UNIVERSIDAD NACIONAL DEL ALTIPLANO - PUNO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

"ANÁLISIS DEL TIEMPO DE RECUPERACIÓN EN UN ENLACE REDUNDANTE EN UNA RED CON ENRUTAMIENTO EIGRP Y SERVICIO DE TELEFONÍA IP"

T E S I S

PRESENTADO POR:

JOSE VIZCARDO HUALLPA VARGAS

ABEL APAZA QUISPE

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PUNO - PERÚ

2017

UNIVERSIDAD NACIONAL DEL ALTIPLANO – PUNO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

"ANÁLISIS DEL TIEMPO DE RECUPERACIÓN EN UN ENLACE REDUNDANTE EN UNA RED CON ENRUTAMIENTO EIGRP Y SERVICIO DE TELEFONÍA IP"

TESIS PRESENTADA POR:

JOSE VIZCARDO HUALLPA VARGAS

ABEL APAZA QUISPE

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

APROBADA POR EL JURADO REVISOR CONFORMADO POR:

PRESIDENTE: DR. JOSÉ EMMANUEL CRUZ DE LA CRUZ

PRIMER MIEMBRO: M.Sc. EDDY TORRES MAMANI

SEGUNDO MIEMBRO: Ing. CHRISTIAN AUGUSTO ROMERO GOYZUETA

DIRECTOR/ASESOR: Mg. LUIS ENRIQUE BACA WIESSE

PUNO – PERÚ

2017

Área : Telecomunicaciones

Tema : Enrutamiento EIGRP y telefonía IP con códecs

DEDICATORIA

Esta tesis va dedicada para los docentes y compañeros de la Escuela Profesional de Ingeniería Electrónica, por el apoyo y motivación para mi formación profesional. Así mismo, a los estudiantes que usen como referencia esta tesis.

José Vizcardo Huallpa Vargas

A dios, a mi abuela, a mis padres, a mis hermanos y a todas las personas que más aprecio.

Abel Apaza Quispe

setiembre 2017

AGRADECIMIENTO

Doy gracias a mis queridos padres, mis hermanas y a mis amigos por todo el apoyo brindado económico y moral. Agradezco a los docentes de la Escuela Profesional de Ingeniería Electrónica que me apoyaron para realizar esta tesis.

José Vizcardo Huallpa Vargas

Agradezco con todo cariño a mis padres y mi abuela por permitirme el acceso a una buena educación. A mi universidad que me permitió pertenecer a ella. A mis docentes de Ingeniería Electrónica y a todas las personas que fueron participes, sin ellos no hubiera podido cumplir este objetivo.

Abel Apaza Quispe

Setiembre 2017

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

ÍNDICE DE ACRÓNIMOS

A

ABS
Analysis by synthesis, 54

ACELP
Algebraic code excited linear prediction, 57

ACK
acknowledgement, 45

AD
Distancia publicada, 50

ADPCM
Adaptive differential pulse code modulation, 58

C

CNAME
Canonical Name, 31

CNG
Comfort noise generation, 57

CSRC
Contributing Source, 31

D

DHCP
Protocolo de Configuración Dinámica de Host, 20

DMVPN
Dynamic Multipoint VPN, 43

DTX
Discontinuous transmission, 57

DUAL
Actualización por Difusión, 49

E

EIGRP
Enhanced Interior Gateway Routing Protocol, 42

ETSI
European Telecommunications Standardization Institute, 57

F

FC
Condición de factibilidad, 50

FD
Distancia Factible, 50

FS
Sucesor factible, 50

FTP
File Transfer Protocol, 39

G

GSM
Global System for Mobile communications, 54

H

HTTP
Protocolo de Transferencia de Hipertexto, 18

I

ICANN
Corporación de Internet para la Asignación de Nombres y Números, 13

IETF
Internet Engineering Task Force, 18

IGRP
Interior Gateway Routing Protocol, 43

IP
Protocolo de Internet, 13

IPv4
El Protocolo de Internet versión 4, 13

UAS

Servidor de Agente de Usuario, 20

UDP

User Datagram Protocol, 27

UIT

Unión Internacional de Telecomunicaciones, 51

V

VAD

Voice activity detector, 57

VoIP

Voz sobre IP, 14

RESUMEN

Esta investigación consiste en el análisis del tiempo de recuperación en un enlace redundante en una red con enrutamiento EIGRP y con el servicio de telefonía IP que permitió conocer el códec adecuado entre PCMA, GSM y G722, esto ayudará en la comunicación de telefonía IP en empresas y/o entidades públicas. El problema al implementar una red de telefonía IP es la recuperación del tráfico ante el cambio o ruptura de un enlace principal hasta la adecuación al enlace de respaldo; debido a que los codecs de audio encargados de convertir la voz humana en señales digitales (utilizando diferentes métodos y algoritmos) no son iguales en todos los casos. Por lo tanto, fue oportuno analizar las reacciones de la comunicación ante cada codecs para observar la flexibilidad en el proceso de recuperación. Para realizar esta investigación se implementó la red configurando con el protocolo EIGRP en cada router de la marca Cisco, dos softphone cada uno con su respectivo servidor Elastix y también se usó el capturador de paquetes, para la elección entre los códec fue el softphone Ekiga, la ruta principal fue con un cable UTP y la conexión redundante fue por cables seriales. Se realizaron diez pruebas, las cuales fueron llamadas realizadas para cada códec. Las llamadas duraron una cantidad de 40 segundos en cada prueba se realizó la desconexión del enlace principal a los 20 segundos de iniciado la llamada y fue manual. La investigación concluye que con el códec G722 la recuperación de la comunicación es más rápida con un tiempo promedio de 3.6 segundos con una pérdida de paquetes de 20%.

Palabras Clave: Telefonía IP, EIGRP, PCMA, GSM, G.722.

ABSTRACT

This investigation consists of the analysis of the recovery time in a redundant link in a network with EIGRP routing and with the IP telephony service that allowed to know the proper codec between PCMA, GSM and G722, this will help in the communication of IP telephony in companies And / or public entities. The problem when implementing an IP telephony network is the recovery of traffic to the change or rupture of a main link to the adequacy to the backup link; Because the audio codecs responsible for converting the human voice into digital signals (using different methods and algorithms) are not the same in all cases. Therefore, it was opportune to analyze the reactions of the communication before each codecs to observe the flexibility in the recovery process. In order to carry out this research, the network was implemented by configuring the EIGRP protocol on each router of the Cisco brand, two softphones each with its respective Elastix server, and also the packet grabber was used for the choice between the codecs Ekiga softphone, The main route was with a UTP cable and the redundant connection was by serial cables. Ten tests were performed, which were called for each codec. The calls lasted an amount of 40 seconds in each test the disconnection of the main link was made to the 20 seconds of initiated the call and it was manual. The research concludes that with the G722 codec the retrieval of communication is faster with an average time of 3.6 seconds with a packet loss of 20%.

KeyWords: IP Telephony, EIGRP, PCMA, GSM, G.722.

CAPITULO I

INTRODUCCIÓN

La telefonía IP ofrece una solución de ahorro de costes para la integración de redes de datos con voz, esto es una alternativa viable a los sistemas tradicionales de voz y redes telefónicas públicas conmutadas (PSTN). Esta es flexible en la conducción de nuevos servicios mediante el suministro de interoperabilidad de dispositivos a través de protocolos estandarizados, esta tecnología como una aplicación en tiempo real trae nuevos desafíos para los proveedores de servicios y las empresas debido a que las redes necesitan ser más flexibles, convergentes, seguras y tener un mayor nivel de rendimiento. Al diseñar una red para soportar telefonía IP deben tenerse en cuenta algunas consideraciones como: presupuesto disponible, la calidad de servicio en la red, softwares y un análisis de diferentes códecs para determinar la reacción ante fallas en los enlaces. EIGRP es un protocolo de enrutador dinámico que ofrece tiempos de convergencia extremadamente rápidos con un mínimo tráfico de red, donde el enrutamiento es una función esencial de red de datos que proporciona una entrega de datos en tiempo real eficaz lo que requiere telefonía IP.

El problema al implementar una red de telefonía IP es la recuperación del tráfico ante el cambio o ruptura de un enlace principal hasta la adecuación al enlace de respaldo debido a que los códecs de audio encargados de convertir la voz humana en señales digitales (utilizando diferentes métodos y algoritmos) no son iguales en todos los casos. Por lo tanto, es oportuno analizar las reacciones de la comunicación ante cada códec para observar la flexibilidad en el proceso de recuperación.

El objetivo principal de este proyecto es analizar el tiempo de recuperación hacia un enlace redundante o secundario en una red con enrutamiento EIGRP y transportando el servicio de telefonía IP, analizando el comportamiento de la red con los códec PCMA, GSM y G722. Las conclusiones se determinarán los códecs necesarios para una recuperación más rápida de la comunicación ante estas rupturas de enlaces principales.

En la revisión literaria incluirá toda la fundamentación teórica necesaria sobre telefonía IP, codec PCMA, GSM Y G722, protocolos de transporte SIP, RTP, RTCP y UDP, protocolo de enrutamiento EIGRP, al igual que los antecedentes a esta investigación, los objetivos, e hipótesis planteadas en la investigación.

En métodos y materiales se realizará la instalación de servidores y configuraciones para la investigación de la red que transporta telefonía IP ante un corte en el enlace principal y su

posterior recuperación hacia un secundario. Aquí se incluirá la investigación para poder tener la información necesaria y concluir con la investigación realizada sobre análisis del tiempo de recuperación en un enlace redundante en una red con enrutamiento EIGRP y servicio de telefonía IP.

Los resultados serán analizando todos los protocolos que se usan para telefonía IP, tales como SIP, RTP y RTCP, y el protocolo de enrutamiento EIGRP, de los cuales se tomara más en cuenta los protocolos RTP y RTCP, ya que son los involucrados en transportar los paquetes de voz y reportar su calidad para la posterior mejora, además, cuando se realiza la desconexión solo se envían estos paquetes.

CAPITULO II

REVISIÓN DE LITERATURA

2.1. PROTOCOLO DE INTERNET (IP)

Una IP es un número que identifica de manera lógica, denominada como una dirección IP. Cada host y enrutador que utilice el protocolo IP tiene una dirección IP, que codifica su número de red y su número de host. La combinación es única: no hay dos máquinas que tengan la misma dirección IP. Todas las direcciones IP son de 32 bits de longitud y se usan en los campos de Dirección de origen y de Dirección de destino de los paquetes IP. En importante mencionar que una dirección IP realmente no se refiere a un host. En realidad, se refiere a una interfaz de red, por lo que, si un host está en dos redes, debe tener dos direcciones IP. Sin embargo, en la práctica, la mayoría de los hosts se encuentran en una red y, por lo tanto, tienen una dirección IP. Hay cerca de 500,000 redes conectadas a Internet, y la cifra se duplica cada año. Los números de redes son manejados por una corporación no lucrativa llamada ICANN (Corporación de Internet para la Asignación de Nombres y Números) para evitar conflictos. A su vez, ICANN ha delegado partes del espacio de direcciones a varias autoridades regionales, las cuales han repartido direcciones IP a los ISPs y a otras compañías.

El protocolo IP es el servicio de capa de red implementado por la suite de protocolos TCP/IP. IP se diseñó como protocolo con baja sobrecarga. Provee sólo las funciones necesarias para enviar un paquete desde un origen a un destino a través de un sistema interconectado de redes. El protocolo no fue diseñado para rastrear ni administrar el flujo de paquetes. De ser necesarias, otros protocolos en otras capas llevan a cabo estas funciones. Las características básicas del protocolo IP son las siguientes:

- Sin conexión: no se establece ninguna conexión con el destino antes de enviar los paquetes de datos.
- Máximo esfuerzo (no confiable): la entrega de paquetes no está garantizada.
- Independiente de los medios: la operación es independiente del medio que transporta los datos.

Existen varios protocolos de capa de red; sin embargo, solo dos que se incluyen a continuación se implementan con frecuencia:

- Protocolo de Internet versión 4 (IPv4
- Protocolo de Internet versión 6 (IPv6) (**C**isco Networking Academy. 2014.p.204)

2.2. TELEFONÍA IP

Las redes de telefonía traducen la señal analógica de las ondas sonoras de la voz en señales eléctricas analógicas que son transmitidas tal cual, hasta el otro extremo de la comunicación, donde son de nuevo convertidas en ondas sonoras.

Por otro lado, se llama señal digital a aquella que varía de forma discreta. Quiere esto decir que las señales digitales disponen de un número reducido de estados posibles y van cambiando de uno a otro dependiendo de la información que transmiten. Una señal o van cambiando de uno otro dependiendo de la información que transmiten. Una señal o información es digital binaria cuando el número de estados posibles es dos, representados como 0 y 1 y conocidos como bits. La red internet maneja señales digitales binarias.

Telefonía IP, telefonía sobre internet, voz sobre banda ancha (VoBB, voice over Broad Band), voz sobre IP o VoIP (voice over IP) vienen a significar una misma cosa: un servicio que permite la transmisión de la voz utilizando la red Internet.

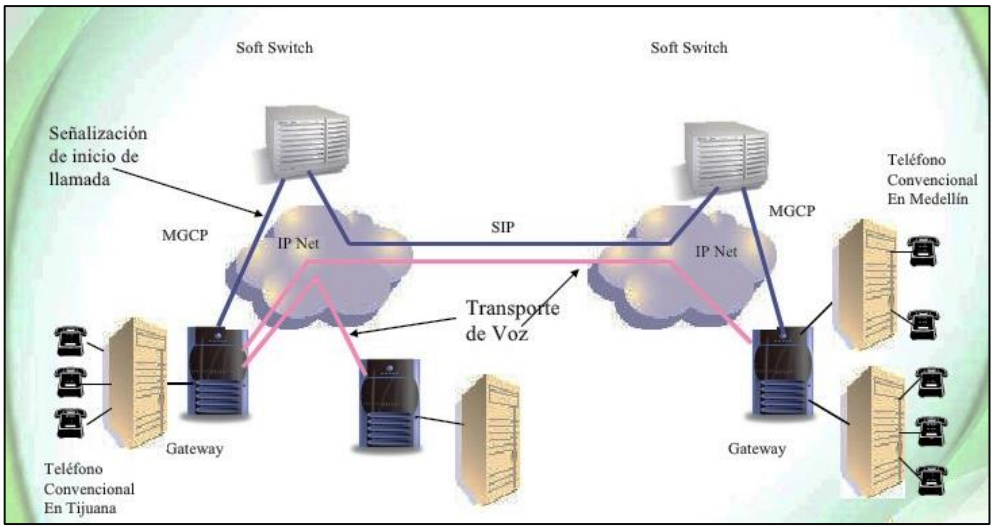


Figura 1: Red de telefonía IP

Fuente: Carballar J. (2008). VoIP. La Telefonia de Internet.

Para enviar la voz utiliza el protocolo de Internet (de ahí las siglas IP). Los operadores de telefonía IP están interconectados a la red telefónica pública, que es el lugar dónde están en contacto todos los operadores y que hace posible que puedas llamar con tu teléfono a un usuario de otra compañía marcando su número de teléfono.

Esta interconexión a la red de telefonía pública permite a los usuarios de telefonía IP realizar llamadas a numeración telefónica convencional, como pueden ser los números de teléfono geográficos, números móviles, números nómadas y/o números de tarificación especial (902,

900, 800…); y disponer de un número geográfico al que cualquier usuario de telefonía le puede llamar.

La telefonía IP está basada en la tecnología VoIP (Voice over Internet Protocol), también llamada voz sobre IP que es la encargada de transformar la voz en paquetes de datos para que se puedan enviar a través de Internet. (Carballar J. 2008. p.50-51).

2.3.1. VOICE OVER INTERNET PROTOCOL (VoIP)

VoIP es exactamente lo que el nombre indica: el envío de voz (y vídeo) IP-Based Network. Esto es completamente diferente al de la telefonía pública con conmutación de circuitos Red. La conmutación de circuitos asigna recursos a cada individuo llamada. Los servicios de telefonía tradicional suelen describirse mediante términos tales como. El sistema de señalización, los portadores T, el servicio telefónico antiguo (POTS), la red telefónica pública conmutada (PSTN), las conexiones de puntas y anillos, los circuitos locales, los circuitos locales y todo lo que provenga de la Unión Internacional de Telecomunicaciones. Todos estos se refieren a un sistema que se ha utilizado durante décadas para ofrecer fiables, de bajo ancho de banda llamadas telefónicas con un alto nivel de calidad. Una topología tradicional simple podría ser similar a la que se muestra en la Figura 2.

Las redes IP son conmutadas por paquetes, y cada paquete enviado es semi-autónomo, tiene su propio encabezado IP y es reenviado por routers por separado.

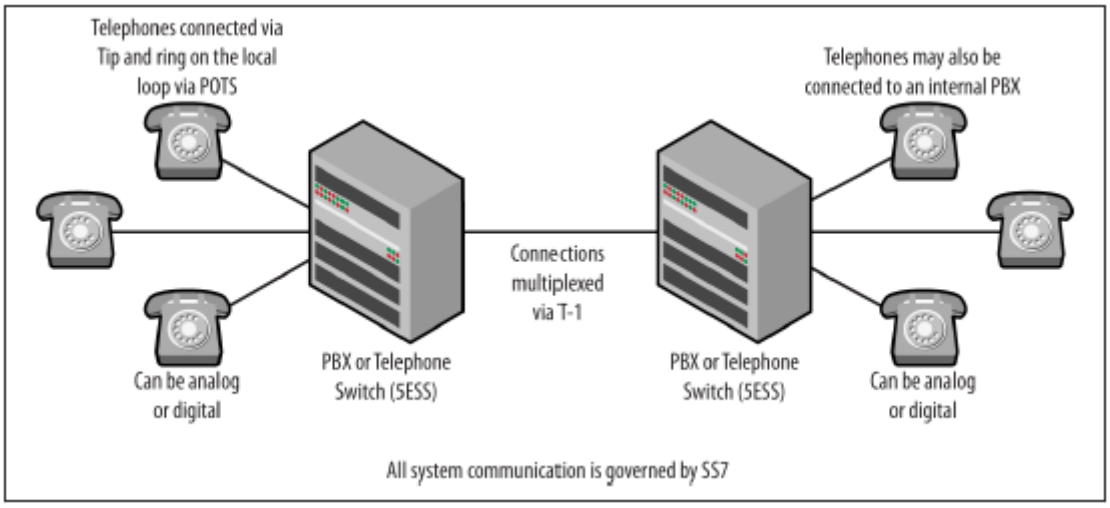


Figura 2: Topología simple de telefonía tradicional

Fuente: Bruce H.. (2013). Packet Guide to Voice over IP

Los sistemas VoIP nativos eliminan gran parte de lo que se considera la telefonía tradicional. Bueno, casi. Un sistema como el que se ilustra en la Figura 2 implica una gran cantidad de

señalización de control para llevar a cabo las diversas tareas requeridas. VoIP toma todos estos mensajes de señalización y los coloca dentro de paquetes IP. Mientras que los teléfonos tradicionales se pueden utilizar junto con un sistema de VoIP, a menudo es el caso de que no lo son. Después de un proyecto piloto, las empresas que implementan un sistema VoIP comúnmente desean desplegar un solo conjunto de equipos para simplificar el soporte y el mantenimiento. Esto también reduce el costo. Después de esto ocurre, los puntos finales no se refieren a los teléfonos más, sólo los teléfonos VoIP o Ethernet. El nombre de PBX se conserva, aunque ahora se llama IP PBX, lo que realmente significa que es un servidor que se ejecuta en una computadora. Al volver a dibujar la topología, podríamos ver algo como el que se muestra en la Figura 3. También vale la pena mencionar que, como el Protocolo de Internet puede ejecutar sobre casi todos los tipos de arquitectura de comunicación de bajo nivel, la Voz sobre IP también puede funcionar.

Un diagrama de Ven que compara las habilidades para cada topología encontraría muy poca intersección. Siguiendo esta línea de pensamiento para las actividades de contratación o formación en una organización, tenemos que concluir que habría una demanda diferente para alguien conocedor en temas de telefonía tradicional en comparación con alguien que posea un fondo de la red de datos. Cuando se enfrentan a la necesidad de apoyar una infraestructura de VoIP, ¿qué tendrían que aprender las dos personas? Si consideramos el despliegue típico en el lado del consumidor, la persona de telefonía tradicional puede poseer conocimientos sobre planes de marcación, enrutamiento de llamadas, T-1 y características, pero no comprenderá el funcionamiento de una red basada en IP o inalámbrica. (Bruce H. 2013. p.59-62).

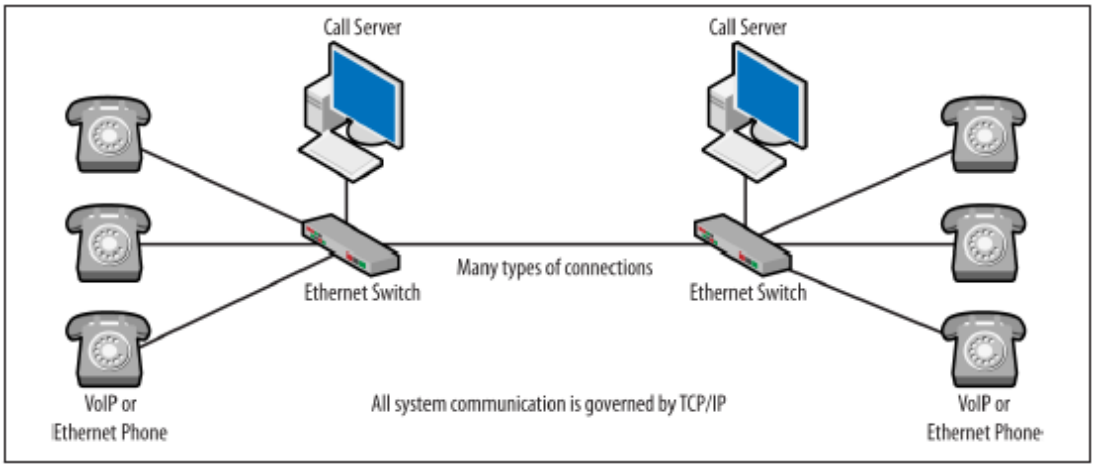


Figura 3: Arquitectura Básica VoIP

Fuente: Bruce H.. (2013). Packet Guide to Voice over IP

2.3.2. Digitalización y transmisión

Por tanto, el primer reto de la telefonía IP es convertir la señal analógica que produce la voz en digital, de forma que pueda ser tratada por Internet. A este proceso se lo conoce como digitalización de la voz. El proceso de digitalización consiste en tomar una muestra de la voz, cuantificada y convertir este valor en un número binario. Si, por ejemplo, cada muestra se representa con 8 bits, y se toman 8.000 muestras por segundo (una cada 0,125 milisegundos), la señal de la voz se podrá convertir en un flujo de datos de 64.000 bits por segundo (8x8.000) como se ve en la figura 4. (Carballar J. 2008. P.80)

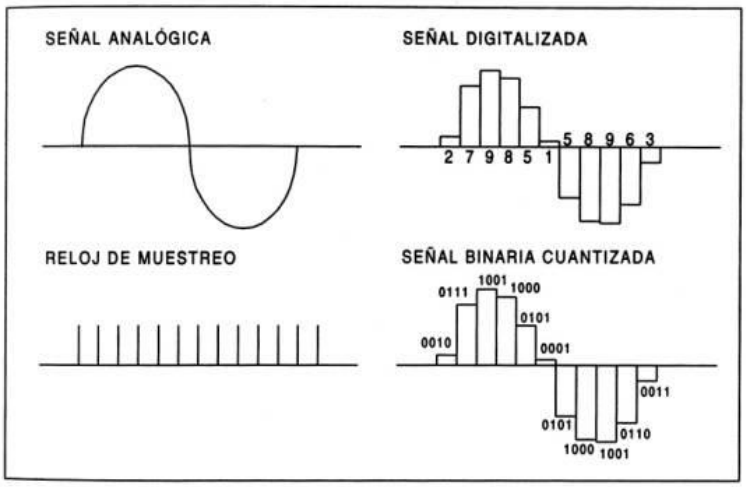


Figura 4: Digitalización de la voz.

Fuente: Carballar J. (2008) La telefonía de internet

2.3. PROTOCOLOS DE TELEFONIA IP

Como se mencionó anteriormente, hay varios protocolos específicos de VoIP, pero sólo dos categorías: señalización y transporte. Los protocolos de señalización manejan las funciones derivadas de la arquitectura del sistema telefónico y los protocolos de transporte llevan los paquetes de voz generados desde el códec. Los teléfonos utilizan el protocolo de señalización para registrarse con el servidor de llamadas, configurar y eliminar llamadas. Los protocolos de señalización también se utilizan para funciones como servicios de directorio y pantallas. Una vez que se ha establecido una llamada, los paquetes de datos de voz normalmente se envían directamente entre los teléfonos que utilizan encapsulación RTP, aunque existen excepciones. Las trayectorias de flujo se muestran en la Figura 5.

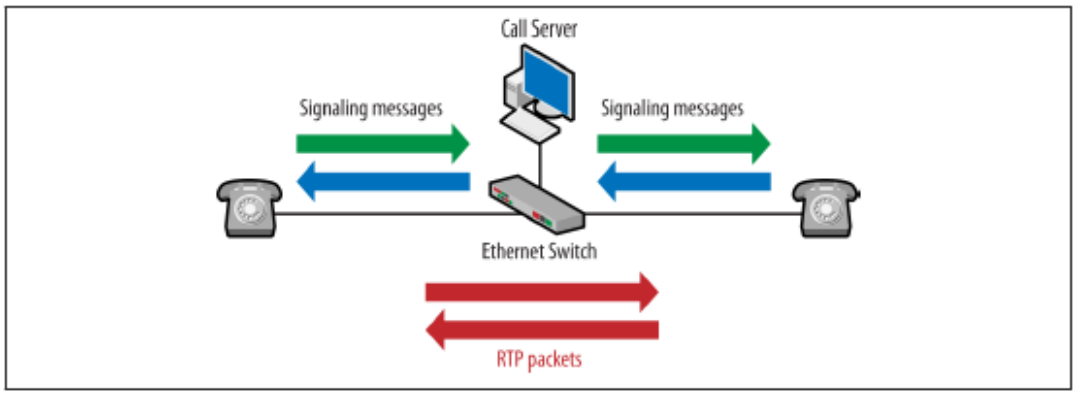


Figura 5: Flujo de protocolo.

Fuente: *Bruce H. (2013). Packet Guide to Voice over IP*

Los paquetes RTP que transportan los datos de voz también pueden fluir desde el teléfono al servidor de llamadas y luego al otro teléfono. (Bruce H. 2013. p.90).

Protocolos de señalización

A pesar de que la arquitectura de VoIP es completamente diferente de la utilizada por la telefonía tradicional, todavía tenemos el requisito básico de la señalización. De alguna manera, los teléfonos tienen que sonar, los números deben ser comunicados, y las rutas tienen que ser configurados, y estas funciones son manejadas por el protocolo de señalización. Los tres tipos más comunes son H.323, Skinny, y el protocolo de inicio de sesión, o SIP.

2.4. PROTOCOLO DE INICIACION DE SESION (SIP)

El protocolo de iniciación de sesión (SIP) es un estándar no propietario de Internet Engineering Task Force, o IETF. El formato de los mensajes SIP es muy similar al de los paquetes de Protocolo de Transferencia de Hipertexto (HTTP), por lo que es muy familiar para la gente en el mundo de las redes de datos. SIP tuvo un comienzo lento, pero ha tomado en gran medida el mundo. Aunque la RFC inicial era algo limitante, es el protocolo de señalización utilizado por la mayoría de las compañías en el futuro, incluyendo Vonage y Skype. Incluso Cisco está pasando de Skinny a SIP. Un ejemplo de paquete SIP se puede ver en la Figura 6.

De la figura 6, podemos ver que el paquete es fácil de leer, tiene un propósito obvio y las partes involucradas están claramente definidas. Estas características y la integración con muchas formas de direccionamiento son algunas de las razones de la popularidad del protocolo.

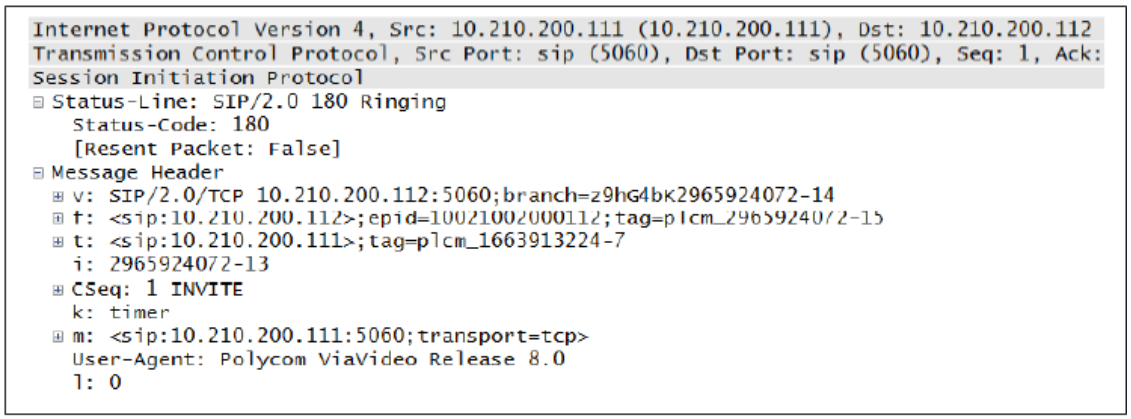


Figura 6: Paquetes SIP

Fuente: Bruce H. (2013). Packet Guide to Voice over IP

SIP es un protocolo Internet Engineering Task Force estandarizado en RFC 3261, aunque hay varias frecuencias RFC. Es un protocolo de señalización no propietario que ahora es compatible con casi todos los proveedores de la industria de VoIP. es probable que las nuevas compilaciones de red adopten SIP sobre las demás. Al igual que los otros protocolos de señalización, SIP se basa en el protocolo de transporte en tiempo real (RTP) para transferir paquetes de voz entre la fuente y el destino. Además, RFC 3261 indica que otros protocolos de soporte (como MEGACO para controlar las funciones de pasarela a la PSTN) pueden ser parte de un despliegue SIP. SIP también tiene una versión segura y se utiliza extensivamente a tronco entre sistemas.

Los primeros trabajos sobre SIP datan de 1999 con RFC 2543. SIP opera en la capa de aplicación con el propósito de iniciar sesiones de usuario para transmisiones multimedia como voz, video, chat, juegos y realidad virtual. Estas sesiones pueden ser unicast o multicast y pueden funcionar con o sin un servidor de llamadas o puerta de enlace. Por la RFC, un sessionCis un intercambio de datos entre los participantes. SIP soporta servicios de asignación y redirección de nombres, características que permiten a los usuarios ser alcanzados o transmitir desde diferentes ubicaciones. Para aquellos de nosotros no se siente cómodo con la terminología RFC, esto significa que cuando los nodos VoIP se conectan entre sí, tiene que haber un mecanismo para establecer la comunicación y establecer algunas reglas. SIP y el Protocolo de descripción de sesión (SDP) se encargan de esto.

Como soporta un conjunto similar de características y codecs, SIP a veces se despliega junto con H.323 o Skinny con el fin de servir a nuevas aplicaciones o características. A menudo se dice que el SIP es mucho más fácil de leer y usar que otros protocolos de señalización no propietarios. Esto puede deberse a que SIP es muy similar en estructura al protocolo de

transferencia de hipertexto, o HTTP. Veremos que hay cierto grado de verdad en este sentimiento. SIP no hace todo lo que ofrece el peso pesado H.323. Está diseñado simplemente para configurar y anular sesiones de medios. Otras funciones incluyen la ubicación y las capacidades del usuario, la disponibilidad y la información de manejo de sesión. Si lee el capítulo H.323, puede haber notado que H.323 es bastante complejo ya menudo intenta negociar o proporcionar información que no se puede utilizar.

Dado que SIP no maneja todo, las implementaciones usan otro protocolo llamado Session Descriptor Protocol, o SDP, para negociar los parámetros de la conexión multimedia. Más allá de esto, las topologías SIP funcionan de la misma forma que cualquier otra configuración de VoIP.

La red está equipada con una PBX VoIP (Private Branch Exchange) en forma de caja Asterisk, un servidor trivial de transferencia de archivos (TFTP), un servidor de protocolo de configuración dinámica de host (DHCP) y un conmutador que proporciona alimentación a través de Ethernet, o PoE. El conmutador también está configurado con puertos duplicados para la captura de paquetes.

Componentes

Al leer acerca de SIP, es útil entender un par de términos específicos de SIP. Los siguientes componentes son los más comunes.

Agente de usuario (UA)

Parte lógica que inicia o responde a transacciones SIP. La UA puede ser un cliente o servidor y tiene estado, por lo que mantiene la sesión.

Cliente de agente de usuario (UAC)

Inicia peticiones y acepta respuestas. Normalmente, es el teléfono SIP que inicia la llamada.

Servidor de agente de usuario (UAS)

Acepta peticiones y envía respuestas.

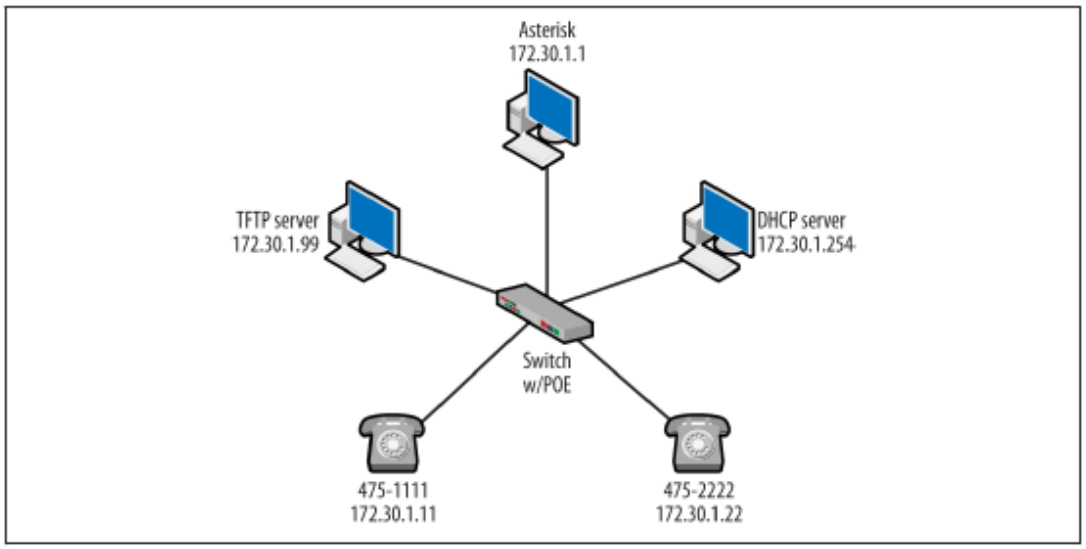


Figura 7: Topología SIP

Fuente: *Bruce H. (2013). Packet Guide to Voice over IP*

Las ubicaciones de UAC y UAS dependen en gran medida de las operaciones de un nodo en particular. Por ejemplo, un nodo puede aceptar peticiones de llamada de otros e iniciar su propio. La topología mostrada en la Figura 7, muestra una configuración particular que puede cambiar a medida que se agregan otros nodos o destinos.

Proxy

Componente intermedio que envía las solicitudes de un UAC a un UAS u otro proxy. Esto se hace principalmente para el enrutamiento, pero puede aplicar políticas como la autenticación. Un ejemplo de implementación estándar es un proxy web. Los clientes envían solicitudes web al proxy, que luego reenvía las solicitudes a los servidores web. Por lo tanto, los clientes nunca se comunican con el servidor web.

Redirect Server

Envía solicitudes de un UAC a un conjunto alternativo de ID de recurso uniforme o URI.

Registrar Server

UAS que acepta los mensajes REGISTER y actualiza la ubicación.

Al actualizar la topología con estas etiquetas de componentes, terminamos con la red mostrada en la Figura 8.

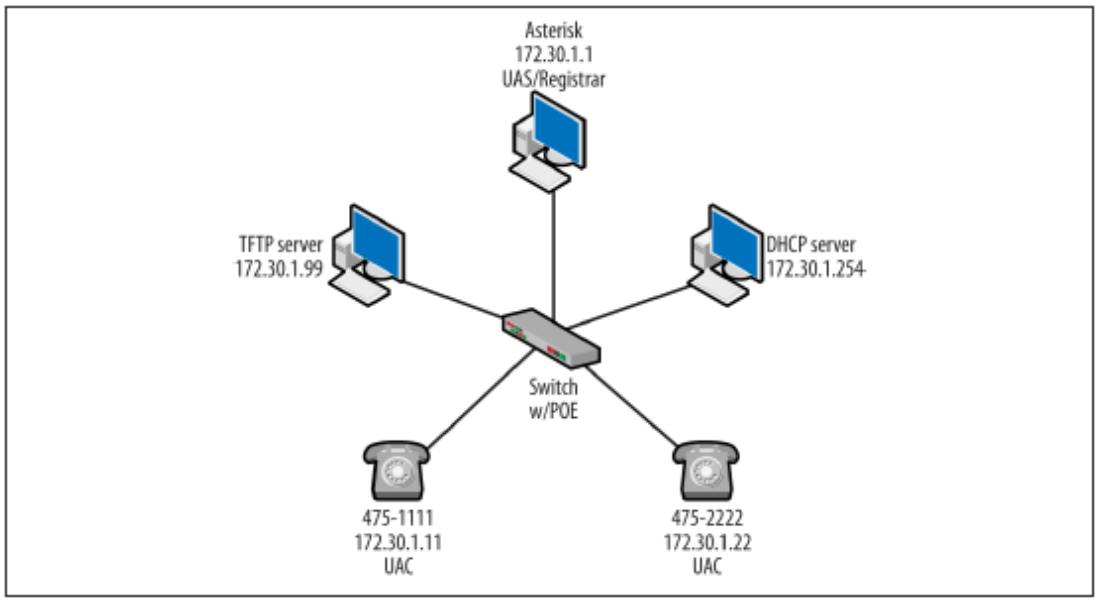


Figura 8: Topología actualizada con etiquetas.

Fuente: *Bruce H. (2013). Packet Guide to Voice over IP*

Esta topología ahora incluye los agentes SIP del cliente y del servidor. Carece de etiquetas para otros componentes porque, en este punto, es un sistema de telefonía aislado que no llama fuera. (Bruce H. 2013. p.102-125).

2.4.1. Direccionamiento

Las conversaciones SIP pueden comenzar poniéndose en contacto con una dirección IP o un nombre de usuario para permitir que el UAC se comunique con otro usuario o recurso de la red. El direccionamiento SIP estándar es similar al correo electrónico, tomando uno de los siguientes formularios (el puerto es opcional y, si no se especifica, se utiliza 5060):

sip:user@domain:port

sip:user@host:port

sip:phone number@domain

2.4.2. Los mensajes SIP

Los mensajes del protocolo de señalización SIP son de dos tipos: solicitudes y respuestas. Los clientes envían mensajes de solicitudes a los servidores; quienes responden a los clientes con mensajes de respuestas. El formato de los mensajes de solicitud y de respuesta es el mismo. Ambos disponen de una cabecera formada por distintos campos y de un cuerpo del mensaje. Como los mensajes de SIP están formados por textos, esto quiere decir que, si una persona viese el contenido de uno de estos mensajes, podría interpretarlo fácilmente.

El formato general de los mensajes (de solicitud y respuesta) esté definido en la recomendación RFC822, y se compone de:

- **Una línea de inicio (*start-line*)**. Esta línea define de tipo de mensajes de que se trata. Existen dos tipos: línea de solicitud, utilizada por los mensajes de solicitud, y línea de respuesta, utilizada por los mensajes de respuesta.
- **Una cabecera** formada por uno o más campo de cabecera. La cabecera se utiliza para incluir información adicional relativa a la solicitud o la respuesta.
- **Una línea en blanco** para indicar el final de la cabecera.
- **El cuerpo del mensaje (message-boy)**. SIP no define la estructura del cuerpo del mensaje ni se ocupa de su contenido. No obstante, normalmente, el cuerpo del mensaje se utiliza para describir el tipo de sesión que se va a establecer, versión del códec a utilizar.

2.4.3. La línea de solicitud

En el caso de los mensajes de solicitud, la línea de inicio recibe el nombre de línea de solicitud y está formada por los siguientes componentes:
A los tipos de solicitudes se los conoce como método (*methods*) y están identificados por una palabra. En la versión 2.0 de SIP se incluyen seis tipos de solicitudes o métodos.

- **INVITE**. Este mensaje se utiliza para invitar a participar en una sesión (una llamada). En el cuerpo del mensaje se incluye el resto de parámetros necesarios: por ejemplo, el asunto de la llamada o el tipo de formato multimedia que puede utilizar el terminal llamante. Por su parte, el terminal llamado incluirá en el cuerpo del mensaje de su respuesta de aceptación los formatos multimedia que acepta.
- **ACK (*aceptación*)**. Esta solicitud se utiliza para que el cliente (llamante) pueda confirmarle al servidor (llamado) que ha recibido su respuesta final de aceptación de participación en la sesión (llamada). Este método se utiliza exclusivamente con solicitudes INVITE, y no con otro tipo de solicitudes.
- **BYE**. Este mensaje se utiliza para terminar una sesión. Generalmente, se envía cuando cuelga el usuario.
- **CANCEL**. Se utiliza para anular una solicitud para que la todavía no se ha recibido respuesta.

- **REGISTER**. Se utilizar para que un cliente pueda registrar su localización actual en un servidor SIP. El cliente puede registrarse en un servidor del que conoce su dirección o en todos los servidores SIP a través de la dirección.

2.4.4. Línea de respuesta

En el caso de tratarse de un mensaje de respuesta, este informara del estado en el que se encuentra el servidor o si la solicitud se ha aceptado o rechazado. La línea de inicio de los mensajes de respuesta se conoce como líneas de estado o línea de respuesta.

El tipo de respuesta se transmite con un código numérico conocido como código de estado (*status code*). La línea de estado está formada por tres componentes: versión del protocolo SIP, el código de estado y un texto con una breve explicación del código de estado incluido en el mensaje. Este texto ayuda a que una persona pueda interpretar directamente el mensaje de respuesta.

Al igual que ocurre con la línea de solicitud, los tres componentes de la línea respuesta están separados por un espacio y termina con un carácter CRLF.

La sintaxis seria la siguiente:

Versión-sip código textoCRLF

Los códigos de estado tienen tres dígitos, donde el primero define la clase de respuesta y los otro dos el mensaje concreto dentro de la clase. Actualmente existen seis clases diferentes de mensaje de respuesta:

- **1xx**. De información (*Informational*). Indica que se ha recibido la solicitud y que se está procesando. Por ejemplo, el mensaje 180 indica que está haciendo sonar el timbre del usuario.
- **2xx**. De aceptación (*Sucessful*). Indica que ha recibido la solicitud y que todo está correcto para ejecutarla.
- **3xx**. Redirección (*Redirection*). Indica que el usuario llamado no está disponible en la dirección utilizada en la solicitud y que será redireccionada a la nueva dirección que se adjunta.
- **4xx**. Fallo en la solicitud (*Request Failure*). Indica que el mensaje de solicitud no es del todo correcto: existen algún error de sintaxis, no se está autorizada, etc.
- **5xx**. Fallo de servidor (*Server Failure*). Indica que, aunque el mensaje de solicitud es válido, el servidor tiene algún problema para aceptarlo: servicio no disponible, saturación, error interno del servidor, etc.

- **6xx**. Fallo general (*Global Failure*). Indica que no se considera respuestas a la solicitud por algún tipo de fallo general.

Salvo las respuestas de información (1xx), el resto se considera respuestas finales que dan terminada la transacción SIP. Las respuestas 1xx son provisionales y no dan por terminada la transacción **SIP.** (Carballar J. 2008. p.90-130)

CÓDIGO DE ESTADO	FRASE PROPUESTA (inglés)	FRASE PROPUESTA (español)
100	Trying	En progreso
180	Ringing	Timbre sonando
181	Call is being forwarded	Llamada en desvió
182	Queued	En cola de espera
183	Session in progress	Sesión en progreso
200	OK	Todo
300	Multiple choice	Múltiples opciones
301	Moved permanenty	Cambiado permanentemente
302	Moved temporarily	Cambiado temporalmente
305	Use proxy	Utiliza proxy
380	Alternative service	Servicio alternativo
400	Bad request	Solicitud incorrecta
401	Unauthorized	Sin autorización
402	Payment required	Se requiere un pago
403	Forbidden	prohibido
404	Not found	No se encuentra
405	Method not allowed	Método no permitido
406	Not acceptable	No aceptable
407	Proxy aunthentication required	Se requiere autentificación del proxy
408	Request timeout	Expirado el tiempo de solicitud
409	Conflict	Conflicto
410	Gone	Recurso no disponible
411	Length required	Contenido insuficiente
413	Request entily too large	Solicitud mayor de lo esperado
414	Request – URI too long	Dirección URI demasiado larga
415	Unsupported media type	Tipo de medio no admitido
416	Unsupported URI scheme	Esquema URI admitido
420	Bad extension	Extensión incorrecta
421	Extension required	Se requiere una extensión
423	Interval too brief	Se requiere una extensión
480	Temporarily not available	No disponible temporalmente
481	Call leg/transaction does not exist	La llamada no existe
482	Loop detected	Detectado un bucle
483	Too many hops	Demasiado saltos
484	Address incomplete	Dirección incompleta
485	Ambiguous	Ambiguo
486	Busy here	Ocupado
487	Request terminated	Solicitud terminada
488	Not aceptable here	Inaceptable
491	Request pending	Solicitud pendiente
493	Undecipherable	Indescifrable
500	Server internal error	Error interno del servidor
501	Not implemented	No implementado
502	Bad gateway	Gateway erróneo
503	Service unavailable	Servicio no disponible
504	Server timeout	Expirado el tiempo del servidor
505	SIP versión not supported	Versión SIP no admitida
513	Message too large	Mensaje demasiado grande
600	Busy everywhere	Todo ocupado
603	Decline	Declinación
604	Does not exist anywhere	No existe
606	Not acceptable	No se acepta

Tabla 1: Código de estado SIP

Fuente: Carballar, J.(2008). VoIP. La telefonía de Internet

2.4.5. Flujos de llamadas SIP

En este tema se describen los flujos de configuración de llamada y de desmontaje en los tres escenarios habituales: llamada directa entre pasarelas SIP, llamada a través de un servidor proxy y llamada a través de un servidor de redireccionamiento.

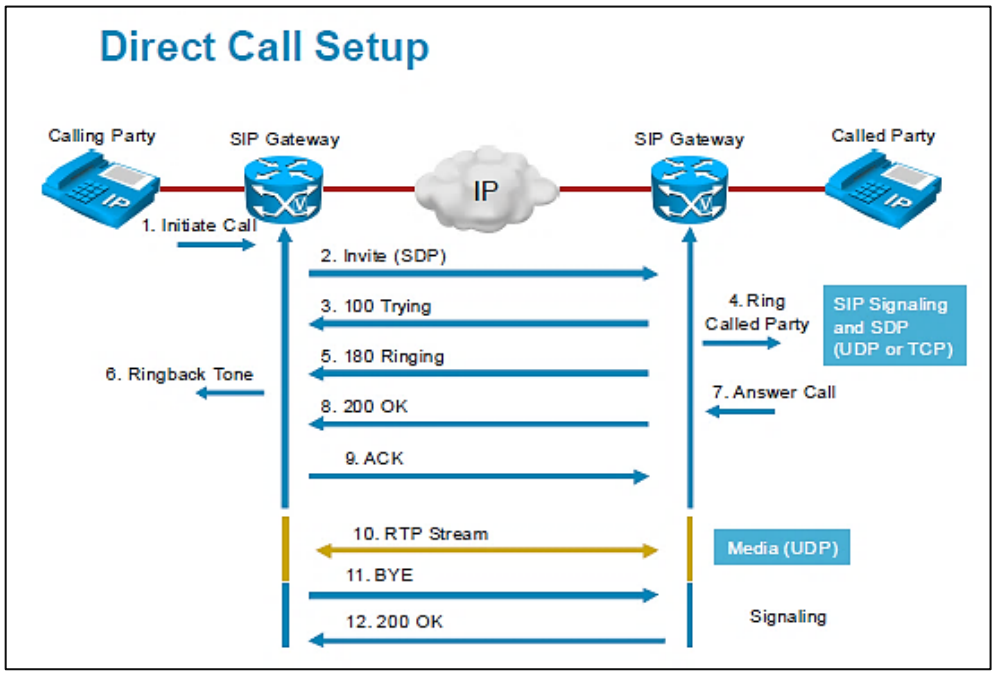


Figura 9: Flujo de llamada SIP

Fuente: Cisco Networking Academy. (2010). Implementing Cisco Voice Communications and QoS. (Vol 1)

Esta figura muestra la configuración de la llamada directa y el desmontaje entre dos pasarelas SIP. Cuando un UAC reconoce la dirección de un punto final de terminación de la información almacenada en caché, o tiene la capacidad de resolverla mediante algún mecanismo interno, el UAC puede iniciar procedimientos de configuración de llamada directos (UAC a UAS). Si un UAC reconoce el destino UAS, el cliente se comunica directamente con el servidor. En situaciones en las que el cliente no puede establecer una relación directa, el cliente solicita la asistencia de un servidor de red.

Paso 1. El punto final inicia una llamada.

Paso 2. El UAC de origen envía una invitación (INVITE) a la UAS del destinatario. los Incluye una descripción de punto final del UAC y la descripción SDP del Soportados.

Paso 3. El UAS del destinatario responde al mensaje INVITE utilizando el comando 100 Tentando mensaje.

Paso 4. La pasarela de terminación envía la señal de llamada al teléfono receptor.

Paso 5. La UAS del destinatario informa a la UAC acerca de la señal de llamada con la llamada mensaje.

Paso 6. La puerta de origen envía el tono de retorno al teléfono de la persona que llama.

Paso 7. El teléfono llamado se quita del gancho.

Paso 8. Si la UAS del destinatario determina que los parámetros de llamada son aceptables, Responde positivamente al UAC del originador utilizando el mensaje 200 OK.

Paso 9. El UAC de origen emite un acuse de recibo (ACK) a la UAS.

Paso 10. En este punto, la UAC y UAS tienen toda la información que se requiere para establecer "Real-Time Transport Protocol" (RTP) entre ellos.

Paso 11. Uno de los participantes termina la llamada. Su UA envía el mensaje BYE al otro UA.

Paso 12. El mensaje BYE es confirmado por el mensaje 200 OK. (Cisco Networking Academy. 2010. p. 300-325)

2.5. EL PROTOCOLO DE TRANSPORTE EN TIEMPO REAL (RTP)

En los años 90, el IETF creo un grupo de trabajo conocido como Audio – Video Transport Working Group (Grupo de trabajo para el transporte de audio y video).su finalidad era desarrollar un protocolo que permitiera el transporte de datos en tiempo real. En 1996 se publicaría el estándar RFC1886 que define el conjunto de protocolos RTP y RTCP. Este estándar quedaría actualizado en 2003 por el RFC3550 y complementado con la RFC3551 y RFC3711.

RTP es el acrónimo de Real Time Transport Protocol (Protocolo de transporte en tiempo real) y se encarga de añadir a los paquetes UDP el número de secuencias, la marca de tiempo y la identificación del tipo de carga útil que transporta. Por su parte, RTCP (RTP Control Protocol, "Protocolo de control RTP") se encarga de informar al remitente de la calidad de recepción y de la identidad de los interlocutores.

El protocolo RTP opera encima de UDP, esto quiere decir que cuando UDP recibe los paquetes se los entrega al protocolo RTP, quien resuelve los posibles problemas que pudieran ocasionar la perdida de paquetes o el cambio de orden de llegada. Para poder hace esto, RTP le añade cierta información adicional a los paquetes, como son: un número de orden y el momento en el que el paquete salió del origen. La primera información se utiliza para detectar la pérdida o desorden de los paquetes, mientras que la segunda resulta útil para calcular parámetros de calidad como el retardo o las fluctuaciones de retardo (jitter). En realidad, RTP no hace nada

para resolver estos problemas, pero los detecta e informa a los protocolos de capas superiores (a la aplicación de VoIP) para que puedan tomar las decisiones correspondientes.

7	**Aplicación**	**Voz sobre IP (VoIP)**
6	Presentación	Codec (ejem. G.722)
5	Sesión	RTP, RTCP
4	Transporte	TCP & UDP
3	Red	IP, Diffserv
2	Enlace	Ethernet
1	Físico	UTP (ejem: Cat 5)

Tabla 2: Protocolo RTP/RTCP dentro del modelo OSI

Fuente: Hersent, O., Petit, J., & Gurle, D. (2009). Beyond VoIP protocols

El protocolo RTCP se utiliza para el intercambio de información de control (número de paquetes perdidos, retardo, jitter, etc.) entre los distintos participantes de la sesión.

En circunstancias normales, el protocolo RTP y RTCP se utilizan conjuntamente, por lo que cuando se asigna un numero de puerto a una sesión RTP, también se asigna otro para la sesión RTCP correspondiente. Generalmente, el número de puerto de la sesión RTP es un número par entre 1.026 y 65.534 (por defecto el 5.004), mientras que el de la sesión RTCP es el número impar correlativo (por defecto el 5.005). no obstante, el uso del protocolo RTCP no es imprescindible para el funcionamiento de la comunicación, por lo que algunas aplicaciones de VoIP le ofrecen al usuario la posibilidad de desactivarlo, aunque esto suponga que no se intercambie información sobre la calidad de la transmisión. (Hersent, O., Petit, J., & Gurle, D. 2009 p. 160-169)

Los protocolos RTP/RTCP pueden ser utilizados tanto para la transmisión de información multimedia unicast como multicast. esto quiere decir que pueden utilizarse tanto para transmisiones en las que hay un solo emisor y receptor (unicast), así como para aquellas en las que un mismo emisor transmite simultáneamente para distintos receptores (multicast). (Carballar J. 2008. p. 139)

CÓDIGO	CODIFICACIÓN	AUDIO/VIDEO	FRECUENCIA (HZ)	CANALES (Audio)	RFC
000	PCMU	Audio	8.000	1	RFC3551
001	Reservado				
002	G726 – 32	Audio	8.000	1	
003	GSM	Audio	8.000	1	RFC3551
004	G723	Audio	8.000	1	Kumar
005	DVI4	Audio	8.000	1	RFC3551
006	DVI4	Audio	16.000	1	RFC3551
007	LPC	Audio	8.000	1	RFC3551
008	PCMA	Audio	8.000	1	RFC3551
009	G722	Audio	8.000	1	RFC3551
010	L16	Audio	44.100	2	RFC3551
011	L16	Audio	44.100	1	RFC3551
012	QCELP	Audio	8.000	1	
013	CN	Audio	8.000	1	RFC3389
014	MPA	Audio	90.000	1	RFC3551
					RFC2250
015	G728	Audio	8.000	1	RFC3551
016	DVI4	Audio	11.025	1	DiPol
017	DVI4	Audio	22.050	1	DiPol
018	G729	Audio	8.000	1	
019	Reservado				
020 – 023	Sin asignar	Audio			
024	Sin asignar	Video			
025	CelB	Video	90.000		RFC2029
026	JPEG	Video	90.000		RFC2435
027	Sin asignar	Video			
028	nv	Video	90.000		RFC3551
029 – 030	Sin asignar	Video			
031	H261	Video	90.000		RFC2032
032	MPV	Video	90.000		RFC2250
033	MP2T	Aud./Vid.	90.000		RFC2250
034	H263	Video	90.000		Zhu
035 – 071	Sin asignar	Video			
072 – 076	Reservado				
077 – 095	Sin asignar				
096 - 127	Para uso de los tipos dinámicos				RFC3551

Tabla 3: Listado de números de identificación de códecs de RTP

Fuente: Carballar, J. (2008). VoIP. La telefonia de Internet.

2.5.1. Formato de los paquetes RTP

Los paquetes RTP se componen de una cabecera de 128 bits y de un cuerpo que contiene la información de la voz codificada o video. El contenido del cuerpo se conoce como carga útil o payload. El tamaño del cuerpo puede ser distinto dependiendo del tipo de carga útil utilizada (tipo de codec), no obstante, siempre debe ser multiplicado de 32 bits.

Determinados tipos de carga útil necesitan incluir más información de control de la que cabe en la cabecera. Para estos casos existen dos alternativas; esta información puede venir incluida como parte de la carga útil (en los primeros n octetos) o se puede utilizar una extensión de la cabecera que se colocara a continuación de la cabecera normal y bits para indicar la longitud de la misma.

Las informaciones que se incluyen en la cabecera de los paquetes RTP son las siguientes:

- **Versión (V).** se trata de dos bits que indican la versión del protocolo RTP utilizado. La versión más reciente actualmente es la 2.
- **Relleno (Padding, P).** se trata de un bit que indica que la carga útil incluye octetos de relleno al final. El último octeto de relleno indica el número total de octetos de relleno existentes. Como el tamaño de la carga útil debe ser múltiplo de 32 bits, el relleno, de haberlo, tendrá un máximo de 24 bits. El bit de relleno se pone 1 para indicar que existe un relleno.
- **Extensión (X).** se trata de un bit que indica que la cabecera utiliza el formato extendido.
- **Cuenta CSRC (CC).** Utiliza 4 bits para indicar el número de identificadores CSRC que se añaden al final de la cabecera fija. Este campo viene a identificar el número de participantes en la comunicación.
- **Marcador (Marker, M).** se trata de un campo de un bit que la RFC1889 deja para que la carga útil lo utilice libremente y que la RFC1890 utiliza para que las aplicaciones que no envían información en los periodos de silencio fijen este bit a un en el primer paquete después de un periodo de silencio.
- **Tipo de carga útil (Payload Type, PT).** Se trata de un campo de 7 bits que contiene el número que identifica el códec utilizado en la carga útil.
- **Numero de secuencia (Sequence Number).** Se trata de un campo de 16 bits que utiliza el remitente para identificar el orden secuencial de envió de los paquetes. Este número le permite al destinatario detectar la posible pérdida o desorden de los paquetes. el número de secuencia del primer paquete se genera de forma aleatoria, incrementándose en una unidad para cada uno de los paquetes siguientes.
- **Contador de tiempo (TimesTamp).** Se trata de un campo de 32 bits que indica el instante en el que se generó la primera muestra de la carga útil. El campo muestra un número entero donde cada unidad es equivalente al periodo de la frecuencia de muestreo utilizada o, lo que es lo mismo, al periodo de tiempo de cada muestra. Por ejemplo, si

la frecuencia de muestreo es 8.000Hz, cada unidad representara el equivalente a 0,125 milisegundos (1/8.000). por otro lado, si cada paquete contiene 5 muestras de voz y el contador de tiempo incluido en el paquete es 31, el siguiente paquete debería mostrar un contador de tiempo igual a 36. Para una frecuencia de 8.000 Hz, esto sería equivalente a indicar que entre la primera muestra del primer paquete y la primera muestra del segundo paquete ha transcurrido un tiempo de 0,625 milisegundos. El contador de tiempo se utiliza para identificar la fluctuación de retardo (jitter).

- **Indetificacion del origen (Synchronization Source, SSRC).** Se trata de un campo de 32 bits que identifica al remitente o a la aplicación intermedia utilizada (mezclador).

Lista de contribuyentes (Contributing Source, CSRC). Cuando se utiliza un mezclador, al campo SSRC identifica al mezclador, utilizándose una lista de campos de 32 bits para identificar a cada una de las fuentes de sonido o video. El número de fuentes de la lista se especifica en el campo CC. Como el campo CC tiene 4 bits, el máximo número de fuentes que permite RTP es 15. (Carballar J. 2008. p. 139-145)

2.6. INTERCAMBIO DE INFORMACIÓN. RTCP

El protocolo RTCP facilita el intercambio periódico de información entre los participantes de la sesión. La finalidad de RTCP es informar a la fuente del sonido o video de la calidad con la que está llegando al destino. Esta información puede ser utilizada por la aplicación o por el operador del servicio para detectar y corregir posibles problemas.

Una información incluida en RTCP que no se incluye en los paquetes RTP es el nombre CNAME (canonical Name, “Nombre canonico”) de los participantes de la sesión. RTP utiliza el numero SSRC para identificar a los participantes, pero este número puede cambiar de una sesión a otra, o incluso el mismo participante podría generar distintos SSRC en una misma sesión (por ejemplo, cuando emite audio y video simultáneamente). El nombre CNAME es único para cada participante y tiene la forma usuario@host. Este nombre no está relacionado con ninguna dirección de correo electrónico, sino que lo crea automáticamente la aplicación componiendo el nombre de usuario y la identificación del ordenador donde se encuentra. Por ejemplo 192.0.2.89 sería un CNAME. A este nombre también se lo conoce como nombre oficial o nombre único.

TIPO	NOMBRE	DESCRIPCIÓN	RFC
192	FIR	Full intra – frame request	RFC2032
193	NACK	Negative acknowledgement	RFC2032
200	SR	Sender report	RFC3551
201	RR	Recelver report	RFC3551
202	SDES	Source description	RFC3551
203	BYE	Goodbye	RFC3551
204	APP	Application – defined	RFC3551
205	RTPFB	Generic RTP feedback	
206	PSFB	Payload – specific	
207	XR	Extended report	RFC3611

Tabla 4: Tipos de paquetes RCTP

Fuente: Carballar, J. (2008). VoIP. La telefonia de Internet.

Se tienen distintos tipos de paquetes RTCP:

- **Informe de emisor** (*SR, Sender Report*). Se utiliza para informar de las estadísticas de los participantes que son emisores activos.
- **Informe de receptor** (*RR, Receiver Report*). Se utiliza para informar de las estadísticas de los participantes que son solo receptores del flujo, no emisores (solo escuchan).
- **Descripción de la fuente** (*SDES, Source Description*). Contiene la descripción de la fuente, incluyendo el nombre CNAME, así como información de carácter personal como el nombre, correo electrónico o número de teléfono del participante.
- **Fin** (Bye). Indica el final de la participación en la sesión.
- **Funciones específicas de la aplicación** (*APP, Application-Specific Functions*). Los paquetes APP permiten enviar información específica de una determinada aplicación o tipo de flujo.

Las especificaciones de RCTP indican que estos paquetes deben enviarse agrupados, de forma que cada grupo incluya, al menos, un paquete de informe (SR o RR) y un paquete SDED. Por tanto, para enviar un paquete de fin de la participación, además habría que incluir, por ejemplo, un paquete SR y otro SDED. Además, él envió de paquete RTCP debe cumplir otras condiciones como: las estadísticas de recepción (SR o RR) se deben enviar tan frecuentemente como lo permita el ancho de banda, los nuevos receptores deben recibir el CNAME de la fuente tan pronto como sea posible, el intervalo de paquetes RCTP debe ser mayor a 5 segundos (este intervalo deber ser calculado aleatoriamente por cada participante para evitar que todos lo hagan al mismo tiempo), etc.

2.6.1. Informe de emisor SR

El informe de emisor o ST lo utilizan los participantes de la sesion que son emisores de paquetes RTP. Los paquetes SR suelen aprovecharse para adjuntar mensajes RR con información sobre los paquetes RTP que se reciben de otros participantes.

Los paquetes SR tienen cuatro secciones distintas:

- Información de cabecera (32 bits)
- El informe de emisor propiamente dicho (160 bits)
- Un informe de receptor RR (192 bits) por cada fuente emisora que se ha escuchado desde el último informe. Si no se ha recibido nada no se adjuntará ningún RR.
- Determinados perfiles específicos necesitan, además, de una extensión de cabecera que sería añadida al final del paquete.

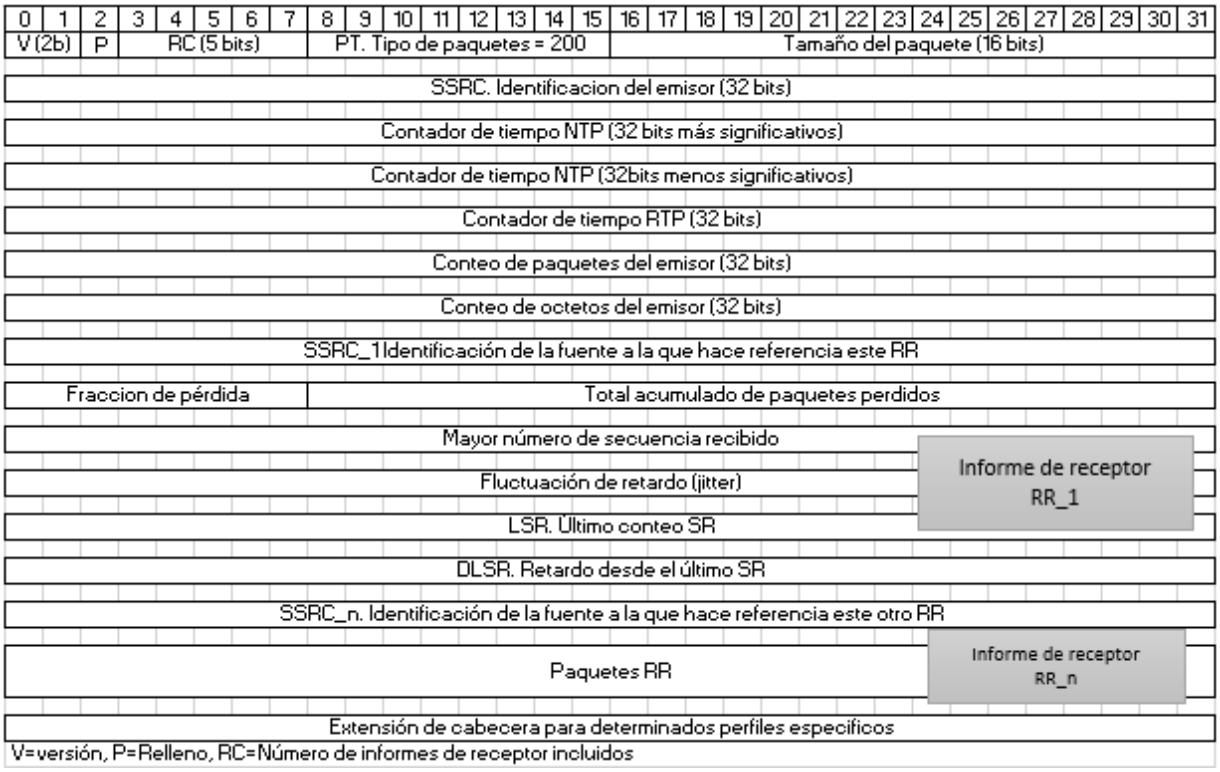


Figura 10: Formato de los paquetes SR.

Fuente: Carballar, J. (2008). VoIP. La telefonia de Internet.

La cabecera de los paquetes SR dispone de los siguientes campos:

- **Versión (V).** Se trata de los bits que indican la versión del protocolo RTP utilizada. La versión actual es la 2.
- **Relleno (P, padding).** Se trata de un bit para indicar que al final del paquete hay octetos de relleno. El último de estos octetos indica el total de ellos.
- **Numero de informes de receptor incluidos en el paquete (RC, Reception Report Count).** Este campo tiene 5bits, por lo que el número máximo de RR que se pueden incluir es 31. El mínimo sería cero.
- **Tipo de paquete (PT, Packet Type).** Son 8 bits que indican el tipo de paquete que se está enviando, En el caso de los paquetes SR tomaría el valor 200.
- **Longitud del paquete (Length).** Indica el número de grupos de 32 bits que forman el paquete RTCP, sin incluir la cabecera. O lo que es lo mismo, número total de grupos menos uno.

SSRC del remitente de este paquete RTCP.

Los campos correspondientes del informe de emisor son los siguientes:

- **Contadores de tiempo NTP** (*Network Tome Protocol, RFC1305*). Se trata de un campo de 64 bits que indica el momento en el que se transmitió este informe SR. Lo que aquí se indica es el tiempo transcurrido en segundos desde el 1 de enero de 1900 (GMT). Los 32 bits menos significativos representan las fracciones de segundos, consiguiéndose una precisión de 200 picosegundos.
- **Contador de tiempo RTP** (*RTP timestamp*). Es un contador de tiempo de 32 bits que emplea el mismo formateo que los contadores RTP. La inclusión de dos contadores de tiempo en el mismo informe le permite al destinatario sincronizarse mejor con el emisor.

Conteo de paquetes del emisor. Indica el número total de paquetes RTP transmitidos por el emisor desde el comienzo de la sesión. Por tanto, este conteo de paquetes es acumulativo.

Conteo de octetos del emisor. Indica el número total de octetos de carga útil (sin incluir cabecera ni relleno) incluidos en los paquetes RTP que ha enviado este emisor desde el comienzo de la sesión.

A la información del emisor le pueden seguir uno o más bloques RR. Incluir estos bloques en el mismo paquete SR ahorra ancho de banda al no tener que enviar paquetes RR independientes con su propia cabecera. No obstante, si no existen bloques RR que transmitir, simplemente se pondrá a cero el campo RC de la cabecera y no se añadirá ningún bloque RR.

2.6.2. Informe de receptor. RR

Todos los participantes que reciben información envían como respuesta los correspondientes informes de receptor RR para mantener informado al emisor de la calidad de recepción. Como hemos visto, en el caso de que el receptor sea también un emisor activo, los bloques RR se podrán incluir al final del paquete SR.

Al igual que los paquetes SR, los RR disponen de su cabecera, con el mismo formato que la de los paquetes SR, y de la posibilidad de añadir una extensión de cabecera. En este caso, el campo PT (tipo del paquete) toma el valor de 201.

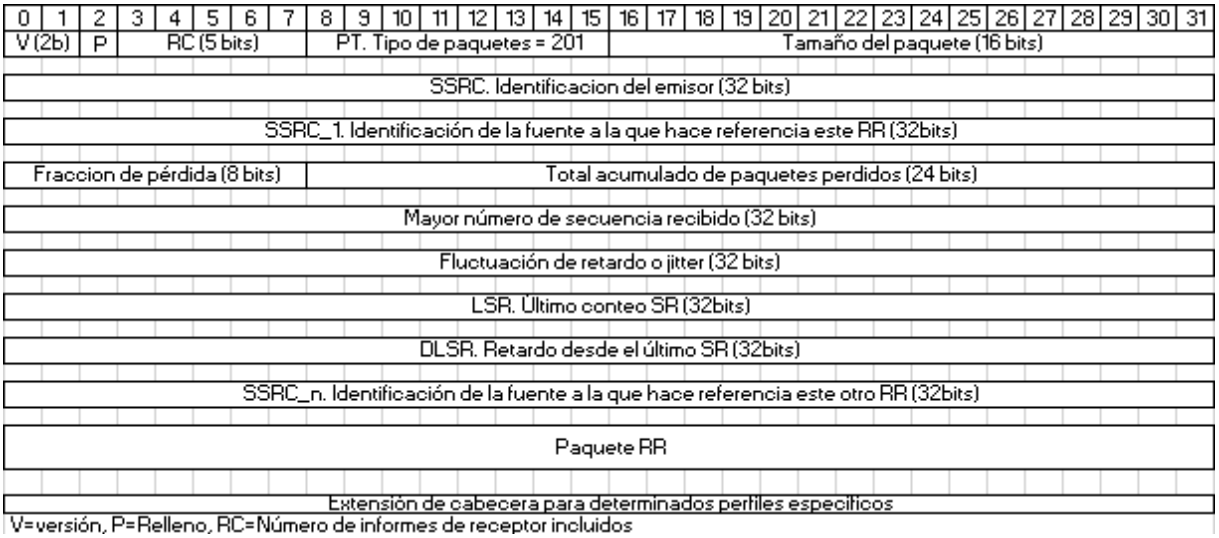


Figura 11: Formato de los paquetes RR

Fuente: Carballar, J. (2008). VoIP. La telefonia de Internet.

A continuación de la cabecera se incluyen tantos bloques RR como sean necesarios (con un máximo de 31). El formato de estos bloques es el siguiente:

- SSRC_n. Es el indicador SSRC del emisor de la información cuyos datos de evaluación se envían a continuación.
- Fracción de pérdida. Es un campo de 8 bits que indica el porcentaje de paquetes RTP que se han perdido desde el último informe. El valor indica el numerador de una fracción donde el denominador es 256. Por ejemplo, si el valor incluido es 64, esto indicara que se han perdido 64/256 = 25%.
- Total, acumulado de paquetes perdidos. Indica el número total de paquetes RTP perdidos desde el comienzo de la sesión.

- Mayor número de secuencia recibido. Se trata del número de secuencia del último paquete RTP que se ha recibido desde ese emisor. Los 16 bits de mayor peso indican simplemente un conteo cíclico.
- Fluctuación de retardo (interarrival jitter). Se trata de una estimación de la variación del retardo entre dos paquetes RTP. La información se ofrece con las mismas unidades que el contador de tiempo RTP.
- Ultimo conteo SR (LSR, Last SR Timestamp). Si SSRC_n es un emisor activo que ha enviado anteriormente un informe de emisor, en este campo se indican los 32 bits centrales de los 64 que se compone el contador de tiempo NTP incluido en el último informe SR recibido de SSRC_n. La utilidad de este campo es informar que se ha recibido bien su último informe SR.
- Retardo desde el último SR (DLSR, Delay Since Last SR). Si SSRC_n es un emisor activo que ha enviado anteriormente un informe de emisor, en este campo se indica el periodo de tiempo entre la recepción del último informe SR y él envió de este informe RR. Este tiempo se indica en unidades de 1/65.536 segundos. (Carballar J. 2008. p.150-166)

2.7. PROTOCOLOS DE TRANSPORTE. TCP/UDP

El protocolo IP fija las normas para que los paquetes alcancen su destino, pero lo que no garantiza es cuando. Cuantos o en qué orden lo van a hacer. De eso se encarga TCP/UDP.

Los servicios como correo electrónico, transferencia de archivo o acceso remoto necesitan que la información generada en un extremo de la conexión llegue al otro extremo en el orden original y sin que se haya perdido o duplicado ningún byte. Para estos casos, el protocolo adecuado es TCP (Transmission Control Protocol,'Protocolo de control de transmisión'). Este protocolo proporciona un flujo fiable de byte en los dos sentidos de la conexión. Garantiza que los bytes que salen del nodo origen sean entregados en el nodo destino de una forma fiable, en su mismo orden y sin duplicación TCP es lo que se conoce como protocolo orientado a la conexión.

NUMERO	PROTOCOLO	DESCRIPCIÓN	REFERENCIA
0	HOPOPT	Opción De IPv6 Hop-By-Hop	RFC1883
1	ICMP	Internet Control Message	RFC792
2	IGMP	Internet Group Management Protocol (Multicast)	RFC1112
3	GGP	Gateway-to-Gateway Protocol	RFC823
6	TCP	Transmition Control	RFC793
17	UDP	User Datagram Protocol	RFC768
27	RDP	Reliable Data Protocol	RFC908
41	IPv6	IPv6	RFC2292
46	RSVP	Resource Reservation Protocol	RFC2205
47	GRE	General Routing Encapsulation	RFC2784
48	MHRP	Mobile Host Routing Protocol	
50	ESP	Encapsulating Header (IPSec)	RFC2406
51	AH	Authentication Header (IPSec)	RFC2402
55	MOBILE	IP Mobility	
57	SKIP	Simple Key Management for Internet Protocol	
58	IPv6 – ICMP	ICMP For IPv6	RFC1883
89	OSPF	Open Shortest Path First	RFC1583
92	MTP	Multicast Transport Protocol	RFC1301
95	MICP	Mobile Internetworking Control Protocol	
115	L2TP	Layer Two Tunnelling Protocol	RFC2661
121	SMP	Simple Message Protocol	
123	PTP	Performance Transparency Protocol	
138 – 252	Sin asignar		
253 – 254	Utilizado para experimentación y pruebas		RFC3692
255	Reservado		

Tabla 5: Ejemplos de números de protocolos asignados por IANA

Fuente: IANA (2010)

Cuando se necesita transmitir voz o video, es más importante transmitir con velocidad que garantizar el hecho de que lleguen absolutamente todos los bytes, o de que no haya ningún byte duplicado. Para estos casos, el protocolo de transporte utilizado es UDP (User Datagram Protocol,'Protocolo de datagrama de usuario'). UDP no tiene mecanismos para confirmar la recepción de los paquetes, por lo que, entre los paquetes enviados con este protocolo, algunos pueden llegar desordenados, duplicados o puede que no lleguen. UDP es un protocolo no orientado a la conexión.

El protocolo UDP puede ser especialmente útil en aquellas redes que ya son suficientemente fiables por si mismas, para aquellas comunicaciones que no requieren más de un paquete, para aquellos servicios que disponen de sus propios procedimientos de corrección de error o para servicios de transmisión de voz o video donde la velocidad es más importante que la fiabilidad. Hay que tener en cuenta que un paquete UDP puede contener información necesaria para reproducir entre 10 y 40 milisegundos de sonido, por lo que la pérdida de un paquete, aun no siendo deseable, no influye grandemente en la calidad de sonido en destino, y mucho menos en

el entendimiento de una conversación. De hecho, la perdida de hasta un 5% de los paquetes puede considerarse aceptable. Otra cosa distinta es que se pierdan grupos de paquetes de forma constante.

Otro problema distinto es si los paquetes llegan desordenados. Como los paquetes UDP no tienen el concepto del orden de salida, los paquetes son entregados a la capa superior en el mismo orden en el que van llegando, lo que podría producir una pérdida de calidad. No obstante, en la práctica, los paquetes de una misma sesión suelen utilizar la misma ruta, lo que hace que lleguen en el mismo orden. La probabilidad de que esto no sea así es extremadamente pequeña. Aunque TCP y UDP son los protocolos de la capa de transporte más utilizados por las aplicaciones de Internet, en realidad existe una larga lista de protocolos de este tipo. La IANA (Internet Assigned Numbers Authority, "Agencia de asignación de números de Internet") dispone de una lista completa que actualmente contiene 134 protocolos (www.iana.org/assignments/protocol-numbers). (Edwards, J., & Bramante, R. 2009. p. 310-324)

2.7.1. Los paquetes TCP Y UDP

Los componentes de la cabecera del protocolo TCP son los siguientes:

- Puerto origen. Son 16 bits que representan el número de puerto de los equipos remitente. Este número identifica la aplicación concreta que transmite los datos.
- Puerto de destino. Se trata de 16 bits que representan el número de puerto del equipo destino. Este número identifica la aplicación concreta del equipo de destino que recibirá los datos. Existen números de puertos ya asignados a ciertas aplicaciones conocidas. Este es el caso del puerto 80, asignado al programa servidor de páginas Web.
- Numero de secuencia. (Sequence number). Es un número secuencial de 32 bits dedicado a asegurar que los paquetes en el destino son reensamblados en el orden correcto.
- Confirmación. (Acknowledgment). El extremo que envía el paquete le indica al otro extremo que ha recibido correctamente todos los paquetes anteriores a este número.
- Tamaño. (Offset). Indica la cantidad de bloques de 32 bits incluidos en la cabecera del paquete.
- Reservado. Se trata de 6 bits que están siempre puestos a cero.
- Indicadores (Flags). Se trata de 6 bits dedicados a determinadas labores de control. El objetivo de cada uno de ellos es el siguiente:

- URG. Urgencia. Cuando está a uno le indica al receptor que lea el dato del campo Puntero de urgencia.
- PSH. Envió forzado (Push). Cuando está a uno le indica a la capa TCP del destino que debe pasar a la capa aplicación estos datos sin demora. Esto evita que los datos puedan estar esperando en TCP a que se complete un segmento. En ocasiones, una aplicación de destino ha recibido todos los datos enviados.
- RST. Inicializar (Reset). Indica que se corte la conexión actual.
- SYN. Sincronización. Este bit se pone a uno en el primer paquete de una sesión TCP para indicarle al destino que empiece a contar la secuencia de números de los paquetes. Este bit nunca está a uno durante el resto de la sesión.
- FIN. Indica que el remitente ha terminado de enviar datos. Esto hace que se termine la sesión.

- Ventana (Window). Indica el número de octetos (bytes) que puede aceptar el destinatario. Esta información la envía el destinatario con cada paquete de confirmación (Acknowledgment). El emisor no puede enviar más datos, octetos, que los indicados por el tamaño de la ventana.
- Suma de verificación. (Checksum). Este valor se utiliza para comprobar la integridad de la cabecera y de los datos. La suma de verificación de los paquetes IP verifica la integridad de la cabecera, pero la de los paquetes TCP comprueba también la integridad de los datos.
- Puntero de datos urgentes. Cuando el indicador URG está a uno, indica cual es el último byte de datos que es urgente. Al destinatario le sirve para saber cuántos datos urgentes llegan. Este campo lo utilizan algunas aplicaciones como Telnet o FTP.
- Opciones. Este espacio hace posible que determinadas aplicaciones puedan intercambiarse parámetros adicionales.
- Relleno. (Padding). Se trata de bits de relleno para completar los 32 bits no cubiertos por los datos de opciones.

En relación con el valor del campo Ventana, Windows 95, 98, Me y XP fijan automáticamente el tamaño de este campo en 8Kb. Windows NT y Windows 2000 lo fijan en 16 Kb. Este tamaño adecuado de este valor depende del tiempo que necesita un paquete para viajar de un extremo a otro, latencia. Tiempos menores a 100 milisegundos se considera una latencia baja, mientras que tiempos mayores a 200 milisegundos se considera una latencia alta. Los tiempos normales están entre ambos valores.

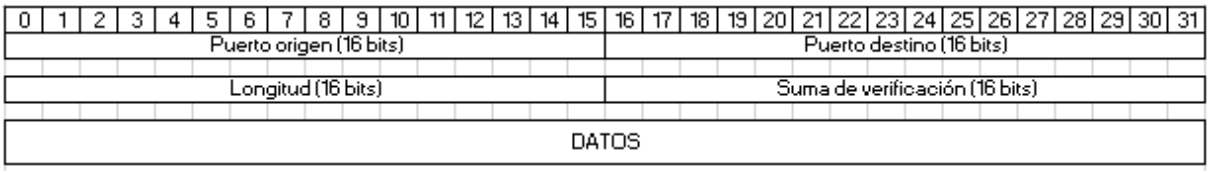


Figura 12: Formato de la cabecera de un paquete UDP

Fuente: Carballar, J. (2008). VoIP. La telefonia de Internet.

A mayor tamaño de ventana menor latencia. En Windows se puede modificar el tiempo de latencia con la utilidad Regedit.

Para comprobar la latencia de nuestra conexión se puede utilizar la utilidad Tracert, presente en la mayoría de los sistemas operativos.

En cuanto a los paquetes UDP, este protocolo es muy ligero, su cabecera silo necesita de los números de puerto origen, puerto destino, longitud del paquete UDP y suma de verificación. (Carballar J. 2008. p.304-310)

2.8. SOFTPHONE

Se llama así al software que se instala en el ordenador y que le permite establecer llamadas de telefonía sobre IP. Este software se encarga tanto de la codificación de la voz como del manejo del protocolo. Este tipo de solución es la forma más económica de acceder a los servicios de VoIP. De hecho, suele ser habitual que el proveedor del servicio facilite el software de forma gratuita. Como Skype, Whatsapp, Messenger, Facebook, etc.

Un softphone (en inglés combinación de software y de telephone) es un software que es utilizado para realizar llamadas a otros softphones o a otros teléfonos convencionales usando un VoIP (Voz sobre IP) o ToIP (Telefonía sobre IP).

Normalmente, un softphone es parte de un entorno Voz sobre IP y puede estar basado en el estandard SIP/H.323 o ser privativo. Hay muchas implementaciones disponibles, como la ampliamente disponible Skype, Windows Messenger o NetMeeting de Microsoft.

Los softphone típicos basados en SIP actualmente comprenden - eyeBeam de CounterPath (anteriormente Xten), OpenWengo, Nexge, sipXphone, Adore Stphone, Express Talk, Zoiper, StarTele Logic, Vippie y SJphone. Funcionan bien con la mayoría de los ITSP - Proveedores de Servicios de Telefonía por Internet. Se puede conectar usando un teléfono USB o un enlace usb a un softphone y obtener un servicio gratuito VoIP de teléfono a teléfono.

El muy popular Skype no es simplemente un softphone sino un servicio P2P VOIP.

Los softphone son realmente parte de un grupo tecnológico mayor, el CTI (Integración Computadora Telefonía).

Algunos softphones están implementados completamente en software, que se comunica con las PABX a través de la (LAN) Red de Área Local - TCP/IP para controlar y marcar a través del teléfono físico. Generalmente se hace a través de un entorno de centro de llamadas, para comunicarse desde un directorio de clientes o para recibir llamadas. En estos casos, la información del cliente aparece en la pantalla de la computadora cuando el teléfono suena, dando a los agentes del centro de llamadas determinada información sobre quién está llamando y cómo recibir y dirigirse a esa persona.

2.8.1. EKIGA

Ekiga, anteriormente llamado GnomeMeeting, es una aplicación de software libre para realizar videoconferencias y telefonía IP para GNOME.

Usa el hardware o software compatible con H.323 (como Microsoft Netmeeting) y se libera bajo licencia GPL. Además, está disponible para sistemas Unix y Windows.

Permite todas las características modernas de una videoconferencia como soporte de proveedor inteligente o llamadas de telefonía desde el ordenador a un teléfono.

Para su correcto funcionamiento debe disponerse de una cuenta SIP, que puede crearse gratuitamente desde. Por otro lado, para poder realizar llamadas a teléfonos convencionales desde el PC se debe disponer de una cuenta con algún servidor de telefonía por internet. El mismo programa recomienda el proveedor Diamondcard Worldwide Communication Service, si bien existen muchos otros como VoIPBuster. Estos servicios no son gratuitos, sino que se paga al proveedor del servicio en función del teléfono de destino según sus tarifas.

Figura 13: Software Softphone Ekiga

Fuente: www.ekiga.org (2010) Pag. principal

2.9.ELASTIX

Elastix es un software de servidor de comunicaciones unificadas que reúne PBX IP, correo electrónico, mensajería instantánea, fax y funciones colaborativas. Cuenta con una interfaz Web e incluye capacidades como un software de centro de llamadas con marcación predictiva.

La funcionalidad de Elastix está basada en proyectos libres como Asterisk, FreePBX, HylaFAX, Openfire y Postfix. Estos paquetes ofrecen las funciones de PBX, fax, mensajería instantánea y correo, respectivamente.

Arquitecturas soportadas

Actualmente Elastix soporta tres arquitecturas.

- Intel x86-compatible (32 bit)
- Intel x86-64 (64 bit).
- ARM

Características

Soporte para hardware de telefonía

Elastix soporta la mayor parte de hardware de telefonía existente que es soportado o fabricado para Asterisk, incluyendo controladores compatibles a través del proyecto Zaptel o versiones

modificadas del mismo. Otros controladores son compatibles con el proyecto mISDN y otros proyectos.

Elastix también es compatible con otras marcas de teléfonos gracias a los protocolos SIP y IAX que implementa Asterisk. El protocolo SIP es actualmente un estándar utilizado en su mayoría por los fabricantes de teléfonos IP y su funcionamiento es nativo para voz con Elastix, independientemente de alguna funcionalidad adicional que estos tengan.

Módulo de centro de llamadas

Elastix fue la primera distribución que incluye un módulo de centro de llamadas con un marcador predictivo, lanzado como software totalmente libre. Este módulo se puede instalar desde la misma interfaz web de Elastix a través de un cargador de módulos. El módulo de centro de llamadas puede manejar campañas entrantes y salientes.

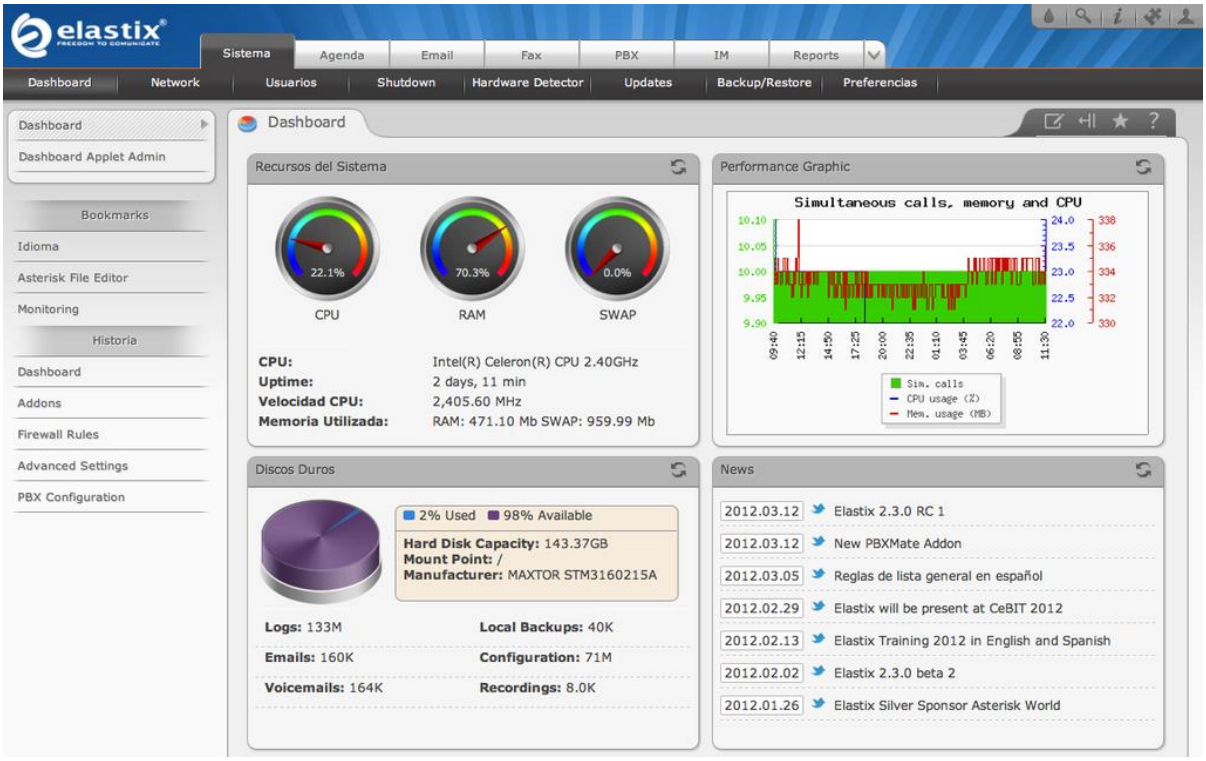


Figura 14: Interfaz web de Elastix

Fuente: www.elastix.org (2016) Pag. principal

2.10. ENRUTAMIENTO EIGRP

EIGRP se lanzó originalmente en 1992 como un protocolo exclusivo disponible solamente en los dispositivos de Cisco. En 2013, Cisco cedió una funcionalidad básica de EIGRP como estándar abierto al IETF, como una RFC informativa. Esto significa que otros proveedores de redes ahora pueden implementar EIGRP en sus equipos para que

interoperen con routers que ejecuten EIGRP, ya sean de Cisco o de otros fabricantes. Sin embargo, las características avanzadas de EIGRP, como las rutas internas de EIGRP necesarias para la implementación de la red privada virtual dinámica multipunto (DMVPN), no se cederán al IETF. Como RFC informativa, Cisco mantendrá el control de EIGRP. EIGRP es un protocolo de routing vector distancia avanzado que incluye características que no se encuentran en otros protocolos de routing vector distancia, como RIP e IGRP. (Edgeworth, B. 2014. p. 125-136)

2.10.1. Tipos de paquetes EIGRP

EIGRP utiliza cinco tipos de paquetes distintos, algunos en pares. Los paquetes EIGRP se envían mediante entrega RTP confiable o poco confiable y se pueden enviar como unidifusión o multidifusión —o, a veces, de ambas maneras. Los tipos de paquetes EIGRP también reciben el nombre de "formatos de paquetes EIGRP" o "mensajes EIGRP". Las cuales son:

- Paquetes de saludo: se utilizan para descubrir a los vecinos y para mantener las adyacencias de vecinos.
- Paquetes de actualización: propagan información de routing a vecinos EIGRP.
- Paquetes de acuse de recibo: se utilizan para acusar recibo de un mensaje EIGRP que se envió con entrega confiable.
- Paquetes de consulta: se utilizan para consultar rutas de vecinos.
- Paquetes de respuesta: se envían en respuesta a consultas EIGRP.

En la figura 1, se muestra que los mensajes EIGRP normalmente se encapsulan en paquetes IPv4 o IPv6. Los mensajes EIGRP para IPv4 usan IPv4 como el protocolo de capa de red. El campo de protocolo IPv4 usa 88 para indicar que la porción de datos del paquete es un mensaje EIGRP para IPv4. Los mensajes EIGRP para IPv6 se encapsulan en paquetes IPv6 que utilizan el campo de encabezado siguiente 88. Al igual que el campo de protocolo para IPv4, el campo de encabezado siguiente de IPv6 indica el tipo de datos transportados en el paquete IPv6.

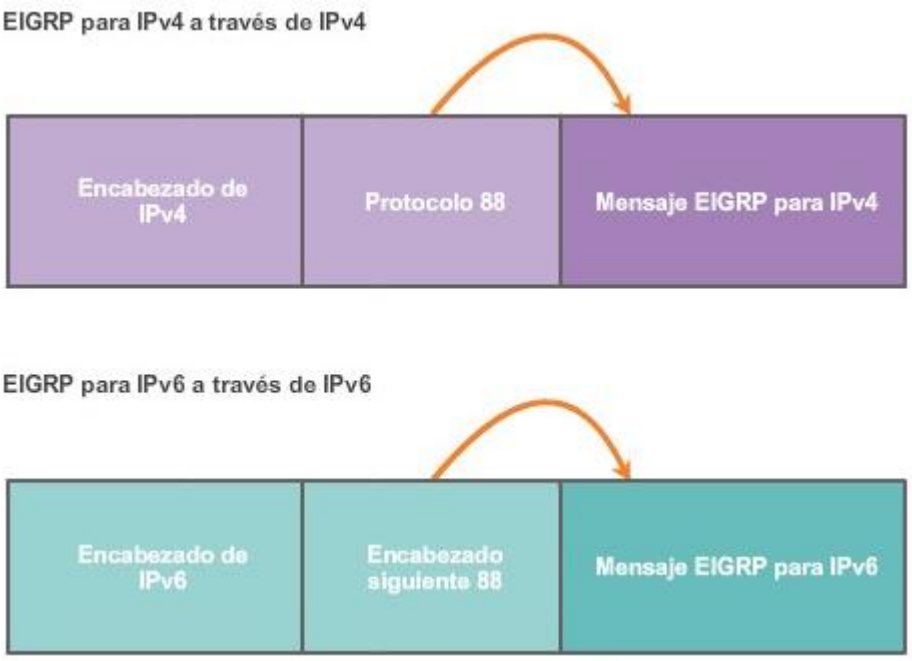


Figura 15: Encapsulación de los mensajes de EIGRP

Fuente: Cisco Networking Academy. (2014). Routing y switching de CCNA: Escalamiento de redes.

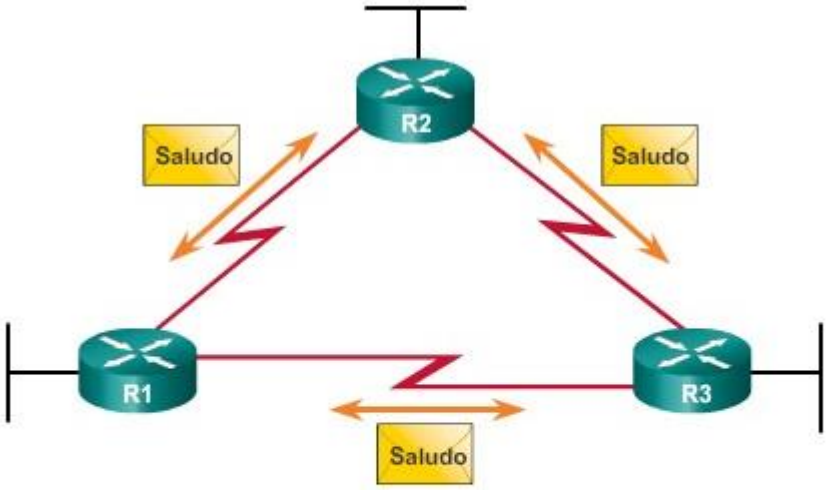
2.10.1.1. Paquetes de saludo EIGRP

Los routers utilizan los paquetes de saludo para formar adyacencias de vecinos EIGRP, también conocidas como "relaciones de vecinos". Los paquetes de saludo EIGRP se envían como transmisiones IPv4 o IPv6 de multidifusión y utilizan entrega RTP poco confiable. Esto significa que el receptor no responde con un paquete de acuse de recibo.

En la mayoría de las redes, los paquetes de saludo EIGRP se envían como paquetes de multidifusión cada cinco segundos. Sin embargo, en redes multipunto multiacceso sin difusión (NBMA), como con enlaces de acceso de T1 (1,544 Mb/s) o más lentos, los paquetes de saludo se envían como paquetes de unidifusión cada 60 segundos.

EIGRP también usa paquetes de saludo para mantener adyacencias establecidas. Un router EIGRP supone que, mientras reciba paquetes de saludo de un vecino, el vecino y sus rutas siguen siendo viables.

EIGRP utiliza un temporizador de espera para determinar el tiempo máximo que el router debe esperar para recibir el siguiente saludo antes de declarar que el vecino es inalcanzable. De manera predeterminada, el tiempo de espera es tres veces el intervalo de saludo, es decir, 15 segundos en la mayoría de las redes y 180 segundos en redes de baja velocidad. Si el tiempo de espera expira, EIGRP declara la ruta como inactiva y DUAL busca una nueva ruta mediante el envío de consultas.



Ancho de banda	Enlace de ejemplo	Intervalo de saludo predeterminado	Tiempo de espera predeterminado
1.544 Mbps	Frame relay multipunto	60segundos	180segundos
Superior a 1544 Mb/s	T1, Ethernet	5segundos	15segundos

Figura 16: Tiempo de saludo y espera para EIGRP

Fuente: Cisco Networking Academy. (2014). Routing y switching de CCNA: Escalamiento de redes.

2.10.1.2. Paquetes de actualización EIGRP

EIGRP envía actualizaciones incrementales solo cuando se modifica el estado de un destino. Esto puede incluir cuando una nueva red está disponible, cuando una red existente deja de estar disponible, o cuando ocurre un cambio en la métrica de routing de una red existente.

En lo que respecta a sus actualizaciones, en EIGRP se utilizan los términos parciales y limitados. El término parcial significa que la actualización sólo envía información acerca de los cambios de ruta. El término "limitada" se refiere a la propagación de las actualizaciones parciales que se envían solo a aquellos routers que se ven afectados por el cambio EIGRP minimiza el ancho de banda que se requiere para enviar actualizaciones EIGRP.

Los paquetes de actualización EIGRP usan entrega confiable, lo que significa que el router emisor requiere un acuse de recibo. Los paquetes de actualización se envían como multicast cuando son requeridos por múltiples routers, o como unicast cuando son requeridos por sólo un router.

2.10.1.3. Paquetes de acuse de recibo EIGRP

EIGRP envía paquetes de acuse de recibo (ACK) cuando se usa el método de entrega confiable. Un acuse de recibo EIGRP es un paquete de saludo EIGRP sin ningún dato. RTP utiliza una entrega confiable para los paquetes EIGRP de actualización, consulta y respuesta. Los paquetes de acuse de recibo EIGRP se envían siempre como transmisiones de unidifusión poco confiables. El sentido de la entrega poco confiable es que, de otra manera, habría un bucle interminable de acuses de recibo.

Nota: en algunos documentos, se hace referencia al saludo y al acuse de recibo como un único tipo de paquete EIGRP.

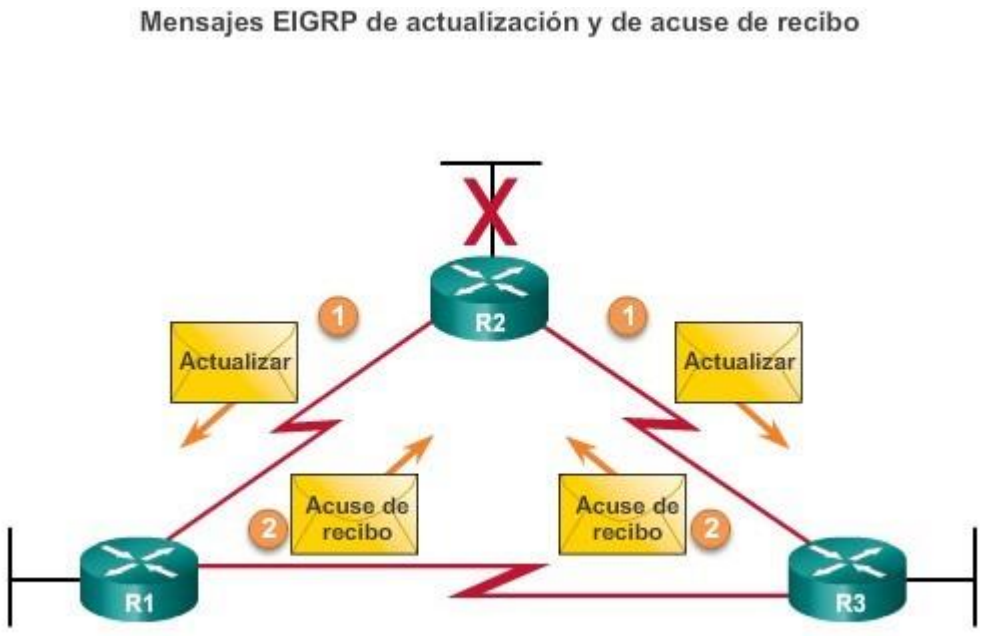


Figura 17: Mensajes EIGRP de actualización y de acuse de recibo

Fuente: Cisco Networking Academy. (2014). Routing y switching de CCNA: Escalamiento de redes.

2.10.1.4. Paquetes de consulta EIGRP

DUAL utiliza paquetes de consulta y de respuesta cuando busca redes y cuando realiza otras tareas. Los paquetes de consulta y respuesta utilizan una entrega confiable. Las consultas utilizan multicast o unicast, mientras que las respuestas se envíen siempre como unicast.

En la figura, R2 ha perdido la conectividad con LAN y envía consultas a todos los vecinos EIGRP y busca cualquier ruta posible hacia la LAN. Debido a que las consultas utilizan entrega confiable, el router receptor debe devolver un paquete de acuse de recibo EIGRP.

El acuse de recibo informa al emisor de la consulta que se recibió el mensaje de consulta. Para que el ejemplo sea más simple, se omitieron los acuses de recibo en el gráfico.

Paquetes de respuesta EIGRP

Todos los vecinos deben enviar una respuesta, independientemente de si tienen o no una ruta a la red fuera de servicio. Debido a que las respuestas también usan entrega confiable, los routers como el R2 deben enviar un acuse de recibo.

Quizá no sea obvio por qué el R2 debería enviar una consulta para una red que sabe que está inactiva. En realidad, solo la interfaz del R2 que está conectada a la red está inactiva. Otro router podría estar conectado a la misma LAN y tener una ruta alternativa a la misma red. Por lo tanto, el R2 consulta por un router tal antes de eliminar completamente la red de su tabla de topología.

Figura 18: Mensajes EIGRP de consulta y de respuesta

Fuente: Cisco Networking Academy. (2014). Routing y switching de CCNA: Escalamiento de redes.

2.10.2. TLV y encabezado de paquetes EIGRP

Los campos importantes incluyen el campo de código de operación y el campo de número de sistema autónomo. El código de operación especifica el tipo de paquete EIGRP de la siguiente manera:

- Actualizar
- Consulta
- Respuesta
- Saludo

El número de sistema autónomo especifica el proceso de routing EIGRP. A diferencia de RIP, se pueden ejecutar varias instancias de EIGRP en una red, y el número de sistema autónomo se usa para realizar el seguimiento de cada proceso EIGRP en ejecución.

El mensaje de parámetros de EIGRP incluye las ponderaciones que EIGRP usa para su métrica compuesta. Solo el ancho de banda y el retardo se ponderan de manera predeterminada. Ambos se ponderan de igual manera, por ello, tanto el campo K1 para el ancho de banda como el campo K3 para el retraso se establecen en uno (1). Los demás valores K se establecen en cero (0).

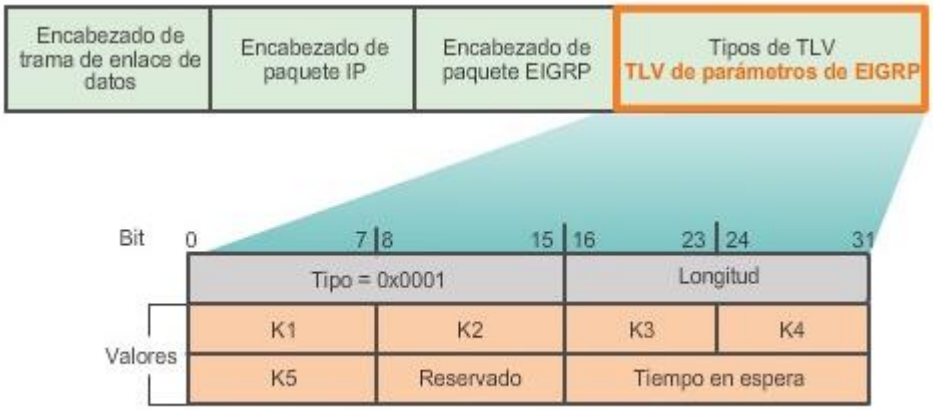


Figura 19: Parámetros EIGRP

Fuente: Cisco Networking Academy. (2014). Routing y switching de CCNA: Escalamiento de redes.

2.10.3. Neighborhood Adjacency EIGRP

El objetivo de cualquier protocolo de routing dinámico es descubrir redes remotas de otros routers y lograr la convergencia en el dominio de routing. Antes de que se pueda intercambiar cualquier paquete de actualización EIGRP entre routers, EIGRP debe descubrir a sus vecinos. Los EIGRP vecinos son otros routers que ejecutan EIGRP en redes conectadas directamente.

EIGRP utiliza paquetes de saludo para establecer y mantener las adyacencias de vecinos. Para que dos routers EIGRP se conviertan en vecinos, deben coincidir varios parámetros entre ambos. Por ejemplo, dos routers EIGRP deben usar los mismos parámetros de métrica de EIGRP y ambos deben estar configurados con el mismo número de sistema autónomo. Cada router EIGRP mantiene una tabla de vecinos, que contiene una lista de los routers en los enlaces compartidos que tienen una adyacencia EIGRP con ese router. La tabla de vecinos se usa para rastrear el estado de estos vecinos EIGRP.

2.10.4. Métrica de EIGRP

De manera predeterminada, EIGRP utiliza los siguientes valores en su métrica compuesta para calcular la ruta preferida a una red:

- Ancho de banda: el ancho de banda más lento entre todas las interfaces de salida, a lo largo de la ruta de origen a destino. El ancho de banda se muestra en kilobits por segundo (kb/s). La mayoría de las interfaces seriales usan el valor de ancho de banda predeterminado de 1544 kb/s o 1 544 000 b/s (1,544 Mb/s).
- Retraso: la acumulación (suma) de todos los retrasos de las interfaces a lo largo de la ruta (en decenas de microsegundos).

Medios	Retardo
Ethernet	1.000
Fast Ethernet	100
Gigabit Ethernet	10
Token Ring 16 M	630
FDDI	100
T1 (serial predeterminada)	20 000
DS0 (64kb/s)	20 000
1024 kb/s	20 000
56 kb/s	20 000

Tabla 6: Valores de retraso de interfaz

Fuente: Cisco Networking Academy. (2013). Routing y switching de CCNA: Principios básicos de routing y switching.

Si bien EIGRP calcula automáticamente la métrica de la tabla de routing utilizada para elegir la mejor ruta, es importante que el administrador de red comprenda cómo se determinaron estas métricas.

$$Metrica = (K1 \times \frac{10^7}{ancho\ de\ banda} + K3 \times \frac{retraso}{10}) \times 256 \ldots\ldots\ldots\ldots \textit{(Ec. 1)}$$

Mediante el uso de los valores predeterminados para K1 y K3, el cálculo puede simplificarse al ancho de banda más lento (o ancho de banda mínimo), más la suma de todos los retrasos.

$$Metrica = (\frac{10^7}{ancho\ de\ banda} + \frac{retraso}{10}) \times 256 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \textit{(Ec. 2)}$$

2.10.5. El Algoritmo De Actualización Por Difusión (DUAL)

El algoritmo de actualización por difusión (DUAL), que es el motor de cómputo detrás del EIGRP, constituye el centro del protocolo de routing. DUAL garantiza rutas de respaldo y sin bucles en todo el dominio de routing. Al usar DUAL, EIGRP almacena todas las rutas

de respaldo disponibles a los destinos, de manera que se puede adaptar rápidamente a rutas alternativas si es necesario. EIGRP utiliza el algoritmo d**e** actualización por difusión (DUAL) para proporcionar la mejor ruta sin bucles y las mejores rutas de respaldo sin bucles.

En el contexto de DUAL se utilizan varios términos:

- Sucesor
- Distancia factible (FD)
- Sucesor factible (FS)
- Distancia publicada (AD, Advertised Distance) o Distancia notificada (RD, Reported Distance):
- Condición factible o Condición de factibilidad (FC)

Estos términos y conceptos son esenciales en el mecanismo de prevención de bucles de DUAL.

2.10.5.1. Sucesor y distancia factible

Un sucesor es un router vecino que se utiliza para el reenvío de paquetes y es la ruta menos costosa hacia la red de destino. La dirección IP del sucesor se muestra en una entrada de tabla de enrutamiento justo después de la palabra vía. FD es la métrica más baja calculada para llegar a la red de destino.

2.10.5.2. Sucesores factibles, condición de factibilidad y distancia notificada

DUAL puede converger rápidamente después de un cambio en la topología, debido a que puede usar rutas de respaldo a otras redes sin recalcular DUAL. Estas rutas de respaldo se conocen como “sucesores factibles” (FS).

La FC se cumple cuando la distancia notificada (RD) desde un vecino hasta una red es menor que la distancia factible desde el router local hasta la misma red de destino. Si la distancia notificada es menor, representa una ruta sin bucles. La distancia notificada es simplemente una distancia factible desde el vecino EIGRP hasta la misma red de destino. La distancia notificada es la métrica que un router informa a un vecino acerca de su propio costo hacia esa red. (Cisco Networking Academy. 2014. P. 586-602)

2.11. CÓDEC´S

2.11.1. Codec PCMA

También denominado G.711 A-law, Estándar internacional para codificar audio de teléfono en un canal de 64 kb/s. Con G.711, la voz codificada ya está en el formato correcto para la entrega de voz digital en la red telefónica pública conmutada (PSTN). Es ampliamente utilizado en el campo de las telecomunicaciones porque mejora la relación señal-ruido sin aumentar la cantidad de datos. A-law: Se utiliza en Europa y en otras partes del mundo. Utilizan el lenguaje comprimido transportado en muestras de 8 bits. Utilizan una frecuencia de muestreo de 8 kHz con 64 kb/s de almacenamiento.

G.711 es aproximado a un cuantificador óptimo, busca una escala cuantificadora que produzca una SNR independiente del nivel de la señal. Se puede demostrar que esto requiere una escala logarítmica: el tamaño del paso del cuantificador se duplica cada vez que se duplica el nivel de entrada. Este proceso se denomina **compresión** (**compresión** y *expansión*): en comparación con la señal PAM, la representación PCM digital de la señal es 'comprimida' por la escala logarítmica, y es necesario expandir cada muestra PCM para obtener la señal PAM (Con ruido de cuantización).

Los expertos en telefonía de la UIT también observaron que la precisión de 12 a 13 bits de los cuantificadores lineales sólo era útil para señales muy débiles y tal precisión no era necesaria a niveles más altos. Por lo tanto, un tamaño de paso equivalente al tamaño de paso de un cuantificador lineal de 12 bits sólo se necesitaría al comienzo de la escala logarítmica.

El codificador de voz logarítmico G.711 de la UIT utiliza el concepto de compresión, con una escala de cuantificación para señales débiles equivalente a una escala lineal de 12 bits. Se definieron dos escalas, la A-law y la μ-law (utilizada en Norteamérica y Japón). Las dos leyes se basan en la misma aproximación de una curva logarítmica: utilizando segmentos con una pendiente que aumenta en un factor de **2**, pero la longitud exacta de los segmentos y las pendientes se diferencian entre la A-law y μ-law. La ley A proporciona un rango dinámico mayor que el μ -law, pero el μ -law proporciona un SNR ligeramente mejor que el A-law para los niveles bajos.

G.711 procesa una señal digital, lineal y cuantificada (generalmente, los convertidores A/D son lineales) en 12 bits (signo+amplitud, con frecuencia las salidas A/D son complementos de 2 que requieren ser convertidos al formato signo+amplitud). A partir de cada muestra de 12 bits, el convertidor G.711 emitirá un código de 8 bits representado en la Figura 19:

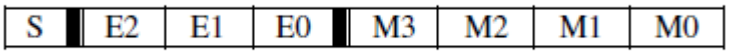


Figura 20: El código G.711 de 8 bits.

Fuente: Hersent, O., Petit, J., & Gurle, D. (2009). Beyond VoIP protocols

En la figura 20, S es el bit de signo, E2 E1 E0 es el valor del exponente, y M3 M2 M1 M0 es el valor de la mantisa. El procedimiento de codificación digital de la ley A de G.711 se representa en la Tabla 7. Los valores X, Y, Z, T vienen del código y se transmiten directamente como M3, M2, M1, M0 (la mantisa). Obsérvese que el área discontinua corresponde al ruido de cuantificación que es claramente proporcional al nivel de entrada (SNR ratio constante).

Numero de segmento (bit de signo omitido)			Amplitud codificada con 11 bits (bit de signo omitido)										
			B10	**B9**	**B8**	**B7b**	**B6**	**B5**	**B4**	**B3**	**B2**	**B1**	**B0**
0	0	0	0	0	0	0	0	0	0	**X**	**Y**	**Z**	**T**
0	0	1	0	0	0	0	0	0	1	**X**	**Y**	**Z**	**T**
0	1	0	0	0	0	0	0	1	**X**	**Y**	**Z**	**T**	N
0	1	1	0	0	0	0	1	**X**	**Y**	**Z**	**T**	N	N
1	0	0	0	0	0	1	**X**	**Y**	**Z**	**T**	N	N	N
1	0	1	0	0	1	**X**	**Y**	**Z**	**T**	N	N	N	N
1	1	0	0	1	**X**	**Y**	**Z**	**T**	N	N	N	N	N
1	1	1	1	**X**	**Y**	**Z**	**T**	N	N	N	N	N	N

Tabla 7: Amplitud de codificación en G.711

Fuente: Hersent, O., Petit, J., & Gurle, D. (2009). Beyond VoIP protocols

La figura 21 representa la característica de la ley A de siete segmentos (tenga en cuenta que, aunque tenemos ocho segmentos que se aproximan a la curva de registro, los segmentos 0 y 1 usan la misma pendiente).

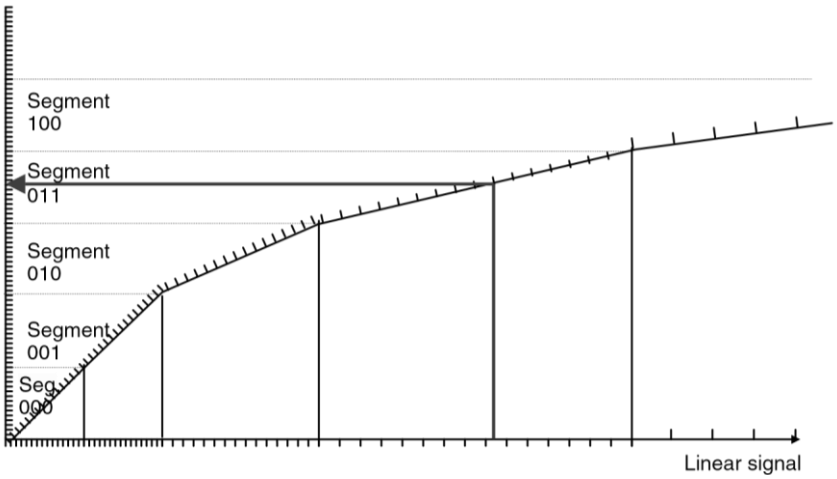


Figura 21: Aproximación logarítmica usada por G.711 A-law.

Fuente: Hersent, O., Petit, J., & Gurle, D. (2009). Beyond VoIP protocols

En el lado de recepción, el código de ley A de 8 bits se expande en 13 bits (signo + amplitud), representando el valor de cuantificación lineal. Con el fin de minimizar el ruido de cuantificación descodificado, un bit extra se establece en '1' para los dos primeros segmentos (ver Tabla 8)

Exponente	bit de signo	Amplitud decodificada utilizando $\frac{1}{2}$ Pasos de cuantificación (12 bits)											
		B10	**B9**	**B8**	**B7**	**B6**	**B5**	**B4**	**B3**	**B2**	**B1**	**B0**	**B-1**
0	**S**	0	0	0	0	0	0	0	**M3**	**M2**	**M1**	**M0**	1
1	**S**	0	0	0	0	0	0	1	**M3**	**M2**	**M1**	**M0**	1
2	**S**	0	0	0	0	0	1	**M3**	**M2**	**M1**	**M0**	1	0
3	**S**	0	0	0	0	1	**M3**	**M2**	**M1**	**M0**	1	0	0
4	**S**	0	0	0	1	**M3**	**M2**	**M1**	**M0**	1	0	0	0
5	**S**	0	0	1	**M3**	**M2**	**M1**	**M0**	1	0	0	0	0
6	**S**	0	1	**M3**	**M2**	**M1**	**M0**	1	0	0	0	0	0
7	**S**	1	**M3**	**M2**	**M1**	**M0**	1	0	0	0	0	0	0

Tabla 8: Tabla de decodificación para códigos de 8 bits G.711

Fuente: Hersent, O., Petit, J., & Gurle, D. (2009). Beyond VoIP protocols

Evidentemente, la ganancia de usar G.711 no es de calidad, sino en la tasa de bits resultante: G.711 codifica una señal cuantificada linealmente de 12 bits en 8 bits. Si la frecuencia de muestreo es 8 kHz (el estándar para las redes de telecomunicaciones), la tasa de bits resultante es de 64 kbit/s.

El único inconveniente de G.711 es reducir la SNR para las señales de entrada de alta potencia en comparación con la cuantificación lineal. Sin embargo, la experiencia muestra que la calidad global percibida (y subjetiva) no se ve afectada dramáticamente por la reducción de la SNR a niveles altos (los oyentes perciben algún ruido independiente de la señal).

De hecho, la mayor parte de la información se pierde durante el muestreo inicial y la cuantificación lineal de 12 bits. Si los oyentes comparan una muestra de calidad de CD grabada a una frecuencia de muestreo de 44,1 kHz a 16 bits, la pérdida crítica de calidad percibida se produce después del submuestreo a 8 kHz en 16 bits: hay una pérdida neta de claridad e introducción de sonoridad extra, especialmente para la voz femenina. La reducción de la cuantización de 16 a 12 bits también introduce un gran ruido granular. La compresión logarítmica final es relativamente poco importante en esta cadena de 'degradación'.

Más allá de las degradaciones mencionadas anteriormente, la señal de audio es filtrada con paso bajo (la banda convencional transmitida es de 300 Hz a 3.400 Hz en Europa y 200 Hz a 3.200 Hz en Estados Unidos y Japón). Esta limitación de bandas para las bajas frecuencias de la señal de voz desecha algunas componentes espectrales esenciales del habla. Va más allá de los requerimientos de Nyquist y se estableció inicialmente para la compatibilidad con esquemas de modulación analógica para enlaces multiplex de teléfono; También tiene en cuenta la respuesta de frecuencia no ideal de los filtros reales.

El proceso de codificación G.711 se puede construir muy fácilmente desde circuitos integrados (codificadores prioritarios, etc.). La codificación y decodificación G.711 requiere una potencia de procesamiento muy baja (cientos de canales pueden ser decodificados en tiempo real en una PC simple). En los primeros días de las telecomunicaciones digitales, esto era obligatorio. *:* (Hersent, O., Petit, J., & Gurle, D. 2009. p. 600-628)

2.11.2. Codec GSM

Utiliza un tamaño de fotograma de 20 ms y una tasa de bits de 13 kb/s. Se trata de un codificador de la excitación de pulso regular con predicción a largo plazo (RPE-LTP). Es necesario para el lenguaje de marcado extensible de voz (VoiceXML) que pueden funcionar como interfaz de usuario para un simple sistema de correo de voz. Este códec admite la infraestructura y los

componentes de aplicaciones de Cisco necesarios para que los proveedores de servicios desplieguen aplicaciones de mensajería unificada.

El codificador de voz ABS más utilizado es el códec GSM full-rate, estandarizado por el ETSI en 1988 para el sistema móvil digital celular.Este esquema de codificación fue propuesto por PKI, IBM France y France Telecom. Utiliza la excitación de pulso regular (RPE) con predicción a largo plazo (LTP), o RPE-LTP , a una velocidad de transferencia de 13 kbit/s. El codificador GSM alimenta el filtro ABS inverso con una señal de excitación optimizada para minimizar la señal de error. GSM utiliza una serie de pulsos regulares, casos especiales de "multi-pulso". La elección de RPE para ' codificar ' la señal residual permite una implementación de menor complejidad comparada con la optimización general de múltiples pulsos.

En el codificador de velocidad completa GSM, la señal es primero tamponada en un marco de 20 ms (160 muestras), entonces el análisis LPC (Codificación predictiva lineal; Coeficiente de predicción lineal) clásico encuentra los ocho coeficientes que modelan el tracto vocal. Estos coeficientes (también llamados paradores para la relación parcial) se codifican y se transmiten en el flujo de bits. El buffer de entrada entero es filtrado inversamente por el filtro LPC inverso, dando como resultado 160 muestras residuales (LPC).

Estas 160 muestras residuales se subdividen en cuatro subtramas de 40 muestras. En cada subtrama, el algoritmo busca la ganancia y el retardo óptimo del filtro LTP. El uso de subtramas refleja el hecho de que el tono (que está entre 75 Hz y 400 Hz dependiendo de la edad y el género del hablante) varía más rápidamente que las características del tracto vocal. El retardo y la ganancia de LTP se codifican y transmiten para cada subtrama.

La contribución LTP es entonces restada de la señal residual para cada subtrama de 40 muestras. Esta señal de diferencia se codifica a continuación utilizando el procedimiento RPE, que divide las 40 muestras originales de la señal de diferencia en cuatro subseries de muestras:

- El primero comienza con el valor del índice de muestra 0, luego elige un valor de muestra de 4, desde el índice 3 hasta el índice 36.
- El segundo comienza con el índice 1, luego escoge un valor de la muestra de 4, desde el índice 4 hasta el 37.
- El tercero comienza con el índice 2, luego selecciona un valor de la muestra de 4, del índice 5 al 38.
- El último comienza con el índice 3, luego elige un valor de muestra de 4, desde el índice 6 hasta el último índice del subtrama.

De las cuatro series, se selecciona la que mejor se adapta a las 40 muestras residuales originales; Se requieren dos bits por subtrama para indicar la elección al receptor. La máxima energía de las muestras en las subsecuencias seleccionadas también se codifica, utilizando 6 bits. Todas las muestras de la subsecuencia se normalizan mediante esta energía cuantificada, luego se cuantifican escalares con 3 bits. Cada serie consiste en un proceso subampleado que es un filtro de paso bajo duro con una frecuencia de corte alrededor de 1.300 Hz. Esto privilegia la voz masculina sobre las voces femeninas o infantiles.

Aunque el RPE-LTP produce una calidad de voz ligeramente inferior a la telefonía estándar, es muy adecuado para sistemas de comunicaciones móviles porque resiste bastante bien los errores de transmisión.

RPE-LTP frame length = 160 samples = 20 ms	
Vocal tract: LPC coefficients; 8 parcors = 36 bits	36
Subframe length = 40 samples = 5 ms (4 subframes)	
Grid selection = 2 bits	8
Maximum of energy of selected series = 6 bits	24
Scalar quantization of 13 samples = 13 * 3 = 39 bits	156
LTP lag = 7 bits	28
LTP gain = 2 bits	8
Total	260
Bit rate = 260/20 ms = 13 kbit/s	

Tabla 9: Asignación de bits GSM a plena velocidad

Fuente: Hersent, O., Petit, J., & Gurle, D. (2009). Beyond VoIP protocols

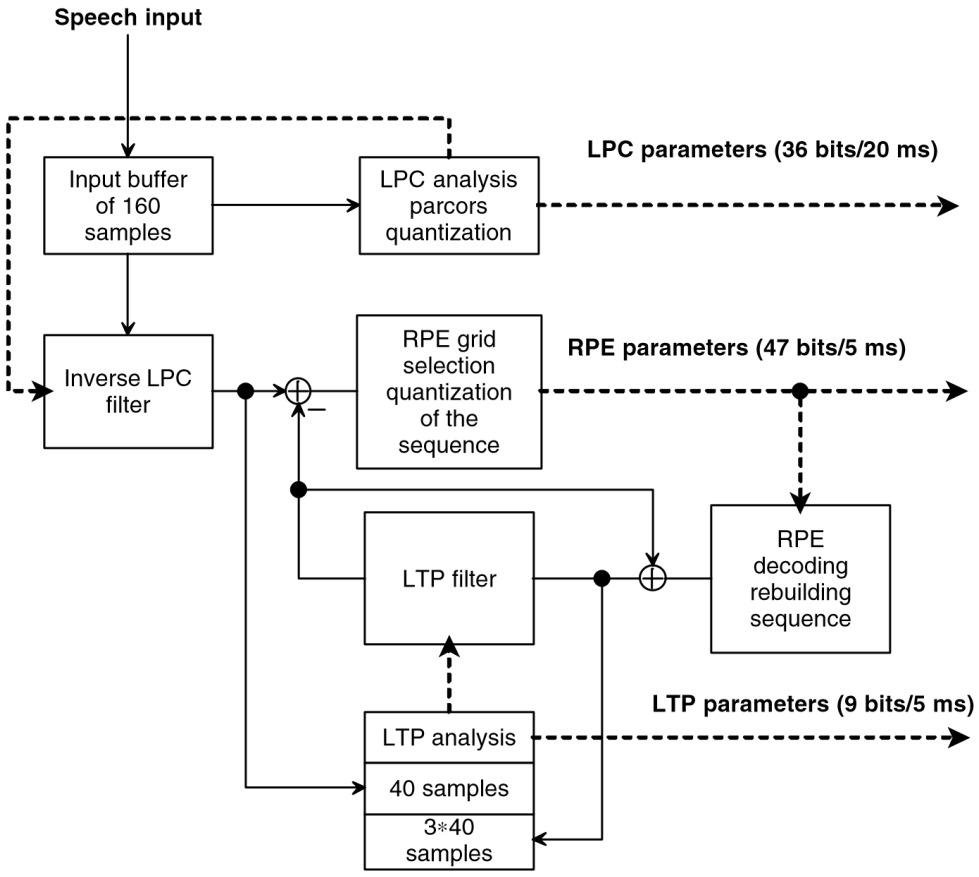


Figura 22: Principio básico del codificador de voz GSM de tarifa completa RPE-LTP (13 kbit / s).

Fuente: Hersent, O., Petit, J., & Gurle, D. (2009). Beyond VoIP protocols

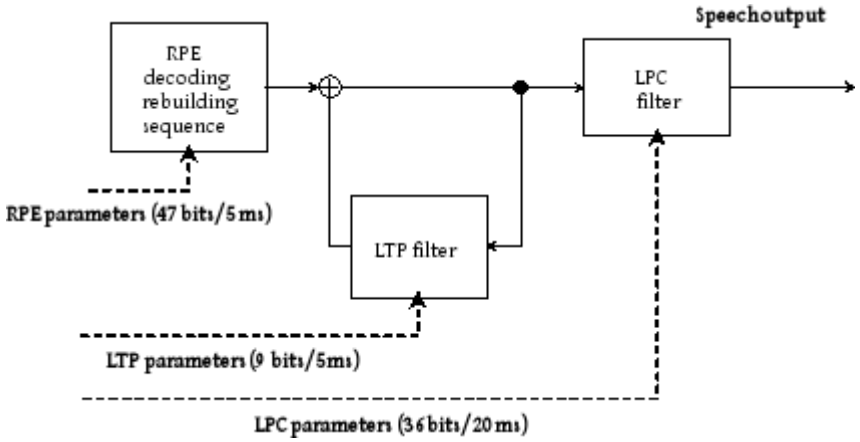


Figura 23: Principio básico del decodificador de voz GSM RPE-LTP de plena velocidad (13 kbit / s).

Fuente: Hersent, O., Petit, J., & Gurle, D. (2009). Beyond VoIP protocols

La recomendación ETSI 06-10 GSM RPE-LTP incluye una descripción detallada de aritmética de punto fijo basada en el uso de "operadores básicos". También se proporcionan secuencias de prueba digitales para verificar la conformidad con la norma. Aunque algunas versiones flotantes de este estándar existen y se utilizan en el software de VoIP, algunos problemas sutiles pueden aumentar la interoperabilidad con la versión de punto fijo genuina.

Además de la codificación de voz básica, se añadió al codificador un esquema VAD (detección de actividad de voz), DTX (transmisión discontinua) y CNG (generación de ruido de confort) VAD detecta si está presente un discurso vocal y de otro modo transmite (menos frecuentemente) parámetros que contienen la información de ruido. En el caso de GSM, estos parámetros se basan en los parámetros LPC y en la energía del ruido. Se envasan en un marco SID (descripción de silencio) que se envía cada 80 ms (cuatro cuadros comparados con la trama del habla de 20 ms). Debe señalarse que el diseño de un algoritmo VAD bueno y eficiente es casi tan complejo como el diseño de un buen codificador de voz.

El codificador GSM 6.10 refleja las limitaciones de la potencia de procesamiento comúnmente disponible en 1988; Está siendo reemplazado progresivamente por GSM 6.60. El codificador GSM 6,60 se basa en la tecnología ACELP propuesta por Nokia y la Universidad de Sherbrooke. Sólo utiliza 12,2 kbit/s (menos de los 13 kbit/s de GSM 6.10, dejando cierta capacidad de protección contra errores). Cuando no hay errores en el canal de transmisión, la calidad de voz es equivalente a G.726 a 32 kbit/s (calidad de peaje). (Hersent, O., Petit, J., & Gurle, D. 2009. p. 425-450)

2.11.3. Codec G722

Códec de voz estándar ITU ADPCM que proporciona 7 kHz de audio de ancho de banda a velocidades de datos de 48 a 64 kb/s. De dos variantes, G.722.1 y G.722.2, G.722.2 ofrece una mejor compresión, así como la capacidad de adaptarse rápidamente a las condiciones cambiantes de la red. El ancho de banda se conserva automáticamente cuando la congestión de la red es alta. Cuando la congestión vuelve a un nivel normal, se restaura una tasa de bits de baja calidad y de menor compresión.

En el mundo de la telefonía, G.711 se utiliza frecuentemente como "la referencia" de la calidad de la voz, ignorando el hecho de que G.711 codifica solamente la banda de 300-3.400 Hz. Y calidad de audio para sistemas de videoconferencia y audioconferencia Mientras que la mayoría de los codificadores se centran en proporcionar una calidad de voz aceptable para la tasa de bits

más baja posible, también es posible aumentar la calidad de audio tanto como sea posible para una velocidad de bits determinada.

Los científicos y los ingenieros eran bien conscientes de las posibilidades de forma de onda ADPCM (Modulación de códigos de impulsos diferenciales adaptativos) codificadores de voz para reducir la tasa de bits en un factor de alrededor de 0,5 y, naturalmente, trató de utilizar una técnica similar para codificar la banda ancha del habla. El ancho de banda se refiere a una banda de frecuencia transmitida de 50 Hz a 7.000 Hz en comparación con el ancho de banda de telefonía tradicional (300 Hz a 3.400 Hz).

G.722 fue propuesta por France Telecom y NTT, y adoptada por la UIT en 1988. La idea fundamental es dividir la banda a transmitir en dos subbandas: una subbanda inferior que abarca desde 0 Hz hasta 4000 Hz y una subbanda superior que abarca desde 4.000 Hz hasta 8.000 Hz. Luego, después de un procedimiento de submuestreo que reduce la frecuencia de muestreo desde el original de 16 kHz hasta 8 kHz, se pueden aplicar dos codificadores ADPCM clásicos para reducir la tasa de bits. El submuestreo es posible porque el filtrado de frecuencia de subbanda ha eliminado el efecto de aliasing.

La separación de subbanda utiliza un par de filtros de espejos cuadráticos. Los filtros QMF son los precursores de la teoría de bancos de filtros utilizados para los codificadores psicoacústicos. De muchas maneras, el codificador de voz y audio de banda ancha UIT-T G.722 es un precursor de los codificadores de audio psicoacústico más recientes: la división de la banda original en dos subbandas y la asignación de más bits en la sub-banda inferior optimiza la eficiencia de la predicción de que la banda de frecuencia más sensible realiza el enmascaramiento de cuantificación de ruido. La energía del habla se concentra más en la sub-banda inferior, y asignar más bits en esta sub-banda aumenta la calidad de la voz decodificada.

G.722 codifica una señal de banda ancha en un flujo de bits de 64 kbit/s (la velocidad de bits PCM básica). En la subbanda inferior, se utilizan 6 bits para el cuantificador adaptativo con una característica incorporada: el cuantificador de núcleo utiliza 4 bits y la versión mejorada utiliza 6 bits. Esto permite al sistema robar algunos bits para propósitos de señalización y para transmitir algunos datos auxiliares. El decodificador debe ser señalado como el modo de operación (64, 56, o 48 kbit / s), aunque algunas realizaciones no señalan el modo y utilizan permanentemente los 6 bits completos. En la sub-banda superior, se utiliza un cuantificador adaptativo de 2 bits (no incorporado) que produce una tasa de bits de 16 kbit/s (muy inferior a los 48 kbit/s utilizados para la subbanda inferior que es perceptualmente más importante).

El esquema de codificación de G.722 se ilustra en la figura 23, y el principio de decodificación de G.722 se muestra en la figura 24.

El codificador de voz de banda ancha ITU-T G.722 se utiliza comúnmente en sistemas de teleconferencia que se adhieren a la recomendación H.320.La calidad es bastante buena para el habla y la música a 64 kbit/s y 56 kbit/s. Como no existe un modelo de producción específico (por ejemplo, para el habla) en ese codificador de forma de onda, las muestras de música están codificadas correctamente. Cuando se utiliza a 48 kbit/s, el habla reproducida se vuelve más ruidosa (debido al cuantificador de 4 bits en la subbanda inferior).

G.722 comparte con otros tipos de codificadores ADPCM de forma de onda una mínima relativa a errores de bits y es más robusto que un flujo directo de PCM. La característica de baja demora del G722 es también una ventaja importante en comparación con los esquemas de codificación de audio basados en cuadros más recientes.

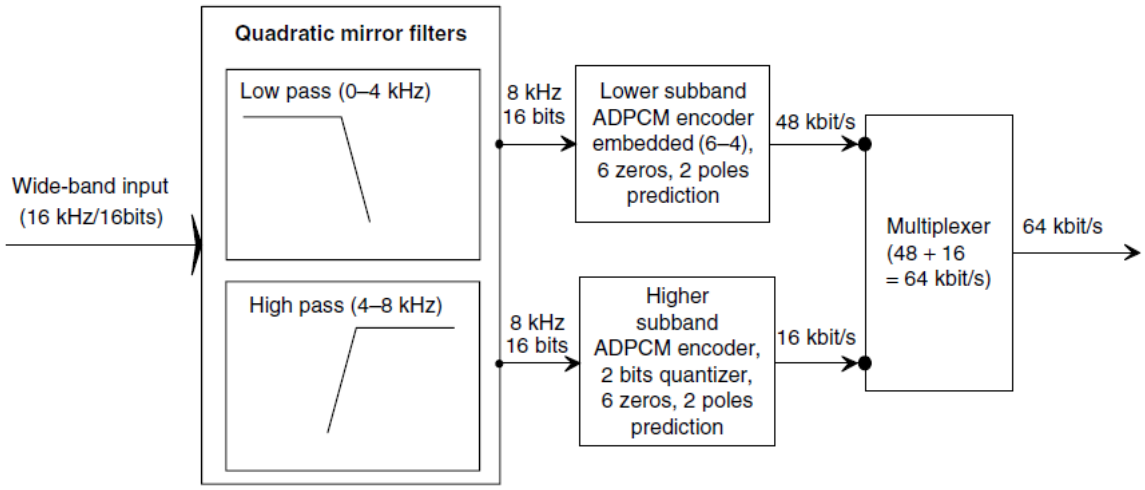


Figura 24: Codificador G.722

Fuente: Hersent, O., Petit, J., & Gurle, D. (2009). Beyond VoIP protocols

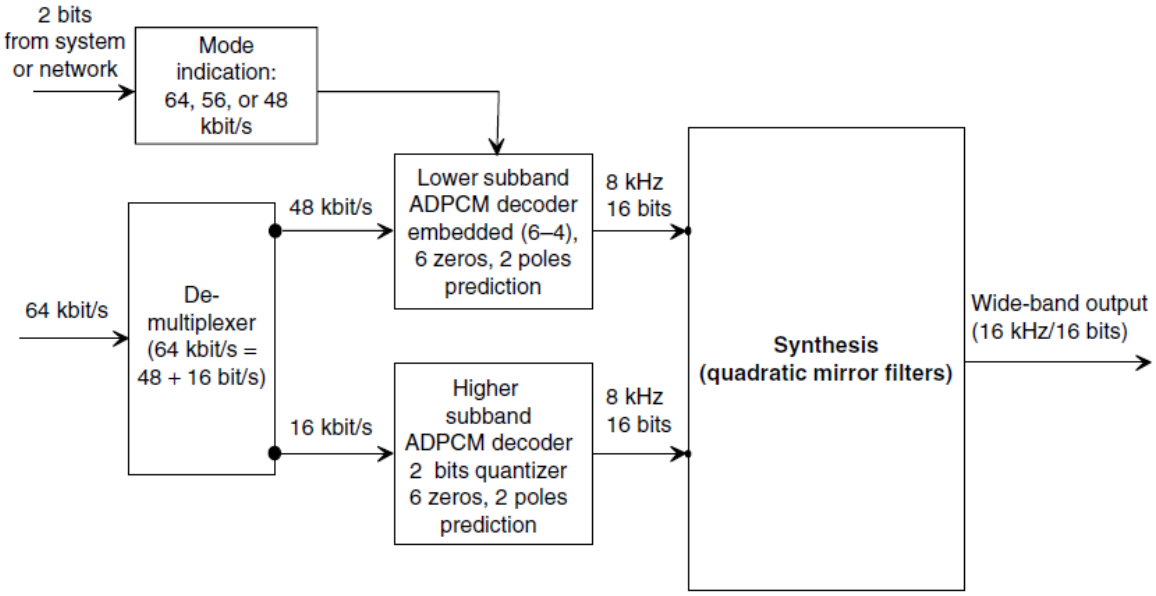


Figura 25: Descodificador G.722

Fuente: Hersent, O., Petit, J., & Gurle, D. (2009). Beyond VoIP protocols

Todos los codificadores de forma de onda, tales como ADPCM y PCM, tienen un retardo algorítmico muy bajo que varía de tres a cuatro muestras (300-500 µs con una frecuencia de muestreo de 8 kHz). En el caso de G.722, los filtros de análisis y síntesis de QMF añaden un retardo de aproximadamente 3 ms. El retardo total resultante sigue siendo excelente y garantiza una buena interactividad para los sistemas de teleconferencia. G.722 es uno de los codificadores recomendados para su uso en sistemas H.323 y está disponible en varias implementaciones comerciales. (Hersent, O., Petit, J., & Gurle, D. 2009. p. 759-768)

2.12. HIPOTESIS

2.12.1. Hipótesis general

El análisis del tiempo de recuperación en un enlace redundante en una red con enrutamiento EIGRP y con el servicio de telefonía IP permite conocer el códec adecuado entre PCMA, GSM y G722, esto ayudará en la comunicación de telefonía IP en empresas y/o entidades públicas.

2.12.2. Hipótesis específicas

a) El enrutamiento EIGRP es una parte importante para la comunicación entre redes de telefonía IP.
b) El servicio de telefonía IP es óptimo con el codec seleccionado en momentos especiales para cada uno de ellos.

2.12.3. Antecedentes

En el artículo realizado por A. S. W. Marzuki, Y. K. Chai, H. Zen, L. L. Wee, K. Lias y D. A. Awg Mat con el título "Performances analysis of VoIP over 802.11b and 802.11e using different CODECs," analizan el rendimiento y la tasa de abandono de paquetes en redes de 8002.11b y 802.11e (ambos denominados comercialmente WiFi). La simulación se llevó a cabo utilizando diferentes codecs tales como G.711, G.729A y G.723.1 y sin tráfico de fondo (datos). Concluyendo que el codec G.711 ofrece la mejor calidad de las llamadas VoIP. Sin embargo, G.723.1 puede soportar la mayoría de las llamadas de VoIP con una calidad aceptable. Además, con la primera prioridad dada por 802.11e a la VoIP, puede proporcionar una muy buena calidad de audio percibida.

Por otra parte en el estudio titulado “Comparative study and analysis of VoIP traffic over WiMAX using different service clases” redactada por T. Anouari y A. Haqiq investigan las actuaciones de los codecs de VoIP más comunes, nombradas como G.711, G.723.1 y G.729 utilizando Best Effort, UGS, RTP, rtPS, nrtPS y ertPS y protocolo de enrutamiento NOAH. Se utiliza el simulador NS-2 para analizar los parámetros de QoS. El objetivo es comparar diferentes clases de servicio en redes WiMAX con respecto a los parámetros de QoS, tales como, la fluctuación promedio, el rendimiento y la demora media.

En este antecedente se utiliza el simulador OPNET para evaluaciones de calidad de servicio en una implementación de VoIP, mientras la observación de los efectos de las variaciones en los códecs de voz y longitudes de los paquetes. Consideran tres códecs de voz principal G.711, G.729 y G.723.1 y tres cargos de imágenes por los valores de paquetes (10, 25 y 50 tramas por paquete de voz) en relación con cada códec. Los resultados de la simulación muestran que la cola de codificación de voz G.723.1 experiencias más alta retrasos y variaciones de retardo de cola para un mayor número de tramas por paquete. Sin embargo, el retardo de menos de paquetes de extremo a extremo se observa en los paquetes de voz codificados con el códec G.729 para todos los valores configurados de tramas por paquete. Esta investigación de título "QoS analysis of VoIP traffic for different codecs and frame counts per packet in multimedia environment using OPNET" es realizada por M. Aamir y S. M. A. Zaidi.

En la investigación "End-to end delay performance analysis of various codecs on VoIP Quality of Service" de S. Sahabudin y M. Y. Alias utilizan los codecs G.711, G.729A, G.723.1 y G.726 analizan el rendimiento de extremo a extremo. A partir de las simulaciones se obtuvieron los resultados para cada uno de los usuarios. Desde los resultados de la simulación se puede ver que para la mayoría de los lugares, G.711 sin utilizar supresión de silencio tiene el retraso

promedio más alto de extremo a extremo. Por otro lado, G.723.1 con la supresión de silencio tiene el promedio más bajo de extremo a extremo.

Por último, el artículo de M. Alshamrani, H. Cruickshank, Z. Sun, B. Elmasri y V. Fami titulado "Evaluation of SIP Signalling and QoS for VoIP over OLSR MANET Routing Protocol" Este documento evalúa las aplicaciones de VoIP basado en SIP a través del protocolo de enrutamiento OLSR, como un protocolo de enrutamiento dinámico para MANET. Los codecs a considerados a evaluar son PCM, LQS, IPTelephony, y GSM para estudiar el comportamiento. Concluyendo que las llamadas VoIP basadas GSM y LQS tienen un nivel aceptable de calidad de servicio, mientras PCM y IPTelephony tienen un bajo nivel de calidad de servicio a través de diferentes tipos de modelos de movilidad. Por otra parte, la ubicación y la movilidad de servidor SIP afectan el número de saltos y el rendimiento de señalización SIP entre las diferentes partes de la llamada de VoIP.

2.13. OBJETIVOS

2.13.1. Objetivos generales

Analizar el tiempo de recuperación hacia un enlace redundante en una red con enrutamiento EIGRP y servicio de telefonía IP.

2.13.2. Objetivos específicos

a) Implementar una red con un enlace redundante con enrutamiento EIGRP y servicio de telefonía IP
b) Analizar el comportamiento de la red con el códec PCMA, códec GSM y códec G.722.

CAPITULO III

MATERIALES Y MÉTODOS

3.1 MATERIALES

3.1.1. Hardware

Softphone A (laptop)

Modelo: ACER 5750

Procesador: Intel(R) Core(TM) i5-2430 2.40GHz

Memoria instalada (RAM): 4.00GB de RAM.

Tipo de sistema: Sistema Operativo de 64 bits Windows 10

Softphone B (laptop)

Modelo: Lenovo Z40-70

Procesador: Intel(R) Core(TM) i5-4200U 2.60GHz

Memoria instalada (RAM):3.00GB

Tipo de sistema: Sistema Operativo de 64 bits Windows 10

Servidores (computadoras)

Procesador: intel(R) Core(TM)2 Duo E8500 3.16GHz

Memoria instalada (RAM): 4.00GB

Tipo de sistema: sistema operativo de 64bits Elastix-2.5.0-STABLE

Routers: Cisco 2901

Cisco IOS Software: 2901 Software Version 15.4(3)M2.

ROM: ystem Bootstrap, Version 15.0(1r)M12

CISCO2901/K9 (revision 1.0) with 483328K/40960K bytes of memory.

Processor board ID FTX154983NW

2 Gigabit Ethernet interfaces

2 Serial(sync/async) interfaces

1 terminal line

1 Virtual Private Network (VPN) Module

DRAM configuration is 64 bits wide with parity enabled.

255K bytes of non-volatile configuration memory.

255744K bytes of ATA System CompactFlash 0 (Read/Write)

3.1.2. Software

Sistema Operativo de 64 bits Windows 10.

Sistema Operativo de 64 bits Elastix-2.5.0-STABLE.

Capturador de paquetes Wireshark v2.2.1

Softphone Ekiga v4.0.1

Software de simulación Packet Tracert v7.0

Microsoft Excel Profesional Plus 2013 v15.0.4569.1506

3.2 MÉTODO

3.2.1. Tipo de estudio

Es exploratoria, porque se examina un tema o problema de investigación poco estudiado, como es el caso de la aplicación de una Red de telefonía IP

Es correlacional por que tiene como propósito medir el grado de relación entre las variables de las hipótesis planteadas; así como también es descriptiva, porque no se da la manipulación de variables, estas se observan y se describen tal como se presentan en la realidad, su metodología es fundamentalmente descriptiva, aunque puede valerse de algunos elementos cuantitativos y cualitativos.

3.2.2. Población

Debido a que la población es pequeña, ya que se realizaron diez pruebas para cada códec de telefonía IP en la red con enrutamiento EIGRP, se ha considerado todo el universo como la población.

3.2.3. Instrumento de recolección de datos

3.2.3.1. Técnicas

La técnica para la recolección de datos es mediante la observación, ya que el investigador actúa sobre los hechos con la ayuda de algún instrumento

3.2.3.2. Instrumentos

Los instrumentos son la guía de observación del campo: esto indica los pasos que adopta el investigador para una buena estrategia en la observación de datos.

3.3 UBICACIÓN DEL LUGAR DONDE SE REALIZO LA INVESTIGACÓN

la investigación se realizó en el laboratorio de CISCO – Escuela Profesional de Ingeniería Electrónica de la Universidad Nacional del Altiplano – Puno.

Figura 26: Lugar de Investigación - Escuela Profesional de Ingeniería Electrónica

Fuente: Google Maps

3.2.4. Técnicas de procesamiento y análisis

3.2.4.1. Plan de recolección de datos:

Todo el proceso de implementación de la red con EIGRP, servidores y softphones se realizó en el laboratorio de CISCO de la Escuela Profesional de Ingeniería Electrónica. Se siguieron los siguientes pasos para luego recolectar de datos:

Configuración del servidor Elastix

El primer paso es la instalación de los servidores con el sistema operativo libre Elastix la versión 2.5.0 que es considerado por los desarrolladores como una versión estable al terminar la instalación se agrega las direcciones IP según la red, esta configuración es mostrada en la figura 26 y 27. Se puede observar que en la figura 26 el archivo ifcfg-eth0 del servidor de la red A (servidor-A) que es editado para la comunicación dentro y fuera de la red. En la figura 27 es el mismo archivo, pero en el segundo servidor de la red B (servidor-B). Para ingresar a este archivo se usó el comando: *nano /etc/sysconfig/network-scripts/ifcfg-eth0*

Figura 27: Datos de red del servidor de la red A

Elaboración: Propia

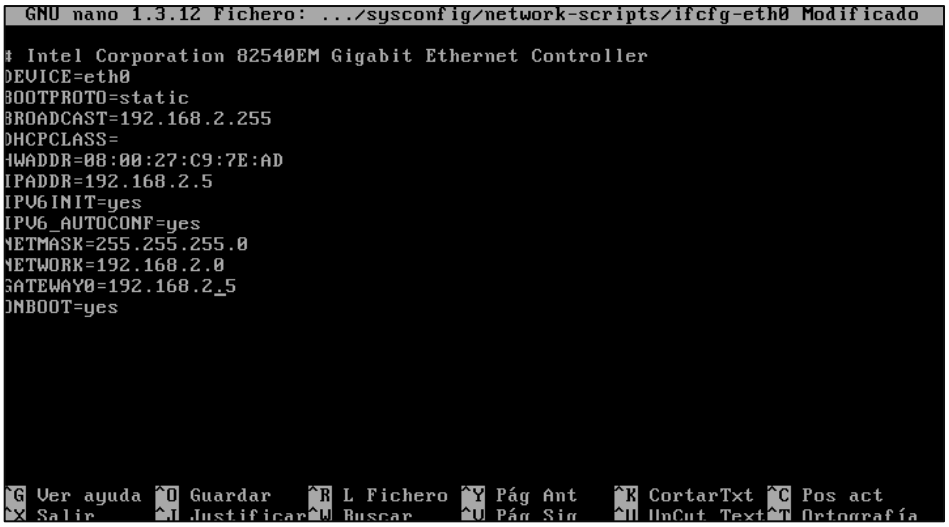


Figura 28: Datos de red del servidor de la red B

Elaboración: Propia

Al terminar la configuración de los interfaces de red de ambos servidores se pasó a crear las extensiones SIP, esto fue realizado en el interfaz gráfico que se ingresa mediante el navegador web de un ordenador con conexión de red al servidor. En la figura 28 se observa la pantalla de configuración para agregar las extensiones. Los datos agregados en los servidores se observan en la tabla 10.

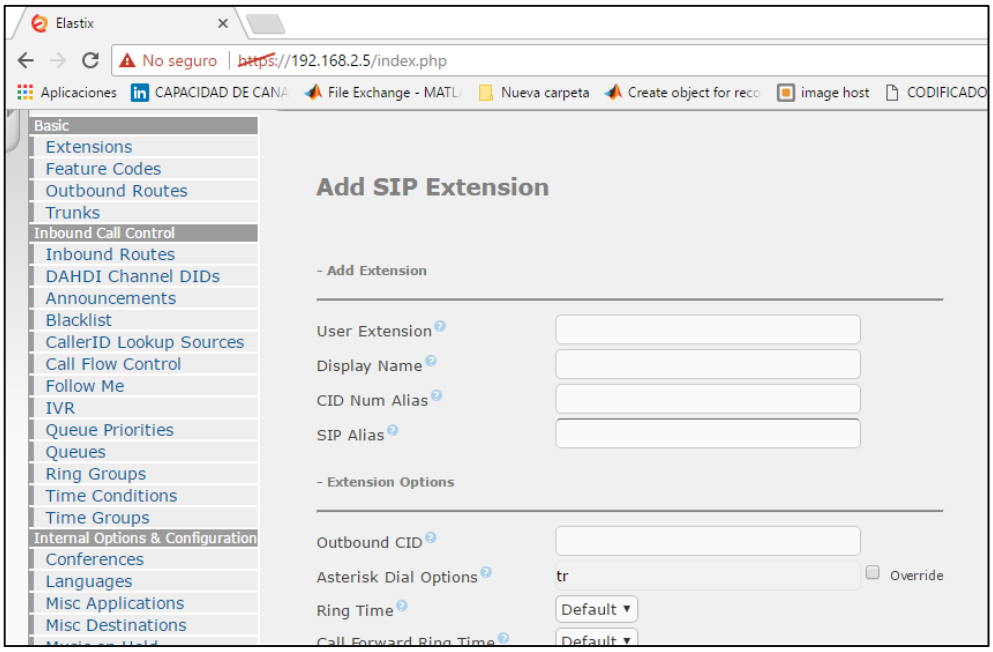


Figura 29: Pestaña para agregar las extensiones SIP

Elaboración: Propia

Nombre del servidor	**SERVIDOR-A**	**SERVIDOR-B**
Dirección IP/Mascara	**192.168.1.5/24**	**192.168.2.5/24**
User extension	101	201
Display name	SoftPhone1A	SoftPhone1B
SIP Alias	101	201
Secret	**********	**********

Tabla 10: Datos necesarios para crear las extensiones.

Elaboración: Propia

En *user extension* se especifica el número de la extensión que se debe marcar para contactar con el usuario. Luego en *display name* es el nombre que se mostrara en la pantalla de visualización de un teléfono esto para no mostrar el número. El *SIP alias* es si se desea asignar un nombre a una extensión para que otras extensiones SIP puedan marcarle de esta forma. En *secret* se crea la contraseña para que se pueda autenticar los teléfonos o softphones al momento de registrarse con esta extensión al servidor.

Luego de ingresar los datos y aplicarlos se procedió a la creación de los troncales SIP. Esta configuración descrita en la tabla 11 y se aplica en la pestaña de Trunks, la captura de pantalla se muestra en la figura 29.

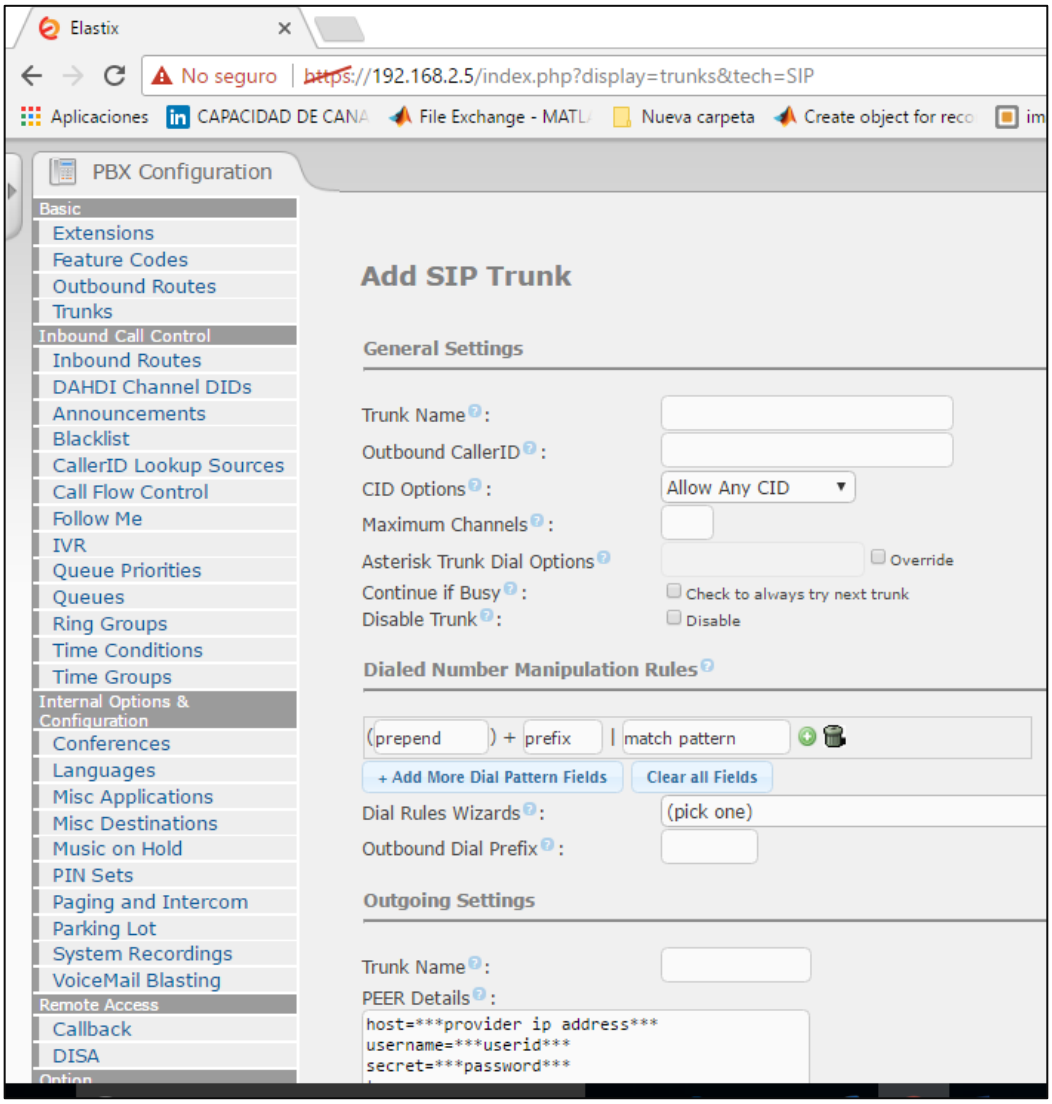


Figura 30: Pestaña para crear la troncal SIP

Elaboración: Propia

	SERVIDOR-A	SERVIDOR-B
Trunk Name	servidorA	servidorB
PEER Details	host=192.168.2.5 username=servidorB secret=123456 encryption=aes128 auth=md5 type=friend trunk=yes	host=192.168.1.5 username=servidorA secret=123456 encryption=aes128 auth=md5 type=friend trunk=yes

Tabla 11: Datos necesarios para tronkalizar

Elaboración: Propia

Una troncal es aquella que permite llevar una llamada a cualquier proveedor de servicio de voz ó a cualquier dispositivo que reciba su intento de llamada y la gestione a otro destino. En este caso el troncal está comunicando dos servidores. Las configuraciones es lo más básico, iniciando con el nombre de la troncal. Luego se da a conocer los detalles del servidor a comunicarse como la dirección IP y su nombre, para la autenticación se ingresa un secret similar en ambos, al igual que el modo de cifrado y autenticación, al final establece que la troncal será confiable y activa el troncal.

Al realizar esta parte de la configuración y también aplicarlo, el servidor necesita la creación de rutas salientes. Esta con figuración está en la tabla 12.

	SERVIDOR-A	**SERVIDOR-B**
Route Name	LocalidadA	LocalidadB
Dial Patterns (match pattern)	2XX	1XX
Trunk Sequence	servidorA	servidorB

Tabla 12: Datos necesarios para las rotas salientes

Elaboración: Propia

Mediante las rutas salientes podemos indicar porque troncal o troncales deben ser enviadas las llamadas. Al igual que las anteriores se establece el nombre de la ruta saliente luego en el patrón de marcado se establece el conjunto de dígitos o patrón de dígitos que Asterisk usa para verificar el “match” con los dígitos marcados por un emisor para determinar el canal por donde debe enviar la llamada. Al poner “X” representa cualquier número entre el 0-9 con esto indicamos todos los números de tres dígitos desde el 100 hasta el numero 199; lo mismo para el otro servidor.

Luego de realizar estos pasos se terminó la configuración en el servidor, ya se encuentran disponibles para registrar los teléfonos. Para la investigación se usa softphones instalados en los laptops esto es para capturar los paquetes de entrada y salida.

Configuración de los softphones

El softphone Ekiga es una aplicación de software libre capaz de realizar videoconferencias y telefonía IP. La elección por la aplicación Ekiga es por contener los tres códecs usados para el análisis (figura 30), también compatible con SIP. Otros aspectos por la que se eligió es la fácil configuración.

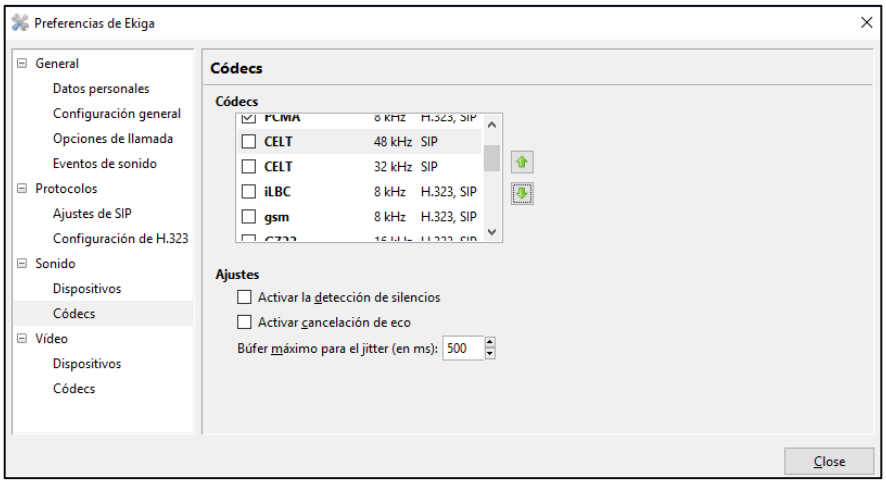


Figura 31: Pestaña de selección de códecs

Elaboración: Propia

Para la configuración solo se registró el softphone con una de las extensiones, para ello nos dirigimos a *cuentas* ubicada en la pestaña *editar*, agregamos una cuenta SIP llenando según como indica la tabla 13

Nombre	Nombre de la extensión creada en el servidor
Servidor de registro	Dirección IP del servidor donde está la extensión
Usuario	El número de *User extension* (ubicada en la tabla 1)
Usuario de autenticación	Validar el número de *User extension*
Contraseña	El *secret* asignado a la extensión (ubicada en la tabla 1)

Tabla 13: Como crear una cuenta SIP en Ekiga

Elaboración: Propia

Implementar la red con enrutamiento EIGRP

La implementación de la red fue en el laboratorio de Cisco en la Escuela Profesional de Ingeniería Electrónica.

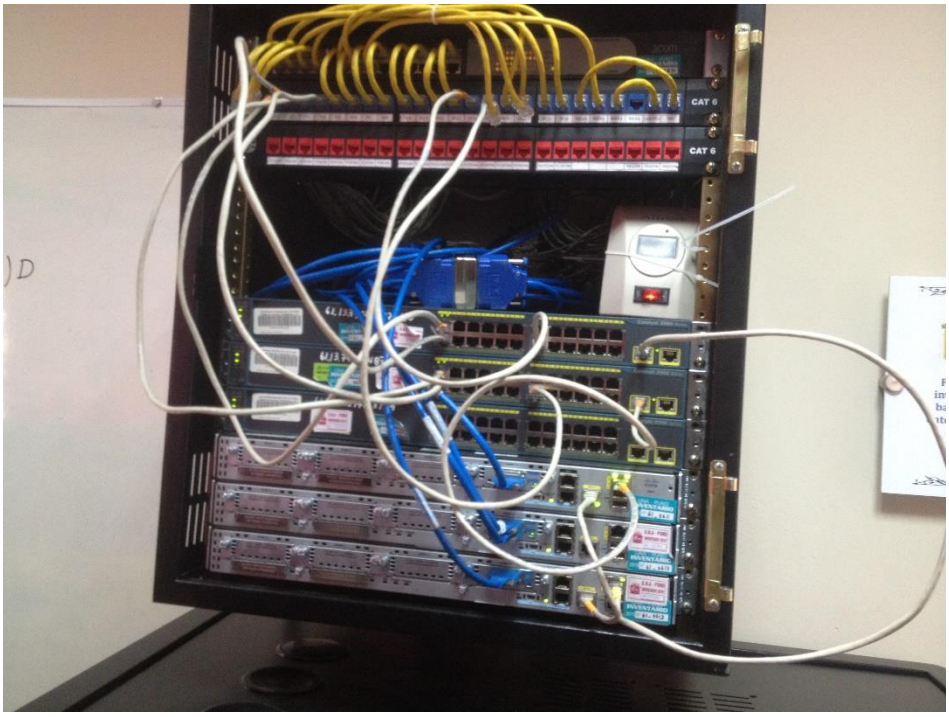


Figura 32: Conexiones físicas

Elaboración: Propia

Esta red se implementó con equipos reales de la marca Cisco, haciendo uso de tres routers y dos switches la topología se muestra en la figura 32. El propósito de usar tres routers es para efectuar el enrutamiento dinámico. Este tipo de topología es usada en varios laboratorios de Cisco en sus academias de redes (Cisco Networking Academy), junto a su enseñanza teórica para este protocolo EIGRP. Los switch aparte de conmutar son usados para crear VLANs específicas para cada red. En ambos extremos hay dos VLANs uno encargado solamente de los datos y otro especial para la telefonía IP.

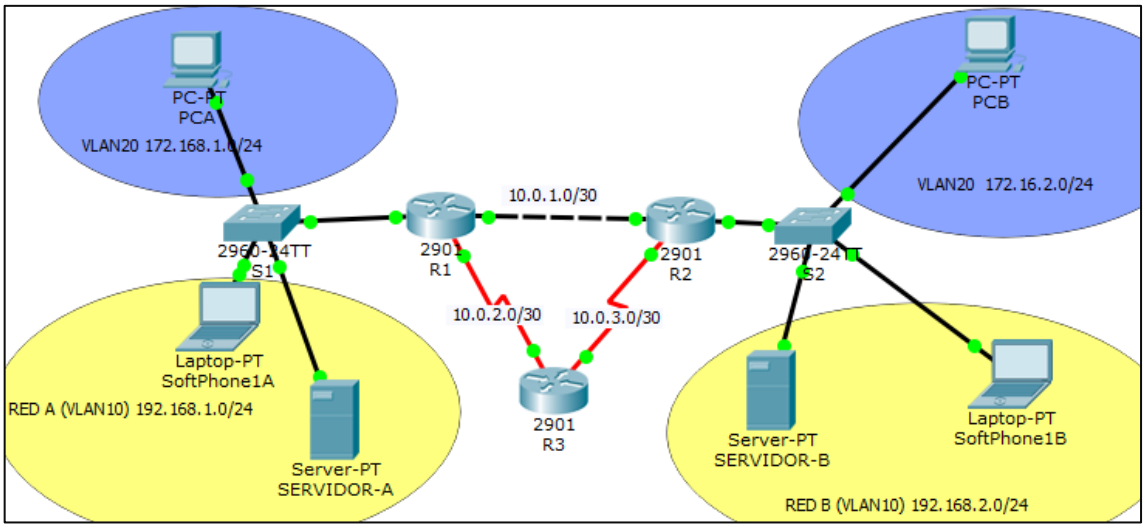


Figura 33: Topología de la red implementada:

Elaboración: Propia

Los comandos ejecutados en los routers se muestran en el ANEXO A, las direcciones usadas se resumen en la tabla 14; mientras que las configuraciones en los routers y switches se describirán a continuación. En R1 y R2 se configuraron los siguientes requisitos:

- Interface g0/0.10 (para la vlan 10)
- Interface g0/0.20 (para la vlan 20)
- Interface s0/0/0 (R2) e interface s0/0/1(R2): con un clock rate de 4000000 (bit por segundo), se tomó para que la comunicación por este enlace sea fluido.
- Habilitación de protocolo EIGRP con número de sistema autónomo 1.
- Para el R1, la identificación del router se puso 1.1.1.1 y para R2 es 2.2.2.2
- Declaración de las redes conectadas en las interfaces del router, declarando a la interface g0/0 como pasiva

En R3 fueron las siguientes:

- Interface s0/0/0.
- Interface s0/0/1.
- Habilitación de protocolo EIGRP con numero de sistema autónomo 1
- Para la identificación de R3 en tablas de EIGRP se puso es 3.3.3.3
- Declaración de las redes conectadas en las interfaces del router.

Configuraciones en el switch S1 y S2:

- Creación de la VLAN 10 con nombre TELEPHONY.
- Creación de la VLAN 20 con nombre DATE.

- Asignación de interfaces a cada VLAN: de la interface fastEthrnet 0/1 hasta fastEthrnet 0/12 se pusieron la vlan 10 y desde la interface fastEthrnet 0/13 hasta fastEthrnet 0/24 pertenecen a la vlan 20
- Troncalización en la interface de salida al router. Esto en cada switch está en la interface g0/1.

Interfaces	**Dirección IP**	**Mascara**
R1	router-id 1.1.1.1	
Interface g0/0.10	192.168.1.1	255.255.255.0
Interface g0/0.20	172.16.1.1	255.255.255.0
Interface g0/1	10.0.1.1	255.255.255.252
Interface s0/0/0	10.0.2.1	255.255.255.252
R2	router-id 2.2.2.2	
Interface g0/0.10	192.168.2.1	255.255.255.0
Interface g0/0.20	172.16.2.1	255.255.255.0
Interface g0/1	10.0.1.2	255.255.255.252
Interface s0/0/1	10.0.3.1	255.255.255.252
R3	router-id 3.3.3.3	
Interface s0/0/0	10.0.2.2	255.255.255.252
Interface s0/0/1	10.0.3.2	255.255.255.252
HOST		
PCA	172.168.1.20	255.255.255.0
PCB	172.168.2.20	255.255.255.0
SERVIDOR-A	192.168.1.5	255.255.255.0
SERVIDOR-B	192.168.2.5	255.255.255.0
SoftPhone1A	192.168.1.10	255.255.255.0
SoftPhone1B	192.168.2.10	255.255.255.0

Tabla 14: Resumen de las direcciones IP configuradas

Elaboración: Propia

3.2.4.2. Plan de procesamiento de datos:

Esto se realizó mediante el software de captura de paquetes denominado Wireshark, que se encuentra instalado en cada softphone:

- Se ignoraron los paquetes no relacionados con la investigación tales como CDP, ARP; LOOP y STP.
- Luego de eso se ingresó a la ventana de *IO Graphs* mediante la pestaña de *statistics.*
- En esta ventana se copió la tabla de paquetes y bits con un intervalo de 100ms esto para luego procesarlo en el programa Microsoft Excel.

Todos estos pasos se realizaron con todas las pruebas, generando tres tablas para cada codec en Microsoft Excel. En este software se realizará el acercamiento para facilitar la observación en el momento que el enlace primario es deshabilitado, hasta su posterior recuperación. La investigación solo se concentra en el proceso que cae la línea principal hasta su recuperación según cada códec.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

Se realizaron diez pruebas para realizar el promedio. Las diez pruebas fueron llamadas realizadas para cada códec, por ejemplo: diez llamadas seleccionando el códec GSM, de igual manera para G722 y PCMA. Las llamadas duraron una cantidad de 40 segundos aproximadamente, desde el inicio del timbrado hasta colgar en el Softphone.

Para cada prueba se realizó la desconexión del enlace principal. La desconexión se realizó de **20 segundos** de iniciado la llamada y fue manual. Se desconectó la conexión que esta entre la interface Gigabit Ethernet 0/1 del router R1 y el interface Gigabit Ethernet 0/1 del router R2 (ver figura 33)

Figura 34: Enlace principal

Elaboración: Propia

El objetivo de esta investigación es ver el tiempo en que se demora cada códec en recuperarse cuando ocurre una ruptura del enlace principal. En la revisión literaria se mostró que el inicio y fin de la llamada es gracias al protocolo SIP y luego la comunicación de voz es transportada en el protocolo RTP, esto es controlado por RTCP en caso de pérdida de paquetes. En este capítulo se analizará los protocolos utilizados para el funcionamiento de la comunicación en telefonía IP en el momento de la desconexión del enlace principal. También se analizará el

protocolo de enrutamiento EIGRP. Estos análisis serán para obtener las conclusiones para la investigación.

4.1. Análisis de EIGRP.

Comenzando a analizar iniciaremos con este protocolo de enrutamiento donde mostraremos la tabla de interfaces con direcciones IP configuradas, la tabla EIGRP de topología y la tabla EIGRP de vecinos todos estos antes y después de la desconexión. Cabe indicar que esto no dará un resultado a la investigación, ya que para todas las pruebas de cada códec no se realizaron cambios en esta capa, solo mostraremos y explicáremos lo ocurrido en el enrutamiento.

En esto se mostrará las tablas de configuración de interfaces en cada router antes de la ruptura del enlace principal intencional:

Las tablas 15, 16 y 17 se obtuvieron ingresando a la línea de consola de cada router y ejecutando el comando *show ip interface brief*, en el modo de exec privilegiado. Estas tablas muestran la dirección IP asignada a cada interface. En las últimas dos columnas de esta línea, se muestra el estado de la capa 1 y de la capa 2 de esta interfaz. El valor up (activo) en la columna Status (Estado) muestra que esa interfaz opera en la capa 1. El valor up en la columna Protocol (Protocolo) indica que el protocolo de capa 2 funciona.

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	NVRAM	up	up
GigabitEthernet0/0.10	192.168.1.1	YES	NVRAM	up	up
GigabitEthernet0/0.20	172.16.1.1	YES	NVRAM	up	up
GigabitEthernet0/1	10.0.1.1	YES	NVRAM	up	up
Serial0/0/0	10.0.2.1	YES	NVRAM	up	up
Serial0/0/1	unassigned	YES	NVRAM	administratively down	down

Tabla 15: Tabla de interfaces del router R1

Elaboración: Propia

En la anterior tabla se muestra la configuración de direcciones IP de los interfaces en el router R1, donde es igual a lo propuesto en la tabla 14. Se observa que todas las interfaces utilizadas están encendidas (UP). El interface GigabitEthernet0/0 no tiene dirección IP asignada, ya que es configurada en sus subinterfaces.

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	NVRAM	up	up
GigabitEthernet0/0.10	192.168.2.1	YES	NVRAM	up	up
GigabitEthernet0/0.20	172.16.2.1	YES	NVRAM	up	up
GigabitEthernet0/1	10.0.1.2	YES	NVRAM	up	up
Serial0/0/0	unassigned	YES	NVRAM	administratively down	down
Serial0/0/1	10.0.3.1	YES	NVRAM	up	up

Tabla 16: Tabla de interfaces del router R2

Elaboración: Propia

La tabla 16 pertenece al router R2, también las direcciones IP son idénticas a la tabla 14. La interface GigabitEthernet0/0 muestra las mismas características en el router R1, ya que se configuraron en las subinterfaces las direcciones IP.

Interface	**IP-Address**	**OK?**	**Method**	**Status**	**Protocol**
GigabitEthernet0/0	unassigned	YES	NVRAM	administratively down	down
GigabitEthernet0/1	unassigned	YES	NVRAM	administratively down	down
Serial0/0/0	10.0.2.2	YES	NVRAM	up	up
Serial0/0/1	10.0.3.2	YES	NVRAM	up	up

Tabla 17: Tabla de interfaces del router R3.

Elaboración: Propia

En el router R3 solo presenta las dos interfaces seriales. La tabla 17 presenta las mismas características que la tabla 14, en cuanto a las direcciones IP

Siguiendo con esto presentaremos la tabla de vecinos de EIGRP. Los espacios de la tabla incluyen lo siguiente:

- **Columna H:** enumera los vecinos en el orden en que fueron descubiertos.
- **Address:** dirección IPv4 del vecino.
- **Interface:** la interfaz local en la cual se recibió este paquete de saludo.
- **Hold:** el tiempo de espera actual. Cuando se recibe un paquete de saludo, este valor se restablece al tiempo de espera máximo para esa interfaz y, luego, se realiza una cuenta regresiva hasta cero. Si se llega a cero, el vecino se considera inactivo.
- **Uptime:** la cantidad de tiempo desde que se agregó este vecino a la tabla de vecinos.
- **SRTT** y **RTO (tiempo de ida y vuelta promedio y tiempo de espera de retransmisión):** utilizados por RTP para administrar paquetes EIGRP confiables.
- **Q Cnt (conteo de cola):** siempre debe ser cero. Si es más que cero, hay paquetes EIGRP que esperan ser enviados.

- **Seq Num (número de secuencia):** se utiliza para rastrear paquetes de actualización, de consulta y de respuesta. (Cisco Networking Academy. 2014. P. 586-602)

Las tablas de vecinos fueron tomadas al igual que las anteriores con el comando *show ip eigrp neighbors*, mostraremos de todo los ruters.

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num
1	10.0.1.2	Gi0/1	2 00:03:34	1548	5000	0	8
0	10.0.2.2	Se0/0/0	2 00:03:34	8	100	0	8

Tabla 18: Tabla de vecinos EIGRP del router R1

Elaboración: Propia

El resultado del router R1 muestra que está conectado a dos vecinos. El primero en ser descubierto fue el vecino con la dirección IP 10.0.2.2, por el interface Serial0/0/0, seguido descubrió al router con dirección IP 10.0.1.2 por la interface GigabitEthernet 0/1. Verificando las tablas de interfaces IP podemos deducir que los router vecinos son R2 por la dirección IP 10.0.1.2 (ver tabla 18) y después R3 deducido gracias a la dirección IP 10.0.2.2 (ver tabla 17)

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num
1	10.0.1.1	Gi0/1	2 00:04:02	1	100	0	7
0	10.0.3.2	Se0/0/1	2 00:04:28	3	100	0	9

Tabla 19: Tabla de vecinos EIGRP del router R2

Elaboración: Propia

Igual que en el router R1 muestra que está conectado a dos vecinos. El primero en la lista fue el vecino con la dirección IP 10.0.3.2, conectada por el interface Serial0/0/1, después descubrió al router con dirección IP 10.0.1.1 por la interface GigabitEthernet 0/1. Verificando las tablas de interfaces IP podemos deducir que los router vecinos son R3 por la dirección IP 10.0.3.2 (ver tabla 18) y después R1 deducido gracias a la dirección IP 10.0.1.1 (ver tabla 16)

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num
1	10.0.2.1	Se0/0/0	2 00:04:12	35	210	0	6
0	10.0.3.1	Se0/0/1	2 00:04:38	20	120	0	9

Tabla 20: Tabla de vecinos EIGRP del router R3

Elaboración: Propia

El router R3 muestra que está conectado a dos vecinos. El primero en la lista fue el router con la dirección IP 10.0.3.1, conectada por el interface Serial0/0/1, luego al router con dirección IP 10.0.2.1 por la interface Serial0/0/0. Verificando las tablas de interfaces IP podemos deducir que los router vecinos son R1 por la dirección IP 10.0.2.1 (ver tabla 16) y después R2 deducido gracias a la dirección IP 10.0.3.1 (ver tabla 17)

El resultado indica que todos se reconocen entre sí, por ejemplo: el router R1 conoce a sus vecinos R2 y R3 al igual que R3 conoce a R1 y R2, los espacios de la tabla incluyen lo siguiente: Con estas tablas queremos comprobar los routers vecinos, junto a las interfaces conectadas y la dirección IP.

Para visualizar sobre los caminos tomados para el envío de datos, mostraremos la tabla de topología EIGRP, esta tabla indica los sucesores y sucesores factibles en cada ruta, la tabla 21 y la tabla 22.

P	**192.168.2.0/24, 1 successors, FD is 3072** **via 10.0.1.2 (3072/2816), GigabitEthernet0/1**
P	10.0.3.0/30, 1 successors, FD is 2170112 via 10.0.1.2 (2170112/2169856), GigabitEthernet0/1 via 10.0.2.2 (2681856/2169856), Serial0/0/0
P	10.0.1.0/30, 1 successors, FD is 2816 via Connected, GigabitEthernet0/1
P	**172.16.2.0/24, 1 successors, FD is 3072** **via 10.0.1.2 (3072/2816), GigabitEthernet0/1**
P	192.168.1.0/24, 1 successors, FD is 2816 via Connected, GigabitEthernet0/0.10
P	10.0.2.0/30, 1 successors, FD is 2169856 via Connected, Serial0/0/0
P	172.16.1.0/24, 1 successors, FD is 2816 via Connected, GigabitEthernet0/0.20

Tabla 21: Tabla de topologia EIGRP del router R1

Elaboración: Propia

La tabla 21 indica los sucesores factibles del router R1, junto con la métrica para llegar hasta esa red, se observa que para llegar a la red 192.168.2.0/24 solo existe una ruta a través de la interface GigabitEthernet0/1 con una distancia factible (metrica) 3072, lo mismo que ocurre para llegar a la red 172.16.2.0/24. Entonces la ruta tomara como se muestra en la figura 34. Los valores de ancho de banda y delay son tomados en cada interface con el comando *show interface "nombre de la interface"*

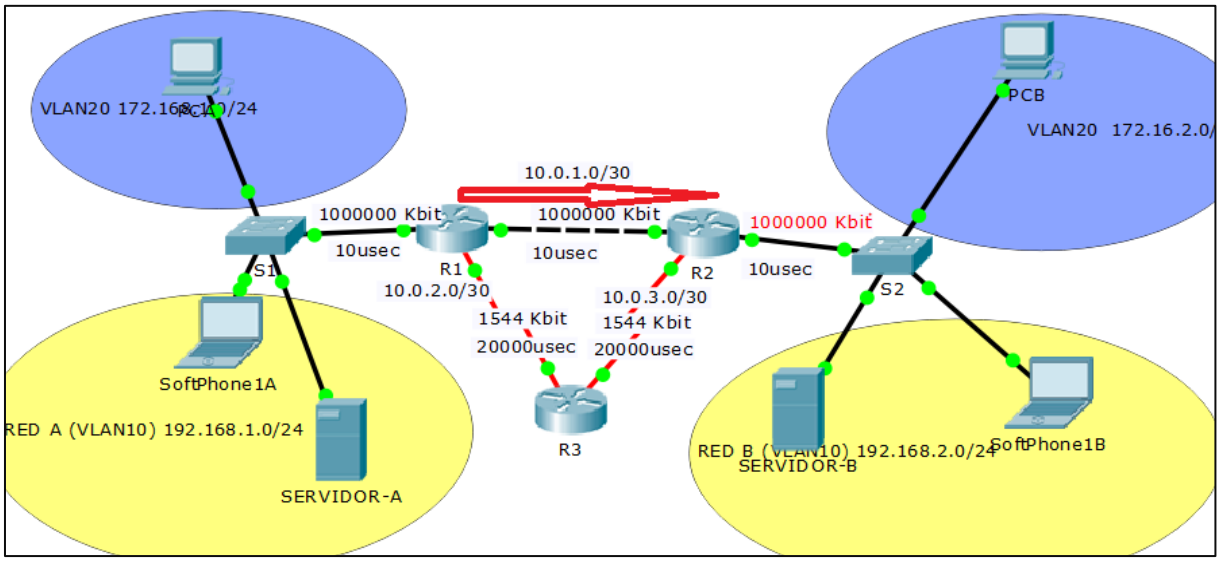


Figura 35: Ruta principal

Elaboración: Propia

La métrica es calculada con los valores de la figura 34, tomando en cuenta el ancho de banda de banda más baja y sumando todo los delay. Se observa que todos los enlaces en la ruta son GigabitEthernet, lo que indica el ancho de banda más bajo será de 1000000 Kbit y el retardo total es de 20 microsegundos; reemplazando en la Ec. 2, terminara de la siguiente manera:

$$Metrica = \left(\frac{10^7}{1000000} + \frac{20}{10}\right) \times 256$$

$$Metrica = (10 + 2) \times 256 = 12 \times 256$$

$$Metrica = 3072$$

En la tabla 22 se muestra la tabla de topología EIGRP del router R2 en esto indica que para llegar a las redes 192.168.1.0/24 y 172.16.1.0/24 solo existe una ruta a través de la interface GigabitEthernet0/1 con una distancia factible (metrica) 3072, al igual que nos muestra la tabla 22, con esto indica que ambos router tienen como ruta principal los enlaces conectados en los interfaces GigabitEthernet0/1 de ambos.

P	192.168.2.0/24, 1 successors, FD is 2816 via Connected, GigabitEthernet0/0.10
P	10.0.3.0/30, 1 successors, FD is 2169856 via Connected, Serial0/0/1
P	10.0.1.0/30, 1 successors, FD is 2816 via Connected, GigabitEthernet0/1
P	172.16.2.0/24, 1 successors, FD is 2816 via Connected, GigabitEthernet0/0.20
P	**192.168.1.0/24, 1 successors, FD is 3072** **via 10.0.1.1 (3072/2816), GigabitEthernet0/1**
P	10.0.2.0/30, 1 successors, FD is 2170112 via 10.0.1.1 (2170112/2169856), GigabitEthernet0/1 via 10.0.3.2 (2681856/2169856), Serial0/0/1
P	**172.16.1.0/24, 1 successors, FD is 3072** **via 10.0.1.1 (3072/2816), GigabitEthernet0/1**

Tabla 22: Tabla de topología EIGRP del router R2

Elaboración: Propia

Después de la ruptura

Mostrado el análisis antes de la ruptura del enlace de la interface GigabitEthernet0/1. Continuando mostraremos las tablas, pero después de esta ruptura. La ruptura fue intencional y de forma física, es decir desconectando el cable conectado en esta interface.

Interface	**IP-Address**	**OK?**	**Method**	**Status**	**Protocol**
GigabitEthernet0/0	unassigned	YES	NVRAM	up	up
GigabitEthernet0/0.10	192.168.1.1	YES	NVRAM	up	up
GigabitEthernet0/0.20	172.16.1.1	YES	NVRAM	up	up
GigabitEthernet0/1	**10.0.1.1**	**YES**	**NVRAM**	**down**	**down**
Serial0/0/0	10.0.2.1	YES	NVRAM	up	up
Serial0/0/1	unassigned	YES	NVRAM	administratively down	down

Tabla 23: Tabla de interfaces del router R1 después de la ruptura

Elaboración: Propia

En la tabla 23 se muestra que la interface GigabitEthernet0/1 está apagado (down), tanto en la capa física y como en la capa de enlace de datos, indicando que ya se realizó la desconexión.

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	NVRAM	up	up
GigabitEthernet0/0.10	192.168.2.1	YES	NVRAM	up	up
GigabitEthernet0/0.20	172.16.2.1	YES	NVRAM	up	up
GigabitEthernet0/1	**10.0.1.2**	**YES**	**NVRAM**	**down**	**down**
Serial0/0/0	unassigned	YES	NVRAM	administratively down	down
Serial0/0/1	10.0.3.1	YES	NVRAM	up	up

Tabla 24: Tabla de interfaces del router R2 después de la ruptura

Elaboración: Propia

El resultado de R2 es similar que el router R1, con un enlace desconectado que se muestra como apagado en las capas 1 y 2 del modelo OSI, al iual que en R1 esto muestra que el enlace esta desconectado. Los resultados de R3 son omitidas, ya que la desconexión no influye a sus enlaces conectadas.

También hay cambios en la tabla de vecinos EIGRP, mostrados a continuación:

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num
0	10.0.2.2	Se0/0/0	2 00:06:34	2	100	0	14

Tabla 25: Tabla de vecinos EIGRP del router R1 después de la ruptura

Elaboración: Propia

La tabla 25, R1 solo reconoce un vecino con una dirección IP 10.0.2.2 que se conecta por la interface Serial0/0/0, revisando la topología de la figura 34 y la tabla 24 se observa que pertenece al router R3, por la desconexión del enlace principal el router R1 desconoce como un vecino a R2

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num
0	10.0.3.2	Se0/0/1	2 00:07:14	1	100	0	16

Tabla 26: Tabla de vecinos EIGRP del router R2 después de la ruptura

Elaboración: Propia

En la tabla 26 demuestra que el router vecino de R2 se reduce a uno, R3 es el que une ambos router (R1 y R2). El enlace redundante que conforma R3 será por donde se reestablecerá la comunicación.

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num
1	10.0.2.1	Se0/0/0	2 00:06:44	17	102	0	11
0	10.0.3.1	Se0/0/1	2 00:07:09	9	100	0	13

Tabla 27: Tabla de vecinos EIGRP del router R3 después de la ruptura

Elaboración: Propia

Como se mencionó anteriormente el router R3 es encargado de comunicar a sus vecinos. La tabla 27 indica que el router aún mantiene comunicación directa con R1 y R2.

En la tabla de topología EIGRP en R1 y R2 se observaron cambios como el cambio de la distancia factible, las vías y sucesores. Analizaremos estas tablas calculando la métrica.

P	**192.168.2.0/24, 1 successors, FD is 2682112**
	via 10.0.2.2 (2682112/2170112), Serial0/0/0
P	10.0.3.0/30, 1 successors, FD is 2170112
	via 10.0.2.2 (2681856/2169856), Serial0/0/0
P	**172.16.2.0/24, 1 successors, FD is 2682112**
	via 10.0.2.2 (2682112/2170112), Serial0/0/0
P	192.168.1.0/24, 1 successors, FD is 2816
	via Connected, GigabitEthernet0/0.10
P	10.0.2.0/30, 1 successors, FD is 2169856
	via Connected, Serial0/0/0
P	172.16.1.0/24, 1 successors, FD is 2816
	via Connected, GigabitEthernet0/0.20

Tabla 28: Tabla de topología EIGRP del router R1 después de la ruptura

Elaboración: Propia

P	192.168.2.0/24, 1 successors, FD is 2816
	via Connected, GigabitEthernet0/0.10
P	10.0.3.0/30, 1 successors, FD is 2169856
	via Connected, Serial0/0/1
P	172.16.2.0/24, 1 successors, FD is 2816
	via Connected, GigabitEthernet0/0.20
P	**192.168.1.0/24, 1 successors, FD is 2682112**
	via 10.0.3.2 (2682112/2170112), Serial0/0/1
P	10.0.2.0/30, 1 successors, FD is 2170112
	via 10.0.3.2 (2681856/2169856), Serial0/0/1
P	**172.16.1.0/24, 1 successors, FD is 2682112**
	via 10.0.3.2 (2682112/2170112), Serial0/0/1

Tabla 29: Tabla de topología EIGRP del router R2 después de la ruptura

Elaboración: Propia

En la tabla 28 indica que el router R1 tiene un sucesor para llegar a las redes 192.168.2.0/24 y 172.16.2.0/24, con una distancia factible de 2682112 a través de interface Serial0/0/0, lo que indica que se tomara la ruta que indica la figura 35.

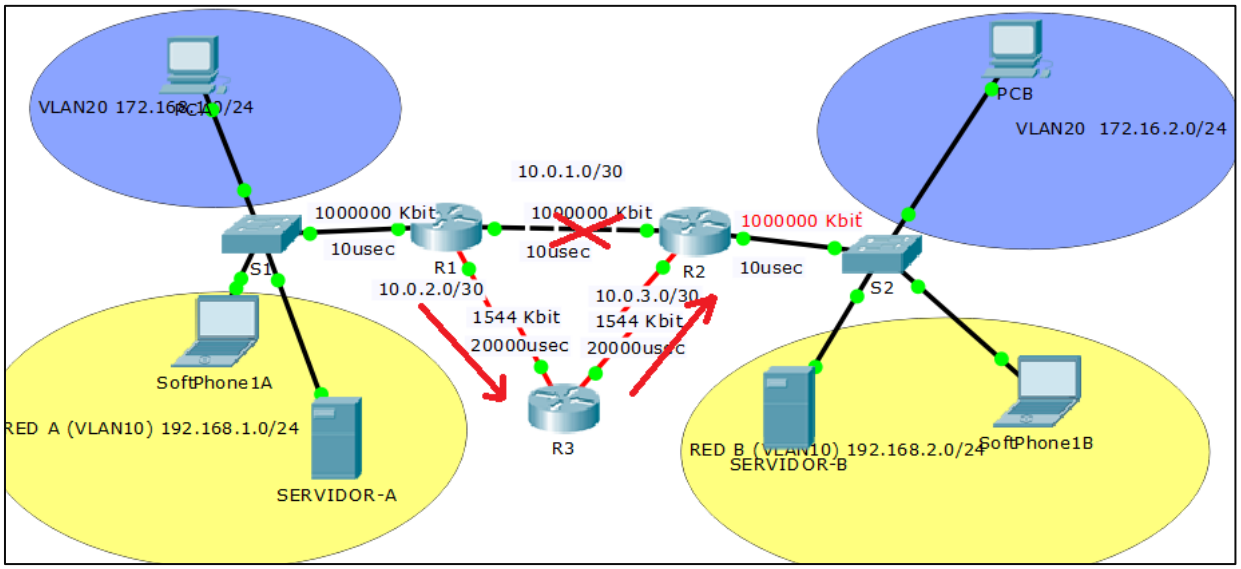


Figura 36: Enlace redundante:

Elaboración: Propia

Para un mejor análisis calcularemos la métrica donde el ancho de banda más bajo es de la interface serial (1544 Kbit) y la suma de retardo (delay) es 20000+20000+10 que es igual a 40010 reemplazando en la Ec. 2:

$$Metrica = \left(\frac{10^7}{1544} + \frac{40010}{10}\right) \times 256$$

$$Metrica = (6476 + 4001) \times 256 = 10477 \times 256$$

$$Metrica = 2682112$$

También se observa que en R2 para llegar a las redes 192.168.1.0/24 y 172.16.1.0/24 es por la interface Serial0/0/1, con una métrica de 2682112 esto indica que es la misma ruta que toma R1 hacia las redes 192.168.2.0/24 y172.16.2.0/24.

4.2.Análisis de SIP

Siendo un protocolo de inicio de sesión, este protocolo no interfiere con la investigación ya que, en el momento de la ruptura, no envía paquetes. Sin embargo, mostraremos lo resultados que nos entrega SIP cuando inicia la llamada al igual que cuando termina. Los paquetes enviados y recibidos son iguales en todas las pruebas (30 pruebas).

No.	Time	Source	Destination	Protocol	Length	Info
1	5060	192.168.2.10	192.168.1.10	SIP/SDP	1366	Request: INVITE sip:101@192.168.1.10 |
2	5060	192.168.1.10	192.168.2.10	SIP	384	Status: 100 Trying |
3	5060	192.168.1.10	192.168.2.10	SIP	605	Status: 180 Ringing |
4	5060	192.168.2.10	192.168.1.10	SIP	523	Request: PRACK sip:101@192.168.1.10 |
5	5060	192.168.1.10	192.168.2.10	SIP	393	Status: 200 OK |

Figura 37: Mensajes SIP para establecer la llamada

Elaboración: Propia

La comunicación inicia con el softphone1B (referencia tabla 9) invitando al softphone1A. en la figura 36, el softphone1B con dirección IP 192.168.2.10 envía al softphone1A (192.168.1.10) un mensaje de requerimiento INVITE para establecer la llamada, es respondido con el mensaje de estado *100 Trying*; indica intentando, posteriormente sigue la respuesta *180 Ringring*, señala que el teléfono está sonando. Al final termina con la respuesta de estado *200 OK*, indica que la llamada se ha establecido exitosamente.

7210	5060	192.168.1.10	192.168.2.10	SIP	488	Request: BYE sip:Abel@192.168.2.10 |
7211	5060	192.168.2.10	192.168.1.10	SIP	391	Status: 200 OK |

Figura 38: Mensajes SIP para finalizar la llamada

Elaboración: Propia

Para cuando se terminaron las llamadas el softphone1A envía el mensaje de requerimiento BYE hacia el softphone1B, esto para finalizar la llamada; es respondido con *200 OK*, indicando que se ha finalizado exitosamente.

Todos estos mensajes son correspondientes al protocolo SIP para establecer y finalizar la llamada. También se observaron otros mensajes de requerimiento, tales como: INFO, PUBLISH y OPTIONS, todos estos son para verificar el estado de la sesión o actualizar la información sobre el softphone (teléfono).

4.3. Análisis de RTP

El análisis principal de esta investigación está dentro de este protocolo, ya que se encarga de transportar la conversación, y es cuando se realizó la desconexión del enlace principal.

Presentaremos el promedio de flujo (diagramas) de paquetes RTP enviados, como se muestra en la figura 38 desde el SoftPhone1A hacía SoftPhone1B. El promedio de los datos numéricos se presentará en el ANEXO B

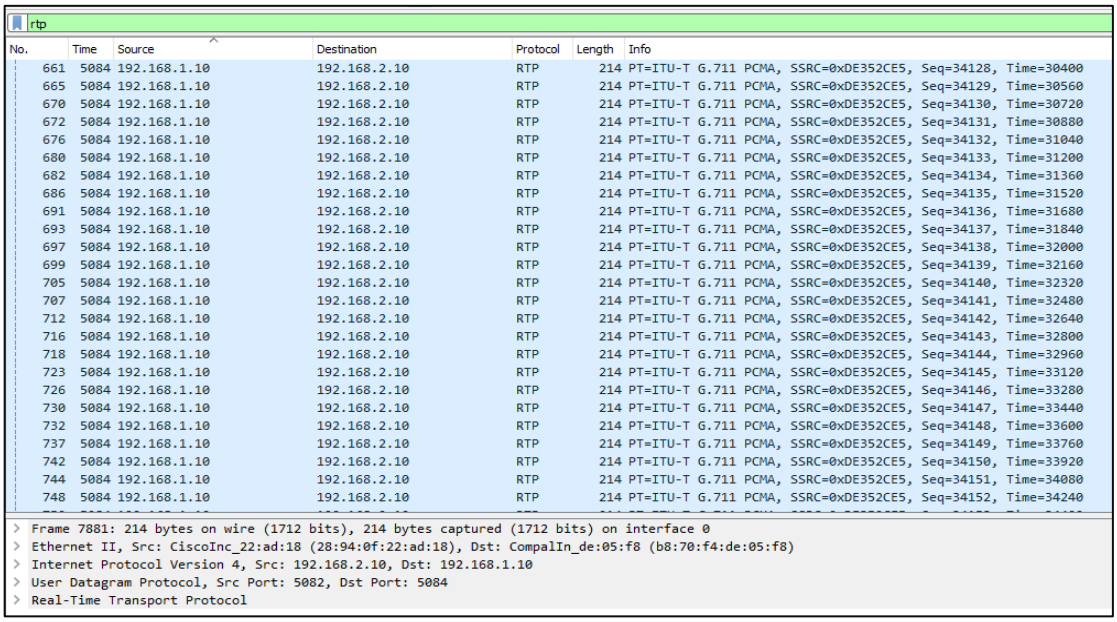


Figura 39: Paquetes RTP enviados

Elaboración: Propia

En la figura 39 procederemos a explicar algunos aspectos importantes de los paquetes RTP. se observa que este protocolo trabaja con UDP utilizando el puerto 5068 para origen y el puerto 5066 para el destino, la longitud es de 180 en todas las pruebas.

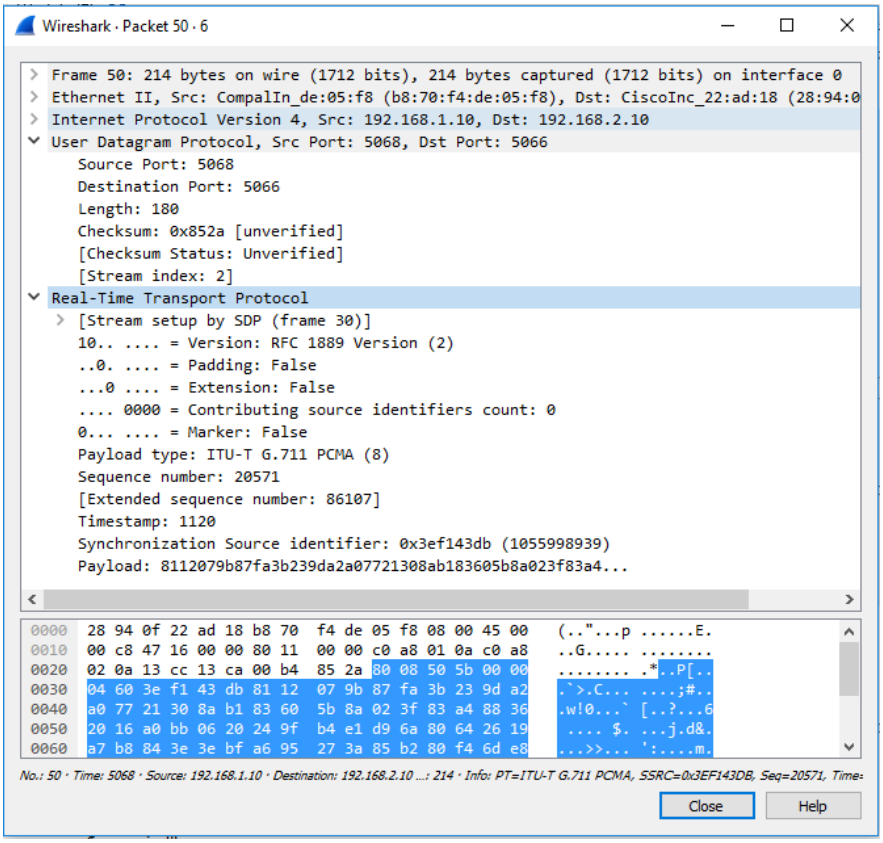


Figura 40: Cabecera de los paquetes RTP

Elaboración: Propia

En la parte de RTP se inicia a ver la versión del protocolo, en todos los paquetes se observó la versión 2. En el siguiente espacio se encuentra el bit de relleno (Padding). se trata de un bit que indica que la carga útil incluye octetos de relleno al final. El bit de relleno se pone 0 para indicar que no existe un relleno. Luego está el bit de extensión, se trata de un bit que indica que la cabecera utiliza el formato extendido, es 0 si ocurre lo contrario. Cuenta CSRC (CC). Utiliza 4 bits para indicar el número de identificadores CSRC que se añaden al final de la cabecera fija. Este campo viene a identificar el número de participantes en la comunicación. El espacio de Marcador (Marker, M). Utiliza para que las aplicaciones que no envían información en los periodos de silencio fijen este bit a un en el primer paquete después de un periodo de silencio. En Tipo de carga útil (Payload Type, PT). Se trata de un campo de 7 bits que contiene el número que identifica el códec utilizado en la carga útil. En el caso nuestro 8 si es PCMA, 9 para G722 y 3 para GSM. Numero de secuencia (Sequence Number). Se trata de un campo de 16 bits que utiliza el remitente para identificar el orden secuencial de envió de los paquetes. Permite al destinatario detectar la posible pérdida o desorden de los paquetes. Contador de tiempo (TimesTamp). Se trata de un campo de 32 bits que indica el instante en el que se generó la primera muestra de la carga útil. Indetificacion del origen (Synchronization Source, SSRC). Se trata de un campo de 32 bits que identifica al remitente o a la aplicación intermedia utilizada (mezclador). Al final termina con el payload que es los datos de voz transportados. (H. Schulzrinne & S. Casner, 2003)

4.3.1. Flujo completo.

En la figura 40 indica el flujo de paquetes RTP respecto a cada códec. Las gráficas no son claras por lo que para el análisis detallado se realizara un acercamiento en el momento de la caída del flujo para cada tipo de códec.

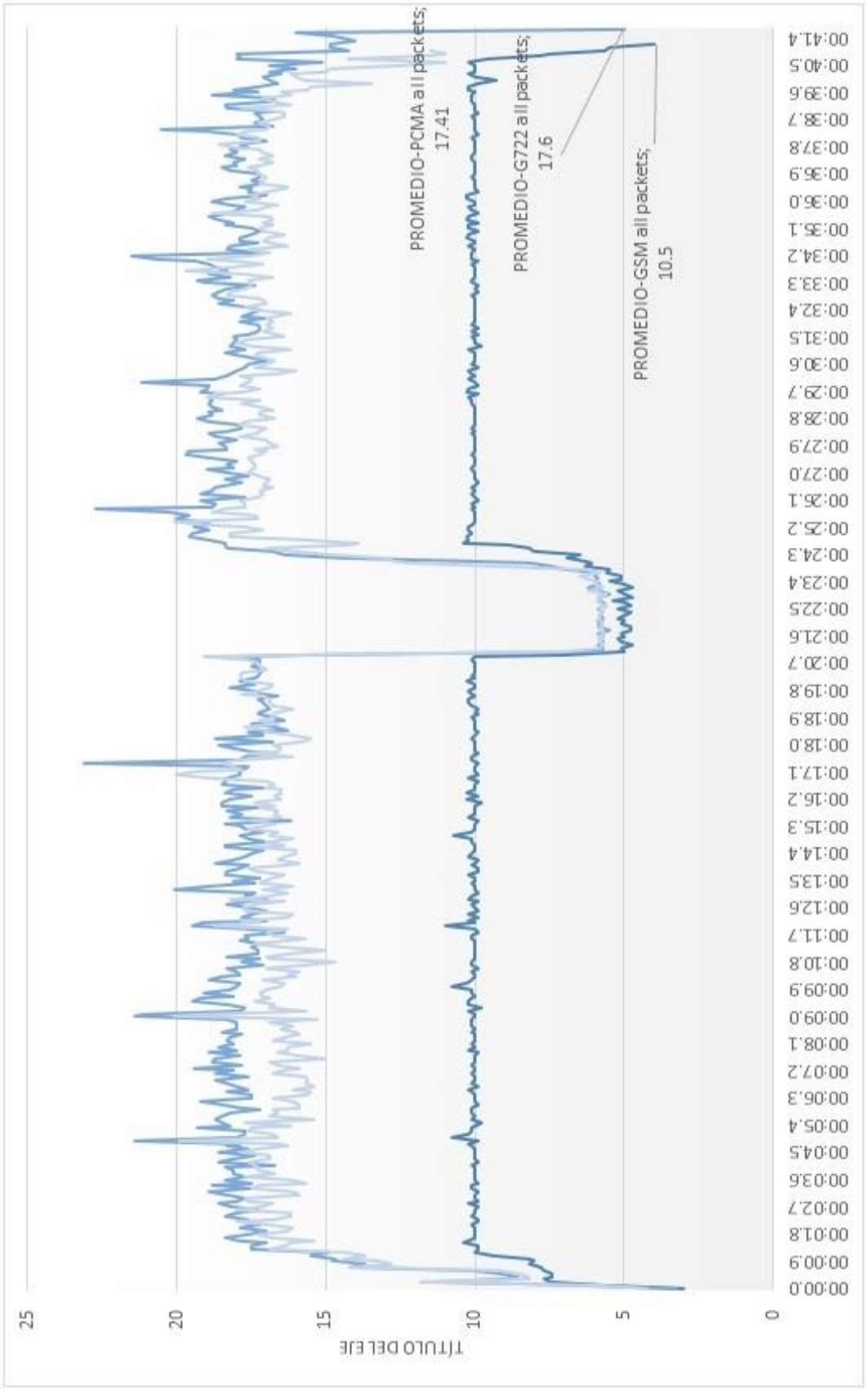


Figura 41: Flujo de paquetes RTP y promedio de paquetes por 100ms

Elaboración: Propia

En la figura 40 y revisando el ANEXO B se puede observar que los paquetes enviados antes de la desconexión y después de la recuperación del enlace principal por el códec GSM son un promedio aproximado a 10 paquetes por 100ms, en caso del códec G722 es de aproximadamente 18 paquetes por el mismo rango de tiempo que del anterior y de PCMA su promedio de paquetes por 100ms es de 17 paquetes aproximadamente.

4.3.2. Flujo con acercamiento

Para el análisis del flujo se toma las siguientes observaciones:

- El conteo de tiempo de recuperación es desde la disminución de paquetes más notorio, aproximadamente a los 00:20,9 segundos en los tres códecs, registrado después de la desconexión del enlace principal
- El flujo es considerado recuperado si los paquetes son mayor o igual a los paquetes antes de la desconexión.

4.3.2.1. Flujo de acercamiento del codec GSM

Iniciando como tiempo de partida desde los 00:20,9 segundos, y luego observando el ANEXO C donde indica que en el tiempo 00:24,7 los paquetes ascendieron a 10.4 esto indica que el flujo está recuperado. Entonces el tiempo de recuperación para GSM es de: $\mathbf{00:24,7 - 00:20,9 = 00:03,8\ segundos.}$

4.3.2.2. Flujo de acercamiento del codec G722

Observando el ANEXO D, en el tiempo 00:20,9 segundos descienden la cantidad de paquetes significativamente. Posteriormente se observa la cantidad de 18,3 paquetes a los 00:24,5, este valor es más alto que antes de la desconexión. El tiempo de recuperación es de: $\mathbf{00:24,5 - 00:20,9 = 00:03,6\ segundos.}$

4.3.2.3. Flujo de acercamiento del codec PCMA

En el ANEXO E, el grafico indica que cantidad de paquetes después de 00:20,9 segundos disminuyo significativamente. A los 00:24,9 hay 18,2 paquetes, este valor es mayo que antes

de la desconexión. El tiempo de recuperación es de: $\mathbf{00:24,9 - 00:20,9 = 00:04,0\ segundos.}$

4.4. Análisis de RTCP

Es un protocolo de comunicación que proporciona información de control que está asociado con un flujo de datos para una aplicación multimedia (flujo RTP). Este protocolo nos ayudara a ver el porcentaje de paquetes perdidos desde la desconexión hasta la recuperación del flujo.

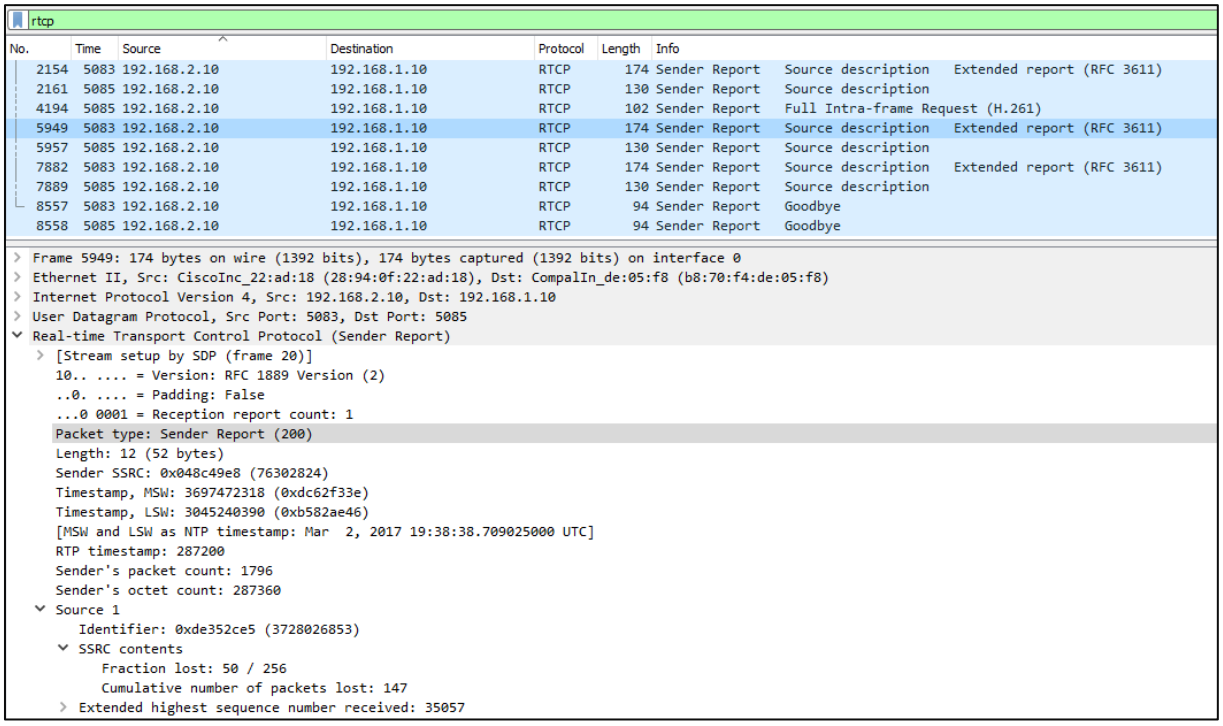


Figura 42: Paquetes RTCP recibidos

Elaboración: Propia

En la sección 4.3 se analizó los paquetes RTP enviados desde el SoftPhone1A (dirección IP: 192.168.1.10) hacia el SoftPhone1B (dirección IP: 192.168.2.10). Los paquetes RTP son controlados mediante respuestas de los paquetes RTCP, por lo que en esta sección se procederá

a analizar los paquetes RTCP recibidas del SoftPhone1B. Estos paquetes contienen varios datos de respuesta como se muestra en la figura 42.

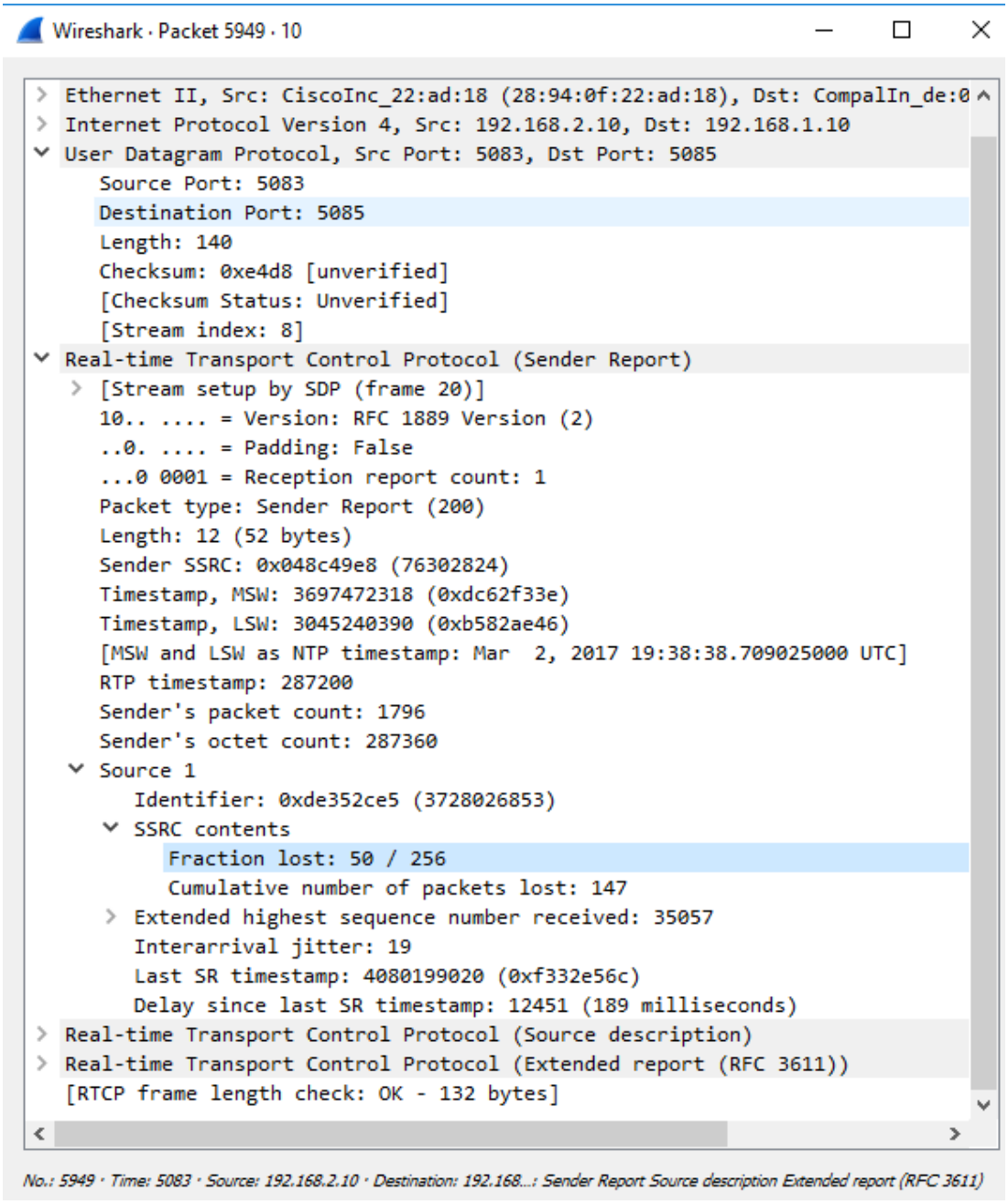


Figura 43: Contenido en los paquetes SR de RTP

Elaboración: Propia

Como se muestra en la figura RTCP es transportado por el protocolo UDP al igual que en RTP, los puertos utilizados son 5083 para el origen y 5085 para el puerto de destino. Luego de esto se muestra la parte de SR (Sender Report), la cual tiene el espacio como:

- Versión Identifica la versión de RTP, que es la misma en paquetes RTCP como en paquetes de datos RTP. La versión definida por esta especificación es dos (2).
- Padding Si se ajusta el bit de relleno, este paquete RTCP contiene algunos octetos de relleno adicionales al final que no forman parte de la información de control. El último octeto del relleno es un recuento de cuántos octetos de relleno deben ser ignorados.
- Conteo de informes de recepción: el número de bloques de informes de recepción contenidos en este paquete. Un valor de cero es válido.
- Tipo de paquete Contiene la constante 200 para identificarlo como un paquete RTCP, en este caso es un SR.
- Longitud: La longitud de este paquete RTCP en 32 bits, incluyendo el encabezado y cualquier relleno.
- SSRC: El identificador de origen de sincronización para el originador de este paquete SR.
- NTP timestamp: Indica el tiempo de reloj de la pared cuando se envió este informe para que pueda ser utilizado en combinación con las marcas de tiempo devueltas en los informes de recepción de otros receptores para medir la propagación de ida y vuelta a esos receptores.
- RTP timestamp: Corresponde al mismo tiempo que la marca de tiempo NTP (anterior), pero en las mismas unidades y con el mismo desplazamiento al azar que las marcas de tiempo RTP en paquetes de datos
- Recuento de paquetes del remitente: Número total de paquetes de datos RTP transmitidos por el remitente desde el inicio de la transmisión hasta el momento en que se generó este paquete SR. El contador se restablece si el remitente cambia su identificador SSRC.
- Cuenta del octeto del remitente: El número total de octetos de carga útil (es decir, sin incluir cabecera o relleno) transmitidos en paquetes de datos RTP por el remitente desde que se inició la transmisión hasta el momento en que se generó este paquete SR.

La tercera sección contiene informes de recepción por este remitente desde el último informe. Cada bloque de informe de recepción transmite estadísticas sobre la recepción de paquetes RTP. Estas estadísticas son:

- SSRC (identificador de fuente): El identificador SSRC de la fuente a la que pertenece la información en este bloque de informe de recepción.

- Fracción perdida: La fracción de paquetes de datos RTP de la fuente SSRC perdida desde que se envió el paquete SR o RR anterior.
- Número acumulado de paquetes perdidos: El número total de paquetes de datos RTP de la fuente SSRC que se han perdido. (Q. Wu, F. Xia, & R. Even, 2012)

Examinaremos el campo de fracción de perdida (fraction lost). Analizamos los paquetes de respuesta del receptor. El informe del receptor, aquellos que reciben paquetes RTP. Esto informa al emisor y otros receptores sobre la calidad del servicio, pero en este caso solo tomaremos la sección de fractión lost. Este campo otorga datos en fracción donde el denominador es 256, al dividir esto indica la cantidad el porcentaje de paquetes perdidos. Los paquetes de reporte de receptor no están visibles, su ubicación está en los paquetes de reporte del emisor. Por ejemplo, si el valor incluido es 64, esto indicara que se han perdido 64/256 = 25%., como indica la figura 37 del SoftPhone1B.

Tomando en cuenta que en cada prueba hay un promedio de 6 paquetes de reporte de emisor. Para sacar estos resultados de cada prueba se usó la fórmula:

$$valor\ promedio = \frac{v_1+v_2+v_3+\cdots+v_n}{n(256)} \quad \text{(Ec. 3)}$$

Donde v es el valor es el numerador en la parte fracction lost, esta fórmula se realizó para cada prueba obteniendo a tabla 30 donde se obtiene el porcentaje de paquetes perdidos en cada prueba y al final se resuelve con un promedio, donde se observa que el códec GSM hay menos perdida de paquetes, opuestamente ocurrido con G722.

Codec	1	2	3	4	5	6	7	8	9	10	PROMEDIO (%)
GSM	0,225	0,034	0,070	0,166	0,164	0,052	0,061	0,057	0,052	0,164	0,1043(10,43%)
G722	0,051	0,169	0,238	0,239	0,237	0,238	0,240	0,166	0,238	0,238	0,2053(20,53%)
PCMA	0,263	0,233	0,167	0,053	0,035	0,167	0,238	0,238	0,234	0,051	0,1678(16,78%)

Tabla 30: Porcentaje de pérdida de paquetes

Elaboración: Propia

Los resultados obtenidos son promediados de las 10 pruebas para cada códec. El códec GSM tiene una pérdida de paquetes del 10.43%. En G722 la perdida de paquetes es del 20.53%. PCMA la perdida de paquetes es de 16.78%

4.5. Discusión de resultados.

Posteriormente de analizar los resultados en cada protocolo de las pruebas realizadas con diferentes códecs, se tomarán todos los resultados para compararlos, para finalizar con las conclusiones. Los resultados que se tomaran en este análisis final son de los protocolos RTP y RTCP, ya que son los protocolos de transportar los códecs y es donde se observaron las diferencias. En la tabla 31 se resume los resultados de estos protocolos respecto a cada códec.

	Obtenido de:	**GSM**	**G722**	**PCMA**
RTP (tiempo de recuperación del flujo)	Sección 4.3.2	00:03,8 segundos	00:03,6 segundos	00:04,0 segundos.
RTP (promedio de paquetes enviados en toda la comunicación)	Figura 40	10.5 paquetes	17.6 paquetes	17.41 paquetes
SRTP (pocentaje de paquetes perdidos)	Tabla 30	10,43%	20,53%	16,78%

Tabla 31: Resumen de resultados de los protocolos RTP y RTCP

Elaboración: Propia

Observando la tabla, se muestra que para el códec GSM el tiempo de demora es de 03,8 segundos con una pérdida de paquetes de solo el 10,43% esto es ya que este códec mantiene la cantidad de paquetes en un promedio de 10.5 lo que es menos comparando a los demás códec. Continuando, el códec G722 tiene una pérdida de 20,53% paquetes y el tiempo de recuperación es solo de 03,6 segundos, el promedio de paquetes enviados es de 17.6 aproximadamente igual al códec PCMA. PCMA tiene tuna perdida de 16,78% y la demora es de 04,0 segundos la más lenta comparando con los demás códecs.

Ya interpretado los resultados podemos observar diferentes ventajas en cada códec según los análisis realizados, por ejemplo: el tiempo de recuperación mínima es del códec G722, seguido por GSM y al final PCMA; en cambio en el promedio de paquetes enviados mínimos el orden es diferentes iniciando con el códec GSM, luego PCMA y termina con G722 y terminando, el porcentaje de paquetes perdidos, el menor porcentaje tiene GSM, luego PCMA y el mayor porcentaje tiene G722.

Aun no se tiene un análisis que determine las conclusiones, ya que existen tres diferentes en las cuales cada códec presenta ventajas. Tomando el objetivo de la investigación en cuenta, el análisis del tiempo de recuperación es la prioridad y los dos análisis sobrantes serán puntos secundarios, de esta manera se determinarán las conclusiones.

CONCLUSIONES

PRIMERO: Se logró implementar una red de enlace redundante con enrutamiento EIGRP y servicios de telefonía IP, permitiendo el estudio de los códec PCMA, GSM Y G722, este análisis permitió estudiar los resultados y comportamiento de los diferentes códecs, la investigación se realizó en el laboratorio de CISCO – Escuela Profesional de Ingeniería Electrónica. Esta investigación valida con los objetivos planteados, el análisis del tiempo de recuperación de un enlace en una red con enrutamiento EIGRP y servicio de telefonía IP, permitió definir el códec adecuado entre PCMA, GSM y G722. Este análisis permitirá que la comunicación de telefonía IP en empresas y/o entidades públicas sea más eficiente.

SEGUNDO: Se analizó el comportamiento del códec G.722, se afirma que el códec ofrece una recuperación rápida, luego de una caída del enlace principal, con un tiempo promedio de 3.6 segundos, tiene una pérdida de paquetes del 20%, el cual es muy alto, por lo tanto, se recomienda usarlo en entornos con alta disponibilidad de ancho de banda. Se analizó el comportamiento del códec GSM con una demora de 3.8 segundos, tiene una pérdida de paquetes del 10% y el promedio de paquetes enviados son 10 paquetes por 100ms que vendría ser menos que los demás códec, en entornos con el ancho de banda mínimo, el códec GSM es la mejor alternativa. Se analizó el comportamiento del codec PCMA, tuvo el tiempo de recuperación más alto, siendo en promedio de 4.0 segundos, una pérdida de paquetes del 16%, este valor es menor al códec G722. En caso si necesita una buena calidad se puede usar este códec, pero tome las precauciones ante fallas.

RECOMENDACIONES

PRIMERO: El uso del software de captura de paquetes es avanzado, recomendamos un conocimiento previo antes de su uso, como filtrado de tipos de paquetes según el protocolo, exportar datos hacia otros formatos o programas, visualización de las cabeceras de protocolos y visualización el flujo de paquetes.

SEGUNDO: Los protocolos RTP y RTCP necesitan un estudio o investigación profunda ya que presenta datos difíciles de entender para personas ajenas a este tema, estos datos son importantes para entender la situación de tu servicio de telefonía IP.

TERCERO: Este resultado solo se basa en el tiempo, pero también hay que ver otro aspecto lo cual sería la frecuencia de muestreo ya que esto indica la cantidad muestras por segundo afectando esto a la calidad del audio en digital. G.722 tiene 16kHz al igual que en PCMA entonces ambos tienen la misma calidad; excepto GSM que es de 8kHz. En este punto no se trata de contradecir los resultados anteriores solo se da a conocer que cuando se elija un códec por la calidad y no por el tiempo de re-direccionamiento es preferible tener en cuenta las frecuencias de muestreo.

CUARTO: El acceso mediante navegador puede ser tedioso por esta razón es bueno tomar estas recomendaciones, desactivar el firewall de ordenador que ingresara al servidor Elastix desactivar la configuración proxy del ordenador y, por último; es posible que el navegado reconozca como una página insegura por lo cual lea bien las alertas que se muestran.

QUINTO: La investigación tuvo resultados favorables para las conclusiones. Los paquetes RTP y RTCP muestran los resultados para el análisis, donde indican RTP el flujo de paquetes enviados cada prueba se obtuvo resultados no similares por lo que se hace 10 pruebas para cada códec y luego promediarlos. Las 10 pruebas indican que el promedio es aceptable. Al igual que los paquetes de respuesta RTCP.

REFERENCIAS

Aamir, M., & Zaidi, S. M. A. (2012, December). QoS analysis of VoIP traffic for different codecs and frame counts per packet in multimedia environment using OPNET. In Multitopic Conference (INMIC), 2012 15th International (pp. 275-281). IEEE.

Alshamrani, M., Cruickshank, H., Sun, Z., Elmasri, B., & Fami, V. (2013, April). Evaluation of SIP Signalling and QoS for VoIP Over OLSR MANET Routing Protocol. In Computer Modelling and Simulation (UKSim), 2013 UKSim 15th International Conference on (pp. 699-706). IEEE.

Anouari, T., & Haqiq, A. (2012, December). Comparative study and analysis of voip traffic over wimax using different service classes. In Next Generation Networks and Services (NGNS), 2012 (pp. 87-93). IEEE.

Blackstone, W., Prest, W., & Gallanis, T. (2016). Commentaries on the laws of England. Oxford: Oxford University Press.

Cisco Networking Academy (2015). Implementing Cisco Voice Communications and QoS (Vol. 1). Cisco.

Cisco Networking Academy. (2014). Routing y switching de Escalamiento de redes. CCNA3 V5. EEUU:

Carballar, J. A. (2008). VoIP. La telefonia de Internet. Madrid, Magallanes, ESPAÑA: International Thomson Editores Spain Paraninfo, S.A.

Cisco Networking Academy. (2010). Implementing Cisco Voice Communications and QoS.(1st ed.). EEUU. Retrieved from http://www.cisco.com/go/archive/ccnavoica

Cisco Networking Academy. (2014). Principios básicos de enrutamiento y switching. CCNA1 V5. EE.UU.

CISCO. (2013). Protocolo de enrutamiento de gateway interior mejorado. 03 -08-2016, de CISCO Sitio web: http://www.cisco.com/cisco/web/support/LA/7/75/75043_eigrp-toc.html

Corletti Estrada, A. (2016). Seguridad en Redes. Madrid, Moralzarzal.

Edgeworth, B. (2014). "IP Routing on Cisco IOS, IOS XE, and IOS XR: An Essential Guide to Understanding and Implementing IP Routing Protocols".

Edwards, J., & Bramante, R. (2009). Networking self-teaching guide. Indianapolis, IN: Wiley Pub.

Hartpence, B. (2013). Packet Guide to Voice over IP: A system administrator's guide to VoIP technologies. " O'Reilly Media, Inc.".

Hersent, O., Petit, J. P., & Gurle, D. (2009). Beyond VoIP protocols: understanding voice technology and networking techniques for IP telephony. John Wiley & Sons.

H. Schulzrinne & S. Casner, (2003). RTP Profile for Audio and Video Conferences with Minimal Control. IETF. Obtenido de https://tools.ietf.org/html/rfc3551

IETF. (1992). TCP Extensions for High Performance. 03-08-2016, de IETF Sitio web: https://tools.ietf.org/html/rfc1323

Ietf.org. (2016). SIP: Session Initiation Protocol. [online] Available at: https://www.ietf.org/rfc/rfc3261 .txt [Accessed 3 Aug. 2016].

Khan, A., Smith, D., Hussein, S., & Helgert, H. (2012, January). Performance analysis of VoIP codecs over multi-rate EDCA. In Consumer Communications and Networking Conference (CCNC), 2012 IEEE (pp. 110-115). IEEE.

Q. Wu, F. Xia, & R. Even, (2012). RTP Control Protocol (RTCP) Extension for a Third-Party Loss Report. IETF. Obtenido de https://tools.ietf.org/html/rfc6642

Recommendation, G. (1988). 722: “7 kHz audio-coding within 64 kbit/s”. International Telecommunications Union

Sahabudin, S., & Alias, M. Y. (2009, December). End-to end delay performance analysis of various codecs on VoIP Quality of Service. In Communications (MICC), 2009 IEEE 9th Malaysia International Conference on (pp. 607-612). IEEE.

Simionovich, N. (2008). AsteriskNOW: A Practical Guide for Deploying and Managing an Asterisk-based Telephony System Using the AsteriskNOW Software Appliance. Packt Publishing.

Slay, J., & Simon, M. (2008, January). Voice over IP forensics. In Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop (p. 10). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

Tanenbaum, A. S., & Wetherall, D. J. (2010). Virtual private networks. Computer Networks, 821

ANEXOS

ANEXO A: LINEA DE COMANDOS PARA CONFIGURACION DE ROUTERS Y SWITCHS

R1:

```
conf t
hostname R1
no ip domain-lookup
line con 0
logging synchronous
exit
int g0/0.10
encapsulation dot1Q 10
ip add 192.168.1.1 255.255.255.0
no shut
int g0/0.20
encapsulation dot1Q 20
ip add 172.16.1.1 255.255.255.0
int g0/0
no shut
int g0/1
ip add 10.0.1.1 255.255.255.252
no shut
int s0/0/0
ip add 10.0.2.1 255.255.255.252
clock rate 8000000
no shut
exit
router eigrp 1
router-id 1.1.1.1
network 192.168.1.0 0.0.0.255
network 172.16.1.0 0.0.0.255
network 10.0.1.0 0.0.0.255
network 10.0.2.0 0.0.0.255
no auto-summary
passive-interface g0/0.10
passive-interface g0/0.10
exit
int g0/1
ip hello-interval eigrp 1 1
ip hold-time eigrp 1 3
int s0/0/0
ip hello-interval eigrp 1 1
ip hold-time eigrp 1 3
```

R2:

```
conf t
hostname R2
no ip domain-lookup
line con 0
logging synchronous
exit
int g0/0.10
encapsulation dot1Q 10
ip add 192.168.2.1 255.255.255.0
no shut
int g0/0.20
encapsulation dot1Q 20
ip add 172.16.2.1 255.255.255.0
int g0/0
no shut
int g0/1
ip add 10.0.1.2 255.255.255.252
no shut
int s0/0/1
ip add 10.0.3.1 255.255.255.252
no shut
exit
router eigrp 1
router-id 2.2.2.2
network 192.168.2.0 0.0.0.255
network 172.16.2.0 0.0.0.255
network 10.0.1.0 0.0.0.255
network 10.0.3.0 0.0.0.255
no auto-summary
passive-interface g0/0.10
passive-interface g0/0.20
 exit
int g0/1
ip hello-interval eigrp 1 1
ip hold-time eigrp 1 3
int s0/0/1
ip hello-interval eigrp 1 1
ip hold-time eigrp 1 3
```

R3:

conf t

hostname R3

no ip domain-lookup

line con 0

logging synchronous

exit

ip domain-name telefoniaIP.com

crypto key generate rsa modulus 1024

username user privilege 15 secret password

line vty 0 4

login local

transport input ssh

int s0/0/0

ip add 10.0.2.2 255.255.255.252

no shut

int s0/0/1

ip add 10.0.3.2 255.255.255.252

clock rate 8000000

no shut

exit

router eigrp 1

router-id 3.3.3.3

network 10.0.2.0 0.0.0.255

network 10.0.3.0 0.0.0.255

no auto-summary

exit

int s0/0/0

ip hello-interval eigrp 1 1

ip hold-time eigrp 1 3

int s0/0/1

ip hello-interval eigrp 1 1

ip hold-time eigrp 1 3

S1 y S2:

conf t

hostname S2 //o S1

vlan 10

name TELEPHONY

vlan 20

name DATA

exit

int range f0/1-12

switchport mode access

switchport access vlan 10

int range f0/13-24

switchport mode access

switchport access vlan 10

int g0/1

switchport mode trunk

ANEXO B: TABLA DE PROMEDIOS DE LAS PRUEBAS REALIZADAS PARA LOS TRES CODECS ANALIZADOS

	PROMEDIO GSM	PROMEDIO G722	PROMEDIO PCMA
	all packets	all packets	all packets
00:00,0	3	3,3	4,2
00:00,1	5,7	6,3	5,9
00:00,2	7,5	11,2	11,8
00:00,3	7,7	8,9	8,2
00:00,4	7,4	8,6	8,2
00:00,5	7,4	9,1	8,5
00:00,6	7,7	10,1	9,2
00:00,7	7,8	14,2	14,2
00:00,8	8,2	13,7	12,8
00:00,9	8	14,8	13,3
00:01,0	8,2	14,7	14,4
00:01,1	9,4	15,5	13,7
00:01,2	10	14,9	14,3
00:01,3	9,9	17,5	16,9
00:01,4	9,9	17,5	16,4
00:01,5	10,4	17	16,2
00:01,6	10,2	17,9	15,4
00:01,7	10	18,4	16,9
00:01,8	10	17,6	17,3
00:01,9	10	17	16,3
00:02,0	10	17,9	16,1
00:02,1	10,1	17,2	17
00:02,2	9,9	17,9	18
00:02,3	9,9	17,6	16,7
00:02,4	10,1	18,4	16,2
00:02,5	10	18	16,2
00:02,6	10	17,3	18
00:02,7	9,9	18,2	17,1
00:02,8	10,2	18,6	16,8
00:02,9	9,9	18	17,6
00:03,0	10	17,7	17,7
00:03,1	10	18,3	15,9
00:03,2	9,9	18,9	16,1
00:03,3	10,1	17,5	17,5
00:03,4	10,1	18,8	17,2
00:03,5	9,9	17,5	15,7
00:03,6	10	18,4	16,1
00:03,7	10	17,7	17,7
00:03,8	10	18,1	16,7
00:03,9	10	18,1	17,3
00:04,0	10	18,4	17,3
00:04,1	10,1	16,7	17,4
00:04,2	9,9	18,6	17,6
00:04,3	10	18,1	16,9
00:04,4	10	17,4	16,9
00:04,5	10	18,6	17,8
00:04,6	10	17,6	17,3
00:04,7	10,1	18,3	16,3
00:04,8	10,2	17,9	16,5
00:04,9	9,9	21,4	19,9
00:05,0	10,8	18	16,6
00:05,1	10,2	17,7	16,8
00:05,2	10,1	17,7	17,6
00:05,3	10,1	19,3	17,5
00:05,4	10	18,2	16,2
00:05,5	9,8	18,5	17,7
00:05,6	10,1	18,7	15,4
00:05,7	10	18,5	16,9
00:05,8	10,1	18,2	16,6
00:05,9	10,1	17,2	16,8
00:06,0	10,1	17,9	15,9
00:06,1	9,9	18,5	15,9
00:06,2	10	19,2	16,1
00:06,3	10	17,5	16,8
00:06,4	10	17,5	15,6
00:06,5	10,1	18,3	15,5

Continua…

00:06,6	10,2	17,6	16,1
00:06,7	9,9	18	15,4
00:06,8	10,1	18,3	15,7
00:06,9	10	18,7	15,6
00:07,0	10	17,6	15,7
00:07,1	10,1	18,7	16,8
00:07,2	10	18,1	16,4
00:07,3	10	19,4	15,9
00:07,4	10,1	17,8	16,6
00:07,5	10	18,8	16,9
00:07,6	10	18,7	15
00:07,7	10	17,9	16
00:07,8	9,9	18,9	16,6
00:07,9	10,2	18	16,3
00:08,0	10	18,6	16,3
00:08,1	10,1	18,1	15,5
00:08,2	10	18,3	16,8
00:08,3	10	18,2	16,4
00:08,4	10	17,8	15,9
00:08,5	10,1	18,5	16
00:08,6	10	18	16,5
00:08,7	10,1	18	16,1
00:08,8	10,1	18	16,9
00:08,9	10,1	18,3	15,3
00:09,0	10	21,4	20,1
00:09,1	10	21,1	19,1
00:09,2	10,2	17,9	15,7
00:09,3	9,8	17,7	16,9
00:09,4	10,2	18,3	16,7
00:09,5	10,2	19,5	17,4
00:09,6	10,1	19,2	16,9
00:09,7	10	18,1	17,1
00:09,8	10,1	19,1	17,2
00:09,9	10,1	18,2	17
00:10,0	10,8	18	16,5
00:10,1	10,3	17,9	16,4
00:10,2	10,1	18,9	17,1
00:10,3	10	18,5	16
00:10,4	10	17,9	16,3
00:10,5	10,1	18	15,9
00:10,6	9,9	18,3	17
00:10,7	10,1	17,1	15,7
00:10,8	10,1	17,8	14,7
00:10,9	10	17,2	16,9
00:11,0	10	18,3	17
00:11,1	10	17,3	16,2
00:11,2	10	17,3	15
00:11,3	10	17,5	16,5
00:11,4	10	17,2	17,4
00:11,5	10	17,9	16,3
00:11,6	10,1	17,6	15,7
00:11,7	10,1	17,7	16,8
00:11,8	9,9	16,4	17
00:11,9	10	17,6	16,3
00:12,0	11	19,5	18,7
00:12,1	10	19,1	17,2
00:12,2	10,2	17	17,8
00:12,3	9,9	17,8	16,3
00:12,4	10,2	17,5	16,1
00:12,5	9,9	17	17,7
00:12,6	10	17,6	17,7
00:12,7	10,1	18,3	17,4
00:12,8	9,9	17,5	16,4
00:12,9	10,2	17	18,2
00:13,0	10,1	17,7	16,9
00:13,1	9,9	17,4	16,3
00:13,2	10	20,1	17,1
00:13,3	10	18,9	16,1
00:13,4	10,1	17,4	17,2
00:13,5	10	18,1	17,1
00:13,6	10	17,2	16,8
00:13,7	10,2	18,4	16,4
00:13,8	9,9	18,3	17,3
00:13,9	9,9	17,9	17,6
00:14,0	10,1	17,6	16,3

Continua…

00:14,1	10	18,7	15,9
00:14,2	9,9	18,1	16,6
00:14,3	10,2	17,7	16,4
00:14,4	10,1	17,5	16
00:14,5	10	17,1	16
00:14,6	10	18,4	17,5
00:14,7	10	18,4	16,4
00:14,8	10,1	17	17
00:14,9	10,1	17,6	16,1
00:15,0	10,7	17,9	16,9
00:15,1	10,1	17,1	16,6
00:15,2	10	17,7	17,6
00:15,3	10	17,9	17
00:15,4	10	18,4	16,7
00:15,5	9,9	16,2	17,5
00:15,6	10,2	18,2	16,5
00:15,7	10	17,8	16,7
00:15,8	10	18,3	16,6
00:15,9	10	17,3	17,2
00:16,0	10	18,5	16,7
00:16,1	9,8	18,5	17,4
00:16,2	10,3	18,2	16,5
00:16,3	9,9	17,5	16,7
00:16,4	10,3	18,4	16,5
00:16,5	10	18,1	16,5
00:16,6	10	17,1	17
00:16,7	10	18,5	16,7
00:16,8	9,9	18,4	17
00:16,9	10,2	18,3	18,9
00:17,0	9,9	17,9	20
00:17,1	10	17,9	19,3
00:17,2	10	17,8	17,8
00:17,3	10	17,6	18,1
00:17,4	9,9	23,1	18,5
00:17,5	10,1	17,9	18
00:17,6	10,1	17,7	16,1
00:17,7	9,9	16,9	17,6
00:17,8	10	17,5	16,6
00:17,9	10	18,1	16,5
00:18,0	10	18,6	16,8
00:18,1	10	16,8	15,8
00:18,2	10,1	18,7	15,5
00:18,3	10	17,1	16,1
00:18,4	9,9	17,6	17
00:18,5	10	16,3	17
00:18,6	10	16,7	17,7
00:18,7	10	17,5	16,6
00:18,8	10	16,4	17,2
00:18,9	10,1	16,8	16,7
00:19,0	9,9	17,3	16,8
00:19,1	10	17,2	16,6
00:19,2	9,9	16,9	16,1
00:19,3	10,1	17	16,8
00:19,4	10,2	17,1	16,9
00:19,5	10,2	17,3	16,9
00:19,6	10	16,6	17,1
00:19,7	10,1	17,1	17,8
00:19,8	10,2	17,4	17,3
00:19,9	10	18,2	16,9
00:20,0	10	17,4	16,8
00:20,1	10,3	17,9	17,7
00:20,2	10	17,4	17,8
00:20,3	10,1	17,3	17,9
00:20,4	10	17,2	17,8
00:20,5	10	17,1	17
00:20,6	10	17,5	17,2
00:20,7	10	17,2	17,3
00:20,8	10,1	17,2	17,6
00:20,9	10	17,9	19,1
00:21,0	6,9	15,5	15,6
00:21,1	5	5,8	7
00:21,2	5,1	5,7	5,8
00:21,3	4,7	5,9	5,7
00:21,4	5,1	5,7	5,8
00:21,5	5,2	5,8	5,7

Continua…

00:21,6	5	5,7	5,9
00:21,7	5,1	5,9	5,7
00:21,8	4,8	5,5	5,7
00:21,9	4,8	5,9	5,8
00:22,0	5,1	5,8	5,7
00:22,1	5	5,9	5,8
00:22,2	5,2	5,7	5,8
00:22,3	5	5,8	5,8
00:22,4	4,8	5,7	5,7
00:22,5	5,2	5,9	5,8
00:22,6	4,8	5,6	5,6
00:22,7	5	5,7	5,9
00:22,8	5,4	5,9	5,9
00:22,9	4,7	5,9	5,9
00:23,0	5	5,5	5,6
00:23,1	5,2	5,9	6,2
00:23,2	4,7	6,2	5,7
00:23,3	5	5,8	6
00:23,4	5,5	6	5,9
00:23,5	5,1	5,9	6,2
00:23,6	5,1	6	6,5
00:23,7	5,6	5,9	5,8
00:23,8	5,5	7	6,3
00:23,9	6,3	7,5	9,4
00:24,0	6,1	8,2	12,2
00:24,1	6,3	10,1	12,7
00:24,2	6,9	14,4	13,1
00:24,3	6,5	16,4	14,9
00:24,4	8	16,8	16
00:24,5	8,2	18,3	17
00:24,6	8,9	18,4	14,3
00:24,7	10,4	18,4	13,9
00:24,8	10,2	18,9	15,7
00:24,9	10,3	19,6	18,2
00:25,0	10,1	19,5	18,2
00:25,1	10,2	18,9	17,1
00:25,2	10,2	19,4	17,7
00:25,3	10,1	18,8	18,9
00:25,4	10	19,2	20,1
00:25,5	10	20	17,3
00:25,6	10	19,6	17,4
00:25,7	10	20,3	18,8
00:25,8	10,1	22,7	18,4
00:25,9	10	18,8	17,7
00:26,0	10,1	18,7	17,7
00:26,1	9,9	19,2	17,9
00:26,2	10	17,7	17,3
00:26,3	10,1	19,2	17,1
00:26,4	10	18,8	17,2
00:26,5	10,1	18,7	16,8
00:26,6	10	18,4	17,1
00:26,7	9,9	17,8	17
00:26,8	10	18,4	16,9
00:26,9	10	17,6	17,3
00:27,0	10	18,3	17,6
00:27,1	10,1	19	17,5
00:27,2	10,1	18,1	17,4
00:27,3	10	18,3	17,4
00:27,4	10	18	17,5
00:27,5	10	18,9	17,6
00:27,6	10,1	19,7	17,2
00:27,7	10	19,6	17
00:27,8	10	18,3	17,4
00:27,9	10	18,4	16,6
00:28,0	10	18,6	16,9
00:28,1	10	18	17
00:28,2	10	18,7	17,9
00:28,3	10,1	18,9	17,3
00:28,4	10	18,3	17,3
00:28,5	10,1	17,8	17
00:28,6	10	17,9	17,9
00:28,7	10	18,9	17,7
00:28,8	10	19,3	16,7
00:28,9	10	18,8	17,2
00:29,0	10	18,9	17,2

Continua…

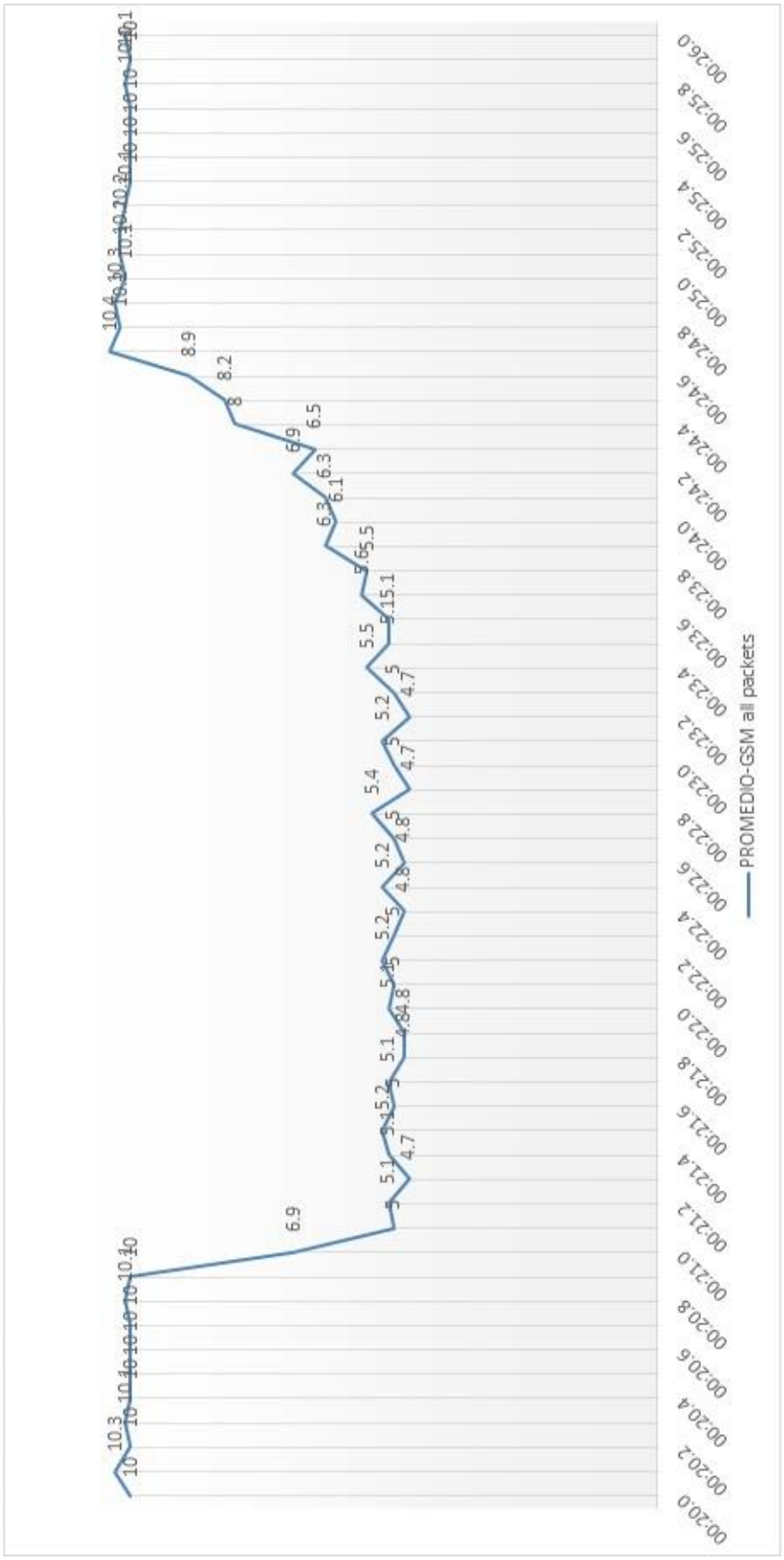
00:29,1	10	18,5	16,8
00:29,2	10	18,8	17,2
00:29,3	10,1	18,9	17,8
00:29,4	10,1	18,8	17,2
00:29,5	10,2	18,9	19
00:29,6	9,9	18,5	18,7
00:29,7	10,3	19,2	17,8
00:29,8	10,2	19	17,2
00:29,9	9,9	18,9	17,9
00:30,0	10	21,2	17,6
00:30,1	10,2	18,7	17,5
00:30,2	10	18,3	17,9
00:30,3	10,1	18,2	16,7
00:30,4	10,2	18	16
00:30,5	9,9	17,7	17,4
00:30,6	10,1	17,6	17
00:30,7	10	17	16,7
00:30,8	10	17,5	17,1
00:30,9	10	17,8	17,4
00:31,0	10	18,4	17,3
00:31,1	10,2	17,7	16,2
00:31,2	9,8	18,2	17,5
00:31,3	10	18,1	18
00:31,4	10	18	17,6
00:31,5	10,1	18,1	16,4
00:31,6	9,9	17,6	16,6
00:31,7	10,1	17,3	17,1
00:31,8	9,9	17,2	16,8
00:31,9	10,1	17,3	17
00:32,0	10	17,9	16,8
00:32,1	10	17	17
00:32,2	10	17,8	16,8
00:32,3	10	17,5	16,2
00:32,4	10	17,2	17,4
00:32,5	10	17,7	17,7
00:32,6	10	18,6	17
00:32,7	10	18,1	17,1
00:32,8	10	18,6	17,2
00:32,9	10,1	18,8	18,3
00:33,0	9,9	18,6	18,2
00:33,1	10	18,3	17,7
00:33,2	9,9	17,4	17,5
00:33,3	10,1	19,1	17,5
00:33,4	10,1	19,3	17,6
00:33,5	10	18,2	16,8
00:33,6	10	18,9	17,9
00:33,7	10	18,3	19,7
00:33,8	10	18,7	18,2
00:33,9	10,1	18,9	17,1
00:34,0	9,9	19,4	18,2
00:34,1	10,1	20,7	19
00:34,2	10,1	21,5	17,5
00:34,3	10,1	17,2	16,9
00:34,4	10	18,3	17,6
00:34,5	10,2	18,2	16,3
00:34,6	10	17,3	16,9
00:34,7	10	17,9	17,1
00:34,8	10,3	17,9	16,9
00:34,9	10,2	17,5	16,4
00:35,0	9,9	17,2	17,1
00:35,1	10,2	17,5	17,2
00:35,2	10,2	18,4	16,8
00:35,3	9,9	18,1	17,1
00:35,4	10,3	18,6	16,8
00:35,5	10,2	18,9	16,9
00:35,6	9,9	18,2	18,8
00:35,7	10,1	18	17,3
00:35,8	10,2	17,7	17
00:35,9	10	18,2	16,6
00:36,0	10	18,8	17,7
00:36,1	10,3	18,3	17,2
00:36,2	10,3	17	17,5
00:36,3	9,9	17,6	17
00:36,4	10	17,5	16,4
00:36,5	10	17,9	16,3

Continua…

00:36,6	10	17,1	17,2
00:36,7	10	17,5	17,1
00:36,8	10,1	17,2	17
00:36,9	10	17,2	17,3
00:37,0	10	18,2	17,3
00:37,1	10	18,5	17,6
00:37,2	10	18	17,2
00:37,3	10	18,1	16,8
00:37,4	10,1	17,7	17,2
00:37,5	10,1	18,4	16,8
00:37,6	10	18	17,1
00:37,7	10	18,2	17,3
00:37,8	10	17,6	18,1
00:37,9	10	17,9	18,6
00:38,0	10	17	17,2
00:38,1	10,1	17,8	17,3
00:38,2	9,9	18	18
00:38,3	10	19,1	17,6
00:38,4	10	20,5	17
00:38,5	10	16,8	16,9
00:38,6	10	17,4	17,3
00:38,7	10	17,1	16,8
00:38,8	10,1	17,2	16,4
00:38,9	9,9	17,4	16,4
00:39,0	10	16,8	16,6
00:39,1	10	18,3	17,8
00:39,2	10	18,4	16,2
00:39,3	10,1	16,9	16,8
00:39,4	10,1	16,7	17,1
00:39,5	10,1	18,8	16,2
00:39,6	10	17,3	16,5
00:39,7	10,2	18,1	15,6
00:39,8	10,2	17,3	15,5
00:39,9	9,9	16,6	13,5
00:40,0	9,3	16,9	15,71428571
00:40,1	10	17,1	16
00:40,2	10,22222222	16,5	16,16666667
00:40,3	10	16,9	15
00:40,4	10	16	14,83333333
00:40,5	10	16,9	12,5
00:40,6	10,22222222	15,1	11
00:40,7	9,555555556	18	14,25
00:40,8	7,777777778	17,875	11,5
00:40,9	7,5	18	11
00:41,0	5,666666667	14,25	11,5
00:41,1	5,5	14,85714286	
00:41,2	4	14,85714286	
00:41,3		14	
00:41,4		14,5	
00:41,5		14,8	
00:41,6		16	
00:41,7		5	

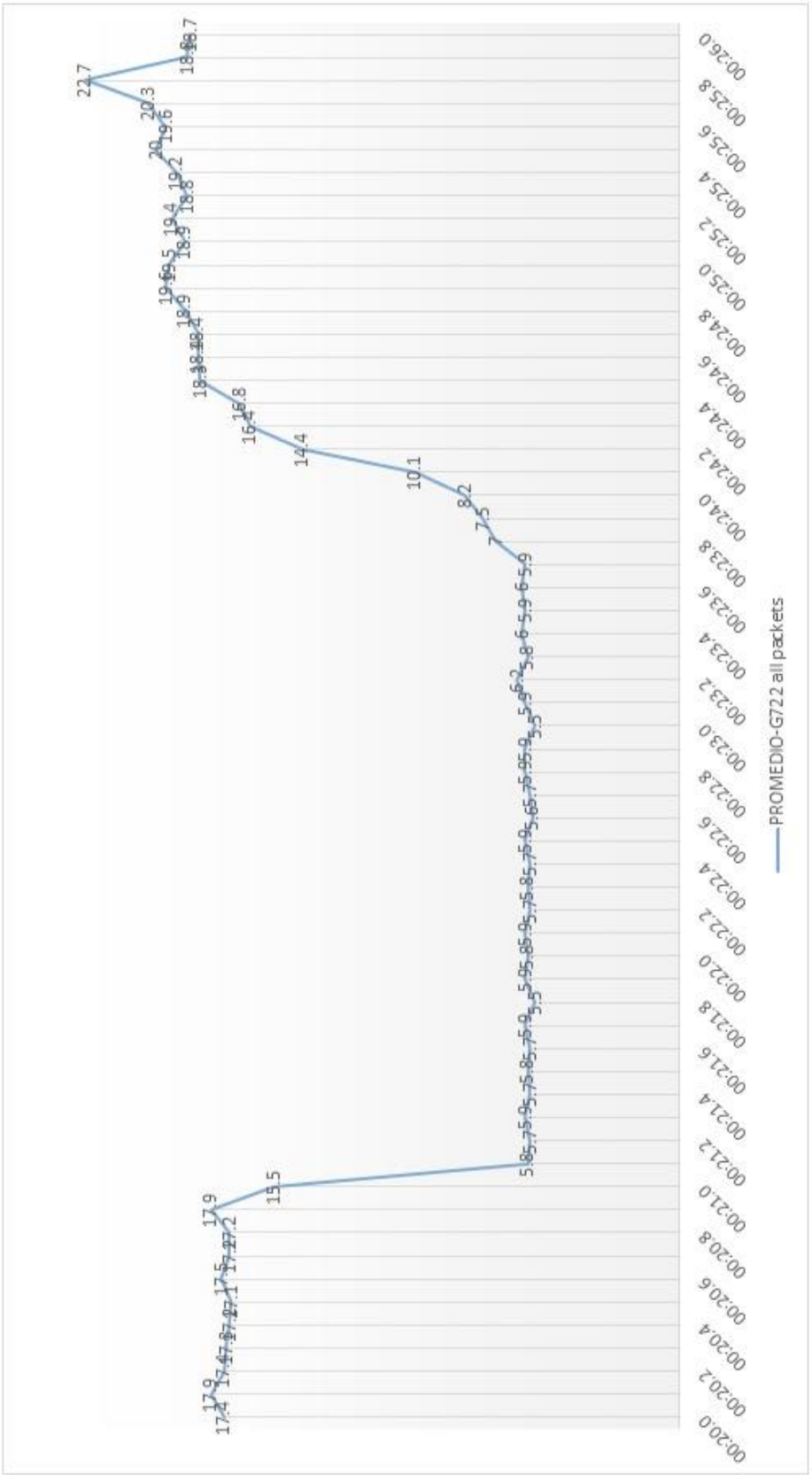
Elaboración: Propia

ANEXO C: ACERCAMIENTO DE FLUJO CON CÓDEC GSM



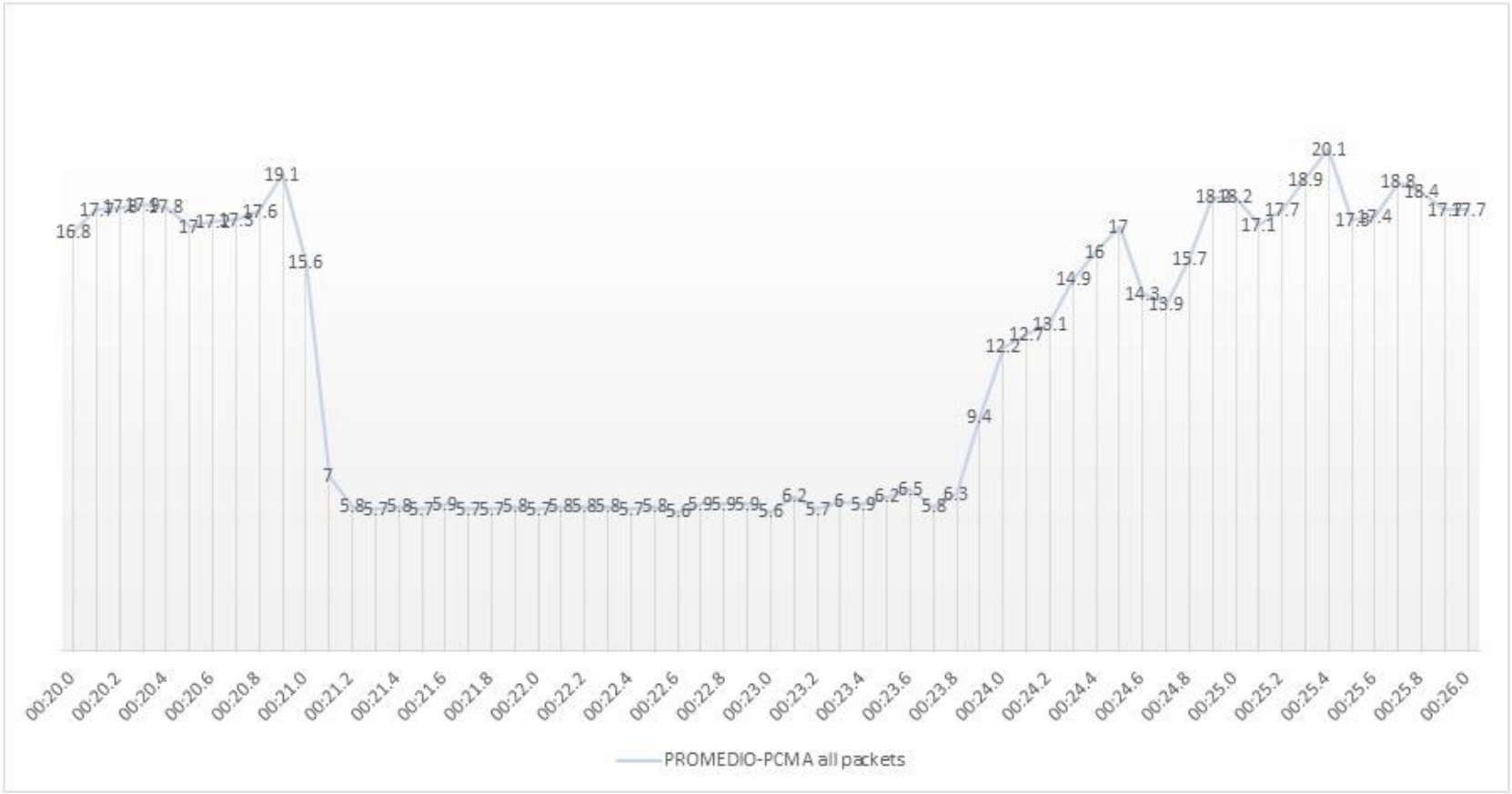
Elaboración: Propia

ANEXO D: ACERCAMIENTO DE FLUJO CON CÓDEC G722



Elaboración: Propia

ANEXO E: ACERCAMIENTO DE FLUJO CON CÓDEC PCMA



Elaboración: Propia