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

Galo Iturralde Orellana.[1], Cristina Abad Robalino.[2]
[1]Estudiante de la FIEC carrera Ingeniería en Computación
[2]Di Ingeniera en Sistemas Computacionales, 1999 (UCSG) Master of Science in Computer Science, 2003 (University of Illinois at Urbana-Champaign).
Profesora Auxiliar con nombramiento desde Octubre de 2004.
e-mail: giturral@fiec.espol.edu.ec, cabad@fiec.espol.edu.ec
Telf.: (04) 2274-099

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.

Palabras Clave: *VoIP, H.323, SIP, Codec, OPNET.*

Abstract

Actually we can find variety of information on the transference of voice over IP (VoIP) and of how implementing this technology, but very little information with respect to how obtaining that these transmissions are safe or of how could be improved their quality. The emphasis is centered generally in as we obtained a functional installation.

This subject faces this problem analyzing both protocols more common in the voice transmission on IP: the H.323 protocol and protocol SIP, comparing its yield in wireless clients and the securities that offer. This way the basic criteria are offered on voice transference on efficient and safe IP.

Key words: *VoIP, H.323, SIP, Codec, OPNET.*

1. 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.
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 mayor rendimiento para ser usados en las pruebas de campo.

Teniendo los parámetros de las simulaciones se configura ocho computadoras conectadas inalambricamente 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 y poder dejar pautas para crear nuevos estudios.

[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.

3. 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.

4. 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 de paquetización, la variación de retardo y la pérdida de paquetes

5. Componentes de una red VoIP

En general una red VoIP esta compuesta por cuatro 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, y los terminales. [1]

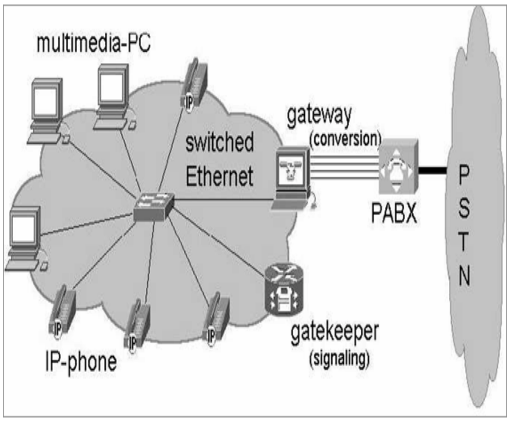

Figura 5-1. Componentes básicos de una red VoIP

6. Protocolo H.323

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).

7. Pila H.323

Los electos que intervienen en el protocolo H.323 se muestran a continuación

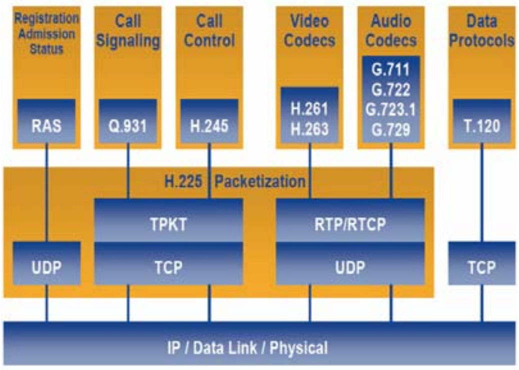

Figura 7-1. Pila del Protocolo H.323

8. Protocolo SIP

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 [5].

9. Arquitectura

En el protocolo SIP se puede encontrar cuatro componentes básicos: user agents (UA), registrars, proxy y redirect servers.

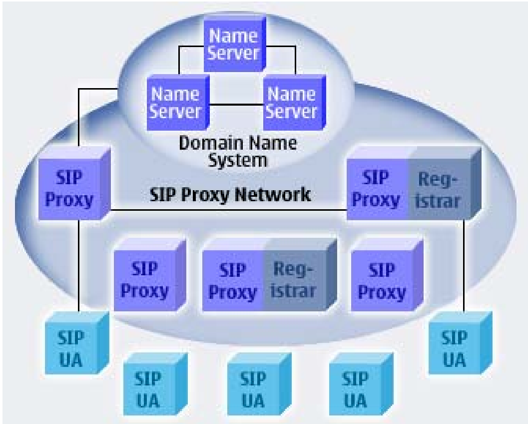

Figura 9-1. Flujo de mensajes SIP

10. Diferencia entre SIP y H.323

Entre las diferencias que podemos encontrar tenemos:

- 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.
- H.323 define mecanismos de gestión y administración de la red.
- En la arquitectura SIP, funciones y servicios como garantía de calidad, directorio o descripción de sesiones, son ortogonales.
- 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[3] ha adoptado SIP como protocolo de señalización.
- Desde las primeras versiones, el inicio de llamadas es más rápido con SIP.**¡Error! No se encuentra el origen de la referencia.**

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

11. 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.

Algunos tipos de seguridades inalámbricas:

- WEP
- RAIUS
- SSL

12. 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. [3][1]

13. 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.[1]

14. Topología celda o celular

La topología tipo celda o celular es una de las dos topologías usadas 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 otra topología de tipo estrella.

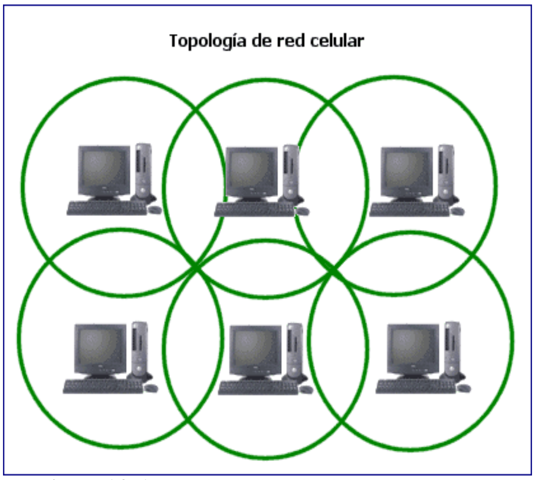

Figura 14 -1. Topología de red celular ¡Error! No se encuentra el origen de la referencia.

13. OPNET

El simulador que uso es el OPNET. Este 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.

14. 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

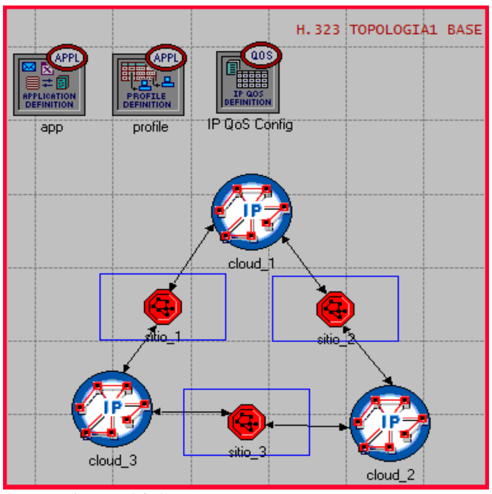

Figura 14-1. Diseño topología 1 con H.323

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

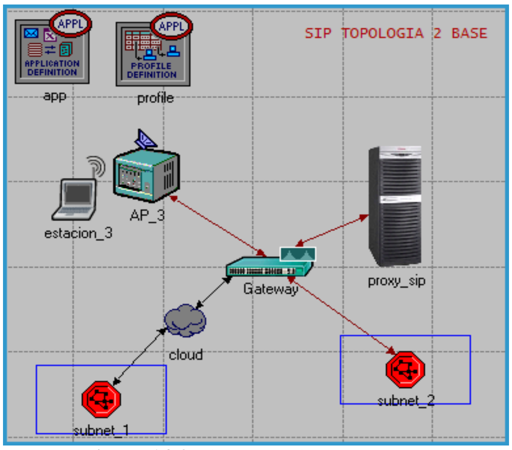

Figura 14-2 Diseño topología 2 con SIP

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.

15. 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 y HMAC-MD5 respectivamente).

Tabla 15- I. 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 segundos*

16. Resultados de las Simulación

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

Codec

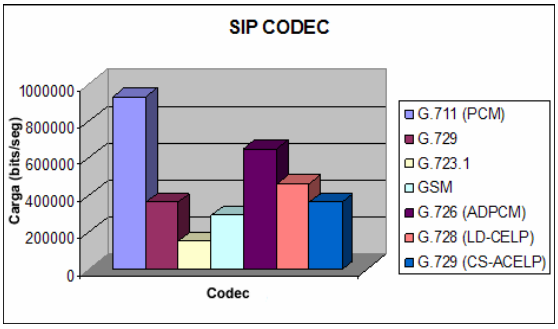

Figura 16-1. Diagrama codec-carga de SIP topología 1

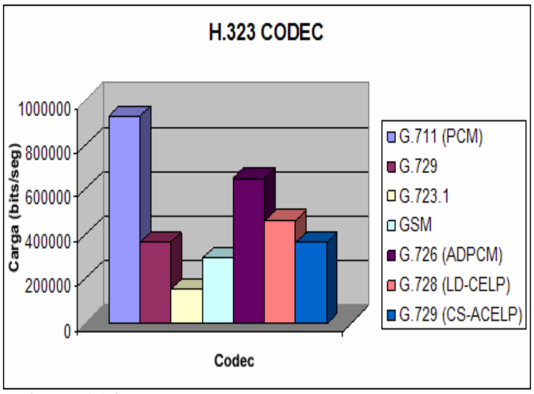

Figura 16-2. Diagrama codec-carga de H.323 topología 1

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 [1]. 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.

17. PRUEBAS DE CAMPO

Diseño del Experimento

El experimento que se realizó se utilizo 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 inalambricamente. 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

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

del protocolo con el programa paketyzer, el cual nos permite evaluar varios parámetros como el jitter, los bytes recibidos y el promedio de utilización del medio.

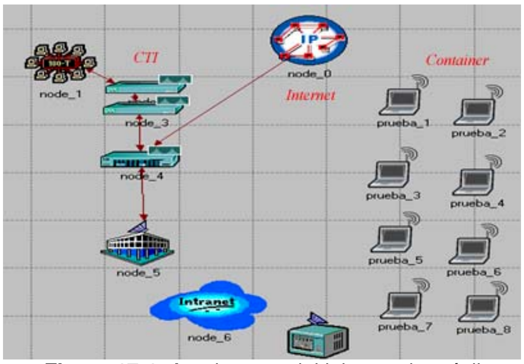

Figura 17-1. Arquitectura del laboratorio móvil

18. 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.

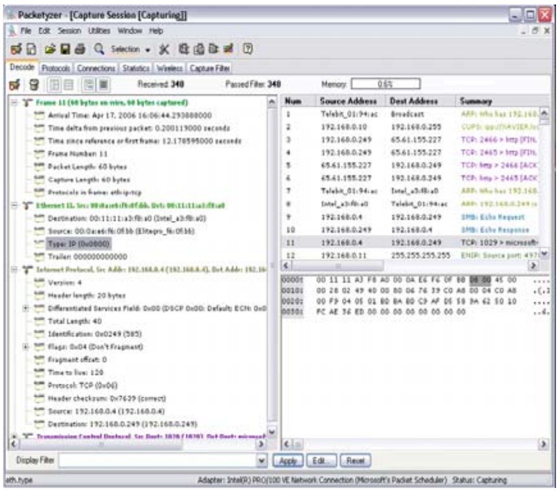

Figura 18-1. Ventana principal del Packetyzer

Dentro de los datos que permite recolectar están:

Tabla 18-I. Parámetros a evaluar en las pruebas de campo.

20. 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.

21. 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 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.

21. Referencia

[1] G Iturralde, “” (Tesis, Facultad de Ingenierria en Computacion, Esuela Superior Politecnica del Litoral, 2006)
[2] Tim Brans, Thomas De Keyser, Chistopher Peirs y Sofie Pollin. “Voice over IP.” (Diciembre 17, 2001)
[3] Mona Habid y Nirmala Bulusu. “Improving QoS of VoIP over WLAN (IQ-VW).” (Enero 5, 2003)
[4] Mohan Krishna Ranganathan, Liam Kilmatin. “Investigation into Impact of Security Protocols in Session Initiation Protocol (SIP) based VoIP Networks.” (Octubre 17, 2001)
[5] Federico Montesino Pouzols, Iris-MMEDIA. “Session Initiation Protocol.” (Mayo 2003)
[6] “IPSec vs. SSL: Why Choose? Remote VPN Access for Anywhere.” Junio 21, 2003. www.openreach.com.
[7] Ermanno Pietrosemoli, Latin American Networking School (Fundación EsLaRed) – ULA. “Voice Over IP.” (Febrero 2004).