ANALISIS COMPARATIVO DE LOS PROTOCOLOS SIP, IAX2 Y H.323 UTILIZADOS EN LA TECNOLOGIA DE VOZ SOBRE IP

CRISTHIAN FABIAN JEREZ CAMARGO
NELSON FABIAN ALDANA PRADA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS
ESCUELA DE INGENIERIA ELECTRICA ELECTRONICA Y TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2013

ANALISIS COMPARATIVO DE LOS PROTOCOLOS SIP, IAX2 Y H.323 UTILIZADOS EN LA TECNOLOGIA DE VOZ SOBRE IP

CRISTHIAN FABIAN JEREZ CAMARGO
NELSON FABIAN ALDANA PRADA

Trabajo de grado para optar al Título de Especialistas en Telecomunicaciones

Director
MIE. WILLIAM ALEXANDER SALAMANCA BECERRA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS
ESCUELA DE INGENIERIA ELECTRICA ELECTRONICA Y TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2013

A DIOS TODOPODEROSO, quien nos provee de sus bendiciones cada día
A mi familia por su apoyo incondicional

Cristhian Fabián

Dedicado a Dios, a mi familia quienes siempre han estado apoyándome en las tareas que emprendo y a mi hija quien es el motor de mi vida.

Nelson Fabián

AGRADECIMIENTOS

Deseamos expresar nuestros sinceros agradecimientos a:

A la Especialización de Telecomunicaciones y sus docentes por su interés en mejorar la calidad y el contenido del programa académico.

A Msc. William Salamanca, por sus aportes su experiencia y conocimiento en este tipo de proyectos y brindarnos las bases y herramientas necesarias en la consecución de este objetivo.

A los compañeros de la especialización.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

RESUMEN

TITULO: ANALISIS COMPARATIVO DE LOS PROTOCOLOS SIP, IAX2 Y H.323 UTILIZADOS EN LA TECNOLOGIA DE VOZ SOBRE IP[*]

AUTORES: Cristhian Fabián Jerez Camargo [**]
Nelson Fabián Aldana Prada

PALABRAS CLAVES: VoIP, SIP, IAX2, H.323, TRAMA, QoS.

DESCRIPCIÓN:

Esta monografía se titula Análisis comparativo de los protocolos SIP, IAX2 y H.323 utilizados en la tecnología de voz sobre ip, la cual presenta el estudio de los protocolos de VoIP, tales como: SIP, IAX2 y H.323

VoIP es un conjunto de protocolos para transporte de voz sobre redes IP. Entorno a este protocolo han surgido diversas herramientas, sistemas y software que son capaces de gestionar comunicaciones con teléfonos digitales, teléfonos analógicos y que proporcionan además las funcionalidades de centralitas PBX hardware, pasarelas con proveedores de servicios VoIP y otras funcionalidades avanzadas.

Los objetivos de este proyecto son: conocer los protocolos SIP, IAX2 y H.323 de VoIP y familiarizarse con sus funcionalidades, características, historia y llevar a cabo una comparación entre dichos protocolos.

H.323 es una gran familia de protocolos que cubren todo lo necesario para el desarrollo de la telefonía sobre IP. Por su parte, SIP tiene capacidades más limitadas, pero está más centrado en las redes IP. IAX es un protocolo de señalización utilizado para manejar conexiones VOIP entre servidores y clientes Asterisk. Las comparaciones se establecen a partir del conocimiento de las tres filosofías, enfocado en la arquitectura y los mecanismos de funcionamiento para proveer los servicios.

Calidad de Servicio nos garantizan la transmisión de cierta cantidad de información en un tiempo dado brinda un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz.

Los principales problemas en cuanto a la calidad del servicio de una red de VoIP, son la **Latencia**, el **Jitter** la pérdida de paquetes y el **Eco**.

[*] Trabajo de Grado

[**] Facultad de Ingenierías Físico-Mecánicas. Escuela de Ingenierías Eléctrica, Electrónica y de Telecomunicaciones. Director: Ing William Salamanca

ABSTRACT

TITLE: COMPARATIVE ANALYSIS OF PROTOCOLS SIP, IAX2 AND H.323 USED IN VOICE OVER IP TECHNOLOGY*

AUTHORS: Cristhian Fabian Jerez Camargo**
Nelson Fabian Aldana Prada

KEYWORDS: VoIP, SIP, IAX2, H.323, TRAMA, QoS

DESCRIPTION

This monograph is titled Comparative Analysis of SIP, IAX2 and H.323 used in Voice over IP technology, which presents the study of VoIP protocols such as SIP, IAX2 and H.323.

VoIP is a set of protocols for transport of voice over IP networks. Around this protocol have been numbers of tools, systems and software that are capable of managing communications with digital phones, analog phones and also provide PBX functionality hardware, gateways with VoIP service providers and other advanced features.

The purposes of this project are: to know SIP, IAX2 and H.323 VoIP and become familiar with its features, characteristics, history and carry out a comparison between these protocols.

H.323 is a family of protocols that cover everything needed for the development of IP telephony. Meanwhile, SIP has more limited capabilities, but is more focused on IP networks.IAX is a signaling protocol used to manage VoIP connections between Asterisk servers and clients. Comparisons are established based on knowledge of the three philosophies, focusing on architecture and operating mechanisms to provide the services.

We guarantee Quality of Service transmitting certain amount of information at a given time provides a good service. It is especially important for certain applications such as streaming video or voice.

The main problems regarding the quality of service of a VoIP network are the Latency, Jitter and packet loss the Echo

* Project of Degree

** Physical-mechanics Engineerings Faculty. Electricity, Electronics and Telecomunication Engineerings School. Eng. William Salamanca

ABREVIATURAS

Abreviatura	Descripción
ATA	Adaptador Telefónico Analógico
DECT	Comunicación Digital Inalámbrica Mejorada
FXO	Foreign Exchange Office
FXS	Foreign Exchange Station
GSM	Sistema Global para Comunicaciones Móviles Global System for Mobile communication
HTTP	(Hyper-text transport Protocol) Es un protocolo de transporte de Hipertexto
H.225	Protocolo de control de llamada que permite realizar una conexión y una desconexión.
H.245	Protocolo que permite el establecimiento y control de una llamada
IAX(2)	Protocolo de Intercambio de Asterisk (versión 2)
IETF	Internet Engineering Task Force Grupo de Trabajo de Ingeniería de la Internet
ITU/UIT	Unión Internacional de Telecomunicaciones International Telecommunications Union
IVR	Respuesta de Voz Interactiva Respuesta Vocal Interactiva Interactive Voice Response
NAT	Traductor de Direcciones de Red Network Address Translator
PBX (PABX)	Centralita Telefónica (Automática) Privada Private (Automatic) Branch Exchange
PCM/MIC	Modulación por Impulsos Codificados Pulse Code Modulation
PSTN/RTB(C)	Red de Telefonía Básica (Conmutada)

	Public Switched Telephone Network
QoS	Calidad de Servicio
	Quality of Service
RAS	Registra el control de admosión, ancho de banda, estado y desconexión.
RDSI	(Red Digital de Servicios Integrados) Red que da soporte a varios canales digitales.
RFC	Documento de Trabajo de Estandarización (Internet)
	Request For Comment
RTP	(Real-time Transport Protocol) Protocolo de Tiempo Real, proporciona servicio de entrega de datos punto a punto.
RTCP	Protocolo de control de tiempo Real, realiza las tareas de control de RTP.
SCCP	Protocolo de Control de Llamadas Skinny
	Skinny Call Control Protocol
SDP	Protocolo de servicio de datos.
SIP	Protocolo de Señalización de Sesión(es)
	Session Initiation Protocol
SS7	Sistema de Señalización (versión) 7
	Signalling System 7
TA/ATA	Adaptador Telefónico
	Telephone Adapter
UA	(User Agent) Son aplicaciones que residen en las estaciones terminales Sip
UDP	User Data Protocol
VoIP	Voz sobre IP. Telefonía IP

GLOSARIO

Ancho de Banda – Es el volumen de datos que pueden ser transmitidos por una línea de comunicaciones en un momento dado. Se suele expresar en bits por segundo o en alguno de sus múltiplos (bit/s, kbit/s, Mbit/s, Gbit/s). Disponer de suficiente ancho de banda en entornos VoIP es esencial para que las conversaciones puedan mantenerse con calidad. Cuando se realizan llamadas telefónicas sin disponer del ancho de banda necesario se producirán cortes en la conversación, silencios prolongados y ecos.

.

ATA -(Analogue Terminal Adapter) – Adaptador de Terminal Analógico. Es un dispositivo electrónico que se conecta a Internet, normalmente a una red donde hay un router, y luego a uno o varios teléfonos analógicos normales, permitiendo que estos puedan recibir servicios VoIP.

Cliente SIP – Es el software donde se configura una línea SIP para que se puedan realizar y recibir llamadas y otras funcionalidades prestadas por el sistema.

Congestión – Se produce cuando no es posible terminar una llamada debido, fundamentalmente, a la falta de recursos en alguno de los puntos entre el llamante y el llamado.

Firewall – Es un dispositivo de seguridad que filtra el tráfico de red entrante y saliente, de manera que impide intrusiones no deseadas. Es conveniente prestar atención a la seguridad de la red pero también a lo que se filtra, para que no se interrumpan servicios esenciales.

Gateway VoIP – Es un dispositivo que permite conectar varios dispositivos analógicos de manera que estos puedan utilizar servicios VoIP. Un ATA es un pequeño gateway. El gateway puede tener puertos FXS y/o FXO, pudiendo conectar teléfonos o líneas analógicas para convertirlas en IP.

Jitter – Es una variación temporal de la entrega de paquetes en la transmisión de datos que provoca ruidos indeseados. Suele solucionarse ampliando el buffer de jitter o el buffer de datos.

LAN (Local Area Network) – Red de área local. Una red local se forma con varios dispositivos de red interconectados entre si a través de un conmutador o switch, y configurados de manera que se puedan transmitir datos entre ellos.

Latencia – Es el retardo en escuchar la voz del otro interlocutor. Técnicamente es el tiempo que tarda un paquete de datos en llegar desde el origen al destino. Si este tiempo es mayor de 200ms se produce un retardo de la voz molesto. Las soluciones habituales a este problema son: ampliar el ancho de banda, reservar un ancho para la VoIP o marcar los paquetes para priorizarlos.

NAT – (Network Address Translation - Traducción de Dirección de Red) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

PBX – (Private Branch Exchange) es un equipo al que se conectan, por un lado, líneas de teléfono y, por otro, teléfonos. Este equipo interpreta si las llamadas tienen como destino teléfonos internos o externos, enrutandolas según corresponda y haciendo posible la comunicación.

Protocolo – Son una serie de normas que hacen posible el intercambio de información entre dos equipos electrónicos.

QoS (Quality of Service) – Calidad de Servicio. Se denomina de esta manera a un conjunto de técnicas que permiten mantener un grado de aceptación en las conversaciones VoIP.

TCP (Transmission Control Protocol) – Es un protocolo para crear conexiones entre dos equipos conectados en una red, que garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. Es parte fundamental de funcionamiento de Internet.

Teléfono IP – Es un tipo de cliente SIP con facilidades de, al menos, teclado numérico, micrófono y auricular.

UDP (User Datagram Protocol) – Es un protocolo de red que permite el envío de paquetes sin que se haya establecido previamente una conexión, por lo que por una parte no se garantiza la entrega pero por otra no introduce retardos, por lo que es óptimo para la transmisión de audio y vídeo.

WAN (Wide Area Network) – Este concepto se refiere a un conjunto de equipos de red conectados entre sí aunque su distancia física sean de cientos de kilómetros. Internet puede considerarse un tipo de WAN.

INTRODUCCIÓN

Internet ha dejado de ser una plataforma solo donde se comparte información de solo datos y ha pasado a ser una red convergente donde coexisten diferentes servicios.

Voz sobre IP es una tecnología que transporta voz sobre redes IP y tiene la capacidad de poder realizar llamadas telefónicas sobre redes de datos, así como transportar datos multimedia.

Desde los comienzos en el desarrollo de la tecnología de VoIp muchos protocolos han sido desarrollados pero el protocolo H.323 puede ser considerado como la primera generación de protocolos para este propósito.

En la actualidad las aplicaciones de voz y video se están convirtiendo en elementos claves para la comunicación entre personas. Cuando se desea implementar tecnologías que permitan el manejo de este tipo de aplicaciones multimedia, VoIP resulta ser la herramienta más apropiada. La tecnología VoIP requiere para su funcionamiento el uso de un protocolo encargado de gestionar los recursos involucrados en la comunicación como: establecer, modificar y cerrar sesiones multimedia. De entre los cuales podemos mencionar el protocolo H323, SIP, AIX2. Siendo SIP el más utilizado actualmente. En este capítulo se presenta los aspectos más importantes del protocolo de inicio de sesión SIP; su historia, estructura, aplicaciones y funcionamiento. Debido a que el funcionamiento de SIP es a través del intercambio de mensajes entre el cliente y servidor; se detallan los mensajes de solicitud y respuesta SIP al mismo tiempo las estructuras de dichos mensajes. Además se muestran los problemas que se deben superar para permitir la comunicación SIP en el entorno NAT.

1. PRESENTACIÓN DEL PROYECTO

1.1 DESCRIPCIÓN DEL CONTENIDO DEL INFORME.

Este documento contiene un informe detallado de cada una de las etapas llevadas a cabo durante el desarrollo del proyecto: ANALISIS COMPARATIVO DE LOS PROTOCOLOS SIP, IAX2 Y H.323 UTILIZADOS EN LA TECNOLOGIA DE VOZ SOBRE IP.

Su distribución es la siguiente:

Capítulo 1: Introducción: Se presenta el proyecto y se hace un análisis de los antecedentes, definición del problema, objetivos generales, específicos, justificación, alcances y limitaciones del proyecto.

Capítulo 2: Detalla las generalidades de lo que es la tecnología VoIP, como lo es su historia, funcionalidades, estructura y aplicaciones; además se explica la diferencia existente y las ventajas que presenta entre el funcionamiento de la telefonía tradicional y la tecnología VoIP.

Capítulo 3: Es centralizado en dar a conocer en detalle los 3 protocolos en el desarrollo de las tecnología VoIP, refiriéndose este a los protocolos SIP, IAX2 Y H.323.Donde se explica su estructura, funcionamiento y la interacción que tiene entre los diferentes elemento que componen una red de comunicación VoIP.

1.2 ANTECEDENTES

Voip es una tecnología que se desarrolló a partir de 1995 y se basa en el proceso de digitalización de la voz para que esta pueda ser transmitida en redes TCP/IP,

su desarrollo ha pasado por múltiples implementaciones donde han participado diversos organismos a nivel internacional y empresas dedicadas al desarrollo de las tecnologías de la información y las comunicaciones (TICS), con el objetivo de poder estandarizar el conjunto de técnicas y protocolos sobre los que se sustenta esta tecnología.

Actualmente existen diversas investigaciones enfocadas a la tecnología VoIP que mencionan básicamente el origen y las tendencias de esta tecnología, en este documento se mencionan algunas de estas investigaciones como referencia para desarrollar este proyecto.

VoIP empieza a ser una realidad en muchas empresas por la rápida amortización y el ahorro de costos que proporciona. En numerosas empresas se está produciendo una evolución silenciosa de sus redes internas. El objetivo es reducir la factura telefónica de las llamadas de voz nacionales e internacionales, que representan un elevado porcentaje del total de pagado a los operadores.

Evolución del mercado de la Voz sobre IP

1995 año del aficionado
1996 año del cliente
1997 Año del Gateway
1998 Año del gatekeeper
1999 Año de la aplicación.
2000 Año de Asterisk [1]
2002 Año de Protocolo SIP
2005 Año de Softphone Gratuito
2006 Año de Skype

[1] Introducción a asterisk [en línea] http://comunidad.asteriskes.org/index.php?title=Introduccion_a_Asterisk [citado el 1 de mayo de 2013]

1.3 DEFINICIÓN DEL PROBLEMA

La tecnología VoIP creada para transportar comunicación telefónica a través de redes IP, ha evolucionado en los últimos años, debido entre otras cosas, al mayor aprovechamiento del ancho de banda y a su menor costo comparada con la telefonía tradicional.

Aplicar esta nueva tecnología implica el uso de uno de los protocolos de señalización, entre los cuales sobresalen los protocolos de inicio de sesión **SIP**, **IAX2** y **H.323** que durante los últimos años se ha convertido en los más utilizados para el desarrollo de aplicaciones en Internet y en redes de voz. Por lo que se necesita saber los detalles de su funcionamiento, las ventajas que posee sobre los demás protocolos diseñados, los elementos necesarios para desarrollar una red, y al mismo tiempo, es importante conocer el funcionamiento, el proceso de instalación y la configuración comunicación de voz en un ambiente privado.[2]

1.4 OBJETIVOS

1.4.1 Objetivo general

- Desarrollar una comprensión completa y estructurada sobre funciones, protocolos y componentes de VoIP.

1.4.2 Objetivos específicos

- Realizar un estudio comparativo entre la telefonía normal y la telefonía IP sobre los aspectos de costos, seguridad y desempeño.
- Investigar de forma comparativa los protocolos SIP, IAX2 y H.232 para el despliegue de servicios de VoIP.

[2] SIP Protocolo Inicio de Sesión [en línea] http://www.quarea.com/es/tutorial/SIP_session_initiation_protocol [citado el 1 de junio de 2012]

- Describir el funcionamiento y la calidad del servicio de los protocolos SIP, IAX2 y H.323 y sus aplicaciones.

1.5 JUSTIFICACIÓN

La innovación que actualmente están dando las comunicaciones telefónicas y multimedia a tecnología VoIP, hace necesario que las personas involucradas en la implementación de esta tecnología; posean los conocimientos sobre aspectos tan importantes como los protocolos de señalización, especialmente conocer el funcionamiento y configuración de los protocolos SIP, IAX2 y H.323 ya que estos se han convertido en un estándar internacional por su rápida aceptación por parte de los desarrolladores de tecnología VoIP.

El desarrollo y aplicación de SIP, IAX2 y H.323 en servicios de VoIP está ampliamente difundido internacionalmente, en Colombia por el contrario, a nivel de educación superiores poca o nula la información proporcionada sobre esta tecnología; por lo que este proyecto pretende servir como herramienta didáctica para comprender el funcionamiento, así como referencia a futuras investigaciones y desarrollo de aplicaciones que involucren la utilización de los protocolos anteriormente nombrados.

1.6 ALCANCES Y LIMITACIONES

1.6.1 Alcances

- Realizar una investigación que describa los protocolos encargados de la Comunicación de Voz en una red IP, haciendo énfasis los Protocolos de SIP, IAX2 y H.323.

- La investigación a desarrollar pretende servir como marco de referencia de modo tal que se pueda implementar Voip para integrar los servicios de voz y datos.

1.6.2 Limitaciones

- El estudio comparativo se limita o es de tipo investigativo por lo que implica la descripción de protocolos de estándar abierto, tales como: H323, SIP e IAX2. La metodología empleada no comprendió la realización de experimentos o prácticas que involucren la aplicación de los protocolos en cuestión.

2. INTRODUCCIÓN A LA TECNOLOGIA VOZ SOBRE IP

2.1 GENERALIDADES DE LA TELEFONÍA

Definición: VoIP es la voz transportada sobre Internet; comprende también un conjunto de recursos tecnológicos que hacen posible que la señal de voz viaje a través de la red de Internet empleando el protocolo IP (Protocolo de Internet).

Se trata de transformar la voz en paquetes de información (paquetes de datos binarios) manejables por una red IP, para que se puedan transmitir a través de la redes de datos existentes.

Esto significa que se envía la señal de voz en forma digital en paquetes a través del Internet o de una red de datos privada, en lugar de enviarla a través de circuitos utilizados por las compañías telefónicas convencionales o PSTN (Red Telefónica Pública Conmutada).

2.1.1 Evolución histórica de la telefonía. En 1857, Antonio Meucci (1808-1889) había inventado una máquina cuyo componente esencial era un elemento vibrador unido a un imán; era el primer aparato telefónico, pero sería Graham Bell (1847-1922) quien, finalmente, tras patentar un aparato semejante en 1876, pasaría a la historia como el verdadero padre del teléfono.[3]

Algunas evoluciones son mostradas a continuación.

- Telefonía fija o convencional, que hace referencia a las líneas y equipos que se encargan de la comunicación entre terminales telefónicos no portables, y

[3] Historia y evolución del teléfono [en línea] http://myprofetecnologia.wordpress.com/2011/02/14/historia-y-evolucin-del-telfono/ [citado el 2 de junio de 2012]

generalmente enlazados entre ellos o con la central por medio de conductores metálicos.

La central telefónica de conmutación manual para la interconexión mediante la intervención de un operador/a de distintos teléfonos creando de esta forma un primer modelo de red.

- La introducción de las centrales telefónicas de conmutación automática, constituidas mediante dispositivos electromecánicos, de las que han existido, y en algunos casos aún existen, diversos sistemas: sistema de conmutación rotary, sistema con conmutador de barras cruzadas y otros más complejos.

- Las centrales de conmutación automática electromecánicas, pero controladas por computadora. También llamadas centrales semielectrónicas.

- Las centrales digitales de conmutación automática totalmente electrónicas y controladas por ordenador, la práctica totalidad de las actuales, que permiten multitud de servicios complementarios al propio establecimiento de la comunicación (los denominados servicios de valor agregado). Sistemas AXE (de Ericsson), Sistema 12 o 1240 (Alcatel) y sistema 5ESS (Lucent).

- La introducción de la Red Digital de Servicios Integrados (RDSI) y las técnicas DSL o de banda ancha (ADSL, HDSL), que permiten la transmisión de datos a más alta velocidad.

- Tecnología VoIP que consiste en el transporte de Voz sobre redes IP y es la tecnología más reciente.

2.1.2 Características de la telefonía. De las principales características que presenta la tecnología VoIP son:

- El tráfico de voz puede pasar a través de cualquier red IP, tanto como las conectadas a internet como las redes de área local.
- Se puede hablar de Estándares abiertos e internacionales, interoperatividad, precios bajos y gran cantidad de fabricantes de hardware.
- Es posible conseguir la misma o similar calidad en las llamadas que en las de la red PSTN. Hoy en día la mayoría de las empresas prestadoras de servicios de comunicación ofrecen la telefonía de VoIp.
- Posibilidad de enlace con la red de telefonía tradicional
- Posibilidad de desarrollar e implementar nuevos servicios.
- Costos más reducidos para los clientes.

Tabla 1. Telefonía Tradicional Vs Telefonía IP

Telefonía Tradicional	Telefonía IP
Se basa en la conmutación de circuitos	Se basan en la conmutación de paquetes
Los recursos que intervienen en otra llamada no pueden ser usados por otra hasta que ésta no finalice.	Los recursos pueden se utilizados en otras conexiones.
La red analógica se encarga de la transmisión de voz.	La red IP es una red convergente donde concluyen Datos, Video y Voz.
Los elementos de seguridad para la información que viaja por esta red deben ser adquiridos y monitoreados por separado.	Existen elementos que realizan la autenticación de usuarios, por ejemplo el gatekeeper
Es costosa en mantenimiento y el valor de las llamadas.	Es económica en cuanto a mantenimiento, el costo de las llamadas, especialmente las internacionales son más baratas
La movilidad es prácticamente nula Poca escalabilidad.	Posee gran movilidad, ya que basta tener acceso a internet y se podrá tener acceso desde cualquier parte donde se encuentre. Gran escalabilidad, producto de su estructura y características que posee.

Fuente:
https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&sqi=2&ved=0CCoQFjAA&url=http%3A%2F%2Fbibdigital.epn.edu.ec%2Fbitstream%2F15000%2F2143%2F1%2FCD-2892.pdf&ei=3W0uUp3cOYea8wS1nIGYBQ&usg=AFQjCNETQ5udwfH44Wd1Ahiq9tGK3_y0_g&bvm=bv.51773540,d.eWU

3. PROTOCOLO SIP

3.1 GENERALIDADES DEL PROTOCOLO SIP

SIP o Protocolo de Iniciación de Sesión, es un protocolo de control de señalización, definido en el RFC 2543 (año 1999) del grupo de investigación IETF (*Engineering Task Force*), organismo responsable de administrar y desarrollar los mecanismos que comprenden todo lo relacionado con Internet, para el establecimiento, modificación y terminación de las sesiones multimedia con uno o más participantes. SIP hace suposiciones mínimas sobre el transporte básico y la red de protocolo de capa, que puede proporcionar ya sea un servicio de flujo de paquetes para que el servicio sea o no confiable.

El propósito del protocolo SIP es establecer la comunicación entre dos dispositivos multimedia a través de dos protocolos RTP/RTCP y SDP. El protocolo RTP se usa para transportar los datos de voz en tiempo real, mientras que el protocolo SDP se emplea para la negociación de las capacidades de los participantes y tipo de codificación. Este protocolo considera a cada conexión como un par y se encarga de negociar las capacidades entre ellos. Tiene una sintaxis similar al HTTP.

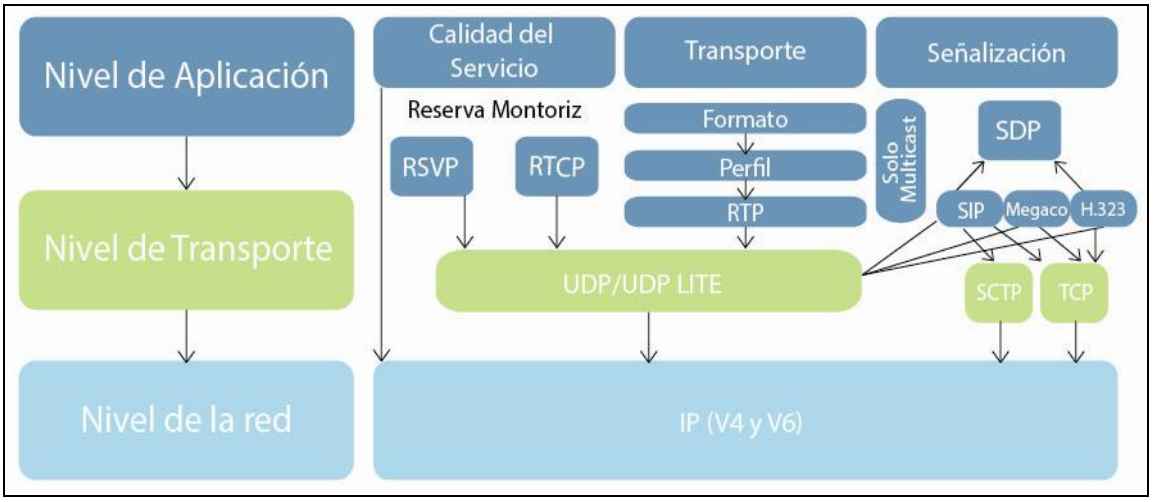
El protocolo SIP se basa en varios componentes para poder establecer la comunicación, localización, disponibilidad, utilización de recursos y características de negociación. Para poder implementarse se basa principalmente en los agentes de usuario y los servidores.

El protocolo SIP sigue un enfoque basado en la web para la señalización, al contrario de los protocolos de las telecomunicaciones tradicionales. Se asemeja a un modelo cliente / servidor, donde los clientes SIP envían solicitudes y los Servidores SIP regresan una o más respuestas. El conjunto de protocolos de señalización está construido de solicitudes y respuestas, que se agrupan en "transacciones". Muchas de las entidades SIP se componen de un cliente y un

servidor y el protocolo ha sido diseñado de manera que las entidades puedan tener cualquiera de los dos estados.

SIP no establece canales de señalización separados para la creación y el control de la llamada, en su lugar, define la noción de operaciones que consisten de una sola petición, enviada por un cliente a un servidor, seguido por cero o más respuestas provisionales y una respuesta definitiva del servidor.
Todos los mensajes de una transacción comparten un identificador único común y atraviesan el mismo conjunto de hosts.

Figura 1. Protocolos sobre IP.



Fuente:
http://www.konradlorenz.edu.co/images/stories/articulos/explorando_bases_telecomunicaciones.pdf

3.2 FUNCIONALIDAD BÁSICA

SIP se utiliza para la creación, gestión y terminación de comunicaciones multimedia. Se debe hacer hincapié en que la entrega real del contenido de medios se encuentra fuera del alcance de la especificación SIP. SIP aborda los siguientes aspectos de las comunicaciones multimedia:

- Ubicación del usuario. El sistema proporciona un medio para determinar la dirección de transporte, donde el servidor de agente de usuario del punto extremo llamado SIP escucha solicitudes SIP.

- Capacidades de los usuarios. El sistema se encarga de determinar las capacidades multimedia de cada punto final que participan en la convocatoria y debe asegurarse de que puedan comunicarse entre sí, si sus capacidades son compatibles.

- Disponibilidad usuario. El sistema debe determinar si el usuario llamado está dispuesto a participar en la comunicación con el punto extremo solicitante.

- Configuración de llamadas. El sistema debería alertar al usuario y configurar ambos extremos de tal manera que la llamada se pueda realizar.

- Gestión de llamadas. El sistema, mientras que no es responsable de la transferencia del contenido de medios, debe proporcionar los medios para modificar las características de la sesión de llamada, tales como añadir / eliminar canales o medios de los participantes de las llamadas.

- Terminación de llamadas. Por último, el sistema debe terminar la sesión de llamamiento a los usuarios, solicitar y asegurar que, incluso cuando algunos puntos finales no siguen la terminación adecuada procedimiento, los recursos de llamadas son liberados y la sesión de llamada se da por terminada.

Una sesión típica de llamada consiste en un número de transacciones entre los agentes de usuario y las entidades de protocolo que intervienen. Las solicitudes se emiten desde un agente de usuario cliente, un servidor proxy que actúa en nombre de un agente de usuario cliente o en otro servidor proxy. Cada solicitud pide una o

más respuestas de un servidor de agente de usuario o un servidor proxy que redirecciona la solicitud que recibió.

Todos los mensajes de la petición hasta que la respuesta final constituyen una transacción y pueden ser intercambiado directamente por dos entidades o poligonal uno o más servidores proxy en el camino.

3.3 ENTIDADES EN UN SISTEMA SIP

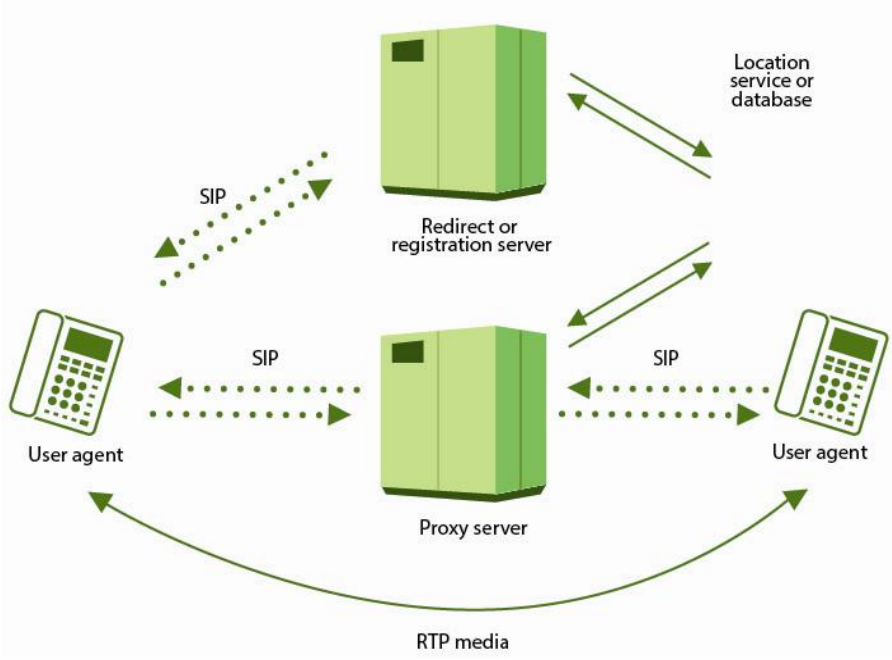
Un sistema característico se basa en un modelo cliente / servidor y se compone de las siguientes entidades:

• Un agente de usuario (UA): Es una aplicación que actúa en nombre del usuario, tanto como cliente (Usuario Agente de cliente) y como un servidor (User Agent Server). Como un cliente que envía solicitudes SIP y como un servidor que acepta llamadas y responde a las peticiones SIP realizadas por otras entidades. El agente de usuario es generalmente una aplicación parte de un terminal multimedia.

Un servidor de registro: Es un servidor SIP que sólo acepta solicitudes de registro hechas por el usuario agente con el fin de localizar el destinatario de una llamada. Aquí intervienen los servidores proxy y de redirección, los cuales buscan el destinatario para asignarle la llamada y así conectar, si es el caso los medios (voz, imágenes o mensajes) a intercambiar.

Por tanto, la función del servidor de registro es satisfacer solicitudes SIP REGISTER y actualizar los datos de localización, con la debida información del usuario que se registre. Su función es asociar una URI (*Uniform Resource Identifier*) con una o varias direcciones IP.

Figura 2. Interacción de los Servidores SIP y Agentes de Usuarios.



Fuente: Los Autores

Un servidor de redireccionamiento: Es un servidor SIP que proporciona servicios de mapeo de direcciones, responde a una petición SIP, traduce la dirección de destino en una o varias direcciones de red y las devuelve al cliente. Un servidor de redirección no acepta llamadas, no reenvía solicitudes, ni inicia ninguna propia.

Un servidor proxy es un servidor SIP que actúa tanto como un servidor de aplicaciones del usuario mediante el envío de peticiones SIP y como un cliente a otro servidor SIP mediante la presentación de las solicitudes remitidas a ellos en nombre de los agentes de usuario o servidores proxy.

Existen dos tipos de servidores proxy SIP: proxy sin estado y proxy con estado

- **Proxy sin Estado** es el encargado de reenviar los mensajes SIP. Ellos reenvían los mensajes de forma independiente el uno del otro.

Los proxy sin estado son más rápidos que los servidores proxy con estado. Uno de los inconvenientes de la representación sin estado es que son incapaces de absorber la retransmisión de mensajes y realizar el enrutamiento avanzado.

- **Proxy con Estado** Los Proxy con estado en la recepción de una solicitud, pueden crear un estado y mantenerlo hasta que finalice la transacción. Algunas transacciones, pueden durar bastante tiempo (hasta el destinatario toma o rechaza la llamada). El rendimiento de estos servidores es limitado debido a que deben mantener el "estado" de acuerdo a la duración de las transacciones que maneje, pero pueden desempeñar tareas mucho más complejas.

Con la excepción del agente de usuario, que es normalmente parte de un terminal multimedia, el resto de las entidades lógicas (registrador, reorientar y servidores proxy) se pueden combinar en una sola aplicación. Por lo tanto, una sola entidad puede actuar ya sea como un proxy o como un servidor de redirección, de acuerdo a la petición SIP, y al mismo tiempo aceptar solicitudes de registro. Una llamada SIP se define como la conferencia multimedia que consta de todos los participantes invitados.

3.3.1 Características del Protocolo SIP

- SIMPLICIDAD: SIP es un protocolo muy simple. El tiempo de desarrollo del software es muy corto comparado con los productos de telefonía tradicional. Debido a la similitud de SIP a HTTP y SMTP, el rehúso de código es posible.

- EXTENSIBILIDAD: SIP ha aprendido de HTTP y SMTP y ha construido un buen grupo de funciones de extensibilidad y compatibilidad.

- MODULARIDAD: SIP fue diseñado para ser altamente modular. Una característica clave es su uso independiente de protocolos. Por ejemplo, un

participante puede gestionar una misma llamada, esto quiere decir que puede invitar a otros participantes en la llamada o puede cancelar las conexiones a otros usuarios, además de que los usuarios pueden ser puestos en espera.

- ESCALABILIDAD: SIP ofrece dos servicios de escalabilidad:
- PROCESAMIENTO DE SERVIDOR: SIP tiene la habilidad para ser Stateful o Stateless (Con o sin estado).
- ARREGLO DE LA CONFERENCIA: Puesto que no hay requerimiento para un controlador central multipunto, la coordinación de la conferencia puede ser completamente distribuida o centralizada.
- INTEGRACION: SIP tienen la capacidad para integrarse con la Web, E-mail, aplicaciones de flujo multimedia y otros protocolos.
- INTEROPERABILIDAD: porque es un estándar abierto, SIP puede ofrecer interoperabilidad entre plataformas de diferentes fabricantes.

3.4 MENSAJES INVOLUCRADOS EN UNA COMUNICACIÓN SIP

Hay dos tipos de mensajes en SIP; solicitudes y respuestas. Ambos utilizan la representación textual del carácter ISO 10646 establece con la codificación UTF-8. La sintaxis del mensaje es la siguiente HTTP/1.1, pero hay que señalar que el SIP no es una extensión para HTTP.

SIP define unos de mensajes de solicitud y una jerarquía de respuestas SIP. Cada solicitud y el método de respuesta se componen de campos de cabecera, de manera obligatoria y un cuerpo de mensaje, que puede ser opcional. La mayoría de las veces, los campos de cabecera son los que tienen la mayor parte de la información intercambiada en el protocolo. Un subconjunto de los campos de

cabecera puede ser abreviado por letras individuales, condensando así el tamaño de los mensajes, esta forma de compresión se conoce como "tokenización".

Al establecer una sesión, los mensajes SIP deben describir las características de la sesión de los agentes de usuario. SIP recomienda pero no obliga a la utilización de la descripción de sesión del Protocolo SDP, que se define en el RFC 2327. La descripción de sesión se utiliza para comunicar los parámetros necesarios para establecer los canales de comunicación para la transferencia de los contenidos de medios de la sesión llamada.

3.4.1 Solicitudes. SIP hace uso de seis métodos de petición: INVITE, ACK, OPTIONS, BYE, cancelación y REGISTRO. La información de estos métodos se encuentran dentro de los campos de cabecera usados.

INVITE Esta solicitud se utiliza para invitar a un usuario a participar en una sesión multimedia, con las características de los medios de comunicación específicos. También se utiliza para modificar una sesión de llamada ya establecida.

ACK Este pedido confirma que un agente de usuario cliente ha recibido la respuesta final a una petición INVITE.

OPCIONES Esta solicitud se envía a un servidor para consultar sus capacidades.

BYE Esta solicitud indica al servidor de agente de usuario que el agente de usuario cliente de otro punto final desea salir de la sesión de llamada.
CANCELAR Esta solicitud se envía para abortar una solicitud anterior.

REGISTRAR esta petición informa el registro de la ubicación actual del agente de usuario, por lo que se puede enlazar con el agente de usuario.

3.4.2 Respuestas SIP. A cada solicitud que reciba un agente de usuario o el servidor proxy, se produce una respuesta respectiva. Las solicitudes deben ser respondidas, menos las solicitudes de ACK que no devuelven algún tipo de respuesta.

Los códigos de respuesta son números enteros de 100 a 699 los cuales indican el tipo de la respuesta. Hay seis clases de respuestas:

- **1xx** son respuestas provisionales. Indica que una solicitud fue recibida, pero el resultado aun no es conocido. Estas respuestas solo se envían cuando un proceso no finaliza de inmediato.

- **2xx** Respuestas Exitosas. Indican que las solicitudes son procesadas y aceptadas.

- **3xx** Se utilizan para redirigir una llamada. Generalmente son enviadas por servidores proxy y dan información sobre una nueva ubicación del usuario o un servicio. Puede ser la ubicación de otro proxy o la ubicación actual del destinatario de la llamada.

- **4xx** Error del cliente. la petición contiene una sintaxis errónea o no se puede realizar en ese servidor.

- **5xx** Significa error de servidor. La solicitud es válida, pero el servidor no puede cumplirla. Se debe reenviar nuevamente la solicitud.
- **6xx** Significa que la solicitud no puede ser realizada. Suelen ser enviadas por algún servidor que tiene información completa acerca de un usuario en particular. Cuando los agentes de usuario no desean participar en sesiones generalmente envían una respuesta 603 para rechazar la invitación.

La solicitud a la que pertenece una determinada respuesta se identifica con el campo de la cabecera. Además del número de secuencia de este campo de encabezado contiene también el método de la solicitud correspondiente.

4. PROTOCOLO IAX2

4.1 GENERALIDADES DEL IAX2

El objetivo con el que se creó el protocolo IAX (Inter-Asterisk eXchange protocol), fue minimizar la tasa de bits requerida en las comunicaciones VoIP y tener un soporte nativo para traspasar dispositivos de NAT, es decir, provee soluciones a los problemas dados en SIP y H.323. Fue creado por Mark Spencer, quien también participó en la codificación de Asterisk. IAX2 usa un único puerto UDP (4569) para transmitir tanto señalización como datos.[4][5]

El tráfico de voz es transmitido en banda, es decir, los datos de voz van encapsulados en el protocolo; SIP, en cambio, se basa del protocolo RTP para la transmisión de los datos (su transmisión es out-band). Esto le permite al protocolo IAX2 prácticamente transportar cualquier tipo de dato.

Otra característica de IAX2 es que soporta Trunking; es decir, un solo enlace puede enviar datos y señalización de varios canales. Cuando se hace Trunking, un solo datagrama IP puede contener información de varias llamadas sin crear latencia adicional. Esto genera una disminución de la tasa de bits y del retraso de los paquetes debido a que ahorra enviar varias veces la cabecera IP.

Todas estas características del IAX2 se deben a que en su diseño se basaron en muchos estándares de señalización y de transmisión de datos, quedándose solo con lo mejor de cada uno.

---

[4] Protocolo Iax2 [en línea] http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/205/QUINTANA_DIEGO_DISENO_RED_TELEFONIA_IP_RAAP.pdf?sequence=2 [citado el 11 de mayo de 2013]

[5] Protocolo Iax2 [en línea] http://www.voipforo.com/IAX/IAX-arquitectura.php [citado el 13 de abril de 2012]

4.2 HISTORIA PROTOCOLO IAX2

Fue creado como parte del desarrollo de la PBX Asterisk. A diferencia del SIP, que usa dos flujos de datos para voz y otros dos para señalización, IAX2 usa sólo un par de flujos donde voz y datos coexisten.

La segunda versión del protocolo de comunicación entre Asterisks se conoce como IAX2.16 IAX2 es una alternativa al protocolo de señalización SIP.

Esta forma de enviar tanto las conversaciones como la señalización por el mismo canal se conoce como in-band, en contraste con el método que usa SIP, el out-of-band. Debido a su diseño, IAX2 es la opción más adecuada en regiones en desarrollo donde existe gran presencia de NATs. Además, IAX2 es capaz de empaquetar llamadas simultáneas en un solo flujo de paquetes IP. Este mecanismo es conocido como “trunking” y su implementación resulta en ahorros en el consumo de ancho de banda.

El concepto de “trunking” se puede explicar con la siguiente metáfora:

La agregación de llamadas en telefonía IP funciona de la misma forma y permite enviar múltiples cartas (llamadas) en un único sobre (paquete IP).En resumen, el diseño de IAX2 es más adecuado para regiones en desarrollo por tres razones:

1. Reduce el uso de ancho de banda por llamada.
2. Está diseñado para operar en presencia de NATs (soporte nativo) y es más fácil de usar detrás de los cortafuegos.
3. Reduce aún más el ancho de banda cuando se realizan varias llamadas simultáneas (como resultado del “trunking”) IAX2 es un protocolo de telefonía IP que utiliza un reducido número de bits en las cabeceras y que está diseñado para permitir la comunicación entre centralitas y clientes Asterisk. El contenido

de voz en los paquetes se envía usando una cabecera de tan solo 4 octetos (32 bits). Una cabecera más compleja de 12 octetos se utiliza con los paquetes de control y en algunos paquetes especiales de voz (uno por minuto aproximadamente).

La idea de enviar la señalización dentro del canal de voz (in-band) obliga a separar los paquetes de voz de los de señalización. Aunque este diseño requiere más gasto de procesamiento ofrece mejores propiedades en presencia de cortafuegos y NATs.

4.3 PROPÓSITOS DE IAX

El principal objetivo de IAX ha sido disminuir el ancho de banda utilizado en la transmisión de voz y vídeo a través de la red IP, con particular atención al control y a las llamadas de voz y proveyendo un soporte nativo para ser transparente a NAT. La estructura básica de IAX se fundamenta en la multiplexación de la señalización y del flujo de datos sobre un simple puerto UDP entre dos sistemas.

IAX es un protocolo binario y está diseñado y organizado de manera que reduce la carga en flujos de datos de voz. El ancho de banda para algunas aplicaciones se sacrifica en favor del ancho de banda para VoIP.

Las metas fundamentales para IAX eran reducir al mínimo la utilización de ancho de banda usada en las transmisiones de medios, con particular atención al control y a las llamadas de voz individuales, y proporcionar un soporte nativo para transmisiones con reglas NAT (*Network Address Translation*).

La estructura básica de IAX es multiplexar señalización y múltiples tramas de medios en un solo canal UDP (*User Datagram Protocol*) fluyendo entre dos computadoras. IAX es un protocolo binario, diseñado para reducir overhead de las transmisiones más que nada a las tramas de voz.

4.4 PROPIEDADES BÁSICAS DEL IAX2

IAX2 es robusto, lleno de novedades y muy simple en comparación con otros protocolos. Permite manejar una gran cantidad de códecs y un gran número de streams, lo que significa que puede ser utilizado para transportar virtualmente cualquier tipo de dato. Esta capacidad lo hace muy útil para realizar videoconferencias o realizar presentaciones remotas. Utiliza un único puerto UDP, generalmente el 4569, para comunicaciones entre puntos finales para señalización y datos. El tráfico de voz es transmitido in-band, lo que hace a IAX2 un protocolo casi transparente a los cortafuegos y realmente eficaz para trabajar dentro de redes internas. En esto se diferencia de SIP, que utiliza una cadena RTP out-of-band para entregar la información.

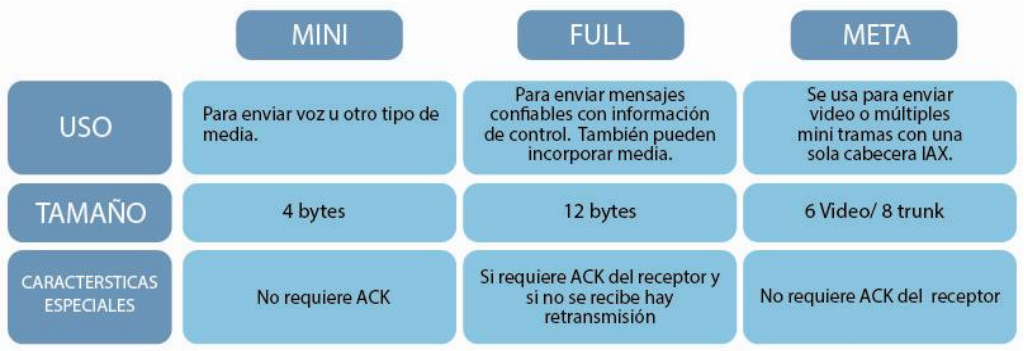
IAX2 soporta Trunking (red), donde un simple enlace permite enviar datos y señalización por múltiples canales. Cuando se realiza Trunking, los datos de múltiples llamadas son manejados en un único conjunto de paquetes, lo que significa que un datagrama IP puede entregar información para más llamadas sin crear latencia adicional. Esto es una gran ventaja para los usuarios de VoIP, donde las cabeceras IP son un gran porcentaje del ancho de banda utilizado.

4.5 TRAMAS IAX2

IAX2 diferencia entre tres distintos tipos de trama: mini, full y meta. Cada una de ellas con diferentes características y propósitos.

Cualquiera de los tres tipos puede ser encriptado. La siguiente tabla resume los tres tipos:

Figura 3. Tramas empleadas por IAX2.

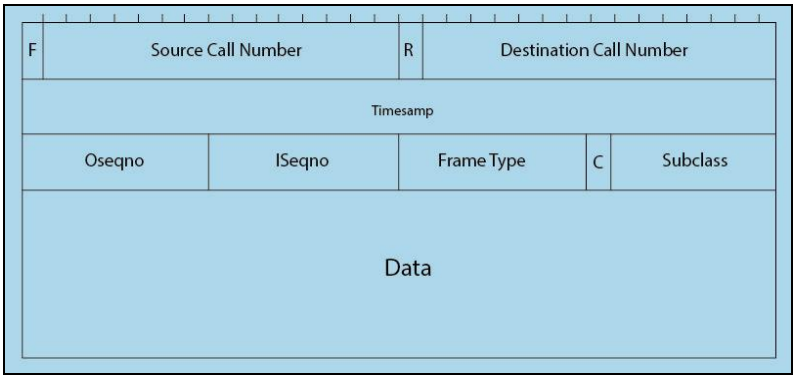


Fuente: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/8161/1/vpeino1_TFC_0611.pdf

4.5.1. Trama full. La trama full o completa se utiliza generalmente para enviar mensajes de señalización. En esta trama también puede viajar información tipo media (audio, video) aunque no es recomendable. Es necesario el envío de un ACK por parte del receptor ya que se implementa el reenvío.

Las tramas full tienen una cabecera de 12 bytes y su formato es el siguiente:

Figura 4. Trama Full.



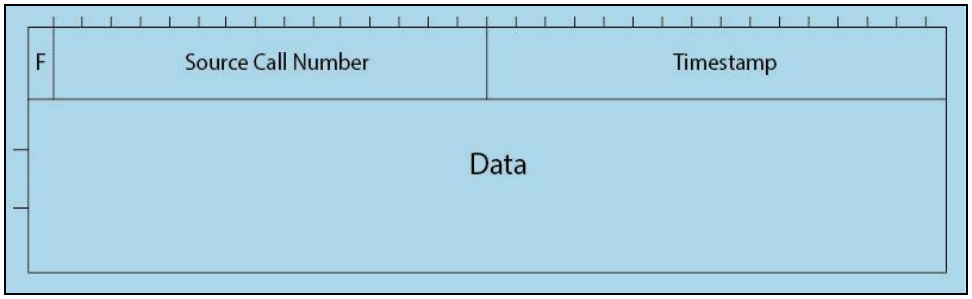
Fuente: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/8161/1/vpeino1_TFC_0611.pdf

- **F:** Este bit debe fijarse a 1 para indicar que se trata de una trama full (1 bit)
- **Source call number:** El identificador de la llamada en el origen (15 bits)

- **R:** indica si es una trama retransmitida (1 bit)
- **Destination Call Number:** El identificador de la llamada en el nodo de destino (15 bits)
- **Time-stamp:** Se utilizan para reordenar las tramas recibidas (32 bits)
- **OSeqno:** Su propósito es identificar los streams de salida dentro de una llamada (8 bits)
- **Iseqno:** Su propósito es identificar los streams recibidos dentro de una llamada (8 bits)
- **Frame Type:** Indica el tipo de la trama (8 bits)
- **C:** Indica el formato del campo SubClass (0 entero sin signo, 1 potencia de dos) (1 bit)
- **SubClass:** Indica la subclase del mensaje enviado por la trama (7 bits)

4.5.2. Trama mini. La longitud de la cabecera se encuentra limitada a 4 bytes y se usan exclusivamente para enviar voz una vez que la llamada ya ha sido establecida. Este tipo de mensajes no requiere de ACK y por lo tanto no hay reenvío en caso de pérdida. Se permite cambiar el códec utilizado en mitad de una comunicación pero para ello es necesario enviar una trama full

Figura 5. Trama Mini.



Fuente: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/8161/1/vpeino1_TFC_0611.pdf

- **F:** Este bit debe fijarse a 0 para indicar que se trata de una trama mini (1 bit)
- **Source call number:** El identificador de la llamada en el origen (15 bits)

- **Time-stamp:** Se utilizan para reordenar las tramas recibidas y su tamaño es la mitad que el empleado en las tramas full (16 bits)

4.5.3. Trama meta. "Este tipo de trama, menos común, se puede emplear en dos casos:

- En el intercambio de streams de video utilizando para ello una cabecera optimizada.
- Para permitir que múltiples streams de diferente media sean incluidos en la misma trama con una sola cabecera y de esta manera optimizar el consumo de bando de ancha.

Estas tramas viajan marcadas con el campo F a 0 para indicar que no son una trama full.

Después llevan un campo llamado meta indicador con 16 ceros indicando que se trata de una trama meta.

Además incorporan, entre otros, un nuevo campo V que si lleva el valor 0 indica que no es una trama meta de video."

4.6. ELEMENTOS DE INFORMACIÓN DEL IAX2

Una de las particularidades del protocolo IAX2 es el uso de elementos de información cuya función es la de contener información requerida para la gestión de las llamadas IAX. Los IE viajan en tramas de tipo Full y tienen la siguiente estructura:

Figura 6. Elementos de información.

Fuente: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/8161/1/vpeino1_TFC_0611.pdf

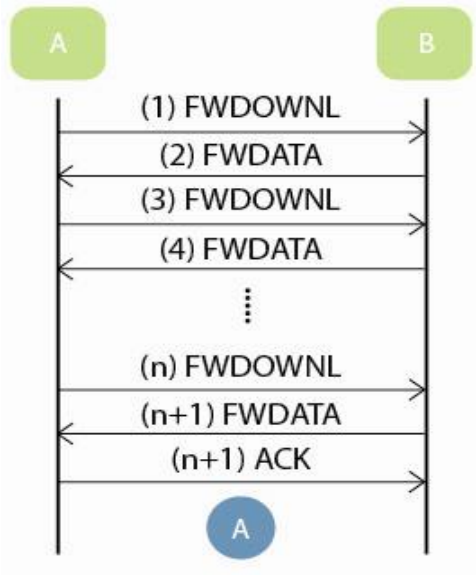
- **IE Index:** Almacena el identificador del IE que se está enviando.
- **Data Lenght:** Especifica el tamaño de los datos.
- **Data:** De tamaño variable contiene los datos codificados en UTF-8.

4.7. OPERACIONES IAX2

A continuación se describen las operaciones más comunes que se llevan a cabo en el protocolo IAX2 y los mensajes implicados:

- **Operaciones de suministro y descarga de firmware para dispositivos.** Permite el envío de información y la descarga de firmware por parte de ciertos dispositivos. Un dialogo de descarga de firmware sería similar al siguiente:

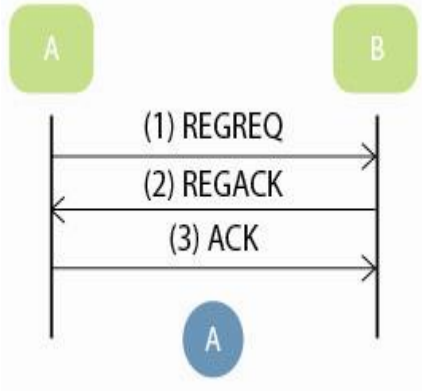
Figura 7. Operaciones de suministro y descarga de firmware para dispositivos.



Fuente: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/8161/1/vpeino1_TFC_0611.pdf

- **Registro:** Esta operación es opcional para aquellas peer con direcciones ip estáticas. Para aquellas con direcciones dinámicas es obligatorio registrarse en un servidor para permitir que otras peer puedan acceder a ellas. Por ejemplo una operación de registro satisfactoria sin autenticación implica el siguiente dialogo:

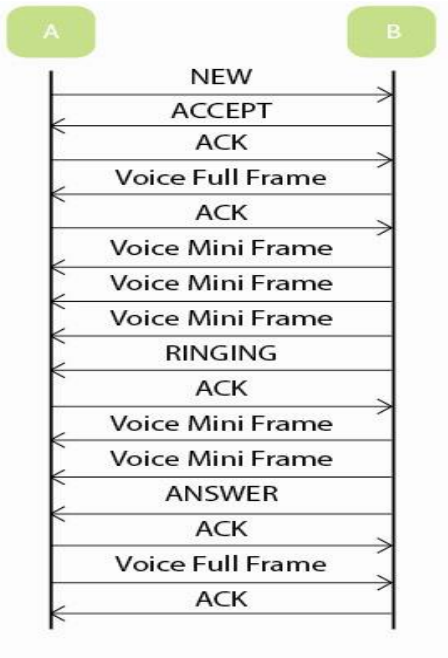
Figura 8. Registro.



Fuente: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/8161/1/vpeino1_TFC_0611.pdf

- **Establecimiento de llamada:** Esta es la función principal del protocolo. Un establecimiento exitoso con autenticación llevado a cabo directamente entre dos nodos incluiría los siguientes mensajes: [6]

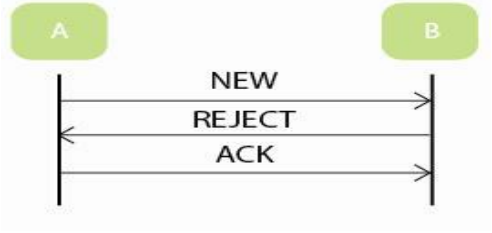
Figura 9. Establecimiento de llamada.



Fuente: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/8161/1/vpeino1_TFC_0611.pdf

Por su parte un intento fallido de establecimiento de llamada implicaría:

Figura 10. Intento fallido de llamada.



Fuente: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/8161/1/vpeino1_TFC_0611.pdf

[6] Tramas Protocolo Iax2 [en línea] http://openaccess.uoc.edu/webapps/o2/bitstream/10609/8161/1/vpeino1_TFC_0611.pdf [citado el 4 de enero de 2012]

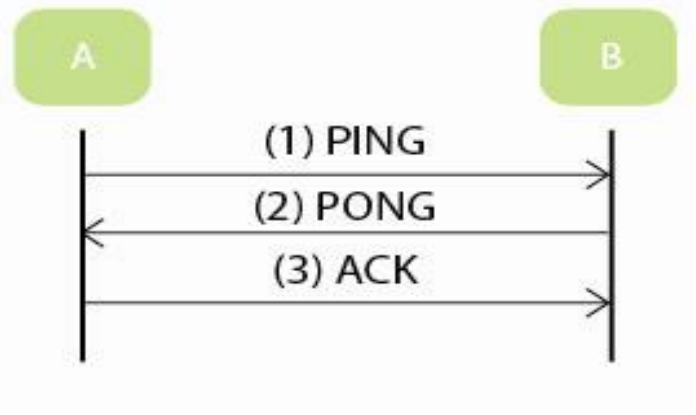
- **Fin de llamada:** Mensajes necesarios para finalizar una llamada:

Figura 11. Establecimiento de llamada.

Fuente: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/8161/1/vpeino1_TFC_0611.pdf

- **Supervisión de llamada:** a diferencia de SIP permite reconocer si una determina peer está conectado o no.

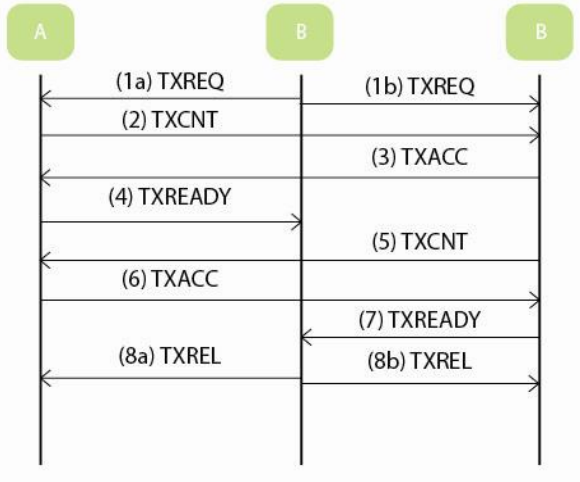
Figura 12. Supervisión de llamada.



Fuente: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/8161/1/vpeino1_TFC_0611.pdf

- **Optimización de llamada:** Su función principal es la de permitir a un nodo intermedio desaparecer de la comunicación entre emisor y receptor de una llamada permitiéndoles conectarse directamente. En el siguiente ejemplo B desaparece de la comunicación entre A y C.

Figura 13. Optimización de la llamada.



Fuente: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/8161/1/vpeino1_TFC_0611.pdf

5. PROTOCOLO H.323

5.1 GENERALIDADES DEL PROTOCOLO H323

H.323, un conjunto de protocolos definidos por la UIT-T en 1996, para la transmisión de voz por Internet (Voz sobre IP o VoIP). Además de las aplicaciones de voz, H.323 proporciona mecanismos para la comunicación de vídeo y datos, en combinación con las normas de la serie T.120 UIT-T. H.323 es uno o los principales estándares de VoIP, así como Megaco y SIP.

H.323 es una especificación que incluye una o varias normas de la UIT. Los componentes menores de la arquitectura H.323 son terminales, gateway, gatekeeper y la unidad de control multipunto (MCU).

Los Terminales representan al dispositivo final de cada conexión. Proporciona en tiempo real comunicaciones de dos vías con otro terminal H.323, GW o MSU. Esta comunicación se compone de datos, voz y video, o una combinación de voz, datos y video.

Los Gateways (puertas de enlace) establecen la conexión entre los terminales en la red H.323 y con los terminales pertenecientes a otras redes con diferente pila de protocolos tales como la red PSTN tradicional o SIP, puntos finales Megaco.

Los Gatekeepers son los responsables de la traducción entre el número de teléfono y las direcciones IP. También gestiona el ancho de banda y proporciona mecanismos para el registro de terminales y autenticaciones. Los Gatekeeper también ofrecen servicios tales como transferencia de llamadas y desvío de llamadas.

MCU se ocupa de establecer conferencias multipunto. Consiste en un control multipunto obligatorio, que es para la señalización de llamadas y control de conferencia y un procesador opcional multipunto, que es para la conexión / mezcla de flujo de medios, y a veces transcodificación en tiempo real de los flujos de audio / vídeo recibidas.

Hay cinco tipos de intercambio de información habilitados en la arquitectura H.323:

- Voz Audio (digitalizado)
- Video (digitalizado)
- Datos (archivos o imágenes)
- Control de la comunicación (intercambio de funciones compatibles, control de canales lógicos)
- Controlar las conexiones y sesiones.

5.1.1 Características del protocolo H.323

- Este estándar o protocolo busca garantizar la transmisión de datos, voz y video a través de la red de acuerdo a las necesidades de los usuarios, aunque no garantiza la calidad del servicio.
- La utilización en las comunicaciones permite un control centralizado y distribuido dependiendo de los requerimientos de servicio.
- Permite la adición de extensiones que permiten adaptarlo a determinados requerimientos.

- Se integra con diferentes tecnologías existentes como RTP/RTCP, URLs y DNS, todo esto para lograr su objetivo de transmisión multimedia.

- Es independiente de la topología de la red

- Permite usar más de un canal (voz, vídeo, datos) al mismo tiempo.

5.1.2 Componentes

El estándar H.323 especifica cuatro tipos de componentes:

- Terminales
- Gateway
- Gatekeeper
- Unidades de Control Multipunto (MCU)

Terminales: Son dispositivos utilizados para las comunicaciones multimedia bidireccionales en tiempo real con otro terminal, pasarela o MCU. Se pueden implementar tanto por software (mediante un computador) como por hardware (dispositivo físico).

Un Terminal dispone de funciones y capacidades descritas a continuación:

- La unidad de control del sistema, (H.245 y H.225.0), que proporciona control de llamada, el intercambio de capacidades, el envío de mensajes y la señalización para un funcionamiento adecuado del terminal H.323[9]

[9] Protocolos que describen la unidad de control del sistema para la recomendación H.323. [en línea].http://www.unipamplona.edu.co/unipamplona/hermesoft/portalIG/home_1/recursos/tesis/contenidos/tesis_septiembre/05092007/estudio_diseno_de_una_red_voz.pdf [citado el 4 de febrero de 2012]

- Transmisión de media, que se encarga de recibir los flujos de audio, video, datos, control y mensajes hacia la interfaz de red.

- Códec de Audio, el cual codifica la señal de audio del micrófono para transmisión y decodifica el audio recibido hacia el altavoz

- Interfaz de red, debe dar servicio de extremo a extremo fiable para el canal de control H.245, los canales de datos y el canal de señalización de llamada; y para los canales de audio, los canales de vídeo y el canal de RAS debe dar un servicio fiable.

- Códec de video, esta función es opcional y su función es codificar y descodificar video de acuerdo con la recomendación H.261.

- Canal de datos. Soporta aplicaciones tales como acceso a bases de datos, transferencias de ficheros, pizarras electrónicas, etc.

Gateways: Son dispositivos que proporcionan la interconexión entre dos redes diferentes, en ambos sentidos y en tiempo real. En el caso de H323, el gateway conecta una red H323 con una red que no maneje el protocolo H323 (red telefónica conmutada), todo esto de manera transparente para el usuario.

Las principales funciones del Gateway son:

- Búsqueda de destino: El Gateway recibe el número al cual se quiere llamar, entonces debe ser capaz de asociarlo a una dirección ip de otro Gateway donde se conecte con el número digitado a través de la PSTN.

- Gestión de la conexión IP: Después que el Gateway almacena el destino al cual se está llamando, éste debe realizar una conexión de VoIP con el Gateway destino sobre la cual se transportaran los paquetes de voz.

- Compresión / Digitalización: aquí el Gateway cumple una de las funciones más importantes y es la conversión de la voz de señal analógica o de la señal digital (PCM) a un flujo de bits de baja velocidad.

- Transporte y Packetization Ip

- Señalización avanzada IP/PSTN

- Autorización de acceso y contabilización: presenta características para la facturación del servicio aplicados en la PSTN.

Gatekeepers: Son dispositivos que pueden ser considerados el cerebro de la red. Desempeñan funciones importantes como el direccionamiento, autorización y autentificación de gateways y terminales, además de manejo de ancho de banda. Normalmente se implementan por software y son el equivalente a las PBX.

En cada una de las zonas puede haber uno o más gatekeeper (aunque el gatekeeper es opcional) y deben prestar las siguientes funciones:

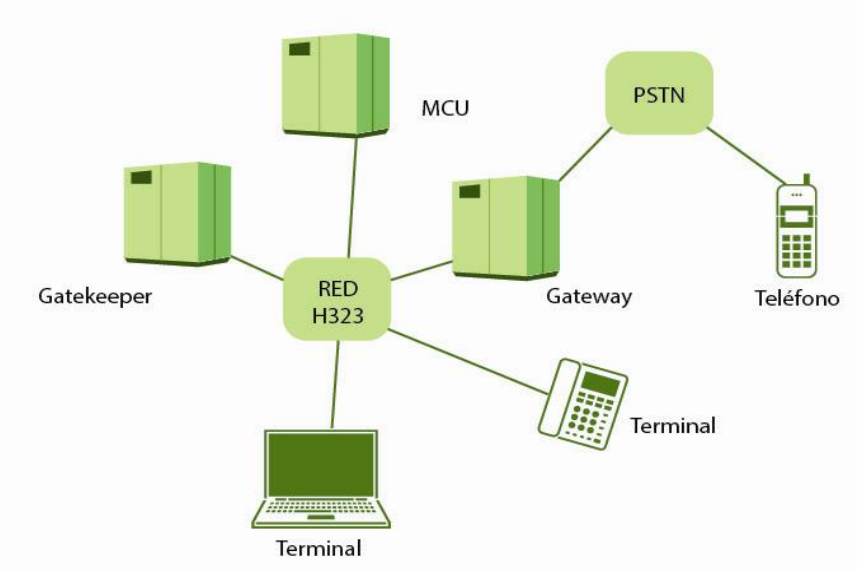
- Conversión de dirección. El gatekeeper traduce alias a dirección IP o a dirección E.164 necesarios para el establecimiento de las comunicaciones a través de una tabla de traducciones.

- Control de admisiones. El gatekeeper controla el establecimiento de llamadas mediante mensajes Admission Request /Admission Confirm / Admission Reject (ARQ/ACF/ARJ).

- Control de ancho de banda. El gatekeeper controla el número de usuarios simultáneo soportados mediante mensajes de Bandwidth Request / Bandwidth Confirm / Bandwidth Reject (BRQ/BRJ/BCF).
- Gestión de zona. El gatekeepers coordina acciones entre dispositivos de la misma zona como terminales registrados, gateways y MCU.

MCU: Es un dispositivo que proporciona la capacidad para que tres o más terminales y gateways participen en una conferencia.

Figura 14. Componentes del Protocolo H.323.



Fuente: Los Autores

5.2 PRINCIPALES PROTOCOLOS UTILIZADOS POR EL H323

- **RAS** La función RAS (Registration Admission and Status) utiliza los mensajes H.225.0 para la comunicación entre terminal y Gatekeepers y entre

gatekeepers. Los terminales usan RAS para registrarse en sus Gatekeeper, para realizar peticiones de permiso para utilizar sus recursos del sistema, para obtener direcciones de usuarios remotos, etc. Gatekeeper usan RAS para vigilar el estado de los terminales y recoger información de los recursos después de la finalización de una llamada.

RAS provee un mecanismo para los usuarios de autentificación de llamada. Se utiliza esta función para registro, control de admisión, control del ancho de banda y estado de la llamada.

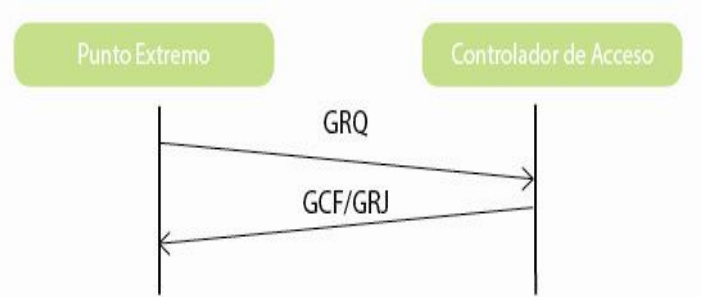
La función RAS realiza las siguientes funciones:

Descubrimiento de Gatekeeper.

Los terminales H.323 se registran en un gatekeeper provisto de servicios básicos como resolución de direcciones para llamadas a otros terminales. Hay dos posibilidades para que los terminales encuentren su gatekeeper:

- Multicast discovery: Los terminales envían un GRQ (gatekeeper request) a una dirección multcast conocida 224.0.1.41 y un puerto conocido 1718.
- Uno o más gatekeeper pueden responder con un mensaje de confirmación GCF (Gatekeeper Confirmation) conteniendo la dirección de transporte del canal de RAS del Gatekeeper o un mensaje de GRJ (Gatekeeper Reject) en caso negativo.
- Configuración: Los terminales conocen la IP del gatekeeper, envían un mensaje GRQ vía unicast y el gatekeeper o confirma o descarta.
- Adicionalmente, el gatekeeper puede proporcionar gatekeepers alternativos con un mensaje GCF.

Figura 15. Descubrimiento de Gatekeeper

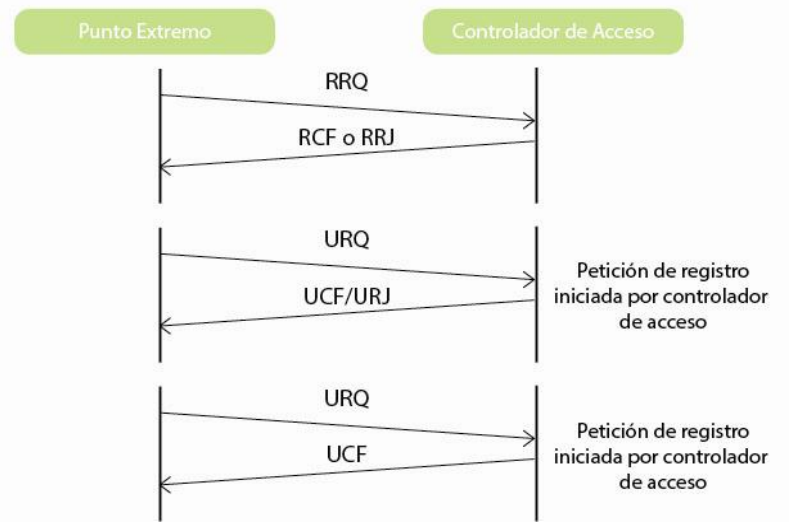


Fuente: http://www.voipforo.com/H323/H323ejemplo.php

Registro.

Después de que el terminal descubra cuál es su gatekeeper, el terminal debe registrarse con un mensaje de RRQ (Registration Request) en el gatekeeper. El gatekeeper responderá con una confirmación de registro RCF, (Registration Confirmation) o un rechazo de registro RRJ (Registration Reject). De igual manera si un terminal quiere desregistrarse deberá enviar un mensaje URQ (Unregistration Request).

Figura 16. Registro/Desregistro de usuario H.323.



Fuente: http://www.voipforo.com/H323/H323ejemplo.php

Localización de los terminales.

Los terminales o gatekeepers pueden determinar información de contacto emitiendo un mensaje de localización LRQ (Location Request) indicando el alias. Este mensaje puede ser enviado al gatekeeper por el canal de RAS o puede ser enviado mediante un GRQ a la dirección multicast. El gatekeeper contestara con LCF, (Location Confirmation) que contendrá información del terminal. Todos los Gatekeepers que reciban el mensaje y no contengan como usuario registrado devolverán un mensaje de rechazo de localización LRJ (Location Reject).

Admisiones y control de ancho de banda.

Estos mensajes se producen entre terminal y gatekeeper para proporcionar funciones de control de admisión y gestión del ancho de banda. Los gatekeepers autorizados acceden a la red H.323 mediante los mensajes de petición de admisión ARQ (Admission Request) especificando el ancho de banda de la llamada. El gatekeeper puede reducir el ancho de banda de llamada en el mensaje de confirmación de admisión ACF (Admission Confirm).

El terminal o el gatekeeper pueden intentar modificar el ancho de banda durante la llamada con un mensaje de petición de ancho de banda (BRQ, bandwidth change request) con una aceptación (BCF, bandwidth confirm) o negación (BRJ, bandwidth reject).

Información de Estado.

Los gatekeepers también pueden obtener información de sus terminales, mediante mensajes de petición de información IRQ (Information Request), los terminales envían un mensaje de respuesta IRR (Information Request Response).

- **H.225**: Se utiliza para establecer llamadas entre dos entidades H.323. Se especifica el uso y soporte de mensajes de señalización. Las llamadas son enviadas sobre TCP por el puerto 1720. Sobre este puerto se inician los mensajes de control de llamada Q.931 entre dos terminales para la conexión, mantenimiento y desconexión de llamadas.

Los mensajes más comunes de Q.931/Q.932 usados como mensajes de señalización H.323 son:

- Setup. Es enviado para iniciar una llamada H.323 y establecer una conexión con una entidad H.323. Entre la información que contiene el mensaje se encuentra la dirección IP, puerto y alias del llamante o la dirección IP y puerto del llamado.
- Call Proceeding. Enviado por el Gatekeeper a un terminal advirtiendo del intento de establecer una llamada una vez analizado el número llamado.
- Alerting. Indica el inicio de la fase de generación de tono.
- Connect. Indica el comienzo de la conexión.
- Release Complete. Enviado por el terminal para iniciar la desconexión.
- Facility. Es un mensaje de la norma Q.932 usado como petición o reconocimiento de un servicio suplementario.

- **H.245**: EL canal de control H.245 es un conjunto de mensajes ASN.1 de control extremo a extremo, negociación de las capacidades de ancho de banda, de la apertura y cierre de los canales lógicos, de los códecs y mensajes de control de flujo.

Unas de las características que se intercambian más relevantes son:

- MasterSlaveDetermination (MSD). Mensaje usado para prevenir conflictos entre dos terminales que quieren iniciar la comunicación. Permite decidir quién actuará de maestro y quién de esclavo.

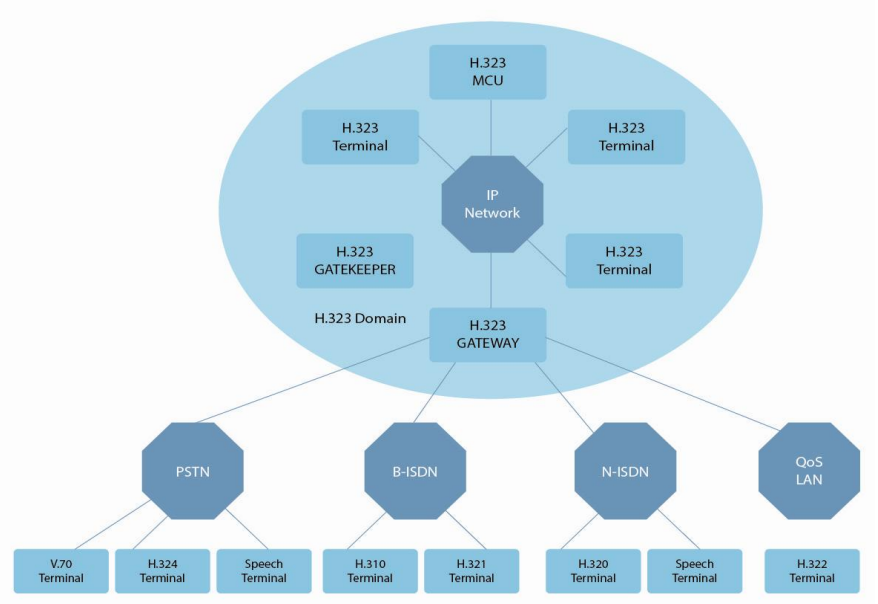
- TerminalCapabilitySet (TCS). Mensaje de intercambio de capacidades soportadas por los terminales que intervienen en una llamada.

- OpenLogicalChannel (OLC). Mensaje para abrir el canal lógico de información contiene información para permitir la recepción y codificación de los datos. Contiene la información del tipo de datos que serán transportados.

- CloseLogicalChannel (CLC). Mensaje para cerrar el canal lógico de Información[10[

- **RTP/RTCP** (*Real-Time Transport Protocol / Real-Time Transport Control Protocol*): Transporte de datos en tiempo real.

Figura 17. Arquitectura H.323.



Fuente: http://www.ciscopress.com/articles/article.asp?p=1339559&seqNum=7

[10] Gómez Vivas Luis Hernando. Ejemplo H.323 [online] [citado el 14 de agosto de 2012] disponible en Internet http://www.voipforo.com/H323/H323ejemplo.php

5.3 COMUNICACIÓN H323

Una comunicación H323 se llevaría a cabo de la siguiente manera:

- **Establecimiento**

Uno de los terminales se registra en el gatekeeper utilizando el protocolo RAS (mensajes ARQ y ACF).

Mediante el protocolo H.225 se manda un mensaje de inicio de llamada (*SETUP*) con los datos (IP y puerto) de llamante y llamado.

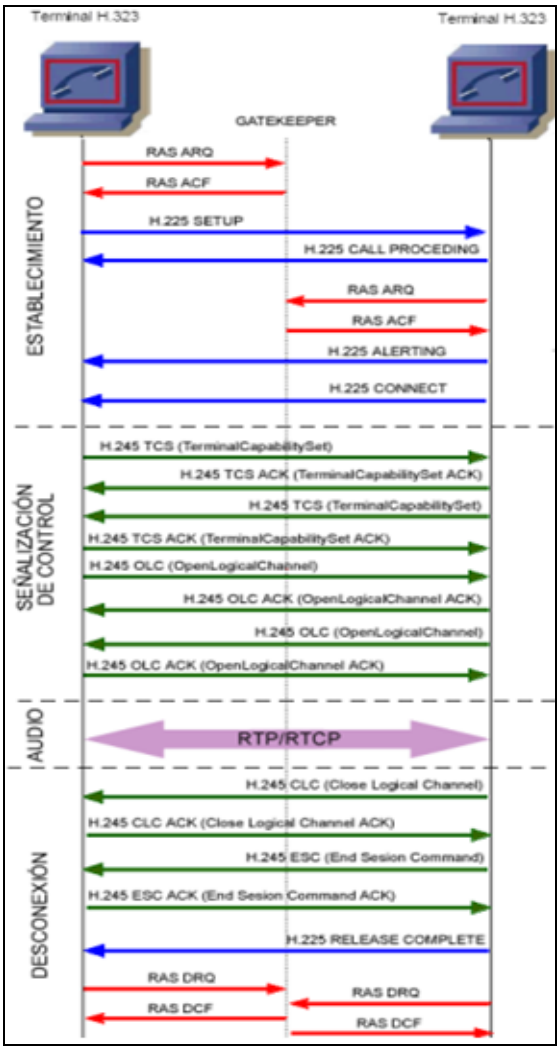
El terminal llamado contesta con *CALL PROCEEDING*.

El segundo terminal tiene que registrarse con el gatekeeper de manera similar al primer terminal.

ALERTING indica el inicio de generación de tono.

CONNECT indica el comienzo de la conexión.

Figura 18. Comunicación H.323



Fuente: http://www.voipforo.com/H323/H323ejemplo.php

- **Señalización de Control**

Se establece una negociación mediante el protocolo H.245, para indicar quién será servidor y quién será el cliente, las capacidades de los participantes y los códecs a utilizar. Al final de esta negociación se abre el canal de comunicación (direcciones IP, puerto).

- **Audio (+ DATOS y/o VÍDEO)**

Mediante RTP/RTCP. Los terminales inician la comunicación y el intercambio de audio (+ datos y/o vídeo)

- **Desconexión**

– Cualquiera de los participantes activos puede iniciar el proceso de finalización de llamada mediante mensajes Close Logical Channel y End Session Comand de H.245.
– Posteriormente utilizando H.225 se cierra la conexión con el mensaje RELEASE COMPLETE
– Por último se liberan los registros con el gatekeeper utilizando mensajes del protocolo RAS.

6. CALIDAD DE SERVICIO (QOS)

La VoIP comúnmente se despliega en redes convergentes de IP que transportan datos, tráfico de voz y vídeo. Cuando estas se congestionan, los recursos de red pueden afectar gravemente la calidad del tráfico VoIP causando una mala experiencia en la prestación del servicio.

Por lo tanto, es muy importante para una empresa implementar QoS para el tráfico VoIP en sus redes. Esto puede ayudar a garantizar la buena calidad de voz cuando se congestionan los recursos de red.

Hay una serie de factores que pueden afectar a la calidad del tráfico VoIP percibida por el usuario. Algunos de los factores comunes son retardo, jitter y pérdida de paquetes. Estos factores pueden ser los principales indicadores de la estado general de la red de voz y se define de la siguiente manera:

Retardo:

El tiempo que tarda el tráfico de VoIP para llegar de un extremo a otro se conoce normalmente como el retardo de extremo a extremo. El retraso puede ser medido ya sea en un solo sentido o el retraso de ida y vuelta. La recomendación ITU G.114 señala que el retraso aceptable para la voz es 150 ms. Cualquier retraso> 150 ms puede dar lugar a una calidad de voz degradada y la mala experiencia de usuario.

Los retardos en la red pueden ser reducidos mediante el protocolo de reservación RSVP. El retardo debido a la compresión vocal se puede eliminar usando la velocidad de 64 kbps sin compresión (G.711). Actualmente, con el modelo de una red IP de alta velocidad, la compresión vocal no es obligatoria en una red local. En

este caso, Telefonía-IP se desarrolla para brindar una red de servicios integrados soportada en protocolo IP, sin límites en el ancho de banda.

Cuando se trabaja con señales en Internet en cambio, el ancho de banda es limitado y por ello se requiere compresión vocal. Por ejemplo, el tamaño de un paquete RTP incluye 66 Bytes de encabezado (26 de MAC, 20 de IP, 8 de UDP y 12 de RTP) y 71 de carga útil. El overhead puede ser comprimido. La información vocal puede ser reducida. Por ejemplo: para G.723 trabajando a 6,3 kbps (trama de 30 mseg) sin supresión de silencios se requieren 11 paquetes/seg y 71 Bytes/paquete. Si se integra la supresión de silencios (técnica VAD) esta velocidad se reduce sustancialmente.

- **Retardo de propagación:** Es un problema físico, que aumenta con la distancia a transmitir, y que carece de importancia en redes locales o metropolitanas.

- **Retardo de transmisión del enlace:** El tamaño de los paquetes que transportan la información y el ancho de banda de los enlaces por los que circula influyen directamente en el retardo total. Este retardo impone una fuerte restricción a los tamaños que pueden presentar los paquetes.

- **Retardo de procesado en los nodos:** Cada vez que un paquete atraviesa un nodo, éste tiene que procesarlo, y realizar algunas operaciones con él. En una red de VoIP tenemos también gateways que introducen retardo pasando la información digital a analógica y viceversa.

- **Retardo por saturación de los nodos en redes asíncronas:** Este retardo es debido al encolamiento de los paquetes en los buffers de los nodos. Al llegarle a un nodo paquetes de distintos orígenes tiene que hacer un encolamiento de estos paquetes, y en casos, incluso descartarlos, si no tienen cabida en el buffer de datos. De entre todos los posibles factores que provoca retardo es

éste el más variable y el más difícil de acotar eficientemente. Junto con el retardo de encaminamiento en los nodos, este retraso es el que determina en gran medida la incapacidad de Internet convencional para transportar flujos en tiempo real.

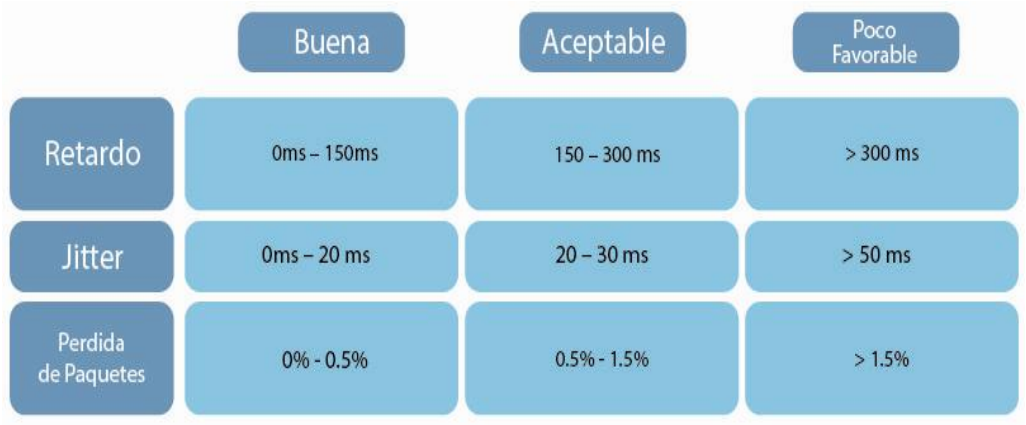
- **Retardo de codificación y descodificación:** La comunicación a través de VoIP requiere de un proceso de codificación-decodificación tanto en el transmisor como en el receptor. Este tiempo hay que añadírselo al que tarda en comprimir los paquetes. Cuanto más comprimidos estén los paquetes, menos retardo de transmisión, pero mayor complejidad de los algoritmos de compresión. Debería entonces existir un compromiso en ese aspecto.

- "**Jitter**: Es la variación en la demora del tiempo utilizado por los paquetes de ir de un extremo a otro. Si el retardo de la transmisión varía también en una llamada de VoIP, la calidad de la llamada se verá muy degradada. La Red de VoIP típicamente compensa esto al tener búferes de fluctuación en los puntos finales, para entregar el tráfico de VoIP para el usuario final a una velocidad constante. Si el Jitter es demasiado alto, puede desbordar el búfer de fluctuación en los puntos finales que resultan en la pérdida de paquetes y la mala calidad de la voz." [7] [8]

- **Eco**. Las características anteriores (retardo y jitter) pueden producir eco sobre la señal, lo cual hace necesario el uso de canceladores de eco (ITU G.168). El cancelador de eco se construye mediante la técnica de ecualización transversal auto-adaptativa. Consiste en usar una parte de la señal de transmisión para cancelar el eco producido por la desadaptación de impedancias en el circuito híbrido que convierte de 4 a 2 hilos.

- **Pérdida de paquetes:** Es el número de paquetes perdidos en la ruta de datos en el tráfico VoIP de un extremo a otro. Una pérdida del 3 por ciento de paquetes es típicamente considerado como el límite máximo tolerable para una buena calidad de voz. La red de VoIP debe ser el diseño de <1,5% de pérdida de paquetes con el fin de garantizar una buena calidad de voz.

Figura 19. Límites aceptables para los factores clave de la QoS.



Fuente: http://www.ciscopress.com/articles/article.asp?p=1339559&seqNum=7

Definición de una metodología de calidad de servicio

La política de calidad de servicio implementada para el tráfico de VoIP debe abarcar la red de voz de extremo a extremo. Se recomienda adoptar un enfoque QoS de capas lo cual hace que sea más fácil de implementar y administrar.

La política de QoS para el tráfico VoIP debe cubrir Capa 2, Capa 3, así como la capa de aplicación. Esto ayudará a garantizar que el tráfico VoIP tenga un trato preferencial, ya que va de un extremo al otro. QoS en la capa de aplicación es útil especialmente cuando los usuarios están usando las aplicaciones de VoIP basados en PC para realizar y recibir llamadas de voz. En este caso, el tráfico VoIP puede recibir el QoS deseada a medida que atraviesa la red, pero la aplicación basada en PC de usuario final puede no priorizar VoIP a través de otras aplicaciones que exigen recursos de la CPU. Esto puede dar como resultado mala

calidad de voz debido al retardo, fluctuación o la pérdida de paquetes como se describió anteriormente.

Algo para tener en cuenta es que la calidad de servicio sólo puede ayudar cuando se congestionan los recursos. Si no hay congestión de ancho de banda y otros recursos de la red, luego aplicar QoS puede no proporcionar ningún beneficio adicional.

Servicios diferenciados para la aplicación de QoS

Una buena política de calidad de servicio implica el marcado y la clasificación del tráfico de VoIP en el borde de la red para que los dispositivos intermedios en la red puedan diferenciar el tráfico de voz del resto del tráfico y el proceso de acuerdo a la política definida.

Dif. Serv define el comportamiento deseado en la ruta de transmisión para proporcionar una calidad de servicio para diferentes clases de tráfico. Un aspecto muy importante en la definición de comportamiento ruta de renvío de QoS es el método de hacer la clasificación de paquetes. Se requiere la clasificación de paquetes de calidad de servicio con el fin de determinar qué tratamiento tendrá un paquete en particular en la asignación de recursos compartidos.

La Calidad de servicio se lleva a cabo mediante la clasificación de los datos, a menudo estableciendo unos bits en la cabecera IP (denominados bits de tipo de servicio “TOS, Type Of Service”, o pueden ser punto de código de servicios diferenciándoos “DSCP Differentiated Services Code Point”; y que permiten que las distintas clases de datos sean tratados de forma diferente, determinadas clases pueden tener más prioridad que otras. A algunas clases se les puede garantizar un ancho de banda mínimo durante una congestión.

Un DSCP (Differentiated Services Code Point) especifica un comportamiento por salto (PHB) para la transmisión de tratamiento. Un PHB especifica un tratamiento de programación que los paquetes marcados con el DSCP recibirán. Un PHB también puede incluir una especificación para el tráfico acondicionado.

La calidad de este servicio se logra bajo los siguientes criterios:

Optimizar el ancho de banda, controlar las fluctuaciones de la red (jitter) que no exceda de 30 ms; minimizar la latencia o retardo que no exceda de 150 ms; y la perdida de paquetes que no exceda del 1 por ciento.
La supresión de silencios, otorga más eficiencia a la hora de realizar una transmisión de voz, ya que se aprovecha mejor el ancho de banda al transmitir menos información.

Compresión de cabeceras que son los flujos de datos que encabezan las comunicaciones de VoIP aplicando los estándares actuales

PROTOCOLOS SIP, IAX2 Y H.323 Y LA CALIDAD DEL SERVICIO QoS

Hay ciertas funciones que deberían cumplir un protocolo que intentara asegurar la calidad de servicio:

- **Clasificación de paquetes:** agrupar los paquetes según alguna propiedad de su cabecera. Detectar flujos individuales teniendo en cuenta la posible presencia de fragmentación, comprensión de cabecera y encriptación.

- **Medida:** monitorizar las características de tráfico. Comprobando si los flujos cumplen sus exigencias e informando a los componentes de red.

- **Control de política:** decidir qué paquete eliminar en caso necesario y bajo qué condiciones.

- **Control de admisión:** a la llegada de paquetes de la red comprobar si éstos pueden ser transportados sin problemas y actuar de alguna forma en caso contrario.

- **Marcado:** marcar paquetes cuando se cumplan ciertas condiciones, para que puedan ser tratados de forma correcta por el mismo u otro equipo de transmisión.

- **Conmutación:** decidir por donde se debe enviar e paquete, consultando las tablas de enrutamiento.

- **Encolado:** si el paquete no puede ser enviado de forma inmediata (congestión), se puede meter en una cola para futuro envío.

CONSIDERACIONES DE SEGURIDAD DE LOS PROTOCOLOS

Protocolo SIP

Respecto al proceso de autenticación de usuarios, SIP utiliza un sistema de reconocimiento/respuesta basado en la siguiente secuencia: inicialmente el cliente origen envía una solicitud INVITE al servidor proxy destino; este envía un mensaje de autorización 407 como repuesta, dicho mensaje contiene un conjunto de caracteres aleatorios, el cual se utiliza junto con la contraseña para generar la función hash MD5; en el siguiente envío de la primitiva INVITE se regresa dicha función. El cliente se autentica sólo si ambas funciones la que genero y la que recibe. Son iguales.

SIP proporciona diversos métodos para minimizar los efectos ocasionados por los ataques de negación de servicio, sin embargo cada vez son más difíciles de prevenir, por lo anterior SIP implementa un mecanismo de seguridad en la capa de transporte entre el llamador y el dominio de llamado, considerando las políticas de seguridad de la red.

Protocolo H.323

H.323 es un protocolo relativamente seguro y no requiere muchas consideraciones de seguridad más allá de las comúnmente utilizadas por cualquier red que se comunica con Internet. H.323 utiliza el protocolo RTP para comunicaciones de media, por lo que soporta la trayectoria encriptada de los medios.

Protocolo IAX2

IAX2 soporta tres procesos de autentificación: texto plano, hash MD5 y contraseña RSA de intercambio. Dichos procesos no consideran el cifrado de medias ni de las cabeceras entre puntos finales para ello existen soluciones que incluyen el uso de un artefacto de red privada virtual o de software para encriptar el canal en cualquier otra capa que establezca un método entre los puntos finales con túneles configurados y operacionales

SERVICIOS INTEGRADOS

Es un modelo que incluye el servicio de Best Effort (mejor esfuerzo) y la reserva de recursos para las transmisiones en tiempo real, es decir, el usuario reserva de antemano los recursos de ancho de banda que necesitará para su transmisión.

Este modelo ofrece ventajas tales como que el administrador cree las reglas de QoS para cada transmisión y ciertas simplicidad de implementación. La desventaja que se puede mencionar es que se deben enviar mensajes de señalización por

cada flujo de datos, lo cual aumenta el tráfico en la red y puede ocasionar congestión.

SERVICIOS DIFERENCIADOS

Es un modelo que permite establecer diferentes niveles de calidad de servicio a diferentes usuarios de la red, esto quiere decir que el tráfico estará distribuido en grupos. No está orientado a la reserva de recursos, por lo cual no se establece ningún canal virtual.

Esta discriminación se logra marcando el tráfico y mediante esta marca se da un tratamiento específico a los datos, de esta manera este modelo es un mecanismo para clasificar el tráfico.

COMPARACIÓN ENTRE LOS PROTOCOLOS SIP, H323 E IAX2

La VoIP requiere un conjunto de protocolos de control para el establecimiento de la conexión, intercambio de capacidades, y el control de la conferencia por lo cual existen diversos tipos de protocolos como SIP, H323 e IAX2. Se comparan entonces los protocolos sobre la complejidad, la extensibilidad, escalabilidad y servicios, además se presentan unas tablas resumen sobre las características a comparar sobre los protocolos.

COMPLEJIDAD

H.323 es un protocolo bastante complejo debido al su uso de varios protocolos que lo componen. No hay una separación clara de estos componentes; muchos servicios requieren interacciones entre varios de ellos. (El desvío de llamadas, por ejemplo, requiere componentes de H.450, H.225.0, y H.245.) El uso de varios protocolos diferentes también complica atravesar los firewall. Los cortafuegos deben actuar como proxies de nivel de aplicación, analizar todo el mensaje para llegar en los campos requeridos. La operación es con estado ya que varios

mensajes están involucrados en el establecimiento de llamada. SIP, por otra parte, utiliza una única solicitud que contiene toda la información necesaria.

H.323 define cientos de elementos, mientras que SIP tiene sólo 37 cabeceras (32 en la base de la especificación, 5 en las extensiones de control de llamadas), cada uno con un pequeño número de valores y parámetros, pero que contienen más información. Un SIP básico, pero interoperable (Aplicación de telefonía por Internet) puede llegar a funcionar con cuatro cabezales (Para, De, Call-ID, y CSeq) y tres tipos de solicitud (INVITE, ACK y BYE).

H.323 utiliza una representación binaria de sus mensajes, basado en ASN.1 y las reglas de codificación compactada (PER). ASN.1 generalmente requiere código de generadores especiales para ser analizado. SIP, en el otro parte, codifica sus mensajes en forma de texto, similar a HTTP.

EXTENSIBILIDAD

Extensibilidad es un indicador clave para medir un protocolo de señalización en la telefonía IP. La telefonía es actualmente muy popular, un servicio crítico y la telefonía VOIP está a punto de suplantar a la existente infraestructura de conmutación de circuitos. Como con cualquier servicio, las características siempre deben evolucionar al tiempo que se desarrollan nuevas aplicaciones. Esto hace que sea fundamental para construir mecanismos de extensión de gran alcance desde el primer momento.

SIP ha aprendido las lecciones de HTTP y SMTP (ambos son protocolos que han evolucionado ampliamente con el tiempo), y construido en un amplio conjunto de funciones de extensibilidad y compatibilidad.

De forma predeterminada, se omiten los encabezados y los valores desconocidos. Usando la cabecera requerida, los clientes pueden indicar los conjuntos de características que el servidor debe entender. Cuando una petición llega a un servidor, se comprueba la lista de las características mencionadas en la cabecera Requerida. Si alguno de ellos no son compatibles, el servidor devuelve un código de error y muestra el conjunto de características que no entiende.

La compatibilidad aún se mantiene a través de diferentes versiones.

Para mejorar aún más la extensibilidad, los códigos de error numéricos son organizados jerárquicamente, como en HTTP. Hay seis clases básicas, cada uno de los cuales se identifica por los dígitos en la respuesta código. El Funcionamiento básico del protocolo está dictado únicamente por la clase, y los terminales sólo necesitan comprender la clase de la respuesta.

Los otros dígitos proporcionan información adicional, por lo general útil pero no crítica. Esto permite funciones adicionales que sean añadido mediante la definición de la semántica de los códigos de error en una clase, mientras que logran la compatibilidad.

Como SIP es similar a HTTP, los mecanismos que se desarrollan para la extensibilidad HTTP también se pueden utilizar en SIP. Entre ellas se encuentran el Protocolo de Extensión de Protocolos (PEP), que contiene documentación referente de varias funciones dentro de los mensajes propios de HTTP.

H.323 requiere plena compatibilidad con cada versión anterior a la actual. Como varias características van y vienen, el tamaño de las codificaciones sólo aumentará. Sin embargo, SIP permite mantener el protocolo de manera eficaz eliminando codificaciones que no son necesarias.

Un elemento crucial para la extensibilidad son los codecs de audio y vídeo.

Hay cientos de códecs que han sido desarrollados, muchos de los cuales son propietarios. SIP utiliza el Protocolo de Descripción de Sesión (SDP) para transmitir los códec soportados por un extremo en una sesión. Lo anterior significa que SIP puede trabajar con cualquier códec, y otras implementaciones. En H.323, cada códec tiene que ser estandarizado.

Como muchos de ellos llevan significativa de la propiedad intelectual, no hay codecs libres, que se puedan utilizar en un Sistema H.323.

Otro aspecto de la extensibilidad es la modularidad. La telefonía por Internet requiere un gran número de funciones diferentes, que incluyen señalización básica, control de conferencia, la calidad del servicio, el directorio acceso, descubrimiento de servicios, etc. Es fundamental utilizar protocolos separados, para cada una de estas funciones.

SIP es razonablemente modular. Abarca la señalización de llamada básica, ubicación del usuario, y el registro. Señalización avanzada es parte de la SIP, pero dentro de una sola extensión. La calidad del servicio, el directorio accesos, servicios de descubrimiento, descripción del contenido de la sesión, y el control de la conferencia pueden residir como protocolos separados. Por ejemplo, es posible utilizar la capacidad de elementos H.245 de descripción en SIP, sin cambios en SIP en absoluto.

H.323 es menos modular. Define una suite de protocolo de integración vertical para una sola aplicación. La combinación de los servicios prestados por los componentes H.323 abarca el intercambio de capacidades, la conferencia de control, las operaciones de mantenimiento, la señalización básica, la calidad del

servicio, el registro y descubrimiento de servicios. Por otra parte, éstas se entrelazan dentro de los diferentes sub-protocolos dentro H.323.

La modularidad de SIP permite que sea utilizado en conjunción con H.323. Un usuario puede utilizar SIP para localizar otro usuario, aprovechando de sus recursos de búsqueda Multi-Salto. Cuando el usuario es finalmente encontrado, se puede utilizar una respuesta para redirigir a una URL H.323, lo que indica que la comunicación se realizará con H.323.

ESCALABILIDAD

H.323 y SIP se diferencian también en términos de escalabilidad.

Se puede observar la escalabilidad en varios niveles: Grandes cantidades de Dominios: H.323 fue originalmente concebido para su uso en una sola LAN. La versión más reciente define procedimientos, el concepto de una zona, y define la ubicación del usuario a través de zonas de nombres de correo electrónico. Sin embargo, para un gran número de dominios, y las operaciones de localización, H.323 tiene problemas de escalabilidad. SIP, sin embargo, utiliza un algoritmo de detección de bucle, el cual se puede realizar de una manera sin estado.

Procesamiento Servidor: En un sistema H.323, ambos gateways de telefonía y gatekeepers tendrán que gestionar las llamadas de una multitud de usuarios. Del mismo modo, los servidores SIP y pasarelas pueden manejar muchas llamadas.
En SIP, una transacción a través de varios servidores y puertas de enlace pueden ser con o sin estado.

El SIP se puede realizar en TCP o UDP. En el caso de UDP, no se requiere el estado de conexión. Esto significa que los servidores grandes, pueden estar basados en UDP y operan de una manera sin estado, lo que reduce significantemente los requisitos de memoria y la mejora de la escalabilidad.

H.323, por otra parte, requiere controladores de acceso, al ser con estado. Deben mantener el estado de la llamada toda la duración de la llamada. Además, las conexiones son basadas en TCP, lo que significa un gateway debe mantener sus conexiones TCP para toda la duración de una llamada. Esto puede plantear graves problemas de escalabilidad a los gateway.

Además, una pasarela o guardián tendrán que procesar los mensajes de señalización para cada llamada. SIP es más fácil de procesar que H.323, así que SIP debería permitir manejar más llamadas por segundo que H.323.

H.323 soporta conferencias entre varios usuarios. Sin embargo, se requiere un punto de control central (llamado MC) para el procesamiento de todas las señales, incluso para las conferencias más pequeñas.

En SIP, no hay necesidad de un control central; la coordinación de la conferencia está totalmente distribuida. Esto mejora la escalabilidad y la complejidad. Por otra parte, ya que puede utilizar UDP, así como TCP, SIP soporta señalización multicast nativo, permite que un solo protocolo escalar sesiones hasta con dos a millones de miembros.

Retroalimentación: define los procedimientos H.245 que permiten a los receptores, control de codificaciones de medios, las tasas de transmisión y recuperación de errores.

Este tipo de retroalimentación tiene sentido en escenarios de punto-a-punto, pero deja de ser funcional en la conferencia multipunto.

SIP, en cambio, se basa en RTCP para proporcionar información sobre la calidad de recepción (y también para la obtención de listas de miembros del grupo). RTCP, como SIP, funciona de una manera totalmente distribuida. La

retroalimentación que proporciona escala automáticamente desde un punto de dos personas a punto de conferencia para grandes conferencias estilo de difusión con millones de participantes.

SERVICIOS

H.323 y SIP ofrecen servicios más o menos equivalentes.

Además de llamar a los servicios de control, tanto SIP (cuando se utiliza con SDP) y H.323, ofrecen servicios de cambio de capacidades. En este respecto, H.323 proporciona un conjunto mucho más rico de funcionalidad.

SIP proporciona un amplio soporte para los servicios mobiilidad, sin embargo. Cuando una persona en contacto con el destinatario de la llamada, el destinatario de la llamada puede redirigir la persona que llama a un número en diferentes ubicaciones. Cada una de estas ubicaciones puede ser un URL arbitrario, y contiene información adicional sobre el terminal en ese lugar.

SIP también soporta multi-salto para la búsqueda de un usuario.

Un servidor Proxy puede tramitar la petición de varios servidores en paralelo. Esto permite que la búsqueda del usuario pueda operar de manera más rápidamente. Para H.323 para este tipo de movilidad es más limitada. El mensaje de instalación puede redirigir una llamada que prueba varias direcciones. Sin embargo, no se puede utilizar para expresar sus preferencias, ni la persona que llama express preferencias en la invitación original llamada. H.323 no era diseñado para una operación de área amplia; lo hace el reenvío de apoyo de solicitudes de llamadas entre servidores, pero no tiene mecanismos de bucle detección. H.323 no permite que un guardián de proxy de una solicitud a varios servidores tampoco.

H.323 soporta varios servicios de control de la conferencia. SIP no proporciona control de la conferencia, basándose en cambio, en otros protocolos para este servicio.

Tabla 2. Comparación entre protocolos de señalización

	H323	SIP	IAX
CODIFICACION Ó TIPO DE MENSAJE	Formato Binaria	Formato Texto	Formato Binario
ARQUITECTURA	Distribuida	Distribuida	Distribuida
NUMERO DE PUERTOS	3	3	1
SEGURIDAD	Via H.235 (Puede usar TLS)	Análogo a http (SSL, TLS, SSH)	MD5. No permite cifrado entre terminales
ESTANDARIZACIÓN	SI(ITU-T)	SI(IETF)	NO Estandarizado
SEÑALIZACIÓN	Datos y señalización por diferentes puertos	Datos y señalización por diferentes puertos	Datos y señalización por diferentes puertos
TRANSPORTE	TCP, UDP	TCP, UDP	UDP
NAT	Definido por el proxy H.323	Requiere de un servidor para realizar NAT	-
ANCHO DE BANDA	Mayor	Mayor	Menor
DISPONIBILIDAD	Menor	Mayor	Menor

Fuente: Los Autores

7. CONCLUSIONES

Se logró con la investigación un conocimiento teórico acerca de los protocolos y herramientas utilizadas notando las ventajas, beneficios y seguridad.

En la comunicación de VoIP, los protocolos de señalización realizan las labores más importantes ya que se dedica a la gestión de los recursos de la red; por esta razón es importante seleccionar un buen protocolo de señalización; debido a que estos definen además la estructura de la red a implementar; así como también la eficiencia de la misma.

El modelo de funcionamiento cliente-servidor del protocolo de inicio de sesión SIP, es una de las razones que le ha permitido ser el protocolo de señalización más utilizado. Ya que le permite ser eficiente y simple. Debido a que su implementación puede ser amplia y fácilmente compatible con diferentes arquitecturas de red: al mismo tiempo facilita el desarrollo de nuevas aplicaciones Voip.

La telefonía IP es una tecnología que tiene todos los elementos para su rápido desarrollo. Aunque actualmente el uso de la telefonía IP no está ampliamente extendida, es previsible que su uso se generalice en un futuro.

Se logró afianzar los conocimientos teóricos acerca de las características de los protocolos enfatizando los temas de ventajas, beneficios, calidad de servicio y seguridad.

La telefonía VoIp ha logrado posicionarse desplazando a la telefonía tradicional, esto sin disminuir la calidad en la prestación del servicio, desarrollando para lo anterior protocolos suficientemente robustos y así vencer los inconvenientes que

se presentan al tratar de cubrir las prestaciones y beneficios que ofrece la telefonía de VoIp.

Aunque los protocolos para VoIp presentan similares características en relación a sus prestaciones, se observa que el protocolo SIP se adapta más fácilmente en cuanto a escalabilidad facilitando la interconexión de forma más sencilla a una cantidad más significativa de usuarios en una conferencia.

Los protocolos aquí analizados demuestran que cada uno tiene sus fortalezas en determinadas tareas, pudiéndose del mismo modo utilizar combinación de estos protocolos en la integración de un sistema completo de VoIP.

BIBLIOGRAFIA

DIAZ GOMEZ, Juan Pablo, Prototipo de Interconexión de Voz sobre IP entre la red de universidades de Santander (UNIRED) y la Red Nacional Universitaria (RENATA), por medio del Protocolo SIP, basados en Herramientas de Código Libre. Trabajo de Grado Especialización en Telecomunicaciones: Universidad Industrial de Santander Facultad de ingenierías Fisicomecanicas. Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones, 2011.

GOMEZ VIVAS, Luis Hernando, VILLAMIZAR JIMENEZ, Gloria Esthella. Diseño de un Modelo de Red con Tecnología Voz Sobre IP para la empresa Coomultrasan Multiactiva entre las sedes del área Metropolitana de Bucaramanga. Trabajo de Grado Especialización en Telecomunicaciones: Universidad Industrial de Santander Facultad de ingenierías Físicomecánicas. Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones, 2010.

HUIDOBRO MOYA, José M. y ROLDAN MARTÍNEZ, David. Comunicaciones en Redes Wlan. Creaciones Copyright 2006. Pág.24

Protocolos que describen la unidad de control del sistema para la recomendación H.323.

E-GRAFÍA

ADEEL Ahmed, Habib Madani, Talal Siddiqui. VoIP Performance Management and Optimization: Managing VoIP Networks. [En línea]. [Citado el 10 de Octubre de 2012]. Disponible en: http://www.ciscopress.com/articles/article.asp?p=1339559&seqNum=7

DIEGO_DISENO_RED_TELEFONIA_IP_RAAP.pdf?sequence=2

PAPAGEORGIOU Pavlos, A Comparison of H.323 vs SIP. [En línea]. [Citado el 13 de Octubre de 2012]. Disponible en: http://www.cs.umd.edu/~pavlos/papers/unpublished/papageorgiou01comparison.pdf

PEINÓ DIAZ, Víctor. Softphone con soporte IAX2 para Android [En línea]. [Citado el 01 de septiembre de 2012]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/8161/1/vpeino1_TFC_0611.pdf

QUINTANA CRUZ, Diego. Diseño e implementación de una red de telefonía IP con software libre en la raap [En línea]. [Citado el 14 de Julio de 2012]. Disponible en: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/205/QUINTANA_

SANTAMARÍA GONZÁLEZ, Wilmer. Protocolos de señalización usada actualmente para terminales móviles e ip. [En línea]. [Citado el 20 de Noviembre de 2012]. Disponible en: http://www.konradlorenz.edu.co/images/stories/articulos/explorando_bases_telecomunicaciones.pdf

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, ITU-T Recommendations H.323 v7 (12/2009). [En línea]. [Citado el 27 de Octubre de 2012]. Disponible en: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=H.323