ESCUELA SUPERIOR POLITECNICA DEL LITORAL

FACULTAD DE INGENIERIA EN ELECTRICIDAD Y COMPUTACION

TESIS DE GRADO

"ANÁLISIS DE SEGURIDAD DE TRANSFERENCIA DE VOIP Y DESEMPEÑO DE LOS PROTOCOLOS EN REDES CON CLIENTES INALAMBRICOS."

Previa a la obtención del título de Ingeniero en Computación especialización Sistemas Tecnológico

PRESENTADA POR:

GALO RAFAEL ITURRALDE ORELLANA

GUAYAQUIL - ECUADOR

2006

AGRADECIMIENTO

A todos quienes me
ayudaron para la
presentación de este trabajo.
En especial a mis padres,
mis hermanos, Diana Moreira y
a mi directora Ing. Cristina Abad
apoyándome y alentándome
en todo momento.

DEDICATORIA

Con cariño, a mis papás.
Galo y Alicia.

TRIBUNAL DE GRADO

PRESIDENTE

Ing. Holger Cevallos U.

DIRECTOR DE TESIS

Ing. Cristina Abad

MIEMBROS PRINCIPALES

Ing. Guido Caicedo

Ing. Galo Valverde

DECLARACIÓN EXPRESA

"La responsabilidad por los hechos, ideas y doctrinas expuestas en esta tesis, me corresponden exclusivamente; y, el patrimonio intelectual de la misma, a la Escuela Superior Politécnica del Litoral"

(Reglamento de exámenes y títulos profesionales de la ESPOL)

Galo Rafael Iturralde Orellana

RESUMEN

Actualmente podemos encontrar variedad de información sobre la transferencia de voz sobre IP (VoIP) y de cómo implementar esta tecnología, pero muy poca información con respecto a cómo lograr que estas trasmisiones sean seguras o de cómo se podría mejorar su calidad. El énfasis se centra generalmente en como logramos una instalación funcional.

Este tema enfrenta este problema analizando los dos protocolos más comunes en la transmisión de voz sobre IP: el protocolo H.323 y el protocolo SIP, comparando su rendimiento en clientes inalámbricos y las seguridades que ofrece. De esta manera se ofrecen los criterios básicos sobre una transferencia de voz sobre IP eficiente y segura.

ÍNDICE GENERAL

AGRADECIMIENTO ii
DEDICATORIA iii
DECLARACIÓN EXPRESA v
RESUMEN vi
ÍNDICE GENERAL vii
ÍNDICE DE FIGURAS x
INTRODUCCIÓN xiii

CAPÍTULO 1 1
1.1. Voz sobre IP (VoIP) 1
1.1.1 General 1
1.1.2 Arquitectura VoIP 1
1.1.3 Requerimientos de Calidad 2
1.1.4 Componentes de una red VoIP 3
1.2. Protocolos VoIP 3
1.2.1 Protocolo H.323 4
1.2.1.1 General 4
1.2.1.2 Arquitectura 5
1.2.1.3 Pila 7
1.2.1.4 Flujo de Mensajes 9
1.2.1.5 Tipo de Seguridad 11
1.2.2 Protocolo SIP 13
2.2.1 General 13
1.2.2.2 Arquitectura 14
1.2.2.3 Pila 16
1.2.2.4 Flujo de Mensajes 17
1.2.2.5 Tipo de Seguridad 18
1.2.3 Diferencias entre SIP y H.323 19
1.2.4 Fallas encontradas 21
1.2.5 Tipos de Seguridad 21
1.3. Tecnología Inalámbrica 24
1.3.1 Estándares 802.11x 24
1.3.2 Seguridad de una Red Inalámbrica 26
1.3.2.1. WEP 26
1.3.2.2. RADIUS 27
1.3.2.3. SSL 27
1.3.3 Vulnerabilidades de VoIP 28
1.4. Seguridad VoIP 28
1.4.1 Requerimientos de Seguridad 28
1.4.2 Tipos de Protección 29
1.4.3 IPSec 32
CAPÍTULO 2 33
2.1. Modelo Analítico 33
2.1.1 Topologías 33
2.1.2 Red Inalámbrica 35
2.1.3 Metodología 40

2.1.3.1 Parámetros a Evaluar 40
2.1.3.2 Jitter (variación del rendimiento) 40
2.1.3.3 Delay (Demora) 41
2.1.3.4 Load (Carga) 41
2.1.3.5 Tiempo de Señalización 41
2.1.3.6 Envío y Recepción de Transferencia de Datos 41
2.1.4 Parámetros a variar 42
2.1.4.1 Codec 42
2.1.4.2 Tipo de Señalización 43
2.1.4.3 Voice Frame per Packets (VFPP) 44
2.1.4.4 ToS 44
2.1.4.5 QoS 45
2.1.4.6 Número de Nodos 46
2.2. Tipos de Simuladores 46
2.2.1 OPNET vs NS2 46
2.2.2.3 Datos de Salida 49
2.2.3 Configuración del Modelo Analítico 50
2.3. Resultados 54
2.4. Evaluación de Resultados 63
2.4.1 SIP 63
2.4.3 Errores 66
CAPÍTULO 3 67
3.1. PRUEBAS DE CAMPO 67
Diseño del Experimento 67
3.1.1 Modelo de Campo 68
3.1.2 Topología 69
3.1.3 Configuración del Modelo de Campo 70
1.4 Software para evaluar los datos 79
3.1.5 Recolección de Datos 81
3.2.-Resultados 84
3.2.1 Comparación de los Resultados Simulados y de Campo 84
3.2.2 Análisis de resultados 85
CONCLUSIONES Y RECOMENDACIONES 87
GLOSARIO 90
APÉNDICES 94
A APÉNDICE A: ELEMENTOS ESCOGIDOS PARA LA SIMULACIÓN DEL PROGRAMA IT-GURU. 94
A.1 Nodos 94
A.2 Descripción de Nodos 95
B APÉNDICE B: RESULTADOS DE LAS SIMULACIONES. 96
B.1 Resultados de la simulación de la topología 1, SIP – CODEC. 96
B.2 Resultados de la simulación de la topología 1, H.323 – CODEC. 96
B.3 Resultados de la simulación de la topología 2, SIP – CODEC 97
B.4 Resultados de la simulación de la topología 2, H.323 – CODEC 97
B.5 Resultados de la simulación de la topología 1, SIP – VFPP 98
B.6 Resultados de la simulación de la topología 1, H.323 – VFPP 98
B.7 Resultados de la simulación de la topología 2, SIP – VFPP 99
B.8 Resultados de la simulación de la topología 2, H.323 – VFPP 99
B.9 Resultados de la simulación de la topología 1, SIP – ToS 100

B.10 Resultados de la simulación de la topología 1, H.323 – ToS 100
B.11 Resultados de la simulación de la topología 2, SIP – ToS 101
B.12 Resultados de la simulación de la topología 2, H.323 – ToS 101
B.13 Resultados de la simulación de la topología 1, H.323 – QoS 102
B.14 Resultados de la simulación de la topología 2, H.323 – QoS 102
B.15 Resultados de la simulación de la topología 1, SIP – N. Nodos ... 103
B.16 Resultados de la simulación de la topología 1, H.323 – N. Nodos 103
B.17 Resultados de la simulación de la topología 2, SIP – N. Nodos ... 104
B.18 Resultados de la simulación de la topología 2, H.323 – N. Nodos 104
B.19 Resultados de la simulación de la topología 1, SIP – VPN 105
B.20 Resultados de la simulación de la topología 1, H.323– VPN 105
B.21 Resultados de la simulación de la topología 2, H.323– VPN 105
B.22 Resultados de la simulación de la topología 2, H.323– VPN 105
C APÉNDICE C: INSTALACIÓN DEL PROGRAMA IT-GURU. 106
C.1 Obtención de licencia del programa IT-GURU 106
C.2 Pasos para la instalación del programa IT-GURU 109
D APÉNDICE D: CONFIGURACIÓN DE LOS NODOS PARA LA SIMULACIÓN. 115
D.1 Configuración para SIP 115
D.2 Configuración para H.323 116
E APÉNDICE E: CONFIGURACIÓN DEL PROYECTO OPENH.323 119
F APÉNDICE F: CONFIGURACIÓN DEL GNU GATEKEEPER. 120
G APÉNDICE D: RESULTADOS DE LAS PRUEBAS DE CAMPO. 124
G.1 Resultados de la estación 1 y estación 2 para SIP 124
G.2 Resultados de la estación Prueba1 y prueba2 para H.323 124
G.3 Resultados de la estación 3 y estación 4 para SIP 125
G.4 Resultados de la estación 3 y estación 4 para H.323 125
G.5 Resultados de la estación 5 y estación 6 para SIP 126
G.6 Resultados de la estación 5 y estación 6 para H.323 126
G.7 Resultados de la estación 7 y estación 8 para SIP 127
G.8 Resultados de la estación 7 y estación 8 para H.323 127
BIBLIOGRAFÍA 128

ÍNDICE DE FIGURAS

Figura 1-1. Componentes básicos de una red VoIP 3
Figura 1-2. Pila del Protocolo H.323 7
Figura 1-3. Flujo de mensajes 9
Figura 1-4. Flujo de mensajes 14
Figura 1-5. Pila del protocolo SIP 16
Figura 1-6. Flujo de mensajes del protocolo SIP 17
Figura 2-1. Topología tipo estrella 34
Figura 2-2. Topología de red celular 35
Figura 2-3. Diseño topología 1 con SIP 35
Figura 2-4. Interior del sitio_1 topología 1 SIP 36
Figura 2-5. Diseño topología 1 con H.323 37
Figura 2-6. Interior del sitio 1 Topología 1 H.323 37
Figura 2-7. Diseño topología 2 con SIP 38
Figura 2-8. Interior subset_1 topología 2 SIP 38
Figura 2-9. Diseño topología 2 con H.323 39
Figura 2-10. Interior subnet_1 topología 2 H.323 39
Figura 2-11. Modelo analítico topología 1 47
Figura 2-12. Modelo analítico topología 2 48
Figura 2-13. Ventana de selección de datos a mostrar 50
Figura 2-14. Diagrama codec-carga de SIP topología 1 54
Figura 2-15. Diagrama codec-carga de H.323 topología 1 54
Figura 2-16. Diagrama codec-carga de SIP topología 2 55
Figura 2-17. Diagrama codec-carga de H.323 topología 2 56
Figura 2-18. Diagrama VFPP-carga de H.323 topología 1 57
Figura 2-19. Diagrama VFPP-carga de SIP topología 2 57
Figura 2-20. Diagrama Carga vs Nodo Topología 1 59
Figura 2-21. Diagrama Carga vs Nodo Topología 2 59
Figura 2-22. Variación del Jitter con VPN topología 1 SIP 61
Figura 2-23. Variación del Jitter con VPN topología 1 H.323 61
Figura 2-24. Variación del Jitter con VPN topología 2 SIP 62
Figura 2-25. Variación del Jitter con VPN topología 2 H.323 62
Figura 3-1. Laboratorio Móvil del C.T.I 67
Figura 3-2. Interior del laboratorio Móvil del C.T.I 68
Figura 3-3. Arquitectura del laboratorio móvil 69
Figura 3-4. Ventana principal del cliente OpenPhone. 70
Figura 3-5. Ventana de selección de opciones del cliente OpenPhone. 71
Figura 3-6. Ventana General de opciones del cliente OpenPhone. 71
Figura 3-7. Opciones del Gatekeeper del cliente OpenPhone. 72
Figura 3-8. Opciones del Codec de Audio del cliente OpenPhone. 72
Figura 3-9. Ventana del GNU Gatekeeper 73
Figura 3-10. Servicios del Gatekeeper. 74
Figura 3-11. Ventana del Xlite – configuración del cliente 79
Figura 3-12. Ventana principal del Packetyzer 80
Figura 3-13. Gráfico de paquetes recibidos de los protocolos SIP y H.323 81
Figura 3-14. Gráfico de la utilización promedio de los protocolos SIP y H.323 82
Figura 3-15. Gráfico de bytes de datos recibidos de los protocolos SIP y H.323 83

Figura C.1-1. Ventana para ingresar usuario y password en OPNET.....106
Figura C.1-2. Ventana para registrar nuevo usuario en OPNET.....107
Figura C.2-1. Ventana para obtener licencia de IT-GURU.....109
Figura C.2-2. Ventana de explicación para obtener licencia de IT-GURU.....110
Figura C.2-3. Ventana para obtener licencia de IT-GURU.....110
Figura C.2-4. Ventana de generación de código.....111
Figura C.2-5. Pegar código generado.....112
Figura C.2-6. Código de activación del programa IT-GURU.....112
Figura C.2-7. Continuación de la activación de IT-GURU.....113
Figura C.2-8. Pegar Código de activación.....114
Figura C.2-7. Ventana fianal de activación.....114
Figura D.1-1. Configuración de la definición de Aplicación – SIP.....115
Figura D.1-2. Configuración de los terminales - SIP.....115
Figura D.1-1. Configuración del servidor Proxy – SIP.....116
Figura D.2-1. Configuración de la definición de Aplicación –H.323.....116
Figura D.2-2. Configuración del protocolo RSVP en los Atributos – H.323. ..117
Figura D.2-3. Configuración del protocolo RSVP en el nodo – H.323.....117
Figura D.2-2. Configuración del protocolo RSVP en las interfaces – H.323. .118

ÍNDICE DE TABLAS

Tabla 1-1. Diferencias entre H.323 y SIP 20
Tabla 2-1. Especificaciones de codecs..... 43
Tabla 2-2. Datos insertados en la simulación para evaluar..... 49
Tabla 2-3. Configuración de los parámetros de voz para SIP..... 51
Tabla 2-4. Configuración de los parámetros de voz en el cliente..... 51
Tabla 2-5. Habilitar el servidor Proxy..... 52
Tabla 2-6. Configuración de los parámetros de voz para H.323..... 52
Tabla 2-7. Activación del protocolo RSVP en las interfaces de los nodos..... 53
Tabla 2-8. Habilitar el estatus del protocolo RSVP..... 53
Tabla 2-9. Variables obtenidas del protocolo SIP – Topología 1 64
Tabla 2-10. Variables obtenidas del protocolo SIP – Topología 2 64
Tabla 2-11. Variables obtenidas del protocolo H.323 – Topología 1..... 65
Tabla 2-12. Variables obtenidas del protocolo H.323 – Topología 2..... 65
Tabla 3-1. Parámetros a evaluar en las pruebas de campo..... 80
Tabla E-1. Programas necesarios para ejecutar el cliente OpenH323 119

INTRODUCCIÓN

Este tema analiza los dos protocolos más comunes en la transmisión de voz sobre IP que son el protocolo H.323 y el protocolo SIP, comparando su rendimiento en clientes inalámbricos y evaluando cómo el añadir seguridades a estos protocolos afecta su rendimiento.

Los objetivos trazados son: análisis y estudio del funcionamiento de los dos protocolos más usados en la transferencia de voz sobre IP el propuesto por la ITU-T[1] (H.323) y el propuesto por la IETF[2] el protocolo (SIP) y a su vez realizar pruebas de los protocolos con la finalidad de evaluar las diferentes ventajas y desventajas al ser implementados y poder decidir cual es el más conveniente o si es posible crear un híbrido del mismo y a su vez encontrar los parámetros que nos permitan saber cuáles son más críticos y pueden mejorar su desempeño.

Primero se recopilan conceptos de VoIP, requerimientos de calidad, análisis de los protocolos H.323 y SIP. Los elementos que intervienen, su arquitectura y tipo de seguridad en tecnología inalámbrica.

---

[1] ITU-T.- “Internacional Telecomunications Union – Telecomunication”. Agencia de la Organización de las Naciones Unidas que trata lo referente a las telecomunicaciones.

[2] IETF.- “Internet Experts Task Force”. Es el comité encargo de elaborar los estándares de Internet.

Luego se realiza un análisis de los programas de simulación mas adecuados, se escoge uno para proceder hacer pruebas. Escogiendo parámetros a variar y a evaluar. Se diseña dos tipos de topologías y se trabaja en base a estas para realizar dichas pruebas. De los parámetros evaluados se escogen los que muestran mejor rendimiento para ser usados en las pruebas de campo.

Teniendo los parámetros de las simulaciones se configura ocho computadoras conectadas inalámbricamente que se encuentra en un laboratorio móvil propiedad de la ESPOL manejado por el Centro Tecnológico de Información. Y se evalúa mediante un software el comportamiento de la carga generada.

Finalmente se evalúan los comportamientos de los parámetros obtenidos en las simulaciones y en las pruebas de campo con la finalidad de observar una coherencia entre ambos, indicar cuáles son los más adecuados para utilizar al momento de implementar una red de VoIP con clientes inalámbricos, y poder dejar pautas para crear nuevos estudios.

CAPÍTULO 1

1.1. Voz sobre IP (VoIP)

1.1.1 General

El término VoIP viene de las siglas en inglés de Voice over IP, que quiere decir voz sobre IP. La transferencia de voz sobre una red IP es una tecnología que básicamente consiste en usar una red de datos como backbone para la transmisión de voz. El reto al principio fue integrar una red diseñada para datos con la transferencia de voz. Gracias a la evolución de los estándares y los compresores de audio se ha podido mejorar esto.

Algunas de las ventajas para escoger la solución VoIP son: Que reduce el costo de instalación ya que se usa el mismo cableado estructurado, otra es que al ser orientado a paquetes no hay una conexión constante solo cuando se lo necesita esto mejora la eficiencia del uso del medio de transmisión[REF.1].

1.1.2 Arquitectura VoIP

Una solución de VoIP puede estar implementada sobre algunas variedades de tipos de redes (normalmente redes LAN). Un Terminal VoIP puede ser tradicionalmente una PC equipado con periféricos de audio (parlantes y micrófonos), algunas redes son implementadas con equipos especiales como terminales VoIP. El

protocolo de Internet (IP) opera sobre la capa de red[3] sobre cualquier tecnología de red. El protocolo de usuario de datagrama (UDP) opera en la capa de transporte el cual permite las comunicaciones de extremo a extremo. El protocolo UDP de por sí no es adecuado para las necesidades de transportar audio en tiempo real. Por esa razón VoIP utiliza dos tipos de protocolos: el protocolo de transporte en tiempo real (RTP) y el protocolo de control de transporte en tiempo real. Además de esto, la capa de aplicación implementa un codec que es usado por los terminales VoIP (ej. G.711, G721, G728 etc.). Además la capa de aplicación implementa protocolos para establecer controlar y terminar las llamadas VoIP (ej. H.323, Session Initiation Protocol). [REF.2]

1.1.3 Requerimientos de Calidad

Al referirse a calidad de voz hay muchos problemas para definir cuándo es aceptable la legibilidad e inteligibilidad de la voz que llega a su destino. Se pude definir algunos parámetros como: la claridad de la voz, el retardo de punta a punta, retardo en la codificación y decodificación (codecs), el retardo producido por la red, el retardo que hay entre uno y otro paquete (jitter), el retardo

[3] Capa de Internet en el modelo de capas TCP/IP. Esta corresponde a la capa de red del modelo OSI.

de paquetización, la variación de retardo y la pérdida de paquetes. [REF.1]

1.1.4 Componentes de una red VoIP

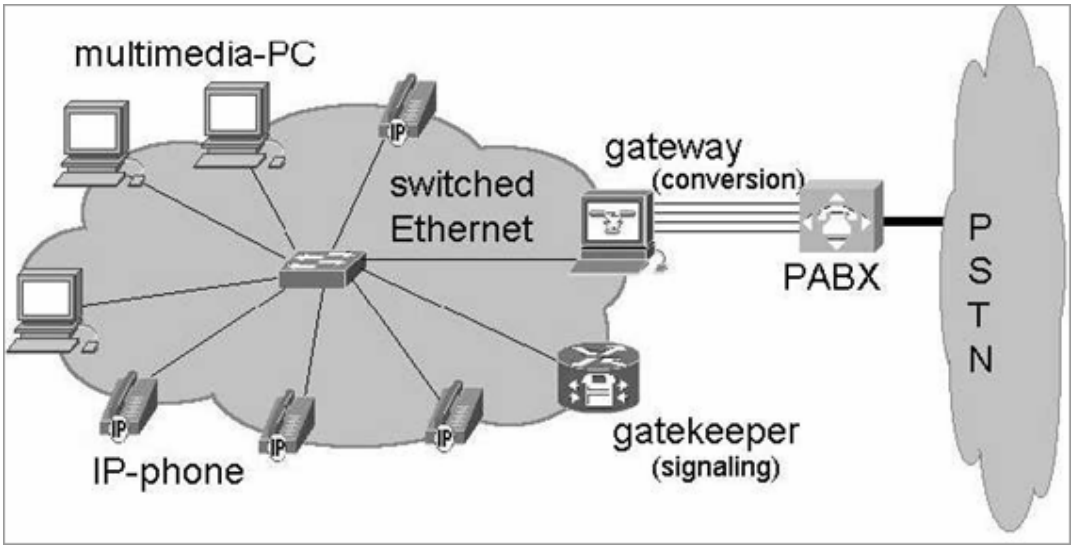


Figura 1-1. Componentes básicos de una red VoIP [REF.1]

En general una red VoIP esta compuesta por tres tipos de componentes: La estación final o Terminal VoIP, Gateways o puertas de enlaces, un Gatekeeper que es el que coordina las llamadas y se encarga de establecerlas. [REF.1]

1.2. Protocolos VoIP

La mayoría de los protocolos de señalización corren sobre TCP.

Esto es una ventaja ya que permite una transferencia confiable de datos.

La transferencia de paquetes en tiempo real es realizada sobre UDP, el

cual no provee una retransmisión de los paquetes perdidos, ya que a la hora de transmitir audio en tiempo real únicamente nos interesa el último paquete que llegó.

Muchos protocolos han surgido para la transmisión de voz sobre IP, pero se abordará los dos más utilizados o conocidos que son H.323 y SIP[REF.3].

1.2.1 Protocolo H.323

1.2.1.1 General

H.323 es un estándar de comunicaciones para una gran gama de protocolos fue desarrollado por la ITU a finales de 1996. Su crecimiento se debió al aumento de la comunicación multimedia en redes de área local (LAN). Es una expansión de la tecnología tradicional H.320 pero optimizada para Internet. H.323 provee de especificaciones técnicas para la transmisión de voz en redes LAN, en las que se asume que no hay calidad de servicio (QoS).

La mayor ventaja del estándar H.323 es que fue diseñado desde el principio para incluir Voz sobre IP y la telefonía sobre IP, así como comunicaciones de datos que implican redes conmutadas por paquetes. Estas redes incluyen las de tipo IP como Internet, las de Intercambio de paquetes (IPX) y redes de área amplia (WAN). H.323 es ampliamente soportado por muchos fabricantes comerciales.

El estándar H.323 define una gran cantidad de información acerca de las propiedades y componentes que interactúan en el ambiente H.323. Esto hace que muchas veces que su configuración no sea tan sencilla.

H.323 propone una arquitectura que consta de cuatro componentes lógicos: Terminales, Gateways, Gatekeepers y Unidades de Control Multipunto (MCUs).[REF.3]

1.2.1.2 Arquitectura

Terminales.

Son los clientes finales ya sean equipos personales o dispositivos independientes. Son los extremos de las líneas de comunicación.

Todos los terminales H.323 deben soportar H.245, H.225, Q.931, RAS (Registration Admission Status) y el protocolo de transporte en tiempo real (RTP). H.245 es usado para el control del uso del canal. RTP es usado como medio de transporte para llevar el tráfico de voz. RAS es usado por el terminal para interactuar con el Gatekeeper. [REF.4]

Gatekeepers.

Estos son una parte muy importante dentro de la arquitectura H.323. Son los cerebros de la red, que proporcionan servicios como direccionamiento, identificación, autorización y administración del ancho de banda. [REF.4]

Gateways.

Los Gateways o compuertas sirven como traductores cuando se interconectan redes distintas (por ejemplo hacia redes H.324). [REF.4]

Unidad de Control Multipunto.

Permite las conferencias entre varios sitios, o el enlace entre más de dos sitios a la vez (algo muy similar a las conferencias telefónicas). [REF.4]

1.2.1.3 Pila

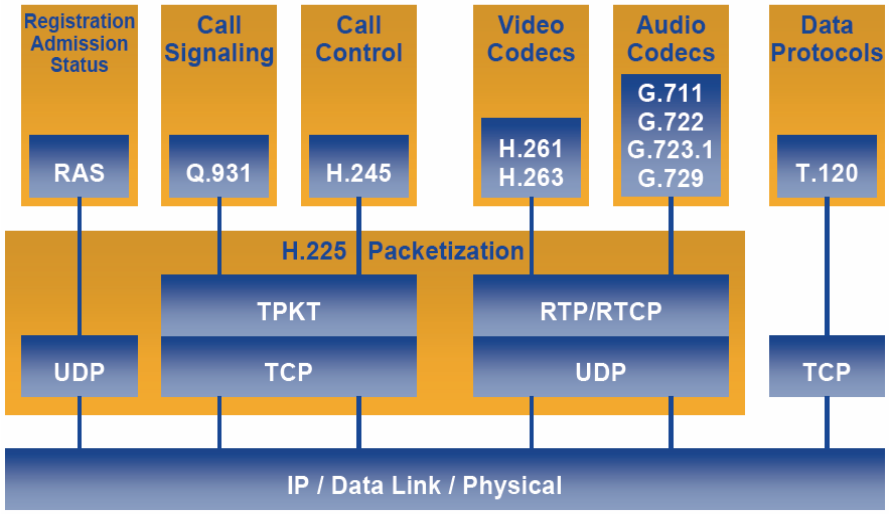


Figura 1-2. Pila del Protocolo H.323 [REF.5]

RAS (Registration Admission Status).

Este canal provee comunicación entre un Terminal y el Gatekeeper. [REF.6]

Call Signaling.

Este canal lleva información de las llamadas de control y servicio suplementarios de control como el protocolo Q.931 (usado sobre canales que son especificados en el protocolo H.225).

Cuando la comunicación es establecida el protocolo Q.931 envía la dirección por canales establecidos en los canales de control H.245. [REF.6]

H.245 (Call Control).

Este canal envía en su información mensajes del protocolo H.245 para control de medios con capacidad de ayuda de intercambio. Una vez establecida la llamada, los participantes intercambian las capacidades para la transferencia de voz y video y de cómo va ser hecho el control. [REF.6]

Audio / Video Codecs.

Los codecs de audio y video determinan qué tipo de codecs va a ser usado en la transmisión de los datos. Estos codecs viajan sobre el protocolo RTP/RTCP que está en el protocolo UDP. [REF.6]

Data Protocol T.120.

Este protocolo es usado para compartir y transferir imágenes y datos, para chat en texto. [REF.6]

1.2.1.4 Flujo de Mensajes

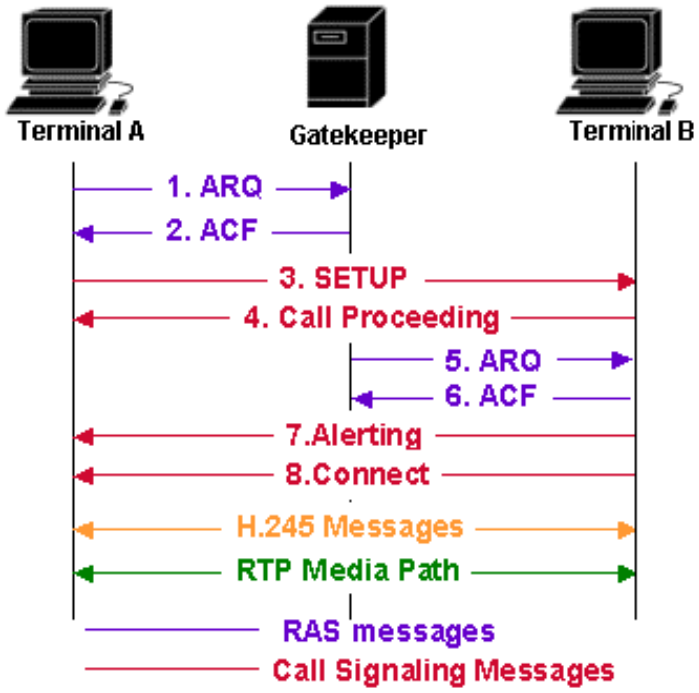


Figura 1-3. Flujo de mensajes [REF.3]

El protocolo H.323 define algunos protocolos para la transferencia entre terminales, gateways y gatekeepers. Antes de establecer la conexión para el envío de voz se establecen una serie de pasos. La siguiente explicación es para establecer la conexión entre dos terminales:

1. El Gatekeeper realiza la autentificación del Terminal (H.245-RAS).

2. Señalizando la llamada ruteada entre los terminales a través del gatekeeper (H.245-RAS y H.225-Q.931).
3. Inicialización de las comunicaciones y la capacidad de intercambio (H.245).
4. Establecimiento de la comunicaron de audio (abrir canal lógico) (H.245).
5. Transmisión del audio (RTP/RTCP).

En la Figura 3 se muestra el flujo de llamada entre dos terminales H.323. Ambos terminales están registrados previamente en el gatekeeper, el terminal A inicia la llamada al gatekeeper (RAS).

El gatekeeper provee de información al Terminal A para poder contactar al Terminal B. El Terminal A envía un mensaje de SETUP al Terminal B y el Terminal B responde con un mensaje de “procesando la llamada”, y al mismo tiempo se contacta con el gatekeeper para los permisos. El Terminal B envía mensajes de alerta y de conexión. Luego el Terminal A y el Terminal B intercambian mensajes H.245 para determinar el rol maestro-esclavo, capacidades del terminal y canales lógicos abiertos. Y por último los dos terminales establecen las rutas RTP.

El protocolo H.323 es bien conocido por su muy compleja señalización, alta latencia al establecer la llamada y dificultades para ser implementado. [REF.4]

1.2.1.5 Tipo de Seguridad

El protocolo H.323 define un estándar como mecanismo de facilitar la negociación de forma segura a través del protocolo H.235. Otro tipo de seguridad es SSL en la capa de transporte.

Protocolo H.235.

Es el estándar de seguridad recomendado para el protocolo H.323. H.235 es aplicable tanto en conferencias punto a punto como multipunto, para cualquier Terminal que utilice el protocolo de control H.245.

El alcance del protocolo H.235 es proveer autentificación, privacidad e integridad para sistemas basados en H.323. H.235 provee medios para que una persona pueda ser identificada.

Los perfiles de seguridad incluyen:

- Un password basado en los perfiles de seguridad.

- Certificados digitales y una dependiente infraestructura de clave pública.
- Una combinación de ambos.

H.235 recomienda mensajes, procedimientos, estructuras y algoritmos para seguridad concerniente a la señalización, control y comunicación bajo arquitecturas H.323.

- La señalización de llamada puede ser asegurada usando TLS[4] o IPSec o la seguridad de algún puerto bien conocido.
- Los usuarios pueden ser autentificados durante la conexión inicial de la llamada, en el proceso de asegurar el canal H.245 e intercambiando certificados en el canal H.245.
- Las capacidades de cifrado de un canal de los medios son determinadas por extensiones al mecanismo existente de la capacidad de la negociación.

---

[4] TLS.- “Transport Layer Security”. es un protocolo que asegura aislamiento entre aplicaciones de comunicación y sus usuarios. Cuando un servidor y un cliente se comunican, TLS se asegura de que ningunos terceros puedan escuchar o tratar de forzar con cualquier mensaje.

- El material principal de distribución es protegido por operaciones del canal H.245 como canal privado o por protección especifica usando un certificado de intercambio.[REF.3]

1.2.2 Protocolo SIP

2.2.1 General

El protocolo SIP (Session Initiation Protocol) es basado en el condigo ASCII y protocolos peer-to-peer. SIP fue desarrollado por IEFT y es un derivado del protocolo HTTP (Hyper-Text Transfer Protocol) y el protocolo SMTP (Simple Mail Transfer Protocol). El primer borrador apareció en febrero de 1996 (SIP v1) y el segundo en diciembre de ese mismo año (SIP v2). En Febrero de 1999, SIP se convierte en estándar, publicado como RFC 2543. En junio de 2002 es publicada una nueva versión (RFC3261) que reemplaza a la RFC2543. SIP no depende del protocolo TCP para su confiabilidad. Esto permite crear soluciones más óptimas que se ajustan a las necesidades de VoIP. Uno de los principales propósitos de SIP es la iniciación, modificación y terminación de sesiones entre dos o más sistemas finales en Internet [REF.7].

1.2.2.2 Arquitectura

En el protocolo SIP se puede encontrar cuatro componentes básicos: User Agents (UA), Registrars, Proxy y Redirect Servers.

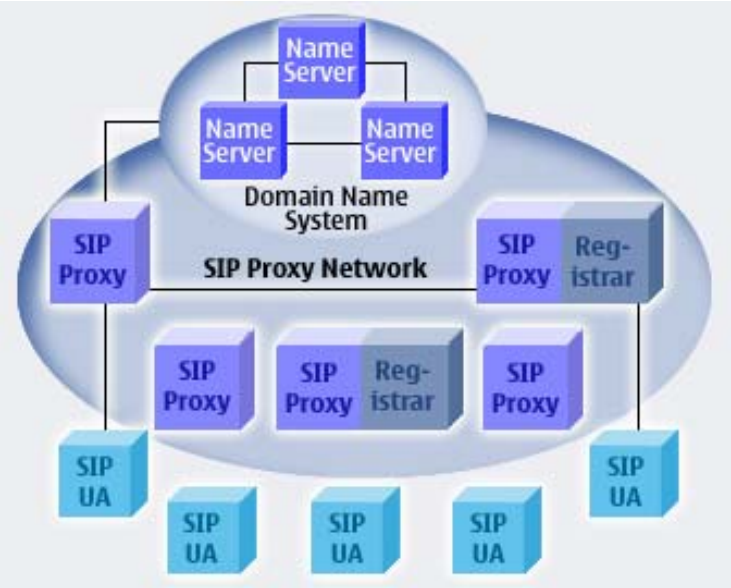


Figura 1-4. Flujo de mensajes [REF.8]

User Agent.

El agente de usuario o User Agent consiste en dos entidades que son el user agent cliente (UAC) y el user agent server (UAS). El UAC es la aplicación que inicializa y envía las peticiones SIP, y es el destino final de las llamadas. El UAS es el encargado de recibir, responder las peticiones de los clientes, aceptar, redireccionar y rechazar llamadas.

Registrars.

El Registrar o secretario mantiene el registro dentro de un dominio de red asignado. Este normalmente está ubicado cerca de un Proxy.

Servidor Proxy.

Estos servidores son los routers de la capa de aplicación que se encargan de enviar las peticiones SIP hacia su destino.

Redirect Server.

Al contrario del Proxy el redirect server no rutea las peticiones SIP. El redirect server mapea la dirección destino de la petición SIP recibida en una o más nuevas direcciones y retorna estas nuevas direcciones al cliente.

Se puede usar a veces un servidor de localización que ayude a los Proxy a obtener información para poder rutear las peticiones[REF.7]

1.2.2.3 Pila

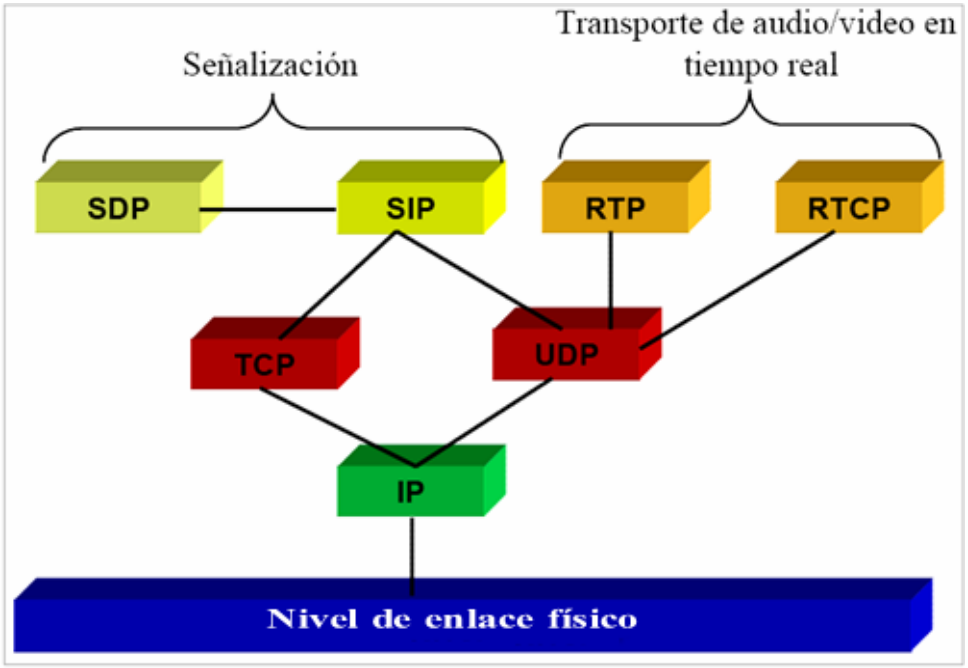


Figura 1-5. Pila del protocolo SIP [REF.10]

SIP puede trabajar en protocolo TCP y UDP. Tiene el manejo de codecs y los protocolos RTP y RTCP que son los protocolos de envío de la voz en tiempo real y de control.

SDP es utilizado para describir las capacidades multimedia de los participantes en la llamada y negociar un conjunto común de capacidades multimedia a utilizar.

1.2.2.4 Flujo de Mensajes

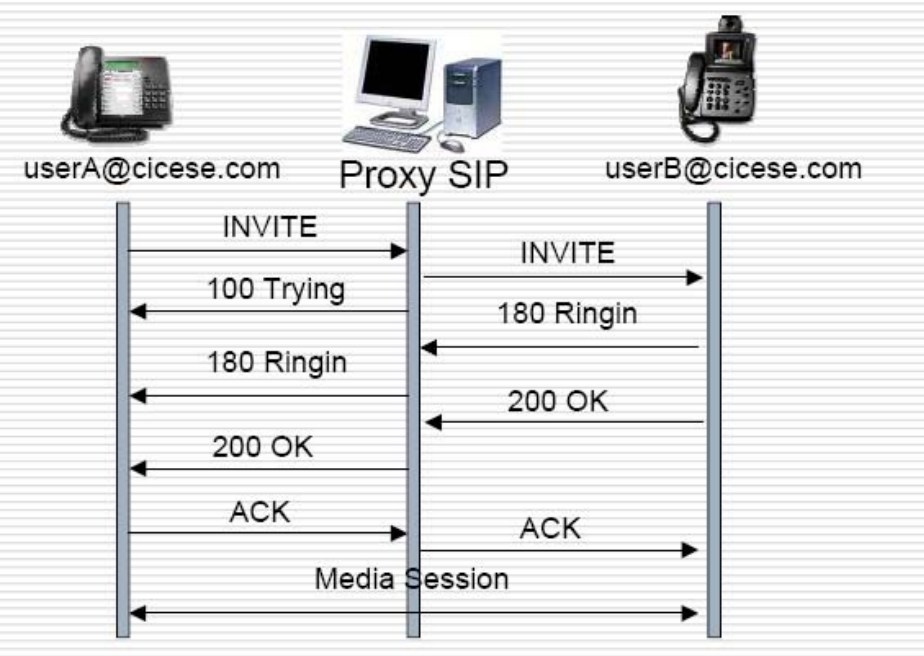


Figura 1-6. Flujo de mensajes del protocolo SIP [REF.3]

Establecida la comunicación, el flujo de mensajes se lo puede definir por seis pasos:

1. Registrando, iniciando y localizando al usuario.
2. Determinación de los medios para utilizar.
3. Determinación de la disponibilidad de las partes que van a intervenir en la llamada (aceptar o rechazar).
4. Configuración de llamada.
5. Modificación o manejo de la llamada.
6. Terminación de la llamada.

El protocolo SIP define métodos para establecer la llamada:

- **INVITE.-** Inicia una llamada invitando al usuario a participar en una sesión.
- **ACK.-** Respuesta que el cliente envía confirmando que recibió la invitación.
- **BYE.-** Indica la terminación de una llamada.
- **CANCEL.-** Cancela las peticiones pendientes.
- **REGISTER.-** Registra los Agentes Usuarios (UAC)
- **OPTION.-** Usado para preguntar la capacidad de un servidor.
- **INFO.-** Usado para llevar información fuera de banda, como los dígitos DTMF[5].[REF.3]

1.2.2.5 Tipo de Seguridad

El protocolo SIP ofrece autentificación para el que realiza y recibe la llamada vía mecanismos HTTP. La autentificación y el cifrado seguro son soportados por SSL/TLS.

---

[5] DTMF (Dual Tone Multi-Frequencies), sistema usado por los tonos de teléfonos fácilmente identificado por un microprocesador.

También soporta mecanismos de seguridad como SSH o S-HTTP, y claves para el cifrado de medios de trasporte a través de SDP[6].

SSL simétrica y asimétrica son también soportados.

El protocolo SIP define la autentificación de cifrado end-to-end usando PGP[7] o S/MIME[8]. [REF.13]

1.2.3 Diferencias entre SIP y H.323

- Entre las diferencias que podemos encontrar tenemos que el protocolo H.323 especifica servicios mientras que el protocolo SIP es un protocolo de señalización para dar base a servicios.
- H.323 engloba un amplio conjunto de protocolos de implementación obligatoria.
- La negociación de capacidades es más completa y compleja en H.323.

---

[6] SDP (Service Discovery Protocol) permite a las aplicaciones cliente descubrir la existencia de diversos servicios proporcionados por uno o varios servidores de aplicaciones.

[7] PGP (Pretty Good Privacy), programa para proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública.

[8] S/MIME (Security MIME), protocolo de seguridad para correos electrónicos usa certificados digitales.

- H.323 define mecanismos de gestión y administración de la red.
- SIP está integrado en la infraestructura Web y proporciona servicios de mensajería instantánea.
- SIP tiene mejores mecanismos de detección de bucles, espirales y otros errores de configuración de la red.
- El 3gpp[9] ha adoptado SIP como protocolo de señalización.
- Desde las primeras versiones, el inicio de llamadas es más rápido con SIP.[REF.14]

Tabla 1-1. Diferencias entre H.323 y SIP [REF.14]

	H.323	SIP
Codificación	Binaria (ASN.1)	Textual (SigComp)
Formatos	Series G.XXX y H.XXX, MPEG, GSM	Tipos MIME – IANA
Ampliabilidad	Campos reservados	Métodos de cabeceras
Autentificación	H.235 (puede usar TLS)	Análogo a HTTP
Localización	Gatekeeper (puede usar DNS)	DNS
Transporte	TCP, UDP	TCP, UDP, SCTP, DCCP

[9] 3gpp (3rd Generation Partnership), estándar destinado a distribuir contenidos multimedia en redes inalámbricas.

1.2.4 Fallas encontradas

A pesar de las advertencias de que VoIP es vulnerable a un conjunto de ataques inherentes a sus características, las mayores amenazas recaen en debilidades de seguridad propias de las redes TCP/IP: gusanos, virus y el uso de vulnerabilidades sobre la tecnología, pueden congestionar o colapsar las redes que sustentan VoIP. Por ejemplo, algunas IP PBX están basadas en Windows o Unix, por lo cual toda brecha de seguridad en estos sistemas operativos afecta directamente al servicio.[REF.15]

Las fallas que comúnmente afectan a VoIP son:

- Continuidad del servicio
- Confidencialidad de la información
- Forjamiento de la identidad del usuario

1.2.5 Tipos de Seguridad

Uno de los problemas más comunes cuando nos referimos a la seguridad de VoIP es tratar esta tecnología como si fuera un tipo de aplicación común dentro de las redes IP. VoIP tiene otras demandas de seguridad, para VoIP es de alta prioridad el tiempo real y la calidad del servicio que se brinda.[REF.17].

La siguiente lista son reglas que permiten establecer un tipo de seguridad VoIP.

1. Actualizar los parches de seguridad.

   Hay que actualizar los programas expuestos a la red para evitar riesgos innecesarios. Algunos de los ataques de red pueden ser evitados actualizando los parches de seguridad.

2. Instalar un buen Antivirus.

   Una de los mejores tipos de seguridad es un buen antivirus y tenerlo actualizado constantemente. Debido al crecimiento de virus y gusanos. Una de las razones por las cuales es combinar un buen antivirus con VoIP es que es que los sistemas de antivirus protegen los componentes VoIP de infecciones de computadoras que están vulnerables en la red.

3. Sistemas de detección y prevención de intrusos.

   Usar un sistema de detección y prevención de intrusos es una técnica que permite proteger contra los ataques presentes en la capa de aplicación y red del modelo OSI.

   Estos sistemas incorporan técnicas como protocolos de detección de anomalías, reconocimientos de ataques, detección de puertas traseras y otros.

4. Instalar Gateways de capa de aplicación (ALGs) entre zonas seguras y no-seguras.

   Estos Gateways son diseñados específicamente para manejar demanda de aplicaciones como aplicaciones VoIP. Pueden prevenir contra ataque maliciosos de otros sistemas.

5. Autentificación, Autorización e IPSec.

   Se utiliza autentificaron y autorización para los protocolos VoIP basados en textos (SIP). Que son muy vulnerables a ataques en la red. IPSec provee de una capa adicional de seguridad en la capa de red, permitiendo encriptar y autentificar todos los paquetes.

6. Utilizar VPNs (Virtual Private Networks)

   Al usar VPNs reducimos el riesgo de que las conversaciones puedan ser escuchadas (aunque el proceso de encriptación y desencriptación aumenta el consumo de ancho de banda e incrementa la latencia) Por esto es aconsejable hacer VPN segmentado, es decir seleccionar las zonas por las que viajan los paquetes en las cuales no es segura su transmisión y ahí aplicar VPN con sus protocolos de seguridad.

7. Usar VLANs (Virtual LANs)

   Ayuda a priorizar el tráfico de voz, segmentando el tráfico de datos y voz. Resultando en una baja latencia y mejor calidad.

8. Proteger contra inundaciones UDP

   Este es un ataque en la red que ocurre cuando un paquete UDP es enviado con la intención de hacer caer los sistemas. Una solución es instalar Firewalls que tengan la opción de proteger contra estos ataques.[REF.17][REF.16].

1.3. Tecnología Inalámbrica

La tecnología inalámbrica ha ido en aumento debido a debido al notable aumento de dispositivos móviles que cada vez requieren más demanda para estar conectados entre sí como por ejemplo: las laptops y PDA's (personal digital assistants). [REF.3]

1.3.1 Estándares 802.11x

Los Estándares 802.11x son desarrollados por el mismo instituto de Ingenieros Eléctricos y Electrónica (IEEE). El numero 802 salio del proyecto 802 que llamado así por el año y el mes en que empezó: Febrero de 1980. La extensión ".11x" define los estándares para las redes inalámbricas[REF.21]

- 802.11- Es el estándar para redes inalámbricas con línea de vista.
- 802.11a - Es el estándar superior al 802.11b, pues permite velocidades teóricas máximas de hasta 54Mbps, apoyándose en la banda de 5GHz. Elimina también el problema de las interferencias múltiples que existen en la banda de los 2.4GHz (hornos microondas, teléfonos inalámbricos, BlueTooth).
- 802.11b – Extensión de 802.11 para proporcionar 11Mbps usando DSSS[10]. También conocida como Wi-Fi (Wireless Fidelity) Es el estándar más utilizado en comunicaciones inalámbricas.
- 802.11e – Estándar encargado de diferenciar entre video-voz-datos.
- 802.11g – Utiliza la banda de 2,4GHz, pero permite transmitir sobre ella a la velocidad de 54Mbps.
- 802.11i- Conjunto de referencias en el que se apoyara el resto de los estándares. El 802.11i supone una solución al problema de autentificación al nivel de la capa de acceso al medio. [REF.21]

---

[10] DSSS es una técnica de la modulación donde la señal transmitida toma más ancho de banda que la señal de información que se está modulando. La corriente de la información que se transmitirá se divide en pedazos pequeños, que se asigna a través de un canal de frecuencia a través del espectro.

1.3.2 Seguridad de una Red Inalámbrica

La seguridad en redes inalámbricas es muy limitada, ya que la capa dos del modelo OSI en este caso es el aire y resulta complicado el tener una sólida y completa seguridad. Sin embargo, se puede enfocar el tipo de seguridad dependiendo del uso que se le va a dar a la tecnología inalámbrica. Por ejemplo si lo usamos con una conexión de Internet para navegar por páginas Web, no es de gran prioridad el tener que encriptar los paquetes enviados. Pero si lo usamos para hacer compras por Internet entonces la privacidad de los paquetes enviados especialmente a la hora de insertar el número de la tarjeta de crédito tiene una prioridad muy alta.

El tipo de seguridad que se desea implementar dependerá del tipo uso que se de a la conexión inalámbrica. [REF.22]

1.3.2.1. WEP

El estándar 802.11 provee algunos mecanismos de seguridad. Dentro de esos encontramos al protocolo WEP (Wired Equivalent Privacy). Este protocolo se basa en el algoritmo RC4 de RSA Data Security para cifrar las transmisiones realizadas a través del aire. [REF.22]

1.3.2.2. RADIUS

RADIUS (Remote Access Dial-up User Service), es un estándar usado para proteger el acceso a las redes inalámbricas. Utiliza un esquema de usuario y contraseña que valida los usuarios en la red. Este estándar no modifica o encripta los datos. Si un usuario quiere acceder algún servicio de la red, se solicita un usuario y una contraseña. [REF.11]

1.3.2.3. SSL

SSL (Secure Sockets Layer) es un protocolo usado en comunicaciones basadas en Web sobre Internet. Se basa en el uso de encriptación y autentificaron para mantener las comunicaciones privadas entre dos dispositivos.

SSL hace uso de la criptografía y de los certificados digitales. Los Certificados Digitales contienen la identificación del servidor, su clave pública y la fecha de validez del certificado. SSL utiliza certificados de 40 bits (criptografía simple) o certificados de 128 bits (criptografía robusta) y otros tipos. [REF.12]

1.3.3 Vulnerabilidades de VoIP

En VoIP, al utilizar la tecnología de paquetes y circuitos, se presentan desafíos en la transmisión de voz sobre redes inalámbricas. VoIP transporta los paquetes en una red conmutadas, por paquetes a través del protocolo de Internet. Esto hace que los hackers puedan usar herramientas como sniffers u otras herramientas hackers para poder identificar, modificar y almacenar el tráfico que atraviesa la red. Un hacker puede romper la secuencia de datos de una trama VoIP y llegar a tener acceso a mucho más que llamadas. El escuchar conversaciones es algo que preocupa a las empresas y organizaciones, más aún teniendo en cuenta las desventajas de seguridad que ofrecen las redes IP. [REF.1]

1.4. Seguridad VoIP

1.4.1 Requerimientos de Seguridad

Ya que son bien conocidas las vulnerabilidades de las redes IP sobre las que se envía los paquetes de voz, hay algunas recomendaciones o requerimientos de seguridad a la hora de implementar VoIP:

1. Protección de la privacidad de la conversación de la llamada
2. Autentificación de las entidades finales de la llamada

3. Protección contra el uso erróneo de los recursos de la red
4. Asegurar la facturación correcta por el proveedor de servicio, y protección de la información de la facturación contra el acceso no autorizado.
5. Protección del comportamiento del llamador o de la información estadística contra el acceso no autorizado.
6. Protección de los servidores de la red y los terminales contra amenazas bien conocidas tales como "negación del servicio" y "ataque del hombre en el medio".

Aunque no puede haber un sistema completamente seguro, sí hay que tomar ciertas medidas para que las vulnerabilidades sean mínimas. [REF.3][REF.1]

1.4.2 Tipos de Protección

Hay que tener en cuenta que si no se tiene ningún tipo de protección contra posibles ataques, estos podrían manipular nuestros datos sin ningún tipo de restricción.

Hay varios tipos de protecciones que se deberían tener en cuenta a la hora de establecer protecciones contra ataques. A continuación se menciona los ataques más comunes y los tipos de protecciones para cada ataque.[REF.18]

IP Spoofing.

Este es un tipo ocurre cuando un atacante fuera de nuestra red pretende ser una computadora confiable.

Se puede lograr esto usando una IP válida dentro de nuestra red. El atacante se tiene que asegurar que la IP no esté siendo usada en ese momento. Normalmente estos ataques son para enviar o recolectar datos directamente del servidor. Una solución para estos ataques es tener buenas reglas en nuestro firewall. [REF.23]

Denial of Service.

Negación de Servicio o Denial of Service (DoS), es un incidente en el cual privan a un usuario o una organización de los servicios de un recurso que esperaban normalmente tener. Típicamente, la pérdida de servicio es la inhabilidad de un servicio de red particular, tal como E-mail, de estar disponible o la pérdida temporal de toda la conectividad y servicios de la red. Por ejemplo, un sitio Web alcanzado por millones de usuarios se puede forzar de vez en cuando a cesar temporalmente la operación. Un DoS puede también destruir la programación y archivos en un sistema informático. Aunque generalmente es intencional y malévolo, una negación de servicio puede suceder a veces accidentalmente.

Un ataque de negación de servicio no da lugar generalmente al hurto de la información o alguna otra pérdida de seguridad. Sin embargo, estos ataques pueden costar a la persona o compañía tiempo y dinero.

Para estos ataques lo mejor es tener bien configurado un firewall aunque hay algunas herramientas como anti-DoS bajo Linux que ayuda a configurar el firewall y nos dan logs (bitácoras) de los posibles ataques.[REF.23]

Man in the middle attacks (Ataques del hombre en el medio).

Man of the middle attacks es el término que se usa cuando un atacante puede leer, insertar y modificar los mensajes que hay entre dos clientes que participan de una conversación, sin que las dos partes atacadas tengan conocimiento del ataque. El atacante está capacitado para observar e interceptar los mensajes que están siendo enviados entre ambos clientes.

Una forma de evitar este ataque es usando el protocolo IPSec. En el protocolo IPSec, el ataque de MITM es evitado teniendo cada extremo de la conexión llaves de autentificación. Esto quiere decir que la conexión en los extremos esta protegida a través de dichas llaves.[REF.23]

Una buena opción es usar SSL y VPNs.

1.4.3 IPSec

Protocolo IPSec (Internet Protocol Security), desarrollado por la IETF provee seguridad a redes que transmiten información que viaja desprotegida, como las redes de Internet. IPSec actúa en la capa de red, protegiendo y autentificando paquetes IP.

En general IPSec provee de los siguientes servicios de seguridad.

- Confiabilidad de datos.- Los paquetes enviados son cifrados antes de ser enviados a través de la red.
- Integridad de datos.- El que recibe los paquetes puede autentificar al que envía y asegurarse que el paquete no haya sido modificado.
- Autentificación de los datos de origen.- El que recibe los datos puede autentificar el origen de los paquetes IPSec enviados.
- Anti-replay.- El que recibe los paquetes IPSec puede detectar y rechazar paquetes retransmitidos.

Con IPSec los datos transmitidos cruzan las redes públicas sin miedo de ser observados.[REF.19]

CAPÍTULO 2

2.1. Modelo Analítico

Dentro del modelo analítico se proponen dos topologías bases que son las que podrían ayudar en su implementación, debido a las características de las redes inalámbricas. Dentro de la variedad de las topologías analizamos la topología tipo Estrella y Celda o Celular

2.1.1 Topologías

Topología tipo estrella

La topología tipo estrella tiene la principal característica que tiene un nodo principal el cual si llega a fallar la red deja de funcionar. La ventaja de esta topología es que si se daña otro nodo, la red sigue funcionando. Además la fácil capacidad de expansión la hace una de las redes mas usadas. Su principal desventaja es que al dañarse el nodo principal todos los nodos que están conectados no pueden comunicarse.[REF.24]

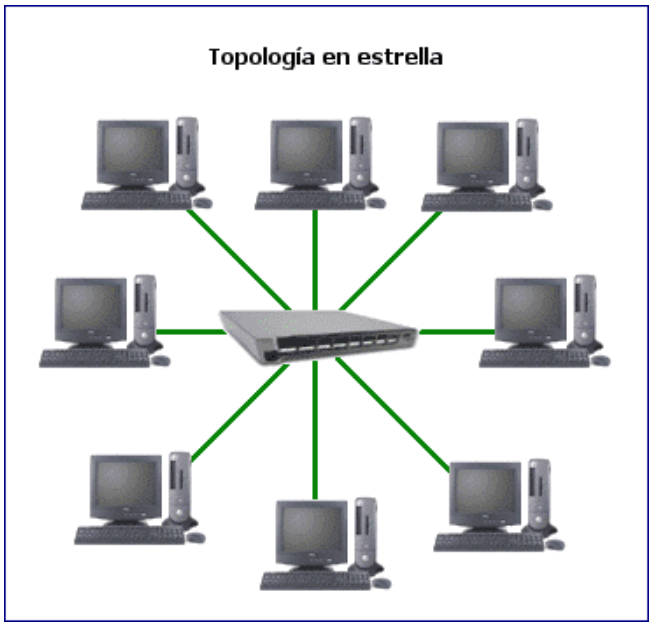


Figura 2-1. Topología tipo estrella [REF.24]

Topología celda o celular

La topología tipo celda o celular es usada para redes inalámbricas ya que está compuesta por áreas circulares o hexagonales, cada una de las cuales consta de un nodo individual. En este tipo de topología no hay enlaces físicos. Otra aplicación es para unir áreas geográficamente distantes. La principal ventaja es que no se necesita de mayor instalación. La desventaja es que la señal está por todos lados y esto causa fallas por ruido y problemas de seguridad.[REF.24]

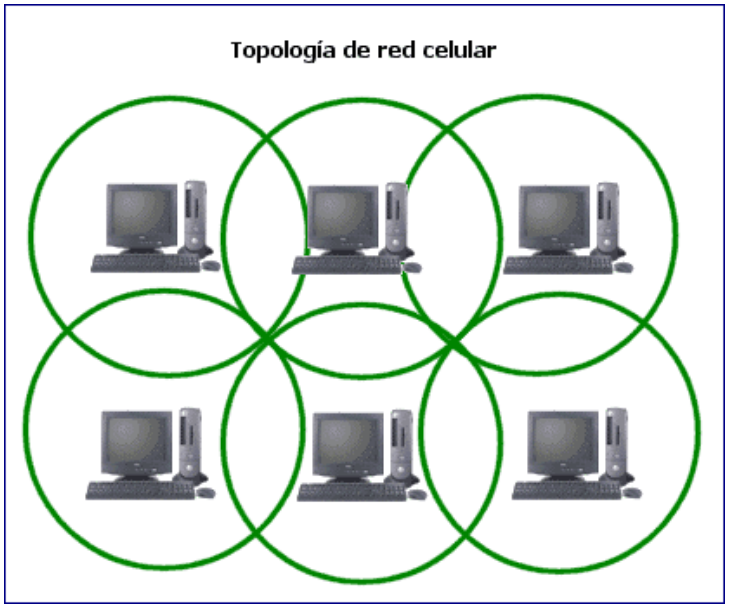


Figura 2-2. Topología de red celular [REF.24]

2.1.2 Red Inalámbrica

Una vez definidas las topologías que se van a utilizar para el análisis de los protocolos, se muestra a continuación el diseño de las redes inalámbricas para los protocolos SIP y H.323 respectivamente

Topología 1 SIP

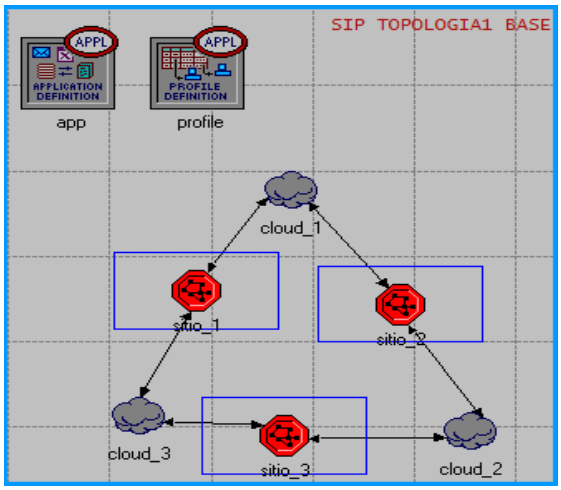


Figura 2-3. Diseño topología 1 con SIP

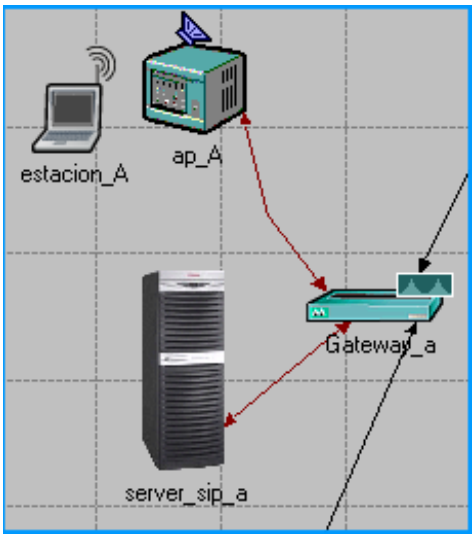


Figura 2-4. Interior del sitio_1 topología 1 SIP

En este diseño el manejo del flujo de paquetes está mejor balanceado. Las llamadas son las mismas para todos los diseños. Se realizan del sito 1 al sitio 2, del sitio 2 al sitio 3 y del sitio 3 al sitio 1. De esta manera todos son caller y callee a la vez. Todos realizan y reciben peticiones para negociar la llamada. El servidor Proxy SIP está ubicado en cada subred para ayudar a la negociación y agilitar el envió de paquetes.

Topología 1 H.323

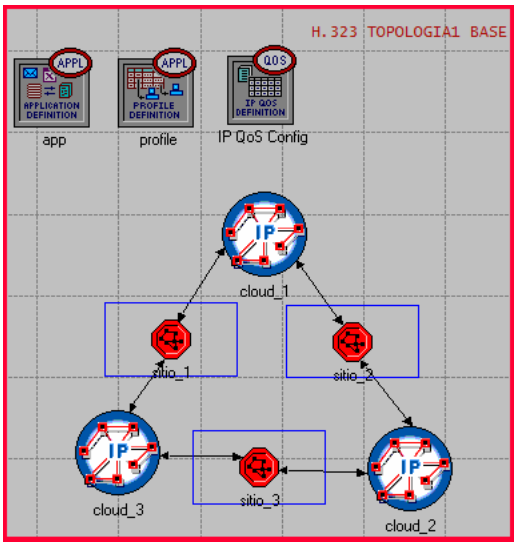


Figura 2-5. Diseño topología 1 con H.323

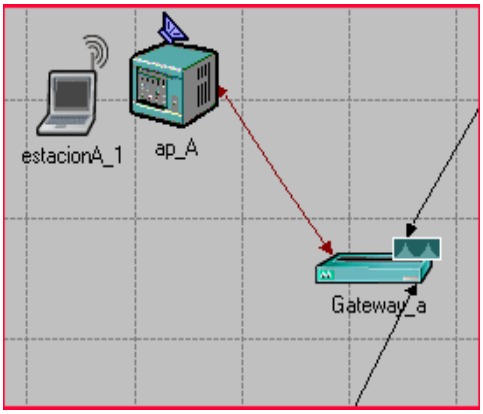


Figura 2-6. Interior del sitio 1 Topología 1 H.323

Para el protocolo H.323 este diseño hace que la negociación para cada cliente tome menos tiempo, debido a que no se concentran en un solo nodo el envió de los paquetes.

Topología 2 SIP

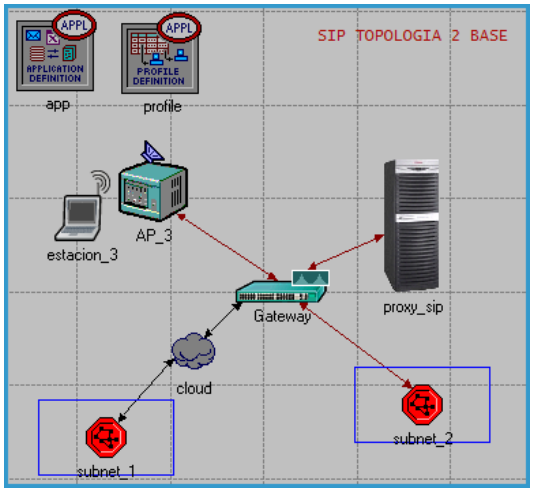


Figura 2-7. Diseño topología 2 con SIP

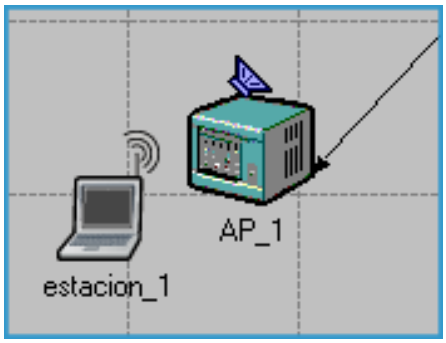


Figura 2-8. Interior subset_1 topología 2 SIP

En este diseño sólo existe un servidor Proxy y todos los paquetes tienen que pasar por un único gateway. El servidor está ubicado próximo al gateway, así se acelera las peticiones de todos los clientes.

Topología 2 H.323

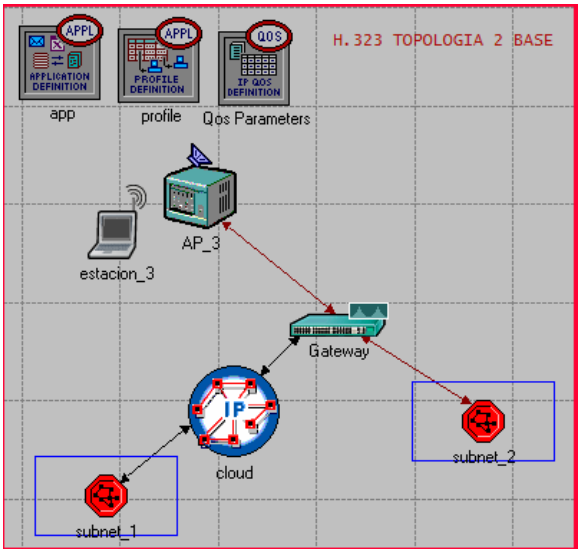


Figura 2-9. Diseño topología 2 con H.323

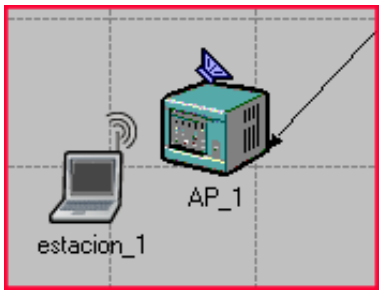


Figura 2-10. Interior subnet_1 topología 2 H.323

Este diseño hace que todos los mensajes de negociación estén limitados a la capacidad de un solo gateway.

2.1.3 Metodología

2.1.3.1 Parámetros a Evaluar

Se seleccionó de una lista de posibles parámetros que tienen mayor incidencia para determinar la calidad y aceptabilidad de la voz de un cliente a otro a través de una red inalámbrica. Estos parámetros se los recolectó después de un estudio donde se recomienda los que se menciona continuación.

2.1.3.2 Jitter (variación del rendimiento)

En voz sobre IP el jitter es la variación de tiempo que hay entre los paquetes que llegan a su destino, es decir el tiempo que hay entre cada paquete al momento de su arribo.

Esto es causado por la cogestión en la red y por rutas alternas a la hora de enviar paquetes. Se aconseja que el valor del jitter sea lo más bajo posible. Para corregir el efecto de un jitter elevado se puede implementar el jitter buffer que ayuda a compartir un área donde los paquetes de voz pueden ser colectados, mantenidos y enviados.[REF.20]

2.1.3.3 Delay (Demora)

Delay es la demora que hay entre la salida del paquete de voz hasta que llega a su destino, este parámetro esta sujeto directamente a la cogestión.[REF.20]

2.1.3.4 Load (Carga)

El load o la carga se refiere a la carga que tiene una red. Es decir, qué tanta información viaja a través de ella y cuántos paquetes puede manejar.[REF.25]

2.1.3.5 Tiempo de Señalización

Se define al tiempo de señalización al tiempo que se demora en establecer y autorizar el envío de paquetes de voz entre el que llama y el que va a recibir la llamada. Es decir, establecer y acordar todos los parámetros requeridos para la transmisión.

2.1.3.6 Envío y Recepción de Transferencia de Datos

Este parámetro se divide en dos: el tiempo de envió de los bits enviados (en segundos) y el tiempo de recepción de

los (bits en segundo). Este parámetro indica cual es el porcentaje de bits perdidos durante la llamada y qué tan confiable puede ser.

2.1.4 Parámetros a variar

Para poder evaluar y decidir que parámetros son los que tienen mayor incidencia. Los parámetros a evaluar son:

2.1.4.1 Codec

Codec es una abreviatura de Compresor-Descompresor. Se puede implementar por software, hardware o una combinación de ambas, los codecs codifican una trama de una señal de datos a ser transmitida. Para poder recuperar los datos, hay que decodificar los mismos.

La mayoría de los codecs provocan pérdidas de datos, esto es debido a que se busca tener el tamaño del paquete lo más pequeño posible. Algunos codecs aumentan el tamaño de la trama para evitar la pérdida de datos.

Los archivos multimedia contienen datos de audio, video y una referencia de cómo sincronizar el audio con el video. Estos tres flujos hay que tener en cuenta para almacenar o transmitir y deben ser almacenados juntos, esto es lo que

se conoce como formato de audio y video, mp3, mpg, avi, rm, etc. Algunos de estos formatos son combinaciones de varios codecs. [REF.14]

Tabla 2-1. Especificaciones de codecs [REF.27]

Codec	Speed (kbps)	Segment (bits)	Segments/s	Duration (ms)	Delay (ms)
G.711 (PCM)	64	8	8000	0.125	0.125
G.721 (ADPCM)	32	4	8000	0.125	0,125
G.723 (ADPCM)	24 – 40	3 – 5	8000	0.125	0.125
G.726 (ADPCM)	16 – 40	2 – 5	8000	0.125	0.125
G.727 (ADPCM)	16 – 64	2 –8	8000	0.125	0.125
G.729 (CS-ACELP)	8	80	100	10	15
G.728 (LD-CELP)	16	10	1600	0,625	0.625
G.723.1	6.3	189	33.33	30	37.5
G.723.1	5.3	159	33.33	30	37.5

2.1.4.2 Tipo de Señalización

Dentro de los parámetros a evaluar se encuentra el tipo de señalización.

Los tipos de señalización son:

Para el protocolo SIP, es “call setup”, para el protocolo H.323, se implementa el protocolo RSVP como protocolo de señalización.

2.1.4.3 Voice Frame per Packets (VFPP)

El Voice Frame per Packets es el número de paquetes o tramas que van a ser agrupados para ser codificados antes de ser enviados.

2.1.4.4 ToS

Type of Service (ToS), el tipo de servicio que va a ser implementado en el sistema VoIP. El ToS provee un indicador de los parámetros de la calidad de servicio que se desea. Estos parámetros son usados para definir la calidad de servicio a la hora de transmitir el datagrama a través de la red. Algunas redes no admiten paquetes a menos que tengan cierto tipo de servicio.

La cabecera del datagrama del protocolo de Internet (IP) contiene un campo de 8 bits que es el destinado para definir el ToS.

- Bits del 0 al 2: Precedencia
- Bit 3: 0 = Retardo Normal, 1 = Retardo Lento
- Bit 4: 0 = Rendimiento Normal, 1 Rendimiento Alto
- Bit 5: 0 = Confiabilidad Normal, 1 = Confiabilidad Alta
- Bits del 6 al 7: Reservados para usos futuros

El uso del retardo, rendimiento y confiabilidad pueden incrementar el costo del servicio.[REF.25]

2.1.4.5 QoS

Quality of Service (QoS), se refiere a la calidad de servicio a la hora de transmisión de datos mediante el uso de control y medición del rendimiento y errores. QoS se refiere a la habilidad de una red de proveer una mejor confiabilidad para seleccionar el trafico de la red sobre varias tecnologías incluyendo redes ruteadas por el protocolo IP.

Al principio el QoS no era tan indispensable ya que los datos que se enviaban no necesitaban que lleguen en tiempo real y los usuarios no percibían la latencia de los datos. Con la implementación de redes inalámbricas y el envió de paquetes multimedia el uso de QoS se ha vuelto indispensable.

La demanda de los usuarios en la percepción del tiempo en las aplicaciones de voz y video en entornos inalámbricos hacen que surjan requerimientos en las aplicaciones tradicionales como la tolerancia mínima de retardo en la entrega de los paquetes y la intolerancia de la perdida de paquetes el jitter. [REF.20]

2.1.4.6 Número de Nodos

El parámetro número de nodos se refiere a la cantidad de clientes que se van a ir agregando en la red lógica que se planteará más adelante. Este parámetro es muy importante ya que se a mayor número de nodos que soporte los protocolos, estos serán más escalables.

2.2. Tipos de Simuladores

Dentro de los tipos de simuladores que podemos encontrar los más recomendados para nuestro propósito son el OPNET y el NS2

2.2.1 OPNET vs NS2

NS2 es un simulador que permite configurar varios parámetros, y aunque es muy recomendado, la gran desventaja que se presenta a la hora de utilizar NS2 es lo complicado de su interfase y lo poco intuitivo para su manejo. OPNET es un simulador que fue desarrollado para poder simular y cubrir las mayores necesidades dentro de una red y por ver los problemas que se presentan o prevenir una mala configuración de una red. La mayor ventaja de OPNET es que es intuitiva su configuración. Su mayor desventaja es que permite configurar tantos parámetros que su configuración tiende a ser un poco tediosa, pero útil.

En este proyecto se usó la versión estudiantil de OPNET que es IT-GURU, el cual tiene algunas limitantes como el número

máximo de eventos (500000) y la falta de de módulos de red más avanzados. Ver el Apéndice C.

2.2.2 OPNET

2.2.2.1 Modelos

Modelo de la topología 1 tipo celda.

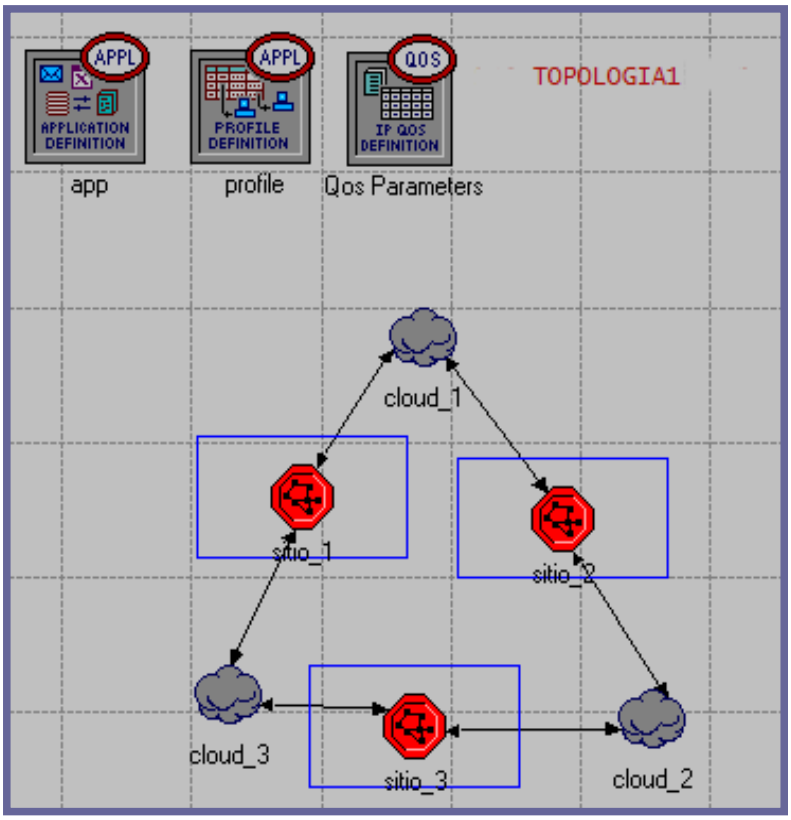


Figura 2-11. Modelo analítico topología 1

Modelo de la topología 2 tipo estrella.

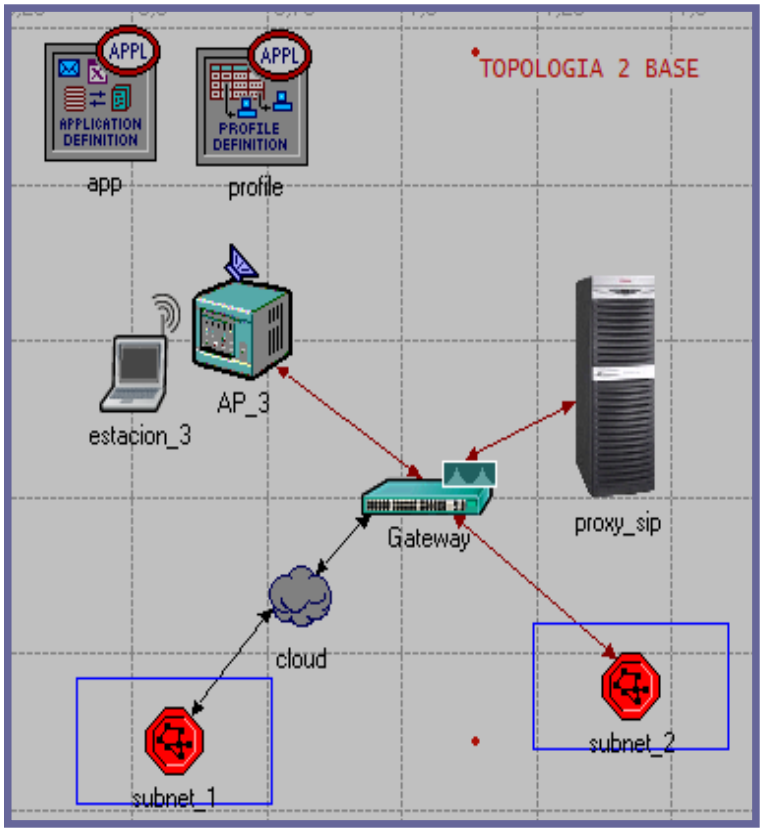


Figura 2-12. Modelo analítico topología 2

2.2.2.2 Datos de Entrada

Los datos de entrada son los rangos de valores que van a ser variados en la simulación.

Dentro de los datos de entrada hay un valor que no se va a variar es solo para evaluar el rendimiento con VPN y sin VPN. El valor introducido son de los algoritmos de

encriptación y de autentificación (DES-CBC[11] y HMAC-MD5[12] respectivamente). [REF.28][REF.29].

Tabla 2-2. Datos insertados en la simulación para evaluar

Nombre	Valor
Codec	*G.711 (PCM), G.729, G.723.1, GSM, G.726 (ADPCM), G.728 (LD-CELP), G.729 (CS-ACELP)*
VFPP	*1,2,3,7,10*
ToS	*Best Effort, Background, Standard, Excellent Effort, Streaming Multimedia, Interactive Voice, Reserved*
QoS	*FIFO, WFQ, Priority Queuing, Custom Queuing, MWRR, DWRR, MDRR*
Nodos	*3, 6, 12*
VPN	*0.0008 (sg)*

2.2.2.3 Datos de Salida

Los datos de salida vienen dados en segundos, bytes por segundos y paquetes por segundo.

[11] DES-CBC (Data Encryption Standard, DES) y Encadenado de bloques de cifras (Cipher block chaining, CBC), estándar de cifrado de datos usa un algoritmo de clave secreta utilizado para proporcionar confidencialidad.

[12] HMAC-MD5. HMAC es un algoritmo de clave secreta que proporciona seguridad e integridad. MD5 es una función hash que da como resultado un valor de 128bit.

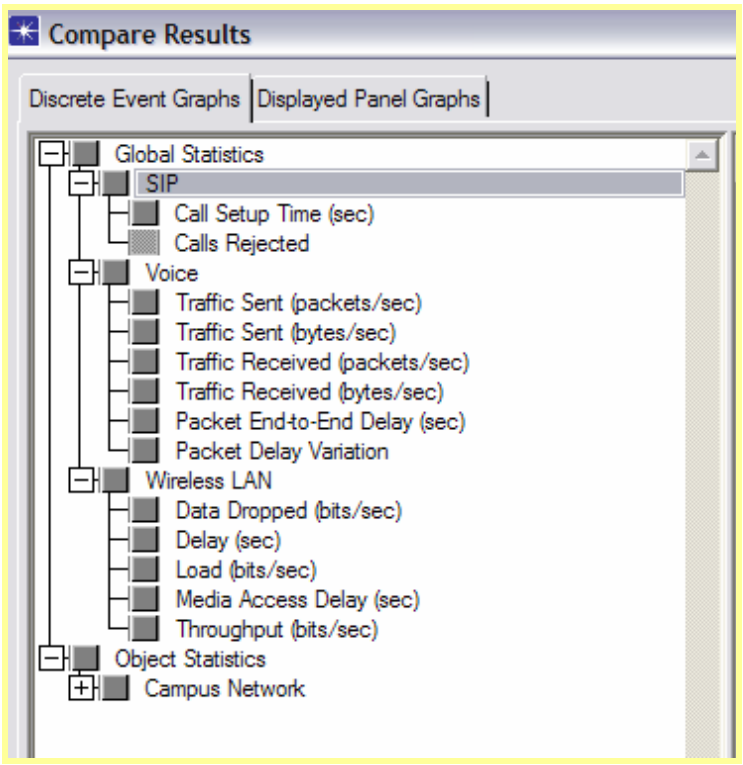


Figura 2-13. Ventana de selección de datos a mostrar

La Figura 18, muestra los diferentes tipos de datos que se pueden escoger para analizar. Se puede escoger resultados de forma individual para cada nodo o de forma general para toda la red.

2.2.3 Configuración del Modelo Analítico

Los nodos que intervienen en la simulación, ver en la sección A.1 del apéndice A.

La configuración de los protocolos SIP y H.323 para los diseños de los modelos de las topologías 1 y 2 son:

Protocolo SIP.

Los parámetros a configurar en la definición de aplicación del modelo de la topología tipo 1 son:

Tabla 2-3. Configuración de los parámetros de voz para SIP

Atributo	**Valor**
Silence Length (seconds)	Default
Talk Spurt Length (seconds)	Default
Symbolic Destination Name	Voice Destination
Encoder Écheme	G.711
Voice Frames per Packet	1
Type of Service	Best Effort (0)
RSVP Parameters	None
Traffic Mix (%)	All Discrete
Signaling	SIP

La configuración en los terminales finales que van a realizar las llamadas y recibirlas es:

Tabla 2-4. Configuración de los parámetros de voz en el cliente

Atributo	**Valor**
UAC Service	Enabled
Proxy Server Specification	(...)
Maximum Simultaneous Calls	Unlimited
Proxy Server Connect Timeout (seconds)	TCP Based

En el parámetro Proxy Server Specification hay que agregar cuál es el servidor Proxy con el cual se va a comunicar el cliente para realizar la llamada.

En el servidor Proxy SIP hay que habilitar la opción de que se pueda aceptar las peticiones SIP. Ver la sección D.1 del apéndice D.

Tabla 2-5. Habilitar el servidor Proxy

Atributo	Valor
Proxy Service	Enabled
Maximum Simultaneous Calls	Unlimited

Protocolo H.323.

Para el protocolo H.323 igual que para el protocolo SIP estas configuraciones se mantienen en los dos tipo de topologías, la configuración en el modelo del simulador OPNET en su versión estudiantil es:

Configuración de la Definición de la Aplicación.

Tabla 2-6. Configuración de los parámetros de voz para H.323

Atributo	Valor
Silence Length (seconds)	default
Talk Spurt Length (seconds)	default
Symbolic Destination Name	Voice Destination
Encoder Écheme	G.711
Voice Frames per Packet	1
Type of Service	Best Effort (0)
RSVP Parameters	(...)
Traffic Mix (%)	All Discrete
Signaling	None

La configuración del protocolo de reservación RSVP se configura por defecto. A esto se le agrega el tipo de calidad de servicio en los modelos donde se utiliza el protocolo H.323.

La configuración del cliente H.323 hay que tener en cuenta que hay que tener habilitado el tipo de señalización tanto en los clientes como en las interfaces de todo el recorrido hasta llegar al cliente que recibe la llamada, pasando por todos los nodos. Igualmente para el tipo de calidad de servicio. Ver la sección D.2 del apéndice D.

Tabla 2-7. Activación del protocolo RSVP en las interfaces de los nodos

Name	RSVP Status	Maximum Reservable BW	Maximum Bandwidth Per Flow	Subinterface Information
	Enabled	0,75	0,75	None

Tabla 2-8. Habilitar el estatus del protocolo RSVP

Atributo	**Valor**
RSVP Status	Enabled
Profile List	Default

IPSec VPN

La configuraron del protocolo IPSec tanto para el protocolo H.323 y SIP es una parte importante de la simulación. Aunque esta parte se la realiza al final de la simulaciones. Para simular este parámetro se escogieron los valores de encriptación y autentificación para insertarlos durante la simulación.[REF.28][REF.29]

2.3. Resultados

Los Resultados de los modelos analíticos en el simulador OPNET en su versión estudiantil son:

2.3.1 Codec

Topología 1

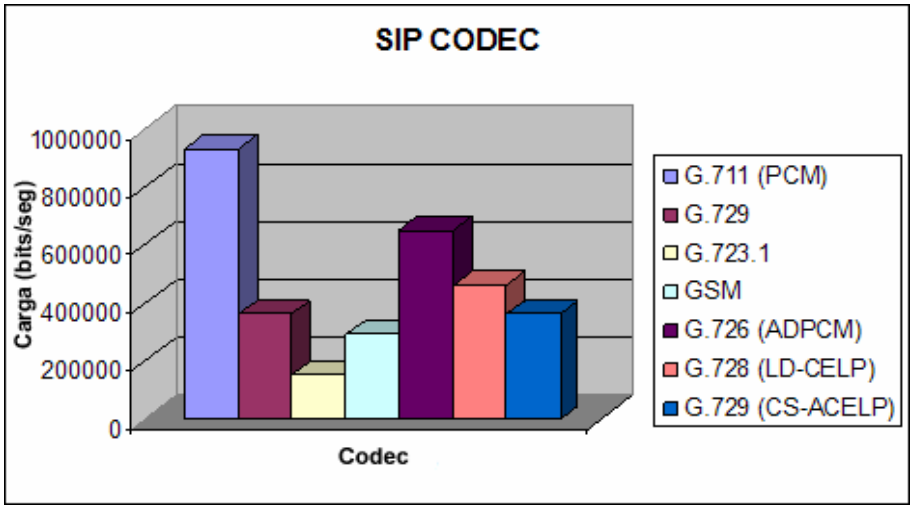


Figura 2-14. Diagrama codec-carga de SIP topología 1

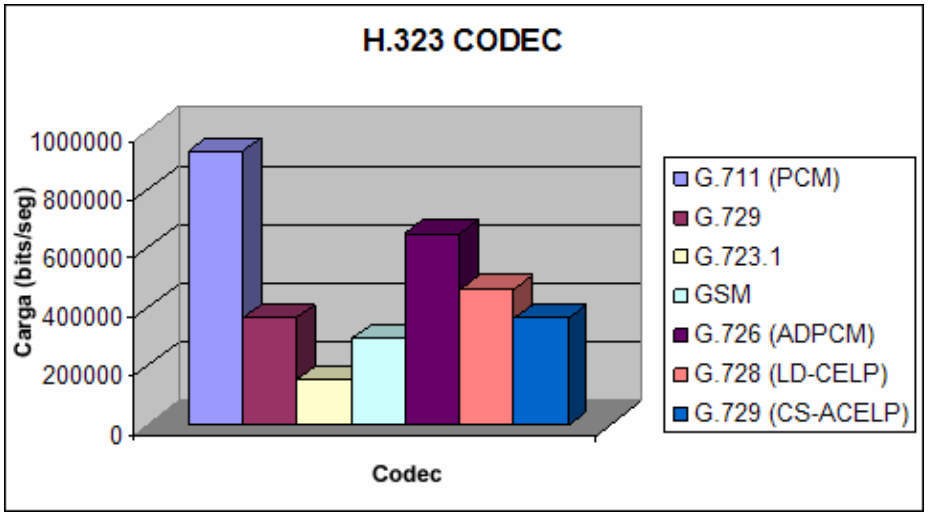


Figura 2-15. Diagrama codec-carga de H.323 topología 1

Para la topología 1, variando el codec tanto para el protocolo SIP como H.323 nos muestra la Figura 2-14 y 2-15 el codec más adecuado es el G.711 (PCM) ya que a pesar de que tiene una menor compresión, esto conlleva a una calidad de voz mejorada, lo cual es una característica deseada en implementaciones de VoIP [REF.27]. Se escoge este codec ya que se quiere una mejor calidad en la voz transmitida. Además, como se demuestra en las simulaciones posteriores y en las pruebas de campo, la sobrecarga incurrida con el uso de G.711 no satura la red. En caso de desearse sobrecargar menos la red (a un costo de calidad de voz reducida), se puede escoger otros de los codecs disponibles. Para un detalle de los resultados ver la sección B.1 y B.3 del apéndice B.

Topología 2

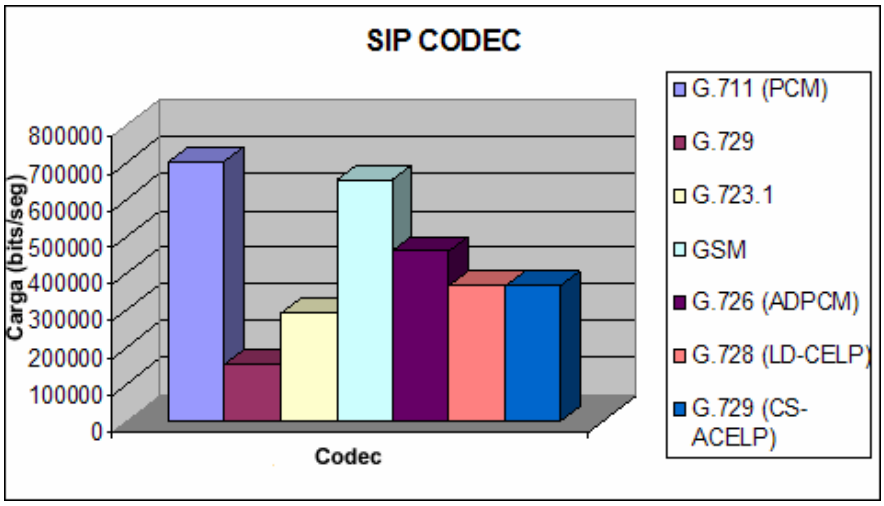


Figura 2-16. Diagrama codec-carga de SIP topología 2

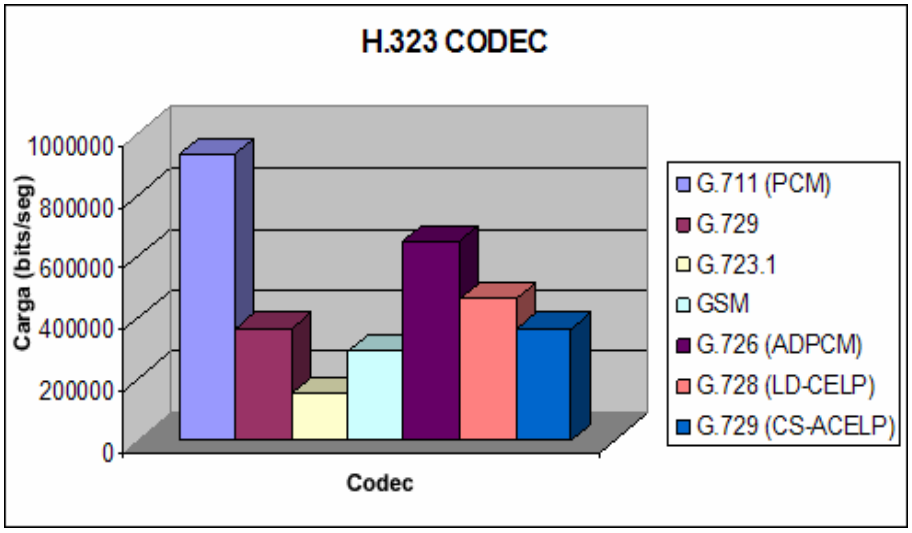


Figura 2-17. Diagrama codec-carga de H.323 topología 2

En la topología 2 se observa en La Figura 2-16, para el protocolo SIP que los codecs que generan mejor calidad de voz son: G.711 y GSM. Y de estos dos el G.711 es que sobresale.

A su vez en la Figura 2-17, el codec G.711 nuevamente es el más indicado debido a que tiene un retardo bajo[REF.27] en comparación con el G.729 que aparentemente podría ser la otra opción. Para un detalle de los resultados ver la sección B.2 y B.4 del apéndice B.

2.3.2 Señalización

Los resultados en las topologías tanto 1 como 2 mostraron que el protocolo SIP tiene menor tiempo para establecer la llamada. Esto debido a que el número de mensajes es menor comparado al protocolo H.323. Para un detalle de los resultados ver el apéndice B.

2.3.3 Voice Frame per Packets (VFPP)

Topología 1

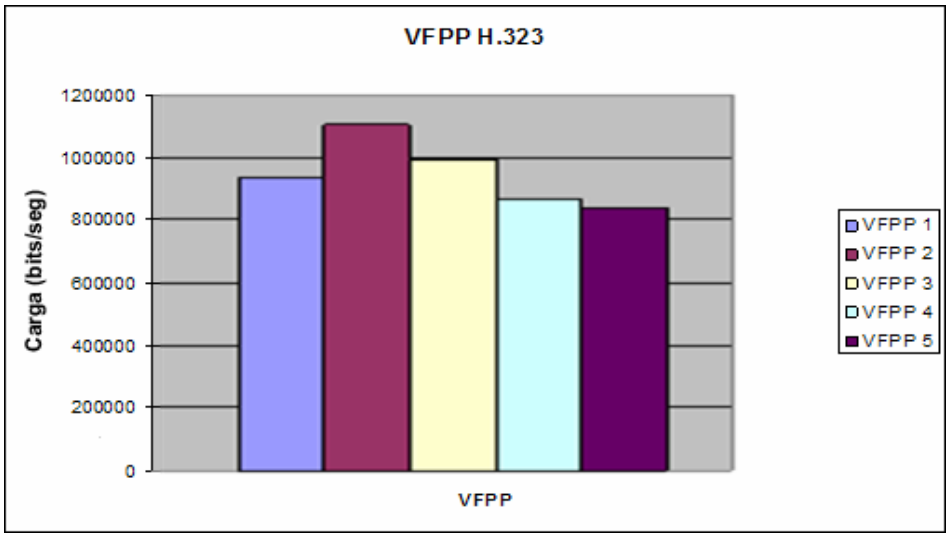


Figura 2-18. Diagrama VFPP-carga de H.323 topología 1

Topología 2

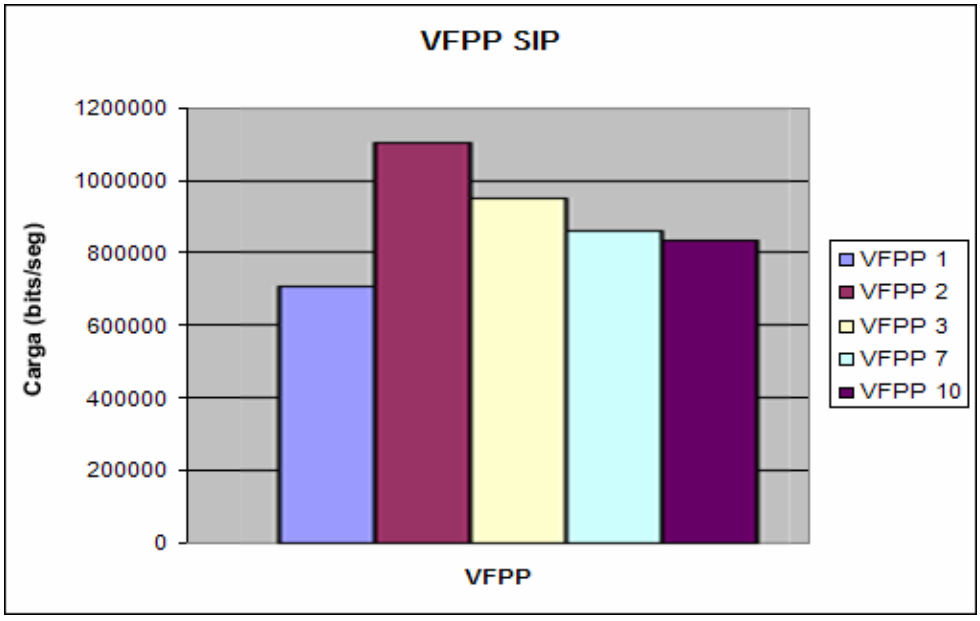


Figura 2-19. Diagrama VFPP-carga de SIP topología 2

El parámetro que se escogió para el VFPP es “2”. Ya que se puede apreciar en las Figuras 2-18 y 2-19 que el que mas carga soporta. También se puede percibir que la variación de este parámetro afecta más al protocolo SIP. Para un detalle de los resultados ver la sección B.5, B.6, B.7 y B.8 del apéndice B.

2.3.4 Tipe of Service (ToS)

En las simulaciones que se realizó el ToS no varió mucho entre los protocolos y las topologías, esto es debido a que el tráfico que se genero fue solo de voz. El parámetro que se escogió es el Iteractive Voice debido a la característica del tráfico enviado. Para un detalle de los resultados ver la sección B.9, B.10, B.11 y B.12 del apéndice B.

2.3.5 Quality of Service

El resultado que se obtuvo con el QoS al variar los tipos de servicios no se obtuvieron grandes cambios debido a que este servicio se visualiza mejor con mayores cargas. Para un detalle de los resultados ver la sección B.13 y B.14 del apéndice B.

2.3.6 Número de Nodos

Topología 1

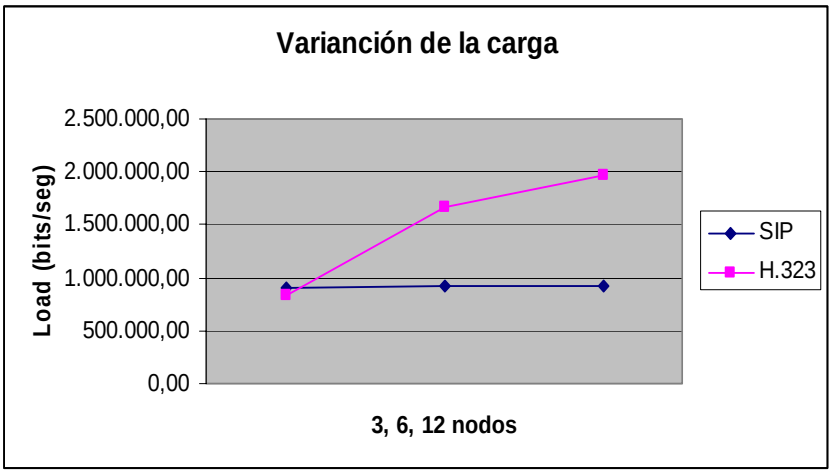


Figura 2-20. Diagrama Carga vs Nodo Topología 1

Topología 2

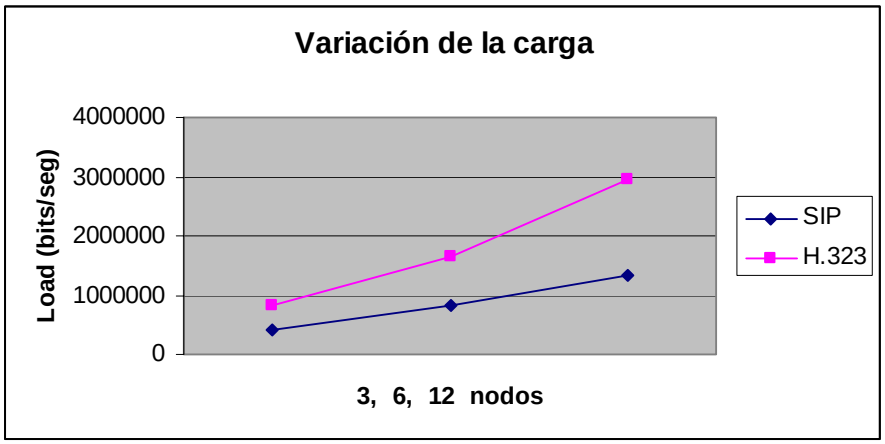


Figura 2-21. Diagrama Carga vs Nodo Topología 2

Los nodos aumentados se configuraron con los parámetros escogidos en los resultados que mejor destacaron en los resultados anteriores y se fue aumentando los nodos y se comparó para cada topología los diferentes protocolos.

De la Figura 2-20 se puede apreciar que para la topología 1 el protocolo SIP tiene un notable mayor desempeño, incluso al aumentar los nodos que intervienen en la conversación su requerimiento de ancho de banda no es tan grande. Por otro lado el protocolo H.323 a partir del nodo 3 su aumento en recursos va en mayor aumento. Se puede llegar a la conclusión de que en la topología 1 aunque la carga esta mas balanceada el protocolo H.323 no tiene un buen rendimiento. Aunque se lo podría usar con pocas estaciones que no superen las 4.

En la Figura 2-21 el protocolo que tiene mejor rendimiento es definitivamente el protocolo SIP, se observa que ambos crecen progresivamente pero el protocolo H.323 tiene mayor su pendiente haciendo la necesidad de recursos de este protocolo muy elevado.

De la Figura 2-21 se aprecia que el protocolo SIP tiene un mayor aumento de carga con respecto a la Figura 2-20, pero el protocolo H.323 sigue teniendo una mayor pendiente. Para un detalle de los resultados ver la sección B.15, B.16, B.17 y B.18 del apéndice B.

2.3.7 VPN

Los resultados de la simulación con IPSec son para evaluar que cual es su desempeño frente a los protocolos H.323 y SIP. Siendo

IPSec uno de los protocolos más recomendados para construir una VPN y así aumentar la seguridad dentro de las redes[REF.19]

Topología 1

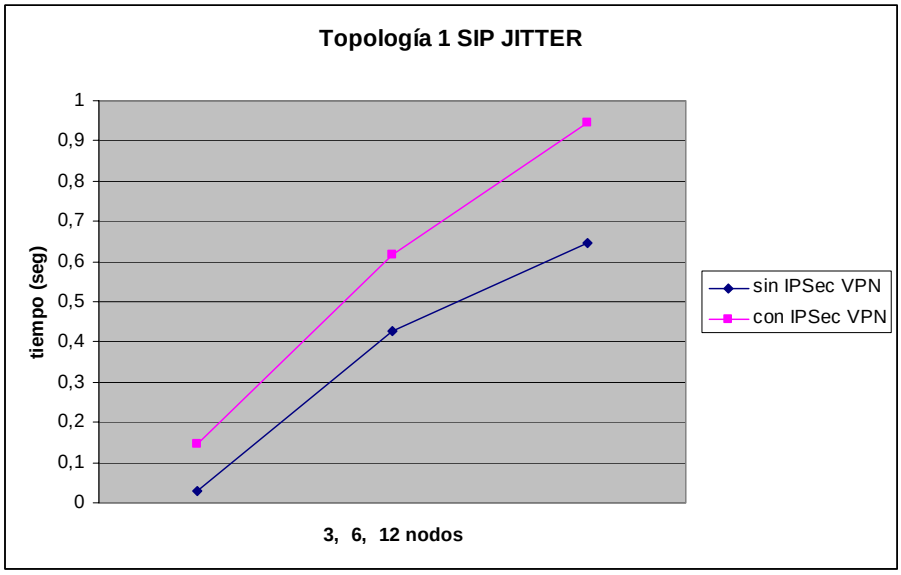


Figura 2-22. Variación del Jitter con VPN topología 1 SIP

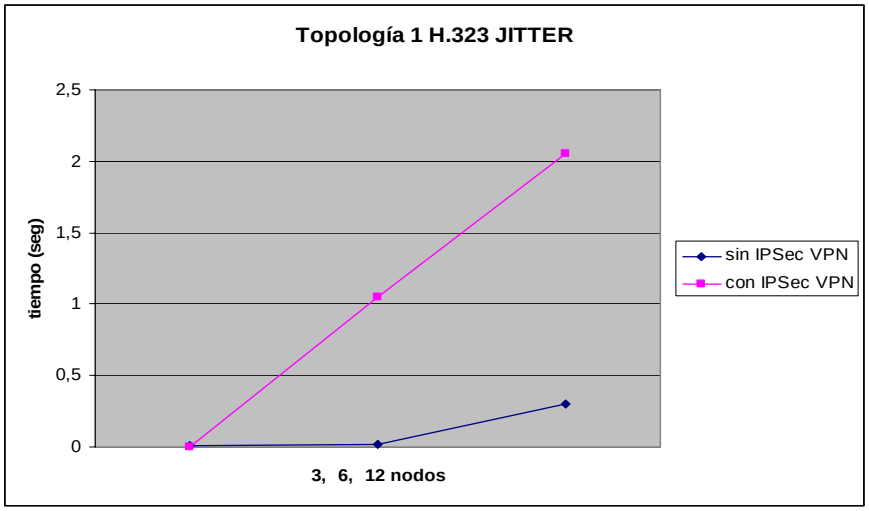


Figura 2-23. Variación del Jitter con VPN topología 1 H.323

Los resultados obtenidos para la topología 1 demuestran que la variación del jitter es considerablemente elevado para ambos protocolos. Debido a que el protocolo IPSec encripta los paquetes IP. Aunque se puede observar que con SIP el uso de IPSec afecta menos el rendimiento. Ver la sección B.19 y B.20 del Apéndice B.

Topología 2

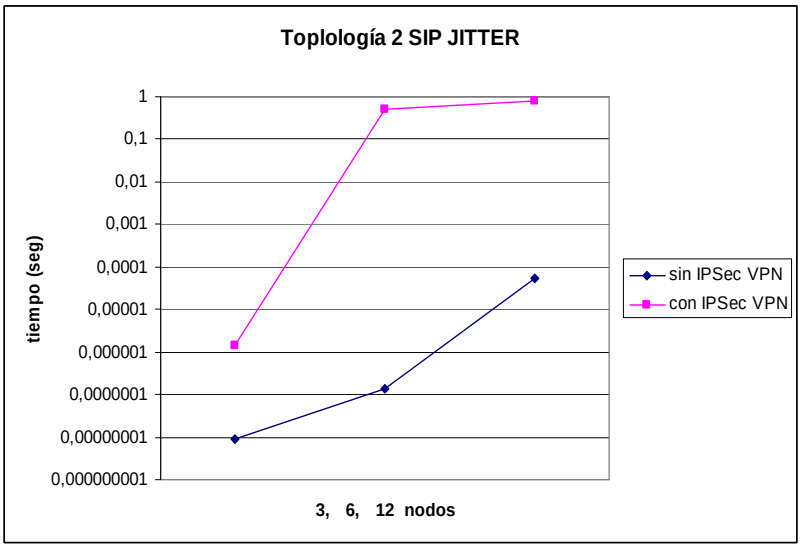


Figura 2-24. Variación del Jitter con VPN topología 2 SIP

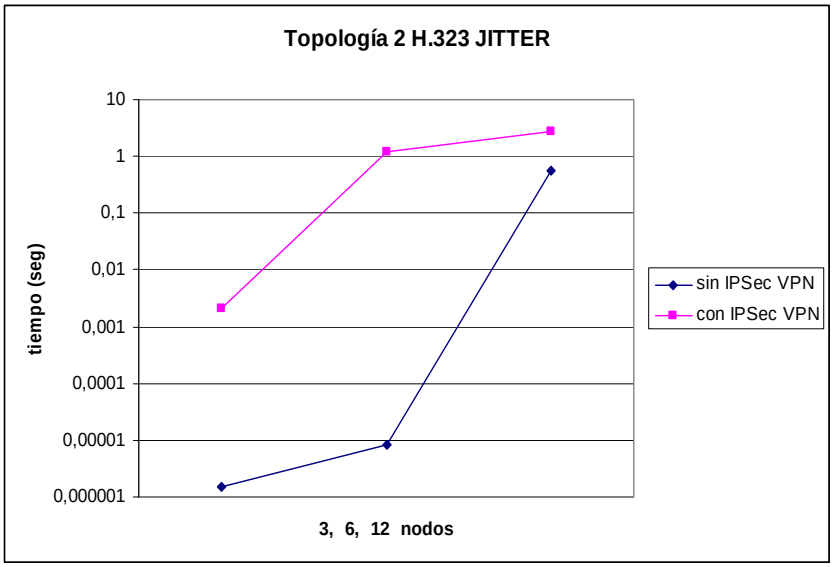


Figura 2-25. Variación del Jitter con VPN topología 2 H.323

En la topología 2 la variación del Jitter es igualmente elevado, las Figuras 2-22 y 2-23 están hecho en una escala logarítmica haciendo evidente su aumento a medida que aumenta los nodos

Como conclusión se llega que la utilización del protocolo IPSec es de gran ventaja pero su uso compromete directamente al retardo de los paquetes. Por esta razón se recomienda el uso sectorizado de este protocolo en zonas que no sean seguras. Ver la sección B.21 y B.22del Apéndice B.

2.4. Evaluación de Resultados

2.4.1 SIP

De los resultados evaluados se obtuvieron para el protocolo SIP las tablas, que nos muestran los parámetros que se deben considerar a la hora de configurar el protocolo SIP. Para la topología 1 el protocolo SIP tuvo mejor resultados y para la topología 2 tuvo un desempeño aceptable.

El uso del protocolo IPSec podría ser una opción teniendo en cuenta su alta latencia.

La siguiente tabla resume los parámetros escogidos con los valores mejores obtenidos en las simulaciones tanto para la topología 1 y 2:

Topología 1

Tabla 2-9. Variables obtenidas del protocolo SIP – Topología 1

Variable	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load (bits/seg)
G.711	0,02418427	1500	927	2,70989641	0,40950247	1,37010195	932080
2	0,02784838	750	750,16	0,00502687	2,05E-06	0,00199762	1103877,3
Interactive Voice	0,02155155	2140	2140	0,00961539	1,65E-06	0,00336806	769396,3

Topología 2

Tabla 2-10. Variables obtenidas del protocolo SIP – Topología 2

Variable	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load (bits/seg)
G.711 (PCM)	0,05282918	1000	646,666667	1,64029711	0,25134538	0,72508578	702666,6
2	0,01484261	750	749,444444	0,00438273	1,46E-06	0,00181796	1103591,1
Interactive Multimedia	52,82	1000	647,22	1,64846664	0,27229847	0,72606414	702666,7

2.4.2 H.323

Para el protocolo H.323 se obtuvo las siguientes tablas con los parámetros y los valores mejor obtenidos en los casos ideales en los que no se encuentre otro tipo de tráfico que no sea el de voz. Se llega a la conclusión de que el protocolo H.323 es un protocolo que es robusto pero al aumentar sus nodos aumenta mucho su carga. El protocolo H.323 aunque sus simulaciones demuestran algunas desventajas, sigue siendo un protocolo robusto especialmente contra ataques. El protocolo IPSec aumenta

considerablemente su carga, así que es aconsejable usarlo en sectores puntuales y usar alguna otras alternativas de seguridad como VLANs.

Topología 1

Tabla 2-11. Variables obtenidas del protocolo H.323 – Topología 1

Variable	RSVP (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load (bits/seg)
G.711 (PCM)	16,6666667	1500	928,333333	2,72312988	0,57064353	1,37	930400
2	27,7777778	750	750	0,00610448	5,05E-06	0,0024279	1104000
Interactive Voice	27,777777	48000	29600	2,711	7,60E-01	1,383	995,55
Priority Queuing	10,55	1500	944,44	2,41	0,5	1,21	935466,6

Topología 2

Tabla 2-12. Variables obtenidas del protocolo H.323 – Topología 2

Variable	RSVP (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load (bits/seg)
G.711 (PCM)	21,1111111	1500	959,444444	2,70943505	0,62111813	1,3681666	934133,3
2	13,5	1500	914	2,71849204	0,14635214	1,37376489	928720
Interactive Voice	52,82	1000	647,22	1,64846664	0,27229847	0,72606414	702666,7
Priority Queuing	8,88888889	1500	1501,66667	0,00243235	2,04E-06	0,00093328	1440000

2.4.3 Errores

Hay que tener presente que se esta simulando voz, y que esta simulación puede tener errores con respecto a la realidad, debido a los diferentes factores que pueden influir en una red real, lo que se trata de demostrar es la tendencia de ambos protocolos. En el capítulo tres se expone un modelo de campo para analizar su comportamiento y compararlas con lo obtenido en estas simulaciones

CAPÍTULO 3

3.1. PRUEBAS DE CAMPO

Diseño del Experimento

El experimento que se realizó se utilizó los datos obtenidos en las simulaciones. Se escogió el laboratorio móvil del Centro tecnológico de información (C.T.I), el cual consta de ocho computadoras conectadas inalámbricamente. Se configuró cada computadora, primero con el protocolo SIP y luego con el protocolo H.323. En ambas configuraciones se forman parejas para hacer las llamadas uno hace de caller y otro de calle.

Se recogen los datos para cada configuración del protocolo con el programa paketyzer, el cual nos permite evaluar varios parámetros como el jitter (variación de la demora o delay), los bytes recibidos y el promedio de utilización del medio.

Figura 3-1. Laboratorio Móvil del C.T.I

3.1.1 Modelo de Campo

El modelo de campo que se usa es el del laboratorio móvil que consta de 8 computadoras conectadas inalambricamente y unidas a la red del CTI.

Las computadoras están dentro del móvil conectadas entre sí a través de un Access Point y éste a su vez está conectado por antenas de radio con la red del CTI, desde la cual se les asigna direcciones IPs por medio de un servidor DHCP[13] a las laptops.

Figura 3-2. Interior del laboratorio Móvil del C.T.I

[13] DHCP.- (Dynamic Host Configuration Protocol). Protocolo de Internet estándar en la industria definido por IETF. Diseñado para proporcionar dinámicamente valores de configuración relacionados con comunicaciones, tales como direcciones de red para equipos clientes de red durante el inicio.

La carga del laboratorio es generada principalmente por la voz de ocho personas ubicada en cada laptop, y teniendo en cuenta que al estar conectado el laboratorio a la red del CTI mediante una antena de radio, esta genera una pequeña parte de la carga total. Debido a las computadoras y servidores que encuentran en dicha red.

3.1.2 Topología

La topología que se plantea en el modelo de campo es una topología tipo celda ya que el medio es inalámbrico para los clientes y la conexión con la red del CTI es de tipo estrella extendida

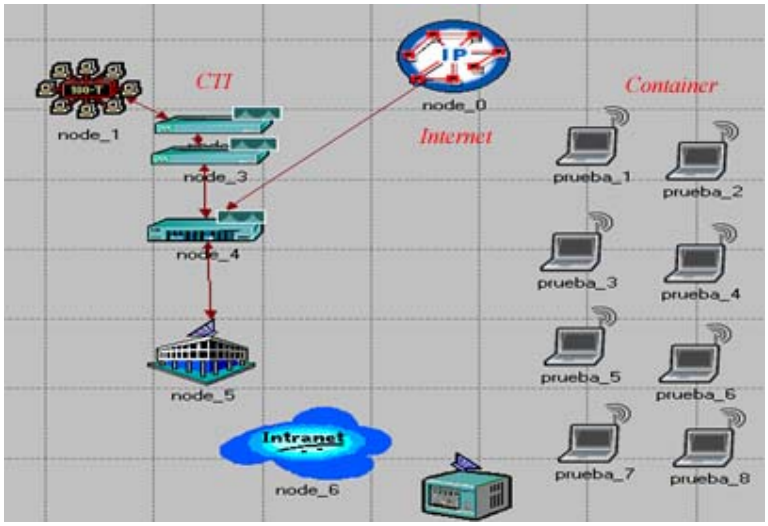


Figura 3-3. Arquitectura del laboratorio móvil

3.1.3 Configuración del Modelo de Campo

El modelo de campo se lo configuró con el protocolo SIP y el protocolo H.323.

Para el protocolo H.323 se utilizó un cliente H.323 y el gatekeeper, el cliente H.323 usado es el programa OpenPhone que es el cliente del proyecto OpenH.323 y se lo encuentra en su versión para Windows y Linux. Para el gatekeeper se utilizó el GNU Gatekeeper y también se lo encuentra para las plataformas de Windows y Linux.

Para el protocolo SIP se utilizó el proyecto Asterisk que funciona bajo la plataforma de Linux con el cliente Xlite cliente SIP para Windows.

Configuración del cliente OpenPhone y GNU Gatekeeper

OpenPhone.-

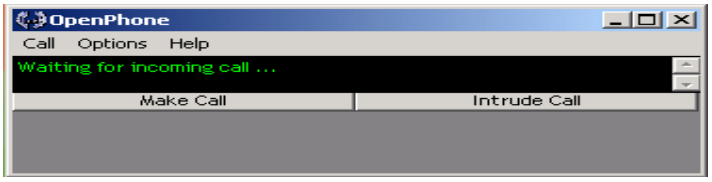


Figura 3-4. Ventana principal del cliente OpenPhone.

El cliente OpenPhone permite configurar varios parámetros entre los cuales están el gatekeeper y el codec y el tamaño de frame a usar.

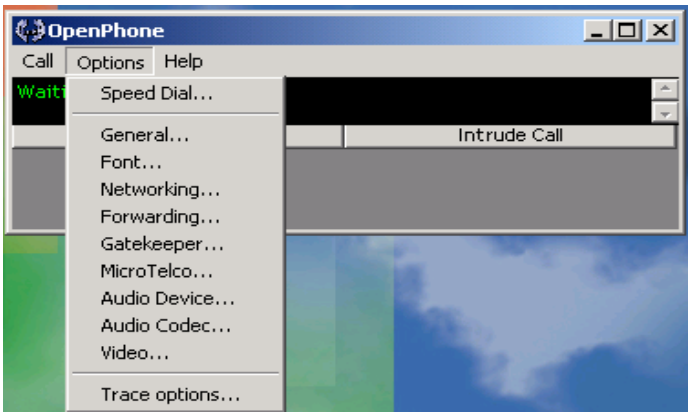


Figura 3-5. Ventana de selección de opciones del cliente OpenPhone.

Dentro de las opciones del programa se configura las opciones Generales, Gatekeeper, Audio Devide y Audio Codec.

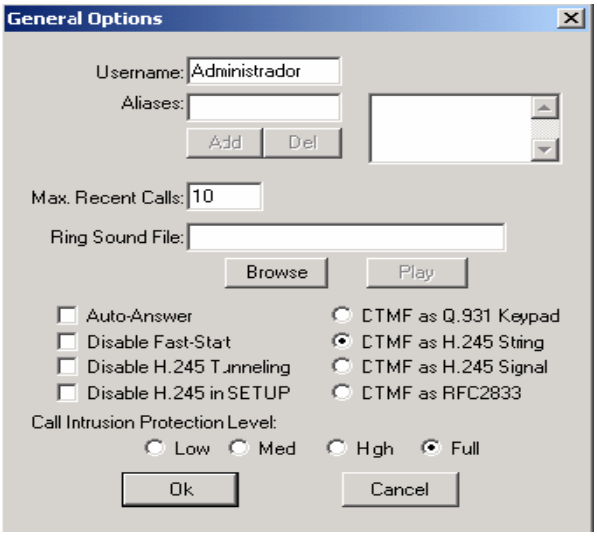


Figura 3-6. Ventana General de opciones del cliente OpenPhone.

En las opciones generales configuramos el usuario que se nos asigna en el gatekeeper, además podemos configurar el Alias con el que se nos va a reconocer durante las llamadas. Seleccionamos el DTMF como H.245 String, ya que de este modo

acentuamos un mejor control de la llamada [REF.30] y el Call Intrusion Protection Level en modo Full, ya que hay interés en el desempeño con seguridades.

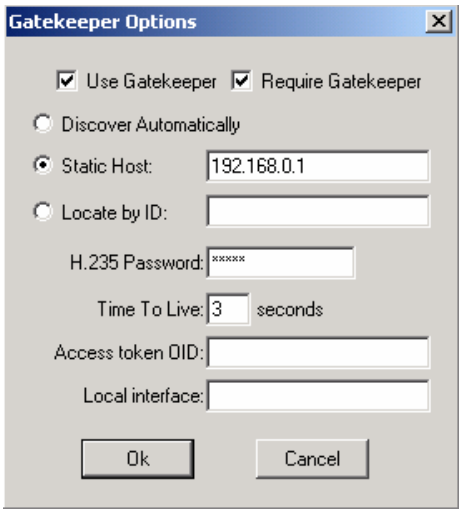


Figura 3-7. Opciones del Gatekeeper del cliente OpenPhone.

Las opciones del Gatekeeper seccionamos que use y requiera. El Gatekeeper para realizar la llamada, se configura la IP del Gatekeeper y la contraseña.

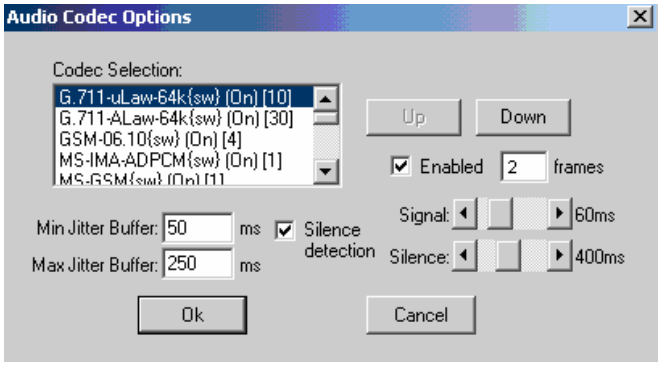


Figura 3-8. Opciones del Codec de Audio del cliente OpenPhone.

En las opciones del codec podemos seleccionar una variedad de codecs, se selecciona le codec G.711 por ser el mas recomendado y por mantener mejor la calidad de voz [REF.27], el valor de frames se lo escoge del valor obtenido en las simulaciones que es: 2. Ver el Apéndice E.

Configuración del Gatekeeper.-

El GNU Gatekeeper presenta la ventana para la instalación del servicio y configuración del mismo

Figura 3-9. Ventana del GNU Gatekeeper

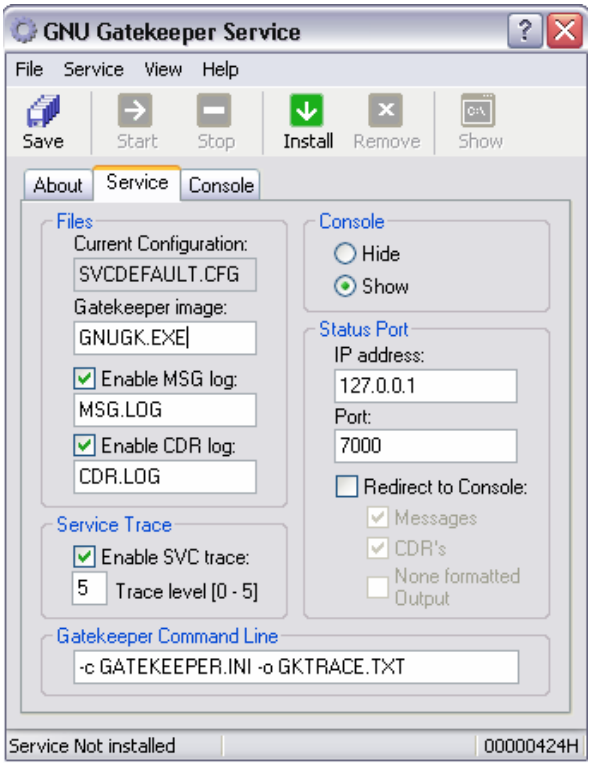


Figura 3-10. Servicios del Gatekeeper.

Las opciones de configuración aparecen en la pestaña de servicio de la Figura 36. Se presiona en el botón instalar y el servicio de gatekeeper se instala. Hay que tener en cuenta que los archivos GNUGK.EXE y gatekeeper.ini deben estar en la misma carpeta donde está el instalador gksvctrl.exe. Ver el Apéndice F.

Configuración del Asterisk.-

Asterisk es un software de telecomunicaciones que soporta los protocolos H.323 y SIP. Su configuración es un poco compleja

pero se parte de su configuración básica para el funcionamiento del protocolo SIP.

Configuración de los archivos sip.conf, extensions.conf.

Sip.conf.-

```
; sip.conf
;
;
[general] ; Opciones Generales.
port = 5060 ; Defino el puerto (SIP usa 5060)
bindaddr = 0.0.0.0 ; La dirección IP a usar (todas
las  posibles que existan)
allow=all ; Permite todo tipo de codecs
context = bogon-calls ; Envia las llamadas SIP que no
conocemos aqui

[2000] ; Defino el primer usuario
type=friend ; Defino el tipo de conexión, en este
caso.. AMIGO
username=prueba ; Nombre de usuario
secret=prueba ; Password :P
host=dynamic ; El host no siempre tiene la misma IP
context=slack-sip ; Las llamadas entrantes van a
slack-sip
mailbox=100 ; Activa la luz de mensaje en espera si
es que
; existe algo en voicemailbox

[2001] ; Es un duplicado de prueba, con diferente
login
type=friend
username=prueba1
secret=prueba
host=dynamic
context=slack-sip
mailbox=101

[2002] ; Es un duplicado de prueba, con diferente
login
type=friend
username=prueba2
secret=prueba
host=dynamic
context=slack-sip
mailbox=102
```

Con estas líneas en el archivo de configuración sip.conf el protocolo esta listo para usarse, ahora se configura el archivo

extensions.conf que es el archivo más importante dentro de todos los archivos de configuración.

```
; extensions.conf
;
[general]
static=yes ; Estas dos lineas previenen que desde la
linea de
writeprotect=yes ; comandos se pueda sobreescribir el
archivo de configuracion

[bogon-calls]
;
; Toma las llamadas desconocidas que encontraron
; el sistema, y les envia una orden de tono.
; El string "_." borra cualquier secuencia, con esto
; todas las llamadas resiviran el tono de ocupado.
; Eventualmente se aburriran y colgaran.
;
exten => _.,1,Congestion
[slack-sip] ; aqui defino la seccion slack-sip
;
; Si el numero marcado por el que llama es "2000",
entonces
; llama al usuario "prueba1" mediante el canal SIP.
Deja que el numero
; suene durante 20 segundos, y si no hay respuesta,
procede a la prioridad 2.
; Si el número retorna un resultado "busy", entonces
salta a la prioridad 102
;
exten => 2000,1,Dial(SIP/2000,20)
;
; La prioridad 2 envia la llamada al voicemail, y da
el mensaje "u"navailable
; para el usuario 2000. La unica forma de salir del
voicemail
; en esta instancia es colgando.
;
exten => 2000,2,Voicemail(u2000)
;
; Si el numero marcado en la prioridad 1 devuelve un
estado
; "busy", entonces el Dial saltara a 101 + (prioridad
actual)
; que en este caso seria 101+1=102. Este +101 es
construido
; dentro de Asterisk y no necesita ser definido.
;
exten => 2000,102,Voicemail(b2000)
exten => 2000,103,Hangup
;
; Ahora, que pasa si el numero marcado es "2001" o
"2002"?
;
exten => 2001,1,Dial(SIP/2001,20)
exten => 2001,2,Voicemail(u2001)
exten => 2001,102,Voicemail(b2001)
exten => 2001,103,Hangup
exten => 2002,1,Dial(SIP/2002,20)
exten => 2002,2,Voicemail(u2002)
exten => 2002,102,Voicemail(b2002)
```

```
exten => 2002,103,Hangup
;
; Ahora defino un número donde los usuarios puedan
alcanzar
; el voicemail. Llamo a la aplicacion VoicemailMain
con el
; numero del que llama pasado como variable, asi
; que lo unico que se necesita hacer es teclear el
password.
;
exten => 2999,1,VoicemailMain(${CALLERIDNUM})
;
; Defino un numero para escuchar el Music on Hold
;
exten => 6601,1,WaitMusicOnHold(30)
;
; Con esto puedo incluir las secciones dento de
slack-sip
;
include => help
include => meetme
;
; Esta seccion esta definida en el archivo por
defecto,
; es un número que entrega información acerca de
Asterisk,
; en el archivo original el numero es una 's'
;
[help]
exten => 666,1,Wait,1 ; Espera un segundo
exten => 666,2,Answer ; Responde la linea
exten => 666,3,DigitTimeout,5 ; Setea el tiempo de
digitar en 5 seg.
exten => 666,4,ResponseTimeout,10 ; Setea el tiempo
de respuesta en 10 seg.
exten => 666,5,BackGround(demo-congrats) ; Reproduce
un mensaje de felicitaciones
exten => 666,6,BackGround(demo-instruct) ; Reproduce
algunas instrucciones
exten => 2,1,BackGround(demo-moreinfo) ; Entrega mas
informacion.
exten => 2,2,Goto(s,6)
exten => 500,1,Playback(demo-abouttotry); Me deja
saber que esta pasando
exten =>
500,2,Dial(IAX2/guest@misery.digium.com/s@default) ;
Llama el demo de Asterisk
exten => 500,3,Playback(demo-nogo) ; No pudo conectar
al demo
exten => 500,4,Goto(666,6) ; Retorna al principio del
;mensaje
```

Cliente Xlite.-

El cliente X-lite es un cliente SIP. Hay que configurar el usuario, contraseña y el servidor SIP que nos autentifique y nos permita hacer las llamadas.

Configuramos los siguientes parámetros:

- Enable: este parámetro nos permite habilitar la configuración.
- Display Name: es el nombre con el cual nos vamos a identificar.
- User Name: es el usuario definido en el archivo sip.conf.
- Authorization User: el usuario de autorización por lo general es el mismo que el user name.
- Password: la calve que es asignada en el archivo sip.conf.
- Domain/Realm: dominio en donde esta alojado el servidor SIP.
- SIP Proxy: el nombre o dirección IP con el puerto por el cual escucha.
- Out Bound Proxy: servidor de salida, por lo general es el mismo del SIP Proxy.

Los parámetros restantes se los configura por defecto.

Figura 3-11. Ventana del Xlite – configuración del cliente

1.4 Software para evaluar los datos

El software que se utilizó para la recolección y evaluación de los datos es el Packetyzer que es un potente programa que nos permite analizar y detectar problemas en las redes. Utiliza la ventaja de su código abierto para el aumento de sus librerías, y es uno de los más usados por los administradores de redes.

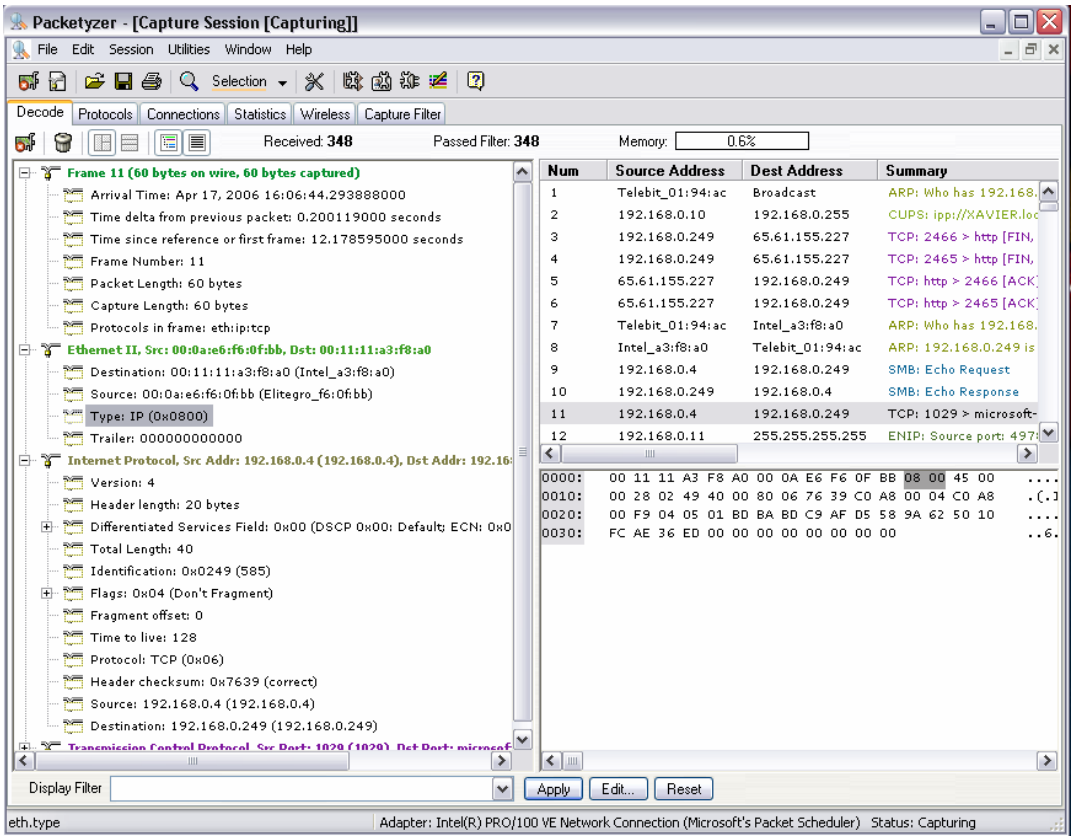


Figura 3-12. Ventana principal del Packetyzer

Dentro de los datos que permite recolectar están:

Tabla 3-1. Parámetros a evaluar en las pruebas de campo

Parámetros	Detalle
Total de Paquetes	Total de Paquetes Recibidos por la estación
Total bytes	Total de bytes Recibidos por la estación
Utilización Promedio (Bit/sec)	La utilización promedio de en envió y recepción de datos
Datos (bytes)	Representa los datos de los bytes enviados

3.1.5 Recolección de Datos

La recolección de datos fueron de las ocho máquinas del laboratorio las cuales a su vez se dividieron en cuatro que hicieron de caller, y las cuatro restantes de callee. Los números impares representan los que realizaron las llamadas mientras que los números pares representan los que recibieron las llamadas. Se realizaron dos pruebas de 30min a 45min para cada protocolo.

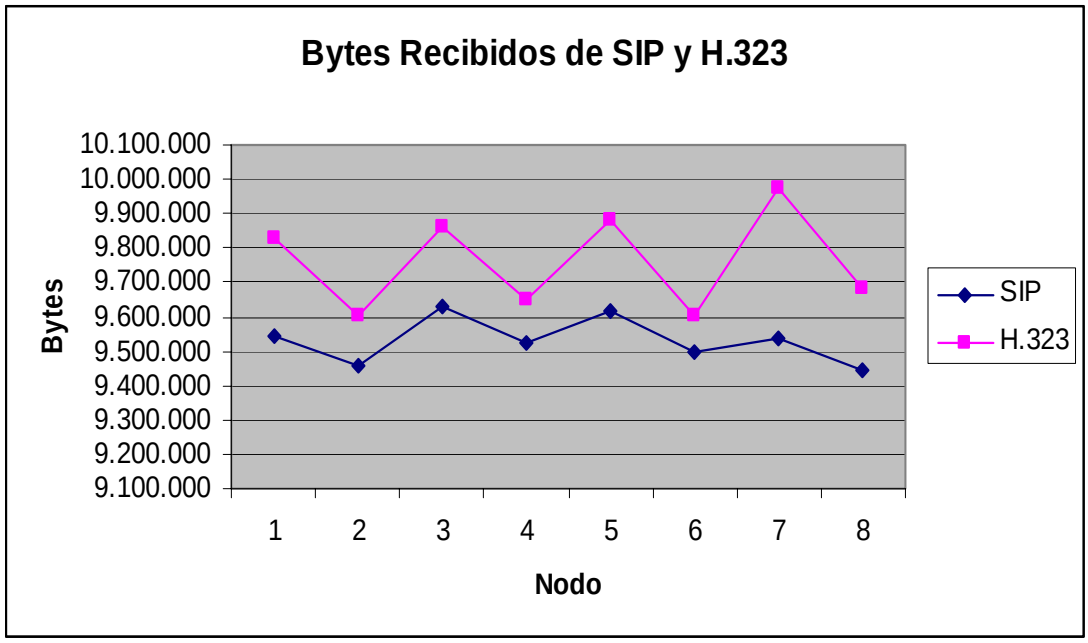


Figura 3-13. Gráfico de paquetes recibidos de los protocolos SIP y H.323

En la Figura 3-13, se observa los bytes recibidos por cada una de las laptops. Lo que se puede observar es que H.323 genera una

mayor sobrecarga de datos. Esta sobre carga causa que el audio pueda llegar con una pequeña latencia a su destino, y si aumenta puede llegar hasta entrecortada. La mayor cantidad de paquetes recibidos por los nodos en el protocolo H.323 es debido a que el este protocolo implementa más control en sus paquetes agregando más información. Para mayor información ver Apéndice G.

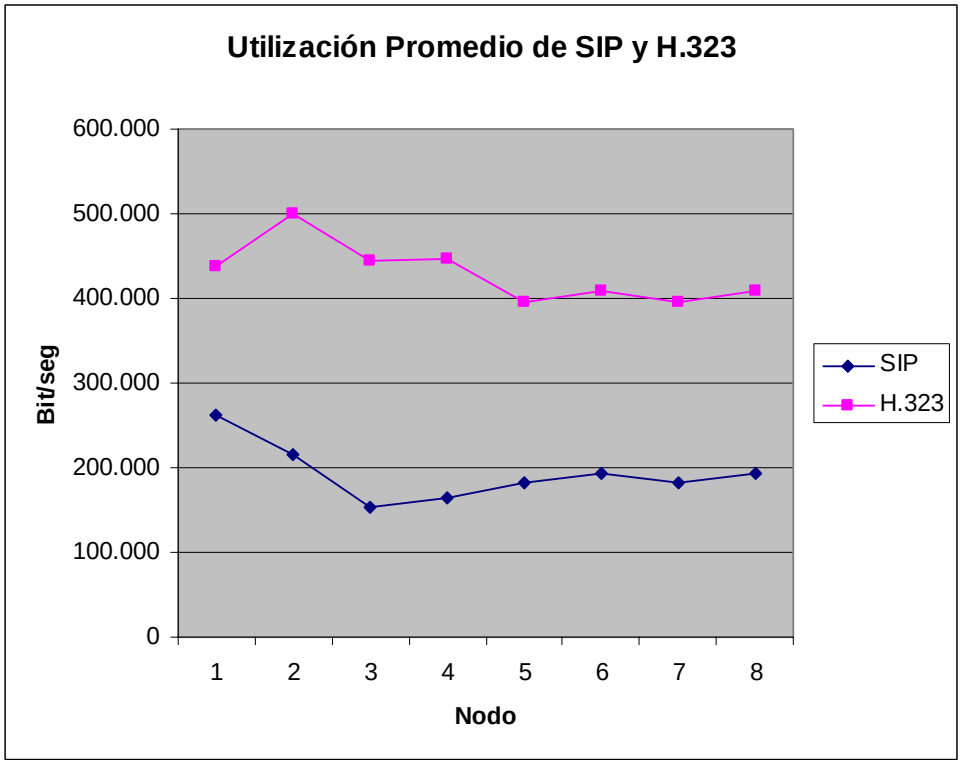


Figura 3-14. Gráfico de la utilización promedio de los protocolos SIP y H.323

La Figura 3-14, nos muestra la utilización promedio en bits/seg. Se observa claramente cómo el protocolo H.323 tiene un mayor promedio que el protocolo SIP. Esto hace que el protocolo H.323 envié mas bytes por la red, pudiendo a llegar a saturar la red si estos aumentan considerablemente. Para mayor información ver Apéndice G.

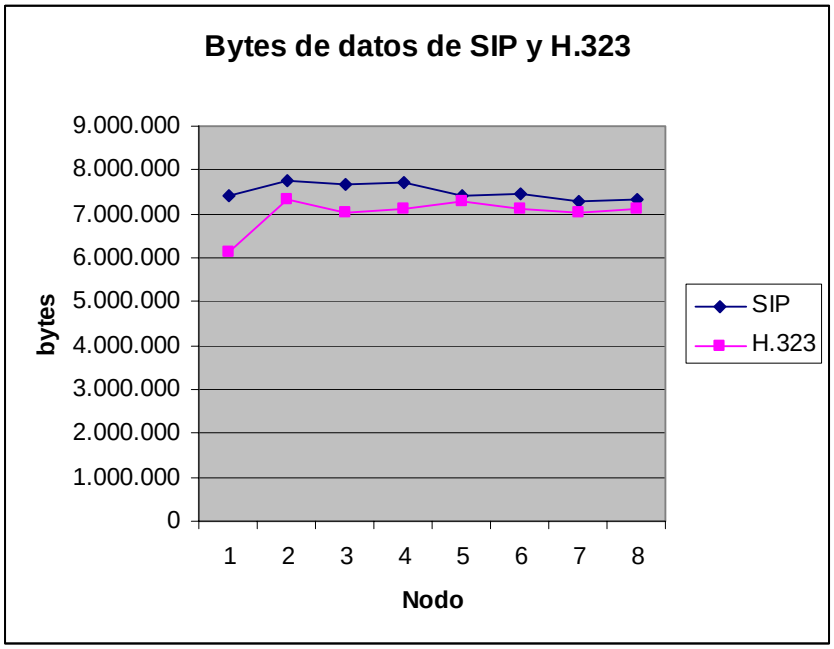


Figura 3-15. Gráfico de bytes de datos recibidos de los protocolos SIP y H.323

La Figura 3-15, muestra los datos que viajan en el intercambio de los paquetes. Estos datos representan la voz que viaja entre cada nodo. Aunque a simple vista no mayor diferencia, la escala de millones de bytes nos indica que el protocolo SIP tiene un mejor envío de datos de voz. Para mayor información ver Apéndice G.

3.2.-Resultados

3.2.1 Comparación de los Resultados Simulados y de Campo

De los resultados obtenidos en las simulaciones se observa que las variables:

- Codec con el valor de G.711.
- Voice Frame Per Packets con el valor de 2.
- Tipe of Service con el valor de Interactive Voice.

Para los protocolos H.323 y SIP y:

- Quality of Service con el valor de WQF

Son las variables que obtuvieron mejor desempeño. Los parámetros que mayor se vieron afectados con las variables fueron: la carga y el jitter. Y el protocolo que tuvo mejor desempeño es SIP.

La utilización del protocolo IPSec para la seguridad de la voz que viaja a través de la red inserta una elevada latencia en ambos protocolos siendo el H.323 el más afectado, debido a su latencia inherente de dicho protocolo, afectando considerablemente su desempeño.

En las pruebas realizadas con los clientes para ambos protocolos, configurando las variables mencionadas, se obtuvo que el

protocolo SIP destacó en su rendimiento. Y los parámetros que se evaluaron son: sobrecarga, utilización promedio y datos de voz.

En las Figuras 3-13, 3-14 y 3-15 se observa que, el protocolo H.323 genera una mayor carga en la red, y además, el protocolo SIP utiliza mejor los recursos que tiene para enviar los datos.

Se puede comparar que los resultados obtenidos tanto en la fase de simulación como en la fase de prueba concuerdan que el protocolo SIP tiene mejor desempeño en el manejo de los datos.

Una gran desventaja del simulador es que no se puede escuchar la voz, que no ocurre con las pruebas de campo. Pero evaluando los resultados obtenidos se observa que el comportamiento de los protocolos SIP y H.323 tiene relación con lo simulado y con lo probado en el campo.

3.2.2 Análisis de resultados

De los resultados comparados se analiza que:

- El simulador IT-Guru se aproxima bastante a la realidad obteniendo resultados semejantes entre lo simulado y las pruebas de campo. Esto se nota en la evaluación de la carga que maneja cada protocolo y

de cómo el protocolo H.323 tiene una mayor sobrecarga que el protocolo SIP.

- En la fase de simulación el protocolo SIP destaca por alto rendimiento en la transmisión de voz al combinar las diferentes variables y observar una cierta estabilidad en su desempeño. El la poca latencia que inserta el protocolo SIP al aumentar los nodos, recalcan que lo simulado se asemeja a la realidad.
- La fase de prueba ayuda a complementar lo evaluado en las simulaciones. Igual que en lo simulado el protocolo que se obtuvo un mejor rendimiento es el protocolo SIP. Aunque el protocolo H.323 manejando mejor la seguridad tuvo un desempeño aceptable.
- Aunque no se puede evaluar a fondo los parámetros se puede concluir en el análisis que el simulador IT-Guru se asemeja a lo real.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Para la topología uno y dos el que tuvo mejor desempeño fue el protocolo SIP, Aunque si se desea usar el protocolo H.323 por alguna característica o requisito se recomienda usarlo en la topología de tipo celda.
- El protocolo SIP tiene un alto desempeño en redes donde el ancho de banda de la red no es muy grande.
- Los protocolos H.323 y SIP utilizados para la transmisión de voz sobre redes IPs, son estructuralmente diferentes.
- El protocolo SIP es el mejor capacitado para la evolución de redes inalámbricas. Debido a su desempeño en las diferentes evaluaciones.
- El protocolo H.323 tiene una alta complejidad en su configuración y manejo de sus mensajes a través de la red.
- La gran desventaja de SIP es su vulnerabilidad que puede ser compensado con el protocolo IPSec.

- El protocolo H.323 es una opción para redes con pocos nodos de 2 a 4. Aunque hay que tener en cuenta su complejidad al ser implementado.
- La gran ventaja del protocolo SIP no es solo su sencillez en la configuración sino su estabilidad al aumentar los nodos que intervienen en la transmisión de voz.
- Hay que tener cuidado al implementar seguridades en los protocolos, ya que estos afectan su latencia considerablemente.
- El protocolo IPSec es el protocolo que ofrece mayor seguridad, pero inserta una alta latencia que hay que saber manejar.

Recomendaciones

- Usar el protocolo SIP para redes inalámbricas, aunque si se usa el protocolo H.323 usarlos con no más de 4 clientes.
- Para el protocolo H.323 y SIP usar los servidores y clientes de código abierto
- Para la seguridad usar el protocolo IPSec sectorizarlo en lugares no confiables.

- Usar el simulador OPNET en su versión completa, para poder evaluar mayores tipos de seguridades.

GLOSARIO

ASCII.- Abreviación de American Standard Code for Information Interchange, un código de 7-bit que sustituye las letras del alfabeto romano por cifras y otros caracteres informáticos.

Backbone.- Un backbone es enlace de gran caudal o una serie de nudos de conexión que forman un eje de conexión principal. Es la columna vertebral de una red.

Binaria (ASN.1).- *ASN.1 (Abstract Syntax Notation): Notacion Abstracta de Sintaxis, un* protocolo para datos estructurados.

HTTP.- Http son las siglas de HyperText Transfer Protocol, el método utilizado para transferir ficheros hipertexto por Internet. La transferencia hipertexto es simplemente la transeferencia de ficheros hipertexto de un ordenador a otro.

IANA.- IANA (Internet Assigned Numbers Authority) Es el organismo de la ISOC que se encarga de la administración de las direcciones Internet direcciones IP así como de la creación de nuevos dominios.

IETF.- "Internet Experts Task Force". Es el comité encargado de elaborar los estándares en Internet.

IP.- Internet Protocol, es la especificación que determina hacia dónde son encaminados los paquetes, en función de su dirección de destino.

IP PBX.- IP Private Branch eXchange. Centralita IP. Dispositivo de red IP que se encarga de conmutar tráfico telefónico de VoIP.

IPX.- (*Internetwork Packet eXchange*). IPX es un protocolo de la capa de red no confiable. Este protocolo transfiere paquetes del origen al destino en forma transparente, aun si la fuente y el destino se encuentran en redes diferentes.

ITU-T.- International Telecommunications Union – Telecommunication. Agencia de la Organización de las Naciones Unidas que trata lo referente a telecomunicaciones.

LAN.- Local Area Network. Red de área local. Una red pequeña de datos que cubre un área limitada, como el interior de un edificio o un grupo reducido de edificios.

MIME.- Multipurpose Internet Mail Extension. Sistema que permite integrar dentro de un mensaje de correo electrónico ficheros binarios (imágenes, sonido, programas ejecutables, etc.).

OSI.- Open System Interconnection. Modelo de 7 capas o niveles, que describe las entidades que participan en la red.

PGP.- Siglas de Pretty Good Privacy. Es un programa freeware de encriptación con considerable soporte en Internet.

Protocolo.- Un protocolo es una serie de reglas que utilizan dos ordenadores para comunicar entre sí. Cualquier producto que utilice un protocolo dado debería poder funcionar con otros productos que utilicen el mismo protocolo.

RTP/RTCP (Real-Time Transport Protocol / Real-Time Transport Control Protocol) Protocolos de transporte en tiempo real que proporciona servicio de entrega punto a punto de datos.

SigComp.- Signaling Compression (SigComp), Una solución para compresión de mensajes generados por aplicaciones de protocolos como SIP y RTSP (Real Time Streaming Protocol).

S/MIME.- protocolo de seguridad para correos electrónicos usa certificados digitales.

S-HTTP.- (Secure HTTP): Sistema encaminado a proporcionar transacciones seguras dentro del entorno World Wide Web.

TCP/IP.- TCP/IP son las siglas de Transmission Control Protocol/Internet Protocol, el lenguaje que rige todas las comunicaciones entre todos los ordenadores en Internet. TCP/IP es un conjunto de instrucciones que dictan cómo se han de enviar paquetes de información por distintas redes.

Topología.- Se refiere a cómo se establece y se cablea físicamente una red. La elección de la topología afectará la facilidad de la instalación, el costo del cable y la confiabilidad de la red. Existen tres topologías principales de red anillo, bus y estrella.

UDP.- Acrónimo en inglés de User Datagram Protocol. Protocolo de Datagramas de Usuario. Protocolo dentro del TCP/IP que convierte mensajes de datos en paquetes para su envío vía IP pero que no pide confirmación de la validez de los paquetes enviados por la computadora emisora (no verifica que hayan sido entregados correctamente).

Unix.- Sistema operativo especializado en capacidades de multiusuario y multitarea. Fue la base inicial de Internet. Entre sus características más importantes se encuentran: Redireccionamiento de Entrada/Salida

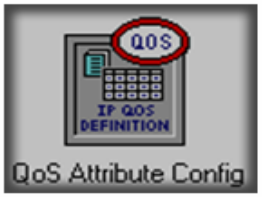
WAN.- (Wide Area Network, Red de Área Amplia). Red de computadoras conectadas entre sí. Usando líneas terrestres o incluso satélites para interconectar redes LAN en un área geográfica extensa que puede ser hasta de miles de kilómetros.

Wi-Fi.- Abreviatura en inglés para "wireless fidelity". Un tipo de red inalámbrica (WLAN - wireless local area networks), que usa el protocolo inalámbrico de alcance limitado IEEE 802.11b, que transmite datos en banda ancha en el rango espectral de 2.4 GHz.

APÉNDICES

A APÉNDICE A: ELEMENTOS ESCOGIDOS PARA LA SIMULACIÓN DEL PROGRAMA IT-GURU.

A.1 Nodos

		
1. Configuración aplicación.	**2. Configuración Profile.**	**3. Configuración QoS.**
		
4. Configuración VPN.	**4. Gateway**	**5. Wireless LAN**
		
6. Servidor SIP	**7. Estación inalámbrica**	**8. Nube de nodos.**
		
9. Enlace de 1.500Mbs	**10. Enlace de 100Mbs**	**11. Subred**

A.2 Descripción de Nodos

N	Nodo	Descripción	Protocolo
1	Application Conf.	Se configura los parámetros que la aplicación de voz que los protocolos van a usar	SIP y H.323
2	Profile Conf.	Se designa a que tipo de usuario pertenece la aplicación configurada	SIP y H.323
3	QoS Attribute Conf	Se configurara los tipos de servicio de calidad soportados por el entorno simulado	H.323
4	IP VNP Conf.	Se configurara las redes virtuales (usado para IPSec)	SIP y H.323
5	ethernet4_slip8_gtwy_adv	Gateways avanzados que permiten una mayor configuración de sus interfaces	SIP y H.323
6	wlan_ethernet_slip4_adv (fix)	Wireless Lan Router, dan conexión inalámbrica entre los clientes	SIP y H.323
7	Sip_proxy_server	Servidor proxy para SIP	SIP
8	wlan_wkstn_adv (fix)	Estaciones Terminales, los que envían la voz	SIP y H.323
9	ip32_cloud	Nodos que introducen latencia en los paquetes	SIP y H.323
10	Subset	Subredes que dividen los dominios	SIP y H.323
11	PPP_DS1	enlace a una velocidad de 1.544 Mbps para conexiones de punto a punto	SIP y H.323
12	100BaseT	enlace a una velocidad de 100Mbps	SIP y H.323

B APÉNDICE B: RESULTADOS DE LAS SIMULACIONES.

B.1 Resultados de la simulación de la topología 1, SIP – CODEC.

Codec	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load (bits/seg)
G.711 (PCM)	0,024184	1500	927	2,709896406	0,4095024	1,37010195	932080
G.729	0,016051	600	600	0,002244532	4,3112E-08	0,0008397	364800
G.723.1	0,015978	200	200	0,002336422	1,9218E-08	0,00083629	153600
GSM	0,015791	300	300	0,002797618	1,9975E-08	0,00100082	292800
G.726	0,017586	600	600	0,003087185	8,0847E-08	0,00110563	652890,6
G.728	0,017088	600	600	0,002755864	4,1452E-08	0,00104773	460800
G.729	0,016498	600	600	0,002244532	4,3112E-08	0,0008397	364800

B.2 Resultados de la simulación de la topología 1, H.323 – CODEC.

Codec	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load (bits/seg)
G.711	16,66666	1500	928,33	2,723129883	0,5706435	1,37028003	930400
G.729	16,66666	600	599,83	0,002258502	4,3272E-08	0,00084312	364800
G.723.1	16,66666	200	200	0,002673591	6,3725E-08	0,00098691	153600
GSM	16,66666	300	300	0,002715592	2,1178E-08	0,00094992	292800
G.726	16,66666	600	600	0,003624983	5,9927E-07	0,00135125	652890,6
G.728	16,66666	600	600	0,002809124	8,0544E-08	0,00106503	460736
G.729	16,66666	600	599,83	0,002258502	4,3272E-08	0,00084312	364800

B.3 Resultados de la simulación de la topología 2, SIP – CODEC

Codec	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load (bits/seg)
G.711 (PCM)	52,829175	1000	646,66	1,640297111	0,2513453	0,72508578	702666,6
G.729	0,012798	200	200	0,001747509	2,58E-09	0,00073638	153600
G.723.1	0,0154081	300	300	0,003124044	3,4754E-07	0,00141539	292800
GSM	0,0161161	600	600	0,003113965	3,071E-07	0,00126617	652800
G.726	0,022698	600	600	0,002199754	6,57E-08	0,00096045	460800
G.728	0,0161886	600	600	0,002400565	5,219E-07	0,00105422	364800
G.729	0,0161886	600	600	0,00240481	5,2726E-07	0,00105257	364698,6

B.4 Resultados de la simulación de la topología 2, H.323 – CODEC

Codec	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load (bits/seg)
G.711	21,111111	1500	959,44	2,709435046	0,621118129	1,368166	934133
G.729	23,333333	600	600	0,002342847	4,23354E-07	0,0009861	364800
G.723.1	23,333333	200	200	0,002029792	2,2466E-08	0,0007989	153600
GSM	23,333333	300	300	0,002479112	4,384E-08	0,0009779	292800
G.726	23,333333	600	600	0,003449889	4,5787E-07	0,0014385	652800
G.728	23,333333	600	600	0,002643417	5,78535E-07	0,001100	460800
G.729	23,333333	600	600	0,002342847	4,23354E-07	0,0009861	364800

B.5 Resultados de la simulación de la topología 1, SIP – VFPP

VFPP	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load (bits/seg)
1	0,030747518	1500	924,33	2,724706965	0,738152294	1,3764471	923120
2	0,027848376	750	750,16	0,005026872	2,04956E-06	0,00199762	1103877,3
3	0,017417843	500	500	0,005632561	1,31786E-06	0,00209367	991448,8
7	0,016635057	213,3	215,55	0,009730003	1,53619E-06	0,00347625	861280
10	0,018349653	150	150	0,012822539	2,32887E-06	0,00453347	835200

B.6 Resultados de la simulación de la topología 1, H.323 – VFPP

VFPP	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load (bits/seg)
1	27,77777	1500	925	2,721532042	0,869542181	1,36909025	935733,33
2	27,77777	750	750	0,006104478	5,0521E-06	0,0024279	1104000
3	27,77777	500	498,8888	0,006007733	2,74992E-06	0,00221902	992000
7	27,77777	213,33	213,3333	0,010020174	1,55948E-06	0,00347498	868000
10	16,66666	150	150	0,011036963	1,70332E-07	0,00360194	835200

B.7 Resultados de la simulación de la topología 2, SIP – VFPP

VFPP	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load (bits/seg)
1	0,016484051	1000	653,8888	1,673017375	0,143432569	0,73173554	710133,33
2	0,014842613	750	749,4444	0,004382725	1,46347E-06	0,00181796	1103591,11
3	0,021356826	500	472,7777	1,078290089	0,153871653	0,5360941	951217,77
7	0,015267867	215	214	0,010251947	3,09331E-06	0,00376472	863520
10	0,019402248	150	150	0,011434629	3,99618E-06	0,00444884	835200

B.8 Resultados de la simulación de la topología 2, H.323 – VFPP

VFPP	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load (bits/seg)
1	27,77777778	1500	925	2,721532042	0,869542181	1,36909025	935733,3
2	27,77777778	750	750	0,006104478	5,0521E-06	0,0024279	1104000
3	27,77777778	500	498,88	0,006007733	2,74992E-06	0,00221902	992000
7	27,77777778	213,33	213,33	0,010020174	1,55948E-06	0,00347498	868000
10	16,66666667	150	150	0,011036963	1,70332E-07	0,00360194	835200

B.9 Resultados de la simulación de la topología 1, SIP – ToS

ToS	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load (bits/seg)
Best Effort	0,0241842	1500	926,333	2,6076	0,280949	1,18855	723177,04
Background	0,0241842	1500	926,333	2,6076	0,280949	1,18855	723177,04
Standard	0,0241842	1500	926,333	2,6076	0,280949	1,18855	723177,04
Excellent Effort	0,0241842	1500	926,333	2,6076	0,280949	1,18855	723177,04
Streaming Multimedia	0,0241842	1500	926,333	2,6076	0,280949	1,18855	723177,04
Interactive Voice	0,0241842	1500	926,333	2,6076	0,280949	1,18855	723177,04
Reserverd	0,0215515	214,16	214,333	0,0096	1,6559E-06	0,00336	669396,35

B.10 Resultados de la simulación de la topología 1, H.323 – ToS

ToS	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load (bits/seg)
Best Effort	27,777777	368,88	925	2,49	0,57	0,0034	728,88
Background	27,777777	368,88	925	2,49	0,57	0,0034	728,88
Standard	27,777777	368,88	925	2,49	0,57	0,0034	728,88
Excellent Effort	27,777777	368,88	925	2,49	0,57	0,0034	728,88
Streaming Multimedia	27,777777	368,88	925	2,49	0,57	0,0034	728,88
Interactive Voice	27,777777	368,88	925	2,49	0,57	0,0034	728,88
Reserverd	27,777777	368,88	935	2,49	0,57	0,0034	728,88

B.11 Resultados de la simulación de la topología 2, SIP – ToS

ToS	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load (bits/seg)
Best Effort	171,16	1000	647,22	1,64	0,27	0,72606	702666,6
Background	52,82	1000	648,16	1,64	0,24	0,72685	702160
Standard	52,82	1000	647,22	1,64	0,27	0,72606	702666,6
Excellent Effort	52,82	1000	647,22	1,64	0,27	0,72606	702666,6
Streaming Multimedia	52,82	1000	647,22	1,64	0,27	0,72606	702666,6
Interactive Multimedia	52,82	1000	647,22	1,64	0,27	0,72606	702666,6
Interactive Voice	52,82	1000	647,22	1,64	0,27	0,72606	702666,6
Reserverd	52,82	1000	647,22	1,64	0,27	0,72606	702666,6

B.12 Resultados de la simulación de la topología 2, H.323 – ToS

ToS	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load (bits/seg)
Best Effort	27,777	48000	29600	2,711	0,7602	1,383	995,55
Background	27,777	48000	29600	2,711	0,7602	1,383	995,55
Standard	27,777	48000	29600	2,711	0,7602	1,383	995,55
Excellent Effort	27,777	48000	29600	2,711	0,7602	1,383	995,55
Streaming Multimedia	27,777	48000	29600	2,711	0,7602	1,383	995,55
Interactive Voice	27,777	48000	29600	2,711	0,7602	1,383	995,55
Reserverd	27,777	48000	29920	2,337	0,552	1,252	995,55

B.13 Resultados de la simulación de la topología 1, H.323 – QoS

QoS	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay (seg)	Load (bits/seg)
FIFO	10,55	1500	964,44	2,75	0,55	1,38	931733,33
WFQ	27,77	1500	908,88	2,7	0,62	1,36	935466,66
Priority Queuing	10,55	1500	944,44	2,41	0,5	1,21	935466,66
Custom Queuing	10,55	1500	964,44	2,75	0,55	1,38	931733,33
MWRR	10,55	1500	964,44	2,759	0,55	1,38	931733,33
DWRR	10,55	1500	964,44	2,75	0,55	1,38	931733,33
MDRR	10,55	1500	964,44	2,758	0,55	1,38	931733,33

B.14 Resultados de la simulación de la topología 2, H.323 – QoS

QoS	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load (bits/seg)
FIFO	8,88	48000	48000	0,0025	2,173E-06	0,00104	1444426
WFQ	20,55	48000	47946	0,0019	1,461E-06	0,00074	1444160
Priority Queuing	8,88	48000	48000	0,0024	2,183E-06	0,00091	1444160
Custom Queuing	20,55	48000	47946	0,0024	1,461E-06	0,00074	1444160
MWRR	8,88	48000	48000	0,0024	2,183E-06	0,00091	1444160
DWRR	8,88	48000	48000	0,0024	2,183E-06	0,00091	1444160
MDRR	8,88	48000	48000	0,0024	2,183E-06	0,00091	1444160

B.15 Resultados de la simulación de la topología 1, SIP – N. Nodos

Nodos	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load (bits/seg)
3	0,02	1500	936,66	2,72	0,529739379	1,3717285	930666
6	11,24	1750	398,33	3,9	1,265127006	1,7237536	909866
12	31,44	2605	447,77	6,37	2,646151746	3,09550492	915466

B.16 Resultados de la simulación de la topología 1, H.323 – N. Nodos

Nodos	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load (bits/seg)
3	27,77	150	150	0,011390445	0,01141563	0,00377936	835200
6	55,55	300	299,44	0,016254715	0,016091104	0,00587609	1668853
12	114,44	600	188,88	2,309631476	3,056237692	1,46029866	1964266

B.17 Resultados de la simulación de la topología 2, SIP – N. Nodos

Nodos	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load (bits/seg)
3	0,0148564	60	60	0,011333395	8,848E-09	0,00411586	410880
6	0,0339456	120	120	0,01212942	1,3283E-07	0,00451274	821760
12	0,022229	240	240	0,022397738	5,4795E-05	0,00966555	1640096

B.18 Resultados de la simulación de la topología 2, H.323 – N. Nodos

Nodos	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay (seg)	Load (bits/seg)
3	23,333333	150	150	0,010950243	1,54365E-06	0,00404	835200
6	39,666667	300	299,666667	0,013957439	8,11593E-06	0,00543	1670400
12	66,666667	600	138,333333	3,104062056	1,570883852	0,90850	1965813

B.19 Resultados de la simulación de la topología 1, SIP – VPN

VPN	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay (seg)	Load (bits/seg)
Con VPN	0,0238	50000	45050,66	0,883	0,147174711	1,3717285	1061528,94
Sin VPN	0,0133	48000	36986,66	0,874	0,0726	0,3100256	862576

B.20 Resultados de la simulación de la topología 1, H.323– VPN

VPN	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay (seg)	Load (bits/seg)
Con VPN	27,777	52000	45050,66	0,053606159	1,053505714	0,14168406	959445
Sin VPN	23,333	48000	35496,66	0,011390445	0,141684061	0,00377936	760916

B.21 Resultados de la simulación de la topología 2, H.323– VPN

VPN	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load(bits/seg)
Con VPN	0,0238	50000	47050,66	0,883	0,147174711	1,3717285	1061528,94
Sin VPN	0,0133	48000	36986,66	0,874	0,0726	0,3100256	862576

B.22 Resultados de la simulación de la topología 2, H.323– VPN

VPN	Call Setup (seg)	trafico enviado (bytes)	Trafico recibido (bytes)	Packet End-to-End Delay (seg)	Packet Delay Varation	Delay(seg)	Load(bits/seg)
Con VPN	27,777	52000	47050,66	0,053606159	1,053505714	0,14168406	959445
Sin VPN	23,333	48000	36986,66	0,011390445	0,141684061	0,00377936	760916

C APÉNDICE C: INSTALACIÓN DEL PROGRAMA IT-GURU.

C.1 Obtención de licencia del programa IT-GURU

La pagina oficial de Opnet es www.opnet.net ahí tenemos que regístranos para poder obtener el instalador del producto IT-Guru que es la versión estudiantil de Opnet. Para registrarnos nos vamos a la página:

https://ds1.opnet.com/4dcgi/AUTH_Login

En esta página nos pide el usuario y el password. Ahí hay que hacer clic en el hipervínculo de la derecha que nos ayuda a registrar a usuarios nuevos

Figura C.1-1. Ventana para ingresar usuario y password en OPNET

Luego nos aparece una ventana que sugiere los diferentes problemas para logoneamos. En la primera opción que dice que somos nuevos usuarios, damos clic en PASSWORD REQUEST, y se muestra una ventana que requiere de llenar algunos datos como: nombre, e-mail y el producto que deseamos descargar.

Figura C.1-2. Ventana para registrar nuevo usuario en OPNET

Después nos llega un mail con los siguientes datos

```
THANK YOU FOR REGISTERING WITH OPNET TECHNOLOGIES.

Please use the username and password below to download OPNET IT
Guru
```

Academic Edition.

username galitorafael
password mqt5m8pr

Please save your username and password because you will need them to access
important information on OPNET's website, including the web pages
referenced below.

If you do not already have the IT Guru Academic Edition installer, download
the software from here:
http://www.opnet.com/itguru-academic/download.html

Once you have downloaded the installer, run it to install the software.
Then run the software, which will guide you through the product activation
process.

For additional information related to IT Guru Academic Edition, including
FAQs:
http://www.opnet.com/itguru-academic/home.html

About IT Guru Academic Edition
OPNET IT Guru Academic Edition provides a virtual environment for modeling,
analyzing, and predicting the performance of IT infrastructures, including
applications, servers, and networking technologies. Based on OPNET's
award-winning IT Guru product, Academic Edition is designed to complement
specific lab exercises that teach fundamental networking concepts. The
commercial version of IT Guru has broader capabilities designed for the
enterprise IT environment, documentation, and professional support. OPNET
software is used by thousands of commercial and government organizations
worldwide, and by over 500 universities.

About OPNET Technologies Inc.
Founded in 1986, OPNET Technologies is the pioneer and leading provider of
Intelligent Network Management software. For more information about OPNET,
please visit us online at www.opnet.com <http://www.opnet.com/>
.

Please do not reply to this automated email message. If you have questions
about OPNET IT Guru Academic Edition, please use the resources available

from the following website: http://www.opnet.com/itguru-academic/home.html

El username y el password se utilizan para obtener la licencia para poder hacer que funcione el IT-Guru, que dura 3 meses y puede ser renovanada.

Para la instalación del IT-Guru se hace doble clic sobre el instalador "ITG_Academic_Edition_v1995.exe" y se sigue los pasos del wizard.

Para la obtención de la licencia del IT-Guru version academica es necesario estar conectado a Internet y Los pasos para la instalacion son:

C.2 Pasos para la instalación del programa IT-GURU

Paso 1.

Iniciar IT Guru Academic Edition

Paso 2.

Clic en el botón "License Management"

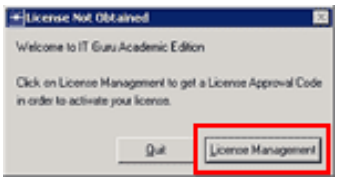


Figura C.2-1. Ventana para obtener licencia de IT-GURU

Paso 3.

Clic en el botón “Next”

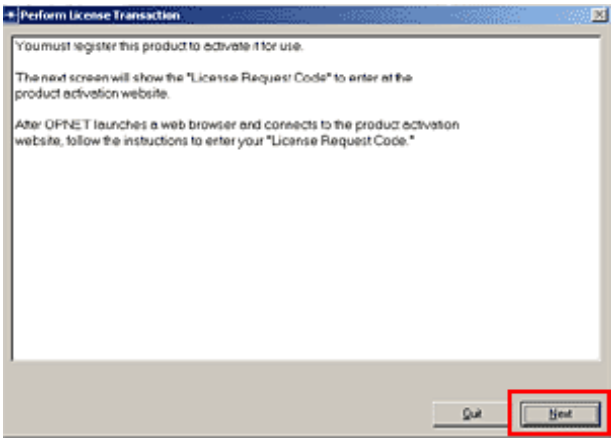


Figura C.2-2. Ventana de explicación para obtener licencia de IT-GURU

Paso 4.

Ingresar el User Name y el Password en la ventana de dialogo que aparece y hacer clic en OK

Figura C.2-3. Ventana para obtener licencia de IT-GURU

Paso 5.

Genera un “License Request Code” hacer clic en el botón copy to clipboard

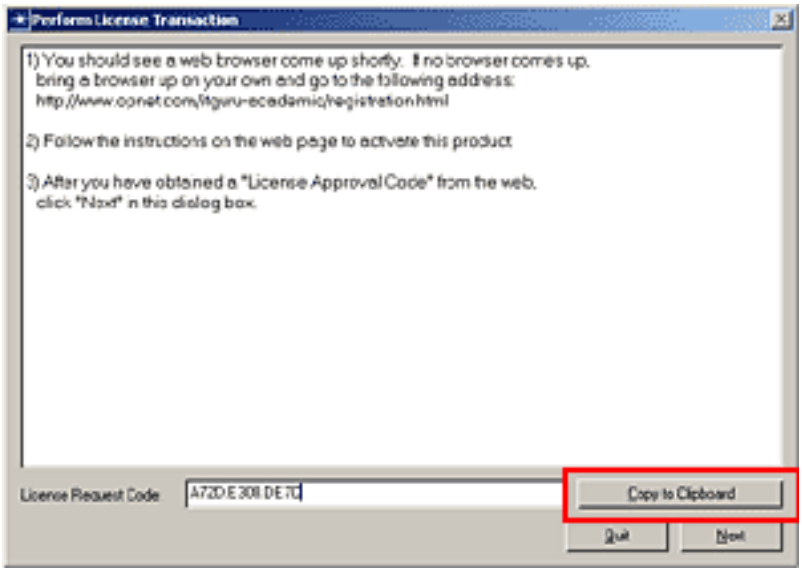


Figura C.2-4. Ventana de generación de código.

Paso 6.

Pegar el “License Request Code"

Paso 7.

Clic en el botón Submit

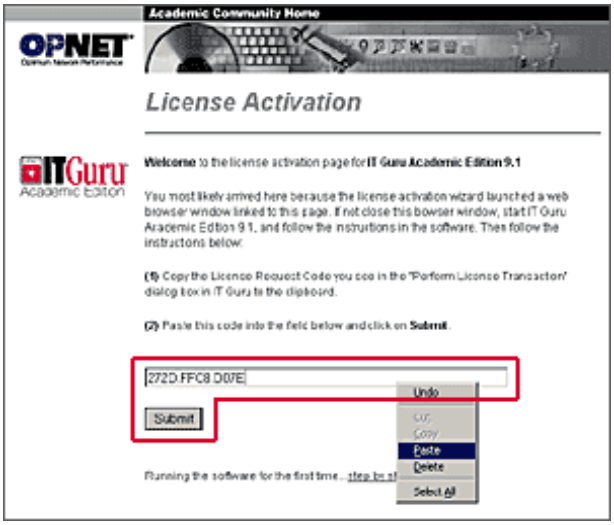


Figura C.2-5. Pegar código generado

Paso 8.

En nuestro browser copiar el código de aprobación

Figura C.2-6. Código de activación del programa IT-GURU.

Paso 9.

En el IT Guru Academic Edition, clic en el boton Next

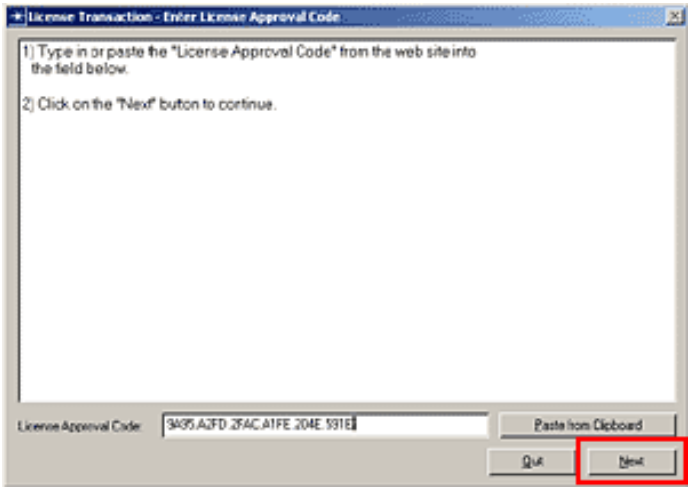


Figura C.2-7. Continuación de la activación de IT-GURU

Paso 10.

En el IT Guru Academic Edition, clic en el boton Paste from Clipboard

Paso 11.
Clic en le boton Next

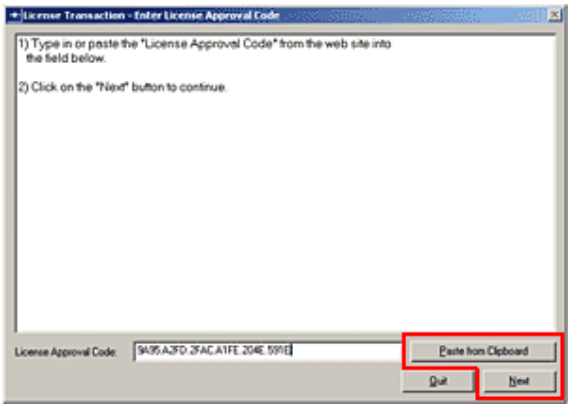


Figura C.2-8. Pegar Código de activación.

Paso 12.

Clic en el boton Close

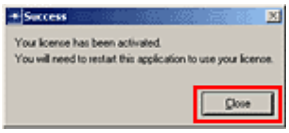


Figura C.2-7. Ventana fianal de activación.

Paso 13.

Reiniciar IT Guru Academic Edition

D APÉNDICE D: CONFIGURACIÓN DE LOS NODOS PARA LA SIMULACIÓN.

D.1 Configuración para SIP

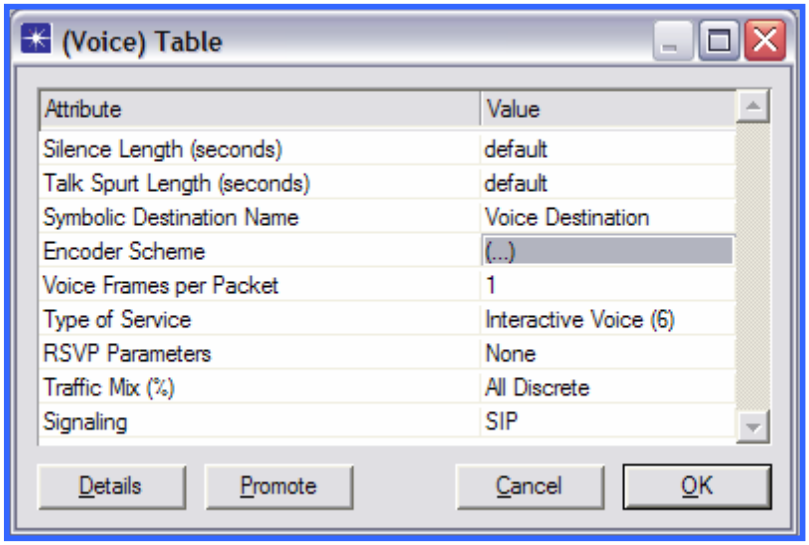


Figura D.1-1. Configuración de la definición de Aplicación – SIP.

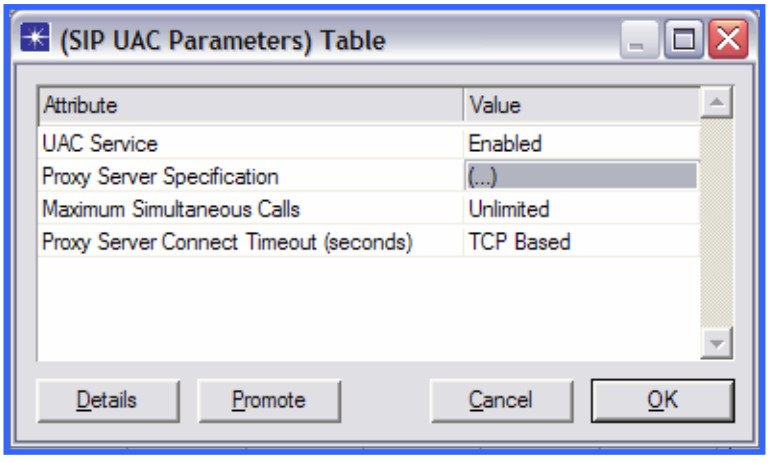


Figura D.1-2. Configuración de los terminales - SIP.

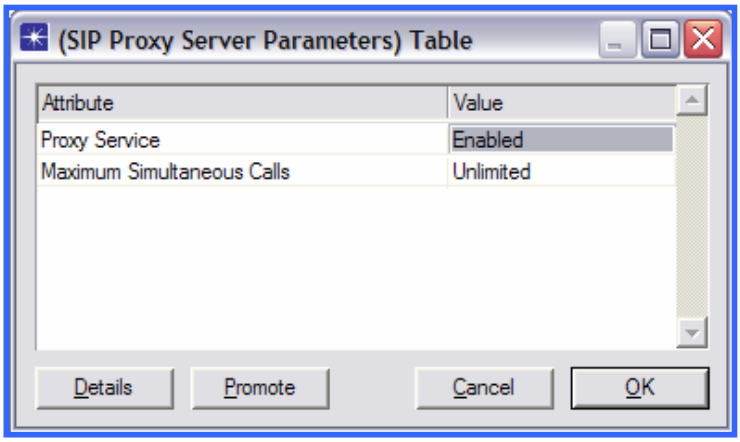


Figura D.1-1. Configuración del servidor Proxy – SIP.

D.2 Configuración para H.323

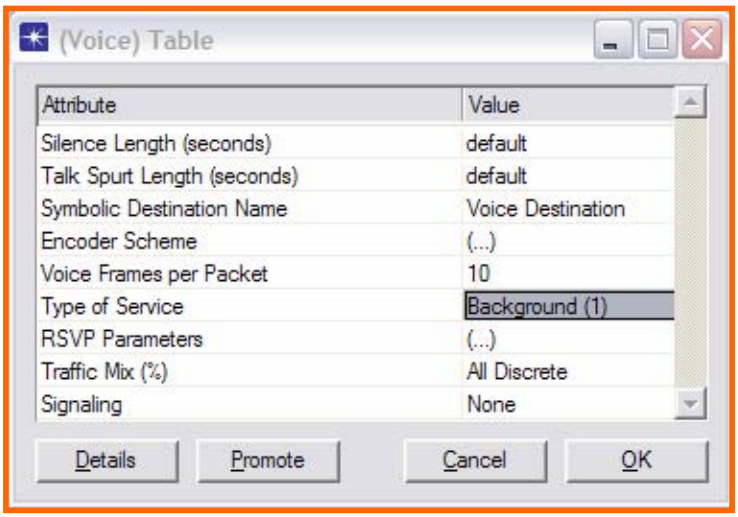


Figura D.2-1. Configuración de la definición de Aplicación –H.323.

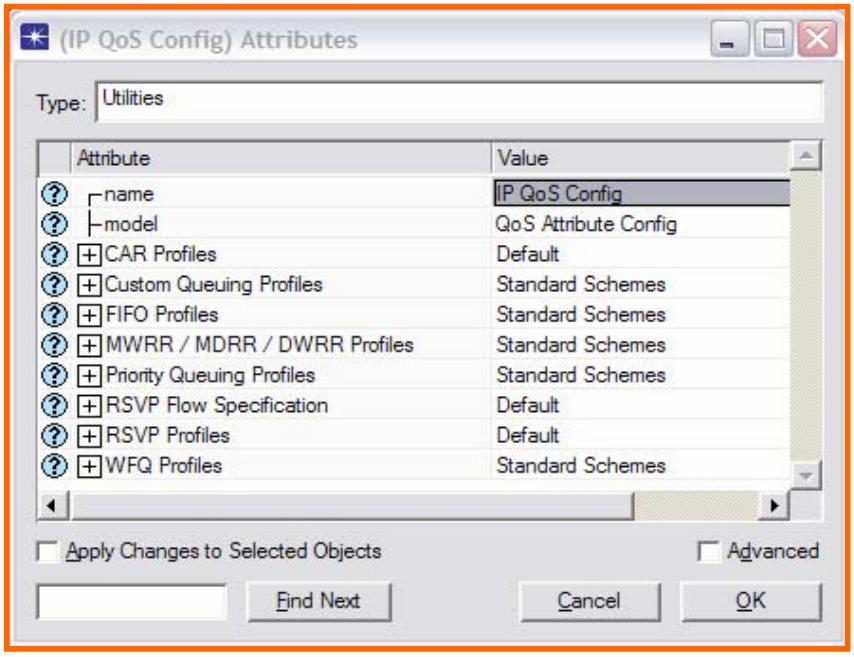


Figura D.2-2. Configuración del protocolo RSVP en los Atributos – H.323.

Interfases de los nodos

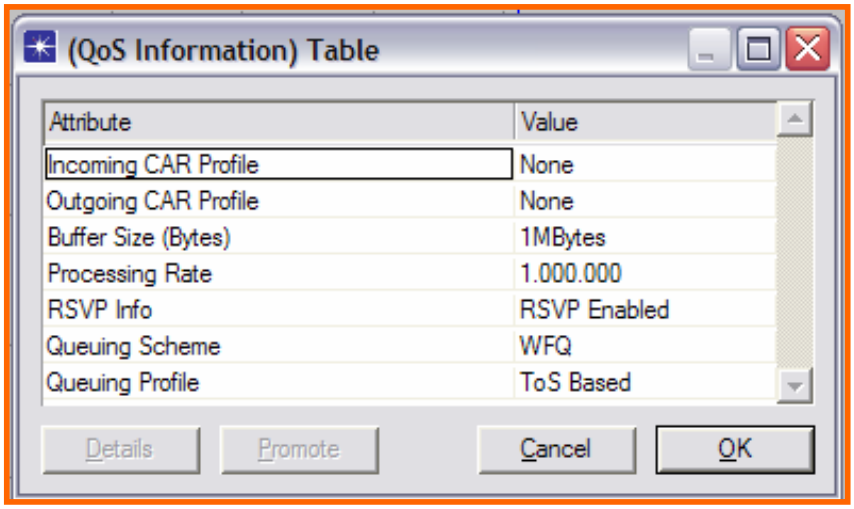


Figura D.2-3. Configuración del protocolo RSVP en el nodo – H.323.

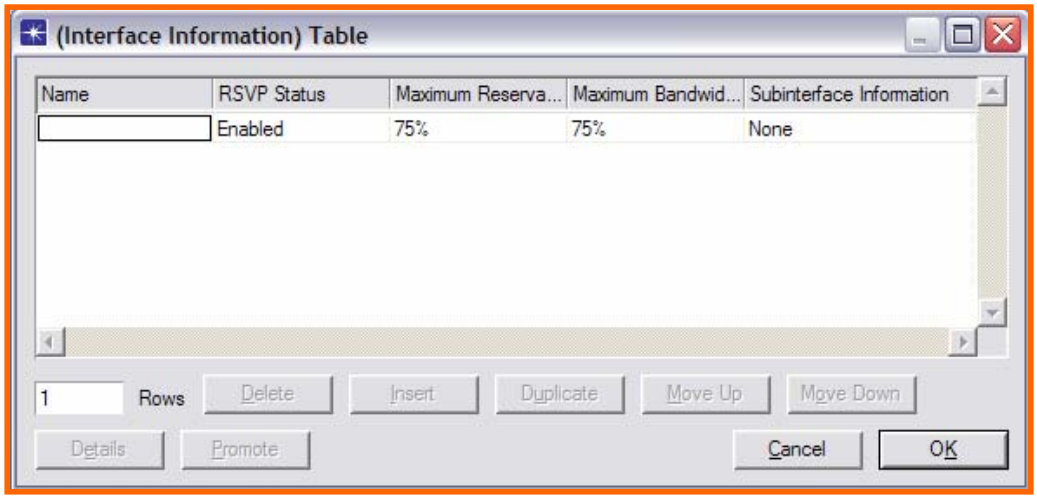


Figura D.2-2. Configuración del protocolo RSVP en las interfaces – H.323.

E APÉNDICE E: CONFIGURACIÓN DEL PROYECTO OPENH.323

Los programas que se necesitan para correr el cliente H.323 se encuentra en la pagina http://www.openh323.org/code.html.

Se necesita todos los programas de la tabla, y el programa a ejecutar el OpenPhone (tener en cuenta que todos los archivos deben estar en la misma carpeta).

Tabla E-1. Programas necesarios para ejecutar el cliente OpenH323

Programa	Descripción	Requerimientos
OpenH323 DLL libraries	librerías compartidas	
OpenPhone	GUI basado en cliente H.323.	
OhPhone	Línea de comando del cliente H.323.	PWLib DLL libraries, OpenH323 DLL libraries
OpenMCU	Servidor de Conferencia H.323.	PWLib DLL libraries, OpenH323 DLL libraries
OpenAM	Maquina de respuesta de H.323.	PWLib DLL libraries, OpenH323 DLL libraries
OpenIVR	Respuesta Interactive Voice de H.323.	PWLib DLL libraries, OpenH323 DLL libraries
OpenGK	Gatekeeper H.323.	PWLib DLL libraries, OpenH323 DLL libraries
PSTNGw	PSTN gateway	PWLib DLL libraries, OpenH323 DLL libraries
CallGen323	Generador de llamada H.323.	PWLib DLL libraries, OpenH323 DLL libraries

F APÉNDICE F: CONFIGURACIÓN DEL GNU GATEKEEPER.

El programa ejecutable se lo puede bajar de la página:

http://www.gnugk.org/h323download.html

Se escoge la versión para Windows, para el proyecto se uso GNU Gatekeeper Versión 2.2.3-2

El ejecutable del archivo se encuentra en la carpeta:

\gnugk-2.2.3-2-win32-x86\gnugk-2.2.3-win32-x86\contrib\winsvc

En esa carpeta hay que copiar el archive “gnugk.exe”, que se encuentra en la carpeta:

\gnugk-2.2.3-2-win32-x86\gnugk-2.2.3-win32-x86\bin

Dentro de esa carpeta hay que crear el archive de configuración “gatekeeper.ini” su configuración es:

```
#Gatekeeper.ini

[Section String]
Key Name=Value String


[Gatekeeper::Main]

Fourtytwo=42
#Default: N/A

Name=OpenH323GK_Galo
#Default: OpenH323GK
```

```
Home=192.168.0.249
#Default: 0.0.0.0

#El gatekeeper escuchará por peticiones desde esta dirección IP.
#Por defecto, el gatekeeper escucha desde todas las #interfaces
#de sus equipos. Usted puede quitar esta opción a menos que
#usted desee que el gatekeeper esté escuchando #desde
#direcciones específicas. Múltiples direcciones pueden agregarse
#separadas por punto y coma (;) o coma (,).

#NetworkInterfaces=192.168.1.1/24,10.0.0.1/0
#Default: N/A

#Aquí se especifica las interfaces de red del gatekeeper. Por
#defecto el gatekeeper detectará las interfaces de sus #equipos
#automáticamente. Existen dos situaciones en las que usted
#podría usar esta opción. Una es en el caso de que #la detección
#automática fallara y la otra cuando el gatekeeper esta detrás
#de un NAT box y permite a endpoints con #claves públicas
#registrarse con el gatekeeper.
#EndpointIDSuffix=_gk1
#Default: _endp

#El gatekeeper asignará un único identificador a cada endpoint
#registrado. Esta opción puede ser usada para #especificar un
#sufijo y añadirlo al identificador del endpoint. Esto es muy
#utilizado solamente cuando se utiliza #más de un gatekeeper.

#TimeToLive=300
#Default: -1


#Esta opción le permite redireccionar endpoints hacia gatekeeper
#alternos cuando el gatekeeper se sobrecarga. Por #ejemplo, en
#la configuración anterior, el gatekeeper rechazará un RRQ si
#los endpoints registrados sobrepasan los #100 o rechazará un
#ARQ si las llamadas actuales sobrepasan las 50. Además, usted
#puede redireccionar todos los #endpoints de manera explícita
#configurando esta opción ya sea de manera temporal o
#permanente. #El gatekeeper #devolverá un mensaje de rechazo RAS
#con una lista #de gatekeepers alternos definida en
#AlternateGks. Debe tener #presente que un redireccionamiento
#permanente significa que los endpoints redireccionados no se
#registrarán #nuevamente con este gatekeeper. Además tenga en
#cuenta que esta función solamente tiene efecto con el estándar
#H323 #versión 4.

#AlternateGKs=1.2.3.4:1719:false:120:OpenH323GK
#Default: N/A

#Este es el puerto de estado para monitorear el gatekeeper. Ver
#this section para más detalle.
StatusTraceLevel=2


[GkStatus::Auth]
```

```
#En esta sección se definen un número de reglas para determinar
#quienes están permitidos de conectarse al gatekeeper #vía
#puerto de estado (vía telnet). Quien quiera que tenga acceso al
#puerto de estado tiene un control completo #sobre el
#gatekeeper. Asegúrese de que ésta sección esté configurada
#correctamente.

rule=allow
#Default: forbid

#      Posibles valores son:
#          o forbid - Prohíbe cualquier conexión.
#          o allow - Permite cualquier conexión.
#          o explicit - Lee el parámetro ip=value donde ip es la
#dirección IP del cliente observado, value puede ser #1,0 o
#allow,forbid o yes,no. Si ip no está en la lista el parámetro
#default es usado.
#          o regex - La IP del cliente se hace corresponder con
la expression regular dada.#
#
#            Ejemplo:
#
#                Para permitir clientes desde 195.71.129.0/24 y
#195.71.131.0/24:
#
#                    regex=^195\.71\.(129|131)\.[0-9]+$
#
#          o password - El usuario tiene un username y password
apropiado para conectarse (login). El formato de
#username/password es el mismo que el de la sección
[SimplePasswordAuth].
#
#      Por otra parte, estas reglas puede ser combinadas por "|"
#o "&". Por ejemplo,
#          o rule=explicit | regex
#            La IP del cliente debe validarse con las reglas
#explicit o regex.
#
#          o rule=regex & password
#            La IP del cliente debe validarse con las reglas
regex, y el usuario tiene que conectarse con un #username y
password.
#
#    * default=allow
#      Default: forbid
#
#      Esta opción es utilizada solamente cuando rule=explicit.
#
#    * Shutdown=forbid
#      Default: allow
#
#      Esta opción es utilizada para especificar si se permite o
no apagar el gatekeeper vía puerto de estado.
#
#    * DelayReject=5
#      Default: 0
#
#      Esta opción especifica que tiempo (en segundos) se debe
#esperar antes de rechazar un username / pa s sword #inválido.
```

```
#[Gatekeeper::Auth]
#FileIPAuth=required;Setup
#authrule=authrule

#[FileIPAuth]
#include=/accesslist.ini
```

G APÉNDICE D: RESULTADOS DE LAS PRUEBAS DE CAMPO.

G.1 Resultados de la estación 1 y estación 2 para SIP

Estación 1 caller	Recibidos
Duración	45min
Total de Paquetes	28635
Total bytes	9541834
Utilización Promedio (Bit/sec)	192593
Data (bytes)	7431052
RTTP (bytes)	555912
RTCP (bytes)	468
h225 (bytes)	2214

Estación 2 callee	Recibidos
Duración	45min
Total de Paquetes	34094
Total bytes	9459457
Utilización Promedio (Bit/sec)	182151
Data (bytes)	7770924
RTTP (bytes)	485154
RTCP (bytes)	5928
h225 (bytes)	4919

G.2 Resultados de la estación Prueba1 y prueba2 para H.323

Estación 1 caller	Recibidos
Duración	45min
Total de Paquetes	35751
Total bytes	9427958
Utilización Promedio (Bit/sec)	437058
Data (bytes)	6143162
RTTP (bytes)	448223
RTCP (bytes)	1456
h225 (bytes)	743

Estación 2 callee	Recibidos
Duración	45min
Total de Paquetes	43656
Total bytes	9.301.404
Utilización Promedio (Bit/sec)	452100
Data (bytes)	7312736
RTTP (bytes)	552245
RTCP (bytes)	6344
h225 (bytes)	314

G.3 Resultados de la estación 3 y estación 4 para SIP

Estación 3 caller	Recibidos
Duración	45min
Total de Paquetes	29548
Total bytes	9630252
Utilización Promedio (Bit/sec)	262545
Data (bytes)	7653414
RTTP (bytes)	485647
RTCP (bytes)	1845
h225 (bytes)	1452

Estación 4 callee	Recibidos
Duración	45min
Total de Paquetes	35704
Total bytes	9521560
Utilización Promedio (Bit/sec)	214582
Data (bytes)	7725444
RTTP (bytes)	7770924
RTCP (bytes)	3576
h225 (bytes)	1500

G.4 Resultados de la estación 3 y estación 4 para H.323

Estación 3 caller	Recibidos
Duración	45min
Total de Paquetes	38552
Total bytes	9862148
Utilización Promedio (Bit/sec)	457504
Data (bytes)	7034570
RTTP (bytes)	543211
RTCP (bytes)	1456
h225 (bytes)	745

Estación 4 callee	Recibidos
Duración	45min
Total de Paquetes	45265
Total bytes	9548614
Utilización Promedio (Bit/sec)	500002
Data (bytes)	7342536
RTTP (bytes)	465213
RTCP (bytes)	4936
h225 (bytes)	325

G.5 Resultados de la estación 5 y estación 6 para SIP

Estación 5 caller	Recibidos
Duración	45min
Total de Paquetes	27547
Total bytes	9715254
Utilización Promedio (Bit/sec)	154000
Data (bytes)	7422247
RTTP (bytes)	545713
RTCP (bytes)	634
h225 (bytes)	2214

Estación 6 callee	Recibidos
Duración	45min
Total de Paquetes	34578
Total bytes	9569256
Utilización Promedio (Bit/sec)	163555
Data (bytes)	7442122
RTTP (bytes)	435754
RTCP (bytes)	5530
h225 (bytes)	4919

G.6 Resultados de la estación 5 y estación 6 para H.323

Estación 5 caller	Recibidos
Duración	45min
Total de Paquetes	45247
Total bytes	9884528
Utilización Promedio (Bit/sec)	444000
Data (bytes)	7283421
RTTP (bytes)	403558
RTCP (bytes)	3568
h225 (bytes)	587

Estación 6 callee	Recibidos
Duración	45min
Total de Paquetes	52471
Total bytes	9301404
Utilización Promedio (Bit/sec)	447028
Data (bytes)	7127656
RTTP (bytes)	568215
RTCP (bytes)	5421
h225 (bytes)	564

G.7 Resultados de la estación 7 y estación 8 para SIP

Estación 7 caller	Recibidos
Duración	45min
Total de Paquetes	30345
Total bytes	9043465
Utilización Promedio (Bit/sec)	182492
Data (bytes)	7102435
RTTP (bytes)	423415
RTCP (bytes)	608
h225 (bytes)	2.164

Estación 8 callee	Recibidos
Duración	45min
Total de Paquetes	32025
Total bytes	9135562
Utilización Promedio (Bit/sec)	192341
Data (bytes)	7345452
RTTP (bytes)	452558
RTCP (bytes)	4256
h225 (bytes)	4652

G.8 Resultados de la estación 7 y estación 8 para H.323

Estación 7 caller	Recibidos
Duración	45min
Total de Paquetes	33457
Total bytes	9534556
Utilización Promedio (Bit/sec)	395044
Data (bytes)	7214363
RTTP (bytes)	446436
RTCP (bytes)	1447
h225 (bytes)	756

Estación 8 callee	Recibidos
Duración	45min
Total de Paquetes	36313
Total bytes	9574234
Utilización Promedio (Bit/sec)	409565
Data (bytes)	7434556
RTTP (bytes)	433664
RTCP (bytes)	6464
h225 (bytes)	359

BIBLIOGRAFÍA

[REF.1] Tim Brans, Thomas De Keyser, Chistopher Peirs y Sofie Pollin. "Voice over IP." Diciembre 17, 2001.

[REF.2] Mohan krishna y Liam kilmartin. "Investigation into the impact of key exchange mechanisms for security protocols in VoIP networks." Noviembre 7, 2001.

[REF.3] Mona Habid y Nirmala Bulusu. "Improving QoS of VoIP over WLAN (IQ-VW)." Enero 5, 2003.

[REF.4] "How Gatekeeper, Terminals and Gateways works together." Cisco Gatekeeper External Internal Reference, Version 3.1. Septiembre 26, 2002

[REF.5] C. Schlatter. "Basic Architecture of H.323." Febrero 25, 2003.

[REF.6] "Voice Over Internet Protocol" The International Engineering Consortium. http://www.iec.org, 2005.

[REF.7] Mohan Krishna Ranganathan, Liam Kilmatin. “Investigation into Impact of Security Protocols in Session Initiation Protocol (SIP) based VoIP Networks.” Octubre 17, 2001.

[REF.8] http://europe.nokia.com/BaseProject/Sites/NokiaCom_CAMPAIGNS_57710/CDA/Categories/NokiaArchitectureUpdate/ArchitectureFrameworks/SIP/_Content/_Static_Files/sip_proxy_network.jpg

[REF.9] Rodolfo Castañeda Segura, Director de Telemática. CICESE. “Protocolo para voz IP.” Enero, 2001

[REF.10] “El estándar VoIP – Voz sobre IP –.“ Junio, 2005. http://www.comunicaciones.unitronics.es/tecnologia/voip.html

[REF.11] William A. Arbaugh, Narender Shankar, Y.C. Justin Wan, Department of Computer Science University of Maryland. “Your 802.11 Wireless Network has No Clothes.” Marzo 30, 2001.

[REF.12] Adbel Nasir Alshamsi, Taakamichi Saito. Tokyo University of Techbology. “A Technical Comparison of IPSec and SSL.” Marzo 30, 2005.

[REF.13] Makarand Bhagwat. “Security in SIP.” Marzo 3, 2004.

[REF.14] Federico Montesino Pouzols, Iris-MMEDIA. “Session Initiation Protocol.” Mayo 2003.

[REF.15] Espiñeira, Sheldon y Asociados. “VoIP: Seguridad y continuidad del Servicio.” Abril 25, 2006.

[REF.16] “Enterprise VoIP Security Best Practices.” Jupiter Networks, Inc. Marzo, 2006.

[REF.17] Amarandei-Stavile Michai. ”Voice over IP Security a Layered Approach.” Marzo 20, 2006.

[REF.18] “VoIP Protection, Guaranteeing Security and Availability of VoIP Services with Network Intrusion Prevention System.” Marzo 17, 2005. www.toplayer.com

[REF.19] “IPSec vs. SSL: Why Choose? Remote VPN Access for Anywhere.” Junio 21, 2003. www.openreach.com

[REF.20] Rie Fujita, Hiroki Shimabara, Hideki Tode, Toshihiro Masaki, Koso Murakami. Graduate School of information science and Technology, Asake University. “QoS Control Écheme Guaranteeing the Delay, Jitter and Throughput in the IP Router.” Noviembre 4, 2004.

[REF.21] "Estándar 802.11." Laboratorio de comunicaciones Digitales. Noviembre 2004.

[REF.22] Pablo Garaziar Sagarminaga. "Seguridad en Redes Inalámbricas 802.11 a/b/g, protección y vulnerabilidad." Marzo 24, 2005.

[REF.23] "Security Technologies, Security Issues When Connecting to the Internet." Febrero 20, 2005. www.cisco.com.

[REF.24] Alfonso Araujo Cárdenas. "Redes y sus Topologías." Junio 5, 2004. http://mx.geocities.com/alfonsoaraujocardenas/topologias.html

[REF.25] David Arrowsmith, Mario di Bernardo y Francesco Sorrentino. "Effects of variations of load distrubution on network performance." 31 de Marzo de 2005.

[REF.26] J. Postel, Network Working Group. "Service Mappings." Septiembre 1981.

[REF.27] Ermanno Pietrosemoli, Latin American Networking School (Fundación EsLaRed) – ULA. "Voice Over IP." Febrero 2004.

[REF.28] J. Touch, Proceedings of ACM SIGCOMM '95, Comp. Comm. Review, Vol. 25, No. 4, pp. 77-86. "Performance analysis of MD5." 1995.

[REF.29] Schneier, John Wiley & Sons, Inc. pp 279. “Applied Cryptography.” 1996.

[REF.30] Armando F. Lima. “IP Telephony y NGN.” 2002.