ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

ESCUELA DE POSTGRADO Y EDUCACION CONTINUA

MAESTRIA EN INTERCONECTIVIDAD DE REDES

PROYECTO DE TESIS

"ANALISIS DE MECANISMOS DE GESTION DE CLAVE PARA LA PROTECCION DE CONTENIDOS DE VOZ SOBRE EL PROTOCOLO IP"

Realizado por:

PATRICIO JAVIER RUIZ ANDINO

RIOBAMBA – ECUADOR

2012

DERECHOS DE AUTORÍA

Yo, Patricio Javier Ruiz Andino, soy responsable de las ideas, doctrinas y resultados expuestos en esta Tesis; y el patrimonio intelectual de la Tesis de Grado pertenece a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO.

_____

Ing. Patricio Javier Ruiz Andino

ÍNDICE GENERAL

ÍNDICE DE FIGURAS ..... **VIII**

INDICE DE ABREVIATURAS ..... **IX**

RESUMEN ..... **XII**

ABSTRACT ..... **XIII**

CAPÍTULO I **14**

INTRODUCCIÓN **14**

1.1 PROBLEMA DE LA INVESTIGACIÓN 15
1.2 JUSTIFICACIÓN 16
1.3 OBJETIVOS 18
1.3.1 OBJETIVO GENERAL 18
1.3.2 OBJETIVOS ESPECÍFICOS 18
1.4 ALCANCE 19

CAPÍTULO II **20**

REVISIÓN DE LA LITERATURA **20**

2.1 INTRODUCCIÓN A LA TELEFONÍA 20
2.1.1 PRINCIPIOS Y TRANSMISIÓN DE VOZ 20
2.1.2 REDES ORIENTADAS A CIRCUITOS Y ORIENTADAS A PAQUETES 21
2.1.3 DTMFs 22
2.1.4 INTRODUCCIÓN A VoIP 23
2.2 SRTP 29
2.3 MECANISMOS DE GESTIÓN DE CLAVE 34
2.3.1 DESCRIPCIÓN DE SEGURIDAD SRTP 36
2.3.2 ZRTP 40
2.4 ASPECTOS RELEVANTES DEL ESTÁNDAR 43
2.4.1 REQUISITOS DE UN PROTOCOLO DE GESTION DE CLAVE 43
2.4.2 PROTOCOLO DE CAMBIO DE CLAVES 45
2.4.3 RENDIMIENTO 47

CAPÍTULO III **49**

MATERIALES Y MÉTODOS **49**

3.1 TIPO DE LA INVESTIGACIÓN 49

3.2 DISEÑO DE LA INVESTIGACIÓN 49
3.3 MÉTODOS Y TÉCNICAS 51
3.3.1 MÉTODOS 51
3.3.2 TÉCNICAS 51
3.4 FUENTES DE INFORMACIÓN 51
3.5 RECURSOS 51
3.5.1 RECURSOS HUMANOS 51
3.5.2 RECURSOS TÉCNICOS 52
3.5.3 RECURSOS MATERIALES 53
3.5.4 RECURSOS ECONÓMICOS 53
3.6 PLANTEAMIENTO DE LA HIPÓTESIS 54
3.7 OPERACIONALIZACIÓN DE LAS VARIABLES 54
3.7.1 OPERACIONALIZACIÓN CONCEPTUAL 54
3.7.2 OPERACIONALIZACIÓN METODOLÓGICA 56
3.8 POBLACIÓN Y MUESTRA 56
3.9 INSTRUMENTOS DE RECOLECCIÓN DE DATOS 56

CAPÍTULO IV 62

RESULTADOS Y DISCUSIÓN 62

4.1 VARIABLE INDEPENDIENTE 62
4.1.1 DETERMINACIÓN DE PARÁMETROS DE COMPARACIÓN 62
4.1.2 PROCESAMIENTO DE LA INFORMACIÓN 76
4.1.3 ANÁLISIS Y PRESENTACIÓN DE RESULTADOS 76
4.2 VARIABLE DEPENDIENTE 79
4.2.1 PAQUETES TRANSMITIDOS Y RECIBIDOS 79
4.2.3 ANCHO DE BANDA 81
4.2.4 USO DE MEMORIA 82
4.2.5 JITTER 83
4.2.6. PAQUETES PERDIDOS 84
4.3 PRUEBA DE LA HIPÓTESIS 85
4.3.1 PLANTEAMIENTO DE LA HIPÓTESIS 85
4.3.3 ZONA DE RECHAZO 86
4.3.4 CÁLCULOS 86
4.3.5 DECISIÓN 87

CAPÍTULO V 88

GUIA REFERENCIAL 88

5.1. INTRODUCCIÓN 88
5.2. DEFINICIONES 88
5.3. CONFORMIDAD Y RENDIMIENTO 89
5.4. FASE 1: TAREAS PRELIMINARES 90
5.4.1. DETERMINAR EL TIPO DE ANALISIS 90
5.4.2. IDENTIFICACIÓN DE LOS RECURSOS NECESARIOS 91
5.5. FASE 2: DOCUMENTACIÓN PRELIMINAR 91
5.6. FASE 3: ANÁLISIS DEL ESTÁNDAR 92
5.7. FASE 4: VALIDACIÓN DE LA CONFORMIDAD 92
5.7.1. IDENTIFICACIÓN DE LOS MECANISMOS CRIPTOGRÁFICOS 93
5.7.2. IDENTIFICACIÓN DE LAS CARACTERÍSTICAS OBLIGATORIAS 93
5.8. FASE 5: EVALUACIÓN DEL RENDIMIENTO 93
5.8.1. RENDIMIENTO DE LOS MECANISMOS CRIPTOGRÁFICOS 94
5.8.2. IDENTIFICACIÓN DE PARÁMETROS DEPENDIENTES DEL TRÁFICO 94
5.8.3. IDENTIFICACIÓN DE PARÁMETROS INDEPENDIENTES DEL TRÁFICO 94
5.9. FASE 6: DISEÑO DE PRUEBAS 95
5.10. FASE 7: OTRAS CONSIDERACIONES 96
5.11. FASE 8: TAREAS FINALES 97

CONCLUSIONES 99

RECOMENDACIONES 100

BIBLIOGRAFÍA 101

BIBLIOGRAFÍA DE LIBROS 101

BIBLIOGRAFÍA DE INTERNET 103

ANEXOS 105

Anexo 1: INSTALACION DE ASTERISK 1.8.7 EN UN VPS
Anexo 2: PARAMETROS DE NEGOCIACION ZRTP
Anexo 3: RESUMEN DE REQUERIMIENTOS DE SEGURIDAD
Anexo 4: DATOS RECOLECTADOS DE LAS PRUEBAS

ÍNDICE DE TABLAS

TABLA 1 FRECUENCIAS PARA CADA DÍGITO. 22
TABLA 2 CÓDEC OVERHEAD 26
TABLA 3 MÉTODOS EN LA SEÑALIZACIÓN SIP 27
TABLA 4 RECURSOS MATERIALES. 53
TABLA 5 RECURSOS ECONÓMICOS A UTILIZARSE EN EL PROYECTO 53
TABLA 6 OPERACIONALIZACIÓN DE LAS VARIABLES DEL PROYECTO DE INVESTIGACIÓN 54
TABLA 7 OPERACIONALIZACIÓN METODOLÓGICA DE LAS VARIABLES. 56
TABLA 8 EQUIPOS UTILIZADOS PARA LLAMADAS IP PARA EL TEST DE CONTROL. 57
TABLA 9 SOFTWARE UTILIZADO PARA LA LLAMADA IP 58
TABLA 10 EQUIPOS UTILIZADOS PARA LLAMADAS IP CON MECANISMOS. 59
TABLA 11 SOFTWARE UTILIZADO PARA LA LLAMADA IP CON MECANISMOS. 60
TABLA 12 SINTAXIS PARA USO DE HERRAMIENTAS SYSSTAT. 61
TABLA 13 CORRESPONDENCIAS PARA LOS NIVELES DE SEGURIDAD. 63
TABLA 14 ESCALA CUANTITATIVA. VARIABLE INDEPENDIENTE. 63
TABLA 15 RESULTADOS ESPECIFICACIÓN MÓDULO CRIPTOGRÁFICO. 65
TABLA 16 RESULTADOS PUERTOS E INTERFACES DEL MÓDULO CRIPTOGRÁFICO. 66
TABLA 17 RESULTADOS CON RESPECTO A LAS FUNCIONES 67
TABLA 18 MODELO DE ESTADO FINITO. 68
TABLA 19 SEGURIDAD FÍSICA. 69
TABLA 20 ENTORNO OPERACIONAL. 70
TABLA 21 GESTIÓN DE CLAVE CRIPTOGRÁFICA 71
TABLA 22 EMI/EMC 72
TABLA 23 SELFT TESTS. 73
TABLA 24 ASEGURAMIENTO DEL DISEÑO 74
TABLA 25 MITIGACIÓN DE ATAQUES. 75
TABLA 26 INDICADORES Y NIVELES DE SEGURIDAD ZRTP. 76
TABLA 27 INDICADORES Y NIVELES DE SEGURIDAD SDESCRIPTIONS. 77
TABLA 28 MEDIA DE PAQUETES RECIBIDOS Y TRANSMITIDOS. 80
TABLA 29 TIEMPO DE CPU. 80
TABLA 30 ANCHO DE BANDA. 81
TABLA 31 USO DE MEMORIA. 82
TABLA 32 JITTER. 83
TABLA 33 PORCENTAJE DE PAQUETES PERDIDOS. 84

TABLA 34 ESTADÍSTICOS DE MUESTRAS RELACIONADAS. 86
TABLA 35 CORRELACIONES DE MUESTRAS RELACIONADAS. 86
TABLA 36 PRUEBAS DE MUESTRAS RELACIONADAS. 86

ÍNDICE DE FIGURAS

FIGURA 1 COMPONENTES END-TO-END DE VOIP. 23
FIGURA 2 PROTOCOLOS VOIP. 25
FIGURA 3 SOBRECARGA DE PROTOCOLO USANDO G.711. 25
FIGURA 4 ENCABEZADO RTP. 28
FIGURA 5 CODIFICACIÓN/DECODIFICACIÓN 31
FIGURA 6 FORMATO DEL PAQUETE SRTP 32
FIGURA 7 NEGOCIACIÓN DE CLAVE USANDO SDESCRIPTIONS EN SIP 33
FIGURA 8 SIP AND SDESCRIPTIONS. 37
FIGURA 9 SECURITY DESCRIPTIONS SIN VALORES LIFETIME O MKI. 38
FIGURA 10 SECURITY DESCRIPTIONS CON VALORES LIFETIME Y MKI. 38
FIGURA 11NEGOCIACIÓN DE CLAVE ZRTP USANDO EL MODO DIFFIE-HELLMAN 41
FIGURA 12 LLAMADA VOIP SIN MECANISMO. 57
FIGURA 13 LLAMADA VOIP CON MECANISMO. 59
FIGURA 14 PORCENTAJE DE MÓDULO CRIPTOGRÁFICO. 65
FIGURA 15 RESULTADOS PUERTOS E INTERFACES DEL MÓDULO CRIPTOGRÁFICO 66
FIGURA 16 RESULTADOS FUNCIONES SERVICIOS Y AUTENTIFICACIÓN. 67
FIGURA 17 RESULTADOS DEL MODELO DE ESTADO FINITO. 68
FIGURA 18 RESULTADOS DE LA SEGURIDAD FÍSICA. 69
FIGURA 19 RESULTADOS DE ENTORNO OPERACIONAL 70
FIGURA 20 RESULTADOS DE GESTIÓN DE CLAVE CRIPTOGRÁFICA. 71
FIGURA 21 RESULTADOS DE EMI/EMC 72
FIGURA 22 RESULTADOS DE SELFT TEST. 73
FIGURA 23 RESULTADOS DE ASEGURAMIENTO DE DISEÑO. 74
FIGURA 24 RESULTADOS DE MITIGACIÓN A OTROS ATAQUES. 75
FIGURA 25 NIVELES DE SEGURIDAD – RESULTADOS. 77
FIGURA 26 PAQUETES ENVIADOS Y TRANSMITIDOS. 80
FIGURA 27 DESOCUPACIÓN DE CPU. 81
FIGURA 28 ANCHO DE BANDA. 81
FIGURA 29 PORCENTAJE DE USO DE MEMORIA. 82
FIGURA 30 PORCENTAJE JITTER 83
FIGURA 31 PORCENTAJE DE PAQUETES PERDIDOS. 84
FIGURA 32 DIAGRAMA DE FLUJO QUE INCLUYEN LAS OCHO FASES DE LA GUÍA REFERENCIAL 98

INDICE DE ABREVIATURAS

ACK.- Acknowledgement – Acuse de recibo

ADSL.- Asymmetric Digital Subscriber Line – Línea de abonado digital asimétrica

AMG.- Access Media Gateway

API.- Application Programming Interface – Interfaz de programación de aplicaciones

BLSR.- Bi-directional Line Switched Ring – Línea bi-direccional conmutado de anillo

CC.- Circuit Switching–Conmutación de circuitos

CNG.- Comfort Noise Generation – generación de ruido confortable.

CP.- Packet Switching – Conmutación de Paquetes

DSL.- Digital Subscriber Line – Línea de suscripción digital

DSP.- Digital Signal Processor – Procesador digital de señal

DTMF.- Dual Tone Multifrecuency – Multifrecuencia de doble tono

ETSI.- European Telecommunications Standards Institute – Instituto Europeo de Normas de Telecomunicaciones

FTP.- File Transport Protocol

IETF.- Internet Engineering Task Force – Grupo Especial sobre Ingeniería de Internet

IM.- Instant Messaging – Mensajería instantánea

IP.-Internet Protocol – Protocolo de Internet

IETF.- Internet Engineering Task Force

ISDN.- Integrated Services Digital Network – Red Digital de Servicios Integrados

ITU.-International Telecommunication Union– Unión Internacional de Telecomunicaciones

MGC.- Media Gateway Controller

MGCP.- Media Gateway Control Protocol

MKI.- Master Key Identifier – identificador de clave maestra.

MMUSIC.- Multiparty Multimedia Session Control

MPLS.- Multi Protocol Label Switching– Conmutación de etiquetas multiprotocolo

NAT.- Network Address Translation – Traducción de Dirección de Red

NGN.- Next Generation Network – Red de Próxima Generación

PBX.- Private Branch Exchange –Central Secundaria Privada Automática

PIN.- Número de identificación personal

PSTN.- Public switched telephone network– Red Pública Telefónica Conmutada

QoS.- Quality of Service – Calidad del servicio

RFC.- Request for Commen – Solicitud de comentario

RT .- Redundant Trees – ArbolesRedundantes

RTCP.- Real Time Transport Protocol–Protocolo de transporte en tiempo real

RTP.- Real Time Protocol– Protocolo de Tiempo Real

SA.- Security Assosiations

SDES.- Session Description Protocol Security Descriptions for Media Streams

SDH.- Synchronous Digital Hierarchy – Jerarquía digital síncrona.

SDP.- Session Description Protocol.

SIGTRAN.- SignalingTransport – Señalizador de transporte

SIP.- Session Innitiation Protocol– Protocolo de iniciación de sesión

SMS.- Short Message Service– Servicio de mensajes cortos.

SRTP.- Security Real Transport Protocol

TCP.-Transmission Control Protocol– Protocolo de control de transmisión

TDM.- Time Division Multiplexing – Multiplexación por división de tiempo

UDP.- User Datagram Protocol – Protocolo de Datagrama de Usuario

VoIP.- VoiceOver Internet Protocol – Voz sobre un protocolo de internet

VPN.- Virtual Private Network – Red privada virtual

ZRTP.- Zinmmerman Real Transport Protocol

DEDICATORIA

A María Antonieta, mi madre, por su amor y motivación presente durante todo mi vida. A Wilson Fernando, mi padre por su manifestación ingente de compresión. A ellos un profundo y eterno agradecimiento pues sin su apoyo y esfuerzo mis metas no se hubiesen hecho realidad.

RESUMEN

La investigación: “Análisis de Mecanismos de Gestión de Clave para la Protección de Contenidos de Voz Sobre el Protocolo IP”, tuvo como finalidad elaborar una guía referencial que constó de ocho fases. Este estudio permitió determinar el nivel de rendimiento en servidores virtuales. En una primera etapa se determinó el nivel de seguridad de los mecanismos ZRTP y SDES. Se realizaron pruebas de llamadas sin utilizar encriptación de audio y posteriormente en el mismo escenario se utilizó el mecanismo SDES.

Se utilizó los métodos cuantitativo, cualitativo y comparativo. Se utilizaron los siguientes materiales, en elementos hardware: 2 computadoras y en software: Linux CentOS 6, Asterisk 1.8.7, Softphone Blink 0.2.7 como cliente SIP, además, el VPS. Las técnicas aplicadas fueron: test de rendimiento aplicado a llamadas realizadas y medidas con: SysStat, Vnstat y Channelsstat.

Mediante el uso del método “t–Student” con diferencia por parejas con un valor de 6 para los grados de libertad, la significancia bilateral para CPU fue de 0.0010 que es menor que 0.05, igual ocurre con la memoria, donde la significancia es menor a 0.05. Por lo tanto se rechaza la hipótesis nula, es decir que el nivel de rendimiento en el servidor de VoIP disminuye con la aplicación del mecanismo SDES.

Se concluye que al implantar SRTP Descriptions sobre el ambiente de pruebas, el nivel de rendimiento en el servidor privado virtual, disminuyó en un 0.12%.

Se recomienda utilizar un simulador para determinar el número de llamadas simultáneas que puede soportar la red, previo a implementarse VoIP en una empresa.

ABSTRACT

.

The research: "Analysis of Key Management Mechanisms for Content Protection Protocol Voice over IP", was developed to obtain a reference guide consisted of eight phases. This study determined the level of performance on virtual servers. In a first stage, it was determined the level of security mechanisms and SDES ZRTP. Tests were performed without using encryption calls recorded and subsequently on the same stage SDES mechanism was used.

It was used quantitative methods, qualitative and comparative. The following materials, such as hardware with 2 computers and software with Linux CentOS 6, Asterisk 1.8.7, 0.2.7 and Blink Softphone SIP client also the VPS were used. The techniques used were: performance test applied to calls made and measures: SysStat, vnstat and channelsstat.

By using the method "t-Student" by far in pairs with a value of 6 for the degrees of freedom, the CPU was bilateral significance of 0.0010 which is less than 0.05, so does the memory where the significance is less 0.05. Therefore the null hypothesis is rejected, meaning that the level of performance in the VoIP server decreases the mechanism SDES.

As conclusion, implementing SRTP descriptions on the test environment, the level of performance in the virtual private server was decreased by 0.12%.

It is recommended the use of a simulator to determine the number of simultaneous calls that can be carried on the network, implemented prior to VoIP in an enterprise.

CAPÍTULO I
INTRODUCCIÓN

En los negocios la seguridad de nuestros datos privados es sumamente importante y relevante cada día. Los beneficios de la comunicación electrónica traen implícitos ciertos riesgos. Los sistemas de negocios críticos pueden y son comprometidos regularmente, además, algunos son usados con propósitos ilegales.

La convergencia de las comunicaciones en redes cableadas, Wireless e internet traen consigo el desarrollo de nuevas aplicaciones y servicios las cuales han revolucionado las comunicaciones. La comunicación entre las redes PSTN (Public Switched Telephone Network) e IP (Internet Protocol) son referidas como NGN (Next Generation Networking) y la interconexión de internet y Wireless es referida como IMS. Ambas arquitecturas juegan un rol importante es su evolución desde las comunicaciones tradicionales hasta las comunicaciones multimedia.

Voz sobre IP esta implementado usando un subconjunto de los mismos protocolos y está considerado como una aplicación multimedia de tiempo real que se ejecuta sobre NGN o IMS. La telefonía IP tiene grandes aplicaciones y debido a sus bajos costos esta llamada a ser el futuro de las telecomunicaciones.

En VoIP se puede interceptar la señalización y los streams de audio de una conversación. Los mensajes de señalización utilizan el protocolo TCP, en cambio los streams se transportan por UDP utilizando el protocolo RTP. Algunos podrían pensar que la intercepción de códecs podría eliminarse con el uso de switches Ethernet que restringen el tráfico multidifusión en la red, porque se limita el acceso al tráfico. Sin embargo, este argumento deja de ser válido cuando se introduce el ARP spoofing. El concepto básico es que el atacante envía a los usuarios avisos con la mac falsificada y por lo tanto, consigue que los paquetes IP lleguen a un host. Por medio del ARP spoofing, un atacante puede capturar, analizar y escuchar comunicaciones VoIP.

Pero si VoIP no se implementa bajo un cifrado, no es seguro, hasta el punto de poder averiguar la dirección IP de sus interlocutores, sus conversaciones y grabarlas, sin embargo, a pesar de la confiabilidad que presentan estos

mecanismos al momento de encriptar voz, no es menos importante saber la forma en que se ve afectado el rendimiento en cuanto al uso de uno de estos mecanismos.

En lo anterior establecido, este proyecto propone el estudio de mecanismos de gestión de clave para el cifrado de la comunicación específicamente ZRTP y SRTPD y además se pretende conocer el nivel de rendimiento intrínseco en una de estas implementaciones tomando en cuenta ciertas métricas como, coste de CPU, memoria, anchado de banda, jitter y paquetes perdidos entre otros, para determinar en qué medida el uso de un mecanismo afecta el rendimiento de una PBX software (Asterisk 1.8) puesto que en telefonía los tiempos de respuesta son un factor clave que determina la comunicación y estos tiempos de respuesta están ligados al número de llamadas simultaneas por segundo que puede procesar nuestro servidor.

1.1 PROBLEMA DE LA INVESTIGACIÓN

La protección de la comunicación se lleva a cabo mediante el uso de protocolos de seguridad que se integran en la pila de protocolos que utilizan los extremos de la comunicación. Dependiendo del nivel de la pila al que se realice la integración, será necesario hacer que las aplicaciones o el sistema operativo incluyan las operaciones correspondientes al protocolo de seguridad, sin embargo, el diseño de estos protocolos de seguridad es una tarea sumamente compleja y un mal diseño pondría en peligro la seguridad, por ello, el diseño y análisis de estos protocolos está en manos de organismos encargados de diseñar y estandarizar el resto de los protocolos de comunicaciones. En los últimos años, múltiples protocolos de seguridad mecanismos de gestión de clave se han estandarizado, de forma que las especificaciones de estos mecanismos para proteger la información están disponibles para cualquier grupo de desarrollo. Esta situación ha llevado aparejada la aparición de múltiples fabricantes con productos que proporcionan mecanismos para asegurar las redes de comunicaciones, sin embargo la competencia en este mercado ha llevado a los fabricantes a tener que mejorar su solución para disponer una ventaja competitiva frente al resto y eso ha hecho que las soluciones de seguridad hayan sido dotadas de características adicionales, por ejemplo, mayor variedad de suites criptográficas son algunas ventajas comunes que podemos

encontrar en soluciones de seguridad. Por desgracia, estas mejoras y modificaciones en la forma en la que el estándar se implementa en la solución de seguridad, hacen de los dispositivos o programas, que incorporan estas soluciones, se vean afectados por problemas de interoperabilidad y en algunas de ellas afectando inclusive el rendimiento.

1.2 JUSTIFICACIÓN

Con la creciente implantación de sistemas de telefonía IP, los ataques contra los sistemas de TI que amenazan a las operaciones comerciales y privacidad de las empresas y de los datos personales ya no tienen un impacto sólo en el mundo de los datos, algunos de los ataques mencionados en el apartado anterior colocan en el entredicho la protección de la información, específicamente en VoIP a la captura de las conversaciones.

La gestión de claves -o dicho en otras palabras, sus implementaciones- son parte fundamental de protección para Internet en aplicaciones multimedia como VoIP. El intercambio de información en las redes de comunicaciones ha pasado a ser parte primordial de las tecnologías de la información, por medio del cual sistemas informáticos llevan a cabo las tareas para las que han sido diseñados.

Estos intercambios están regidos por protocolos de comunicación que gobiernan la forma en la que diferentes entidades proceden a enviarse la información de la forma más eficiente posible, sin embargo, estos intercambios de información requieren de servicios de seguridad.

Los protocolos de gestión de claves son complejos en su diseño, especialmente para aplicaciones multimedia, por ejemplo, videoconferencia, audio (brodcasting o multicast), video o transferencia de archivos, es esta complejidad la que hace que implementaciones de mecanismos de gestión de clave se aparten de los objetivos que se deben cumplir con el estándar, por ejemplo, interoperabilidad, rendimiento, entre los más importantes.

Ahora bien, el análisis que se pretende realizar en esta tesis, sirve para analizar los parámetros que son relevantes en el estándar, y posteriormente identificar los parámetros que resultan relevantes para evaluar el rendimiento de las implementaciones (ZRTP y SRTP Descriptions), además, de sus limitaciones y prestaciones. Con la información que se obtenga se desarrollará una guía referencial que permita evaluar, no solo las implementaciones mencionadas, si no otras que en el futuro puedan aparecer para la protección de contenidos de voz.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

- Analizar los mecanismos de gestión de clave para proteger los contenidos de voz sobre el protocolo IP.

1.3.2 OBJETIVOS ESPECÍFICOS

- Estudiar los mecanismos de gestión de clave para identificar los parámetros asociados al RFC 4046.
- Analizar los mecanismos de gestión de clave SRTP Descriptions y ZRTP para establecer el mecanismo más seguro en un sistema VoIP.
- Desarrollar una guía referencial de evaluación de mecanismos de gestión de clave para determinar el rendimiento en un sistema de VoIP.
- Crear un ambiente de pruebas para demostrar la transmisión de voz encriptado y el rendimiento del mecanismo de gestión de clave seleccionado.

1.4 ALCANCE

El presente proyecto de investigación ofrece una visión referente a la importancia de la encriptación para la protección de contenidos de voz y en particular a la forma cómo afecta el rendimiento en un escenario de pruebas, además, este estudio incluye una breve descripción de los protocolos usados e involucrados en la transmisión de voz.

En una primera etapa se analizar los mecanismos de gestión de clave SRTP Descriptions y ZRTP, lo cual proporcionará, mediante un análisis, la mejor técnica de acuerdo a parámetros de evaluación como: especificación de modulo criptográfico, autentificación servicios y roles, modelo de estado finito, seguridad física, entorno operacional, gestión de clave criptográfica, diseño de seguridad, mitigación a otros ataques.

En una segunda etapa, se utilizó, para la obtención de datos, un servidor privado virtual con procesador Xeon de 512MB de memoria RAM, con 20 GB de almacenamiento y una transferencia de 200 GB, en el cual se instalará el sistema operativo CentOS 6 y se configurará la PBX Software Asterisk 1.8.7, también, se usará el softphone Blink. Una vez realizada esta configuración se procedió a realizar las mediciones de rendimiento en el servidor VPS (Virtual Private Server), en una primera sub-etapa se recolectaron los datos sin configurar un mecanismo de gestión de clave, estos datos serán servirán como control. En una segunda sub-etapa sobre el mismo escenario y configurado un mecanismo de gestión de clave se extraerán los datos. En ambas sub-etapas los datos a tomar en cuenta son: paquetes transmitidos, paquetes recibidos, tiempo de proceso, ancho de banda, uso de memoria, jitter y paquetes perdidos.

Posteriormente a las pruebas realizadas, se elaborará una guía de referencia para que se permita evaluar, otras implementaciones de mecanismos de gestión de clave que en el futuro puedan aparecer para la protección de contenidos de voz sobre IP.

CAPÍTULO II
REVISIÓN DE LA LITERATURA

Este capítulo empieza realizando una introducción a la telefonía, principios de la transmisión humana, digitalización de voz, pasando a continuación a describir de forma resumida los protocolos que están involucrados en la transmisión de voz. Finalmente, se describe de forma sucinta la arquitectura de los mecanismos de gestión de clave (ZRTP Y SRTP Descriptions) incluyendo su definición, las características básicas, y por último, se identificará parámetros relevantes del RFC 4046.

2.1 INTRODUCCIÓN A LA TELEFONÍA

2.1.1 PRINCIPIOS Y TRANSMISIÓN DE VOZ

La voz humana está compuesta por ondas acústicas que viajan a través del aire a la velocidad del sonido, esto es a 1,244 Km/h (o 340 m/s). Otra característica importante de la voz humana es que las cuerdas vocales modulan la voz en un amplio espectro de frecuencias que van de graves a agudos en un rango aproximado de 20Hz a 20kHz.

Esto nos hace suponer que un micrófono debe ser capaz de capturar y transmitir todo este rango de frecuencias. Sin embargo, en la actualidad sabemos que para transmitir voz "entendible" no es necesario transmitir todas las frecuencias sino un rango mucho menor y transmitir un rango menor de frecuencias tiene sus ventajas pues facilita la transmisión. Por lo tanto los teléfonos comerciales solo transmiten un rango aproximado de 400Hz a 4kHz. Esto distorsiona la voz en una escala pequeña pero de todas formas se puede entender. Otra característica fundamental en la transmisión de voz es el ancho de banda En general podemos decir que ancho de banda es una medida de la cantidad de información que podemos transmitir por un medio por unidad de tiempo. Medidas comunes para expresar el ancho de banda son los bits por segundo. Esta medida también equivale a bits/s, bps o baudios. El ancho de banda es un término muy importante cuando se habla

de telefonía pues las comunicaciones en tiempo real necesitan un ancho de banda mínimo asegurado para entregar una comunicación de calidad[1].

Las redes digitales de transmisión de voz y datos son comunes en nuestra era. Fueron creadas ya que presentan ciertas ventajas sobre las redes analógicas como por ejemplo que conservan la señal casi inalterable a través de su recorrido.

Es decir que es más difícil que la comunicación se vea afectada por factores externos como el ruido eléctrico. Además nos provee de métodos para verificar de cuando en cuando la integridad de la señal, entre otras ventajas. Digitalizar una señal de voz no es otra cosa que tomar muestras (a intervalos de tiempo regulares) de la amplitud de la señal analógica y transformar esta información a binario. Este proceso de denomina muestreo.

En 1928 Henry Nyquist, un ingeniero Suizo que trabajaba para AT&T, resolvió el dilema de cuánto es necesario muestrear una señal como mínimo para poder reconstruirla luego de forma exacta a la original. El teorema propuesto decía que como mínimo se necesita el doble de ancho de banda como frecuencia de muestreo. Esto queda reflejado de mejor manera con la siguiente expresión:

$$f_m \geq 2\ BW_s$$

Ecuación 1 Teorema de Nyquist[2].

2.1.2 REDES ORIENTADAS A CIRCUITOS Y ORIENTADAS A PAQUETES

Las redes orientadas a circuitos (circuit switched) son aquellas donde se establece un circuito exclusivo o dedicado entre los nodos antes de que los usuarios se puedan comunicar. Una vez que se establece un circuito entre dos puntos que quieren comunicarse, el resultado básicamente es el equivalente a conectar físicamente un par de cables de un extremo a otro. Una vez establecido el circuito, éste ya no puede ser usado por otros. En cada circuito el retardo es constante, lo cual es una ventaja. Sin embargo, este tipo de redes es costoso debido al mismo hecho de que se necesita un circuito dedicado para cada abonado.

[1] Fuente, LANDIVAR, Edgar. Comunicaciones Unificadas con Elastix Volumen 1. Ecuador, 2009. Pág. 5-20
[2] Fuente, LANDIVAR, Edgar. Comunicaciones Unificadas con Elastix Volumen 1. Ecuador, 2009. Pág. 19

Una red de paquetes es una red que por un mismo medio trafica simultáneamente diferentes flujos de información. Para hacer esto divide el tráfico de cada flujo de información en fragmentos o paquetes que envía intercaladamente. Luego, en el destino los paquetes se re ensamblan para reproducir el mensaje original.

A diferencia de las redes orientadas a circuitos, en este tipo de redes el ancho de banda no es fijo ya que depende del tráfico de la red en un momento dado, adicionalmente cada paquete de un mismo flujo de información no está obligado a seguir el mismo camino por lo que los paquetes que originalmente fueron generados en secuencia pueden llegar desordenados a su destino.

Este tipo de factores son muy importantes a tener en cuenta cuando se trafica voz sobre una red de paquetes ya que afectan la calidad de la llamada. Las redes de paquetes se han vuelto populares, principalmente porque optimizan recursos debido al hecho de poder utilizar el mismo medio para enviar varios flujos de información[3].

2.1.3 DTMFs

Muchas veces es necesario enviar dígitos a través de la línea telefónica tanto para marcar como en medio de una conversación. Con esta finalidad se pensaron los DTMFs. DTMF es un acrónimo de Dual-Tone Multi-Frequency. Es decir que cada DTMF es en realidad dos tonos mezclados enviados simultáneamente por la línea telefónica. Esto se hace así para disminuir los errores. En la Tabla 1 se muestra las frecuencias para cada digito.

Tabla 1 Frecuencias para cada dígito.

	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

[3] LANDIVAR, Edgar. Comunicaciones Unificadas con Elastix Volumen 1. Ecuador, 2009. Pág. 21-24

2.1.4 INTRODUCCIÓN A VoIP

La voz sobre IP o VoIP consiste en transmitir voz sobre protocolo IP. Dicho así puede sonar simple pero las redes IP fueron diseñadas principalmente para datos y muchas de las ventajas de las redes IP para los datos resultan ser una desventaja para la voz pues ésta es muy sensible a retardos y problemas de transmisión por muy pequeños que estos sean. Por tanto transmitir voz sobre protocolo IP es toda una empresa con muchos problemas técnicos que resolver. Por suerte la tecnología ha evolucionado y la pericia de algunos ingenieros talentosos ha resultado en que podamos abstraernos en gran medida de aquellos problemas inherentes a las redes IP que perjudican la calidad de voz. En la figura 1, se identifica los componentes de VoIP end-to-end desde el emisor hasta el receptor. El primer componente es el codificador, el cual periódicamente obtiene muestras de la señal original de voz y asigna un número de tamaño fijo de bits por cada muestra, creando una cadena constante de taza de bits. El tradicional codificador de muestra es el códec G.711 que usa la modulación de código por pulso (PCM, pulse code modulation), para generar muestras de 8 bits cada 0.125ms, conducidos a una taza de datos de 64 kbps. Luego del codificador está el empaquetador, el cual encapsula a un cierto número de muestras de voz dentro de paquetes a los cuales son añadidas las cabeceras RTP (Real Transport Protocol), UDP, IP y Ethernet. La voz viaja a través de la red de datos hacia el receptor donde un importante componente denominado *playback buffer* y su propósito es absorber las variaciones o el retardo provocado por el jitter con el objetivo de proporcionar una reproducción fluida. Los paquetes son entregados al desempaquetador y eventualmente al decodificador, el mismo que reconstruye la señal de voz original.

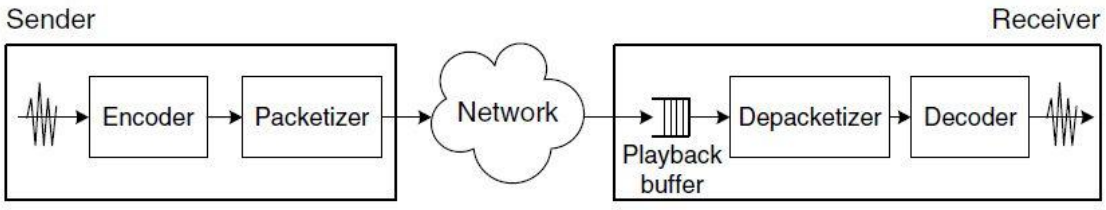


Figura 1 Componentes end-to-end de VoIP[4].

[4]Fuente: Syed A. Ahsas y Mohammad Ilyas, "VoIP Handbook: Applications, Technologies, Reliability and Security," 2009, Pág. 6

Hay muchos protocolos involucrados en la transmisión de voz sobre IP. Ya de por sí hay protocolos de red involucrados como el propio protocolo IP y otros protocolos de transporte como TCP o UDP. Encima de ellos se colocan los protocolos de señalización de voz y como si esto fuera poco existen además muchas opciones de protocolos de señalización disponibles lo que puede hacer que todo suene un poco confuso al principio[5].

2.1.4.1 CLASIFICACIÓN DE LOS PROTOCOLOS VOIP

A esta clasificación podríamos categorizarla de la siguiente manera: protocolos de señalización, protocolos de transporte de voz y protocolos de plataforma IP.
Los protocolos de señalización en VoIP cumplen funciones similares a sus homólogos en la telefonía tradicional, es decir tareas de establecimiento de sesión, control del progreso de la llamada, entre otras. Se encuentran en la capa 5 del modelo OSI, es decir en la capa de Sesión. Existen algunos protocolos de señalización, que han sido desarrollados por diferentes fabricantes u organismos como la ITU o el IETF. Algunos son SIP, IAX, H.323, MGCP y SCCP, mencionados debido a que para el ambiente de pruebas se utiliza Asterisk y como protocolo de señalización SIP.

A los protocolos de transporte de voz no se los debe confundir con protocolos de transporte de bajo nivel como TCP y UDP. Nos referimos aquí al protocolo que transporta la voz propiamente dicha o lo que comúnmente se denomina carga útil. Este protocolo se llama RTP (Real-time Transport Protocol) y función es simple: transportar la voz con el menor retraso posible. Este protocolo entra a funcionar una vez que el protocolo de señalización ha establecido la llamada entre los participantes. Dentro de los protocolos de plataforma IP agruparemos a los protocolos básicos en redes IP y que forman la base sobre la cual se añaden los protocolos de voz anteriores. En estos protocolos podríamos mencionar a Ethernet, IP, TCP y UDP. A continuación en la figura 2 se muestra a los protocolos involucrados en una llamada SIP.

[5] Fuente: LANDIVAR, Edgar. Comunicaciones Unificadas con Elastix Volumen 1. Ecuador, 2009. Pág. 33

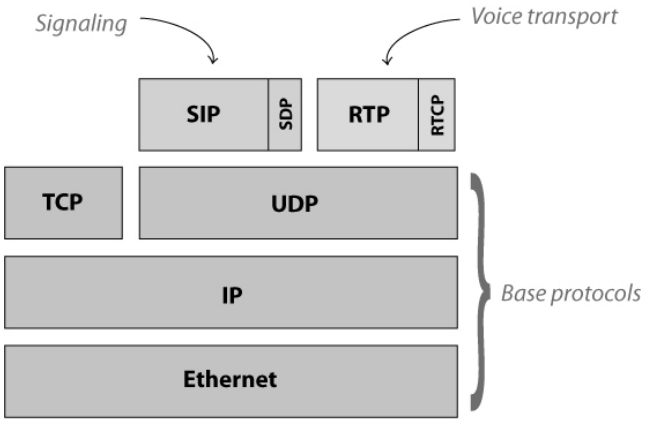


Figura 2 Protocolos VoIP.[6]

Para transportar la voz de un lugar a otro, en una red de paquetes, necesitamos la ayuda de algunos protocolos; pero estos protocolos transmiten data adicional que ocupa ancho de banda extra a la voz propiamente dicha. Algunos de ellos son Ethernet, IP, UDP, RTP. En resumen esto hace que el ancho de banda real para transmitir voz sea mayor al del códec. Por ejemplo, para transmitir voz usando G.711 en teoría deberíamos usar 64Kbps (peso del códec) pero en realidad usamos 95.2Kbps de BW. En otros códecs más compresores la sobrecarga es incluso más significativa. La figura 3 ilustra lo antes dicho.

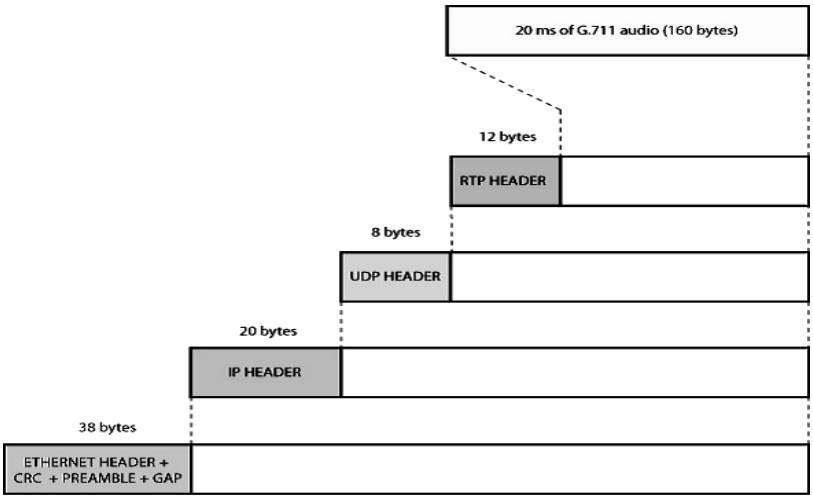


Figura 3 Sobrecarga de protocolo usando G.711[7].

A continuación en la tabla 2 se muestra el overhead para algunos de los códecs más populares soportados por Asterisk.

[6] Fuente: LANDIVAR, Edgar. Comunicaciones Unificadas con Elastix Volumen 1. Ecuador, 2009. Pág.36
[7] Fuente: LANDIVAR, Edgar. Comunicaciones Unificadas con Elastix Volumen 1. Ecuador, 2009. Pág. 44

Tabla 2 Códec overhead[8]

Códec	AB códec	AB real Ethernet	Overhead %
G.711	64 Kbps	95.2 Kbps	48.75%
iLBC	15.2 Kbps	46.4 Kbps	205.26%
G.729A	8 Kbps	39.2 Kbps	390%

2.1.4.2 PROTOCOLO SIP

El protocolo SIP (Session Initialization Protocol) es un protocolo de señalización (application-layer control) creado para administrar sesiones multimedia entre dos o más participantes. Muchos se confunden pensando en que el protocolo SIP es quien transporta la voz propiamente dicha pero no es así, esta labor la realiza otro protocolo que veremos más adelante; de lo que sí se encarga SIP es de la comunicación necesaria para establecer una llamada, modificarla, así como para finalizarla.

El protocolo SIP fue diseñado con la premisa de la simplicidad en mente, se trata de un protocolo de texto con mensajes de comunicación sencillos. Inclusive SIP comparte algunos códigos de estatus con HTTP como el familiar “404: Not found” Es un protocolo peer-to-peer. Es decir que prácticamente toda la lógica es almacenada en los puntos finales. A continuación se listan detalles del protocolo:

- RTP es el portador de la voz y el video.
- SDP se usa para negociar las capacidades de los puntos finales.
- Usa dos importantes protocolos como RTP/RTCP y SDP.
- La última versión del estándar es la RFC3261.
- Basado en texto, lo que nos permite entender los mensajes de una manera relativamente fácil.

La señalización SIP está dada por los métodos y respuestas, la tabla 3 muestra los métodos.

[8] Fuente: VoIP Foro, Tabla resumen de códec, http://www.voipforo.com/codec/codecs.php

Tabla 3 Métodos en la señalización SIP[9]

Método	Descripción
INVITE	Invita a un usuario a una llamada
ACK	Facilita el intercambio de mensajes confiables.
BYE	Termina una conexión entre usuarios o declina una llamada
CANCEL	Termina un requerimiento o búsqueda por un usuario
OPTIONS	Solicita información acerca de capacidades del servidor SIP
REGISTER	Registra una ubicación de usuario
INFO	Usado para señalización en mitad de sesión. Para intercambiar información

Las respuestas en la señalización SIP pueden ser:

- 1xx Informational (e.g. 100 Trying, 180 Ringing)
- 2xx Successful (e.g. 200 OK, 202 Accepted)
- 3xx Redirection (e.g. 302 Moved Temporarily)
- 4xx Request Failure (e.g. 404 Not Found, 482 Loop Detected)
- 5xx Server Failure (e.g. 501 Not Implemented)
- 6xx Global Failure (e.g. 603 Decline)

Algunos detalles a tener en cuenta cuando se usa el protocolo SIP con Asterisk son los siguientes:

- A pesar de que SIP es independiente de la capa de transporte (puede ser usado con TCP, UDP, ATM, X.25, entre otros) en Asterisk su implementación está limitada a UDP
- Por omisión se usa el puerto 5060, pero este parámetro se puede modificar en el archivo sip.conf
- SIP adolece de problemas de NAT
- En Asterisk es posible hacer diagnóstico del protocolo SIP.

[9] Fuente: VoIP Foro, Resumen de señalización SIP http://www.voipforo.com/codec/codecs.php

2.1.4.3 PROTOCOLO RTP

RTP es el protocolo que se encarga de transportar la voz propiamente dicha. Muchas personas se confunden y piensan que ese es el trabajo de SIP pero no es así. Una vez que SIP establece una llamada es RTP quien transportar la voz a su destino.RTP trabaja sobre UDP y por lo tanto no hay mucho control de transmisión. Es decir que el equipo emisor envía la voz hacia el otro extremo con la esperanza de que llegue, pero no espera recibir confirmación de esto y a decir verdad tampoco hay tiempo para hacerlo pues la voz necesita ser transmitida en tiempo real. Si un paquete de voz se pierde en el camino simplemente se rellenará ese espacio con un silencio. Lo que técnicamente se llama ruido confortable (confort noise generation CNG).

Es por esta necesidad de transmitir la información en tiempo real que resulta obvio que RTP sea un acrónimo de Real Time Protocol. A pesar de encargarse de casi toda la labor de transportar la voz, RTP no está solo y tiene un protocolo de apoyo llamado RTCP. RTCP no es del todo indispensable pero proporciona valiosa ayuda al momento de transportar la voz de manera óptima pues proporciona estadísticas e información de control que le permiten a Asterisk o al otro extremo tomar decisiones para mejorar la transmisión en caso de ser posible. Por lo tanto, los paquetes RTCP se transmiten periódicamente para comunicar dicha información a los equipos de voz involucrados. Un paquete RTP se compone de un encabezado y la data (o payload). Para tener una mejor visión de lugar que ocupa un paquete RTP en el modelo TCP/IP veamos la figura 4.

<table>
<tr><th colspan="6">Byte 1</th><th colspan="2">Byte 2</th><th>Byte 3</th><th>Byte 4</th></tr>
<tr><td>V=2</td><td>P</td><td>X</td><td colspan="3">CC</td><td>M</td><td colspan="2">PT</td><td colspan="2">Número de Secuencia</td></tr>
<tr><td colspan="10">Timestamp</td></tr>
<tr><td colspan="10">Synchronization Source (SSRC)</td></tr>
<tr><td colspan="10">Contributing Source (CSRC)</td></tr>
<tr><td colspan="10">Extensión (opcional dependiendo del bit X)</td></tr>
<tr><td colspan="10">Data…</td></tr>
</table>

Figura 4 Encabezado RTP[10].

Se explica brevemente qué información contiene un encabezado RTP.

[10] Fuente: VoIP Foro, Encabezado RTP, http://www.voipforo.com/codec/codecs.php

- V es el número de versión. Este campo es de 2 bits de longitud y su valor contenido siempre es el número 2.
- P o padding es un bit que indica si hay relleno al final de la data o no. Si el bit está en uno quiere decir que si hay relleno. El relleno no es otra cosa que bytes adicionales al final del Payload.
- X o extensión es un bit que indica si hay extensión del encabezado
- CC es un identificador de 4 bits que indica el conteo CSRC
- M o marcador de un bit
- PT o tipo de carga útil (Payload Type) es un identificador de 7 bits que nos indica el tipo de carga útil que contiene este paquete RTP. Ejemplos de tipos son G729, GSM, PCMU (G711 u-law), entre otros.
- Número de Secuencia (sequence number) es un número entero que identifica cada paquete del presente flujo de datos. Este es un identificador secuencial que se incrementa en uno con cada paquete transmitido. Ocupa 16 bits.
- Timestamp representa el instante de tiempo (en formato timestamp) en el que se comenzó a muestrear la data que está siendo transmitida en el payload. Ocupa 32 bits.
- SSRC identifica la fuente de sincronización ya que el mismo equipo puede estar “hablando” con diferentes fuentes de paquetes RTP. Es un número aleatorio de 32 bits por lo que hay la posibilidad (aunque la probabilidad es baja) de que este número se repita entre dos fuentes. Existen mecanismos para resolver este problema.
- CSRC es un número de 32 bits que identifica las fuentes contribuyentes para el payload.
- Luego de la cabecera vienen los datos.

2.2 SRTP

El protocolo seguro en tiempo real (SRTP) es una descripción para el Protocolo de tiempo real (RTP, el IETF RFC 3550) para garantizar la confidencialidad, integridad y autenticación de flujos de datos en los medios de comunicación, se define en el IETF RFC 3711.

Aunque existen varios protocolos de señalización (por ejemplo, SIP, H.323, Skinny) y varios mecanismos de intercambio de claves (por ejemplo, SDESCRIPTIONS,

ZRTP), SRTP es considerado uno de los mecanismo estándar para la protección en tiempo real de los medios de comunicación (voz y de vídeo) en las aplicaciones multimedia.

Además de proteger a los paquetes RTP, proporciona protección para los mensajes RTCP (Real-time Transport Control Protocol). RTCP se utiliza principalmente para proporcionar calidad de servicio de respuesta (por ejemplo, demora de ida y vuelta, jitter, bytes y paquetes enviados) a los puntos finales que participan de una sesión. Los mensajes RTCP se transmiten por separado de los mensajes de RTP, y los puertos se utilizan por separado para cada uno de los protocolos. Por lo tanto, ambos RTP y RTCP deben ser protegidos durante una sesión multimedia. Si se deja sin protección RTCP, un atacante puede manipular los mensajes RTCP entre los participantes y provocar la interrupción del servicio o realizar análisis de tráfico.

Los diseñadores de SRTP se centraron en el desarrollo de un protocolo que puede proporcionar una protección adecuada para los flujos de datos en los medios de comunicación, sino también mantener las propiedades clave a las redes cableadas e inalámbricas en el que las limitaciones de ancho de banda o de transporte subyacentes pueden existir. Algunos de las propiedades destacadas son las siguientes:

- La capacidad de incorporar nuevas transformaciones criptográficas.
- Mantener bajo el ancho de banda y coste computacional.
- Conservar el tamaño del código de implementación. Esto es útil para los dispositivos con memoria limitada (por ejemplo, teléfonos celulares).
- La independencia de transporte, incluyendo capas de red y físico que pueden ser utilizadas, y quizás propenso a la reordenación y la pérdida de paquetes.

Por ejemplo, el uso de SDES para el intercambio de claves y SRTP para los medios de protección es una combinación de mecanismos para proporcionar una seguridad adecuada para aplicaciones de Internet multimedia, incluyendo VoIP, vídeo y conferencia. La aplicación que implementa SRTP tiene que convertir los

paquetes RTP a paquetes SRTP antes de enviarlos a través de la red. El mismo proceso se utiliza en sentido inverso para descifrar paquetes SRTP y convertirlas en paquetes RTP. La figura 5 muestra este proceso.

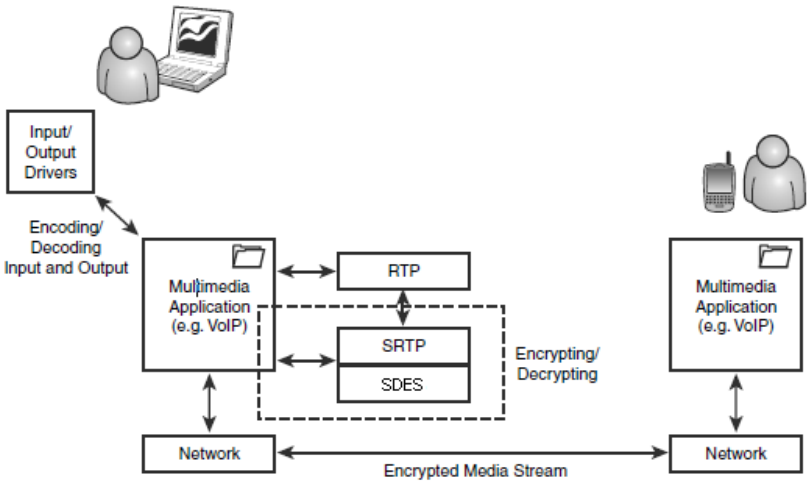


Figura 5 Codificación/Decodificación[11]

Después que la aplicación captura la entrada de un dispositivo (por ejemplo, un micrófono o una cámara), se codifica la señal utilizando el estándar de codificación de negociación (por ejemplo, G.711, G.729, H.261, H.264) y crea la carga útil del paquete RTP. A continuación, la carga útil de RTP se cifra mediante el algoritmo de cifrado. El algoritmo de cifrado por defecto para SRTP es AES (Advanced Encryption Standard) en el modo de contador con una longitud de clave de 128 bits.

Además de proporcionar cifrado de datos, el estándar SRTP admite la autenticación de mensajes y la integridad del paquete RTP. El mensaje predeterminado algoritmo de autenticación es SHA-1 con una longitud de clave de 160 bits. El código de autenticación de mensajes (MAC) se produce mediante el cálculo de un hash de todo el mensaje de RTP, incluyendo las cabeceras RTP y la carga útil encriptado, y colocando el valor resultante en el encabezado de etiqueta de autenticación, como se muestra en la figura 6.

[11]Fuente: THERMOS, Peter and TAKANEN, Ari. Securing VoIP Networks. USA. Pág. 244

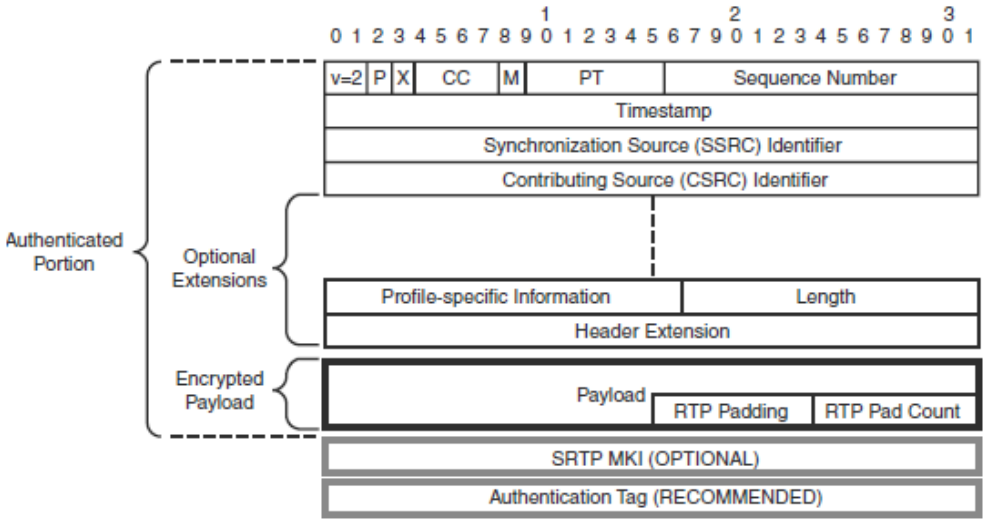


Figura 6 Formato del paquete SRTP[12]

Es posible que tenga en cuenta que el mensaje SRTP se asemeja al formato de un mensaje de RTP, con la excepción de dos cabeceras adicionales: el MKI y la etiqueta de autenticación. El MKI (Master Key Identifier) es utilizado por el mecanismo de gestión de claves (por ejemplo, sdes), y su presencia es opcional en las implementaciones de acuerdo al estándar SRTP (RFC 3711). El MKI se puede utilizar para volver a teclear o para identificar la clave maestra de la cual las claves de sesión se derivaron para ser utilizado por la aplicación para descifrar o verificar la autenticidad de la carga asociada SRTP. El mecanismo de intercambio de claves genera y gestiona el valor de este campo a lo largo de la duración de la sesión.

El uso de la etiqueta de cabecera de autenticación es importante y proporciona protección contra ataques de repetición de mensajes. En las implementaciones de VoIP, se recomienda que la autenticación de mensajes se utilice, como mínimo, si el cifrado no es una opción. El uso de ambos se puede considerar como un enfoque óptimo.

Hay que tener en cuenta que los encabezados de los mensajes cifrados no son una casualidad (por ejemplo, el número de secuencia, SSRC) para brindar apoyo a la compresión de la cabecera e interoperar con aplicaciones o elementos de una red intermedia que podría no ser usada para admitir SRTP pero si es necesario

[12]Fuente: THERMOS, Peter and TAKANEN, Ari. Securing VoIP Networks. USA. Pág. 246

para procesar las cabeceras RTP (por ejemplo, la facturación). Esta limitación permite a un atacante realizar análisis de tráfico mediante la recopilación de información de las cabeceras RTP y sus extensiones, junto con la información de transporte subyacente (por ejemplo, IP, UDP).

La figura 7 muestra un ejemplo de una aplicación que utiliza SDescriptions (Descripciones de Seguridad) para transmitir una clave criptográfica para su uso con SRTP. La clave se transmite dentro de la porción SDP de un mensaje SIP. El SDP medios atributo de cifrado define el tipo de algoritmo, el modo de cifrado, y la longitud de la clave (AES_CM_128), junto con el algoritmo de resumen del mensaje y su longitud (SHA1_32).

Figura 7 Negociación de clave usando SDescriptions en SIP[13].

La línea indica el método que el material de claves actual es capturado in el campo key-info de la cabecera. La sintaxis de la cabecera es definida como sigue:
a=crypto:<tag><crypto-suite><key-params> [<session-params>]

[13]Fuente: THERMOS, Peter and TAKANEN, Ari. Securing VoIP Networks. USA. Pág. 265

<crypto-suite> identifica los algoritmos de autentificación y encriptación (en este caso, AES en modo contador usando una longitud de clave de 128 bits y SHA-1). El siguienteatributoes<key-params>, donde:

key-params = <key-method> ":" <key-info>

En este caso la línea <key-method>

<key-info> = UlrbLlfNTNw3blKHQVLGze6oHsyFdjGj3NheKoYx

2.3 MECANISMOS DE GESTIÓN DE CLAVE

La gestión de claves es una parte fundamental de la protección de aplicaciones multimedia en Internet, como VoIP. Así mismo, los protocolos de gestión de claves son difíciles de diseñar, especialmente para aplicaciones multimedia que requieren la participación del grupo (por ejemplo, la videoconferencia, la difusión o multidifusión de transferencia de audio, video o archivo). Hasta hace poco, diversos mecanismos de intercambio de claves, tales como IKE fueron probados para soportar comunicaciones asíncronas (es decir, la transferencia de archivos) pero no es adecuado para aplicaciones de Internet o grupos de multidifusión o multimedia. Por lo tanto, un esfuerzo distinto se ha iniciado dentro de la IETF para establecer esa capacidad. El IETF RFC 4046, "Grupo de MSEC Arquitectura de administración de claves", define una arquitectura que consta de abstracciones y principios de diseño para el desarrollo de protocolos de gestión de claves[14].

La arquitectura de MSEC define un conjunto de requisitos para el desarrollo de protocolos gestión de claves. Estos requisitos discuten las propiedades y los principios que los protocolos de gestión de claves debe exhibir para la escalabilidad, políticas de grupo de seguridad, asociaciones (clave de cifrado, tiempo de vida, y así sucesivamente), pertenencia al grupo, cambio de claves, la disuasión de ataque, y la recuperación del compromiso. Comunicaciones multimedia, como VoIP requieren protocolos de negociación de clave que puede proporcionar capacidades sólidas y extensibles para la comunicación multicast y unicast.

[14]Fuente: Himanshu Dwivedi, Hacking VoIP – protocols, attacks and countermeasures, USA 2009, cap 9.

Por ejemplo, los protocolos como TLS e IKE no proporcionan tales capacidades. Protocolos de gestión de claves se pueden utilizar para proteger las comunicaciones multicast y unicast entre los usuarios, grupos y subgrupos (a través de la asociación de grupo de seguridad). Además, tienen que demostrar la resistencia a los ataques de fuentes externas e internas (es decir, suplantaciones, DoS). Dentro de la arquitectura MSEC, se define en el que la negociación de claves y de gestión de claves son los componentes. La negociación de material de claves es uno de los temas más difíciles para VoIP (y, en general, para las aplicaciones multimedia de Internet). Aquellos que quieren mantener la confidencialidad e integridad de la comunicación necesitan un mecanismo robusto y seguro para el intercambio de claves criptográficas de forma fiable. En primer lugar, hay dos métodos de intercambio de mensajes claves:

- Codificación integrada, a través del protocolo de establecimiento de sesión, como SIP2. Este enfoque requiere un menor número de mensajes de intercambio, por lo que minimiza los retrasos asociados en la introducción debido al intercambio de mensajes.
- Intercambio Nativo de Clave a través de un proceso distinto. Este enfoque requiere más mensajes que se generan entre los puntos finales, y por lo tanto aumenta el riesgo de retrasos asociados en la introducción debido al intercambio de mensajes. Además, en un dispositivo no se puede determinar de antemano si el punto final remoto puede admitir un mecanismo de intercambio de clave en particular.

Las funciones criptográficas son computacionalmente intensas debido a los cálculos matemáticos que deben realizar para obtener el producto correspondiente (por ejemplo, el Código de autenticación de mensajes o las claves de cifrado). Por lo tanto, es importante definir un conjunto de requisitos en el diseño de los protocolos de negociación de clave, sobre todo cuando se utilizan en combinación con aplicaciones de transmisión en tiempo real que son sensibles al tiempo.
En el diseño de protocolos de intercambio de claves, debe considerar lo siguiente:

- Consumo de los recursos computacionales clave, los mecanismos de negociación consumen muchos recursos y el impacto de los recursos de procesamiento y de almacenamiento (es decir, CPU, memoria), que

también consumen energía (por ejemplo, duración de la batería). En el caso de aplicaciones multimedia, como VoIP, el tratamiento de los flujos de los medios de comunicación, también poseen computación intensiva, es fundamental mantener requisitos de bajo consumo de recursos, especialmente para los dispositivos móviles como teléfonos y PDAs. Establecer un cuidadoso equilibrio entre la cantidad de procesamiento requerido por las funciones criptográficas y las capacidades de los dispositivos correspondientes.

- Retraso en el establecimiento de sesión en las aplicaciones multimedia (y, por supuesto, VoIP), la negociación de claves añade otra capa de intercambio de mensajes para establecer una sesión segura entre dos o más partes. Esta capa adicional puede introducir retrasos en el establecimiento de una sesión, que puede afectar a la calidad de servicio. Por lo tanto, es necesario ser lo más conservador posible y minimizar el número de mensajes necesarios para negociar claves.
- Evitar una implosión, esta consideración es importante en el diseño de un protocolo de gestión de claves, que puede ser un elemento de sobrecarga en la red por un número abrumador de mensajes legítimos. Hay dos variaciones de esta condición: out-of-sync y la implosión retroalimentada. La implosión de fuera de sincronización se refiere al intento simultáneo de los participantes legítimos para actualizar sus asociaciones de seguridad o cambio de claves, que se traducirá en carga al servidor de claves con los mensajes de solicitud de actualización. La implosión de retroalimentación se refiere a la entrega fiable de mensajes de cambio de claves. Normalmente, los protocolos fiables multicast están diseñados para retransmitir los paquetes cuando se produce la pérdida de paquetes. Por lo tanto, muchos miembros del grupo al mismo tiempo pueden transmitir mensajes de información (es decir, NACK o ACK) hacia el servidor de claves, y así abrumar el servidor.

2.3.1 DESCRIPCIÓN DE SEGURIDAD SRTP

SRTP Descriptions es un mecanismo para negociar las claves de cifrado entre los usuarios en las sesiones unicast utilizando como transporte el protocolo SRTP (por ejemplo, RTP / SAVP o RTP / SAVPF). El mecanismo SRTP Descriptions no es

compatible con flujos comunes a los medios de comunicación multicast o unicast multipunto. Para comunicar los datos de claves, el campo *crypto* se utiliza dentro de SDP (Session Description Protocol). La figura 2.7 muestra que el atributo crypto se define en la parte SDP de un mensaje SIP INVITE. El formato del atributo de *crypto* es el siguiente:

a = cripto =: <tag><crypto-suite><key-params> [<session-params>]

En la figura 8, la suite crypto es AES_CM_128_HMAC_SHA1_32, key-params es definido por el texto que comienza con "inline", y session params depende de la implementación. El campo tag es un número decimal y se utiliza como parte del modelo de offer/answer para distinguir el atributo crypto elegido por los participantes para cada flujo de los medios de comunicación en una sesión. Por ejemplo, Chichan puede ofrecer dos o más suites de cifrado a Patokun en la oferta inicial, (p.ej. AES_CM_128_HMAC_SHA1_80, AES_CM_128_HMAC_SHA1_32, y f8_128_HMAC_SHA1_80) Patokun puede responder a Chichan seleccionando la opción f8_128_HMAC_SHA1_80 como la transformación de cifrado para proteger el flujo de los medios de comunicación respectivos.

Figura 8 SIP and SDescriptions.

El campo *crypto-suite* es un identificador que describe los algoritmos de cifrado y autenticación (p.ej. AES_CM_128_HMAC_ SHA1_80). El campo *key-params*

ofrece uno o más conjuntos de material de claves para *crypto-suite* y consiste de un método, en este caso "inline", lo que indica que el material de claves actual (la llave maestra y salt) se encuentra en el propio campo *key-info*. La información adicional incluye una política asociada de clave maestra, como su vida útil y el uso de MKI (Master Key Identifier). El MKI se utiliza para asociar los paquetes SRTP con una llave maestra en una sesión multimedia. Sobre la base del estándar IETF Security Descriptions, cada clave tiene este formato:"inline:" <key||salt> ["|" lifetime] ["|" MKI ":" length]

La sintaxis de la clave es la siguiente:

- *Key || salt,* es la concatenación de la llave maestra y salt decodificado en formato base64.
- *lifetime,* indica la vida útil de la clave maestra.
- *MKI: Length*, indica el MKI y la longitud del campo de MKI en los paquetes SRTP.

Los parámetros MKI y lifetime no pueden estar presentes en algunas implementaciones, ya que se definen como opcionales de acuerdo al estándar. La figura 9 muestra un ejemplo de una clave sin valores lifetime o MKI.

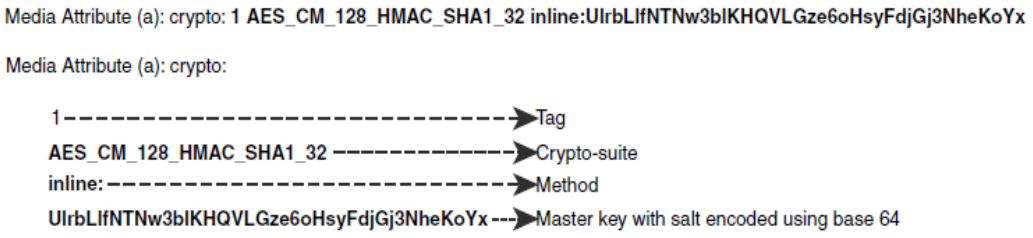


Figura 9 Security Descriptions sin valores lifetime o MKI.

La figura 10 muestra el caso de que el atributo de lifetime y MKI están presentes.

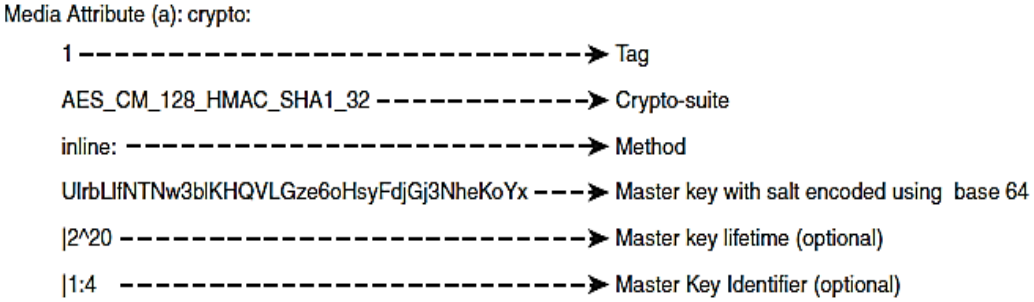


Figura 10 Security Descriptions con valores lifetime y MKI.

La notación 2^{20} (p.ej. 2 a la potencia de 20) indica que el valor de duración de la clave maestra que se mide en paquetes (p.ej. el número máximo de paquetes SRTP que deben ser cifrados utilizando esta clave en particular).

La notación 1:4 indica el MKI y su longitud. Este parámetro también es opcional. El identificador es 1 (uno) y su longitud es de 4 bytes de longitud. Otro ejemplo es la siguiente:

inline: UlrbLlfNTNw3blKHQVLGze6oHsyFdjGj3NheKoYx | 1024:4

Donde el identificador de clave es 1024, con una longitud de 4 bytes.

Los parámetros de sesión [<session-params>] que se pueden incluir en una interacción offer/answer son las siguientes (según se define en el RFC):

- KDR, la tasa de derivación clave SRTP es la tasa que el PRF es aplicado a una llave maestra.
- UNENCRYPTED_SRTP-SRTP, los mensajes no están cifrados.
- UNENCRYPTED_SRTCP-SRTCP, los mensajes no están cifrados.
- UNAUTHENTICATED_SRTP-SRTP, los mensajes no están autenticados.
- FEC_ORDER, Orden de reenvió de corrección de errores (FEC) en relación a los servicios de SRTP.
- FEC_KEY, clave maestra para FEC cuando el flujo FEC se envía a un puerto o a dirección separada.
- WSH, indicio del tamaño de la ventana, que se utiliza para proteger contra ataques de repetición.
- Extensions, extensión de parámetros que pueden ser definidos.

Tenga en cuenta que las descripciones de seguridad están definidas dentro SDP, que suelen ser encapsuladas en protocolos como SIP o MGCP. Por lo tanto, se espera que el protocolo de transporte subordinado (por ejemplo, TLS, IPSec) le provea de autenticación y confidencialidad necesaria para proteger el material de claves de los ataques como espionajes, reproducciones de audio, y la modificación del mensaje.

2.3.2 ZRTP[15]

ZRTP es otro protocolo de acuerdo de claves que se pueden utilizar para admitir SRTP. La diferencia fundamental entre ZRTP y otros mecanismos existentes de intercambios de claves es que las claves criptográficas se negocian a través de los flujos en los medios de comunicación (RTP) a través del puerto UDP, en lugar de utilizar la ruta de señalización, como SDescriptions.

Por lo tanto, la clave de negociación se realiza directamente entre pares sin requerir el uso de intermediarios, como proxies SIP para transmitir el material de claves. Si es necesario, sin embargo, el diseño ZRTP también ofrece la opción de intercambiar el material de claves a través de mensajes de señalización.

En primer lugar, el protocolo utiliza claves efímeras DH (Diffie-Hellman) para establecer un secreto compartido entre los compañeros, pero no requiere un PKI, que hace que el protocolo de una alternativa atractiva para las organizaciones que no mantienen un PKI. Al escribir estas líneas, ZRTP se denomina "proyecto", pero se espera que sea ratificado como RFC de la IETF, ya que ha sido implementada por algunos proveedores.

2.3.2.1 NEGOCIACIÓN DE CLAVE ZRTP

La negociación de la clave en ZRTP se lleva a cabo utilizando la ruta de medios de comunicación (RTP), y hay dos modos de acuerdo de claves: Diffie-Hellman y secreto pre-compartido. Cuando Diffie-Hellman es utilizado, el proceso de acuerdo de claves se realiza mediante cinco pasos para anunciar soporte ZRTP entre compañeros para iniciar, gestionar y terminar el intercambio de claves, como se muestra en la figura 11.

En modo pre-compartido, los puntos finales omiten el cálculo de DH, porque se supone que el secreto compartido se conoce de una sesión anterior, pero el DHPart1 y los mensajes siguen siendo intercambiados DHPart2 para determinar qué claves compartidas deben ser utilizados. En lugar de los valores DH (HVI y

[15] DWIVEDI, Himanshu. Hacking VoIP. USA, 2008. Págs. 180 -185

PVR), los puntos finales junto con las llaves se mantienen en secreto para obtener el material clave.

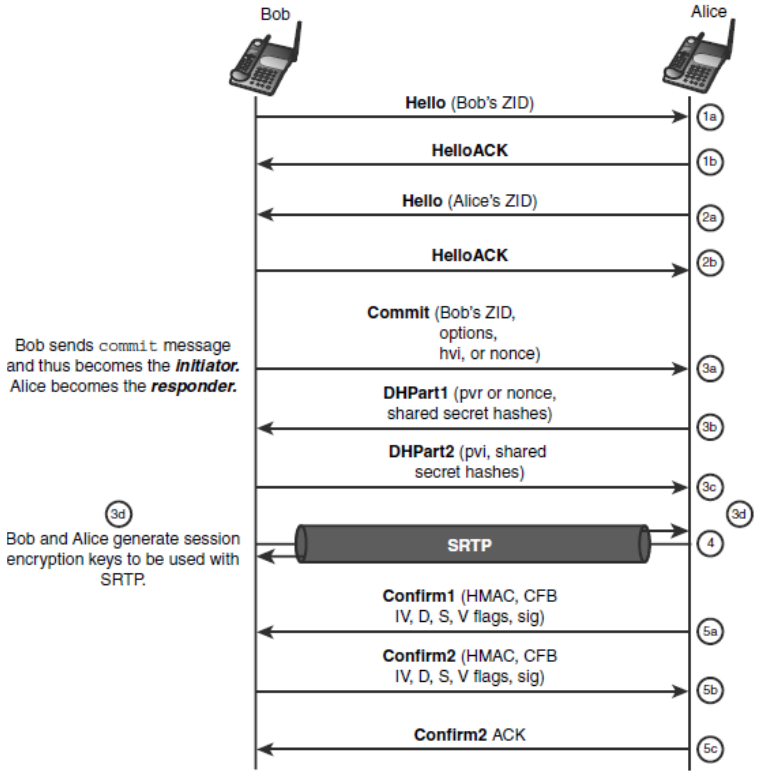


Figura 11 Negociación de clave ZRTP usando el modo Diffie-Hellman

En el Paso 1a, el teléfono de Bob envía un mensaje ZRTP *Hello* que contiene el valor ZRTP ID (ZID), la versión del protocolo, y las opciones para ser utilizado con ZRTP. La ZID es una cadena aleatoria de 96 bits generada al mismo tiempo durante la instalación del software que implementa ZRTP. Las opciones incluyen un hash, cifrado, métodos de autenticación y la longitud de la etiqueta, el tipo de acuerdo de claves y algoritmos compatibles con SAS (Short Authentication String).

Este mensaje inicial (Hello) se utiliza para verificar si el punto final remoto es compatible con ZRTP y también, anuncia los algoritmos de cifrado que pueden ser soportados por el destinatario. La ZID es un identificador único generado durante la instalación del ZRTP, y se utiliza como índice de caché para secretos compartidos que se han acumulado en las sesiones anteriores e identificar el secreto compartido del correspondiente punto final. Esto minimiza la necesidad de una renegociación de clave adicional si la misma ya es conocida por los puntos finales.

En el paso 1b, Alice envía un Hello ACK de su mensaje a Bob. Esto indica al teléfono de Bob que el teléfono de Alice soporta ZRTP y anuncia su ZID si no se sabe de una sesión anterior. El mensaje Hello ACK puede omitirse en los casos en que un punto final quiere entrar en el modo de negociación de inmediato, y el mensaje de confirmación se envía en su lugar. En el paso 2a, Alice envía un mensaje Hello similar al de Bob, quien a su vez responde con una Hello ACK (Paso 2b).En el paso 3a, los puntos finales pueden comenzar el acuerdo de la clave cuando el intercambio de mensajes del saludo inicial y Hello ACK se ha completado. El primer individuo que envía el mensaje de confirmación se considera el iniciador, la otra parte se convierte en el contestador. Si ambas partes envían el mensaje de confirmación al mismo tiempo, el individuo que ha generado el mayor HVI (valor hash) asume el papel de iniciador.

La HVI se calcula así, HVI = hash (PVI | Hello mensaje de respuesta), y el PVI (DH valor público) se calcula como PVI = g^{svi} mod p. El SVI (valor secreto) es una cadena generada aleatoriamente que se utiliza como el exponente en base g (un número basado en Diffie-Hellman grupo cíclico G). Además de los valores ZID y HVI, el mensaje de confirmación contienen un conjunto de opciones que consisten en el modo ZRTP, el tipo de valor hash, el cifrado, keya y SAS.

En el paso 3b, Alice (contestador) envía un mensaje a Bob DHPart1. El mensaje contiene un PVR y comparte secretos hashes (HMAC) que se utilizaron en la generación del secreto ZRTP. Hay cinco parámetros HMAC: rs1IDr, rs2IDr, sigsIDr, srtpsIDr y other_secretIDr.
En el paso 3c, Bob envía un mensaje DHPart2 que contiene su valor público DH y el ID secreto es calculado, al igual que DHPart1.

En el paso 3d, cada participante genera la llave maestra SRTP y salt utilizando el intercambio de un secreto compartido. Tenga en cuenta que hay dos flujos RTP en la sesión, uno de Bob a Alice y otro de Alice a Bob. Por lo tanto, cada flujo RTP usa diferentes claves RTP y salts. Cada extremo usa el srtpkey (i / r) y srtpsalt (i/ r) para cifrar y descifrar el correspondiente flujo RTP.

En los pasos 5a y 5b, los dos extremos intercambian de información sobre los puntos de esperanza de vida de la clave secreta compartida (el intervalo caché de vencimiento) con el mensaje de confirmación. Este mensaje sólo se envía en respuesta a un mensaje DHPart2 válida cuando la clave de negociación se ha realizado correctamente. Parte del mensaje de confirmación se cifra mediante CFB (Cipher Feedback Encryption mode) y protección de la integridad utilizando HMAC.

En el paso 5c el mensaje Conf2ACK envía al receptor un Confirm2 válido, y que se utiliza para detener la retransmisión de un mensaje más Confirm2. Para terminar el cifrado de los flujos, el mensaje GoClear usado. El mensaje no termina la sesión, pero altera el estado de los flujos RTP para ser encriptado y desencriptado. El Anexo 2proporciona una descripción de los campos de cabecera ZRTP.

2.4 ASPECTOS RELEVANTES DEL ESTÁNDAR

En este apartado se expondrá de forma sucinta cuales son las características que es necesario evaluar para realizar un análisis acerca de la conformidad con el estándar para la implementación de mecanismos de gestión de clave.
En el RFC 4046 se define la arquitectura de seguridad común para la multidifusión (MSEC) en protocolos de gestión clave para apoyar una variedad de aplicaciones, el transporte y protocolos de seguridad en capa de red. También se define el grupo de asociación de seguridad (GSA, group security association), y describe los protocolos de gestión de claves que ayudan a establecer un GSA.

El marco y las directrices descritas en el RFC 4046 permiten un diseño modular y flexible de los protocolos del grupo de gestión de claves para una variedad de configuraciones diferentes que se especializan en las necesidades de las aplicaciones. Los protocolos de gestión de claves MSEC se pueden utilizar para facilitar la seguridad en la comunicación de uno a muchos, muchos-a-muchos, o de uno-a-uno.

2.4.1 REQUISITOS DE UN PROTOCOLO DE GESTION DE CLAVE

Un grupo de protocolos de gestión de claves (GKM) permite la comunicación protegida entre los miembros de un grupo de seguridad. Un grupo de seguridad es una colección de principios, miembros de una llamada, emisores, receptores o

ambos de un grupo y la pertenencia a un grupo puede variar con el tiempo. Los protocolos de gestión de clave ayudan a asegurar que solo los miembros del grupo puedan tener acceso a los datos y puedan autenticarse. El objetivo de un grupo de protocolos de gestión de clave es proporcionar a los miembros legítimos del grupo con el cifrado necesario para asegurar la discreción y la autenticación.
Aplicaciones multidifusión, tales como transmisión de video, por lo general tienen los siguientes requisitos de gestión de claves. Hay que tener en cuenta que el RFC dice, que la lista no es adaptable a todas las aplicaciones.

1. Los miembros del grupo reciben asociaciones de seguridad que incluyen claves de cifrado, claves de autenticación / integridad, políticas de cifrado que describen las claves, y atributos para hacer referencia a la asociación de seguridad (SA) o de los objetos particulares que figuran en el SA.

2. Además de las políticas relacionadas con las claves de grupo, el propietario del grupo o el controlador del grupo y el servidor de claves (GCKS, Group Controller and Key Server

3. Definir y hacer cumplir la pertenencia al grupo, administración de claves de seguridad de datos, y otras políticas que pueden o no pueden ser comunicados a todos los miembros.

4. Las claves tienen una duración predeterminada y pueden ser actualizada periódicamente.

5. La clave debe ser entregada de forma segura a los miembros del grupo para que sean secretas, integras, protegidas y obtenidas de una fuente autorizada verificable.

6. El protocolo de administración de claves debe ser protegido contra ataques de repetición y de denegación de servicio (DoS).

7. El protocolo debe facilitar la adición y remoción de los miembros del grupo.

8. El protocolo debe ser compatible con las necesidades de infraestructura y el rendimiento de la aplicación de seguridad de datos, como por ejemplo, protocolos de seguridad en la capa aplicación como SRTP [RFC3711].

9. El protocolo de administración de claves debe ofrecer un marco para la sustitución o la renovación en la infraestructura de autorización de los sistemas de autenticación.

10. El protocolo de administración de claves debe ser protegido contra la confabulación entre los miembros excluidos y no miembros. En concreto, la confabulación no debe dar lugar a que los atacantes logren un secreto. En otras palabras, combinando el conocimiento de las entidades cómplices no deben dar lugar a revelar secretos del grupo adicionales.

11. El protocolo de administración de claves debe proporcionar un mecanismo para recuperar de forma segura desde un compromiso a la totalidad del material clave.

12. El protocolo de administración de claves debe hacer frente a problemas del mundo real de implementación, como NAT-transversal e interactuar con mecanismos de autenticación heredados.

2.4.2 PROTOCOLO DE CAMBIO DE CLAVES

El grupo del protocolo de cambio de claves sirve para transportar las claves y realizar una asociación segura (SA) entre un GCKS y los miembros de un grupo de comunicaciones seguras. A continuación, se listan algunas propiedades del protocolo para el cambio de claves:

El protocolo de cambio de claves se asegura de que todos los miembros reciben la información de cambio de claves en el momento oportuno.
El protocolo de cambio de claves especifica mecanismos que permitan a las partes estar en contacto con el GCKS y volver a sincronizarse, cuando expiran las llaves y no han recibido actualizaciones. El protocolo de cambio de claves evita los problemas de implosión y garantiza la fiabilidad en la entrega de información

Rekey. Además, el protocolo rekey es el principal responsable de la escalabilidad de la arquitectura del grupo de gestión de claves. Por lo tanto, es imperativo que nos proporcione las propiedades mencionadas anteriormente de una manera escalable.
Los objetivos del protocolo de cambio de claves son las siguientes:

- Sincronización con un GSA,
- Ofrecer privacidad y autenticación (simétrica o asimétrica), protección contra la reproducción y la protección contra la denegación de servicio,
- Cambio de claves eficaz después de los cambios en la pertenencia al grupo o cuando las llaves (KEKs) expiran,
- Entrega fiable de mensajes de cambio de claves,
- Recuperación de un miembro de GSA fuera de sincronización,
- Alto rendimiento y baja latencia
- Compatibilidad con IP multidifusión o multi-unicast.

Identificamos varias cuestiones importantes en el diseño de un protocolo de regeneración de claves:

1. Reintroducir el formato del mensaje,
2. Transporte fiable de mensajes de cambio de claves,
3. Implosión,
4. Recuperación de sincronización GSA,
5. Incorporación de GKMAs en los mensajes de cambio de claves, y
6. Interoperabilidad de los GKMAs.

Aunque estos mecanismos pueden ser incluidos en el área de correcta implementación de las herramientas criptográficas debido a que los mecanismos de autenticación se basan en herramientas criptográficas más o menos complejas, la importancia de la autenticación en los protocolos de seguridad aconseja prestar especial atención a este aspecto. Los diferentes mecanismos de autenticación que se utilizan en la actualidad pueden variar desde una simple contraseña (un secreto preestablecido) hasta cadenas de certificación que utilizan los servicios de una autoridad de certificación y una infraestructura de clave pública completa. En el caso en que un protocolo soporte múltiples métodos de autenticación, la guía de referencia debería proporcionar los medios determinar el adecuado.

2.4.3 RENDIMIENTO

El hardware en conjunto con el software, conforman las piezas fundamentales e indispensables de un Sistema Informático. Como bien sabemos, el hardware, actúa en sintonía en todo momento con el software. Por esta razón básica, de nada sirve tener buen hardware si nuestro sistema posee problemas ajenos a éste, como pueden ser los cuellos de botella, sobrecarga de procesos en relación a la memoria disponible, poco espacio en disco a razón de una mala administración de las cuotas. Para poder lo anteriormente, es necesario realizar lo que se conoce como pruebas de rendimiento. Como su nombre lo indica, las pruebas de rendimiento son aquellas que tratan de probar un determinado comportamiento de un sistema bajo ciertas condiciones. Las pruebas de rendimiento realizadas en un lapso de tiempo nos dan la pauta de que estamos considerando distintos instantes y variaciones del estado actual de un sistema, el cual nos proveerá un flujo de información más homogénea a la hora de analizar. A estas pruebas de rendimiento también se las suele denominar, de manera indistinta, como pruebas de stress. Las condiciones demandantes básicas que afectan de manera directa a la ejecución y tiempo de respuesta de los recursos del sistema son las siguientes:

- CPU, Tiempo consumido en el procesado de datos sobre el o los CPU(s) de una máquina.
- Memoria, Tiempo consumido en lectura y escritura para y proveniente de la memoria real.
- Redes, Tiempo consumido en lectura y escritura para y proveniente de la red.

Para analizar de manera objetiva el resultado de las pruebas de rendimiento y así poder mejorar las prestaciones de un sistema, es conveniente tener en cuenta una serie de factores.

- Conocer el Entorno de Ejecución, es conveniente saber qué es lo que realmente hace el sistema. Es decir, conocer qué servicios tiene activados, qué procesos arrancan en conjunto con el sistema, para qué sirven y se utilizan. No es necesario saber absolutamente todo, pero sí una vaga noción del entorno donde estaremos realizando las pruebas, así a la hora de encontrar problemas, nos sea más fácil identificar la raíz de los mismos.
- Conocer básicamente el hardware a optimizar: para mejorar algo es primordialmente necesario saber si es susceptible de mejora. Cuando se

realicen las pruebas de rendimiento, el encargado de las mismas deberá conocer básicamente el hardware subyacente (CPU, Memorias, Cache, I/O, etc.) y su interconexión para poder determinar dónde están sus problemas.

Para realizar las pruebas de rendimiento, utilizare particularmente la herramienta sar (System Activity Report). Esta herramienta nos permite mostrar una gran cantidad de información estadística de rendimiento de nuestro equipo, como por ejemplo el uso de las distintas CPUs, la carga del sistema, el uso de memoria, I/I, redes, etc. Para ello tendremos que definir los parámetros que queremos monitorizar, el período entre cada muestra y el número de muestras que vamos a tomar.

Esta herramienta forma parte del paquete SysStat que es una colección de herramientas de monitorización de rendimiento. Esta suite nos proporciona herramientas que nos pueden mostrar datos instantáneos de rendimiento, así como almacenarlos como históricos para nuestra futura referencia. Especialmente en entornos de servidor, sus datos nos proporcionan información muy valiosa sobre las posibles carencias y cuellos de botella de nuestro sistema. En particular, haremos especial enfoque sobre la herramienta sar, que es la más completa de todas e incluso nos proporciona la misma información que nos brindan otras herramientas en conjunto.

Otra herramienta que proporcionará información relevante es Vnstat, la cual emitirá informes de uso de ancho de banda. Para verificar jitter y paquetes perdidos nos ayudaremos de la herramienta incorporada en el CLI de Asterisk, esta es channelsstats.

CAPÍTULO III
MATERIALES Y MÉTODOS

En esta sección se muestra los procesos metodológicos para la elaboración de esta tesis. Se presentan el tipo de investigación, las técnicas y procedimientos que fueron utilizados en esta investigación.

3.1 TIPO DE LA INVESTIGACIÓN

Por la naturaleza de la investigación se considera que el tipo de estudio que se va a realizar es una investigación correlacional: este tipo de estudio descriptivo tiene como finalidad determinar el grado de relación o semejanza entre dos variables sin pretender establecer una explicación completa de la causa. "Se caracterizan porque primero se miden las variables y mediante pruebas de hipótesis correlacionales y a la aplicación de técnicas estadísticas, se estima la correlación. Aunque la investigación correlacional no establece de forma directa relaciones causales, puede aportar indicios sobre las posibles causas de un fenómeno. Este tipo de investigación descriptiva busca determinar el grado de relación existente entre las variables"[16].

3.2 DISEÑO DE LA INVESTIGACIÓN

El presente proyecto de Investigación se enmarca en una forma de diseño cuasi experimental – transaccional:

- Cuasi experimental: las unidades de análisis no se asignan al azar ni por apareamiento aleatorio. La carencia de aleatorización implica la presencia de posibles problemas de validez tanto interna como externa. La validez interna se ve afectada por el fenómeno de selección, la regresión estadística y el proceso de maduración. La validez externa se ve afectada por la variable población, es decir, resulta difícil determinar a qué población pertenecen los

[16] Fuente: http://www.buenastareas.com/ensayos/Investigacion-Correlacional/1511889.html.

grupos. La estructura de los diseños cuasi experimentales implica usar un diseño solo con pos prueba.

- Transversal: en donde se recopilan datos en un momento único, con el propósito de describir variables y analizar su incidencia e interrelación en un momento dado.

Se ha realizado las siguientes consideraciones para la investigación:

- Se elabora un marco teórico que ayude a crear una idea general para la realización del trabajo de investigación.
- Se analizará los siguientes mecanismos de gestión de clave: SRTP Descriptions y ZRTP.
- Se elegirá al mecanismo de gestión de clave que mejor prestaciones presente.
- Se justifican los motivos por los cuales se propone realizar la investigación.
- Se plantea una hipótesis la cual es una posible respuesta al problema planteado y posee una íntima relación entre el problema y el objetivo.
- Se propone la operacionalización de las variables en base a la hipótesis planteada.
- Se realiza la recolección de datos, y se observará el comportamiento del ambiente de pruebas en la transferencia de datos, en una primera instancia sin la utilización de mecanismos de gestión de clave, en una segunda instancia con el uso del mecanismo de gestión de clave elegido, se procederá a configurarlo y tomar datos.
- Se realiza la prueba de la hipótesis con los resultados obtenidos.
- Se elaborará una Guía Referencial (Ver Cap. 5) para la evaluación de mecanismos de gestión de clave que en el futuro puedan surgir.
- Se elabora las conclusiones y recomendaciones, producto de la investigación realizada.

3.3 MÉTODOS Y TÉCNICAS

3.3.1 MÉTODOS

Los Métodos utilizados en la presente investigación son los siguientes:

- **Método Comparativo:** Comparación de los mecanismos de gestión de clave.
- **Cualitativo**: Delineación de la Guía Referencial para la evaluación de nuevos mecanismos de gestión de clave**.**
- **Cuantitativo**: Se interpreta y se procesa para explicar eventos o análisis de información a través de ciertos datos.

Análisis descriptivo e interpretación de las mediciones a partir de un estudio comparativo.

3.3.2 TÉCNICAS

Además se utilizará ciertas técnicas, en las que se enmarcan:

- Observación
- Análisis
- Recopilación de información
- Razonamiento y pruebas

3.4 FUENTES DE INFORMACIÓN

- Artículos científicos, revistas especializadas
- RFC (del ingles, Request For Comment), eestándares

3.5 RECURSOS

3.5.1 RECURSOS HUMANOS

- Investigador
- Tutor
- Colaboradores y asesores Externos

3.5.2 RECURSOS TÉCNICOS

a. HARDWARE

- PC
- Impresora

b. SOFTWARE

- Sistema Operativo
    - CentOS 6
    - Microsoft Windows Xp.
- PBX Software
    - Asterisk 1.8.7
- Softphome
    - Blink 0.2.7 SIP client.
    - Xlite 4.0
- Gstat y SPSS 20
- Cliente ssh
    - PuTTy
- Microsoft Office.
    - Microsoft Office Word 2007
    - Microsoft Office Excel 2007
- Navegador
    - Google Crhome.

c. OTROS

- Bibliografía
- Internet
- Revistas Especializadas

3.5.3 RECURSOS MATERIALES

Tabla 4 Recursos Materiales.

MATERIAL	DESCRIPCIÓN	CATEGORÍA
Bibliográfico	Actualidad	Investigación Actual
Libros		
Revistas		
Papers		
Escritorio	Dispositivo Almacenamiento Dispositivo Impresión	Respaldo Información Impresión Documentos
Flash Memory		
CD		
Tonner		
Hojas		

3.5.4 RECURSOS ECONÓMICOS

El desarrollo de este proyecto será autofinanciado, se presenta un detalle del presupuesto tentativo a ser utilizado en la tabla mostrada a continuación.

Tabla 5 Recursos económicos a utilizarse en el proyecto

Nominación	Cantidad	Precio Unitario	Subtotal	Total
Pc	1	$ 800	$ 800	$ 800,00
VPS	1	$25	$150	$150
Hojas	2	$ 5,00	$ 10	$ 30,00
Tonner	1	$ 20,00	$ 20	$ 20,00
Internet	6 meses	$ 40,00	$240	240,00
Total				**$ 1240,00**

3.6 PLANTEAMIENTO DE LA HIPÓTESIS

La selección de un mecanismo de gestión de clave determinará el nivel de rendimiento en la transmisión de voz segura sobre el protocolo IP

3.7 OPERACIONALIZACIÓN DE LAS VARIABLES

- **Variable Independiente**
  Mecanismos de gestión de clave
- **Variable Dependiente**
  Nivel de rendimiento en la transmisión de voz segura sobre IP

La operacionalización conceptual y metodológica de las variables se muestra en la tabla 6 y tabla 7 respectivamente.

3.7.1 OPERACIONALIZACIÓN CONCEPTUAL

Tabla 6 Operacionalización Conceptual de las variables del proyecto de investigación

VARIABLE	TIPO	DEFINICIÓN
Mecanismos de Gestión de Claves	Independiente	Estudio de mecanismos de gestión de clave, considerando el estándar para elaborar la guía referencial.
Nivel de rendimiento en la transmisión de voz segura sobre IP	Dependiente	Esta establecido por el ancho de banda, tiempo de proceso, memoria, jitter, paquetes perdidos, paquetes transmitidos y recibidos.

3.7.2 OPERACIONALIZACIÓN METODOLÓGICA

Tabla 7 Operacionalización Metodológica de las variables.

HIPÓTESIS	VARIABLES	INDICADORES	INSTRUMENTOS
La selección de un mecanismo de gestión de clave seguro determinará el nivel de rendimiento en la transmisión de voz sobre el protocolo IP.	Mecanismos de gestión de claves.	• Especificación de módulo criptográfico. • Puertos del módulo criptográfico. • Funciones servicios y autentificación. • Modelo de estado finito. • Seguridad física. • Entorno operacional. • Gestión de clave criptográfica • EMI/EMC. • Selttests. • Aseguramiento del diseño. • Mitigación a otros ataques.	• Análisis • Razonamiento • Recopilación de información.
	Rendimiento en la transmisión de voz sobre IP.	• Paquetes transmitidos. • Paquetes recibidos • Tiempo de proceso. • Ancho de banda. • Uso de memoria • Jitter • Paquetes perdidos	• Experimentos • Documentos bibliográficos • Recopilación de información.

3.8 POBLACIÓN Y MUESTRA

La población constituye el objeto de la investigación y de ella se extrae la información requerida para el estudio respectivo, es decir los mecanismos de gestión de clave: SRTP Descriptions y ZRTP
Esta población se seleccionó basándose en una muestra no probabilística, tomada de dos fuentes de selección: artículos científicos (Referirse a la bibliografía) y revistas especializadas para determinar el apropiado.

La población es el conjunto total de individuos, objetos o medidas que poseen algunas características comunes observables en un lugar y en un momento determinado, constituye el objeto de la investigación, de donde se extrae la información requerida para el estudio; es decir, en este caso para nuestro objetivo la población serán las llamadas VoIP realizadas a través de una PBX software, en este caso Asterisk y utilizando softphones.

Luego debemos seleccionar una porción representativa de la población, que permita generalizar los resultados de una investigación. El objetivo principal de la selección de la muestra es extraer información que resulta imposible estudiar en la población, porque esta incluye la totalidad.

Anteriormente se indicó, que se ha definido la utilización de una muestra no aleatoria ya que los elementos representativos están determinados por el tipo de investigación realizada, por lo tanto, se considerará la implementación de una central telefónica software la misma que se instalará sobre un VPS y dos computadores en las que se instalará el softphone Blink 0.2.4 para realizar una llamada con una duración aproximada de dos minutos.

3.9 INSTRUMENTOS DE RECOLECCIÓN DE DATOS

De acuerdo a los procedimientos generales establecidos se ha determinado la utilización de dos computadores en los que se instaló el softphone Blink, además, la utilización de un VPS, como su nombre lo indica es un servidor virtual que funciona sobre hardware real, teniendo la posibilidad de compartir los recursos físicos entre varios usuarios, esto hace que los costos e

implementación del servidor de telefonía se reduzcan drásticamente. La idea básicamente es tener dos escenarios, el primero realizar pruebas sin el uso de algún mecanismo de gestión de clave y el segundo luego de un análisis escoger el mecanismo adecuado para realizar pruebas y obtener los datos necesarios.

ESCENARIO 1: Llamada IP sin mecanismo de protección.

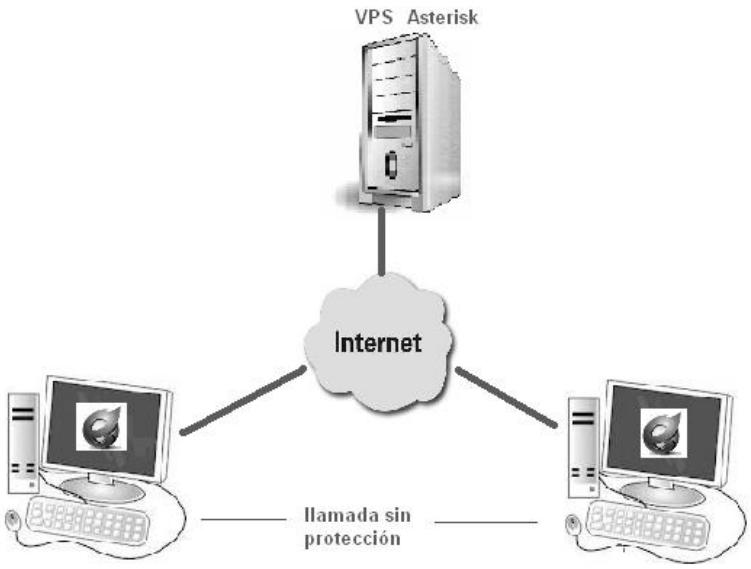


Figura 12 Llamada VoIP sin mecanismo.

Descripción de equipos y software, presentados en las tablas 8 y 9.

Tabla 8 Equipos utilizados para llamadas IP para el test de control.

Cantidad	Equipo	Marca	Modelo	Especificaciones
1	VPS	Linode	Xeon	512 MB de Ram, 20 GB almacenamiento y transferencia de 200 GB.
2	Pc	Clon	Intel PIV	1 GB de Ram, 250 MB HD.

Tabla 9 Software utilizado para la llamada IP

Nombre	Descripción
Asterisk 1.8.7	Aplicación de software libre con licencia GPL que proporciona funcionalidades de central telefónica.
Blink 0.2.4	Cliente simple de SIP que permite realizar las llamadas entre usuarios, disponible en Windows, Linux y Mac
SysStat	Herramienta que cuenta con varias utilidades que permiten el monitoreo del desempeño y actividad de diferentes objetos del servidor.
Vnstat,	Es una utilidad que permite monitorear el tráfico de red, en nuestro Linux CentOS. Si se activa como servicio, guardará todas las estadísticas de dicho tráfico.
Sip show channelstat	Aplicación incluida en Asterisk y accesible desde el CLI, permite observar jitter y packet perdidos de una comunicación.

En este escenario básicamente se realiza la llamada entre dos usuarios con una duración aproximada de dos minutos y con la ayuda de las herramientas que figuran en la Tabla 9, se extraen y recopilan los datos.

ESCENARIO 1: Llamada IP aplicando algún mecanismo de protección.

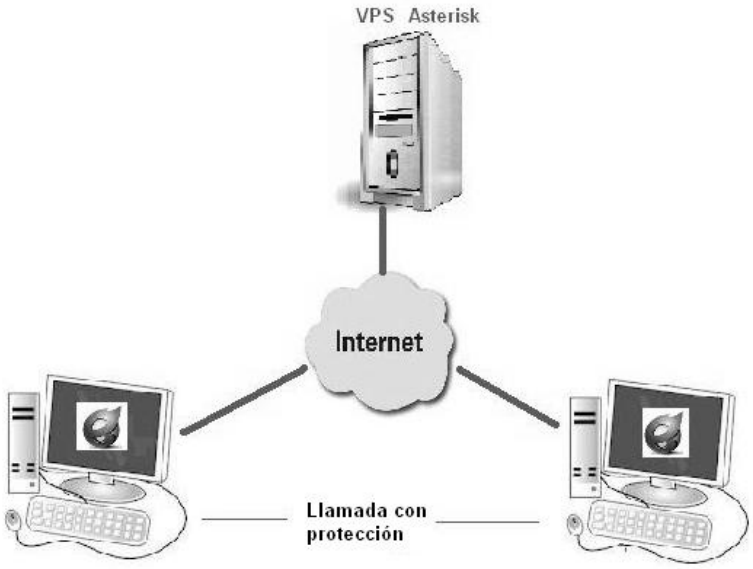


Figura 13 Llamada VoIP con mecanismo.

Descripción de equipos y software, mostrados en las tablas 10 y 11.

Tabla 10 Equipos utilizados para llamadas IP con mecanismos.

Cantidad	Equipo	Marca	Modelo	Especificaciones
1	VPS	Linode	Xeon	512 MB de RAM, 20 GB almacenamiento y transferencia de 200 GB.
2	Pc	Clon	Intel PIV	1 GB de RAM, 250 MB HD.

Tabla 11 Software utilizado para la llamada IP con mecanismos.

Nombre	Descripción
Asterisk 1.8.7	Aplicación de software libre con licencia GPL que proporciona funcionalidades de central telefónica.
Blink 0.2.4	Cliente simple de SIP que permite realizar las llamadas entre usuarios, disponible en Windows, Linux y Mac
SysStat	Herramienta que cuenta con varias utilidades que permiten el monitoreo del desempeño y actividad de diferentes objetos del servidor.
Vnstat,	Es una utilidad que permite monitorear el tráfico de red, en nuestro Linux CentOS. Si se activa como servicio, guardará todas las estadísticas de dicho tráfico.
Sip show channelstat	Aplicación incluida en Asterisk y accesible desde el CLI, permite observar jitter y packet loss de una comunicación.
Libsrtp	Librería que permite el soporte para la encriptación del medio.

En este escenario básicamente se realiza la llamada entre dos usuarios con una duración aproximada de dos minutos y con la ayuda de las herramientas que figuran en la Tabla 3.8, se extraen y recopilan los datos, pero en este caso se aplicará algún mecanismo de gestión de clave sobre SRTP.

Para la ejecución de las utilidades de SysStat, éste cuenta con un estándar básico para la mayoría de sus comandos, los cuales deben ir seguidos de un intervalo de tiempo a monitorear y cuantas mediciones se debe realizar, es decir, debe tener la siguiente sintaxis[17]:

[17]GODARD, Sebastien. Sysstat. Documentation. http://sebastien.godard.pagesperso-orange.fr/documentation.html. Fecha de publicación: 02/2010 Fecha Acceso: 04/2011

Tabla 12 Sintaxis para uso de herramientas SysStat.

Comando [opción] intervalo [contador_mediciones]
Ejemplo: sar – B 300 5
Descripción: Ejecuta el comando sar con la opción –B reportando estadísticas de paginación cada 5 minutos, tomando 5 mediciones.

El estudio de la variable independiente esta específicamente relacionada a un estudio teórico para determinar el mecanismo mejor con respecto a la seguridad. En la tabla 12 se muestra la sintaxis a ser utilizada en el VPS, específicamente se tomaran muestras de la variable dependiente, es decir, paquetes transmitidos, paquetes recibidos, tiempo de CPU y uso de memoria usando la herramienta SysStat. Para la medición del ancho de banda se utilizara la herramienta Vnstat y para la medición de jitter se hará uso de channelsstat una herramienta incorporada en Asterisk. En el anexo 4 se incluyen los datos recolectados en el test de control como el test utilizando un mecanismo de gestión de clave.

CAPÍTULO IV
RESULTADOS Y DISCUSIÓN

4.1 VARIABLE INDEPENDIENTE

4.1.1 DETERMINACIÓN DE PARÁMETROS DE COMPARACIÓN

Para realizar el estudio y selección de un mecanismo de gestión de clave y con el cual se realizarán las pruebas, se tomó en consideración los parámetros necesarios, que permitirán evaluar las cualidades o falencias de srtp descriptions y zrtp. La gestión de claves es un asunto fundamental en la seguridad, es la base para establecer una comunicación segura mediante tecnologías de cifrado entre los participantes de una conversación VoIP.

Los indicadores han sido tomados de artículos científicos, de la FIPS (del inglés, Federal Information Processing Standards Publication), RFC 4568 y RFC 6189. El análisis de la variable independiente básicamente se enfoca en la norma de FIPS PUB 140-2, la cual establece cuatro niveles de seguridad. Estos niveles se destinan a cubrir una amplia gama de posibles aplicaciones y entornos en los que módulos criptográficos pueden ser empleados. Los requisitos de seguridad cubren once áreas relacionadas con el diseño y la ejecución segura de los módulos criptográficos y estas son las siguientes[18]:

- Especificaciones del módulo criptográfico.
- Puertos del módulo criptográfico e interfaces.
- Funciones servicios y autentificación.
- Modelo de estado finito.
- Seguridad física.
- Entorno operacional.
- Gestión de clave criptográfica
- Interferencia electromagnética/Compatibilidad electromagnética (EMI/EMC).
- Selt tests.
- Aseguramiento del diseño.

[18] NIST http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

- Mitigación de otros ataques.

.

Para el análisis de cada indicador de la variable independiente se le dará a la calificación cualitativa un valor como se muestra a continuación, teniendo en ella cuatro niveles de seguridad:

Tabla 13 Correspondencias para los niveles de seguridad.

Calificación	Abreviatura	Valor asignado
Nivel de Seguridad 1	NS1	1
Nivel de Seguridad 2	NS2	2
Nivel de Seguridad 3	NS3	3
Nivel de Seguridad 4	NS4	4

Los valores referidos en los índices de la variable independiente se asignan de acuerdo a la siguiente escala cuantitativa:

Tabla 14 Escala cuantitativa. Variable independiente.

Valoración			
NS1 (1)	NS2 (2)	NS3 (3)	NS4 (4)
25%	50%	75%	100%

4.1.1.1 NIVEL DE PROTECCIÓN 1

Este nivel se presenta como el más bajo en seguridad. Los requisitos básicos de seguridad especificados para un módulo criptográfico, por ejemplo, debe ser utilizado, al menos un algoritmo aprobado o función de seguridad autorizado. No existen mecanismos específicos de seguridad física los cuales son requeridos en un módulo a nivel de seguridad de cifrado.

El nivel de seguridad 1 permite a los componentes software y firmware de un módulo criptográfico a que se ejecuten en un sistema informático de uso general, utilizando un sistema operativo sin evaluar. Estas implementaciones pueden ser adecuadas para algunas aplicaciones de seguridad de bajo nivel cuando otros controles, tales como la seguridad física, seguridad de red y los procedimientos administrativos son limitados o inexistentes.

4.1.1.2 NIVEL DE PROTECCIÓN 2

Este nivel mejora los mecanismos de seguridad física de un módulo de cifrado mediante la adición de un requisito de prueba de manipulación criptográfico, además, este nivel requiere como mínimo la autentificación y autorización de un operador para asumir su rol especifico y realizar un conjunto de correspondientes servicios, también, permite a los componentes software y firmware de un módulo criptográfico a que se ejecute en un sistema informático de uso general que cumpla con los requisitos funcionales especificados en el Common Criteria (CC).

4.1.1.3 NIVEL DE PROTECCIÓN 3

Además de los mecanismos de seguridad a prueba de manipulaciones físicas, el nivel 3 intenta evitar que el intruso tenga acceso a los CSP del módulo criptográfico. En este nivel se requiere que los mecanismos de autentificación mejoren la autentificación basándose en roles específicos, es decir, un módulo criptográfico autentica la identidad de un operador y comprueba que el operador autentificado está autorizado a asumir el papel específico para así poder realizar el conjunto correspondiente de servicios.

4.1.1.4 NIVEL DE PROTECCIÓN 4

Este nivel proporciona el máximo nivel de seguridad, en este nivel los mecanismos de seguridad proporcionan una completa protección al módulo criptográfico con la intención de detectar y responder a todos los intentos no autorizados de acceso. El nivel de seguridad 4 los módulos criptográficos son útiles para el funcionamiento en entornos físicamente sin protección.

- **Indicador 1:** Especificaciones del módulo criptográfico

Tabla 15 Resultados Especificación módulo criptográfico.

MGC	NS 1 (25%)	NS 1 (50%)	NS 1 (75%)	NS 1 (100%)
Zimmermannsecure RTP	-	-	-	✓
SDescriptions	-	-	-	✓

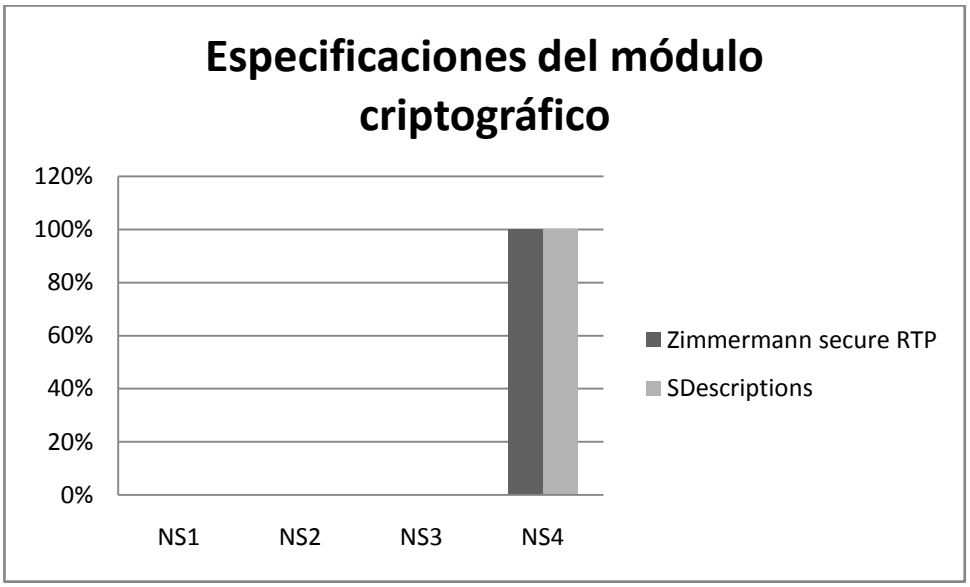


Figura 14 Porcentaje de módulo criptográfico.

Interpretación:

Un módulo criptográfico será un conjunto de hardware, software, firmware o alguna combinación de estos, que implementan las funciones criptográficas o de procesos, incluidos los algoritmos de cifrado y opcionalmente la generación de claves dentro de un límite definido de cifrado, un módulo criptográfico llevará a cabo al menos una función de seguridad aprobada. El algoritmo criptográfico que usan las implementaciones es AES, por lo tanto ambos mecanismos tienen un nivel de seguridad del cien por ciento.

- **Indicador 2:** Puertos del módulo criptográfico e interfaces

Tabla 16 Resultados puertos e interfaces del módulo criptográfico.

MGC	NS 1 (25%)	NS 1 (50%)	NS 1 (75%)	NS 1 (100%)
Zimmermannsecure RTP	-	-	✓	-
SDescriptions	-	-	-	✓

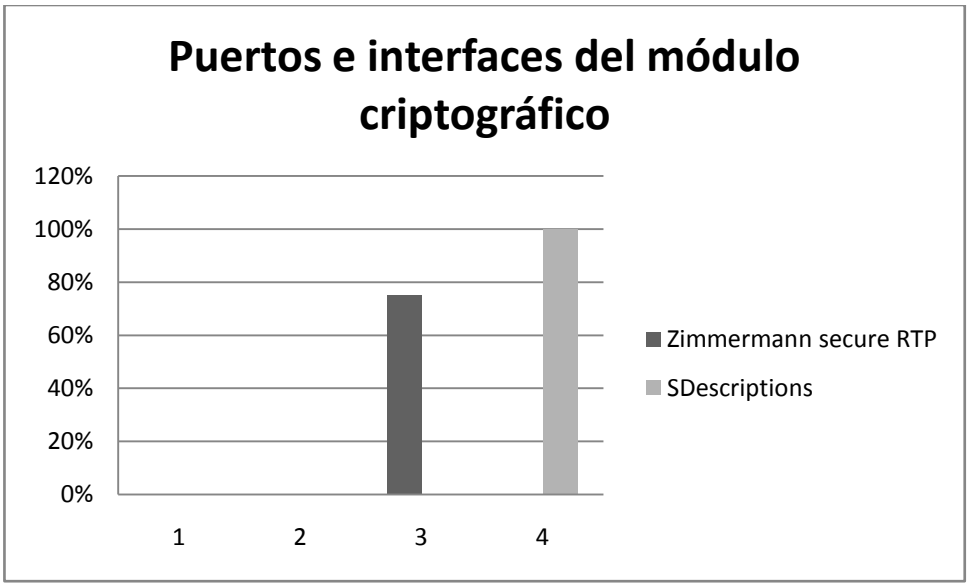


Figura 15 Resultados puertos e interfaces del módulo criptográfico

Interpretación:

Consiste en que el módulo criptográfico restringirá todo flujo de información y puntos de acceso físico a los puertos e interfaces lógicas que definen todos los puntos de entrada y salida desde o hacia el modulo. Las interfaces de módulo criptográfico serán lógicamente distintas unas de otras a pesar de que pueden compartir un puerto físico. A ZRTP. se le otorga el 75% debido a que este implementa un software llamado zfone el mismo que se ejecuta como una aplicación en una PC y los puertos en dicho ordenador podrían estar abiertos, en cambio SDescriptions tiene el 100%, pues ejecuta la encriptación a través de la PBX en el que los puertos están debidamente cerrados.

- **Indicador 3:** Funciones, servicios y autenticación

Tabla 17 Resultados con respecto a las funciones

MGC	NS 1 (25%)	NS 1 (50%)	NS 1 (75%)	NS 1 (100%)
Zimmermannsecure RTP	-	-	✓	-
SDescriptions	-	-	✓	-

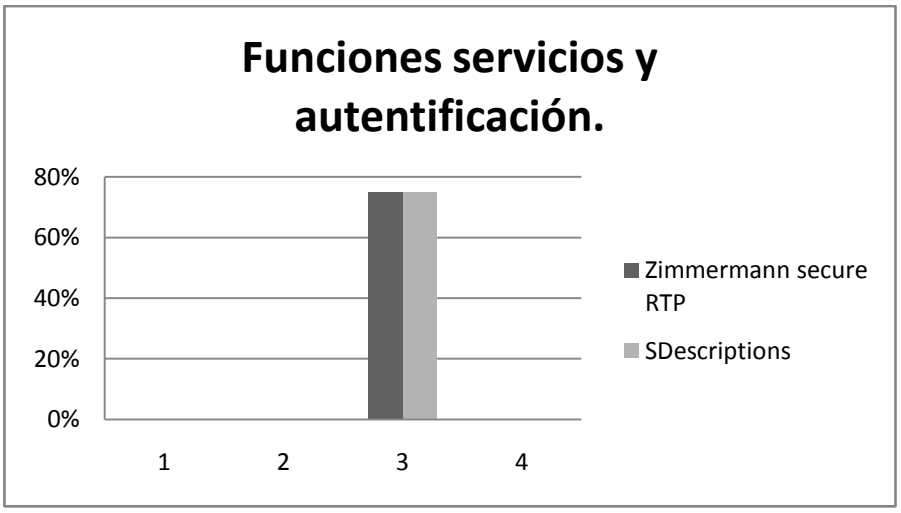


Figura 16 Resultados funciones servicios y autentificación.

Interpretación:

Un módulo criptográfico deberá dar soporte a funciones autorizadas para los operadores y los servicios correspondientes dentro de cada función. Múltiples funciones pueden ser asumidas por un solo operador. Mecanismos de autenticación pueden ser necesarios en un módulo criptográfico para autentificar a un operador y dar acceso al módulo, también, para verificar que el operador este autorizado a asumir la función y realizar los servicios solicitados. Los servicios se refieren a los servicios, operaciones o funciones que pueden ser realizados por un módulo de cifrado. Las entradas se compondrán de los datos o entradas de control para el inicio del módulo criptográfico. Las salidas se compondrán de todas las salidas de datos y el estado que se derivan de los servicios, operaciones o funciones iniciadas u obtenidas en la entrada. Los RFC's no especifican claramente estas funciones de autenticación como certificados digitales que usa SRTPDES o clave efímera de ZRTP, por ello se les asignó el porcentaje de 75%.

- **Indicador 4:** Modelo de estado finito

Tabla 18 Modelo de estado finito.

MGC	NS 1 (25%)	NS 1 (50%)	NS 1 (75%)	NS 1 (100%)
Zimmermannsecure RTP	**-**	✓	**-**	**-**
SDescriptions	**-**	**-**	✓	**-**

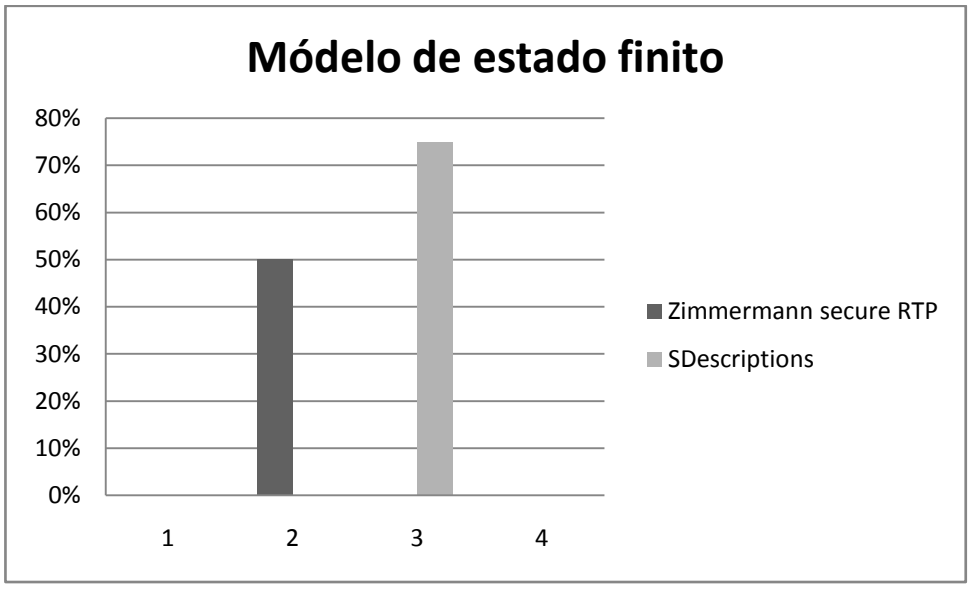


Figura 17 Resultados del modelo de estado finito.

Interpretación:

El funcionamiento de un módulo criptográfico se especifica mediante un modelo de estados finitos, representado por un diagrama y/o una tabla de transición de estado.

El diagrama y/o una tabla de transición de estado incluye: todos los estados de funcionamiento y error de un módulo criptográfico, las correspondientes transiciones de un estado a otro, los eventos de entrada que hacen transición de un estado a otro y los eventos de salida resultantes de transición de un estado a otro. Es la recuperación entre dos nodos de comunicación con el objetivo de poseer una alta disponibilidad en la red. El RFC 6189 no hace referencia a este

modelo, pero ello no quiere decir que no posea, por ello se le otorga un valor 50%, en cambio el RFC 3711 lo hace de forma explicativa en este sentido tiene el 75%.

- **Indicador 5:** Seguridad física

Tabla 19 Seguridad física.

MGC	NS 1 (25%)	NS 1 (50%)	NS 1 (75%)	NS 1 (100%)
Zimmermannsecure RTP	-	✓	-	-
SDescriptions	-	-	✓	-

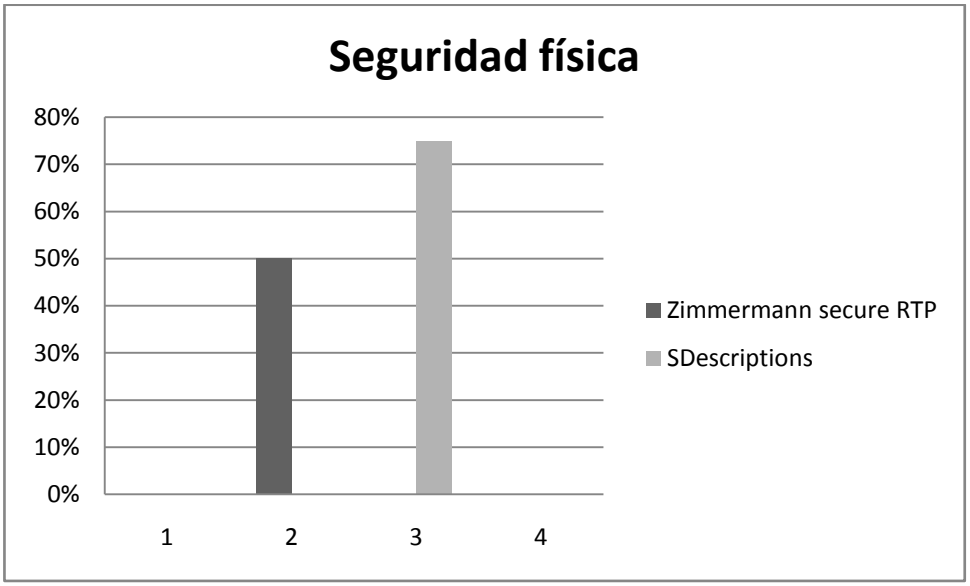


Figura 18 Resultados de la seguridad física.

Interpretación:

Un módulo criptográfico emplea mecanismos de seguridad física con el fin de restringir el acceso físico no autorizado a los contenidos del módulo e impedir el uso no autorizado o la modificación del módulo cuando se instala. Todo el hardware, software, firmware y componentes de datos dentro de los límites criptográficos deben estar protegidos. Un módulo criptográfico completamente software la seguridad física es proporcionado únicamente por la plataforma escogida y no está sujeta a los requisitos de seguridad física del estándar FIPS

PUB 140-2 del NIST. Debido a que Zrtp se ejecuta como una aplicación en un ordenador personal puede no brindar la seguridad necesaria por ello se le asignó un valor del 50% en cambio a SDescriptions se le asigna un 75% por que los servidores podrían ser vulnerados.

- **Indicador 6:** Entorno operacional

Tabla 20 Entorno operacional.

MGC	NS 1 (25%)	NS 1 (50%)	NS 1 (75%)	NS 1 (100%)
Zimmermannsecure RTP	-	✓	-	-
SDescriptions	-	-	-	✓

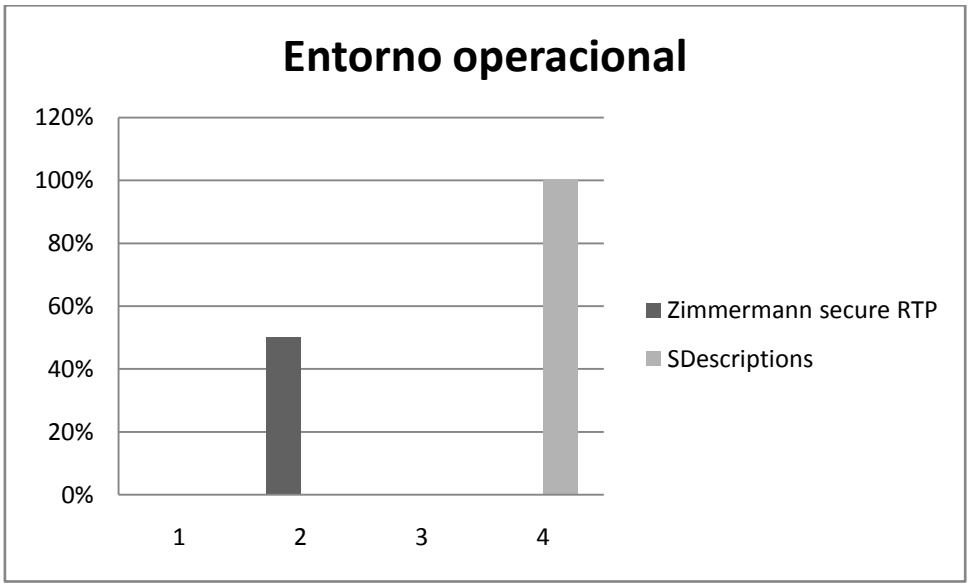


Figura 19 Resultados de entorno operacional.

Interpretación:

El entorno operativo de un módulo criptográfico se refiere a la gestión del software, firmware y/o a los componentes hardware necesarios para operar el módulo. El entorno operativo puede no ser modificable (p.ej. el firmware contenida en la memoria ROM o software contenido en el computador) o modificable (p.ej. firmware contenida en la memoria RAM o el software ejecutado por un computador de propósito general). Un sistema operativo es un componente importante para el

módulo criptográfico. Zrtp tiene el 50% debido a que se ejecuta como un software de capa de aplicación y los riesgos de vulnerar el sistema operativo son altos, sin embargo, SDescriptions se ejecuta bajo Linux un sistema operativo robusto para la ejecución de este tipo de módulos criptográficos por ello tiene un nivel de seguridad alto, es decir, 100%.

- **Indicador 7:** Gestión de clave criptográfica

Tabla 21 Gestión de clave criptográfica.

MGC	NS 1 (25%)	NS 1 (50%)	NS 1 (75%)	NS 1 (100%)
Zimmermannsecure RTP	-	-	-	✓
SDescriptions	-	-	-	✓

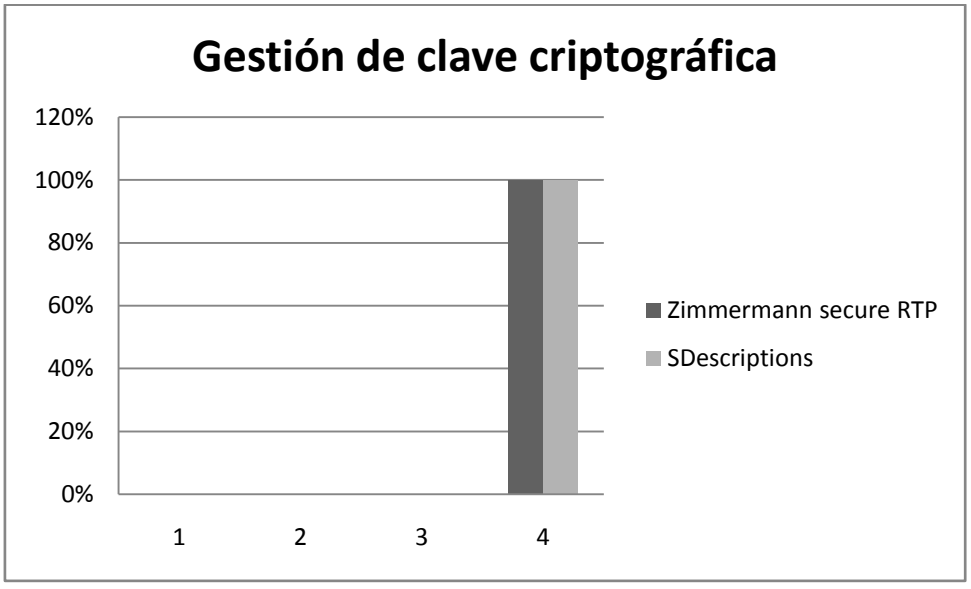


Figura 20 Resultados de Gestión de clave criptográfica.

Interpretación:

Los requisitos de seguridad para la gestión de claves criptográficas abarcan todo el ciclo de vida del cifrado de claves, cifrado de componentes clave y los parámetros de seguridad críticos empleados por el módulo criptográfico. La gestión de clave incluye números aleatorios y generación de clave, establecimiento de clave, distribución de clave, clave de entrada/salida, almacenamiento de clave y el

borrado electrónico de todos los datos almacenados y claves criptográficas (zeroization). Un módulo criptográfico también puede emplear mecanismos de gestión de clave de otros módulos criptográficos. En este sentido ambos mecanismos permiten realizar lo anterior descrito, esto de acuerdo a los RFC's.

- **Indicador 8:** Interferencia electromagnética y Compatibilidad electromagnética (EMI/EMC)

Tabla 22EMI/EMC

MGC	NS 1 (25%)	NS 1 (50%)	NS 1 (75%)	NS 1 (100%)
Zimmermannsecure RTP	✓	-	-	-
SDescriptions	✓	-	-	-

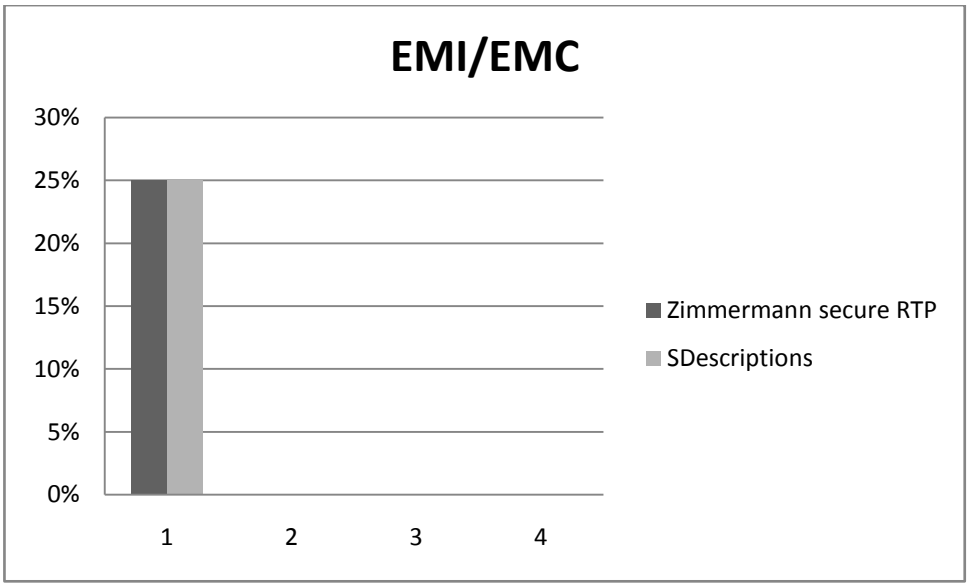


Figura 21 Resultados de EMI/EMC.

Interpretación:

Los módulos criptográficos deberán cumplir los requisitos para EMI/EMC. Los radios están explícitamente excluidos de estos requisitos, pero deberán cumplir todos los requisitos de la FCC. La documentación debe incluir la prueba de

conformidad con los requisitos para EMI/EMC. Los RFC's no hacen referencia a EMI/EMC, es por ello que se la ha asignado el porcentaje más bajo de la escala.

- **Indicador 9.** Auto pruebas

Tabla 23 SelftTests.

MGC	NS 1 (25%)	NS 1 (50%)	NS 1 (75%)	NS 1 (100%)
Zimmermannsecure RTP	**-**	**-**	✓	-
SDescriptions	**-**	**-**	✓	-

Figura 22 Resultados de Selft test.

Interpretación:

Un módulo criptográfico debe llevar a cabo el inicio de auto-exámenes y pruebas de auto-condicionamiento para asegurarse que el módulo está funcionando correctamente. Las pruebas power-up se llevan a cabo cuando el módulo criptográfico esta encendido. Pruebas de condicionamiento se llevarán a cabo cuando una función de seguridad es aplicable o se invoca una operación. Si un módulo criptográfico no pasa la prueba, el módulo entrara en estado de error y producirá un estado de error en la interfaz de salida o como también podría no

presentar ninguna salida, sin embargo, no implica el uso del módulo criptográfico, es decir, no se realiza ninguna operación de cifrado.

- **Indicador 10:** Aseguramiento del diseño

Tabla 24 Aseguramiento del diseño.

MGC	NS 1 (25%)	NS 1 (50%)	NS 1 (75%)	NS 1 (100%)
Zimmermannsecure RTP	-	-	-	✓
SDescriptions	-	-	-	✓

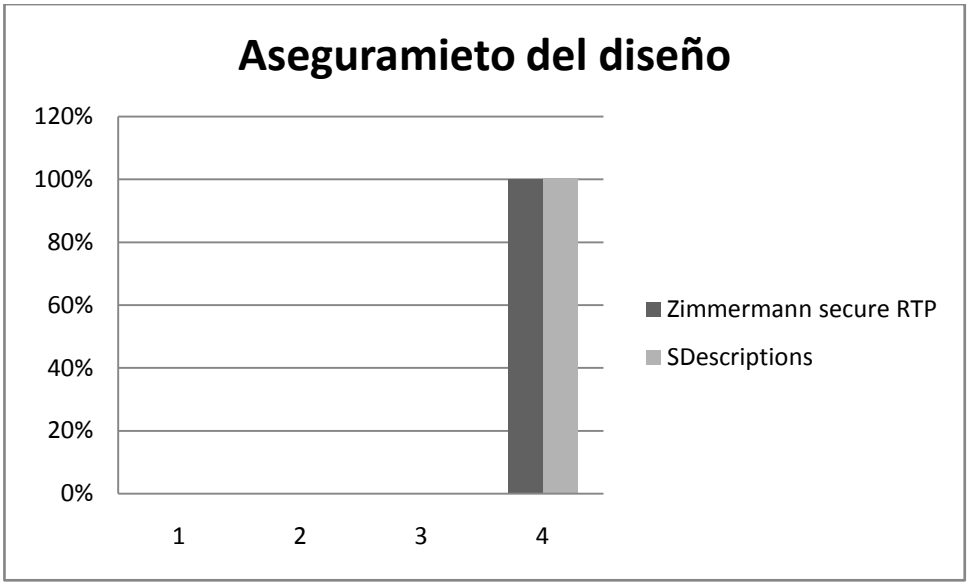


Figura 23 Resultados de aseguramiento de diseño.

Interpretación:

El aseguramiento del diseño se refiere al uso de las mejores prácticas por parte del vendedor o diseñador de un módulo criptográfico en cuanto tiene que ver con el diseño, implementación y operación del módulo criptográfico, proporcionando seguridad de que el módulo está correctamente probado, configurado, entregado, instalado y desarrollado, además, la documentación necesaria debe ser proporcionada como también la guía de usuario.

- **Indicador 11:** Mitigación de ataques

Tabla 25 Mitigación de ataques.

MGC	NS 1 (25%)	NS 1 (50%)	NS 1 (75%)	NS 1 (100%)
Zimmermannsecure RTP	**-**	✓	**-**	-
SDescriptions	**-**	✓	**-**	-

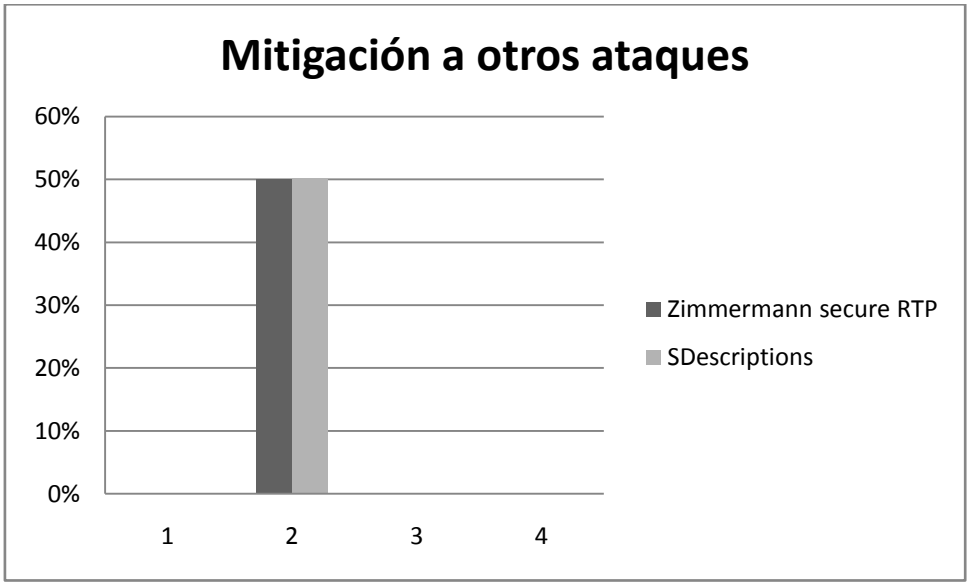


Figura 24 Resultados de mitigación a otros ataques.

Interpretación:

Los módulos criptográficos pueden ser susceptibles a los ataques con respecto a otros requisitos que no estaban disponibles en el momento que fue emitida la versión o los ataques estaban fuera de alcance de la norma (p.ej. TEMPEST). La susceptibilidad de un módulo criptográfico de tales ataques depende del tipo de módulo, implementación, ejecución y entorno. Estos ataques pueden ser de especial interés para los módulos criptográficos implementados en ambientes hostiles (p.ej. donde los atacantes pueden ser los operadores autorizados del módulo). Estos tipos de ataques se basan generalmente en el análisis de la información obtenida de fuentes externas. En todos estos casos, los ataques tratan de determinar algún conocimiento acerca de las claves y los CSP del módulo

criptográfico. En el Anexo 3 se muestra un resumen de los requerimientos de seguridad para los mecanismos de gestión de clave. Y de acuerdo a esa tabla se realizara la comparación en cuanto seguridad brindan los mecanismos de gestión de clave estudiados.

4.1.2 PROCESAMIENTO DE LA INFORMACIÓN

Para el análisis de la variable independiente (mecanismos de gestión de clave), se realizó mediante el análisis de los RFC's con los indicadores propuestos y basado en la tabla del Anexo 3, se especificará el mecanismo más seguro entre, ZRTP y SDescriptions.

4.1.3 ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

ANÁLISIS DEL MECANISMO DE GESTION DE CLAVE ZRTP.

Tabla 26 Indicadores y niveles de seguridad ZRTP.

Indicadores	**Niveles de Seguridad**			
	1	**2**	**3**	**4**
1. Cryptographic Module Specification				X
2. Cryptographic Module Ports and Interface			X	
3. Roles, Services and Authentication			X	
4. Finite State Model		X		
5. Physical Security		X		
6. Operational Environment		X		
7. Cryptographic Key Management				X
8. EMI/EMC	X			
9. Self-Test			X	
10. Design Assurance				X
11. Mitigation of Other Attacks		X		
Total	**1**	**4**	**3**	**3**
Porcentajes	***9,1***	***36,4***	***27,3***	***27,3***

Tabla 27 Indicadores y niveles de seguridad SDescriptions.

Indicadores	Niveles de Seguridad			
	1	**2**	**3**	**4**
1. Cryptographic Module Specification				X
2. Cryptographic Module Ports and Interface				X
3. Roles, Services and Authentication			X	
4. Finite State Model			X	
5. Physical Security			X	
6. Operational Environment				X
7. Cryptographic Key Management				X
8. EMI/EMC	X			
9. Self-Test			X	
10. Design Assurance				X
11. Mitigation of Other Attacks		X		
Total	**1**	**1**	**4**	**5**
Porcentajes	***9,1***	***9,1***	***36,4***	***45,5***

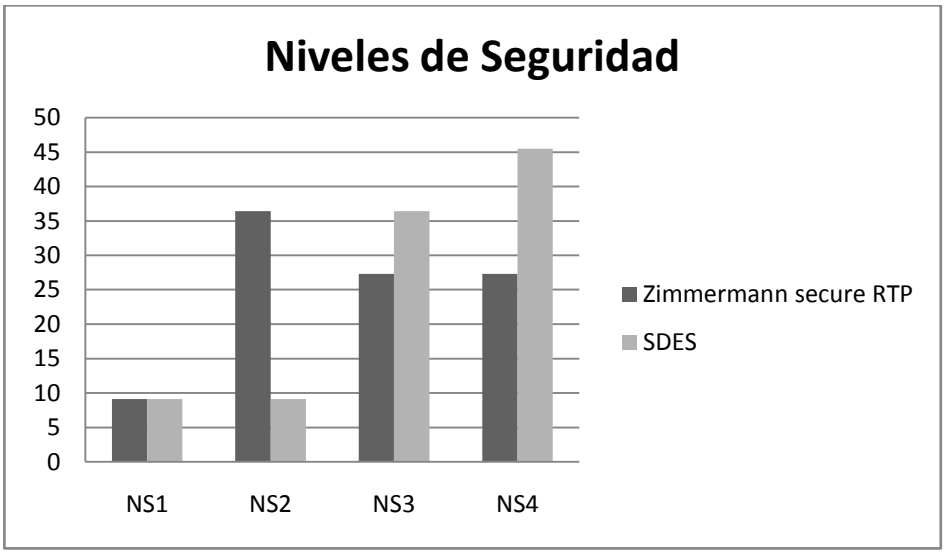


Figura 25 Niveles de seguridad – Resultados.

Interpretación

“SRTP Security Descriptions es un mecanismo para negociar claves criptográficas de usuarios en sesiones unicast utilizando el transporte SRTP. Security Descriptions se definen en SDP (Session Description Protocol), que suele ser encapsulada en protocolos como SIP. Por lo tanto, está en espera que el protocolo de transporte subordinado (p.ej. TLS, IPSec) le proveerá de autenticación y confidencialidad para proteger las claves de los ataques como eavesdropping, reproducción y modificación de mensajes. SRTP Security Descriptions (Session Description Protocol Security Descriptions for Media Streams o SDES) es un método para negociar la clave criptográfica para SRTP.

Estandarizado por el IETF como el RFC 4568. Durante el intercambio, las claves son transportadas en el adjunto SDP dentro de un mensaje SIP. Por lo tanto, la capa de transporte SIP deberá hacerse cargo de que nadie más pueda ver la información adjunta. Esto lo puede hacer usando TLS. Al usar TLS se supone que el próximo salto en la cadena hacia el proxy SIP es confiable y tendrá en cuenta los requisitos de seguridad. La gran ventaja de este método es que resulta extremadamente simple. El método de intercambio de claves ha sido elegido ya por varios fabricantes, como por ejemplo, Digum, empresa que proporciona con licencia GPL Asterisk. A pesar de que algunos de ellos no usen un mecanismo seguro para transportar la clave, este hecho ayuda a alcanzar la implementación necesaria para convertir a este método en un estándar de facto. Este hecho hace que el nivel de seguridad sea más alto (45,5%) comparado con Zrtp.

ZRTP es un protocolo de acuerdo de claves que se puede utilizar para apoyar SRTP. La diferencia fundamental entre ZRTP y otros mecanismos de intercambio de claves radica en que las claves criptográficas son negociadas a través de stream (RTP) en el mismo puerto UDP en lugar de utilizar el camino de señalización, como lo hace SDescriptions.

Por lo tanto, la negociación de la clave se realiza directamente entre pares sin necesidad de utilizar intermediarios como proxies SIP para transmitir el material de claves. ZRTP también ofrece la opción de intercambio de material de claves a través de mensajes de señalización. En primer lugar, el protocolo utiliza claves efímeras DH (Diffie-Hellman) para establecer un secreto compartido entre pares, pero no requiere una PKI, lo que hace que el protocolo sea una alternativa atractiva para las

organizaciones que no mantienen una PKI. ZRTP se describe en el Internet-Draft como un "protocolo de acuerdo de claves que realiza un intercambio de claves Diffie-Hellman durante el establecimiento en banda (in-band) de una llamada en el flujo de datos Real-time Transport Protocol (RTP) que ha sido establecido empleando otro protocolo de señalización como puede ser SIP. Esto genera un secreto compartido que es usado para generar las claves para una sesión de SRTP"[19]. El nivel de seguridad de Zrtp es de 27,3%, este nivel de seguridad ofrece bajas expectativas con respecto SDES, resultado principalmente que es mecanismo se lo utiliza como software de aplicación.

4.2 VARIABLE DEPENDIENTE

Una vez que en el apartado anterior se realizó la selección de SDescriptions como el mecanismo más seguro, se procederá a continuación a describir los indicadores que permitirán medir el rendimiento.

- Paquetes transmitidos.
- Paquetes recibidos
- Tiempo de proceso.
- Ancho de banda.
- Uso de memoria
- Jitter
- Paquetes perdidos

4.2.1 PAQUETES TRANSMITIDOS Y RECIBIDOS

Los paquetes transmitidos son aquellos que se envían del servidor hacia los clientes SIP. Con esta caracterización podemos determinar la cantidad media de paquetes. De igual forma los paquetes recibidos son los paquetes que se transmiten desde los clientes SIP hacia el servidor. En el anexo 4 se muestran los datos completos.

[19] PORTER Thomas, BASKIN Brian, CHAFFIN, Larry, CROSS Michael. Practical VoIP security 2009. Pág. 420 – 428

Tabla 28 Media de paquetes recibidos y transmitidos.

Pruebas	Media de rxpck/s y txpck/s	
	Recibidos	Transmitidos
Test control	86.27	93.77
SDescriptions	101.15	101.38

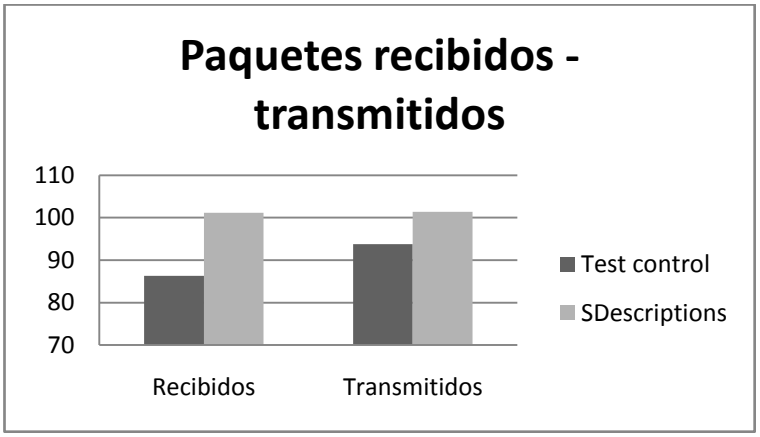


Figura 26 Paquetes enviados y transmitidos.

4.2.2 TIEMPO DE PROCESADOR

El tiempo de proceso es la capacidad que tiene el procesador para realizar o ejecutar tareas, en este sentido el factor relevante es el porcentaje de desocupación del mismo, la Herramienta SysStat indica que más cercano a 0 sea el porcentaje de *idle* (tiempo de desocupación del CPU) es más probable que existan cuellos de botella.

Tabla 29 Tiempo de CPU.

Pruebas	Media de CPU	
	%Steal	%Idle
Test control	0,02	99,97
SDescriptions	0,03	99,95

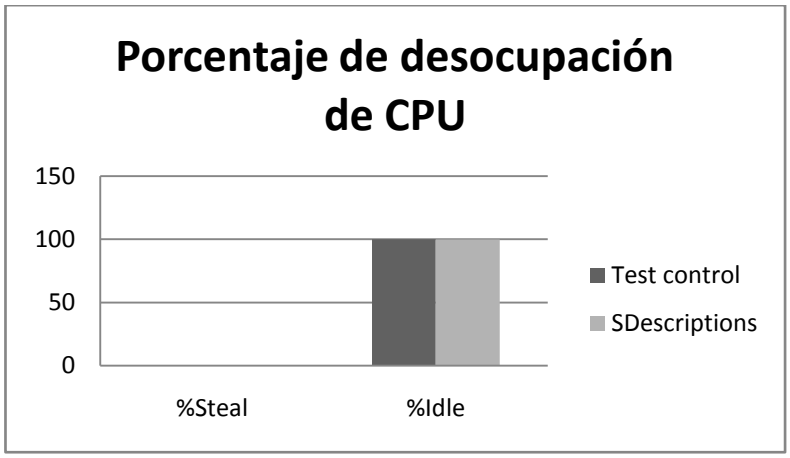


Figura 27 Desocupación de CPU.

4.2.3 ANCHO DE BANDA

El ancho de banda es la cantidad de información o de datos que se pueden enviar a través de una conexión de red en un periodo dado. El ancho de banda se indica generalmente en kilobits por segundo (kbps).

Tabla 30 Ancho de Banda.

Pruebas	Media de Bandwith Kbps	
	Rx	Tx
Test control	75,81	79,91
SDescriptions	167,64	169,65

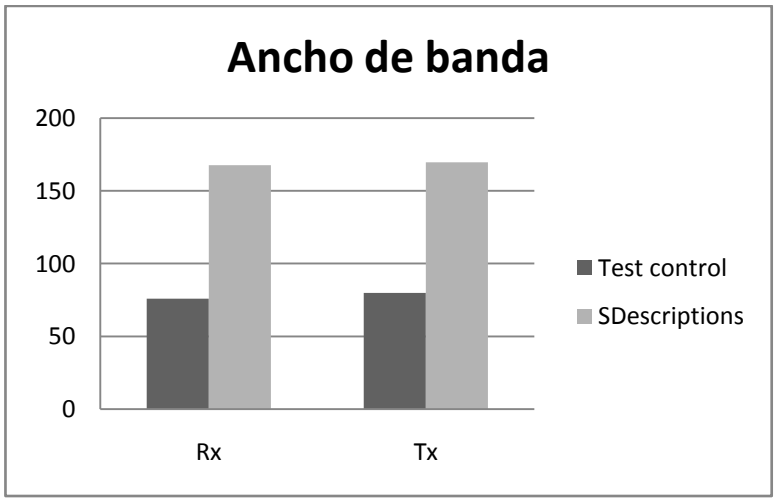


Figura 28 Ancho de Banda.

4.2.4 USO DE MEMORIA

El uso de memoria al igual que el de CPU son de mucha importancia para caracterizar el rendimiento de un servidor, en este sentido tomaremos en cuenta el porcentaje de utilización de memoria.

Tabla 31 Uso de memoria.

Pruebas	Media de uso memoria	
	%menused	%swpused
Test control	94,32	0,01
SDescriptions	94,44	0,01

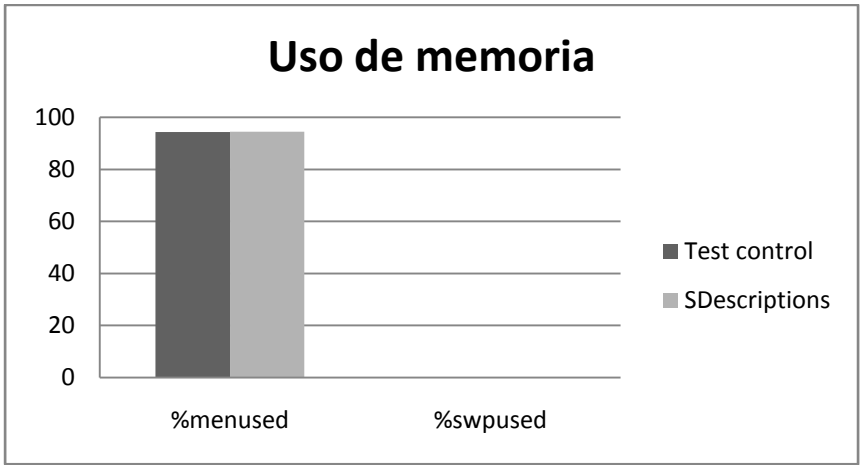


Figura 29 Porcentaje de uso de memoria.

4.2.5 JITTER

El jitter o también conocida como fluctuación es la variabilidad temporal durante el envío de señales digitales, como consecuencia causa efecto en aplicaciones multimedia, ya que provoca que algunos paquetes lleguen demasiado pronto o tarde para entregarlos a tiempo.

Tabla 32 Jitter.

Pruebas	Porcentaje Jitter	
	Rx	Tx
Test control	0	0,0272
SDescriptions	0	0,0040

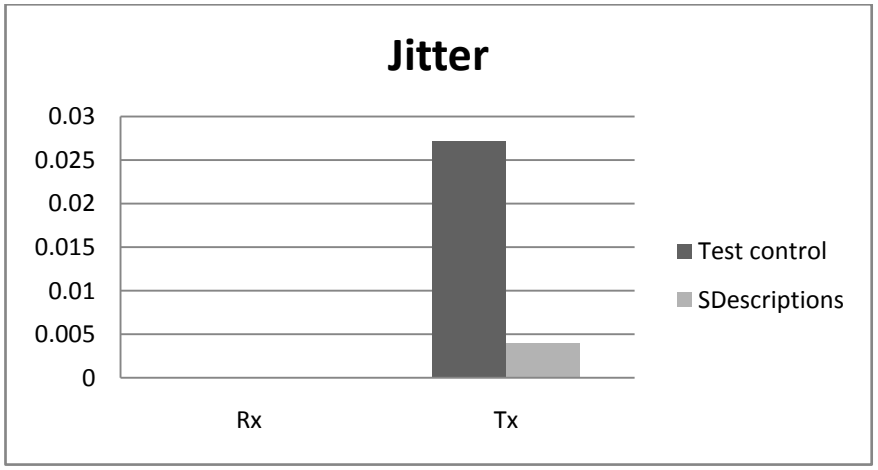


Figura 30 Porcentaje Jitter.

4.2.6. PAQUETES PERDIDOS

En transmisiones en tiempo real, como lo es la VoIP, que son sensibles, no debería existir perdida de paquetes, sin embargo, en la literatura[20] se menciona que la perdida entre 0.1% y 5% es inevitable, en la practica la perdida de paquetes debe estar por debajo del 1%.

Tabla 33 Porcentaje de Paquetes perdidos.

Pruebas	Paquetes perdidos	
	Rx	Tx
Test control	0,06	0,67
SDescriptions	0,72	0,94

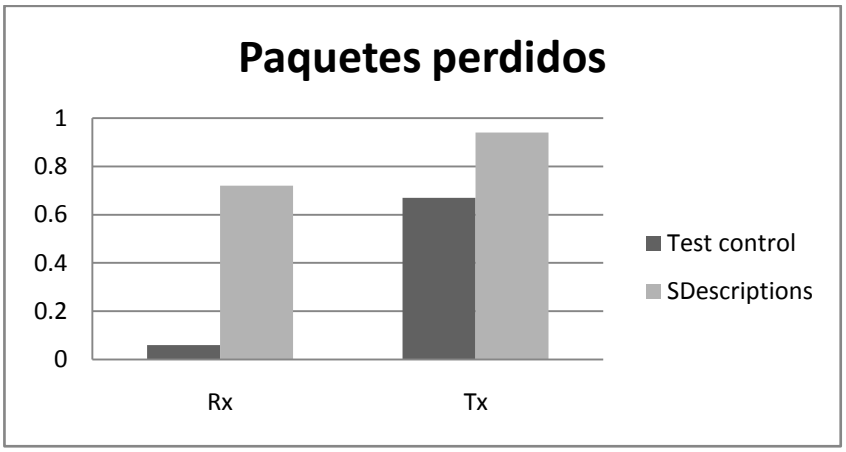


Figura 31 Porcentaje de paquetes perdidos.

[20]Fuente: K. Salah, On the deployment of VoIP in Ethernet networks: Methodology and case study. "International journal of Computer Communications", Elsiever Science, vol. 29, no. 8, pág. 1039 – 1054.

4.3 PRUEBA DE LA HIPÓTESIS

Las hipótesis científicas son sometidas a prueba para determinar si son apoyadas o refutadas de acuerdo con lo que el investigador observa, no se puede probar que una hipótesis sea verdadera o falsa, sino argumentar que fue apoyada o no de acuerdo con ciertos datos obtenidos en la investigación. Por lo tanto no existe un método que permita saber con seguridad que una desviación es el resultado exclusivo del azar, sin embargo hay pruebas estadísticas que permiten determinar algunos límites de confianza.

Para la demostración de la hipótesis de investigación se utiliza t de Student con diferencia por parejas.

"Sea (x_1,y_1), (x_2,y_2), ……., (x_n,y_n) una muestra de pares de observaciones; donde (x_i,y_i) representan dos mediciones tomadas de la misma unidad muestral, antes y después de un tratamiento o fenómeno que la afectó. Se desea conocer si la población cambió de manera apreciable después del fenómeno indicado; para ello se emplea la prueba de diferencias por parejas de la manera que a continuación se describe. Se construye una muestra aleatoria de las diferencias d_1, d_2, …., d_n, donde $d_i = x_i – y_i$ (i = 1, 2, 3, …, n), que las supondremos siguen una ley normal de media μ_d y varianza δ_d^2 . Para estos parámetros poblacionales se calculan sus estimadores" (Galindo, 2008, p 255):

$$d = \frac{1}{n}\sum_{i=1}^{n} d_i \;\; y \;\; s^2 = \frac{1}{n-1}\sum_{i=1}^{n}(d_i - d)^2$$

Ecuación 2 T de student[21]

4.3.1 PLANTEAMIENTO DE LA HIPÓTESIS

Hipótesis nula (H0). El nivel de rendimiento en el servidor de VoIP es igual antes y después de la aplicación del mecanismo SDES.

Hipótesis alternativa (H1). El nivel de rendimiento en el servidor de VoIP disminuye con la aplicación del mecanismo SDES.

4.3.2 NIVEL DE SIGNIFICACIÓN

Para un nivel de significación de α= 0.05

[21] GALINDO, Edwin. Estadística Métodos y Aplicaciones, Segunda edición 2008. Pág. 255–256

4.3.3 ZONA DE RECHAZO

Para todo valor de probabilidad igual o menor que 0.05, se acepta H1 y se rechaza H0.

4.3.4 CÁLCULOS

Cálculos: para la obtención de los datos que se muestran en la tabla, se utilizó el software SPSS el cual es un programa estadístico informático.

Tabla 34 Estadísticos de muestras relacionadas.

		Media	N	Desviación típ.	Error típ. de la media
CPU	TCONTROL	99,9690	60	,05891	,00761
	SDES	99,8465	60	,26867	,03468
MEMORIA	TCONTROL	94,3195	60	,00387	,00050
	SDES	94,4373	60	,03522	,00455
P-Rx	TCONTROL	86,2715	60	27,71932	3,57855
	SDES	101,1502	60	1,37292	,17724
P-Tx	TCONTROL	93,7712	60	23,27555	3,00486
	SDES	101,3838	60	1,66720	,21524

Tabla 35 Correlaciones de muestras relacionadas.

		N	Correlación	Sig.
CPU	TCONTROL y SDES	60	-,012	,930
MEMORIA	TCONTROL y SDES	60	-,122	,354
P-Rx	TCONTROL y SDES	60	-,037	,780
P-Tx	TCONTROL y SDES	60	-,081	,538

Tabla 36 Pruebas de muestras relacionadas.

		Diferencias relacionadas					t	gl	Sig. (bilateral)
		Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia				
					Inferior	Superior			
CPU	TCONTROL y SDES	,12250	,27572	,03559	,05128	,19372	3,442	59	,001
MEM	TCONTROL y SDES	-,11783	,03589	,00463	-,12711	-,10856	-25,428	59	,000
PRx	TCONTROL y SDES	-14,87867	27,80364	3,58943	-22,06111	-7,69622	-4,145	59	,000
PTx	TCONTROL y SDES	-7,61267	23,46976	3,02993	-13,67555	-1,54979	-2,512	59	,015

4.3.5 DECISIÓN

La significancia bilateral para CPU es 0,0010 que es menor que 0.05, igual ocurre con Memoria, PRx y PTx, donde la significancia es menor a 0.05. Por lo tanto se rechaza H0, esto quiere decir que el nivel de rendimiento en el servidor de VoIP disminuye con la aplicación del mecanismo SDES.

CAPÍTULO V
GUIA REFERENCIAL

5.1. INTRODUCCIÓN

Una vez estudiados y revisados aquellos factores que deben ser analizados al momento de llevar a cabo estudios acerca de la conformidad (Cap. 2), se plantea la situación de presentar una guía referencial de evaluación de mecanismos de gestión de clave. La guía de referencia se divide de forma que inicialmente se presentan las definiciones de términos que utilizará la guía (Cap. 5.2) y un análisis acerca de la conformidad y el rendimiento (Cap. 5.3). Posteriormente se presentan ocho fases en las que se abarcan desde tareas preliminares hasta los procedimientos de finalización (Cap. 5.4 – 5.8). Estas fases se desarrollarán de forma secuencial, aunque la ejecución de cada una de ellas es opcional, si los objetivos que se persiguen no se ajustan a los de la persona que utilizará la guía.

5.2. DEFINICIONES

A continuación se presentan algunas definiciones utilizadas en esta guía referencial:

- IPE.- Implementación de pruebas
- Conjunto de Pruebas.- Un conjunto completo de pruebas individuales que se llevan a cabo para obtener información acerca de una determinada característica o funcionalidad en la IP.
- Medios de Prueba.- Combinación de equipos y procedimientos que pueden llevar a cabo la validación o evaluación deseada.
- Perfil de Tráfico.- Conjunto de características que definen un uso de la red determinado, así como el estado de la propia red.
- Pruebas de Conformidad.- Validación del nivel de conformidad con el estándar.
- Pruebas de Rendimiento.- Evaluación del rendimiento de la IPE en diversas condiciones de operación.

- Registro de Pruebas.- Registro en formato legible por las personas de los resultados obtenidos en la realización de una prueba o un conjunto de pruebas.
- Resultado Obtenido.- Resultado de una prueba de obtenido para una IPE concreta.
- Sistema de Pruebas.- Conjunto de equipos, dispositivos y software utilizado para realizar las diferentes pruebas sobre la IPE.

5.3. CONFORMIDAD Y RENDIMIENTO

Una implementación de un protocolo o arquitectura de seguridad es conforme a la especificación si dicha implementación presenta todas las características y requisitos descritos en esa especificación. Estos requisitos de conformidad pueden ser obligatorios, cuando deben ser respetados en todo momento, condicionales, cuyo cumplimiento se reduce a los casos en los que se dan un conjunto determinado de condiciones, u opcionales, cuando su cumplimiento por parte de las implementaciones es totalmente voluntario. Adicionalmente, nos encontramos con que los requisitos de conformidad pueden estar expresados de forma positiva (se especifica lo que debe hacerse) o negativa (cuando se detalla lo que no debe hacerse). Por último, podemos comprobar cómo los requisitos de conformidad se pueden agrupar en requisitos de conformidad estática o conformidad dinámica[22].

La conformidad estática es aquella que establece límites a las combinaciones de características permitidas en las implementaciones de los protocolos o arquitecturas de seguridad, así como el conjunto de características mínimo que permite la interoperabilidad. Por su parte, la conformidad dinámica especifica el comportamiento observable que es admisible para las implementaciones del protocolo en cuestión. La definición de los protocolos de seguridad en los estándares es el caso más claro de conformidad dinámica: el uso y formato que se asigna a las unidades de información, transiciones entre estados, etc. La conformidad dinámica establece límites a la funcionalidad de las implementaciones, por lo que define el máximo conjunto de características que una implementación puede tener.

[22]Esta nomenclatura es la misma utilizada por las normas ISO/IEC 9646 e ITU-T X.290. http://webstore.iec.ch/preview/info_isoiec9646-7%7Bed1.0%7Den.pdf

En cuanto al rendimiento que ofrece una implementación de un mecanismo de seguridad, los parámetros que se evalúan pueden ser dependientes del tráfico de red o independientes del tráfico de red. Aquellos parámetros que dependen del tráfico de red modifican sus resultados en función del tipo de mensajes que se utilizan para evaluarlo. También se ven afectados por el tráfico existente en la red en la que se realizan las pruebas, y por la saturación de dicha red. Esta variabilidad afecta a la respetabilidad de los resultados de rendimiento que se obtienen al llevar a cabo la evaluación.

Los parámetros de rendimiento que no dependen del tráfico de red son aquellos en los que las características de los mensajes intercambiados no influyen en los resultados obtenidos. En la medición de estos parámetros el nivel de saturación de la red afecta de forma marginal a los resultados, por lo que la respetabilidad de las pruebas no resulta afectada.

5.4. FASE 1: TAREAS PRELIMINARES

En la fase inicial de las pruebas, se determinará cuáles son los mecanismos a validar y evaluar, quién llevará a cabo dichos procesos y qué recursos serán necesarios para completar esta tarea. Para poder llevar a cabo este proceso será preciso determinar cuál va a ser el objetivo de los análisis que se lleven a cabo, y obtener los recursos necesarios para desarrollar esos estudios. En este estudio se tomarán como referencia los RFC's tanto de SrtpDES y ZRTP, como recurso se utilizó la investigación de los mecanismos de gestión de clave y el objetivo obtener las características principales de los MGC.

5.4.1. DETERMINAR EL TIPO DE ANALISIS

Puede existir la posibilidad de realizar tres tipos de análisis dependiendo del tipo de información que se desea obtener:
Validación de la conformidad.- En este caso únicamente se llevarán a cabo estudiando la conformidad. Se obtendrá información acerca de la conformidad del mecanismo con el estándar.

Evaluación de rendimiento.- Al llevar a cabo este análisis se someterá la IPE a pruebas de rendimiento que proporcionen información acerca de la capacidad. Los análisis están compuestos de conjuntos de pruebas de caracterización de comportamiento.

Validación de la conformidad y evaluación del rendimiento.- Es posible llevar a cabo los procesos de validación de la conformidad y evaluación de rendimiento de forma conjunta. El análisis final constará de la ejecución de cada uno de los análisis de forma secuencial. En este estudio se llevo a cabo la validación de los mecanismos de gestión de clave tomando en consideración el estándar 4046 con respecto a los RFC 6189 y 371, así como también, la validación de rendimiento, por ejemplo utilizando la herramienta SysStat.

5.4.2. IDENTIFICACIÓN DE LOS RECURSOS NECESARIOS

Es posible que no todos los recursos necesarios determinados en el apartado anterior sean accesibles al público en general, por lo que en esta fase el responsable del estudio deberá llevar a cabo las gestiones necesarias para averiguar qué herramientas y utilidades pueden dar el servicio necesario, identificando aquellas cuya disponibilidad sea mayor. Todos los recursos que se emplearán para llevar a cabo los análisis se incluirán en un registro para su posterior comprobación en la fase final de esta guía. Es así, que se utilizó herramientas como SysStat, Vnstat y channelsstat incorporado en Asterisk para determinar tanto el porcentaje de desocupación de la CPU, uso de memoria así como también el jitter y paquetes de voz perdidos. Otro recurso es el VPS.

5.5. FASE 2: DOCUMENTACIÓN PRELIMINAR

Puede ser que los evaluadores no dispongan de conocimientos previos acerca del mecanismo de gestión de clave cuya implementación se evaluará, es necesario que, previamente al diseño de pruebas de conformidad (en base a teoría) y de rendimiento, se adquiera este conocimiento. De similar modo, en esta fase si incluirá la documentación acerca de los problemas de interoperabilidad de los mecanismos de gestión de clave. Se procederá también, en lo posible, instalar la implementación de referencia en un entorno de pruebas para adquirir conocimientos adicionales acerca de las implementaciones del estándar que

amplíen los conocimientos del evaluador en esta área. Para finalizar la presente fase se documentarán los aspectos generales del mecanismo de gestión de clave, así como los problemas de interoperabilidad y rendimiento más frecuentes en la actualidad. En este sentido en la presente tesis por falta de interoperatibilidad, específicamente de la librería que ZRTP no dispone para Linux CentOS 6, este mecanismo de gestión de clave no se implemento.

5.6. FASE 3: ANÁLISIS DEL ESTÁNDAR

En esta fase se llevará a cabo un estudio exhaustivo del estándar que permita ampliar los conocimientos adquiridos en la fase anterior. Al finalizar este proceso, los evaluadores deben tener la capacidad de:

- Identificar aquellos aspectos fundamentales del estándar que deban ser evaluados en lo referente a la conformidad.
- Identificar aquellos aspectos del estándar que deben ser evaluados debido a su importancia para la seguridad.
- Identificar aquellos aspectos del estándar que deben ser avaluados por su importancia en determinadas situaciones o arquitecturas determinadas, por ejemplo, el uso de SRTP para el transporte del contenido de voz encriptado.
- Identificar aquellos aspectos del estándar que deben tenerse en cuenta en la evaluación del rendimiento.

La presente fase finalizará documentando la información obtenida en cuanto a los aspectos del estándar que deben ser incluidos en los análisis. Los RFC's hacen mención sobre los tipos de protocolos de señalización son soportados, así por ejemplo, ZRTP soporta SIP, H323, puesto que su negociación de claves está dentro del flujo de datos RTP.

5.7. FASE 4: VALIDACIÓN DE LA CONFORMIDAD

Para llegar a definir un conjunto de pruebas que permitan el análisis de la implementación en pruebas, es necesario identificar aquellas capacidades que aparecen recogidas en el estándar y que deben ser desarrolladas por las

implementaciones de una forma determinada. Los RFC's 6189 y 3711, realizan consideraciones de seguridad de los flujos RTP tanto del header y payload o también, los escenarios en los que flujo de datos de audio pueden transmitirse o recibirse pudiendo ser estos Unicast o Multicast, al validarlos con el estándar de conformidad 4046, los mecanismos de gestión de clave analizados no cumplen con características de envío de streams multicast.

5.7.1. IDENTIFICACIÓN DE LOS MECANISMOS CRIPTOGRÁFICOS

Dado que muchas de las diferentes configuraciones surgirán a partir de variaciones en los mecanismos criptográficos que se utilizan, es necesario identificar cuáles son las suites criptográficas permitidas por el estándar. Adicionalmente, se identificarán aquellos mecanismos que deben ser implementados obligatoriamente y aquellos que son opcionales. Teniendo en cuenta la constante evolución de los estándares de los protocolos, se prestará especial atención a la presencia de mecanismos opcionales en la actualidad pero pasarán a ser obligatorios en un corto periodo de tiempo (normalmente identificados como SHOULD+ en los estándares) y aquellos que son obligatorios pero dejarán de serlo (señalados como MUST-).

5.7.2. IDENTIFICACIÓN DE LAS CARACTERÍSTICAS OBLIGATORIAS

Las especificaciones de los protocolos y arquitecturas de seguridad incluyen un conjunto mínimo de funcionalidades que deben ser incluidas en cualquier implementación de dicho protocolo o arquitectura. Este conjunto mínimo de funcionalidades debe ser identificado para poder incluir su validación en el conjunto de pruebas. Por ejemplo, el RFC 4046 establece que los mecanismos de gestión de clave deben prevenir ataques de denegación de servicios DoS, tanto ZRTP como SRTDES en sus RFC's no son explícitos en la eliminación de este ataque.

5.8. FASE 5: EVALUACIÓN DEL RENDIMIENTO

Para llegar a definir un conjunto de pruebas que permita el análisis del rendimiento ofrecido por la implementación en pruebas, es preciso identificar aquellos aspectos del rendimiento del protocolo o arquitectura de seguridad que es necesario

evaluar. Como por ejemplo, sobrecarga de procesador, uso de memoria entre otros, refiérase al Anexo 4.

5.8.1. RENDIMIENTO DE LOS MECANISMOS CRIPTOGRÁFICOS

El rendimiento de los diferentes mecanismos criptográficos es muy variable entre distintos sistemas, incluso de la misma arquitectura. Por este motivo es necesario identificar los diferentes conjuntos de mecanismos involucrados en cada uno de los aspectos del rendimiento que es necesario evaluar, para así poder llevar a cabo la evaluación del rendimiento de dicho aspecto considerando la utilización de cada uno de esos mecanismos, en nuestro caso ZRTP y SRTPDES.

5.8.2. IDENTIFICACIÓN DE PARÁMETROS DEPENDIENTES DEL TRÁFICO

Aquellos parámetros de rendimiento que sean dependientes del tráfico que circule por la red, o de las características concretas del tráfico que se utiliza para llevar a cabo la evaluación, deberían ser identificados. En los conjuntos de pruebas que evalúen estos parámetros debería determinarse cuáles son las condiciones en las que dicha prueba debe llevarse a cabo, con el fin de facilitar la repetitividad de la evaluación. Por ejemplo, parámetros como los paquetes transmitidos o recibidos, el delay, son dependientes del trafico debido a que son paquetes de datos que atraviesan infraestructuras de red externas, en nuestro caso los datos atravesaban routers hasta llegar al servidor VPS de la empresa Linode ubicado en América del norte.

5.8.3. IDENTIFICACIÓN DE PARÁMETROS INDEPENDIENTES DEL TRÁFICO

Se identificarán los aspectos del rendimiento a los que el estado de la red y las características de tráfico de prueba no afectan directamente. Los conjuntos de pruebas que evalúen estos parámetros no deben considerar el estado de la red ni el tipo de tráfico utilizado. Sin embargo, dado que es posible que al llegar a los límites de rendimiento que ofrece la IPE se produzcan variaciones por estos motivos, por ejemplo, cantidad de memoria usada, uso de cpu, cantidad de procesos ejecutados simultáneamente, ancho de banda utilizado, entre otros. Remítase al Anexo 4.

5.9. FASE 6: DISEÑO DE PRUEBAS

Una vez se disponga de información suficiente acerca de los aspectos del rendimiento que se van a evaluar, se procederá a definir el conjunto de pruebas. Las pruebas de rendimiento son pruebas de comportamiento únicamente, por lo que ninguna prueba debería considerar a la IPE como algo más que una caja blanca. En este apartado también se puede considerar el uso de simuladores. La definición de cada prueba de rendimiento constará de:

- Objetivos, aspecto que se pretende evaluar con cada una de las pruebas.
- Medios de prueba, configuración del sistema de pruebas, y arquitectura necesaria.
- Configuraciones válidas, variaciones de parámetros que es necesario realizar a la hora de llevar a cabo el análisis del rendimiento.
- Medición de los resultados, incluyendo los registros de pruebas.

Los perfiles de tráfico definen las condiciones de la red en el momento de llevarse a cabo la validación y la evaluación de la IPE. También recogen cuales son las características del tráfico que se utiliza para llevar a cabo los análisis de los diferentes aspectos de rendimiento. Dado que las pruebas de conformidad y algunas pruebas de rendimiento no se ven afectadas por estas condiciones, únicamente en algunos conjuntos de pruebas de rendimiento se hace uso de estos perfiles. Ver Anexo 4.

Las características que deben aparecer recogidas en un perfil de tráfico son:

- Protocolo: Cuál es el protocolo o protocolos utilizados para el envío de datos. En el caso de ser varios protocolos, se informará de la distribución porcentual de los mensajes en dichos protocolos.
- Medición: Equipo o sistema que lleva a cabo la medición del parámetro de rendimiento.
- Retardo: Retardo artificial incluido en la red.
- Pérdida de paquetes: Porcentaje de pérdida de paquetes.

- Reenvío de paquetes: Porcentaje de paquetes reenviados.
- Paquetes transmitidos: Porcentaje de paquetes transmitidos.
- Paquetes recibidos: Porcentaje de paquetes recibidos.
- Bytes transmitidos Porcentaje de Bps transmitidos.
- Bytes recibidos: Porcentaje de bps recibidos.
- Tiempo de CPU: Porcentaje de desocupación del procesador.
- Uso de Memoria: Porcentaje de utilización de memoria RAM.
- Errores de red: Porcentaje de errores producidos en el envío de datos por la red.
- Ancho de banda
- Jitter

Se definirán perfiles de tráfico que permitan la obtención de información del rendimiento a efectos comparativos (esto es, que permitan obtener información acerca del rendimiento máximo que la implementación es capaz de ofrecer), y perfiles que aporten información acerca del rendimiento de la implementación en condiciones más realistas en cuanto a tipo de tráfico a proteger y estado de la red durante su operación.

5.10. FASE 7: OTRAS CONSIDERACIONES

En esta fase se analizarán otras consideraciones que deban ser tenidas en cuenta a la hora de llevar a cabo la validación y evaluación de la IEP. Aspectos tales como recomendaciones de arquitecturas a utilizar, limitaciones de los conjuntos de pruebas propuestos, herramientas necesarias o recomendadas para la realización de las pruebas, deben ser analizados y documentados en esta fase de la metodología. En esta fase hay que tener en cuenta la una metodología de ocho pasos para el despliegue de una infraestructura de VoIP[23]. Se puede considerar en esta fase realizar una simulación utilizando, por ejemplo, OPNET o VoIP Analitic Symulator [7], en los que se pueden crear escenarios en los que se puede manipular características como el ancho de banda, la latencia de la red, el tamaño de los paquetes a transmitirse o el número de llamadas simultaneas que en condiciones configuradas pueden soportar.

[23]Flowchart of an eight-step methodology. (Source: K. Salah, “On the deployment of VoIP in Ethernet networks: Methodology and case study,” International Journal of Computer Communications, Elsevier Science, vol. 29,no. 8, 2006, pp. 1039–1054.

5.11. FASE 8: TAREAS FINALES

Para finalizar el proceso de análisis de la IPE, se llevará a cabo la recopilación de todo el material generado en fases anteriores, tanto referente al protocolo o mecanismos de gestión de clave, como las definiciones de los conjuntos de pruebas que deben aplicarse. Esta información se compilará en un formato que sea fácilmente accesible y manejable por los responsables de los análisis.

Se prestará especial atención a la utilización de herramientas necesarias para llevar a cabo el análisis de las implementaciones, con el fin de asegurar que las herramientas seleccionadas en la fase 1 de esta metodología fueran acertadas y no se deban realizar modificaciones en ese aspecto. En la practica la documentación se puede esquematizar de acuerdo a las fases propuestas, por ejemplo, la recopilación de pruebas y datos obtenidos con respecto a la evaluación de ZRTP versus SRTPDES se llevaron a cabo tomando como referencia las recomendadas por el NIST ver Anexo 3 lo que permitió plasmar las fases 1 a la 4 o los datos de las pruebas de rendimiento en las que se utilizaron herramientas como SysStat, Vnstat y Channelsstat remitirse al Anexo 4, para evidenciar y comprobar el rendimiento en la fase con el despliegue piloto.

A continuación se muestra en la figura 32, un diagrama de flujo que presenta los pasos a seguir en esta guía referencial, los primeros cuatro pasos son independientes y pueden realizarse en paralelo con el paso 6.

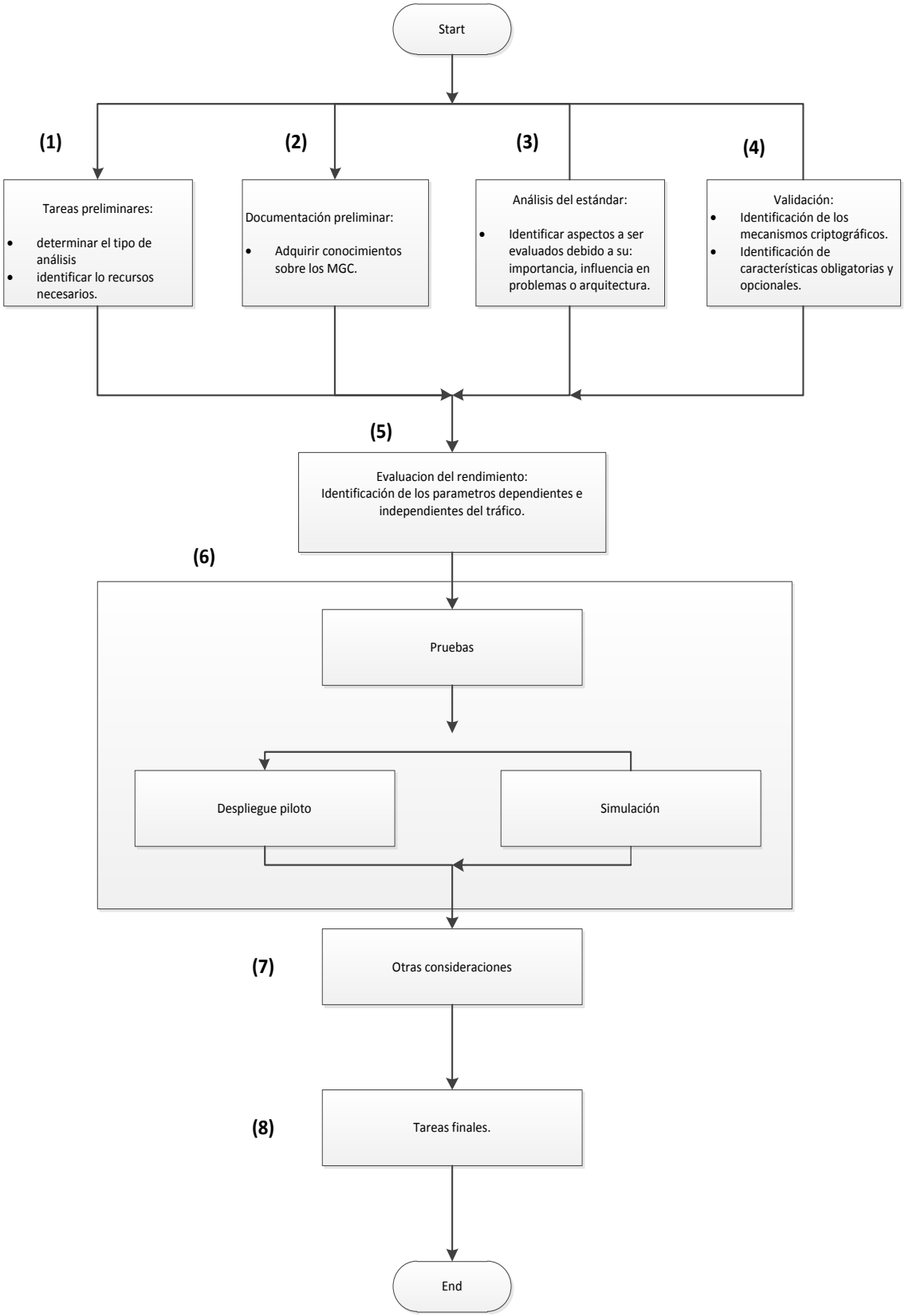


Figura 32 Diagrama de flujo que incluyen las ocho fases de la guía referencial.

CONCLUSIONES

- Mediante el estudio del RFC 4046 se identificaron los parámetros de seguridad asociados a los mecanismos de gestión de clave, los mismos que permitieron elegir el mecanismo de cifrado más seguro.

- El análisis de los mecanismos de gestión de clave determinó que SRTP Descriptions es el mecanismo más seguro para cifrar voz en comparación con ZRTP, debido a que, además de encriptar los flujos de voz también encripta el proceso de señalización con SIP.

- La guía referencial de evaluación de mecanismos de gestión de clave permite determinar el nivel de seguridad y de rendimiento en un sistema de VoIP.

- Al implantar el mecanismo de gestión de clave SRTP Descriptions sobre el ambiente de pruebas, el nivel de rendimiento en el servidor privado virtual, disminuyó en un 0.12%.

- El mecanismo de gestión de clave ZRTP no se implantó en el ambiente de pruebas debido a que en Asterisk 1.8.7 el archivo parche para esta versión es obsoleto y no es interoperable con versiones actuales de esta PBX Software.

RECOMENDACIONES

- Para garantizar la seguridad en VoIP mediante un mecanismo de gestión de clave, es necesario considerar los parámetros de seguridad multicast contenidos en el RFC 4046.

- Las comunicaciones de voz deben ser cifradas si estas contienen información privada o sensible a ataques, al usar SRTP Descriptions, se garantiza la confidencialidad y la integridad de los datos.

- Cuando SRTP Descriptions se configura y utiliza, se debe usar TLS en todo momento en conjunto con SIP, para asegurar la comunicación entre interlocutores, por lo tanto, hay que usar TLS con SIP.

- Configurar voz en una red de datos requiere servicios de red con un bajo retardo, además de mantener un mínimo jitter y paquetes perdidos, en este sentido, si es necesario, para minimizarlos se debe incrementar el ancho de banda, escoger diferentes tipos de códec, fragmentar los paquetes de datos y priorizar los paquetes de voz.

- Para mejorarla administración de usuarios, así como un plan de marcación unificado y soporte remoto a más teléfonos se debe utilizar un servidor privado virtual desplegado en la red IP WAN, tomando en consideración elementos como el ancho de banda y el retardo.

- Para desplegar telefonía IP en la red de una empresa ya sea pequeña, mediana o grande es recomendable utilizar un simulador para determinar el número de llamadas simultaneas que puede soportar la red, así como también, prever el consumo de ancho de banda a contratarse.

BIBLIOGRAFÍA

BIBLIOGRAFÍA DE LIBROS

1. **Endler D., and Collier M.,** Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions., 2da ed., New Jersey – Estados Unidos., McGraw-Hill/Osborne., 2009., Pp. 250-321.

2. **Gebali F.,** Computing Communication Networks: Analysis and Designs., 3ra ed., Northstar Digital Design, Inc., 2005., Pp. 60-85.

3. **Himanshu Dwivedi.,** Hacking VoIP Protocols, Attacks, and Countermeasures., 2da ed., Megan Dunchak Inc., 2009, Pp. 150-180.

4. **Karacali B., Denby L., and Melche J.,** Scalable Network Assessment for IP Telephony., Proceedings of IEEE International Conference on Communications (ICC04), Paris – Francia., 2004., Pp. 1505-1511.

5. **Meggelen J., Madsen L., and Smith J.,** Asterisk: The Future of Telephony., 2da ed., Estados Unidos., O'Reilly Media, Inc., 2007., Pp. 37-144.

6. **Peter Thermos and Ari Takanen.,** Securing VoIP networks: threats, vulnerabilities, countermeasures., 1r ed., Estados Unidos., Pearson, Inc., 2008, Pp. 90-130.

7. **Portoles M., Comeras j., Mangues B., and Cardenete-Suriol.,** Performance issues for VoIP call routing in a hybrid ad hoc office environment, 2da ed., Estados Unidos., McGraw-Hill., 2007, Pp. 1–5.

8. **Salah K., and Alkhoraidly A.,** An OPNET-based Simulation Approach for Deploying VoIP., International Journal of Network Management, John Wiley, Vol. 16 (3-4)., Estados Unidos., 2006, Pp. 159-183.

9. **Sanders C.,** Practical Packet Analysis., 1ra ed., San Francisco – Estados Unidos., Starch Press, Inc., 2007., Pp. 121-133.

10. **Surtees, M. West, and A.B. Roach.,** Signaling compression (Sig Comp) corrections and clarifications, RFC 4896., Estados Unidos., 2007, Pp.90-110.

11. **Tanenbaum, Andrew S.,** Computer Networks., Patti Guerrieri., 4ta ed., Estados Unidos., Pearson Education., 2003., Pp. 396-500.

12. **Thomas Porter, Jan Kanclirz, Andy Zmolek and Antonio Rosela.,** Practical VoIP Security., Estados Unidos., Syngress Publishing, Inc, 2009, pp. 15-60.

BIBLIOGRAFÍA DE INTERNET

13. ASTERISK

ww.digum.org/

2010/06/20

14. CISCO 2621 MODULAR ACCESS ROUTER SECURITY POLICY

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/secure/2621rect.pdf

2010/04/28

15. HACKING VOIP EXPOSED

http://www.hackingvoip.com/

2010/05/10

16. ITU-T RECOMMENDATION P.800, METHODS FOR SUBJECTIVE DETERMINATION OF TRANSMISSION QUALITY

www.itu.in/publications/main_publ/itut.html

2010/04/18

17. NIST SECURITY PUBLICATIONS INCLUDING FIPS AND SPECIAL PUBLICATIONS

http://csrc.nist.gov/publications

2011/03/15

18. RFC 4046

http://tools.ietf.org/html/rfc3261#page-193

2010/07/05

19. RFC 3711

http://www.ietf.org/rfc/rfc3711.txt

2010/08/10

20. RFC 6189

http://zfone.com/docs/ietf/rfc6189.html

2010/09/12

21. VOIP SECURITY ARTICLES

http://voipsa.org/Resources/articles.php

2010/06/15

22. VOIP ANALYTIC SIMULATOR

http://faculty.kfupm.edu.sa/ics/salah/voiptool/index.htm

2010/08/20

ANEXOS

Anexo 1

Instalación de Asterisk 1.8.x sobre un VPS

La mayoría de recomendaciones para la instalación de Asterisk fueron tomadas de Andrea Sanucci[24] y del servicio que brinda la empresa Linode[25] dando recomendaciones de como instalar Asterisk es sus VPs.

Asterisk es el programa Opens Source más conocido para implementar una PBX. Para una lista completa de las funcionalidades brindadas visiten la página de los desarrolladores. Entre ellas:

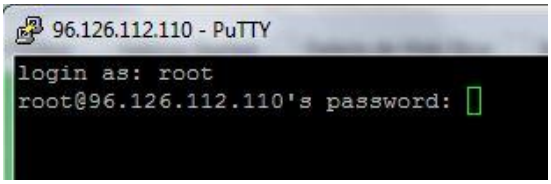
- Registro de llamadas
- Desvío de llamadas
- Trasferencia de llamadas
- Conferencias
- ENUM
- Música en espera
- Gestión de colas (call center)
- Soporte para tarjetas FXO, FXS y digitales

Este manual abarca la instalación de Asterisk en un VPS (Servidor Virtual Privado) y es válida para cualquier Servidor Linux CentOS. Con el VPS la ventaja es tener una PBX siempre activa, independiente de la banda ancha disponible en la casa/oficina y evita tener una computadora dedicada y siempre encendida. Hay empresas que ofrecen VPS a costos relativamente bajos. Entre todas hay dos que tienen una óptima relación calidad/precio. La primera es SliceHost que con 20 dólares mensuales brinda un VPS de 256 Megabyte de memoria RAM, 10 Gigabyte de disco duro, 100 Gigabyte de tráfico. La segunda empresa es Linode que con 19,95 dólares mensuales brinda una VPS de 512 Megabyte de memoria RAM, 16 Gigabyte de disco duro y 200 Gigabyte de tráfico. La distribución Linux que se utilizará para la instalación de Asterisk es **CentOS**.

Para manejar el servidor Linux desde una computadora con sistema operativo Microsoft Windows se debe utilizar el programa putty. Se descarga y se abre dando clic dos veces en el icono del programa. Aparecerá la siguiente ventana:

[24] http://voztovoice.org/
[25] http://www.linode.com

Se coloca la dirección IP del VPS en la casilla “Host name, orIPaddress”, se deja en Port el numero 22 y se presiona el botón Open. Aparecerá una nueva ventana:



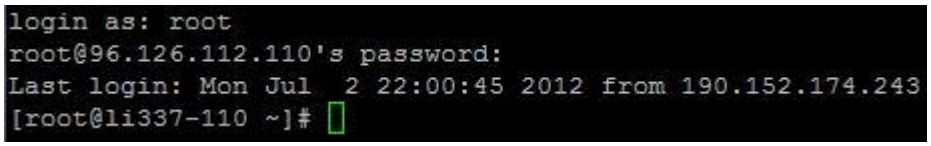
Se introducen las credenciales para acceder al servidor remoto. Se digita root y se presiona la tecla envío. Cuando el sistema lo pide, se digita la contraseña.

Para la conexión desde un servidor Linux el comando es:

ssh root@ipservidorremoto

Si no se usa el puerto estándar (22) habrá que indicarlo de la siguiente forma:

ssh -p 20000 root@ipservidorremoto



Una vez dentro del servidor Linux se puede empezar con la instalación de Asterisk. Antes que nada se necesita instalar un buen editor de textos como **NANO**, indispensable para modificar los archivos de configuración de Asterisk y en general para crear/modificar cualquier archivo de texto.

Para instalar NANO el comando es:

Yum install nano

YUM es un programa que permite gestionar todos los paquetes precompilados para la distribución Linux CentOS. Para una lista de las opciones disponibles se usa el siguiente comando:

yum --help

Una buena práctica es actualizar el sistema:

yumupdate

Si se quiere configurar la hora del servidor remoto hay que seguir estos pasos (para Ecuador):

rm /etc/localtime

luego se crea un enlace simbólico al huso horario de Ecuador:

ln -s /usr/share/zoneinfo/America/Guayaquil /etc/localtime

Para que la hora se actualice de forma automática, se instala el servidor NTP (Network Time Protocol):

Yum install ntp

Se configura para que se inicie automatice e se inicia:

Chkconfig ntpd on

Service ntpd start

Se continúa con la instalación de **VORBIS** (un codificador/decodificador de archivos audio) y las relativas librerías:

yum install libvorbislibvorbis-develvorbis-tools libogglibogg-devel

Para instalar la función **CURL**:

Yum install curl curl-devel libidn-devel

Se sigue con unas cuantas utilidades y librerías necesarias para la compilación de las fuentes:

yum install gccncursesncurses-devel make gcc-c++ libtermcaplibtermcap-develzlibzlib-devellibtool bison bison-developenssl-devel bzip2 bzip2-devel wget newt newt-devel flex

Si se quiere utilizar **MySQL** como base de datos predefinida:

yum install mysql mysql-server mysql-devel

ODBC para crear conexiones a bases de datos:

yum install unixODBC unixODBC-develmysql-connector-odbclibtool-ltdl-devel

Un sintetizador vocal - **FESTIVAL**:

Yum install festival festival-devel

SPEEX es un codificador decodificador específicamente diseñado para la compresión de la voz. Se instalará partiendo de las fuentes:

cd /usr/src

wget http://downloads.xiph.org/releases/speex/speex-1.2rc1.tar.gz

Para descomprimirlo:

tar -xf speex-1.2rc1.tar.gz

Se entra en la carpeta creada y se compila:

cd speex-1.2rc1

./configure --prefix=/usr

make

make install

Se continúa con un decodificador/codificador MP3 - **LAME**. Útil para usar música en espera en formato MP3.

cd /usr/src

wget http://ufpr.dl.sourceforge.net/sourceforge/lame/lame-3.98.4.tar.gz

Se descomprime:

tar -xf lame-3.98.4.tar.gz

Se entra en la capeta de Lame:

cd lame-3.98.4

Se compilan las fuentes:

./configure --prefix=/usr

make

make install

Para “manipular” los archivos MP3 (por ejemplo para bajar la calidad del sampling) antes de compilar SOX se necesita la librería **LIBMAD**.

Para instalarla:

cd /usr/src

wget http://prdownloads.sourceforge.net/mad/libmad-0.15.1b.tar.gz

tar -xf libmad-0.15.1b.tar.gz

cd libmad-0.15.1b

./configure --prefix=/usr

make

make install

Para terminar esta primera parte se instalará el programa **SOX** (SoundeXchange) muy útil para convertir archivos audio de un formato a otro.

cd /usr/src

wget http://ufpr.dl.sourceforge.net/sourceforge/sox/sox-14.3.1.tar.gz

se descomprime:

tar -xf sox-14.3.1.tar.gz

Se Entra en la carpeta:

cd sox-14.3.1

y se compila:

./configure --prefix=/usr

make

make install

DADHI

El paquete **DADHI** (Digium Asterisk Hardware Device Interface) permite cargar los drivers y configurar distintos tipos de tarjetas en Asterisk (analógicas, digitales, RDSI/ISDN, cancelador de ECHO). Asterisk, además, se apoya en DAHDI para la generación del "timing" indispensable para las conferencias y el trunking IAX2. Para las conferencias, desde las versión 1.6.2, existe también la aplicación ConfBridge que no necesita del timing generado por DAHDI. Los VPS alquilados en Linode utilizan como sistema de virtualización XEN. Por eso para una correcta instalación de DAHDI se tendrá que seguir el procedimiento que sigue.

Primero se averigua la versión del kernel que se está usando:

uname -r

Un ejemplo del resultado del comando es:

2.6.18.8-linode22

Se crea la carpeta donde se guardarán las fuentes del kernel:

mkdir /usr/src/kernel

se entra en la carpeta

cd /usr/src/kernel

Se descargan las fuentes desde la página dedicada de Linode.

Para el ejemplo arriba mencionado sería:

wget http://www.linode.com/src/2.6.18.8-linode22.tar.bz2

Se descomprime:

tar -xf 2.6.18.8-linode22.tar.bz2

Se crea un enlace simbólico a las fuentes descargadas:

cd /lib/modules/2.6.18.8-linode22/

ln -s /usr/src/kernel/2.6.18.8-linode22/ build

Terminada esta operación, empieza el proceso de instalación de DAHDI:

cd /usr/src

wget http://downloads.asterisk.org/pub/telephony/dahdi-linux/dahdi-linux-current.tar.gz

tar -xf dahdi-linux-current.tar.gz

cd dahdi-linux-2.4.1

make

make install

DAHDI Tools:

cd /usr/src

wget http://downloads.asterisk.org/pub/telephony/dahdi-tools/dahdi-tools-current.tar.gz

tar -xf dahdi-tools-current.tar.gz

cd dahdi-tools-2.4.1

./configure

make

make install

make config

Se modifican dos parámetros en el script de arranque de DAHDI porque hay que forzar la instalación del módulo DAHDI en el Kernel:

nano /etc/init.d/dahdi

estas dos líneas:

modprobe dahdi
modprobe dahdi_dummy 2> /dev/null

para que queden:

modprobe -f dahdi
modprobe -f dahdi_dummy 2> /dev/null

Ahora se modifica un archivo para desactivar los módulos de DAHDI que no se utilizarán ya que no hay tarjetas instaladas:

nano /etc/dahdi/modules

Se comentan estas líneas:

wct4xxp
wcte12xp
wct1xxp
wcte11xp
wctdm24xxp
wcfxo
wctdm
wcb4xxp
wctc4xxp
xpp_usb

Para que queden:

#wct4xxp
#cte12xp
#wct1xxp
#wcte11xp
#wctdm24xxp
#wcfxo
#wctdm
#wcb4xxp
#wctc4xxp
#xpp_usb

Ahora podemos iniciar DAHDI:

/**etc/init.d/dahdistart**

No hardware timing source found in /proc/dahdi, loading dahdi_dummy

Runningdahdi_cfg: [OK]

Para el soporte fax hay que instalar Span DSP. Span DSP es un procesador de señales digitales y en Asterisk su función es permitir el envío y la recepción de faxes. Trabaja con archivos Tiff y para compilarlo hay que instalar esas librerías, cabe señalar que esta configuración no es ***utilizada para este trabajo de investigación sin embargo se anota aquí por si se desea configurarla:***

yum install libtiff libtiff-devel llibxml2 libxml2-devel

Se puede continuar con la descarga y instalación de SpanDSP

cd /usr/src

wget http://www.soft-switch.org/downloads/spandsp/spandsp-0.0.6pre17.tgz

tar -xf spandsp-0.0.6pre17.tgz

cd spandsp-0.0.6

./configure --prefix=/usr

make

make install

Asterisk puede conectarse a **GoogleTalk** o a otro servidor de tipo Jabber como cliente. Para que sea posible se debe instalar **GNUTLS** y **IKSEMEL**. Gnutls permite crear conexiones basadas en el protocolo TLS. En CentOS están disponibles los paquetes precompilados:

Yum install gnutls gnutls-develgnutls-utils

Ahora se puede instalar iksemel:

cd /usr/src

wget http://iksemel.googlecode.com/files/iksemel-1.4.tar.gz

tar -xf iksemel-1.4.tar.gz

cd iksemel-1.4

./configure --prefix=/usr

make

make check

Con make check se verifica que la compilación esté sin errores. El comando ejecuta una serie de test y devuelve el resultado. Para completar la instalación:

Make install

Instalamos **SENDMAIL**, un servidor de correo electrónico. Asterisk lo utiliza para enviar correos de notificación cada vez que llegue un correo de voz a las casillas configuradas en el buzón de voz.

yum install sendmailsendmail-develsendmail-cf

Se configura sendmail para que se inicie en automático:

chkconfigsendmail on

Se inicia:

/etc/init.d/sendmailstart

OpenLDAP es la versión open source del protocolo Lightweight Directory Access. Normalmente se utiliza para crear un directorio de usuarios que puede ser consultado y/o modificado desde remoto. Muchos programas implementan la posibilidad de conectarse a un servidor OpenLDAP y en Asterisk, desde la versión 1.6.2.X, se puede utilizar OpenLdap para el realtime de extensiones y dialplan:

yum install compat-openldapopenldapopenldap-clients openldap-developenldap-servers

SNMP es el Protocolo Simple de Administración de Red y sirve para controlar y monitorear el desempeño de nuestro servidor Linux. En Asterisk permite monitorear, entre otras cosas, los canales y las llamadas.

yum install net-snmp net-snmp-devel net-snmp-libs net-snmp-utils

Ahora se puede empezar con la instalación de Asterisk (versión 1.6.2.X). Primero se descargan las fuentes:

cd /usr/src

wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-1.6.2-current.tar.gz

se descomprime:

tar -xf asterisk-1.6.2-current.tar.gz

Se entra en la carpeta:

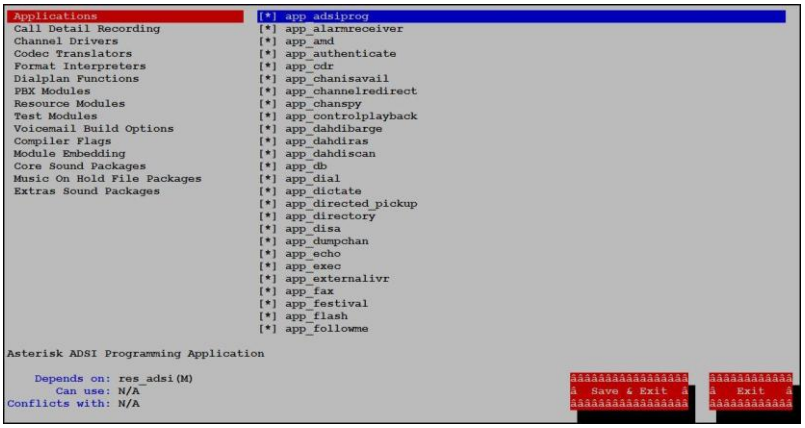
cd asterisk-1.6.2.17

Se compila:

./configure

makemenuselect

Aparecerá:



Desde este menú se pueden configurar todos los módulos que se quiere que Asterisk instale. Se baja con los cursores del teclado hasta “Resource Modules” y averiguar que a lado de res_jabber haya un asterisco. Si no lo hay y aparecen tres XXX significa que no se puede instalar (hubo seguramente algún problema con la instalación de iksemel).

Para tener todas las locuciones y la música en espera en todos los formatos audio disponibles, bajar hasta el menu “CoreSoundPackages” y seleccionar todos los paquetes presentes. Seguir el mismo procedimiento para el menu “Music OnHold File Packages” y “Extras SoundPackages”. Se puede navegar entre los varios menús para seleccionar/deseleccionar los módulos. Para guardar los cambios desde el menú principal hundir el botón “Save&Exit”.

Ahora se compila e instala Asterisk. Esto tomará un tiempo:

make

make install

Para los archivos de configuración de muestra:

Make samples

Para el inicio automático al boot de Linux:

Make config

Asterisk Addons – MySQL, MP3, Chan_mobile

Asterisk Addons es un paquete que añade cuatro funcionalidades principales a la centralita Asterisk:

1. La posibilidad de tener un registro de las llamadas en una base de datos MySQL;
2. Utilizar archivos MP3 para la música en espera
3. Añadir el protocolo H323 (versión propietaria)
4. El canal chan_mobile que permite conectar, viabluetooth, un celular a la centralita y usarlo como Gateway GSM y, si el celular está soportado, envío de SMS.

Antes de empezar iniciar el servidor MySQL

El comando es:

/etc/init.d/mysqldstart

Para que arranque cada vez que se inicia el servidor Linux:

chkconfigmysqldon

Se crea una contraseña para el usuario root:

mysqladmin -u rootpasswordsesamo

Se descarga el paquete de Asterisk addons en la carpeta /usr/src:

cd /usr/src

wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-addons-1.6.2-current.tar.gz

Se descomprime:

tar -xf asterisk-addons-1.6.2-current.tar.gz

Se entra la carpeta recién creada:

cd asterisk-addons-1.6.2.2

Se compila:

./configure

make

make install

Para los archivos de muestra:

Make samples

Ahora para que la centralita tenga un registro de todas las llamadas en MySQL hay que seguir este procedimiento. Crear una base de datos:

Mysql admin createasteriskcdr -u root -psesamo

Entrar en el cliente MySQL como usuario root y la contraseña que se ha creado anteriormente:

mysql -u root -psesamo

Crear la tabla para registrar las llamadas en la base de datos:

mysql> **use asteriskcdr**

mysql> **CREATE TABLE cdr (**

calldatedatetime NOT NULL default '0000-00-00 00:00:00',

clidvarchar(80) NOT NULL default '',

srcvarchar(80) NOT NULL default '',

dstvarchar(80) NOT NULL default '',

dcontextvarchar(80) NOT NULL default '',

channelvarchar(80) NOT NULL default '',

dstchannelvarchar(80) NOT NULL default '',

lastappvarchar(80) NOT NULL default '',

lastdatavarchar(80) NOT NULL default '',

durationint(11) NOT NULL default '0',

billsecint(11) NOT NULL default '0',

dispositionvarchar(45) NOT NULL default '',

amaflagsint(11) NOT NULL default '0',

accountcodevarchar(20) NOT NULL default '',

uniqueidvarchar(32) NOT NULL default '',

userfieldvarchar(255) NOT NULL default ''

);

Crear un nuevo usuario y darle todos los privilegios para manejar la base de datos desde local y remoto:

mysql> **GRANT ALL PRIVILEGES ON asteriskcdr.* TO 'asterisk'@'localhost' IDENTIFIED BY 'sesamo';**

mysql> **GRANT ALL PRIVILEGES ON asteriskcdr.* TO 'asterisk'@'%' IDENTIFIED BY 'sesamo';**

mysql> **flushprivileges;**

mysql> **quit**

Lo único que falta es añadir unas líneas en el archivo de configuración de Asterisk que se encarga de conectarse a la base de datos creada. Se abre el siguiente archivo de texto con nano:

mv /etc/asterisk/cdr_mysql.conf /etc/asterisk/cdr_mysql.conf.old

nano /etc/asterisk/cdr_mysql.conf

y se añaden estas líneas:

[global]
hostname=localhost
dbname=asteriskcdr
table=cdr
password=sesamo
user=asterisk
port=3306
sock=/var/lib/mysql/mysql.sock

Se guardan los cambios (CTRL-O CTRL-X).

Se inicia asterisk:

/etc/init.d/asteriskstart

Se averigua que esté corriendo:

/etc/init.d/asterisk status

asterisk (pid 2403) is running...

Para controlar la conexión a la base de datos, se entra en la consola de Asterisk:

asterisk -rvvvvv

y se escribe el siguiente comando:

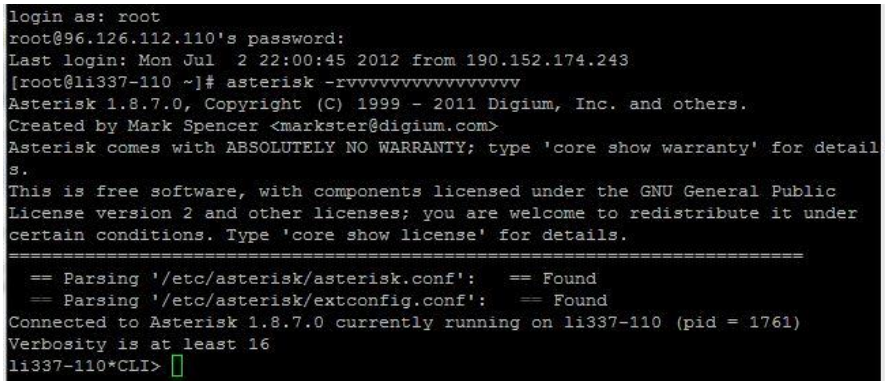
CLI> **cdrmysql status**

Debeaparecer:

Connected to asteriskcdr@localhost, port 3306 using table cdr for 45 seconds.
Wrote 0 records since last restart.

CLI> **quit**

Executing last minute cleanups



Anexo 2

Parámetros de negociación de clave ZRTP

Variable	Description	Comments
ZID	Unique identifier of ZRTP end point	96-bit-long random string generated during initial installation.
hvi/r	Hash value initiator/responder	Computed as hvi = hash (pvi | responder's Hello message).
pvi/r	Public value initiator/responder	Computed as pvi = g^{svi} mod p (initiator). Computed as pvr = g^{svr} mod p (responder).
svi/r	Secret value initiator/responder	Random Diffie-Hellman value based on DH-4096 or DH-3072. The svi value is twice as long as the AES key length. For example, if AES key is 128 bits, svi should be 256 bits.
hash	Supported hash type block	S256; SHA-256 is the only one currently supported.
cipher	Supported cipher types	AES1; AES-CM with 128-bit keys, as defined in RFC 3711. AES2; AES-CM with 256-bit keys, as defined in RFC 3711.
at	Authentication tag	HS32; HMAC-SHA1 32-bit authentication tag, as defined in RFC 3711. HS80; HMAC-SHA1 80-bit authentication tag, as defined in RFC 3711.
keya	Key agreement types	DH3k; DH mode with p=3072-bit prime, as defined in RFC 3526. DH4k; DH mode with p=4096-bit prime, as defined in RFC 3526. Prsh; Pre-shared non-Diffie-Hellman mode uses shared secrets.
SAS	SAS type	B32; Short Authentication String using Base32 encoding. B256; Short Authentication String using Base256 encoding. The SAS value is calculated as the hash of the ZRTP messages (responder's Hello, commit, DHPart1, and DHPart2).

Parámetros de negociación de clave ZRTP (continuación)

Variable	Description	Comments
rs1IDi/r	Retained secret ID	Computed as rs1IDi = HMAC(rs1, "Initiator"). Computed as rs1IDr = HMAC(rs1, "Responder").
rs2IDi/r	Retained secret ID	Computed as rs2IDi = HMAC(rs2, "Initiator"). Computed as rs2IDr = HMAC(rs2, "Responder").
sigsIDi/r	Signaling secret	The HMAC of the initiator's/responder's signaling shared secret. These values are exchanged using the signaling protocol (for example, SIP) and passed to ZRTP. Computed as sigsIDi = HMAC(sigs, "Initiator"). Computed as sigsIDr = HMAC(sigs, "Responder")
srtpsIDi/r	SRTP secret ID	The HMAC of the initiator's/responder's SRTP secret. Computed as srtpsIDi = HMAC(srtps, "Initiator"). Computed as srtpsIDr = HMAC(srtps, "Responder").
other_secretIDi/r	Other secret	HMAC of an additional shared secret in case multiple shared secrets are available. Computed as other_secretIDi = HMAC(other_secret, "Initiator"). Computed as other_secretIDr = HMAC(other_secret, "Responder").
srtpkeyi/r	SRTP key	The ZRTP initiator and responder generate this value using the following: srtpkeyi = HMAC(s0,"Initiator ZRTP key") srtpkeyr = HMAC(s0,"Responder SRTP master key")
srtpsalti/r	SRTP salt	The ZRTP initiator and responder generate this value using the following: rtpsalti = HMAC(s0,"Initiator HMAC key") rtpsaltr HMAC(s0,"Responder HMAC key")

Parámetros de negociación de clave ZRTP (continuación)

Variable	Description	Comments
hmackeyi/r	HMAC key	This value is used only with ZRTP but not SRTP. The ZRTP initiator and responder generate this value using the following: hmackeyi = HMAC(s0,"Initiator HMAC key") hmackeyr = HMAC(s0,"Responder HMAC key") This HMAC key is used to ensure that GoClear messages are unique and cannot be replayed by an attacker to force a connection to go in to unencrypted mode.

Anexo 3

Resumen de los requerimientos de seguridad

Summary of Security Requirements for FIPS 140-2				
	Security level 1	**Security level 2**	**Security level 3**	**Security level 4**
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, approved algorithms and approved modes of operation. Description of cryptographic module including all hardware, software and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output paths.		Data ports for unprotected CSPs, logically or physical separated from all other data ports.	
Roles, Services and Authentication	Logical separation for required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and operational states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for doors and covers.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key input/output, key storage and key zeroization.			
EMI/EMC	47 CFR FCC Part 15, Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15, Subpart B, Class B (Home use).	
Self-Tests	Power-up tests, cryptographic algorithm tests, software/firmware integrity tests, critical functions tests, conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation, design and policy correspondence. Guidance documentation.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations. (informal proofs). Pre-conditions and post-conditions.
Mitigation of Other Attacks	Specification of mitigation of other attacks for which no testable requirements are currently available.			

Anexo 4

Recolección de datos de las pruebas

Test de Control

Uso de CPU

13:00:46	CPU	%user	%nice	%system	%iowait	%steal	%idle
13:00:48	all	0,00	0,00	0,00	0,00	0,12	99,88
13:00:50	all	0,00	0,00	0,00	0,00	0,00	100,00
13:00:52	all	0,00	0,00	0,00	0,00	0,00	100,00
13:00:54	all	0,00	0,00	0,00	0,00	0,00	100,00
13:00:56	all	0,00	0,00	0,00	0,00	0,00	100,00
13:00:58	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:00	all	0,00	0,00	0,13	0,00	0,00	99,87
13:01:02	all	0,00	0,00	0,00	0,00	0,12	99,88
13:01:04	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:06	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:08	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:10	all	0,00	0,00	0,00	0,00	0,13	99,87
13:01:12	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:14	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:16	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:18	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:20	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:22	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:24	all	0,00	0,00	0,00	0,00	0,13	99,87
13:01:26	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:28	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:30	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:32	all	0,00	0,00	0,00	0,00	0,14	99,86
13:01:34	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:36	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:38	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:40	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:42	all	0,00	0,00	0,12	0,00	0,12	99,75
13:01:44	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:46	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:48	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:50	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:52	all	0,00	0,00	0,00	0,00	0,12	99,88
13:01:54	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:56	all	0,00	0,00	0,00	0,00	0,00	100,00
13:01:58	all	0,00	0,00	0,00	0,00	0,00	100,00
13:02:00	all	0,00	0,00	0,00	0,00	0,00	100,00
13:02:02	all	0,00	0,00	0,00	0,00	0,00	100,00
13:02:04	all	0,00	0,00	0,00	0,00	0,12	99,88
13:02:06	all	0,00	0,00	0,00	0,00	0,00	100,00
13:02:08	all	0,00	0,00	0,00	0,00	0,00	100,00
13:02:10	all	0,00	0,00	0,00	0,00	0,00	100,00
13:02:12	all	0,00	0,00	0,00	0,00	0,12	99,88
13:02:14	all	0,00	0,00	0,00	0,00	0,00	100,00
13:02:16	all	0,00	0,00	0,00	0,00	0,00	100,00
13:02:18	all	0,00	0,00	0,00	0,00	0,00	100,00
13:02:20	all	0,00	0,00	0,00	0,00	0,00	100,00
13:02:22	all	0,00	0,00	0,00	0,00	0,12	99,88
13:02:24	all	0,00	0,00	0,00	0,00	0,00	100,00
13:02:26	all	0,00	0,00	0,00	0,00	0,00	100,00
13:02:28	all	0,12	0,00	0,00	0,00	0,00	99,88
13:02:30	all	0,00	0,00	0,00	0,00	0,00	100,00

13:02:32	all	0,00	0,00	0,00	0,00	0,12	99,88
13:02:34	all	0,00	0,00	0,00	0,00	0,00	100,00
13:02:36	all	0,00	0,00	0,00	0,00	0,00	100,00
13:02:38	all	0,00	0,00	0,00	0,00	0,00	100,00
13:02:40	all	0,00	0,00	0,00	0,00	0,00	100,00
13:02:42	all	0,00	0,00	0,00	0,00	0,00	100,00
13:02:44	all	0,00	0,00	0,00	0,00	0,12	99,88
13:02:46	all	0,00	0,00	0,00	0,00	0,00	100,00
Media:	all	0,00	0,00	0,00	0,00	0,02	99,97

Uso de memoria

17:52:19	**kbmemfree**	**kbmemused**	**%memused**	**kbbuffers**	**kbcached**	**kbswpfree**	**kbswpused**	**%swpused**	**kbswpcad**	
17:52:21	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:52:23	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:52:25	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:52:27	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:52:29	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:52:31	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:52:33	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:52:35	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:52:37	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:52:39	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:52:41	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:52:43	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:52:45	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:52:47	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:52:49	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:52:51	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:52:53	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:52:55	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:52:57	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:52:59	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:01	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:03	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:05	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:07	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:09	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:11	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:13	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:15	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:17	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:19	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:21	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:23	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:25	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:27	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:29	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:31	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:33	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:35	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:37	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:39	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:41	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:43	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:45	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:47	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:49	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:51	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:53	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:55	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:57	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:53:59	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:54:01	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:54:03	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:54:05	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:54:07	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:54:09	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:54:11	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:54:13	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:54:15	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:54:17	29808	494664	94,32	41956	352420	262104	32	0,01	0	
17:54:19	29932	494540	94,29	41956	352420	262104	32	0,01	0	
Media:	29810	494662	94,32	41956	352420	262104	32	0,01	0	

Paquetes transmitidos

19:10:25	IFACE	rxpck/s	txpck/s	rxbyt/s	txbyt/s	rxcmp/s	txcmp/s	rxmcst/s
19:10:27	eth0	103,02	101,01	22741,71	22593,97	0,00	0,00	0,00
19:10:29	eth0	102,49	102,49	22585,07	22869,65	0,00	0,00	0,00
19:10:31	eth0	102,49	101,99	22590,05	22758,21	0,00	0,00	0,00
19:10:33	eth0	102,00	102,50	22532,00	22872,00	0,00	0,00	0,00
19:10:35	eth0	103,00	102,50	22645,00	22872,00	0,00	0,00	0,00
19:10:37	eth0	101,49	101,99	22425,87	22795,02	0,00	0,00	0,00
19:10:39	eth0	102,50	103,00	22665,00	23063,00	0,00	0,00	0,00
19:10:41	eth0	100,99	101,49	22308,91	22645,54	0,00	0,00	0,00
19:10:43	eth0	103,00	102,50	22703,00	22872,00	0,00	0,00	0,00
19:10:45	eth0	103,00	102,50	22645,00	22872,00	0,00	0,00	0,00
19:10:47	eth0	101,00	102,49	22250,75	22921,39	0,00	0,00	0,00
19:10:49	eth0	103,50	102,50	22868,00	22872,00	0,00	0,00	0,00
19:10:51	eth0	101,49	101,99	22419,90	22758,21	0,00	0,00	0,00
19:10:53	eth0	104,50	105,00	23547,00	23759,00	0,00	0,00	0,00
19:10:55	eth0	101,50	102,00	22499,00	22839,00	0,00	0,00	0,00
19:10:57	eth0	101,99	102,49	22479,60	22906,47	0,00	0,00	0,00
19:10:59	eth0	101,50	102,50	22499,00	22951,00	0,00	0,00	0,00
19:11:01	eth0	102,50	103,00	22650,00	22969,00	0,00	0,00	0,00
19:11:03	eth0	101,49	101,49	22440,80	22725,37	0,00	0,00	0,00
19:11:05	eth0	102,50	102,50	22644,00	22872,00	0,00	0,00	0,00
19:11:07	eth0	103,00	102,00	22645,00	22812,00	0,00	0,00	0,00
19:11:09	eth0	102,50	103,50	22644,00	23096,00	0,00	0,00	0,00
19:11:11	eth0	101,99	101,99	22473,63	22758,21	0,00	0,00	0,00
19:11:13	eth0	101,99	101,99	22531,34	22758,21	0,00	0,00	0,00
19:11:15	eth0	102,00	102,50	22532,00	22872,00	0,00	0,00	0,00
19:11:17	eth0	102,50	102,00	22586,00	22812,00	0,00	0,00	0,00
19:11:19	eth0	105,00	106,00	23579,00	24300,00	0,00	0,00	0,00
19:11:21	eth0	101,99	101,99	22473,63	22758,21	0,00	0,00	0,00
19:11:23	eth0	61,19	57,21	13275,62	12921,39	0,00	0,00	0,00
19:11:25	eth0	52,00	52,50	11332,00	11672,00	0,00	0,00	0,00
19:11:27	eth0	52,00	52,00	11332,00	11612,00	0,00	0,00	0,00
19:11:29	eth0	43,50	39,50	9397,00	9064,00	0,00	0,00	0,00
19:11:31	eth0	1,99	1,99	131,34	409,95	0,00	0,00	0,00
19:11:33	eth0	4,50	5,50	1782,00	1367,00	0,00	0,00	0,00
19:11:35	eth0	46,27	44,28	9917,41	10244,78	0,00	0,00	0,00
19:11:37	eth0	27,00	54,00	6388,00	12130,00	0,00	0,00	0,00
19:11:39	eth0	40,00	89,50	9035,00	20488,00	0,00	0,00	0,00
19:11:41	eth0	52,24	101,49	11387,06	22698,51	0,00	0,00	0,00
19:11:43	eth0	51,74	101,99	11222,89	22758,21	0,00	0,00	0,00
19:11:45	eth0	52,50	103,00	11444,00	22984,00	0,00	0,00	0,00
19:11:47	eth0	52,00	102,50	11332,00	22924,00	0,00	0,00	0,00
19:11:49	eth0	52,00	103,00	11274,00	22932,00	0,00	0,00	0,00
19:11:51	eth0	50,00	101,49	11049,50	22642,57	0,00	0,00	0,00
19:11:53	eth0	52,50	104,50	11803,00	24082,00	0,00	0,00	0,00
19:11:55	eth0	83,00	103,00	18223,00	23240,00	0,00	0,00	0,00
19:11:57	eth0	102,99	103,48	22954,23	23347,26	0,00	0,00	0,00
19:11:59	eth0	102,50	103,00	22586,00	22932,00	0,00	0,00	0,00
19:12:01	eth0	102,50	102,00	22586,00	22812,00	0,00	0,00	0,00
19:12:03	eth0	101,99	102,49	22531,34	22869,65	0,00	0,00	0,00
19:12:05	eth0	102,00	102,50	22532,00	22872,00	0,00	0,00	0,00
19:12:07	eth0	103,48	103,48	23012,94	23355,22	0,00	0,00	0,00
19:12:09	eth0	103,00	103,50	22643,00	22965,00	0,00	0,00	0,00
19:12:11	eth0	103,50	102,50	22775,00	22869,00	0,00	0,00	0,00
19:12:13	eth0	100,50	101,49	22354,23	22803,98	0,00	0,00	0,00
19:12:15	eth0	101,50	102,00	22499,00	22839,00	0,00	0,00	0,00
19:12:17	eth0	101,99	101,49	22531,34	22698,51	0,00	0,00	0,00
19:12:19	eth0	102,50	103,50	22586,00	23044,00	0,00	0,00	0,00
19:12:21	eth0	102,50	102,50	22592,00	22909,00	0,00	0,00	0,00
19:12:23	eth0	101,49	101,49	22445,54	22835,64	0,00	0,00	0,00
19:12:25	eth0	102,50	103,50	22589,00	23049,00	0,00	0,00	0,00
Media:	eth0	86,27	93,77	19052,17	21005,47	0,00	0,00	0,00

Ancho de banda

```
                           rx         |       tx
--------------------------------------+-----------------
bytes                        815 KiB  |         859 KiB
--------------------------------------+-----------------
max                        96 kbit/s  |      104 kbit/s
average                 75.81 kbit/s  |    79.91 kbit/s
min                         0 kbit/s  |        4 kbit/s
--------------------------------------+-----------------
packets                       3877  |            3852
--------------------------------------+-----------------
max                          56 p/s |          56 p/s
average                      45 p/s  |          44 p/s
min                           2 p/s  |           2 p/s
--------------------------------------+-----------------
time                   2.00 minutes
```

Paquetes perdidos y Jitter

Peer	Call ID	Duration	Recv: Pack	Lost	(%)	Jitter	Send: Pack	Lost	(%)	Jitter
190.152.32.123	0d5ff6f8361	00:00:03	0000000170	0000000000	(0.00%)	0.0000	0000000169	0000000000	(0.00%)	0.0025
190.152.32.123	0d5ff6f8361	00:00:10	0000000488	0000000000	(0.00%)	0.0000	0000000486	0000000000	(0.00%)	0.0030
190.152.32.123	0d5ff6f8361	00:00:13	0000000633	0000000000	(0.00%)	0.0000	0000000631	0000000004	(0.63%)	0.0023
190.152.32.123	0d5ff6f8361	00:00:15	0000000756	0000000000	(0.00%)	0.0000	0000000754	0000000004	(0.53%)	0.0029
190.152.32.123	0d5ff6f8361	00:00:17	0000000843	0000000000	(0.00%)	0.0000	0000000841	0000000004	(0.48%)	0.0023
190.152.32.123	0d5ff6f8361	00:00:18	0000000923	0000000000	(0.00%)	0.0000	0000000921	0000000004	(0.43%)	0.0024
190.152.32.123	0d5ff6f8361	00:00:21	0000001067	0000000000	(0.00%)	0.0000	0000001066	0000000009	(0.84%)	0.0028
190.152.32.123	0d5ff6f8361	00:00:24	0000001216	0000000000	(0.00%)	0.0000	0000001215	0000000009	(0.74%)	0.0022
190.152.32.123	0d5ff6f8361	00:00:26	0000001290	0000000000	(0.00%)	0.0000	0000001288	0000000009	(0.70%)	0.0027
190.152.32.123	0d5ff6f8361	00:00:27	0000001368	0000000000	(0.00%)	0.0000	0000001367	0000000009	(0.66%)	0.0022
190.152.32.123	0d5ff6f8361	00:00:29	0000001447	0000000000	(0.00%)	0.0000	0000001446	0000000009	(0.62%)	0.0023
190.152.32.123	0d5ff6f8361	00:00:31	0000001541	0000000000	(0.00%)	0.0000	0000001540	0000000011	(0.71%)	0.0022
190.152.32.123	0d5ff6f8361	00:00:32	0000001613	0000000000	(0.00%)	0.0000	0000001612	0000000011	(0.68%)	0.0026
190.152.32.123	0d5ff6f8361	00:00:34	0000001713	0000000000	(0.00%)	0.0000	0000001716	0000000011	(0.64%)	0.0091
190.152.32.123	0d5ff6f8361	00:00:36	0000001803	0000000000	(0.00%)	0.0000	0000001802	0000000011	(0.61%)	0.0028
190.152.32.123	0d5ff6f8361	00:00:39	0000001935	0000000000	(0.00%)	0.0000	0000001933	0000000011	(0.57%)	0.0026
190.152.32.123	0d5ff6f8361	00:00:40	0000002012	0000000000	(0.00%)	0.0000	0000002011	0000000015	(0.75%)	0.0026
190.152.32.123	0d5ff6f8361	00:00:42	0000002083	0000000000	(0.00%)	0.0000	0000002081	0000000015	(0.72%)	0.0028
190.152.32.123	0d5ff6f8361	00:00:43	0000002158	0000000000	(0.00%)	0.0000	0000002157	0000000015	(0.70%)	0.0022
190.152.32.123	0d5ff6f8361	00:00:45	0000002240	0000000000	(0.00%)	0.0000	0000002239	0000000015	(0.67%)	0.0023
190.152.32.123	0d5ff6f8361	00:00:46	0000002317	0000000000	(0.00%)	0.0000	0000002316	0000000015	(0.65%)	0.0023
190.152.32.123	0d5ff6f8361	00:00:48	0000002393	0000000000	(0.00%)	0.0000	0000002392	0000000015	(0.63%)	0.0038
190.152.32.123	0d5ff6f8361	00:00:49	0000002462	0000000000	(0.00%)	0.0000	0000002462	0000000015	(0.61%)	0.0104
190.152.32.123	0d5ff6f8361	00:00:51	0000002559	0000000002	(0.08%)	0.0000	0000002559	0000000018	(0.70%)	0.0025
190.152.32.123	0d5ff6f8361	00:00:55	0000002752	0000000002	(0.07%)	0.0000	0000002752	0000000018	(0.65%)	0.0024
190.152.32.123	0d5ff6f8361	00:00:58	0000002888	0000000002	(0.07%)	0.0000	0000002888	0000000018	(0.62%)	0.0027
190.152.32.123	0d5ff6f8361	00:01:02	0000003098	0000000002	(0.06%)	0.0000	0000003118	0000000021	(0.67%)	0.0272

Test con el mecanismo SDes

Uso de CPU

18:39:13	CPU	%user	%nice	%system	%iowait	%steal	%idle
18:39:15	all	0,00	0,00	0,13	0,00	0,00	99,87
18:39:17	all	0,00	0,00	0,00	0,00	0,12	99,88
18:39:19	all	0,00	0,00	0,00	0,00	0,00	100,00
18:39:21	all	0,00	0,00	0,00	0,00	0,00	100,00
18:39:23	all	0,00	0,00	0,00	0,00	0,00	100,00
18:39:25	all	0,00	0,00	0,00	0,00	0,00	100,00
18:39:27	all	0,00	0,00	0,00	0,23	0,12	99,65
18:39:29	all	0,00	0,00	0,00	0,00	0,00	100,00
18:39:31	all	0,00	0,00	0,00	0,00	0,00	100,00
18:39:33	all	0,00	0,00	0,00	0,00	0,12	99,88
18:39:35	all	0,00	0,00	0,00	0,00	0,00	100,00
18:39:37	all	0,00	0,00	0,00	0,00	0,00	100,00
18:39:39	all	0,00	0,00	0,00	0,00	0,00	100,00
18:39:41	all	0,00	0,00	0,00	0,00	0,13	99,87
18:39:43	all	0,00	0,00	0,00	0,00	0,00	100,00
18:39:45	all	0,00	0,00	0,00	0,00	0,00	100,00
18:39:47	all	0,00	0,00	0,00	0,00	0,00	100,00
18:39:49	all	0,12	0,00	0,00	0,00	0,12	99,75
18:39:51	all	0,00	0,00	0,00	0,00	0,00	100,00
18:39:53	all	0,00	0,00	0,00	0,00	0,00	100,00
18:39:55	all	0,00	0,00	0,00	0,00	0,00	100,00
18:39:57	all	0,00	0,00	0,00	0,00	0,12	99,88
18:39:59	all	0,00	0,00	0,00	0,00	0,00	100,00
18:40:01	all	0,00	0,00	0,00	0,00	0,11	99,89
18:40:03	all	0,00	0,00	0,00	0,00	0,00	100,00
18:40:05	all	0,00	0,00	0,00	0,00	0,00	100,00
18:40:07	all	0,00	0,00	0,00	0,00	0,00	100,00
18:40:09	all	0,00	0,00	0,00	0,00	0,00	100,00
18:40:11	all	0,00	0,00	0,00	0,00	0,13	99,87
18:40:14	all	0,00	0,00	0,00	0,00	0,00	100,00
18:40:16	all	0,00	0,00	0,00	0,00	0,00	100,00
18:40:18	all	0,00	0,00	0,00	0,00	0,00	100,00
18:40:20	all	0,00	0,00	0,00	0,00	0,11	99,89
18:40:22	all	0,00	0,00	0,00	0,00	0,00	100,00
18:40:24	all	0,00	0,00	0,00	0,00	0,00	100,00
18:40:26	all	0,12	0,00	0,00	0,00	0,00	99,88
18:40:28	all	0,00	0,00	0,00	0,00	0,12	99,88
18:40:30	all	0,00	0,00	0,00	0,00	0,00	100,00
18:40:32	all	0,00	0,00	0,00	0,00	0,00	100,00
18:40:34	all	0,00	0,00	0,00	0,00	0,00	100,00
18:40:36	all	0,12	0,00	0,00	0,00	0,00	99,88
18:40:38	all	0,00	0,00	0,00	0,00	0,12	99,88
18:40:40	all	0,00	0,00	0,00	0,00	0,00	100,00
18:40:42	all	0,00	0,00	0,13	0,00	0,00	99,87
18:40:44	all	0,00	0,00	0,00	0,00	0,00	100,00
18:40:46	all	0,00	0,00	0,00	0,00	0,00	100,00
18:40:48	all	0,00	0,00	0,00	0,00	0,12	99,88
18:40:50	all	0,00	0,00	0,00	0,00	0,00	100,00
18:40:52	all	0,00	0,00	0,00	0,00	0,00	100,00
18:40:54	all	0,00	0,00	0,00	0,00	0,13	99,87
18:40:56	all	0,00	0,00	0,00	0,00	0,00	100,00
18:40:58	all	0,00	0,00	0,00	0,00	0,00	100,00
18:41:00	all	0,00	0,00	0,00	0,00	0,00	100,00
18:41:02	all	0,00	0,00	0,00	0,00	0,00	100,00
18:41:04	all	0,00	0,00	0,00	0,00	0,12	99,88
18:41:06	all	0,00	0,00	0,00	0,00	0,00	100,00
18:41:08	all	0,00	0,00	0,00	0,00	0,00	100,00
18:41:10	all	0,00	0,00	0,00	0,00	0,12	99,88
18:41:12	all	0,00	0,00	0,00	0,00	0,00	100,00
18:41:14	all	0,00	0,00	0,00	0,00	0,00	100,00
Media:	all	0,01	0,00	0,00	0,00	0,03	99,95

Uso de memoria

13:09:04	kbmemfree	kbmemused	%memused	kbbuffers	kbcached	kbswpfree	kbswpused	%swpused	kbswpcad	
13:09:06	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:08	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:10	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:12	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:14	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:16	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:18	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:20	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:22	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:24	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:26	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:28	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:30	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:32	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:34	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:36	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:38	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:40	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:42	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:44	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:46	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:48	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:50	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:52	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:54	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:56	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:09:58	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:10:00	29376	495096	94,40	41900	355564	262104	32	0,01	0	
13:10:02	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:04	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:06	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:08	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:10	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:12	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:14	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:16	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:18	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:20	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:22	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:24	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:26	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:28	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:30	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:32	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:34	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:36	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:38	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:40	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:42	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:44	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:46	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:48	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:50	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:52	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:54	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:56	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:10:58	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:11:00	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:11:02	29004	495468	94,47	41900	355568	262104	32	0,01	0	
13:11:04	29004	495468	94,47	41900	355568	262104	32	0,01	0	
Media:	29178	495294	94,44	41900	355566	262104	32	0,01	0	

Ancho de banda

rx		tx
bytes	4.07 MiB	4.12 MiB
max	184 kbit/s	184 kbit/s
average	167.64 kbit/s	169.65 kbit/s
min	0 kbit/s	0 kbit/s
packets	19221	19252
max	105 p/s	105 p/s
average	96 p/s	96 p/s
min	0 p/s	0 p/s
time	2.00 minutes	

Paquetes perdidos y Jitter

Peer	Call ID	Duration	Recv: Pack	Lost	(%)	Jitter	Send: Pack	Lost	(%)	Jitter
190.152.242.248	5c36b29ae06	00:00:40	0000000529	0000000099	(15.76%)	0.0000	0000000616	0000000000	(0.00%)	0.0064
192.168.1.4	121928d34fc	00:00:40	0000000616	0000000019	(2.99%)	0.0000	0000000529	0000000000	(0.00%)	0.0067
190.152.242.248	5c36b29ae06	00:00:47	0000000841	0000000099	(10.53%)	0.0000	0000000928	0000000090	(9.70%)	0.0043
192.168.1.4	121928d34fc	00:00:47	0000000928	0000000019	(2.01%)	0.0000	0000000841	0000000004	(0.48%)	0.0051
190.152.242.248	5c36b29ae06	00:00:57	0000001341	0000000099	(6.88%)	0.0000	0000001428	0000000096	(6.72%)	0.0043
192.168.1.4	121928d34fc	00:00:57	0000001428	0000000019	(1.31%)	0.0000	0000001341	0000000008	(0.60%)	0.0048
190.152.242.248	5c36b29ae06	00:01:00	0000001524	0000000099	(6.10%)	0.0000	0000001611	0000000096	(5.96%)	0.0035
192.168.1.4	121928d34fc	00:01:00	0000001611	0000000019	(1.17%)	0.0000	0000001524	0000000008	(0.52%)	0.0043
190.152.242.248	5c36b29ae06	00:01:07	0000001885	0000000099	(4.99%)	0.0000	0000001972	0000000104	(5.27%)	0.0041
192.168.1.4	121928d34fc	00:01:07	0000001972	0000000019	(0.95%)	0.0000	0000001885	0000000013	(0.69%)	0.0045
190.152.242.248	5c36b29ae06	00:01:13	0000002181	0000000099	(4.34%)	0.0000	0000002268	0000000104	(4.59%)	0.0040
192.168.1.4	121928d34fc	00:01:13	0000002268	0000000019	(0.83%)	0.0000	0000002181	0000000016	(0.73%)	0.0043
190.152.242.248	5c36b29ae06	00:01:18	0000002399	0000000099	(3.96%)	0.0000	0000002485	0000000110	(4.43%)	0.0047
192.168.1.4	121928d34fc	00:01:18	0000002485	0000000019	(0.76%)	0.0000	0000002399	0000000016	(0.67%)	0.0049
190.152.242.248	5c36b29ae06	00:01:19	0000002475	0000000099	(3.85%)	0.0000	0000002562	0000000110	(4.29%)	0.0042
192.168.1.4	121928d34fc	00:01:19	0000002562	0000000019	(0.74%)	0.0000	0000002475	0000000016	(0.65%)	0.0044
190.152.242.248	5c36b29ae06	00:01:23	0000002681	0000000099	(3.56%)	0.0000	0000002768	0000000117	(4.23%)	0.0048
192.168.1.4	121928d34fc	00:01:23	0000002768	0000000019	(0.68%)	0.0000	0000002681	0000000018	(0.67%)	0.0053
190.152.242.248	5c36b29ae06	00:01:26	0000002800	0000000099	(3.41%)	0.0000	0000002887	0000000117	(4.05%)	0.0050
192.168.1.4	121928d34fc	00:01:26	0000002887	0000000019	(0.65%)	0.0000	0000002800	0000000018	(0.64%)	0.0055
190.152.242.248	5c36b29ae06	00:01:30	0000003010	0000000099	(3.18%)	0.0000	0000003097	0000000117	(3.78%)	0.0038
192.168.1.4	121928d34fc	00:01:30	0000003097	0000000019	(0.61%)	0.0000	0000003010	0000000018	(0.60%)	0.0048
190.152.242.248	5c36b29ae06	00:01:37	0000003357	0000000099	(2.86%)	0.0000	0000003426	0000000120	(3.50%)	0.0071
192.168.1.4	121928d34fc	00:01:37	0000003426	0000000019	(0.55%)	0.0000	0000003357	0000000022	(0.66%)	0.0066
190.152.242.248	5c36b29ae06	00:01:40	0000003514	0000000099	(2.74%)	0.0000	0000003587	0000000120	(3.35%)	0.0040
192.168.1.4	121928d34fc	00:01:40	0000003587	0000000036	(0.99%)	0.0000	0000003514	0000000022	(0.63%)	0.0043
190.152.242.248	5c36b29ae06	00:01:45	0000003748	0000000099	(2.57%)	0.0000	0000003818	0000000126	(3.30%)	0.0038
192.168.1.4	121928d34fc	00:01:45	0000003818	0000000036	(0.93%)	0.0000	0000003748	0000000027	(0.72%)	0.0047
190.152.242.248	5c36b29ae06	00:01:49	0000003978	0000000099	(2.43%)	0.0000	0000004048	0000000126	(3.11%)	0.0048
192.168.1.4	121928d34fc	00:01:49	0000004048	0000000036	(0.88%)	0.0000	0000003978	0000000027	(0.68%)	0.0052
190.152.242.248	5c36b29ae06	00:01:52	0000004116	0000000099	(2.35%)	0.0000	0000004186	0000000133	(3.18%)	0.0042
192.168.1.4	121928d34fc	00:01:52	0000004186	0000000036	(0.85%)	0.0000	0000004116	0000000037	(0.90%)	0.0046

```
190.152.242.248  5c36b29ae06  00:01:55 0000004267  0000000099 ( 2.27%) 0.0000 0000004337  0000000133 ( 3.07%) 0.0043
192.168.1.4      121928d34fc  00:01:55 0000004337  0000000036 ( 0.82%) 0.0000 0000004267  0000000037 ( 0.87%) 0.0048
190.152.242.248  5c36b29ae06  00:02:00 0000004517  0000000099 ( 2.14%) 0.0000 0000004587  0000000139 ( 3.03%) 0.0047
192.168.1.4      121928d34fc  00:02:00 0000004587  0000000036 ( 0.78%) 0.0000 0000004517  0000000043 ( 0.95%) 0.0052
190.152.242.248  5c36b29ae06  00:02:07 0000004843  0000000099 ( 2.00%) 0.0000 0000004913  0000000139 ( 2.83%) 0.0045
192.168.1.4      121928d34fc  00:02:07 0000004913  0000000036 ( 0.73%) 0.0000 0000004843  0000000043 ( 0.89%) 0.0048
190.152.242.248  5c36b29ae06  00:02:12 0000005119  0000000099 ( 1.90%) 0.0000 0000005189  0000000147 ( 2.83%) 0.0064
192.168.1.4      121928d34fc  00:02:12 0000005189  0000000036 ( 0.69%) 0.0000 0000005119  0000000046 ( 0.90%) 0.0046
190.152.242.248  5c36b29ae06  00:02:16 0000005293  0000000099 ( 1.84%) 0.0000 0000005363  0000000147 ( 2.74%) 0.0049
192.168.1.4      121928d34fc  00:02:16 0000005363  0000000036 ( 0.67%) 0.0000 0000005293  0000000046 ( 0.87%) 0.0051
190.152.242.248  5c36b29ae06  00:02:17 0000005376  0000000099 ( 1.81%) 0.0000 0000005445  0000000147 ( 2.70%) 0.0047
192.168.1.4      121928d34fc  00:02:17 0000005445  0000000036 ( 0.66%) 0.0000 0000005376  0000000052 ( 0.97%) 0.0046
190.152.242.248  5c36b29ae06  00:02:24 0000005722  0000000099 ( 1.70%) 0.0000 0000005791  0000000152 ( 2.62%) 0.0043
192.168.1.4      121928d34fc  00:02:24 0000005791  0000000036 ( 0.62%) 0.0000 0000005722  0000000052 ( 0.91%) 0.0041
190.152.242.248  5c36b29ae06  00:02:27 0000005841  0000000099 ( 1.67%) 0.0000 0000005911  0000000152 ( 2.57%) 0.0042
192.168.1.4      121928d34fc  00:02:27 0000005911  0000000036 ( 0.61%) 0.0000 0000005841  0000000057 ( 0.98%) 0.0043
190.152.242.248  5c36b29ae06  00:02:29 0000005984  0000000099 ( 1.63%) 0.0000 0000006054  0000000156 ( 2.58%) 0.0042
192.168.1.4      121928d34fc  00:02:29 0000006054  0000000036 ( 0.59%) 0.0000 0000005984  0000000057 ( 0.95%) 0.0039
190.152.242.248  5c36b29ae06  00:02:32 0000006120  0000000099 ( 1.59%) 0.0000 0000006189  0000000156 ( 2.52%) 0.0048
192.168.1.4      121928d34fc  00:02:32 0000006189  0000000036 ( 0.58%) 0.0000 0000006120  0000000057 ( 0.93%) 0.0051
190.152.242.248  5c36b29ae06  00:02:35 0000006267  0000000099 ( 1.56%) 0.0000 0000006337  0000000156 ( 2.46%) 0.0044
192.168.1.4      121928d34fc  00:02:35 0000006337  0000000036 ( 0.56%) 0.0000 0000006267  0000000060 ( 0.96%) 0.0049
190.152.242.248  5c36b29ae06  00:02:39 0000006446  0000000100 ( 1.53%) 0.0000 0000006500  0000000161 ( 2.48%) 0.0035
192.168.1.4      121928d34fc  00:02:39 0000006500  0000000053 ( 0.81%) 0.0000 0000006446  0000000060 ( 0.93%) 0.0044
190.152.242.248  5c36b29ae06  00:02:47 0000006844  0000000100 ( 1.44%) 0.0000 0000006898  0000000164 ( 2.38%) 0.0042
192.168.1.4      121928d34fc  00:02:47 0000006898  0000000053 ( 0.76%) 0.0000 0000006844  0000000062 ( 0.91%) 0.0048
190.152.242.248  5c36b29ae06  00:02:49 0000006954  0000000100 ( 1.42%) 0.0000 0000007012  0000000164 ( 2.34%) 0.0114
192.168.1.4      121928d34fc  00:02:49 0000007012  0000000053 ( 0.75%) 0.0000 0000006954  0000000062 ( 0.89%) 0.0071
190.152.242.248  5c36b29ae06  00:02:55 0000007272  0000000100 ( 1.36%) 0.0000 0000007327  0000000169 ( 2.31%) 0.0033
192.168.1.4      121928d34fc  00:02:55 0000007327  0000000053 ( 0.72%) 0.0000 0000007272  0000000068 ( 0.94%) 0.0040
```