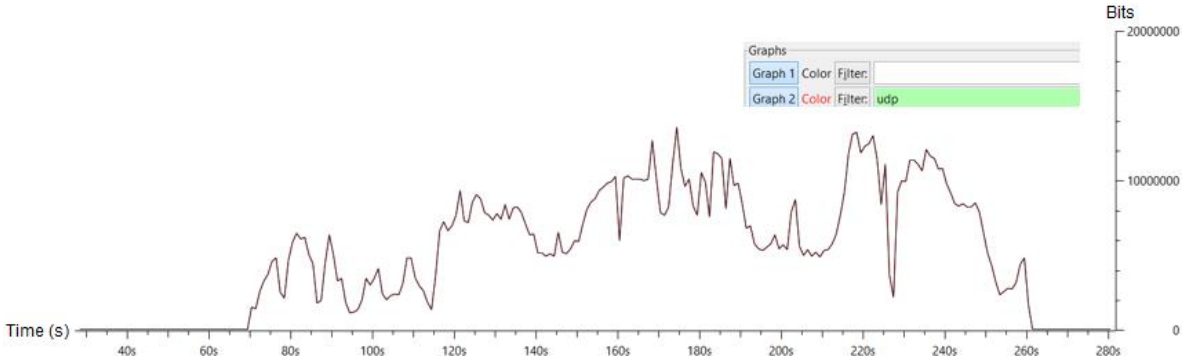


Figura 5.26. Gráfica de tráfico en VLAN de video en escenario 3.

- **Resumen de resultados**

En la tabla 5.3 se muestra el resumen de los resultados del análisis VoIP obtenidos en este escenario. Recordando que la llamada fue inicializada por el usuario 2 (VLAN de usuarios, AP-3) con dirección IP 192.168.15.253 hacia el usuario 1 (VLAN de VoIP AP-1) con dirección IP 192.168.10.3.

Medición	Resultado
Total de paquetes RTP	9890
Pérdida de paquetes RTP	1 (0.01%)
Secuencias de error	1
Jitter promedio	3.78ms
Máximo *jitter*	13.56ms
Máximo *delta*	139.92ms
Duración	197.78s
Tirados por *buffer jitter*	114 (1.2%)
Fuera de secuencia	1 (0.0%)
Paquetes perdidos x sec. de error	5 paquetes
Paquetes desfasados x sec. de error	5 paquetes
Tiempo de inestabilidad en sec. de error	1.5s

Tabla 5.3. Análisis de VoIP en redes WDS ***mesh*** parciales con VLAN's, y tráfico alto de fondo.

Como muestra la tabla 5.3 las llamadas de voz se pueden llevar acabo, sin problema alguno aún en congestionamiento del enlace con 6.89Mbps, ya que el valor de delta o latencia de la aplicación de VoIP, no supera los 150ms.

La pérdida de paquetes total, considerando los paquetes tirados por buffer y los paquetes perdidos por secuencia de error fue del 1.21%.

$$Pérdida\ de\ paquetes\ total = \left(\frac{114\ +5+1}{9890}\right) = 0.01213 = 1.21\%$$

Este porcentaje de pérdida continúa por debajo del 3%, que soporta la aplicación de VoIP.

Ahora procederemos a realizar el mismo escenario con tráfico alto, pero provocando un fallo en uno de los enlaces WDS para ver el tiempo de recuperación, y así determinar si es posible mantener la conexión de la llamada de VoIP nuevamente.

5.1.4. Análisis de VoIP en redes WDS ***mesh*** parciales con VLAN's, y tráfico alto de fondo, con un fallo de enlace.

La figura 5.27 muestra el diagrama de la ruta del tráfico enviado desde usuario 2 como iniciador de llamada y trasmisor de ráfaga de video, hacia VLAN de VoIP y VLAN de video respectivamente, provocando el fallo en un enlace inalámbrico WDS del AP3, se mostrará comportamiento de la VLAN de VoIP.

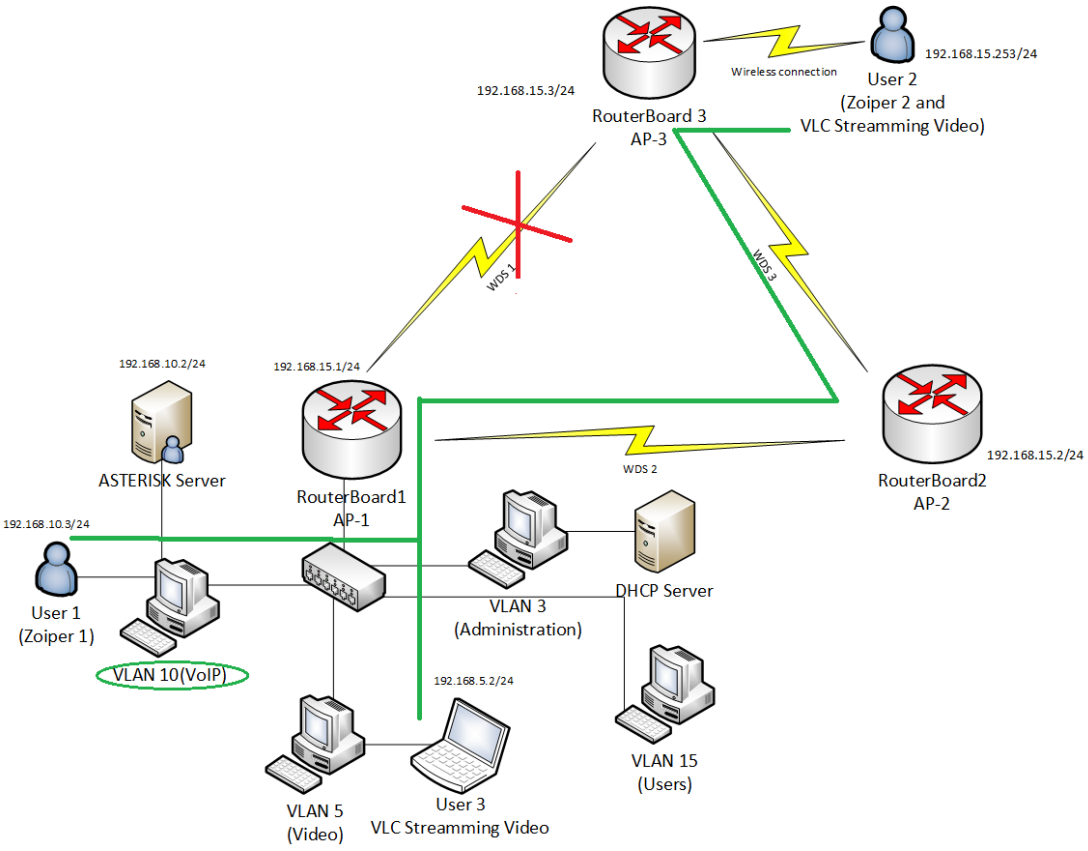


Figura 5.27. Diagrama de la ruta del tráfico en escenario 4 con VLAN's.

- **Tráfico en VLAN de usuarios**

La figura 5.28 muestra el envío y recepción de tráfico RTP (VoIP) y UDP (ráfaga de video) en la VLAN de usuarios.

El promedio de tráfico UDP que se encuentra en la VLAN de usuarios fue de 7044616.16bps o 7.0446Mbps, siendo éste el tráfico de video

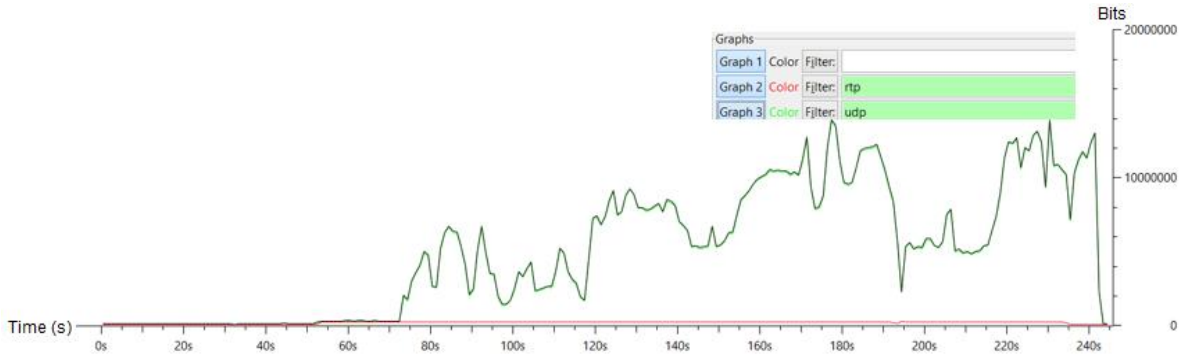


Figura 5.28. Gráfica del tráfico en la VLAN de usuarios en escenario 4 con VLAN's.

- ***Paquetes que se recibieron y emitieron en la VLAN de VoIP***

En la figura 5.29 se observa que se están emitiendo y recibiendo un total de 100 paquetes por segundo aproximadamente, en la VLAN de VoIP.

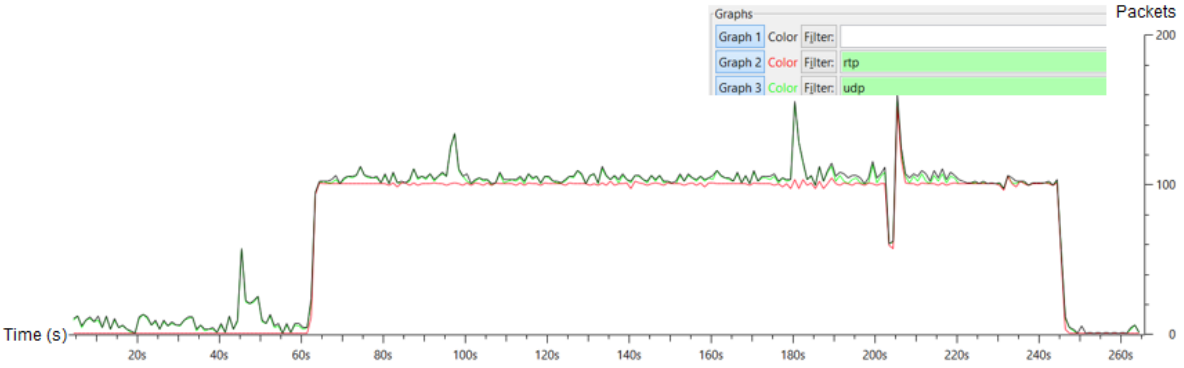


Figura 5.29. Gráfica paquetes que se recibieron y emitieron en VLAN de VoIP en escenario 4.

- ***Utilización en la VLAN de VoIP***

La figura 5.30 muestra la utilización en la VLAN de VoIP de la llamada establecida desde el usuario 2 al usuario 1, la cual fue de 175kbps aproximadamente.

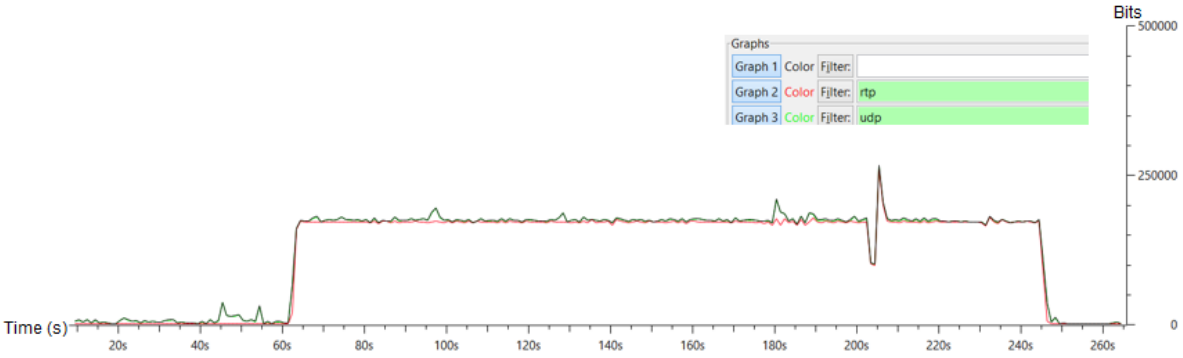


Figura 5.30. Utilización de llamada en VLAN de VoIP en escenario 4.

- ***Jitter***

El *jitter* promedio del envío fue de 6.31ms y de recepción 4.01ms, un máximo de 6.61ms y 65.12ms respectivamente, como puede apreciarse en la figura 5.31:

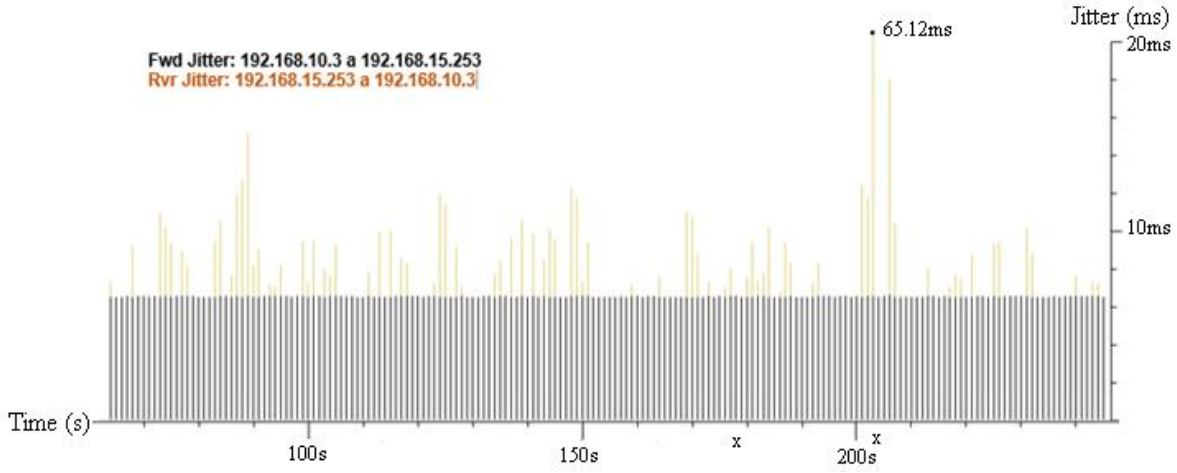


Figura 5.31. *Jitter* en escenario 4 con VLAN's.

- ***Delta***

Dentro de *delta (latencia)* en la dirección de envío se tiene un promedio de 35.54 ms. *Delta* máximo de 31.89ms en envío y 477.51ms en recepción como se muestra en la figura 5.32.

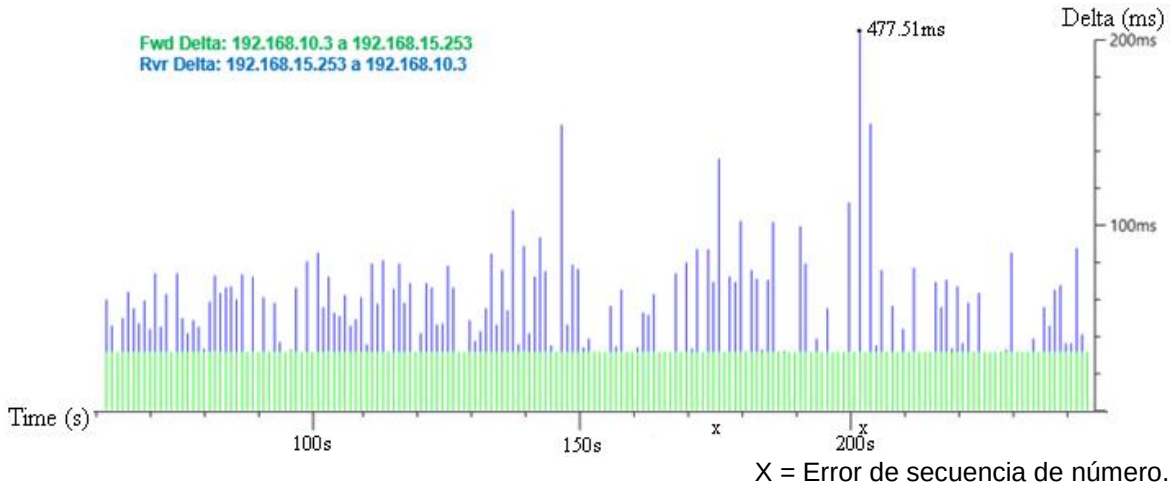


Figura 5.32. *Delta* en escenario 4 con VLAN's.

- ***Delta zoom* en error de secuencia de número ¨X¨**

La figura 5.33 muestra gráficamente la voz transmitida en la VLAN de VoIP, capturando el momento donde ocurre el error secuencia de número.

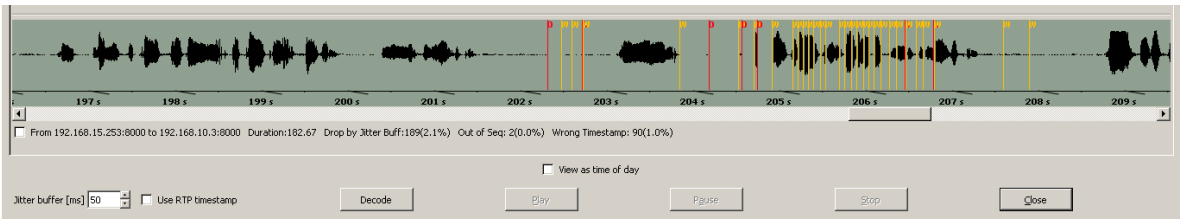
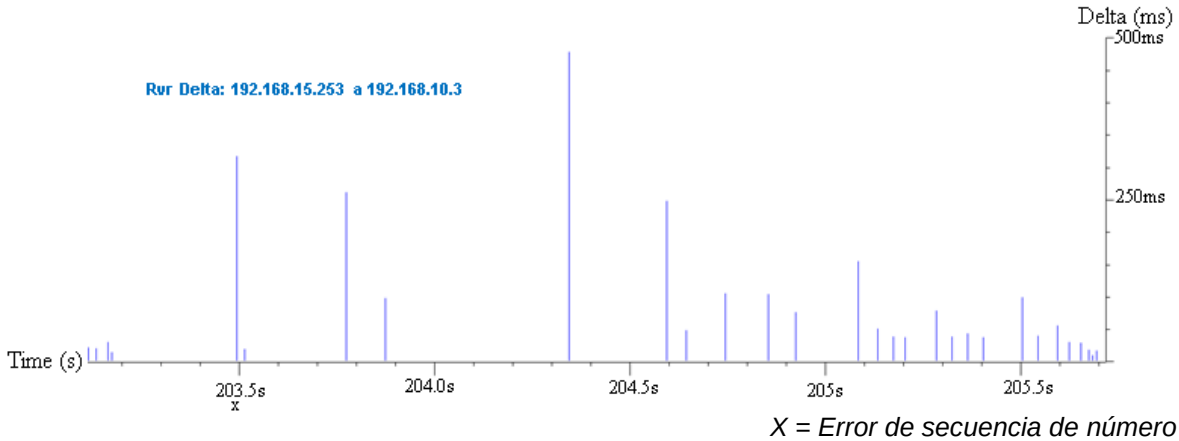


Figura 5.33. Captura de voz en forma gráfica en escenario 4.

Se da el primer error de secuencia de número en el segundo 177.7 y el segundo error en el segundo 203.5. Nos enfocaremos al segundo error de secuencia de número, que es donde realmente se dispara el valor del *jitter* y del *delta*.

Realizando un *zoom* en un intervalo dentro del cual ocurre la segunda secuencia de error, se puede concluir que la inestabilidad debido a la falla se dio a partir del segundo 203.1s hasta 206.3s, teniendo un total de 3.2s con inestabilidad. Se tuvieron 77 paquetes perdidos y 23 llegaron con retraso en el intervalo mencionado anteriormente. La figura 5.34 muestra la gráfica del *zoom delta* cuando ocurre el segundo error de secuencia de número ¨X¨.



X = Error de secuencia de número

Figura 5.34. *Delta zoom* en el segundo error de secuencia de número ¨X¨ en escenario 4.

➢ Tráfico en VLAN de video

El promedio del tráfico UDP recibido en la VLAN de video fue de 7015192.71bps o 7.0152Mbps, como se muestra en la figura 5.35.

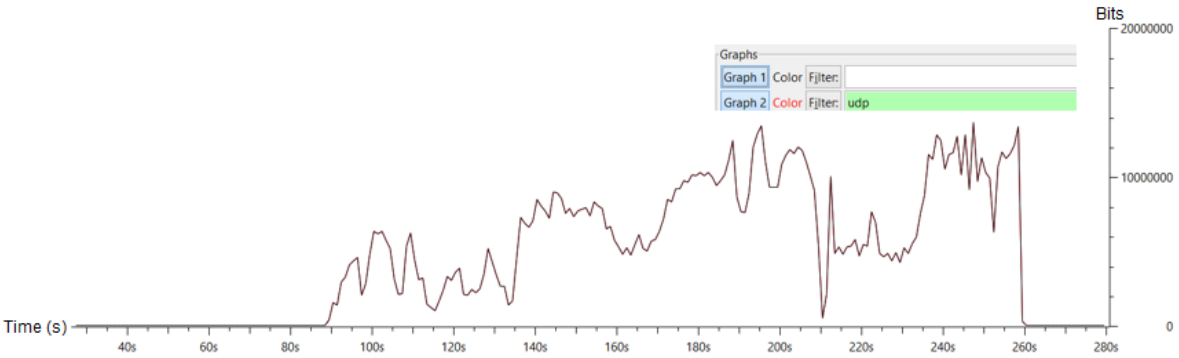


Figura 5.35. Gráficas de tráfico en VLAN de video en escenario 4.

➢ Resumen de resultados

En la tabla 5.4 se muestra el resumen de los resultados del análisis VoIP obtenidos en este escenario. Recordando que la llamada fue iniciada por el usuario 2 (VLAN de usuarios, AP-3) con dirección IP 192.168.15.253 hacia el usuario 1 (VLAN de VoIP AP-1) con dirección IP 192.168.10.3.

Medición	Resultado
Total de paquetes RTP	9098
Pérdida de paquetes RTP	18 (0.20%)
Secuencias de error	2
Jitter promedio	4.01ms
Máximo *jitter*	65.12ms
Máximo *delta*	477.51ms
Duración	181.94s
Tirados por *buffer jitter*	189 (2.1%)
Fuera de secuencia	2 (0.0%)
Paquetes perdidos x sec. de error	77 paquetes
Paquetes desfasados x sec. de error	23 paquetes
Tiempo de inestabilidad en sec. de error	3.2s

Tabla 5.4. Análisis de VoIP en redes WDS ***mesh*** parciales con VLAN's, y tráfico alto de fondo, con un fallo de enlace.

En este escenario, aún cuando se estreso el enlace con tráfico alto de fondo, en comparación con los dos primeros escenarios, y habiendo provocado la caída de un enlace inalámbrico WDS, el protocolo RSTP tardo aproximadamente 3.2 segundos en restablecer la conectividad. Cabe resaltar que estos 3.2 segundos de reconexión no provocaron la caída de la llamada de VoIP, y la pérdida total de paquetes fue del 3.12%.

$$Pérdida\ de\ paquetes\ total = \left(\frac{189 + 77 + 18}{9098}\right) = 0.03121 = 3.12\%$$

Este valor se encuentra un .12% por arriba de lo que soporta la aplicación de VoIP. Además el valor de *delta* o *latencia* máximo supera los 150ms, resultado del fallo en el enlace inalámbrico.

A continuación se procederá a evaluar dos escenarios, dentro de los cuales se omitirán las configuraciones de VLAN's en la red ***mesh*** parcial, congestionando la red con tráfico de fondo alto, para así poder evaluar si la aplicación de VoIP es funcional.

5.2. Comportamiento dinámico de VoIP en redes WDS ***mesh*** parciales, sin VLAN´s

5.2.1. Análisis de VoIP en redes WDS ***mesh*** parciales sin VLAN's, y tráfico alto de fondo.

La figura 5.36 muestra el diagrama de la ruta del tráfico enviado desde usuario 2, como iniciador de llamada y trasmisor de ráfaga de video, hacia el usuario 1 y usuario 3 de video respectivamente.

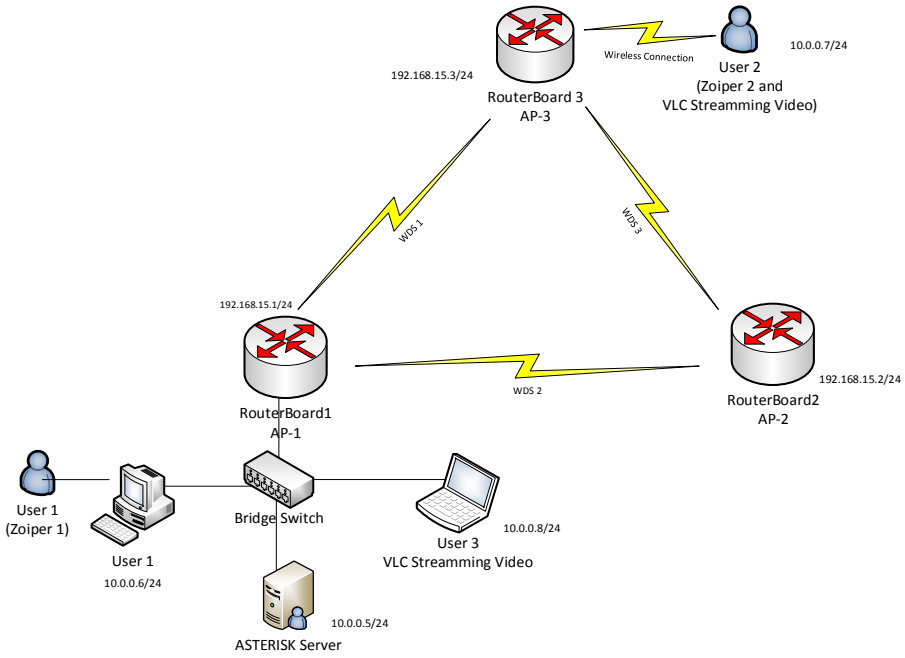


Figura 5.36. Diagrama de la ruta de tráfico, en escenario 5 sin VLAN's.

- **Tráfico en enlace WDS1**

La figura 5.37 muestra el envío y recepción del tráfico RTP (VoIP) y UDP (ráfaga de video), en el enlace WDS1.

El tráfico UDP que existe en el enlace de usuarios es de 4.4050Mbps, siendo éste el tráfico de video.

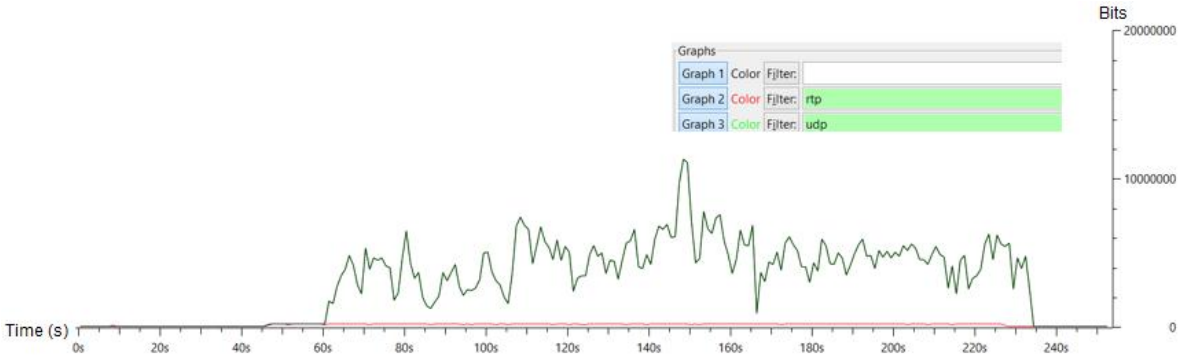


Figura 5.37. Gráfica del tráfico en el enlace inalámbrico del AP3, en escenario 5 sin VLAN's.

- ***Paquetes VoIP que se recibieron y emitieron en AP1***

En la figura 5.38 se observa que el promedio de paquetes de VoIP capturados (emitidos y recibidos), fue de 100 paquetes por segundo aproximadamente en el AP 1.

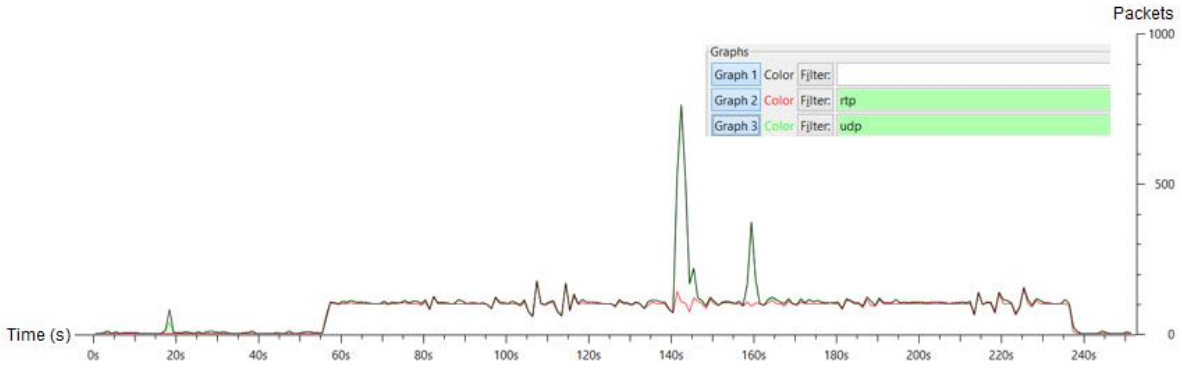


Figura 5.38. Gráfica paquetes VoIP que se recibieron y emitieron en AP 1 en escenario 5.

- ***Utilización de llamada VoIP en AP 1***

La figura 5.39 muestra la utilización de la llamada establecida desde el usuario 2 al usuario 1, la cual fue de 175kbps aproximadamente.

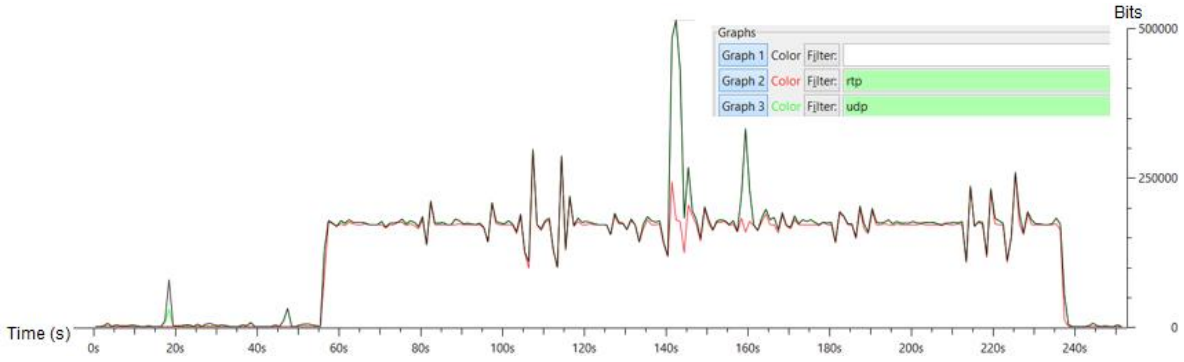


Figura 5.39. Utilización de llamada de VoIP en AP 1 en escenario 5.

- ***Jitter***

El *jitter* promedio del envío fue de 6.34ms y de recepción 9.74ms, un máximo de 7.49ms y 80.85ms respectivamente, como puede apreciarse en la figura 5.40.

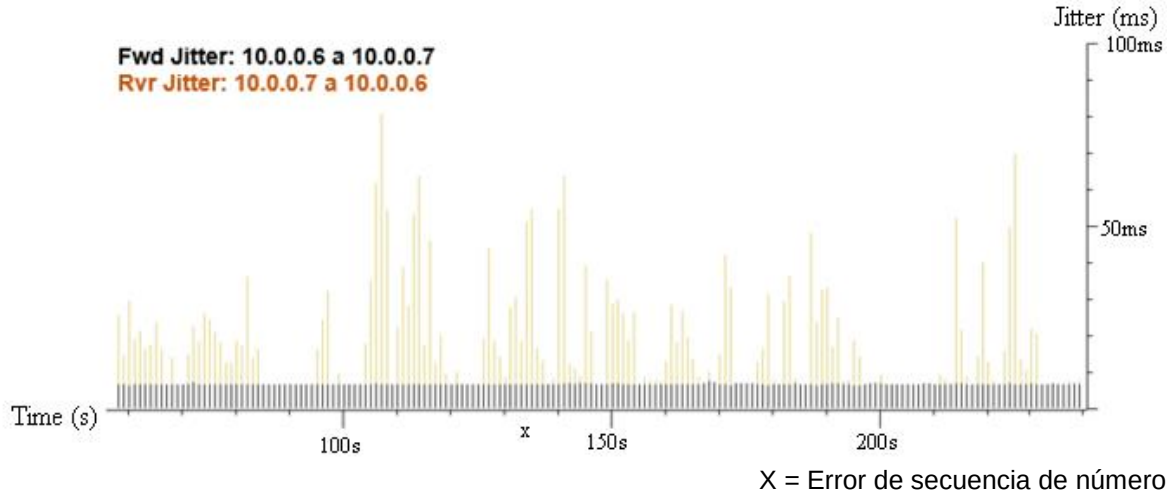


Figura 5.40. *Jitter* en escenario 5 sin VLAN's.

- ***Delta***

En *delta (latencia)* en la dirección de envío se tiene un promedio de 31.35 ms. *Delta* máximo de 36.67ms en envío y 673.17ms en recepción, como se muestra en la figura 5.41.

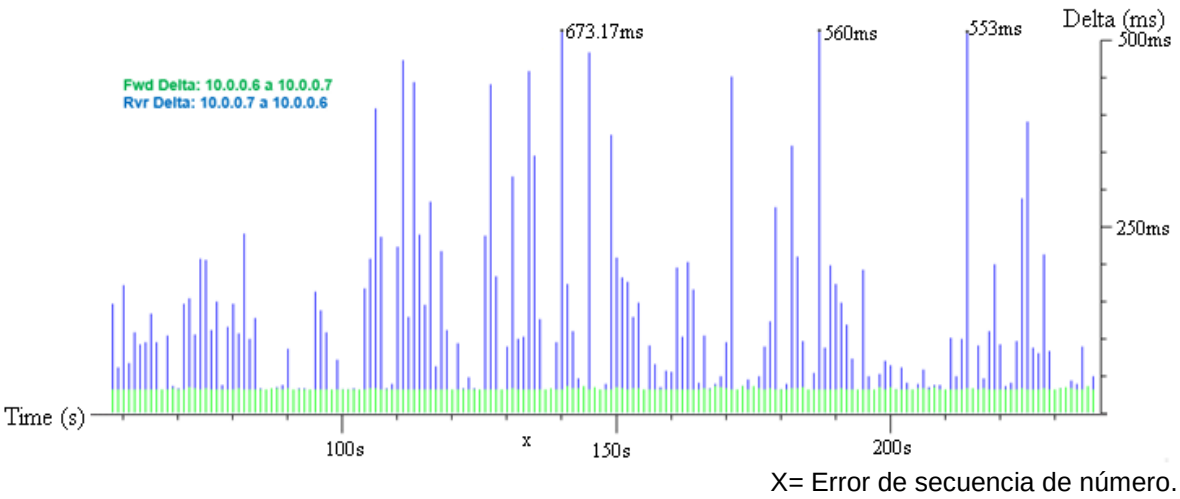


Figura 5.41. *Delta* en escenario 5 sin VLAN's.

- ***Delta zoom* en error de secuencia de número ¨X¨**

La figura 5.42 muestra gráficamente la voz transmitida al usuario 1, capturando el momento donde ocurre la secuencia de error de número.

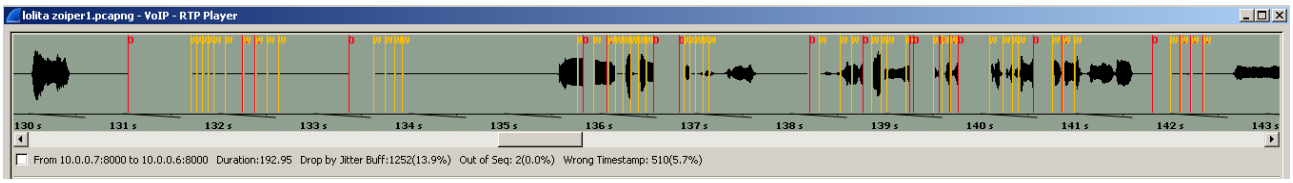


Figura 5.42. Captura de voz en forma gráfica en escenario 5.

El primer error de secuencia de número fue dado en el tiempo 134.3s y el segundo error de secuencia fue dado en el tiempo 134.35s**.**

Realizando un *zoom* en un intervalo dentro del cual ocurre la secuencia de error, se puede concluir que la inestabilidad empezó a partir del segundo 132.7 al 135.6 siendo un total de 2.9 s. Se perdieron 51 paquetes y 17 llegaron desfasados durante la inestabilidad. La figura 5.43 muestra la gráfica de *zoom delta* cuando ocurren los errores de secuencia de número ¨X¨.

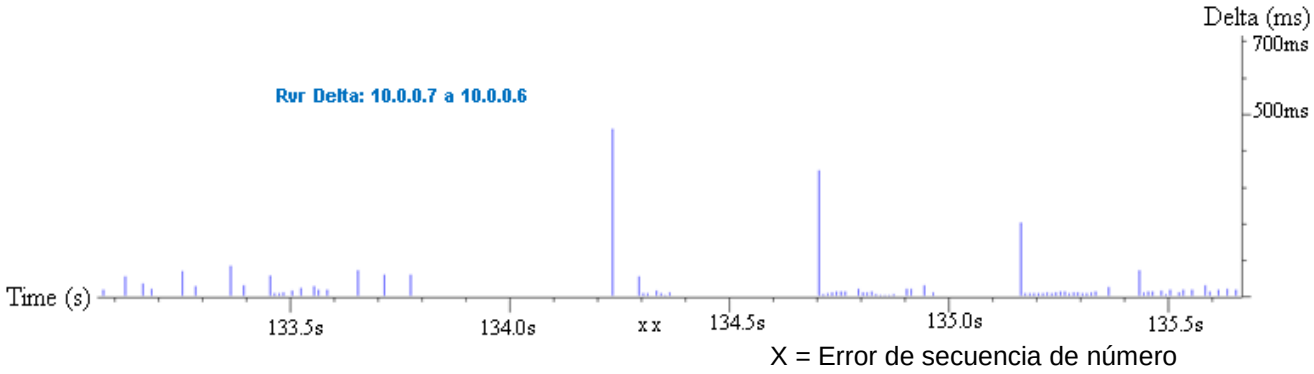


Figura 5.43. *Delta zoom* en los errores de secuencia de número ¨X¨ en escenario 5.

➢ Tráfico de video

El tráfico UDP recibido en el AP 1 o usuario 3 fue de 4.4007Mbps aproximadamente, como se muestra en la figura 5.44.

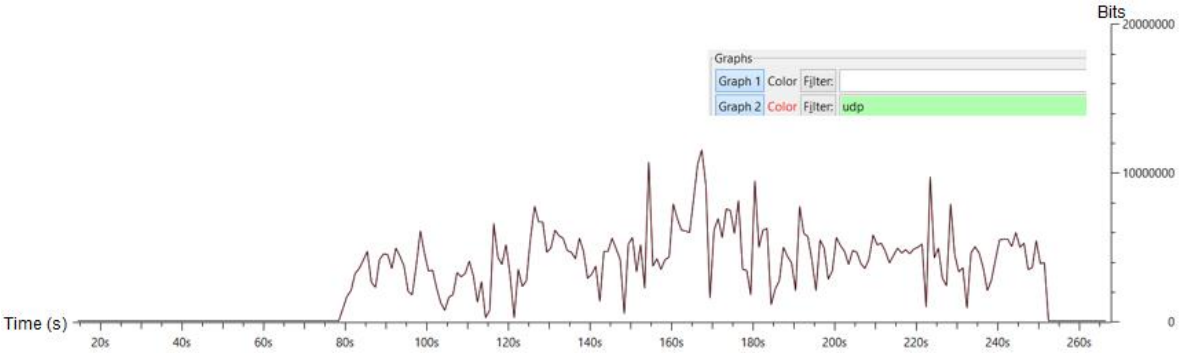


Figura 5.44. Gráfica de tráfico de video en usuario 3 o AP1 en escenario 5.

➢ Resumen de resultados

En la tabla 5.5 se muestra el resumen de los resultados del análisis VoIP obtenidos en este escenario. Recordando que la llamada fue inicializada por el usuario 2 (AP-3) con dirección IP 10.0.0.7 hacia el usuario 1 (AP-1) con dirección IP 10.0.0.6.

Medición	Resultado
Total de paquetes RTP	9039
Pérdida de paquetes RTP	17(0.19%)
Secuencias de error	2
Jitter promedio	9.74ms
Máximo *jitter*	80.85ms
Máximo *delta*	673.17ms
Duración	180.29s
Tirados por *buffer jitter*	1252(13.9%)
Fuera de secuencia	2 (0.0%)
Paquetes perdidos x sec. de error	51 paquetes
Paquetes desfasados x sec. de error	17 paquetes
Tiempo de inestabilidad en sec. de error	2.9s

Tabla 5.5. Análisis de VoIP en redes WDS ***mesh*** parciales sin VLAN's, y tráfico alto de fondo.

Como puede apreciarse en la tabla 5.5, las llamadas de VoIP no pueden llevarse a cabo de forma funcional, ya que la pérdida de paquetes total supera el valor del 3% permitido, para soportar la aplicación de VoIP. Sin embargo, esta situación no provoco la caída de la llamada de VoIP, a pesar de existir un tráfico de fondo alto de por medio.

$$Pérdida\ de\ paquetes\ total = \left(\frac{1252\ + 51 + 17}{9039}\right) = 0.14603 = 14\%$$

Además del 14% de la pérdida de paquetes totales, el valor de delta o latencia de la aplicación de VoIP supera los 150ms en su valor máximo de forma notable.

Ahora procederemos a realizar el mismo escenario con tráfico alto, pero provocando un fallo en uno de los enlaces WDS para ver el tiempo de recuperación, y así determinar si es posible mantener la conexión de la llamada de VoIP nuevamente.

5.2.2 Análisis de VoIP en redes WDS ***mesh*** parciales sin VLAN's, y tráfico alto de fondo, con un fallo de enlace

La figura 5.45 muestra el diagrama de la ruta del tráfico enviado desde usuario 2 (AP-3) como iniciador de llamada y trasmisor de ráfaga de video, hacia el usuario 1 (AP-1) y usuario 3 (AP-1) de video respectivamente.

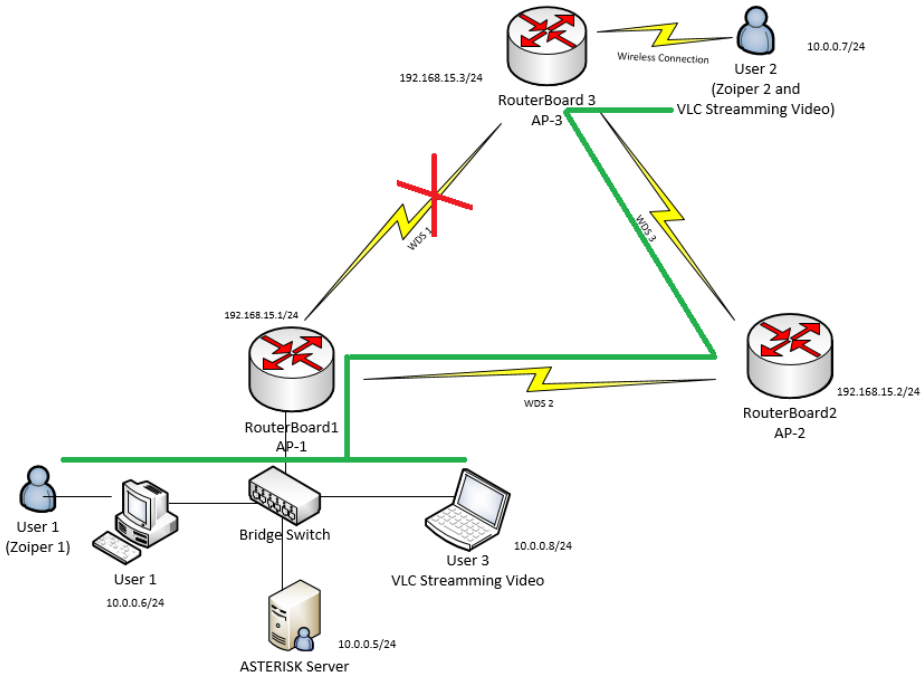


Figura 5.45. Diagrama de la ruta de tráfico en caso 6 sin VLAN's.

- **Tráfico entre usuarios**

La figura 5.46 muestra el envío y recepción de tráfico RTP (VoIP) a usuario 1 desde el usuario 2 y UDP (ráfaga de video) a usuario 3.

El tráfico UDP enviado al usuario 3 es de 4.0861Mbps aproximadamente, siendo éste el tráfico de video.

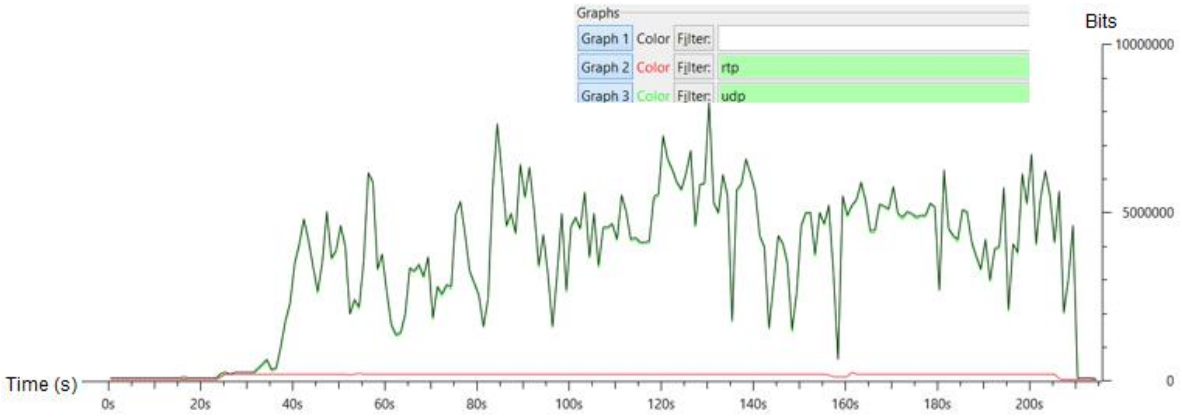


Figura 5.46. Gráfica del tráfico emitido y recibido entre usuarios.

- ***Paquetes de VoIP que se recibieron y emitieron en AP 1***

En la figura 5.47 se observa que el promedio de paquetes de VoIP capturados (emitidos y recibidos), fue de un total de 100 paquetes por segundo aproximadamente en el AP1.

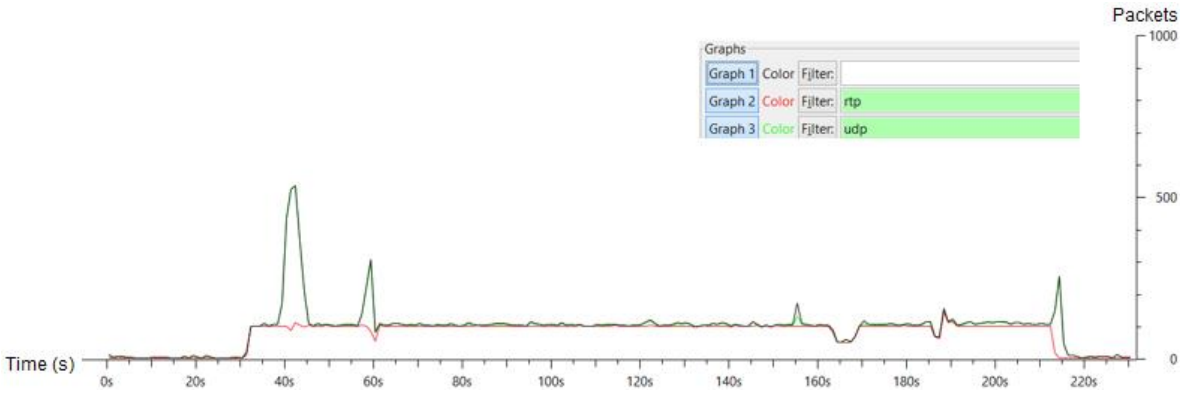


Figura 5.47. Gráfica paquetes VoIP que se recibieron y emitieron en AP1 en escenario 6.

- ***Utilización de llamada de VoIP en el AP 1***

La figura 5.48 muestra la utilización de la llamada establecida desde el usuario 2 al usuario 1, la cual fue de 175kbps aproximadamente.

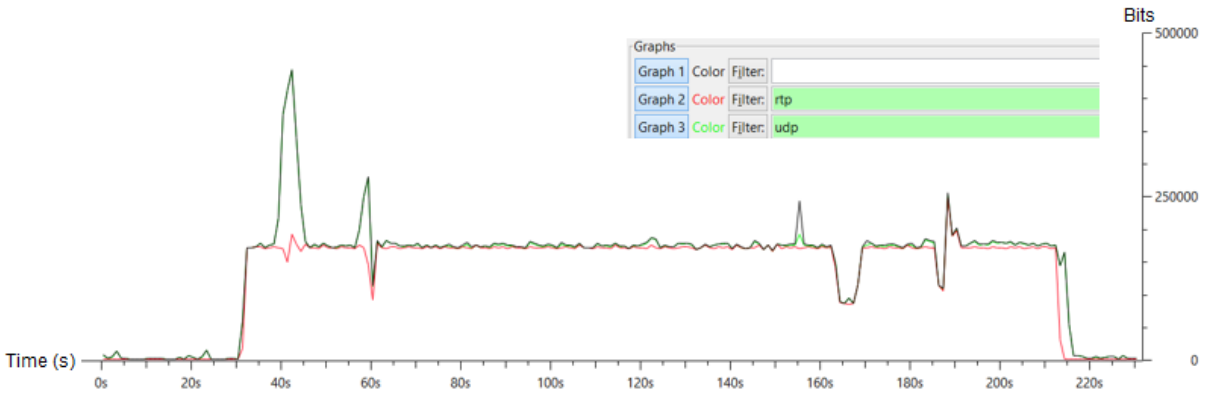


Figura 5.48. Utilización de llamada de VoIP en AP 1 en escenario 6.

- ***Jitter***

El *jitter* promedio del envío fue de 6.34ms y de recepción 3.72ms, un máximo de 7.13ms y 56.40ms respectivamente, como puede apreciarse en la figura 5.49.

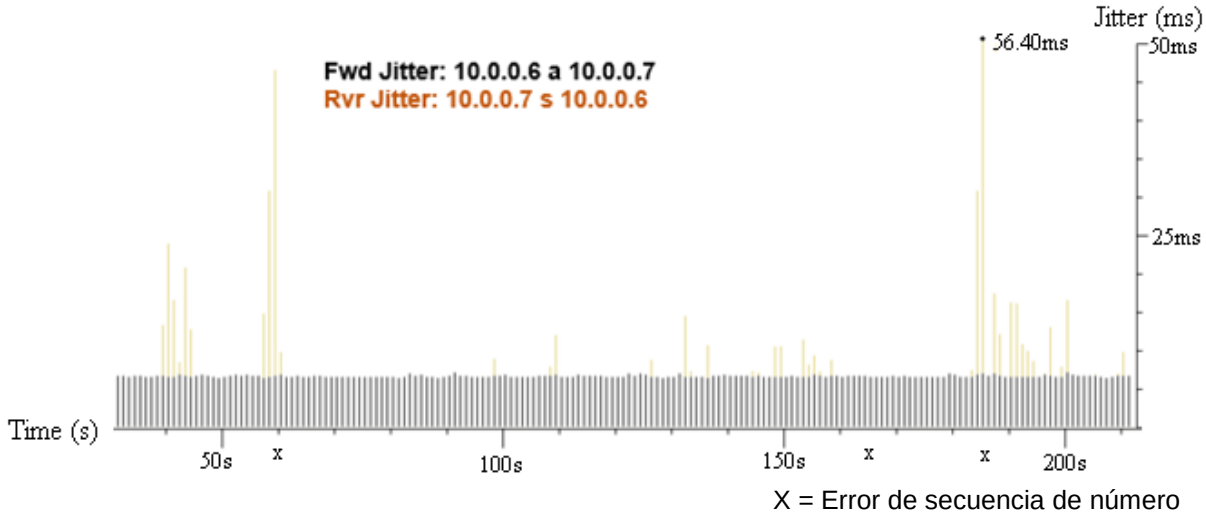


Figura 5.49. *Jitter* en escenario 6 sin VLAN's.

- ***Delta***

En el *delta (latencia)* en la dirección de envío se tiene un promedio de 31.35 ms. *Delta* máximo de 36.50ms en envío y 5040.54ms (5.04s) en recepción, como se muestra en la figura 5.50.

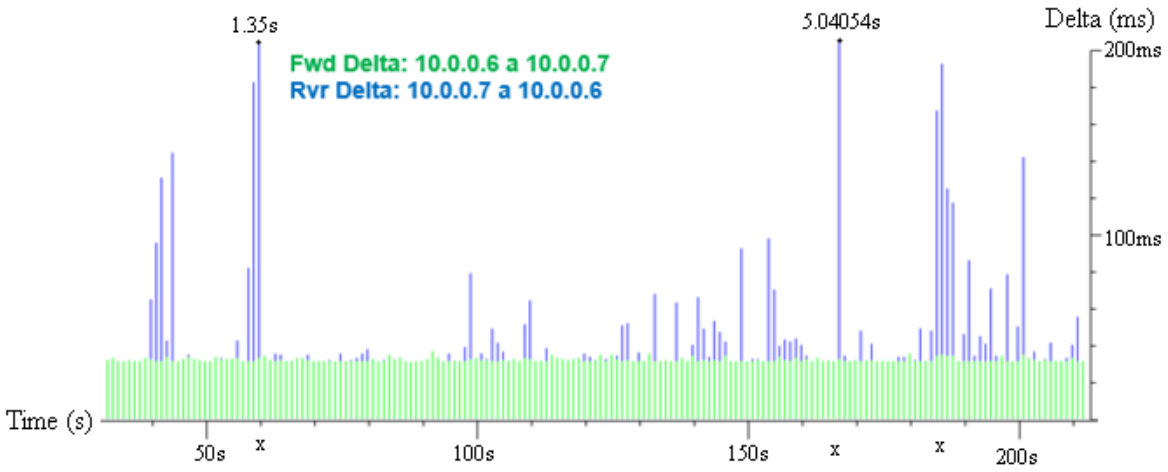


Figura 5.50. *Delta* en escenario 6 sin VLAN's.

Se pueden observar 3 errores de secuencia de número, sin embargo solo se estudiara el error con mayor valor de *delta* que en su caso fue de 5.04054s con el valor en tiempo 168.8s.

- ***Delta zoom* en error de secuencia de número ¨X¨**

La figura 5.51 muestra gráficamente la voz transmitida al usuario 1 de VoIP, capturando el momento donde ocurre la secuencia de error de número con mayor valor de *delta,* dentro de este escenario.

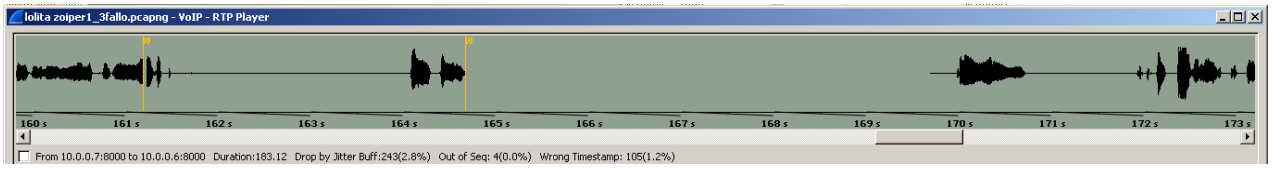


Figura 5.51. Captura de voz en forma gráfica en escenario 6.

El mayor error de secuencia ocurrió en el segundo 168.8, por tanto nos basaremos en éste.

Realizando un *zoom* en un intervalo dentro del cual ocurre la secuencia de error, se puede indicar que la inestabilidad comenzó en el segundo 163.7 al 168.8, y se tuvieron 250 paquetes perdidos en ese intervalo de 5.1s que fue dado el fallo en el enlace WDS del AP 3. La figura 5.52 muestra la gráfica del *zoom delta* cuando ocurre el error de secuencia de número ¨X¨.

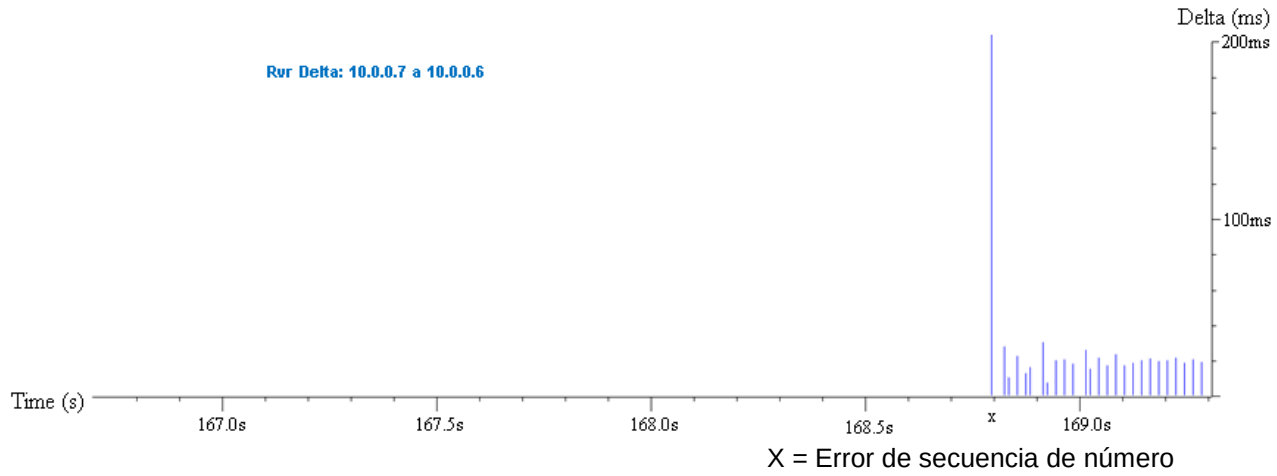


Figura 5.52. *Delta zoom* en el error de secuencia de número ¨X¨ en escenario 6.

➢ Tráfico de Video

El tráfico UDP recibido en el AP 1 o usuario 3 fue de 3.9589Mbps aproximadamente, como se muestra en la figura 5.53.

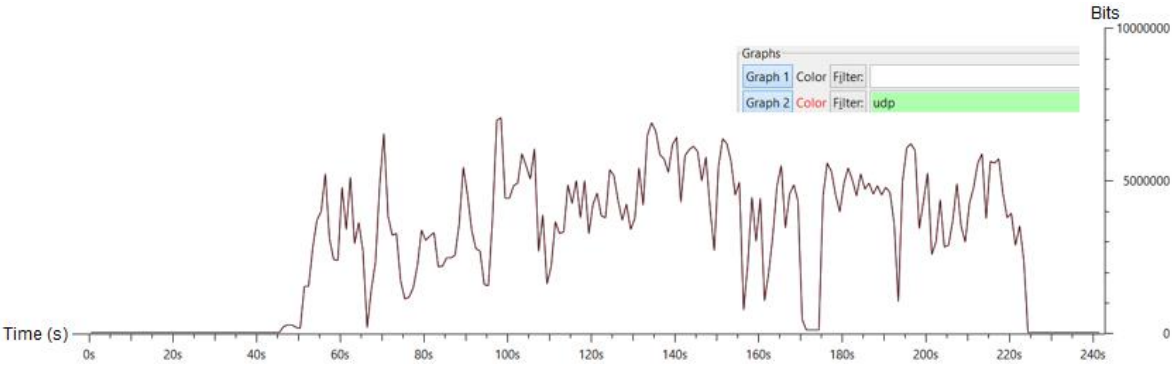


Figura 5.53. Gráfica de tráfico de video en usuario 3 o AP 1 en escenario 6.

➢ Resumen de resultados

En la tabla 5.6 se muestra el resumen de los resultados del análisis VoIP obtenidos en este escenario. Recordando que la llamada fue inicializada por el usuario 2 (AP 3) con dirección IP 10.0.0.7 hacia el usuario 1 (AP 1) con dirección IP 10.0.0.6.

Medición	Resultado
Total de paquetes RTP	9076
Pérdida de paquetes RTP	313(3.45%)
Secuencias de error	4
Jitter promedio	3.72ms
Máximo *jitter*	56.40ms
Máximo *delta*	5040.54ms
Duración	181.05s
Tirados por *buffer jitter*	243(2.8%)
Fuera de secuencia	4 (0.0%)
Paquetes perdidos x sec. de error	250 paquetes
Paquetes desfasados x sec. de error	0 paquetes
Tiempo de inestabilidad en sec. de error	5.1s

Tabla 5.6. Análisis de VoIP en redes WDS ***mesh*** parciales sin VLAN's, y tráfico alto de fondo, con un fallo de enlace.

En este último escenario, se estresó el enlace inalámbrico con tráfico alto utilizando video, y habiendo provocado el fallo de un enlace inalámbrico WDS, la conectividad fue reestablecida después de 5.1 segundos provocando la caída de la llamada de VoIP, y la pérdida total de paquetes fue de 8.88%.

$$Pérdida\ de\ paquetes\ total = \left(\frac{313\ + 250 + 243}{9076}\right) = 0.0888 = 8.88\%$$

El valor de la pérdida de paquetes total, está muy por arriba del que soporta la aplicación de VoIP, además de que el valor de *delta* o *latencia* de la aplicación supera notablemente el valor de 150ms. Por todos estos aspectos, se llegó a la conclusión de que la implementación de VoIP en este escenario sin VLAN's es completamente no funcional en todos los aspectos.

5.3. Análisis del códec G.711 a través de la red implementada

Debido a que se utilizó el códec G.711 para la trasmisión de VoIP, se analizaran sus parámetros y los encabezados que registraron durante las pruebas:

- $Tasa\ de\ paquetes\ = 100 \frac{paquetes}{segundo}$

  Cada 10 ms se transmite un paquete, esto es: $\frac{1\ segundo}{100\ paquetes} = 0.01 = 10ms$

- $BW = Tasa\ de\ datos = 64kbps$

$$BW = (Tasa\ de\ paquetes) \times (Tamaño\ de\ paquete) = [bps]$$

- $Tamaño\ de\ paquete = \frac{BW}{Tasa\ de\ paquetes} = \left[\frac{Bytes}{Paquete}\right]$

$$Tamaño\ de\ paquete = \frac{64kbps}{100\frac{paquetes}{s}} = 640\frac{bits}{paquete} = 80\frac{Bytes}{paquetes}$$

Análisis de *frame* de 214 Bytes capturado

De acuerdo con la captura realizada a través de *Wireshark,* se logró visualizar la etapa de encapsulación y la agregación de encabezados en los paquetes RTP. Se encapsularon dos paquetes consecutivos, siendo de 160 bytes (2 × 80 bytes), agregándole la cabecera de RTP / UDP de 20 bytes, IP de 20 bytes y finalmente el encabezado Ethernet de 14 bytes, nos da un total de 214 Bytes por *frame*.

Obteniendo de ésta forma 50 paquetes transmitidos por segundo al utilizar el códec G.711.

La figura 5.54 nos muestra la captura del tráfico de VoIP, así como el tipo de códec utilizado, el tamaño del paquete, el protocolo utilizado, etc.

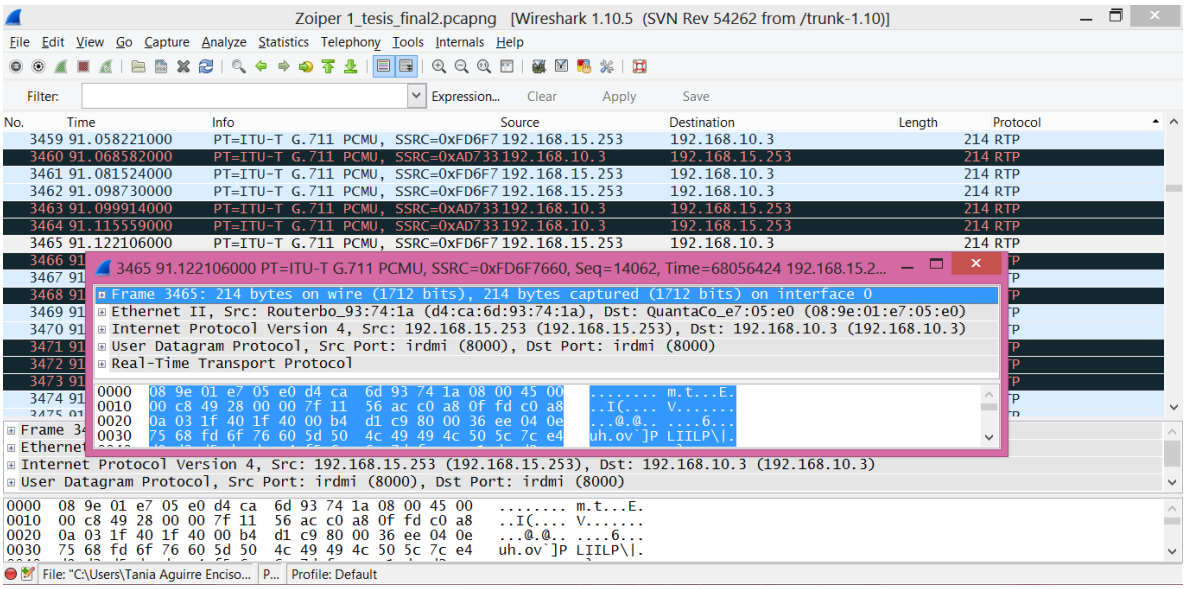


Figura 5.54. Análisis de *frame* y captura de tráfico de VoIP en *Wireshark*.

CONCLUSIONES

Conclusiones generales

Es importante mencionar que al aislar en las redes WDS las redes inalámbricas tipo ***mesh***, éstas no permiten tener múltiples portales que dirigen a las redes Ethernet. Sin embargo, al implementar redes ***mesh*** en conjunto con WDS podemos tener una convergencia con otras redes, en las cuales son necesarios el uso de portales para tener una interacción con Internet, tecnología o simplemente el servicio de VoIP sea completamente funcional.

Sin duda alguna el utilizar redes inalámbricas ***mesh*** ayuda en diferentes aspectos como: conectividad en zonas de difícil acceso, bajo costo, facilidad de incorporarse en redes convergentes, etc.

Las redes ***mesh*** parciales son una excelente opción para acercar a los usuarios a las capas más altas, además brindar un buen servicio debido a que utilizan el protocolo RSTP para prevención de ciclos.

Algunos de los parámetros que nos permitieron evaluar el desempeño de la aplicación de VoIP en la red mesh parcial fueron: pérdida de paquetes totales, paquetes tirados por *buffer jitter, delta* o *latencia*, *jitter*, errores de secuencia de número, paquetes perdidos por errores de secuencia de número, tiempo de restablecimiento de enlaces, etc.

Conclusiones de tesis

Se pudo comprobar en la red inalámbrica ***mesh*** parcial, que al utilizar VLAN's se implementó una clasificación del tráfico correspondiente de voz, video y datos, el cual beneficia notablemente el comportamiento dinámico de la red. Al no utilizar VLAN's, la calidad del tráfico de voz disminuye de forma muy notable, convirtiendo completamente a la aplicación de VoIP en no funcional. Ésto es debido al aumento del valor de *delta* o *latencia,* mayor porcentaje en pérdida total de paquetes e intolerancia a fallos en enlaces WDS, al grado de provocar la caída de la llamada de VoIP establecida.

A pesar de que se provocaron fallas en los enlaces, las llamadas de VoIP no perdieron la comunicación al utilizar VLAN's, tan solo se observaron errores en la asignación de números de secuencia dentro de los paquetes RTP, lo cual es considerado como un comportamiento normal en dichas condiciones.

Contribución en un futuro

La mejoría que puede realizarse en este tema de investigación es la implementación de QoS, ya que podemos ver que el comportamiento dinámico de la red con los escenarios propuestos con VLAN's es bueno, pero al tener QoS puede verse mejorada de forma muy notable el rendimiento de este tipo de redes. En cuanto a su desempeño, la marcación de paquetes hoy en día es muy necesaria para manejar tasas de transmisión altas y ofrecer servicios para evitar cuellos de botella, pérdidas de paquetes, disminución en la velocidad de transmisión, etc.

Es necesario hacer notar que la falta de un mayor número de usuarios o llamadas, se vio limitada por la cantidad de equipos con los que se contaban en la facultad, es por ésto que intervinieron en pruebas de tesis tres usuarios únicamente. Siendo utilizadas laptops para poder realizar las capturas del tráfico, a través de *Wireshark*.

Referencias

[1] Jean Marie Vella & Saviour Zammit, “Infrastructure Dependent Wireless Multicast over 802.11n WLAN”. Dept. of Computer and Communications Engineering University of Malta.

[2] Tech. Rep. IEEE 802.11-09/0247r0, “Quasi-reliable Multicast”, Mar. 2009.

[3] Malte Cornils, Institute of Medical Informatics Charite Universitatsmedizin Berlin. Michael Bahr, Corporate Technology, Siemens AG. Thomas Gamer, Institute of Telematics, Karlsruhe Institute of Technology Artículo IEEE, “Simulative Analysis of the Hybrid Wireless Mesh Protocol (HWMP)”. 2010 European Wireless Conference.

[4] Pejman Roshan, Jonathan Leary, “Wireless LAN Fundamentals”, Cisco Press, December 23, 2003.

[5] Trainning Class, Certification MTCNA for Mikrotik equipment. “Mikrotik RouterOS”.

[6] IEEE Std 802.11™, “IEEE Standard for Information technology Telecommunications and information exchange between systems Local and metropolitan area networks, Specific requirements. IEEE Standard for Information technology, Telecommunications and information exchange between systems Local and metropolitan area networks, Specific requirements”. 29 March 2012.

[7] Guido R. Hiertz, Rwth Aachen University. Dee Denteneer, Philips Research. Sebastian Max, Rwth Aachen University. Rakesh Taori, Samsung Electronics Co. Ltd. Javier Cardona, Cozybit Inc. Lars Berlemann, T-Mobile International. Bernhard Walke, Rwth Aachen University. “IEEE 802.11S: THE WLAN MESH STANDARD”. IEEE Wireless Communications, February 2010.

[8] Recomendación ITU-T G.711: Pulse code modulation (PCM) of voice frequencies.

[9] Recomendación ITU-T G.723.1 : Códec de voz de doble velocidad para la transmisión en comunicaciones multimedia a 5,3 y 6,3 kbit/s.

[10] Recomendación G.726 : 40, 32, 24, 16 kbit/s Adaptive Differential Pulse Code Modulation (ADPCM).

[11] Recommendation ITU-T G.729: Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP).

[12] Cisco Systems, “Voice Over IP Fundamentals”, A Systematic Approach to Understanding the Basics of Voice over IP, Copyright 2000 Cisco Press. Indianapolis, USA.

[13] H. Schulzrinne et al , Request for Comments 3550: “RTP: A Transport Protocol for Real – Time Applications”, July 2003.

[14] Recomendación ITU-T, www.itu.int/rec/T-REC-G.114-200305-I/es.

[15] Jose Joskowicz IIE/FING/UDELAR, Rafael Sotelo IIE/FING/UDELAR – FI/UM.Articulo IEEE, “Medida de calidad de Voz en redes IP”, Montevideo, Uruguay.

[16] Tauseef Gulrez, Rajib Chakraborty, Rami Al-Hmouz, Zenon Chaczko, [1] & Md. Russell Iqbal[2], Artículo IEEE, “CONGESTION DETE CTION AND CONTROL IN PARTIAL MESH USING BAYESIAN APPROACH”, 1. Information & Communications Technology Group Faculty of Engineering, University of Technology Sydney, Australia. 2. Social Science & Professional Ethics Group Faculty of Social Sciences, University of NewSouthWales, Sydney, Australia.

[17] http://wiki.mikrotik.com/wiki/Wireless_WDS_Mesh

[18] http://download.Mikrotik.com/what_is_RouterOS.pdf

Glosario

ACELP Algebraic Code Excited Linear Prediction. Es un algoritmo de códec de voz utilizado para la codificación con una tasa de bits entre 2,4 y 8 kbit / s. ACELP es una técnica mejorada utilizado para codificadores de voz CELP

AP Punto de Acceso, es un dispositivo cuyo papel es crear una red inalámbrica y permitirles a las terminales que se encuentran dentro de su área de cobertura el acceso a la red.

Backbone Núcleo estructural de la red, que conecta todos los componentes de la red de manera que se pueda producir la comunicación.

BPDU Bridge Protocol Data Unit. Son tramas que contienen información del protocolo Spanning Tree (STP).

BSS Conjunto de Servicios Básicos es el bloque constructor básico de una LAN IEEE 802.11.

Buffer Memoria intermedia que se utiliza como memoria de datos temporal durante una sesión de trabajo.

CDMA Acceso al Medio por División de Código

Conmutación Proceso de tomar una trama entrante de una interfaz y enviarla a través de otra interfaz.

CS-ACELP Conjugate Structure Algebraic Code Excited Linear Prediction. Algoritmo de compresión de voz se define en UIT-T G.729, el cual es orientado al modo multicanal.

CSMA/CA Acceso Múltiple de Detección de Portadora con Evitación de Colisiones. Algoritmo que define el estándar IEEE 802.11 cuando se usa DCF.

DHCP Acrónimo de Protocolo de Configuración Dinámica de Host. Mediante este protocolo se puede realizar la asignación automática de direcciones IP, máscaras de subred y default Gateway a cada uno de los elementos

	que forman parte de una red.
Dirección MAC	Dirección de Control de Acceso al Medio, identificador de la tarjeta de red que consiste en un conjunto de 48 bits agrupados en grupos de cuatro y representados en forma hexadecimal. Los primeros 6 dígitos identifican al fabricante y los últimos 6 identifican a la tarjeta en particular.
DS	Sistema de Distribución. Es el medio por el cual un AP se comunica con otro AP para intercambiar *frames*.
EDCA	Acceso al Canal Distribuido Mejorado. Mecanismo que tiene como objetivo controlar el acceso al canal inalámbrico.
Enrutamiento estático	Ruta que se ha configurado e introducido explícitamente en la tabla de enrutamiento. Las rutas estáticas tienen prioridad sobre las rutas elegidas por los protocolos de enrutamiento dinámico.
ESS	Conjunto de Servicios Extendido. Definido como dos o más BSSs conectados por medio de un DS común.
Gateway	En la comunidad IP, termino antiguo que se refiere a un dispositivo de enrutamiento. Actualmente, el termino router se utiliza para describir nodos que desempeñan esta función, y Gateway se refiere a un dispositivo especial que realiza conversión de la capa de aplicación de la información de una pila de protocolos a otro.
HWMP	Hybrid Wireless ***Mesh*** Protocol. Protocolo de enrutamiento básico para redes inalámbricas *mesh.*
IEEE	Son las siglas del Instituto de Ingenieros Eléctricos y Electrónicos, es una asociación sin fines de lucro que se encarga de aplicar los avances en las tecnologías de la información.
IEEE 802.11 g	Estándar de comunicaciones inalámbricas que desarrolla las especificaciones técnicas para una WLAN, usa la frecuencia de 2.4 GHz y alcanza hasta 54 Mbps.
	Protocolo de Internet. Protocolo de capa de red de la pila TCP / IP que ofrece un servicio de internetwork de

IP	redes no orientadas a conexión. El IP brinda funciones de direccionamiento, especificaciones del tipo de servicio, fragmentación y re ensamblaje, y seguridad. Se define en RFC 791.
IPv4	Protocolo Internet versión 4 es un protocolo de conmutación no orientado a conexión de máximo esfuerzo.
ISM	Instrumental Científico y Médico. Son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica.
MAC	Control de Acceso al Medio. Parte de la capa de enlace de datos que incluye la dirección de 6 bytes (48 bits) del origen y del destino, y el método para obtener permiso para transmitir.
MCS	Esquema de Modulación y Codificación. Es un esquema utilizado para la calidad del canal de radio.
Mesh	Topología de red en la cual los dispositivos se organizan de manera administrable, segmentada, con varias interconexiones a menudo redundantes, colocadas de forma estratégica entre los nodos de red.
OFDM	Multiplexaje por División de Frecuencias Ortogonales. Es una técnica de comunicación que divide un canal, de frecuencia, en un número determinado de bandas de frecuencias
PCM	Modulación por Codificación de Pulsos, Método utilizado para digitalizar las señales analógicas.
PHY	Capa Física, es la interfaz entre el MAC y el medio inalámbrico.
PREP	Path Response. Cuando el destino crea un mensaje PREP, el cual es unicast hacia la fuente.
PREQ	Petición de ruta, mensaje transmitido en broadcast por una fuente STA mesh.
PSTN	Red Telefónica Pública Conmutada. Es una red con conmutación de circuitos tradicional, optimizada para comunicaciones de voz en tiempo real.

Redundancia	Duplicación de dispositivos, servicios o conexiones, de modo que, en caso de que se produzca una falla, los dispositivos, servicios o conexiones redundantes puedan realizar el trabajo de aquellos en los que se produce la falla.
Router	Dispositivo de capa de red que usa una o más métricas para determinar cuál es la ruta optima a través de la cual se debe enviar el tráfico de red.
RSTP	Protocolo de Árbol de Expansión Rápido. Es una evolución STP y reduce significativamente el tiempo de convergencia de la topología de la red.
RTP	Protocolo de Tiempo Real. Es un protocolo de nivel de sesión utilizado para la transmisión de información en tiempo real.
SIP	Protocolo de Iniciación de Sesión. Estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia.
SRTP	Protocolo de Trasporte de Tiempo Real. Proporciona cifrado, autenticación del mensaje e integridad, y protección contra reenvíos a los datos RTP en aplicaciones unicast y multicast
SS	Espectro Disperso (Spread-Spectrum). Técnica de modulación empleada en telecomunicaciones, para la transmisión de datos digitales y por radiofrecuencia.
STP	Protocolo de Árbol de Extensión. Protocolo de capa 2, que gestiona la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes.
TTL	Tiempo de Existencia. Campo en un encabezado IP que indica el tiempo durante el cual se considera válido un paquete.
UDP	Protocolo de Datagrama de Usuario. Protocolo no orientado a conexión de la capa de trasporte de la pila de protocolo TCP / IP. UDP es un protocolo simple que intercambia datagramas sin confirmación o garantía de entrega y que requiere que el procesamiento de errores y las retransmisiones sean manejados por otros protocolos. UDP se define en la RFC 768.

VLAN	LAN Virtual. Grupo de dispositivos de una LAN que están configurados (usando el software de administración) de tal modo que se pueden comunicar como si estuvieran conectados al mismo cable, cuando, en realidad, están ubicados en una serie de segmentos de LAN distintos. Debido a que las LAN virtuales están basadas en conexiones lógicas en lugar de físicas, son extremadamente flexibles.
VoIP	Tecnología que transmite paquetes de voz a través de una red de conmutación de paquetes usando el protocolo IP.
WDS	Sistema de Distribución Inalámbrico. Sistema que permite la interconexión inalámbrica de puntos de acceso en una red IEEE 802.11.
WLAN	Red de Área Local Inalámbrica, transmite y recibe datos entre sus elementos utilizando ondas electromagnéticas que utilizan el aire como medio de transmisión. Su radio de cobertura es de unas decenas de metros.
802.11	Familia de estándares que especifica una interfaz aérea entre dos clientes inalámbricos o entre un cliente inalámbrico y un Punto de Acceso, es para tecnologías de redes WLAN y fue desarrollada por la IEEE.

APÉNDICE A

A.1. Programación de AP1 en RouterBoard

```
#
/interface bridge
add name=Bridge-interface
/interface bridge
add l2mtu=1514 name=VLAN_3_Service protocol-mode=rstp
add name=VLAN_15_Users protocol-mode=rstp
/interface ethernet
set 0 comment="Trunk to Test_Switch"
/interface wireless
set 0 band=2ghz-onlyg disabled=no frequency=2412 hw-retries=15 l2mtu=2290 \
    mode=ap-bridge radio-name=AP1 ssid=MikroTik tx-power=5 tx-power-mode=\
    card-rates wds-default-bridge=Bridge-interface wds-mode=dynamic-mesh
add disabled=no l2mtu=2290 mac-address=02:0C:42:26:93:8E master-interface=\
    wlan1 name=wlan2 ssid=USUARIOS wds-cost-range=0 wds-default-cost=0
add hide-ssid=yes mac-address=02:0C:42:26:93:8F master-interface=wlan1
name=\
    wlan3 ssid=WLAN15_Users wds-cost-range=0 wds-default-
bridge=VLAN_15_Users \
    wds-default-cost=0 wds-mode=dynamic-mesh
add hide-ssid=yes mac-address=02:0C:42:26:93:90 master-interface=wlan1
name=\
    wlan4 ssid=WLAN3_Service wds-cost-range=0 wds-default-bridge=\
    VLAN_3_Service wds-default-cost=0 wds-mode=dynamic-mesh
```

```
/interface wireless manual-tx-power-table

set wlan1 manual-tx-
powers="1Mbps:17,2Mbps:17,5.5Mbps:17,11Mbps:17,6Mbps:17,9M\


bps:17,12Mbps:17,18Mbps:17,24Mbps:17,36Mbps:17,48Mbps:17,54Mbps:17,HT2
0-0:\

    0,HT20-1:0,HT20-2:0,HT20-3:0,HT20-4:0,HT20-5:0,HT20-6:0,HT20-7:0,HT40-
0:0,\

    HT40-1:0,HT40-2:0,HT40-3:0,HT40-4:0,HT40-5:0,HT40-6:0,HT40-7:0"

/ip neighbor discovery

set ether1 comment="Trunk to Test_Switch"

/interface vlan

add interface=Bridge-interface name=vlan3_MESH vlan-id=3

add interface=ether1 l2mtu=1514 name=vlan3_switch vlan-id=3

add interface=ether1 l2mtu=1514 name=vlan5_switch vlan-id=5

add interface=ether1 l2mtu=1514 name=vlan10_switch vlan-id=10

add interface=Bridge-interface name=vlan15_MESH vlan-id=15

/interface wireless security-profiles

set [ find default=yes ] group-ciphers="" unicast-ciphers=""

/ip hotspot user profile

set [ find default=yes ] idle-timeout=none keepalive-timeout=2m \

    mac-cookie-timeout=3d transparent-proxy=yes

/ip pool

add name=dhcp_pool1 ranges=192.168.15.2-192.168.15.254

/ip dhcp-server

add address-pool=dhcp_pool1 disabled=no interface=VLAN_15_Users
name=dhcp1
```

```
/port
set 0 baud-rate=115200 name=serial0
/system logging action
set 3 remote=0.0.0.0
/interface bridge port
add bridge=VLAN_3_Service interface=vlan3_switch
add bridge=VLAN_3_Service interface=ether2
add bridge=VLAN_15_Users interface=wlan2
add bridge=VLAN_3_Service interface=vlan3_MESH
add bridge=VLAN_15_Users interface=vlan15_MESH
add bridge=VLAN_3_Service interface=ether3
/ip address
add address=10.0.0.1/24 interface=Bridge-interface network=10.0.0.0
add address=192.168.3.1/24 interface=VLAN_3_Service network=192.168.3.0
add address=192.168.15.1/24 interface=VLAN_15_Users network=192.168.15.0
add address=192.168.5.1/24 interface=vlan5_switch network=192.168.5.0
add address=192.168.10.1/24 interface=vlan10_switch network=192.168.10.0
add address=192.168.100.1/24 interface=Bridge-interface network=192.168.100.0
/ip dhcp-client
add dhcp-options=hostname,clientid disabled=no interface=ether3
/ip dhcp-server network
add address=192.168.3.0/24 gateway=192.168.3.1
add address=192.168.15.0/24 dns-server=192.168.15.1 gateway=192.168.15.1
/ip dns
set max-udp-packet-size=512 servers=192.168.10.1,192.168.10.254
```

```
/routing rip
set redistribute-connected=yes
/system identity
set name=MikroTik-RB133_AP1
/tool bandwidth-server
set max-sessions=10
```

A.2. Programación en AP2 y AP3 en RouterBoard

```
/interface bridge
add name=Bridge-Interface
/interface bridge
add l2mtu=1526 name=VLAN_3_Service protocol-mode=rstp
add name=VLAN_15_Users protocol-mode=rstp
/interface wireless
set 0 band=2ghz-onlyg disabled=no frequency=2412 l2mtu=2290 mode=ap-bridge
\
    radio-name=AP2 ssid=MikroTik tx-power=10 tx-power-mode=card-rates \
    wds-default-bridge=Bridge-Interface wds-mode=dynamic-mesh
add disabled=no l2mtu=2290 mac-address=02:0C:42:26:9D:89 master-interface=\
    wlan1 name=wlan2 ssid=USUARIOS_AP2 wds-cost-range=0 wds-default-
cost=0
add hide-ssid=yes mac-address=02:0C:42:26:9D:8A master-interface=wlan1
name=\
    wlan3 ssid=WLAN3_Service wds-cost-range=0 wds-default-bridge=\
    VLAN_3_Service wds-default-cost=0 wds-mode=dynamic-mesh
```

```
add hide-ssid=yes mac-address=02:0C:42:26:9D:8B master-interface=wlan1
name=\
    wlan4 ssid=WLAN15_Users wds-cost-range=0 wds-default-
bridge=VLAN_15_Users \
    wds-default-cost=0 wds-mode=dynamic-mesh
/interface ethernet
set 8 comment="Salida WAN" disabled=yes
/ip neighbor discovery
set ether9 comment="Salida WAN"
/interface vlan
add interface=Bridge-Interface name=vlan3_MESH vlan-id=3
add interface=Bridge-Interface name=vlan15_MESH vlan-id=15
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip hotspot user profile
set [ find default=yes ] idle-timeout=none keepalive-timeout=2m \
    mac-cookie-timeout=3d
/ip pool

add name=dhcp_pool1 ranges=192.168.15.1,192.168.15.3-192.168.15.254
/ip dhcp-server
add address-pool=dhcp_pool1 name=dhcp1 relay=192.168.15.2
/port
set 0 name=serial0
/interface bridge port
add bridge=VLAN_3_Service interface=ether1
```

```
add bridge=VLAN_15_Users interface=wlan2
add bridge=VLAN_3_Service interface=vlan3_MESH
add bridge=VLAN_3_Service interface=vlan15_MESH
/ip address
add address=10.0.0.2/24 interface=Bridge-Interface network=10.0.0.0
add address=192.168.3.2/24 interface=VLAN_3_Service network=192.168.3.0
add address=192.168.100.2/24 disabled=yes interface=Bridge-Interface network=\
    192.168.100.0
add address=192.168.15.2/24 interface=VLAN_15_Users network=192.168.15.0
/ip dhcp-client
add dhcp-options=hostname,clientid disabled=no interface=ether7
/ip dhcp-server network
add address=192.168.15.0/24 dns-server=8.8.8.8 gateway=192.168.15.2
/ip firewall mangle
add action=mark-packet chain=forward disabled=yes new-packet-mark=VoIP \
    passthrough=no src-address=192.168.10.0/24
add action=mark-packet chain=forward disabled=yes dst-address=192.168.10.0/24
\
    new-packet-mark=VoIP passthrough=no
add action=mark-packet chain=forward disabled=yes dscp=46 new-packet-mark=\
    "VoIP TOS 46" passthrough=no
/ip firewall nat
add action=masquerade chain=srcnat disabled=yes out-interface=ether9
add action=masquerade chain=srcnat disabled=yes src-address=192.168.15.0/24
/ip route
```

```
add distance=1 gateway=192.168.3.1
/routing rip
set redistribute-connected=yes
/system identity
set name=MikroTik-RB493-AP2
```