UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESTUDIO Y DISEÑO DE UN SISTEMA DE VIDEOCONFERENCIA BASADO EN IP PARA EL SECTOR EMPRESARIAL Y ORGANISMOS ESTATALES DEL PERÚ

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

SEGUNDO CELSO GARCIA QUINTANILLA

PROMOCIÓN

2012-I

LIMA-PERÚ

2015

ESTUDIO Y DISEÑO DE UN SISTEMA DE VIDEOCONFERENCIA BASADO EN IP PARA EL SECTOR EMPRESARIAL Y ORGANISMOS ESTATALES DEL PERÚ

DEDICATORIA:

A mis abuelas Isabel y Teodora por su cariño, atención y dedicación en todos estos años.

SUMARIO

El presente informe tiene como finalidad presentar y describir el estudio y diseño de un sistema de videoconferencia basada en el protocolo IP para el sector empresarial y organismos estatales del Perú. Como caso de estudio se analiza un proyecto de telecomunicaciones del Organismo Supervisor de las Contrataciones del Estado (en adelante OSCE), llamado *Adquisición de un Sistema de Videoconferencia*.

La solución de ingeniería de redes se enfoca en la elección y diseño de un sistema de videoconferencia que se integre al actual sistema de telefonía IP, el cual controla los teléfonos de todas las sedes del OSCE, obteniendo como resultado la mayor cantidad de beneficios para el OSCE. Para el diseño y estudio se presenta el análisis de la situación inicial evaluando sus vulnerabilidades para luego proponer, se proponen dos alternativas de solución denominadas: "Alternativa Cisco" y "Alternativa Polycom"; ambas consisten en la elección de la marca mencionada para la elaboración del diseño del Sistema de Videoconferencia; al finalizar se sustenta la elección de una de estas

La adquisición de un Sistema de Videoconferencia para el OSCE, incrementa el número de reuniones y audiencias públicas del Tribunal del OSCE con empresas licitantes, se reducen los tiempos de planificación de reuniones y mejora la interacción, comunicación y productividad de los trabajadores de todas las sedes del OSCE a nivel nacional.

ÍNDICE

INDICE DE FIGURAS

INDICE DE TABLAS

GLOSARIO DE TÉRMINOS

AAA	Authentication, Authorization, Accounting
ACE	Application Control Engine
ACL	Access Control List
ACS	Access Control *Server*
ATM	Asynchronous Transfer Mode
CUCM	Cisco Unified Communication Manager
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
HSRP	Hot Standby Routing Protocol
HTTP	Hypertext Transport Protocol
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
ILS	Internet Locator Service
IP	Internet Protocol
IPS	Intrusion Prevention System
ISP	Internet ServiceProvider, Proveedor de Servicios de Internet
ITU	International Telecommunication Union
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
MCU	Unidad de Control Multipunto de Video
MOS	Mean Opinion S*Core*
NAT	Network AddressTranslation
OSCE	Organismo Supervisor de las Contrataciones del Estado
OLC	Open Logical Channel
PAM	Modulación por amplitud de pulso
PBX	Private Branch Exchange
PCM	Modulación por codificación de pulsos
PSTN	Public *Switch*ed Telephone Network
RADIUS	Remote Authentication Dial-In User *Server*
RTP	Real-Time Transport Protocol

RSVP	Resource Reservation Protocol
RTSP	Real Time Streaming Protocol
SAP	Session Announcement Protocol
SCCP	Skinny Client Control Protocol
SIP	Session Initiation Protocol
SDP	Session Discovery Protocol
SNR	Signal Noise Relation
SSH	(Secure Shell)
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network (Cioara & Valentine, 2012)
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

INTRODUCCIÓN

El objetivo del trabajo descrito en el presente informe es mostrar los elementos de un sistema de videoconferencia basado en el protocolo IP para el sector empresarial y entidades públicas del Perú, mediante un diseño aplicado a la entidad estatal OSCE.

La solución se enfoca en el tratamiento de la data de videoconferencia generada en los terminales de cada sede, como punto de inicio y llevada por toda la red, a través de sistemas de control de llamadas de video.

Un sistema de videoconferencia está conformado, y se explica en el diseño, por códecs de video (codificador de video), unidades de control multipunto de video (MCU), Sistema de registro de terminales de videoconferencia IP (H.323 y/o SIP), terminales de videoconferencia IP, servidores (contiene el sistema encargado de hacer el control de llamadas), servidor de control de acceso y servicios de red y red de transporte del Proveedor de Servicios de Internet (ISP).

El diseño se realiza para las 21 sedes de la entidad estatal OSCE, distribuidas en varios departamentos del Perú. Cada sede, tendrá un terminal de videoconferencia y este se enlazará a la nube internet a través de un *Router* Cisco 2901 en donde se implementará protocolos de enrutamiento BGP, MPLS (Se explica en el marco teórico) y un *Switch Catalyst* 2960 como punto de acceso al terminal. La conexión a internet deberá ser dedicada y síncrona, es decir velocidad similar de envío y de recepción de paquetes. La sede de Lima es la sede central en la cual estarán dos terminales de videoconferencia de mayores capacidades a los que están en provincia, y la infraestructura de videoconferencia Cisco (Se explica en el capítulo IV).

El desarrollo del proyecto de ingeniería se basa principalmente en la documentación técnica del equipamiento utilizado, proveniente de *Cisco Systems Inc.* También se ha consultado diversa bibliografía referente a códecs de video y recomendaciones ITU. El informe de ingeniería fue realizado gracias a la experiencia adquirida durante dos años, en proyectos similares de ingeniería de redes. El informe se divide en cuatro capítulos:

Capítulo I: Planteamiento de ingeniería del problema.- Se describe el problema y los objetivos, se explica la justificación de la solución, se determina el alcance del proyecto y finalmente se hace una síntesis del informe.

Capítulo II: Marco teórico conceptual.- Se expone las bases teóricas conceptuales relacionadas con la solución. En este capítulo se desarrollan los siguientes temas: Servidores de Control de llamadas IP, protocolos y características relacionadas con la alta disponibilidad, seguridad informática, estándares de señalización, códec de Video, etc.

Capítulo III: Caso de Estudio.- Se presenta el caso de estudio con la finalidad de mostrar un diseño de red de videoconferencia para la entidad gubernamental OSCE.

Capítulo IV: Metodología para la solución del problema.- Este capítulo describe la ingeniería en el diseño del proyecto de sistema de videoconferencia. Se realiza el análisis preliminar para determinar la solución a implementar, posteriormente se explica la solución implementada y finalmente, se hace una descripción técnica del equipamiento utilizado.

Capítulo V: Análisis y presentación de resultados.- En él se presenta la estructura de costos del proyecto, el cronograma de trabajos así como las pruebas a realizar.

CAPÍTULO I
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

En este capítulo se realiza el planteamiento de ingeniería del problema. Se describe el escenario actual, descripción del problema y se expone el objetivo del trabajo. Se hace una evaluación del problema y se precisan los alcances del informe; para concluir, se presenta una síntesis de la solución.

1.1 Descripción y Presentación del problema: Sistema de Videoconferencia para Entidad Estatal

La entidad gubernamental OSCE usa terminales de videoconferencia como apoyo tecnológico para llevar a cabo una de sus funciones, "resolver, en última instancia administrativa, las controversias que surjan entre las Entidades y los postores durante el proceso de selección, así como de aplicar sanciones de suspensión o inhabilitación a proveedores, postores y contratistas por infracción de las disposiciones de la Ley, su Reglamento y demás normas complementarias". (Tribunal de la OSCE, 2015)

Actualmente el OSCE cuenta con una solución de videoconferencia, la cual presenta limitaciones en la administración ya que el servicio es ofrecido en la modalidad de arrendamiento o alquiler, la marca de estos terminales no es un líder en el mercado de videoconferencia ni de redes. El servicio no muestra calidades en HD de las videoconferencias generadas con estos terminales.

La institución cuenta con enlaces de internet dedicado por cada sede que comprende este estudio, además de una infraestructura de red disponible como enrutadores Cisco ISR 2911 y *Switches* Cisco *Catalyst* 2960.

1.2 Objetivos del Informe

El objetivo del trabajo descrito en el presente informe es dar a conocer los elementos de un sistema de videoconferencia basado en el protocolo IP para el sector

empresarial y entidades públicas del Perú, mediante un diseño aplicado a la entidad estatal OSCE.

Esto es llevado a cabo mediante la interconexión de sistemas de videoconferencia como sistemas de control multipunto de video, terminales de videoconferencia (con protocolos H.323 y SIP), *Firewalls* y servidores.

En el caso de estudio, se tendrá en cuenta los requerimientos y requisitos mencionados en las especificaciones técnicas del proyecto sistema de videoconferencia, se requiere que debe integrarse a la central de telefonía IP que actualmente tiene el OSCE. Para dar cumplimiento al objetivo principal mencionado se plantea abarcar los siguientes objetivos secundarios:

- Descripción de las características y beneficios de los sistemas de videoconferencias IP en las comunicaciones empresariales.
- Plantear un diseño de red que cumpla con los requerimientos del proyecto.
- Realizar un presupuesto y costeo de los gastos implicados en la realización del proyecto. Este presupuesto estará acorde al valor referencial del presente proyecto.

1.3 Evaluación del problema

El uso de la videoconferencia en la situación de la entidad OSCE es para brindar el apoyo tecnológico para la ejecución de diversos procedimientos administrativos, como son audiencias públicas, entrenamientos, reuniones, etc.

Actualmente el OSCE no cuenta con un sistema de videoconferencia propio. La necesidad de contar con tal sistema para este ente estatal, trae muchos beneficios que se pueden cuantificar en materia de productividad laboral, comunicación a través del lenguaje corporal para la toma de decisiones, competitividad, ahorro de logística en la generación de reuniones, entre otras. Los beneficios se pueden cuantificar en términos económicos, es por eso que la entidad pública OSCE puesta por contar con esta tecnología en sus instalaciones.

Las funcionalidades que hoy en día tienen los sistemas de videoconferencia ofrecen más que solo la comunicación a través del video, como por ejemplo servicios de compartir contenido de las PC, a través de los terminales de video que participan en una sesión. Esta funcionalidad ofrecerá una comunicación más rica de video para las audiencias públicas en la cual es necesario mostrar documentos, exponer o sustentar algún tema mediante una presentación.

El sistema de videoconferencia se deberá integrar con la Central de telefonía IP de marca *CISCO SYSTEMS* Inc. (*Cisco Unified Communication Manager*, en adelante CUCM), debido a que el OSCE cuenta con esta central y desea tener la facilidad de llamar desde un videoteléfono, que está registrado al CUCM, a un terminal de videoconferencia.

En resumen la solución del problema no sólo es a nivel de ingeniería o tecnología sino trasciende más allá en beneficios laborales y sociales, siendo esta la finalidad de la carrera de ingeniería.

1.4 Alcance del informe

El informe desarrolla el diseño de un sistema de videoconferencia que se puede aplicar para una empresa en especial el caso de estudio se centra en la Oficina Supervisora de las Contrataciones del Estado.

La solución se enfoca en la elección del diseño de un sistema de videoconferencia que deberá integrarse al actual sistema de telefonía IP del OSCE, el cual controla los teléfonos de todas sus sedes, obteniendo como resultado la mayor cantidad de beneficios para el OSCE. Las sedes del OSCE son denominadas por la institución como "Sedes Desconcentradas" y están ubicadas en cada uno de los departamentos del Perú, excepto Iquitos.

1.5 Síntesis del informe

En el informe se explica la metodología para cumplir con los requerimientos, el dimensionamiento del equipamiento y de las aplicaciones a ejecutar; se muestran y explican, tanto la topología previa como la topología a implementar. También se menciona las especificaciones técnicas mínimas presentes en las Bases Integradas (Licitación Pública) del presente proyecto, el diseño y solución deben de cumplir con todas las especificaciones técnicas mínimas su totalidad

Además se describe de manera resumida los aspectos técnicos del nuevo equipamiento. En la figura 1.1 se muestra un cuadro sinóptico de la metodología de la solución del problema. En el análisis preliminar se describe la topología de la Red con todos los componentes de *networking* del OSCE, que tienen interacción con el sistema de videoconferencia, y se presentan dos alternativas de solución, las cuales son denominadas en el presente informe como: "Alternativa Polycom" y "Alternativa Cisco". En esta sección se presenta el análisis de costos del proyecto, se muestra el costo económico total de la adquisición del proyecto por parte del OSCE a Telefónica del Perú S.A.A, y se realizar un análisis de la gestión de tiempo (responsabilidades, trabajos, tareas realizadas,

tiempos), mediante un diagrama de Gantt.

El informe se complementa con los aspectos técnicos, teóricos y conceptuales relacionados a la solución del diseño del Sistema de Videoconferencia IP. En la figura 1.2 se presenta un cuadro sinóptico del marco teórico, en el que se describen los conceptos de *Voice over IP* (VoIP), Telefonía IP y Videoconferencia. El marco teórico está enfocado en la solución del problema, contiene todos los temas para un correcto entendimiento del diseño del sistema de Videoconferencia propuesto. Se abarca una gran variedad de temas de VoIP, protocolos H.323 y SIP, como introducción para una mejor explicación del marco teórico sobre la Telefonía IP y Sistemas Videoconferencia.

El lector que estudie el presente informe de suficiencia, deberá poseer conocimientos básicos del modelo OSI, *Routing* y *Switching* para un mejor entendimiento del marco conceptual y la resolución del Caso de Estudio del OSCE. El presente informe no tiene como objetivo explicar a detalle el modelo OSI ni cada las siete capas que la componen, así como tampoco explicar el funcionamiento de equipos de Redes como *Switches*, *Routers* y Servidores.

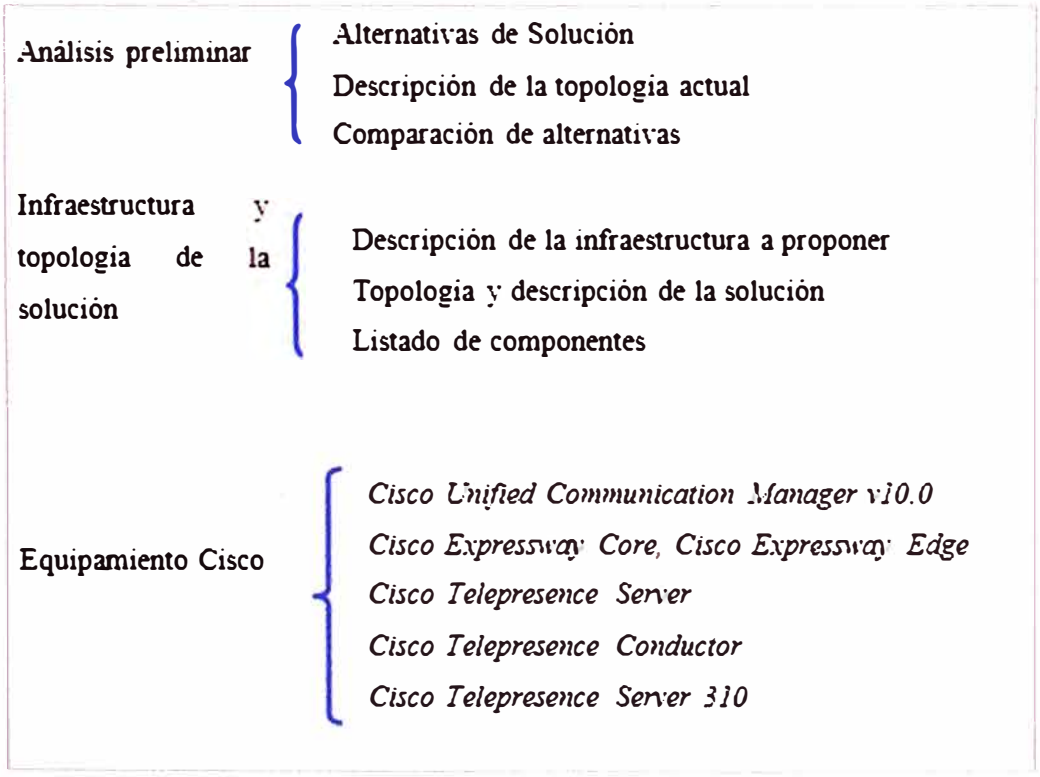


Figura 1.1 Cuadro sinóptico de la Metodología de Solución del Problema

(Fuente Ref. Elaboración propia)

Conceptos Previos de la PSTN	Componentes de la PSTN PBX. Conexiones a la PSTN, y entre la PSTN Plan Numérico en la PSTN
Introducción a los Gateways de Voz	Comunicaciones Unificadas Arquitectura de Comunicaciones Unificadas Operación de los Gateways
Fundamentos de VoIP	Descripción General de VoIP Las principales etapas de Procesamiento de Voz de VoIP Componentes de VoIP Paquetización VoIP Transmisión de Media VoIP Detección de Voz Activa Principales ventajas de VoIP
Protocolo de Señalización de Voz: H.323	Arquitectura H.323 Flujos de llamada H.323
Protocolo de Señalización de Voz: SIP	Arquitectura SIP Flujos de Llamadas SIP
Central de Telefonía IP	
Protocolos y características de redes	Redes de Área Local Virtuales (VLAN) Troncales Protocolo de agregación de enlaces (LACP) Metodología para modificar direcciones de red (NAT) Parámetros de Calidad de Servicio (QoS) Conmutación de Etiquetas Multiprotocolo (MPLS)
Seguridad informática	Generalidades Tipos de ataque Las tres principales metas de seguridad de red Firewall (corta fuego) DMZ Inspección de protocolos de aplicación Listas de acceso
Sistemas de Videoconferencia y características de video	Formatos de compresión de video, codificador y decodificador de video

Figura 1.2 Cuadro sinóptico del Marco Teórico

(Fuente Ref. Elaboración propia)

CAPÍTULO II
CONCEPTOS DE VoIP, TELEFONÍA IP Y VIDEOCONFERENCIA

En este capítulo se exponen las bases teóricas conceptuales directamente relacionadas con la solución desarrollada en este informe de suficiencia. El capítulo consta de los siguientes tópicos: Conceptos de la PSTN, VoIP, Servidores de Control de llamadas IP, protocolos y características de red relacionadas con la transmisión de voz y video por las redes IP.

2.1 Conceptos Previos de la PSTN

La red de telefonía pública conmutada (*Public Switched Telephone Network PSTN*) es una red con conmutación de circuitos tradicional optimizada para comunicaciones de voz en tiempo real. "Esta red no es diferente de muchas de las redes de datos de hoy en día. Su objetivo principal es establecer las vías de todo el mundo para que la gente se conecte fácilmente, conversar, y desconecte" (Cioara & Valentine, 2012, pág. 13)

2.1.1 Componentes de la PSTN

La PSTN moderna es ahora una red mundial (como Internet), construido a partir de las siguientes piezas, como se muestra en la figura 2.1:

a) Teléfonos Análogos (*Analog Telephone*): Dispositivo que se conecta directamente a la PSTN y es el dispositivo más común en la PSTN. Convierte audio en señales eléctricas.

b) Bucle de abonado (*Local loop*): Es el enlace entre las instalaciones del cliente (tanto en los hogares o edificios) y el proveedor de servicio de telecomunicaciones.

c) Conmutador de la Central (CO *Switch*): Proporciona servicios a los dispositivos en el bucle de abonado. Estos servicios incluyen la señalización, colección de dígitos, enrutamiento de llamadas, configuración y terminación de llamadas.

d) Troncal (*Trunk*): Provee la conexión entre conmutadores o *Switches*. Estos *Switches* pueden ser del CO *Switches* privados.

e) Conmutador privado (Private *Switch*): Permite a una empresa operar como una

"PSTN miniatura" dentro de su empresa. Esto proporciona eficiencia y ahorro de costes, ya que cada teléfono en la empresa no requiere una conexión directa con el interruptor de CO.

f) Teléfonos digitales (*Digital telephones*): Típicamente están conectados a sistemas PBX. Tienen como función convertir audio en binarios 1s y 0s, que permite comunicación más eficiente que la de los teléfonos analógicos.

Muchos creen que la PSTN finalmente será absorbida por la Internet. Aunque esto puede ser cierto, se deben realizar mejoras y avances en Internet para asegurar la calidad adecuada de servicio (*QoS: Quality of Service*) garantías para llamadas de voz.

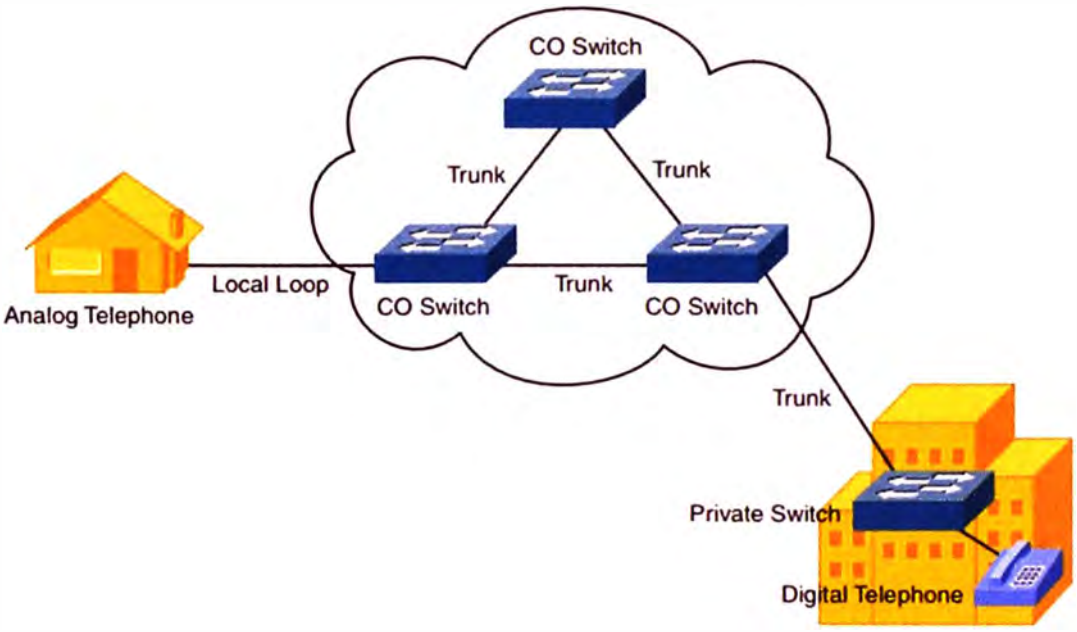


Figura 2.1 Componentes de la PSTN

(Fuente Ref. CCNA Voice 640-461 Finke & Hartmann, 2012, pág. 13)

2.1.2 PBX

La PBX (siglas en inglés de *Private Branch Exchange*) cuya traducción en inglés sería Ramal privado de conmutación, o más bien Central secundaria privada, es en realidad una central telefónica conectada directamente a la red pública de telefonía por medio de líneas troncales para gestionar además de las llamadas internas, las entrantes y salientes con autonomía sobre cualquier otra central telefónica.

Algunas Empresas tienen cientos o quizás miles de teléfonos que soportan en su organización. Si la Empresa tuviera que comprar una conexión PSTN directa por cada uno de sus teléfonos, el costo podría ser astronómico. En cambio, la mayoría de organizaciones

escoge usar una PBX internamente para administrar los teléfonos internos. Este sistema permite a los usuarios internos realizar llamadas dentro de la oficina sin usar algún recurso de la PSNT. Las llamadas a la PSTN son derivadas fuera del enlace troncal PSTN de la compañía.

2.1.3 Conexiones a la PSTN, y entre la PSTN

Existe una variedad de opciones para conectarse a la PSTN. Los usuarios domésticos y empresas pequeñas y medianas pueden conectarse usando puertos analógicos. Cada conexión analógica de dos hilos tiene la capacidad de soportar una sola llamada. Para los usuarios domésticos, una sola conexión analógica a la PSTN puede ser suficiente. Para empresas pequeñas y medianas, el número de conexiones analógicas entrantes se relaciona directamente con el tamaño de la oficina y el volumen de llamadas promedio. A medida que crecen las empresas, puede consolidar las múltiples conexiones analógicas en una o más conexiones T1 o E1 digitales, como se muestra en la figura 2.2.

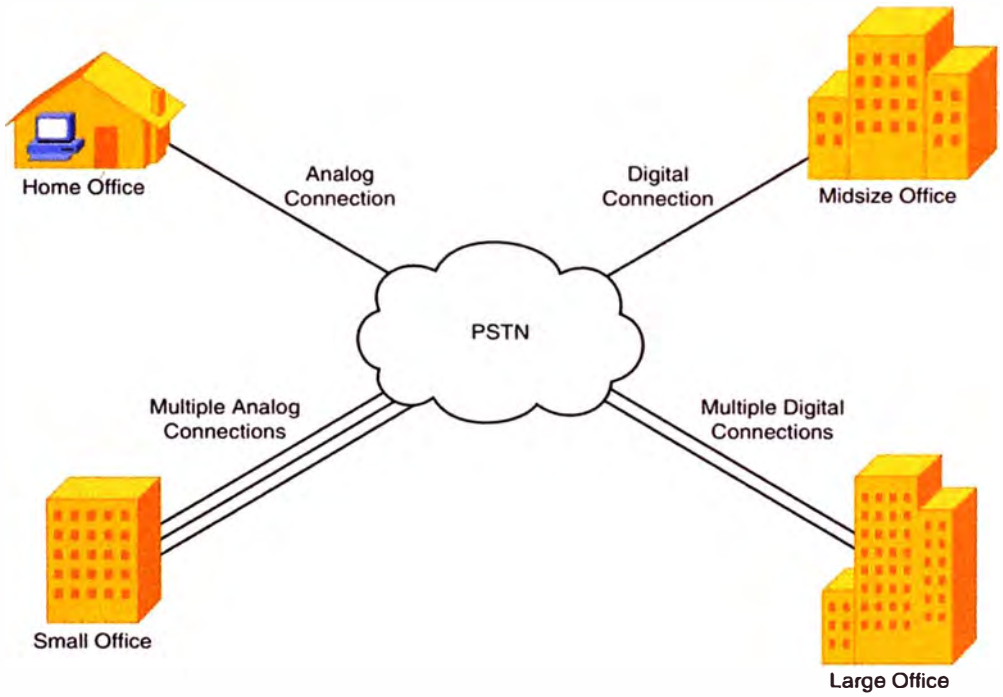


Figura 2.2 Conexiones a la PSTN

(Fuente Ref. *CCNA Voice 640-461*, Finke & Hartmann, 2012, pág. 13)

En la PSTN yace una red de redes, de forma similar a la Internet, que conecta las oficinas de varios proveedores de telefonía juntos en una red mundial masiva. Para todos los proveedores de telefonía del mundo para comunicarse juntos, un protocolo de señalización común debe ser utilizado, similar a la forma en que TCP / IP funciona en el ámbito de datos. El protocolo de señalización de voz utilizado en todo el mundo es el SS7.

2.1.4 Plan Numérico en la PSTN

Así como las redes de datos utilizan direccionamiento IP para organizar y localizar los recursos en las redes, las redes de voz utilizan un plan de numeración para organizar y localizar los teléfonos en todo el mundo. Organizaciones que gestionan sus propios sistemas de telefonía internos pueden desarrollar cualquier esquema de número interno que mejor se adapte a las necesidades de la empresa (similar al direccionamiento IP privado). Sin embargo, cuando se conecta a la red PSTN, debe utilizar una dirección norma válida, E.164 para su sistema telefónico. E.164 es un plan de numeración internacional creado por la Unión Internacional de Telecomunicaciones (UIT). Cada número en el plan de numeración E.164 contiene los siguientes componentes:

- Código de país.
- Código nacional de destino.
- Número de abonado.

Los números E.164 están limitados a una máxima longitud de 15 dígitos. Como ejemplo, el Ministerio de Transporte y Comunicaciones (MTC) es la entidad del Gobierno del Perú que administra el Plan de Numeración de Telefonía en todas sus modalidades, el número telefónico de teléfonos fijos en Lima está representado en la siguiente imagen:

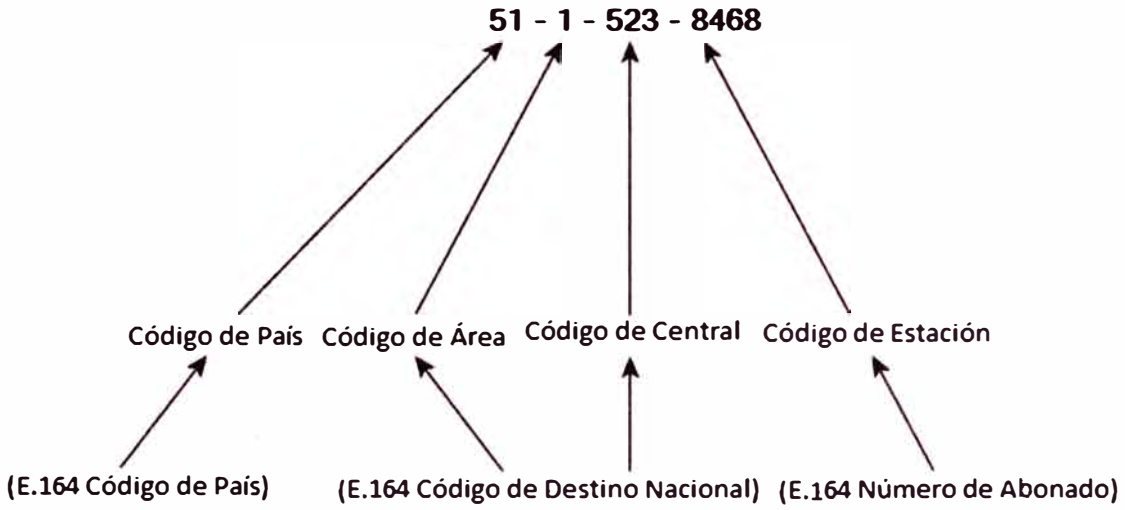


Figura 2.3 Ejemplo de número telefónico de Perú

(Fuente Ref. Elaboración propia)

2.2 Introducción a los *Gateways* de Voz

Los *Voice Gateways o Gateway* de Voz (puerta de enlace de voz) son dispositivos en las redes de datos de hoy en día que tienen la función principal es la de convertir formatos de voz, señales y métodos de transmisión como la información de voz se desplaza

sobre diferentes tipos de redes.

Esta sección describe los modos de funcionamiento de un *Gateway* de voz y como el *Gateway* se ajusta en la arquitectura de Comunicaciones Unificadas en la actualidad. Se explica las funciones del *Gateway* de Voz en cada modelo de implementación de Comunicaciones Unificadas.

2.2.1 Comunicaciones Unificadas

El sistema de Comunicaciones Unificadas integran completamente las comunicaciones de datos que permitan, voz y video para ser transmitidos a través de una única infraestructura de red que usa IP basada en estándares. Los Comunicaciones Unificadas incorporan e integra las siguientes tecnologías de la comunicación:

- Comunicaciones mediante IP son la tecnología que transmite comunicaciones de voz y vídeo a través de una red IP utilizando estándares. Los sistemas de comunicaciones unificadas de múltiples vendedores o marcas, incluyen productos de hardware y software, tales como agentes de procesamiento de llamadas (*call-processing agents*), teléfonos IP (tanto cableadas e inalámbricas), sistemas de mensajería de voz, dispositivos de video y muchas aplicaciones especiales.
- Las aplicaciones móviles mejoran el acceso a los recursos de la empresa, aumentan la productividad y aumentan la satisfacción de los usuarios móviles.
- La atención al cliente permite comunicaciones eficientes y eficaces de los clientes a través de una red global. Esta estrategia permite a las organizaciones sacar de una gama más amplia de los recursos a los clientes del servicio. Incluyen acceso a un gran número de agentes y múltiples canales de comunicación, así como las herramientas de auto-ayuda al cliente.
- Sistemas de Telepresencia (Videoconferencia) y conferencias mejoran el entorno de reunión virtual con un conjunto integrado de herramientas basadas en IP para voz, video y conferencias web.
- Sistemas de Mensajería proporciona la funcionalidad para enviar y gestionar mensajes de voz y vídeo a los usuarios.
- Software Social para la Empresa, incluye aplicaciones que permiten la comunicación con la empresa que no se limita estrictamente a las actividades orientadas a los negocios.

2.2.2 Arquitectura de Comunicaciones Unificadas

La arquitectura de Comunicaciones Unificadas, como se ilustra en la figura 2.4, se

compone de las siguientes capas lógicas:

- Infraestructura: La infraestructura consta de componentes de red. Proporciona y mantiene un alto nivel de disponibilidad, calidad de servicio (*QoS*) y seguridad para la red.
- Servicios: Servicios son responsables de proporcionar la funcionalidad principal de las Comunicaciones Unificadas, tales como la señalización y enrutamiento de llamadas.
- Aplicaciones: Las aplicaciones incluyen una amplia gama de software que ofrece una colección de funciones a los usuarios.
- *Endpoints* o Puntos finales: Los puntos finales incluyen productos de hardware del usuario final y de software que constituyen puntos de fijación para el sistema de Comunicaciones Unificadas.

Figura 2.4 Arquitectura de Comunicaciones

(Fuente Ref. Elaboración propia)

2.2.3 Operación de los *Gateways*

Gateways de comunicaciones unificadas son puntos de conexión entre diferentes redes de comunicaciones. Dependiendo del tipo de implementación, un *Gateway* puede realizar una o varias de estas acciones:

- Actuar como un conmutador de voz que interconecta múltiples circuitos tradicionales de telefonía. Los circuitos pueden ser analógica o digital. El *Gateway* participa en la señalización y podría tener que convertir los canales de medios. Los *Gateways* proporcionan acceso físico para dispositivos analógicos y digitales de voz local, tales como teléfonos, máquinas de fax y PBX.

- Actuar como un *Gateway* PSTN a VoIP que proporciona la traducción entre redes VoIP y no VoIP, tales como la PSTN. Además de la funcionalidad de los conmutadores de voz tradicionales, las *Gateways* PSTN a IP permiten comunicaciones de voz y vídeo entre la infraestructura PSTN tradicional y las redes IP convergentes.
- Actuar como un elemento que interconecta dos redes IP y permite la comunicación entre los puntos finales distribuidos entre ellos. Cuenta con funcionalidades como el filtrado, la traducción de direcciones, y las funciones relacionadas con la seguridad.

Los *Gateways* utilizan varios protocolos de control y señalización de llamada. Estos protocolos son:

- **H.323**: H.323 es un estándar que especifica los componentes, protocolos y procedimientos que proporcionan servicios de comunicación multimedia y audio en tiempo real, video y comunicaciones de datos sobre redes de paquetes, incluyendo las redes IP. H.323 es parte de una familia de recomendaciones del sector de Unión Internacional de Telecomunicaciones Normalización de las Telecomunicaciones (UIT-T) llamada H.32x que proporciona servicios de comunicación multimedia a través de una variedad de redes. H.32x es un paraguas de normas que define todos los aspectos de voz sincronizada, vídeo y transmisión de datos. También define la señalización de llamada de extremo a extremo.
- ***Media Gateway Control Protocol* (MGCP):** MGCP es un método para el control de *Gateway* PSTN. Especificado en el RFC 2705, MGCP define un protocolo que controla *Gateways* de VoIP que están conectados a dispositivos de control de llamadas externas, conocidas como agentes de llamadas (*call-agents*). MGCP proporciona la capacidad de señalización para los dispositivos frontera, tales como *Gateways*, que podrían no haber implementado completamente un protocolo de señalización de voz, como H.323. Por ejemplo, en cualquier momento de un evento, tal como un descolgado que se produce en un puerto de voz de un *Gateway*, el puerto de voz informa que evento al agente de llamada. El agente de llamada y luego señala el puerto de voz para proporcionar un servicio, tales como la señalización de marcación por tonos.
- ***Session Initiation Protocol* (SIP):** SIP es un protocolo detallado que especifica los comandos y respuestas para configurar y acabar las llamadas. SIP también detalla las características tales como la seguridad, *Proxy* y Protocolo de Control de Transmisión (TCP) o servicios *User Datagram Protocol* (UDP). SIP y sus protocolos asociados, Session Announcement Protocol (Protocolo de Anuncio de Sesión - SAP) y *Session*

Description Protocol (SDP), proporcionan avisos e información acerca de las sesiones de multidifusión a los usuarios de una red. SIP define señalización de llamada *end-to-end* (punto a punto) entre dispositivos. SIP es un protocolo basado en texto que toma prestados muchos elementos de HTTP, usando la misma solicitud de transacción y el modelo de respuesta y códigos de cabecera y de respuesta similares. También adopta una forma modificada del esquema de URL de direccionamiento utilizada dentro de correo electrónico que se basa en *Simple Mail Transfer Protocol* (SMTP).

La siguiente sección describe cada protocolo de forma detallada:

a) La Suite de protocolos H.323

H.323 es un conjunto de protocolos definidos por la UIT para las conferencias multimedia sobre redes de área local. El protocolo H.323 fue diseñado por el UIT-T y fue aprobado inicialmente en febrero de 1996. Fue desarrollado como un protocolo que proporciona redes IP con la funcionalidad de la telefonía tradicional. Hoy en día, H.323 es el estándar de voz videoconferencia basada en estándares de mayor despliegue de las redes de conmutación de paquetes.

Los protocolos especificados por H.323 incluyen los siguientes:

- **H.225 *Call Signaling* (Señalización de llamada)**: Señalización de la llamada H.225 se utiliza para establecer una conexión entre dos puntos extremos H.323. Esto se consigue mediante el intercambio de mensajes de protocolo H.225 en el canal de señalización de llamada. Se abre el canal de llamada de señalización entre dos puntos finales H.323 o entre un punto final y un *Gatekeeper* H.323.
- **H.225 *Registration, Admission, and Status* (Registro, Admisión y Estado)**: Registro, admisión y estado (RAS) es el protocolo entre puntos finales (terminales y *Gateways*) y *Gatekeeper*. RAS se utiliza para realizar el registro, control de admisión, los cambios de ancho de banda, el estado y terminar los procedimientos entre los puntos finales y *Gatekeeper*. Un canal de RAS se utiliza para intercambiar mensajes RAS. Se abre este canal de señalización entre un *endpoint* y un *Gatekeeper* antes del establecimiento de cualquier otro canal.
- **H.245 *Control Singnaling* (Señalización de Control):** H.245 señalización de control se utiliza para intercambiar mensajes de extremo a extremo de control que regulan el funcionamiento de un *endpoint* H.323. Estos mensajes de control llevan la información relacionada con lo siguiente datos:
  - Intercambio de capacidades

- Apertura y cierre de canales lógicos utilizados para transportar flujos de medios
- Mensajes de control de flujo
- Comandos generales e indicaciones

- **Códecs de audio:** Un códec de audio codifica la señal de audio desde un micrófono para la transmisión por el terminal H.323 de transmisión y decodifica el código de audio recibido que se envía al altavoz en el terminal H.323 receptor. Debido a que el audio es el servicio mínimo previsto por la norma H.323, todos los terminales H.323 deben tener al menos un códec de audio compatible, como se especifica en la recomendación ITU-T G.711 (codificación de audio a 64 kbps). Adicionales recomendaciones de códec de audio, tales como G.722 (64, 56, y 48 kbps), G.723.1 (5,3 y 6,3 kbps), G.728 (16 kbps), y G.729 (8 kbps), también puede estar soportado.
- **Códecs de vídeo:** Un códec de vídeo codifica vídeo de una cámara para la transmisión por el terminal H.323 de transmisión y decodifica el código de vídeo recibido en una pantalla de vídeo del terminal H.323 receptor. Debido a que H.323 especifica soporte de vídeo como opcional, el soporte de los códecs de vídeo es opcional también. Sin embargo, todas las comunicaciones de vídeo que ofrecen terminales H.323 deben soportar la codificación y decodificación de vídeo como se especifica en la recomendación ITU-T H.261.

En entornos de Comunicaciones IP del fabricante *Cisco Systems*, H.323 es ampliamente utilizado con *Gateways*, *Gatekeeper*s, y los clientes H.323 de terceros, tales como terminales de vídeo. Las conexiones pueden ser configuradas entre los dispositivos que utilizan direcciones IP de destino estática.

b) MGCP

MGCP es un protocolo de control de llamadas de cliente / servidor basada en una arquitectura de control centralizado. MGCP ofrece la ventaja de la administración centralizada del *Gateway* y la proporciona para soluciones de telefonía IP en gran medida escalables. Toda la información del plan de marcado reside en un agente de llamada (*Call-Agent*) por separado. El *Call Agent* que controla los puertos en el *Gateway*, realiza el control de llamada. Un *Gateway* MGCP hace la traducción entre las redes PSTN y VoIP para llamadas externas. En una red basada en equipos *Cisco Systems*, el *Cisco Unified Communication Managers* funciona como *Call Agent*.

MGCP es un protocolo de texto sin formato que utilizan los dispositivos de control de llamadas para gestionar *Gateways* de telefonía IP. MGCP se define en el RFC 2705, que

fue actualizado por el RFC 3660, y reemplazado por el RFC 3435, que fue actualizado por el RFC 3661.

Con MGCP, *Cisco Unified Communication Manager* (*Cisco UCM*) conoce y controla los puertos de voz individuales en un *Gateway MGCP*. Este enfoque permite el control completo de un plan de marcado de *Cisco UCM* y da control por puerto de conexiones a la red PSTN, PBX, los sistemas de correo de voz, y planes de servicios telefónicos antiguos. MGCP es implementado con el uso de una serie de comandos de texto sin formato enviados a través de *User Datagram Protocol (UDP)* puerto 2427 entre el *Cisco UCM* y un *Gateway*.

Un *Gateway* MGCP es relativamente fácil de configurar. Debido a que el *Call-Agent* tiene todo la inteligencia del enrutamiento de llamadas, no es necesario configurar el *Gateway* con todos los pares de marcado que de otra forma necesite.

Una desventaja es que un *Call-Agent* debe estar siempre disponible. *Gateways* Cisco MGCP pueden utilizar de Survivable *Remote Site Telephony* (SRST) y MGCP se reserva para permitir el protocolo H.323 para hacerse cargo y proporcionar enrutamiento de llamada local en ausencia de un *Cisco UCM* (por ejemplo, durante un corte de WAN).

c) Session Initiation Protocol (SIP)

SIP es un protocolo desarrollado por el *Internet Engineering Task Force (IETF) Multiparty Multimedia Session Control (MMUSIC)* como alternativa a H.323. Las características SIP cumplen con IETF RFC 2543, publicado en marzo de 1999; RFC 3261, publicado en junio de 2002; y RFC 3665, publicado en diciembre de 2003. Debido a que SIP es un estándar común basada en la lógica de la *World Wide Web* y es muy fácil de implementar, es ampliamente utilizado con puertas de enlace y servidores *Proxy* dentro de las redes de proveedores de servicios para la señalización interna y cliente final.

SIP es un protocolo *peer-to-peer*, donde los agentes de usuario *(User Agent* - UA) inician sesiones, similar a H.323. Sin embargo, a diferencia de H.323, SIP utiliza mensajes de texto basados en ASCII para comunicarse. Por lo tanto, puede implementar y solucionar problemas de SIP con mucha facilidad.

Debido a que SIP es un protocolo *peer-to-peer*, el Cisco UCM no controla los dispositivos SIP y *Gateways* SIP no se registra con Cisco UCM. Al igual que con *Gateways* H.323, sólo la dirección IP está disponible en Cisco UCM para que la comunicación entre un UCM Cisco y un *Gateway* de voz SIP sea posible.

2.3 Fundamentos de VoIP

Voz sobre IP (*VoIP-Voice over Internet Protocol*) define una forma de llevar a las llamadas de voz sobre una red IP, incluyendo la digitalización y paquetización de los flujos de voz. Telefonía IP utiliza los estándares de VoIP para crear un sistema de telefonía donde las características de alto nivel tales como enrutamiento avanzado de llamadas, correo de voz, centros de contacto, etc., pueden ser utilizados.

VoIP está diseñado para reemplazar las tecnologías y redes TDM por una red de datos basada en IP. La voz digitalizada es llevada en paquetes de datos IP en una red LAN y/o WAN.

La red telefónica ha proporcionado comunicaciones de voz de alta calidad y fiable durante muchos años. Ofrece voz sobre un canal de 64 Kbps estandarizado. El ancho de banda de 64 Kbps está garantizado para cada llamada y el trayecto de conversación se lleva como un flujo digital continúa. La voz digital no se realiza en paquetes. Empresas y usuarios domésticos utilizan DTMF *(Dual-ToneMulti-Frequency)*, el canal TI y señalización por canal D de la RDSI para configurar y gestionar la llamada. Dentro de RDSI, la señalización es llevada en paquetes en un separado canal de señalización sobre conexiones *Basic Rate Interface (BRI)* y *Primary Rate Interface (PRI)* con el portador. El portador luego traduce la señalización (de todo tipo) en un protocolo de señalización interno denominado Sistema de Señalización No. 7. Los protocolos de señalización están activas principalmente al principio y al final de una llamada.

En una red de VoIP, existe un protocolo de señalización y un protocolo de transmisión de voz. Ambos protocolos requieren que toda la información se transporte en paquetes IP. Varios estándares están disponibles para los protocolos de señalización, incluyendo H.323, SIP, MGCP y H.248 (MEGACO). La mayoría de marcas de Sistemas de Telefonía IP han desarrollado su protocolo de señalización propietario, el más común es el de *Cisco Systems*: SCCP (*Skinny Client Control Protocol*). RTP (*Real-time Transport Protocol*) es el protocolo de transmisión de voz estándar utilizado con redes VoIP. La voz es digitalizada, colocada en paquetes, y transmitida a través de la red IP. Se requieren múltiples paquetes para llevar una sola palabra hablada. La voz se digitaliza usando uno de los estándares G.7xx. Cada una de estas normas será discutida de forma detallada más adelante.

Los beneficios de una red de VoIP frente a las redes TDM son:

- Reducción de cargos por llamadas larga distancia, específicamente largas distancias

internacionales.

- La reducción de personal de TI mediante la combinación de la red de voz y la gestión de la red de datos y eliminación de funciones redundantes.
- Adición de amplias aplicaciones que no son ofrecidos por los sistemas basados en TDM.
- Tener una red común para diferentes formas de comunicación.
- Los proveedores TDM no están ofreciendo nuevos sistemas, lo que obliga a los clientes a adoptar finalmente los sistemas de telefonía basados en IP.

Las características propias de una red de voz y datos IP convergente presentan ciertos desafíos a los ingenieros de redes y administradores en la entrega de tráfico de voz correctamente. Esta sección describe los desafíos de la integración de una red de voz y datos y explica las tecnologías que permiten la transmisión de los medios de comunicación de voz.

2.3.1 Descripción General de VoIP

VoIP transporta información de voz sobre redes IP, que utilizan el reenvío de paquetes conmutados. Este principio difiere de la tecnología de conmutación de circuitos de teléfono tradicional redes, donde un canal se crea entre los extremos comunicantes a través de la infraestructura de telecomunicaciones. La tabla 1.1 contrasta la telefonía tradicional con VoIP.

Tabla 2.1 Comparación de Telefonía Tradicional y VoIP

(Fuente Ref.: Elaboración Propia)

	Telefonía tradicional	**VoIP**
Tecnología de transmisión	Conmutación de circuitos	Conmutación de Paquetes
Funciones básicas de señalización.	Supervisión, dirección, informativo.	Supervisión, dirección, informativo
Métodos y protocolos de señalización	Digital: SS7, ISDN, QSIG Analog: loop-start, groundstart, immediate-start, winkstart, delay-start, DTMF, pulse	H.323, SIP, MGCP, SCCP

Métodos de transmisión		Circuito dinámico.	Flujos UDP.

Antes de que se establezca una llamada, los métodos de señalización se utilizan para detectar un estado descolgado, recoger un número llamado, e informar a la red acerca de la llamada. Los protocolos de señalización cumplen funciones similares, y deben cumplir con los requisitos adicionales impuestos por el ejemplo de método para la transmisión basada en IP, la negociación de parámetros de transmisión de VoIP como códecs.

La media es transportada sobre redes IP en paquetes *Real-Time Transport Protocol* RTP que se encapsulan en User Datagram Protocol (UDP) fluye. Un flujo RTP es unidireccional. Por lo tanto, una llamada de voz típicamente incluye dos flujos RTP unidireccionales.

2.3.2 Las principales etapas de Procesamiento de Voz de VoIP

Para la transmisión sobre una red IP, la longitud de onda de voz debe ser muestreada, cuantificado, codificado, opcionalmente comprimida, y luego encapsulado en un paquete de VoIP, como se ilustra en la figura 2.5.

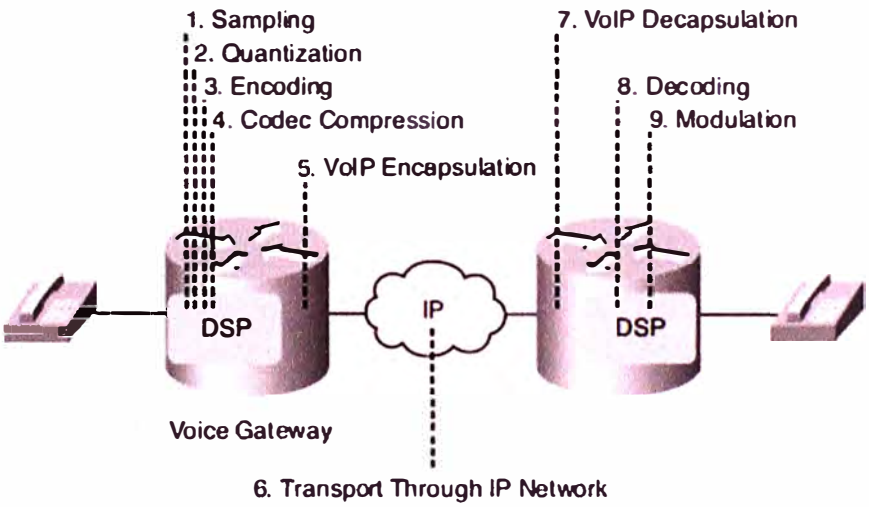


Figura 2.5 Etapas de procesamiento de llamada VoIP

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 167)

Los primeros cuatro pasos se realizan por un procesador de señales digitales (DSP) en el *Gateway* de origen y se detallan en el siguiente apartado. Los paquetes de VoIP luego son entregados al *Gateway* de destino, y la información de voz se recupera a partir del paquete. Finalmente, un DSP en el *Gateway* de terminación decodifica la carga útil y

modula la longitud de onda para invertir el proceso realizado en el *Gateway* de origen.

2.3.3 Componentes de VoIP

La figura 2.6 representa los componentes básicos de una red de paquetes de voz, con componentes de la marca *Cisco Systems.* Se presenta tal marca ya que, como se verá más delante de manera justificada, el diseño del sistema de videoconferencia será de mencionada marca.

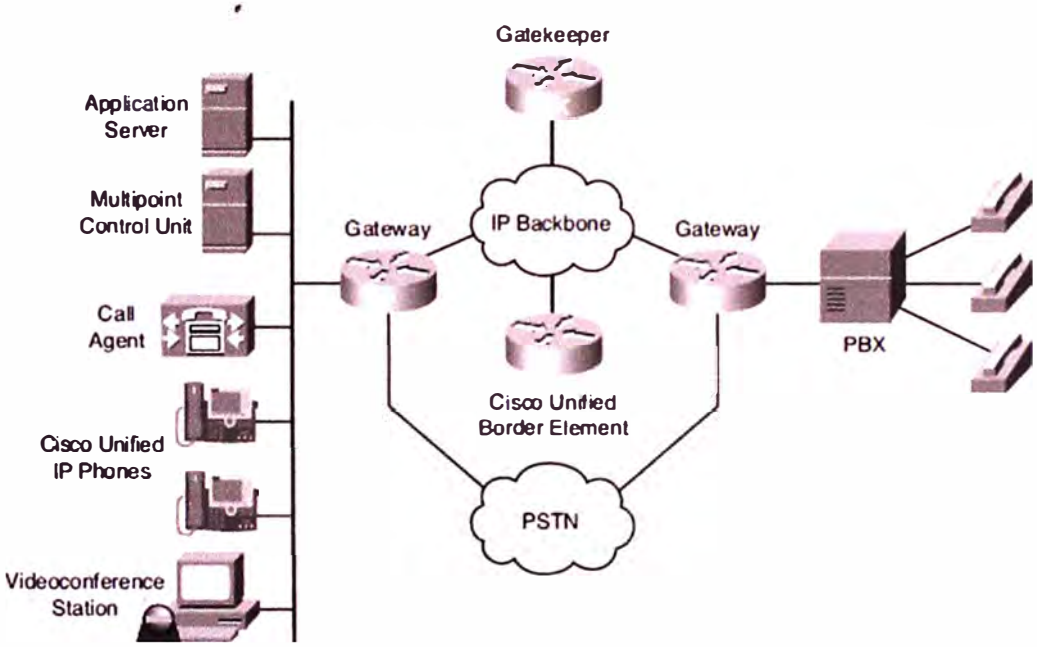


Figura 2.6 Componentes de una red de VoIP

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 167)

Los componentes de la figura 2.6 son:

- IP Phones (Teléfonos IP): Los teléfonos proporciona un punto final IP para la comunicación de voz.
- *Gatekeeper*: Provee la funcionalidad de control de llamada *(Call Admision Control - CAC)*, control y gestión de ancho de banda, y traducción de direcciones.
- *Gateway*: Provee traducción entre redes VoIP y redes no-VoIP tales como la PSTN. Los *Gateways* también provee acceso físico para dispositivos para voz analógicos y digitales tales como teléfonos, faxes y PBXs.
- *Cisco Unified Border Element (Cisco UBE)*: Interconecta dos redes VoIP. Este elemento actúa como un *Proxy* entre protocolos de señalización y puede ser configurado para proveer servicios *Proxy*.
- *Multipoint control unit (MCU)*: Unidad de control multipunto, provee conectividad en tiempo real a los participantes en diferentes ubicaciones para asistir la misma

videoconferencia o reunión.

- *Call Agent:* Provee control de llamada para los teléfonos IP, también se encarga de controlar la admisión de la llamada (Call Admision Control), control y gestión de Ancho de Banda, y traducción de direcciones.
- *Application Servers*: Servidores de aplicaciones, proveen servicios tales como email de voz, mensajería unificada, respuesta interactiva de voz (*Interactive Voice Response – IVR*), aplicaciones de estados presencia y mensajería instantánea para empresas, conferencias multimedia, y otros.
- *Videoconference station:* Estación de Videoconferencia, provee acceso a usuarios finales a participar en videoconferencias. La estación de videoconferencia contiene un dispositivo de recepción de video para entrada de video y un micrófono para entrada de audio. El usuario puede ver flujos de video y escuchar el audio que origina la estación del usuario remoto.

La Tabla 2.2 describe los pasos para convertir la información de voz a VoIP.

Tabla 2.2 Convirtiendo Voz VoIP

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 168)

Telefonía tradicional	**Descripción**
Muestra de señal análoga.	La frecuencia de muestreo debe ser al menos el doble de la frecuencia más alta para producir la señal que no aparezca entrecortada. La tasa de muestreo usada en telefonía es 8000 muestras por segundo (8KHz), lo que refleja el hecho de que la mayor parte de la energía voz humana se realiza en el espectro de 0-4 KHz.
Cuantización de la muestra	Cuantificación consiste en una escala compuesta por 8 segmentos principales. Cada segmento se subdivide en 16 intervalos. Los segmentos no están igualmente espaciados pero en realidad son más finos cerca del origen. Los intervalos son iguales dentro de los segmentos pero diferente cuando se comparan entre los segmentos. Graduaciones más finas en el resultado origen en menos distorsión para muestras de menor volumen.

Codificar el valor en forma digital de 8 bit	La codificación asigna un valor derivado de la cuantización a un número de 8 bits (octetos).
(Opcional) Compresión de las muestras para reducir **el** ancho de banda.	Compresión de la señal, es usada para reducir el ancho de banda dado por cada llamada.

Los tres primeros pasos describen el proceso de modulación por impulsos codificados (PCM), que corresponde al códec G.711. Paso 4 explica la compresión que se realiza por los códecs de bajo ancho de banda, tales como G.729, G.728, G.726, *o Internet Bitrate Códec Bajo (iLBC).*

a) Muestreo de la Señal

El muestreo de la señal, como se ilustra en la figura 2.7, es un proceso que toma lecturas de la amplitud de forma de onda a intervalos regulares, por un proceso llamado de modulación por amplitud de pulso (PAM).

La salida es una serie de pulsos que se aproxima a la forma de onda analógica. Para esta salida tenga un nivel aceptable de calidad para la señal a ser reconstruida, la tasa de muestreo debe ser lo suficientemente rápida.

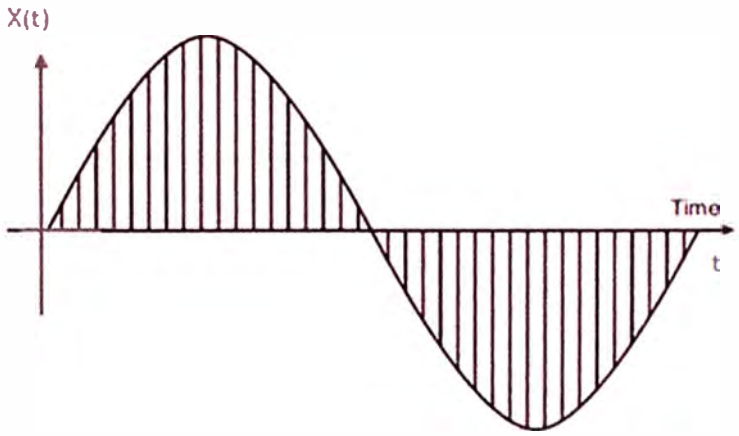


Figura 2.7 Muestreo de la señal

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 169)

Harry Nyquist desarrolló una prueba matemática sobre la velocidad a la que una forma de onda puede ser muestreada y la información que se puede recuperar a partir de esas muestras. El teorema de Nyquist establece que cuando una señal se muestrea de forma instantánea en el transmisor en intervalos regulares y tiene una tasa de al menos dos veces la frecuencia de canal más alto, las muestras contendrán información suficiente para

permitir una reconstrucción exacta de la señal en el receptor.

Aunque el oído humano puede percibir sonidos de 20 a 20.000 Hz, el habla abarca sonidos de alrededor de 200 a 9000 Hz. El canal telefónico fue diseñado para operar a frecuencias de 300 a 4000 Hz. Este económico rango ofrece suficiente fidelidad para comunicaciones de voz, aunque no se transmiten las muestras de mayor frecuencia.

b) Cuantización

Cuantización divide la gama de valores de amplitud que están presentes en una muestra de la señal analógica en una serie de pasos discretos que están más cerca en valor a la señal analógica original. Cada paso se le asigna una palabra de código digital único. La cuantización coincide con una señal PAM a una escala segmentada. La escala mide la amplitud (altura) de la señal PAM y asigna un número entero para definir esa amplitud.

En la figura 2.8 se muestra la cuantización en acción. En el ejemplo, el eje x representa el tiempo, y el eje y representa el valor de la tensión. La salida es una serie de pulsos que se aproxima a la forma de onda analógica.

El rango de tensión se divide en 16 segmentos (0 a 7 positivo y negativo de 0 a 7). Comenzando con el segmento 0, cada segmento tiene intervalos menos granulares que el segmento anterior, lo que reduce la relación señal a ruido (*Signal Noise Relation - SNR*) y hace el segmento uniforme. Esta segmentación también corresponde estrechamente con el comportamiento logarítmico del oído humano.

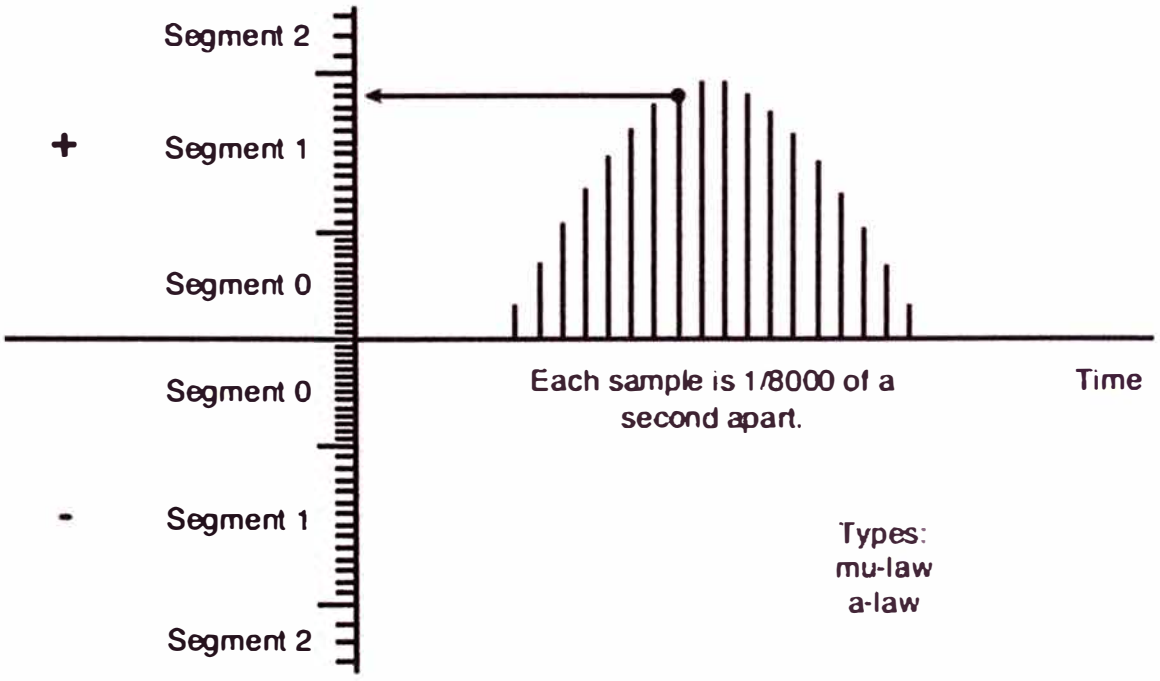


Figura 2.8 Cuantización de la señal

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 170)

Los dos principales esquemas de generación de estas muestras en la comunicación electrónica son *a-law* y *mu-law*. Son esquemas de compresión de audio, que se define por la UIT-T G.711, que comprimen 16 bits de datos PCM lineal hasta 8 bits de datos logarítmico. El estándar *a-law* se utiliza principalmente en Europa y el resto del mundo, mientras que *mu-law* se utiliza en Norteamérica y Japón.

Las semejanzas entre mu-law y a-law incluyen lo siguiente:

- Ambos son aproximaciones lineales de la relación de entrada / salida logarítmica.
- Palabras de código de ocho bits permiten una velocidad de bits de 64 kbps. Esto se calcula multiplicando la velocidad de muestreo (dos veces la frecuencia de entrada) por el tamaño de la palabra de código (2 * 4 kHz * 8 bits = 64 kbps).
- Ambos rompen un rango dinámico en un total de 16 segmentos:
  - Ocho positivo y ocho segmentos negativos.
  - Cada segmento es el doble de la longitud de la precedente.
  - Cuantización uniformes usado dentro de cada segmento.
- Ambos utilizan un enfoque similar para la codificación de la palabra de 8 bits:
  - Primer bit (MSB) identifica polaridad.
  - Bits dos, tres, y cuatro identifican segmento.
  - Finales cuatro bits cuantifican el segmento.
- Las diferencias entre mu-law y a-law incluyen lo siguiente:
  - Diferentes aproximaciones lineales conducen a diferentes longitudes y pendientes.
  - La asignación numérica de las posiciones de bit en la palabra de código de 8 bits a los segmentos y los niveles de cuantificación dentro de los segmentos son diferentes.
  - a-law proporciona un mayor rango dinámico que mu-law.
  - mu-law proporciona un mejor rendimiento de distorsión de señales de bajo volumen que a-law.
  - A-law requiere 13 bits, mientras que mu-law requiere 14 bits.
  - Una conexión internacional debe utilizar una a-law, y conversión de mu-law a a-law es la responsabilidad del país con mu-law.

c) Codificación

Codificación convierte un número en base 10 entero a un número binario. La salida de la codificación es una expresión binaria en la que cada bit es o bien un (pulso) 1 o un 0 (sin pulso). Después de muestras PAM una señal de voz analógica de entrada, el siguiente

paso es para codificar estas muestras en la preparación para la transmisión sobre una red de telefonía. Este proceso se denomina modulación por impulsos codificados (PCM).

El proceso de PCM, como se muestra en la figura 2.9, convierte matemáticamente el valor obtenido de muestreo PAM a otro valor binario dentro del rango -127 a 127. Es en esta etapa de-expansión, el proceso de la primera comprimir una señal analógica en la fuente y luego ampliar esta señal de nuevo a su tamaño original cuando llega a su destino, se aplica. Todo este proceso se conoce generalmente como la codificación PCM. Un DSP, que es un chip especializado, realiza rápidamente el proceso de PCM.

En el Perú se usa a-law. Ambos mu-law y a-law producen PCM valores en los rangos -127 a +127. Ambos mu-law y a-law representan un valor de signo positivo con un valor 1, y un valor de signo negativo con un valor de 0. Esta representación es una desviación del uso computacional "normal" en positivo es generalmente representado por 0.

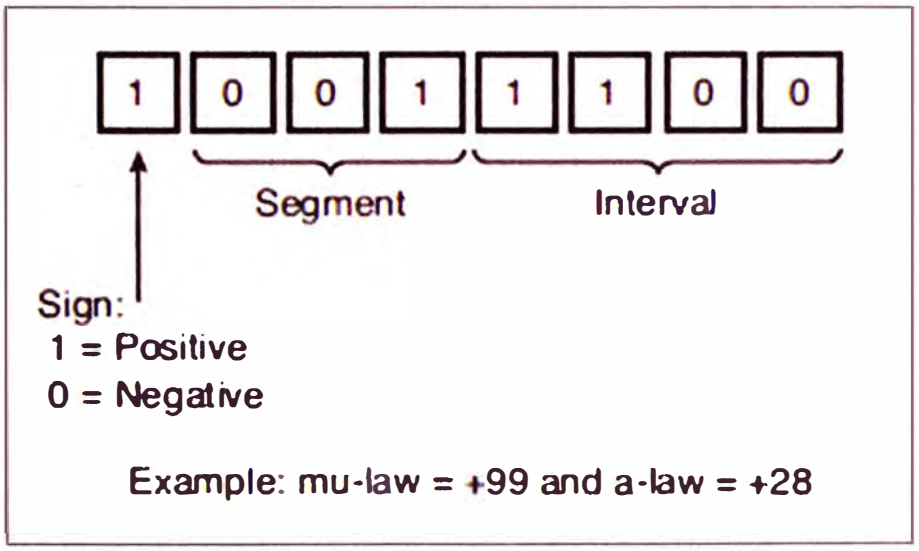


Figura 2.9 Codificación

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 172)

De los dos métodos, a-law aparece para ser el método más lógico, porque un valor PCM de +127 es representado como 11111111; en otras palabras, un valor de signo positivo (el primer bit) seguido por un valor binario de 127 compuesto de los segmentos e intervalos de bits. Similarmente, -32 es representado como 00100000. Mu-law funciona un poco diferente por lógicamente invirtiendo el segmento y los bits de intervalo. Usando mu-law, el valor de +127 se transforma a 10000000; en otras palabras, un valor de signo positivo (el primer bit) seguido por el bit inverso de +127.

Las señal digital de voz sin comprimir es muestreada a una velocidad de 8.000

muestras por segundo, siendo cada muestra que consta de 8 bits. Esto corresponde a 64 kbps por cada llamada.

Múltiples algoritmos se han desarrollado para permitir la transmisión de voz con un consumo menor o inferior del ancho de banda. Estos algoritmos están representados y reconocidos como Códec. Los códecs más comunes están señalados en la Tabla 2.3, junto con el consumo ancho de banda que realizan. Uno de los códecs más usados por los usuarios de telefonía IP, es el códec G.729 esto debido a su capacidad de compresión de cada llamada, llegando a ser hasta 8 Kbps.

Tabla 2.3 Compresión del Códec

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 172)

Códec	**Ancho de Banda (Kbps)**
G.711	64
G.726r32	32
G.726r24	24
G.726r16	16
G.728	16
iLBC (Internet Low Bitrate Códec)	15.2, 13.3
GSM Full Rate (GSM-FR)	13
G.729 (A/B/AB)	8
G.723r63	6.3
G.723r53	5.3

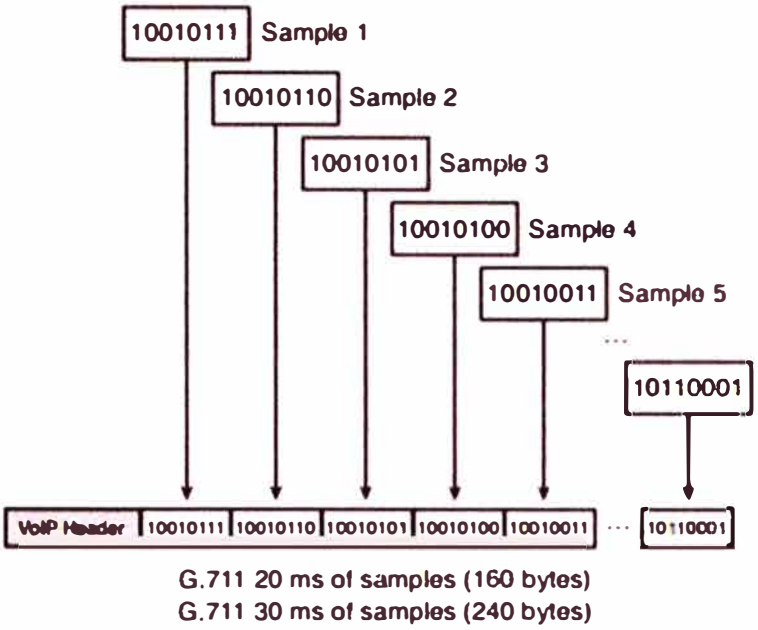


Figura 2.10 PCM (G.711)

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 174)

2.3.4 Paquetización VoIP

Después de que la longitud de onda de la voz es digitalizada, esta pasa a un procesador digital de señales (DSP), el cual recoge los datos digitalizados para una cantidad de tiempo hasta que haya datos suficientes para llenar la capacidad de carga de un solo paquete.

El ejemplo en la figura 2-10 muestra cómo muestras de PCM se empaquetan en la carga útil de un solo paquete usando el códec G.711. Con G.711, ya sea 20 ms o 30 ms valor de la longitud de onda de voz se transmite en un solo paquete.

El valor de la longitud de onda de voz correspondiente a 160 muestras es de 20ms (en 8000 muestras por segundo, 10 ms se corresponden con 80 muestras, y 20 ms serían 160 muestras). Con 20 ms de valor de la longitud de onda de voz, 50 paquetes de VoIP se transmiten en cada dirección en 1 segundo (1 segundo consiste en 50 intervalos de 20 ms: 1 seg / 20 ms = 50).

De manera simimilar, 30 ms de valor de la longitud de onda de voz corresponde a 240 muestras (en 8000 muestras por segundo, 10 ms serían iguales a 80 muestras, y 30 ms serían 240 muestras). Con 30 ms por valor de la voz, a unos 33 paquetes de VoIP se transmiten en cada dirección en 1 segundo (1 segundo consiste en 33. [3] intervalos de 30-ms: 1 seg / 30 ms = 33. [3]).

a) Tasa de Paquetización

La longitud de la información de voz transportada en un solo paquete afecta el tamaño de carga útil, que se conoce en la Tabla 2.4 como el tamaño de las muestras G.711 para un único paquete.

Tabla 2.4 Tasa de Paquetización

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 174)

Códec	**20 ms de Voz en un Paquete**	**30 ms de Voz en un Paquete**	**40 ms de Voz en un Paquete**	**60 ms de Voz en un Paquete**	**80 ms de Voz en un Paquete**
Tasa de Paquetización	50pps	33.3 pps	25 pps	16.7 pps	12.5 pps
Tamaño de muestras G.711 reunidas por paquete	160 bytes	240 bytes	320 bytes	480 bytes	640 bytes
Ancho de banda de voz cruda sin comprimir.	64 kbps	64 kbps	64 kbps	64 kbps	64 kbps
Ancho de banda de VoIP más capa 3 en adelante, sin comprimir.	80 kbps	74.7 kbps	72 kbps	69.3 kbps	68 kbps

Antes de que las cargas útiles se transmitan a través de la red IP, deben ser encapsulados en un paquete que introduce una sobrecarga adicional causada por las capa 3 y superiores de modelo OSI *(Open Systems Interconnection)*. Estas cabeceras consumen ancho de banda adicional, además de los 64 kbps requeridos para la transmisión de voz en bruto. La sobrecarga de ancho de banda depende de la tasa de paquetes, como se muestra en la Tabla 2.4.

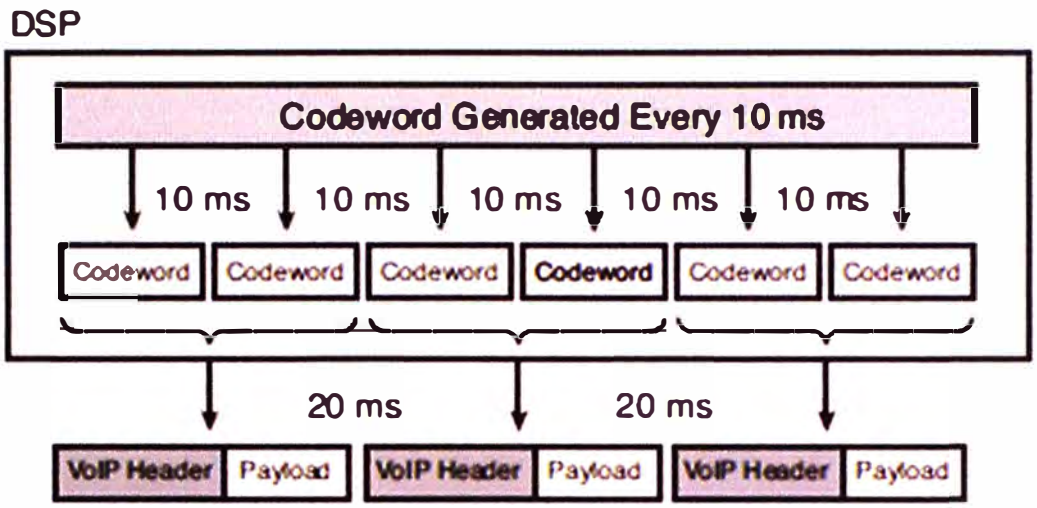


Figura 2.11 Operación de códec G.729

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 175)

b) Operaciones de Códec

En la figura 2.11 ilustra el funcionamiento de un algoritmo códec opcional. G.729 se presenta en este ejemplo. El DSP muestrea, cuantifica, y codifica la forma de onda analógica en la entrada.

El DSP genera una palabra de código por cada 10 ms por valor de voz. Las palabras de código están encapsuladas en la carga útil de los paquetes de VoIP. Un solo paquete VoIP lleva por defecto 20 ms valor de audio, encapsulando dos palabras de código G.729 en una carga útil. Otro tipo de paquetización soportado es 30 ms, en el que los paquetes de VoIP se generan cada 30 ms y llevan tres palabras de código G.729 en cada paquete.

c) Ejemplo de Paquetización y Compresión

La tabla 2.5 ilustra los modos de funcionamiento comunes del códec G.729: a una tasa de 50 pps con 20 ms de valor de la longitud de onda de voz en un solo paquete, y la tasa de 33.3 pps con 30 ms de valor de la longitud de onda de voz en un solo paquete. Después de realizar la compresión, el tamaño de carga útil es 20 bytes y 30 bytes, respectivamente. En ambos modos (50 pps y 30 pps), el ancho de banda de voz en bruto comprimido es de 8 kbps, también se tiene que el ancho de banda adicional de la capa 3 y las restantes capas superiores dependen de la tasa de paquetización que se elija, esta suma de anchos de banda adicionales hace que el nuevo total sea 24 kbps y 18,7 kbps, respectivamente.

Tabla 2.5 Tasa de Paquetización

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 175)

Códec	**20 ms de Voz en un Paquete**	**30 ms de Voz en un Paquete**
Tasa de Paquetización	50pps	33.3 pps
Tamaño de muestras G.729 reunidas por paquete	20 bytes	30 bytes
Ancho de banda de voz cruda sin comprimir.	8 kbps	8 kbps
Ancho de banda de VoIP G.729 más capa 3 en adelante, sin comprimir.	24 kbps	18.7 kbps

El ancho de banda de llamada se puede calcular utilizando la siguiente fórmula:

Ancho de banda por llamada = (Voz de carga útil + Capa 3 *Overhead* + capa 2 arriba) *

Paquetes por segundo * 8 bits / bytes

Los ejemplos mostrados en la Tabla 2.5 no consideran la capa 2 de sobrecarga u *overhead*, que varía basado en la tecnología de paquetes en uso.

2.3.5 Transmisión de Media VoIP

En una red de VoIP, las conversaciones de voz reales se transportan a través de los medios de transmisión que utilizan RTP y RTCP, o sus derivados, SRTP y cRTP. RTP define un formato de paquetes estándar para enviar audio y vídeo a través de Internet. RTCP es un protocolo que acompaña a RTP, y prevé la entrega de información de control para los flujos individuales RTP. cRTP y SRTP fueron desarrollados para mejorar el uso

de RTP.

Protocolos de datagramas, como UDP, envían el flujo de contenido multimedia como una serie de pequeños paquetes. Esto es simple y eficiente; sin embargo, los paquetes pueden ser perdidos o dañados en tránsito. Dependiendo del protocolo y el alcance de la pérdida, el cliente podría ser capaz de recuperar los datos con técnicas de corrección de errores, podría interpolar sobre los datos que faltan. RTP y RTCP fueron diseñados específicamente para transmitir contenido multimedia a través de redes. Ambos se construyen en la parte superior de la capa UDP.

RTP se transmite entre dos puntos extremos VoIP, tales como puertas de enlace H.323, como se ilustra en la figura 2.12.

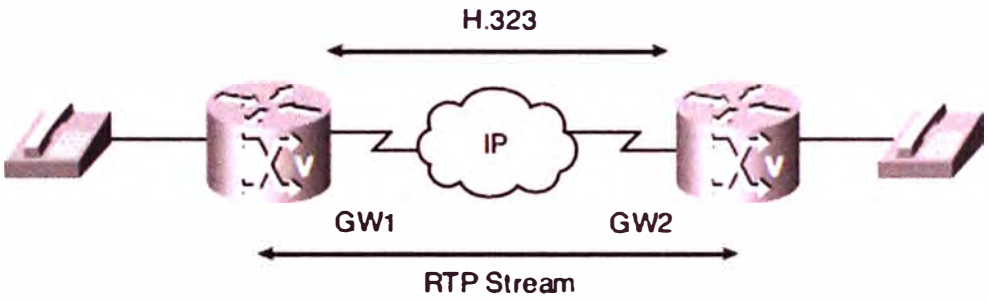


Figura 2.12 Stream RTP

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 176)

Los protocolos principales involucrados en la transmisión de los medios de comunicación de voz:

- *Real-time Transport Protocol (RTP):* Proporciona los flujos de audio y vídeo a través de redes reales.
- *Real-time Transport Control Protocol (RTCP):* Proporciona información fuera de la banda de control para un flujo RTP.
- *Compressed RTP (cRTP):* Comprime cabeceras IP / UDP / RTP sobre enlaces seriales de baja velocidad.
- *Secure RTP (SRTP):* Proporciona cifrado, autenticación y la integridad del mensaje y protección de repetición a RTP.

En la siguiente sección se describe con más detalle a cada protocolo.

a) Real-Time Transport Protocol

RTP, se describe en el RFC 3550, define un formato de paquete estandarizado para la entrega de audio y vídeo sobre una red IP.

RTP normalmente se ejecuta en la parte superior del protocolo UDP para que pueda utilizar los servicios de multiplexación y de suma de comprobación de ese protocolo. Aplicaciones RTP son típicamente sensibles a los retrasos; así, UDP es una opción mejor que el más complejo TCP. RTP no tiene un puerto de serie en el que se comunica. La única norma que obedece es que las comunicaciones UDP se realizan a través de un puerto, y el siguiente puerto impar superior se utiliza para las comunicaciones RTCP. Aunque no existen normas asignadas, RTP utiliza comúnmente puertos 16384 a 32767. El hecho de que RTP utiliza un intervalo de puertos dinámicos hace que sea difícil para él para atravesar *Firewalls*.

- *Payload type identification* (Identificación del tipo de carga útil), que identifica el tipo de carga útil transportada en el paquete, como códec o formato multimedia. Este identificador permite el cambio de códecs y formatos de datos mientras que el flujo está activo, como es el caso con fax y módem de paso a través.
- *Sequence numbering* (Secuencia de numeración), que controla la secuencia de los paquetes que llegan y se utiliza principalmente para detectar la pérdida de paquetes. RTP no solicita la retransmisión si se pierde un paquete.
- *Time stamping* (Tiempo de estampado), que es necesaria para colocar los paquetes que llegan en el orden de sincronización correcta. El buffer *dejitter* evalúa este parámetro cuando compensa el retardo del trayecto variable.

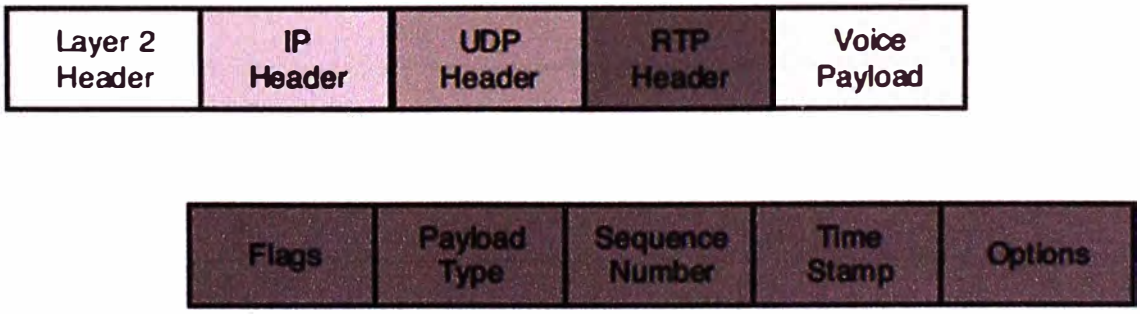


Figura 2.13 Cabecera RTP

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 177)

b) Real-Time Transport Control Protocol

El protocolo RTCP definido en RFC 3550, un protocolo hermano de RTP. RTCP proporciona información fuera de la banda de control para un flujo RTP.

Aunque se utiliza periódicamente para transmitir paquetes de control a los participantes en una sesión de transmisión multimedia, la función principal de RTCP es

proporcionar información sobre la calidad de servicio (QoS) está proporcionado por RTP.

RTCP reúne estadísticas sobre una conexión de los medios de comunicación, tales como bytes enviados, los paquetes enviados, los paquetes perdidos, jitter, retroalimentación y retardo de ida y vuelta. Las aplicaciones utilizan esta información para ajustar los parámetros de transmisión.

Una muestra de los diferente tipos de paquetes RTCP: *sender report packet* (paquete reporte emisor), receiver *report packet* (paquete reporte emisor), *source description* RTCP packet (paquete descripción fuente RTCP), *goodbye RTCP packet* (paquete de despedida RTCP), y *application-specific* RTCP *packet* (paquete de aplicación específica RTCP).

RTCP proporciona la siguiente información sobre las condiciones actuales de la red:

- RTCP provee un mecanismo para hosts involucrados en un sesión RTP para intercambiar información acerca del monitoreo y control de la sesión. RTCP monitorea. RTCP controla la calidad de los elementos como el recuento de paquetes, la pérdida de paquetes, retardo y *jitter* entre llegadas. RTCP transmite paquetes como un porcentaje del ancho de banda de sesión, pero a una tasa específica de por lo menos cada 5 segundos.
- El estándar RTP establece que la marca de tiempo *Network Time Protocol (NTP)* es basada en los relojes sincronizados. La correspondiente marca de tiempo RTP se genera y se basa en un muestreo paquete de datos al azar. Tanto la información NTP y la información RTP se incluyen en los paquetes RTCP por el remitente de los datos.

El protocolo RTCP proporciona un flujo separado de RTP para el transporte utilizado por UDP, como se muestra en la figura 2.14. Cuando a un flujo de voz se le asigna números de puerto UDP, el protocolo RTP se suele asignar a un puerto de número par y RTCP se le asigna el siguiente puerto impar. Cada llamada de voz tiene cuatro puertos asignados: RTP con RTCP en la dirección de transmisión y RTP con RTCP en la dirección de recepción.

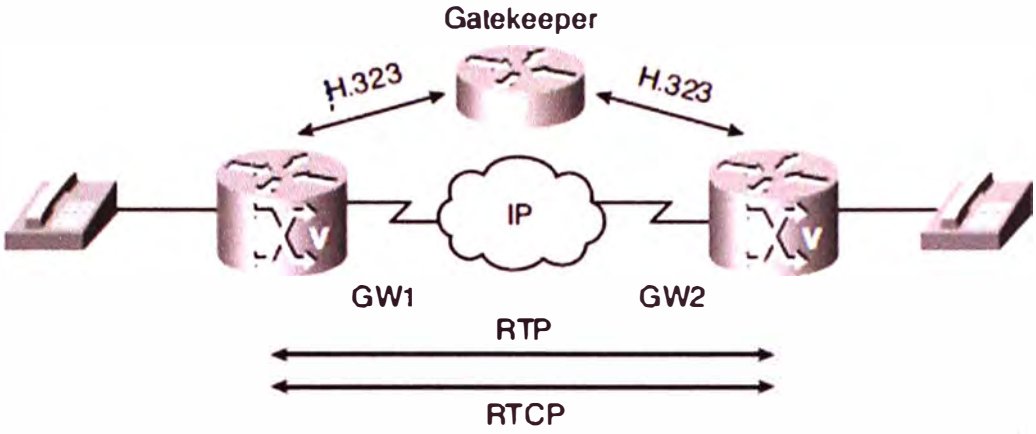


Figura 2.14 Flujo RTCP

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 179)

c) Compressed RTP

El *overead* (sobrecarga) introducida por cabeceras de los paquetes es a menudo considerablemente mayor que el *payload* (carga útil) de voz. El *overhead* se compone de IP (20 octetos), UDP (8 octetos), y la cabecera RTP (12 octetos) y equivale a 40 bytes.

El protocolo cRTP, se especifica en el RFC 2508, 2509 y 3545, fue desarrollado para reducir el tamaño de las cabeceras IP, UDP y RTP. cRTP mapea la cabecera IP / UDP / RTP a 2 bytes (sin *checksum*) o 4 bytes (con la suma de comprobación).

La compresión de la cabezera RTP es soportada en interfaces *point-to-point* (punto a punto), tales como líneas seriales usando *Frame Relay, High-Level Data Link Control* (HDLC), o encapsulación PPP. Es un mecanismo de enlace local que debe habilitarse en ambos lados del enlace.

El protocolo cRTP es recomendado para enlaces de baja velocidad menor que o igual a 768 kbps, como se subraya en la figura 2.15. En los enlaces más rápidos, el ahorro de ancho de banda puede ser compensado por un incremento en el uso de CPU en el *Router*.

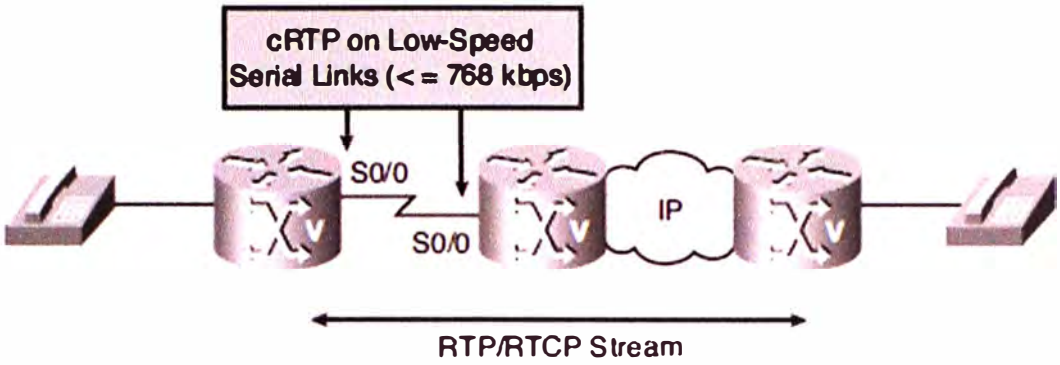


Figura 2.15 Flujo cRTP

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 179)

Durante la compresión de un flujo de RTP, un contexto de la sesión se define. Para cada contexto, se establece el estado de la sesión y se comparte entre el compresor y el descompresor.

El estado contexto consiste en las cabeceras completas IP / UDP / RTP, unos valores diferenciales de primer orden, un número de secuencia de enlace, un número de generación, así como una tabla de codificación delta. El estado contexto debe ser sincronizado entre el compresor y descompresor para la descompresión exitosa a tener lugar.

d) Secure RTP

SRTP definido en el RFC 3711, está diseñado para proporcionar encriptación, autenticación de mensajes y la integridad, y protección de repetición de los datos RTP en ambas aplicaciones unicast y multicast. La figura 2.16 muestra un flujo SRTP entre dos *Gateways* de voz.

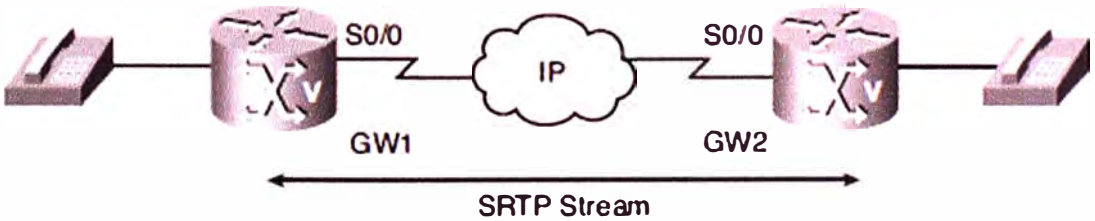


Figura 2.16 Flujo SRTP

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 179)

SRTP también tiene un protocolo hermana, llamada *Secure RTCP (SRTCP).* SRTCP ofrece las mismas características relacionadas con la seguridad de RTCP como los

proporcionados por SRTP a RTP. SRTP se puede utilizar en conjunto con comprimido RTP.

Características de seguridad de SRTP incluyen el cifrado, autenticación e integridad y protección de repetición, como se explica en las siguientes secciones.

- **Encriptación**

El cifrado es la conversión de datos en un formulario, llamado un texto cifrado, que no puede ser entendido por personas no autorizadas. Esta característica también se refiere como la privacidad. Se asegura que el contenido de la conversación se mantiene como privado entre los puntos finales. Si un atacante intercepta los paquetes, el atacante no será capaz de descifrar ellos. El descifrado es el proceso de convertir los datos cifrados de nuevo en su forma original, por lo que se puede entender. SRTP utiliza *Advanced Encryption Standard (AES)*.

- **Autenticación e Integridad**

Los algoritmos de cifrado no garantizan la integridad del mensaje a sí mismos, lo que permite al atacante falsificar datos. SRTP proporciona los medios para garantizar la integridad de los paquetes.

Hashed Message Authentication Code-Secure Hash Algorithm 1 (HMAC-SHA-1) autentica el mensaje y protege su integridad. La autenticación proporciona la seguridad de que el flujo de VoIP está llegando desde el punto final auténtico, y no alguien haciéndose pasar por el punto final. Este método produce un resultado de 160 bits, que luego se trunca a 80 bits para convertirse en la etiqueta de autenticación que más adelante se adjunta al paquete. El HMAC se calcula sobre la carga útil del paquete y el material de la cabecera del paquete, incluyendo el número de secuencia de paquete. Si un atacante interfiera con los paquetes, los destinatarios detectar la manipulación verificando el autenticador *HMAC*.

- **Protección de Repetición**

SRTP utiliza secuenciación para proteger contra ataques de repetición. Un ataque de repetición es una forma de ataque criptográfico, en el que el hacker envía información obsoleta para forzar algún tipo de acción en el extremo receptor. Para evitar este tipo de ataques, el receptor mantiene los índices de mensajes recibidos anteriormente, comparándolas con el índice de cada mensaje recién recibido y admitiendo el nuevo mensaje sólo si no se ha jugado antes. Esta función se basa en la protección de la integridad que evita la suplantación de los índices de mensajes.

- **Formato de Paquete RTP**

SRTP difiere de RTP sólo en la carga útil de voz cifrada y el SHA-1 etiqueta de

autenticación 32-bit que se añade al paquete. La etiqueta de autenticación contiene los primeros 32 bits de la 160-bit hash SHA-1 digerir que se calculó a partir de la cabecera RTP y la carga útil de voz encriptada ("huella digital truncada"). El acortamiento de la huella dactilar 20-4 bytes se considera para ofrecer suficiente protección de la integridad mientras se mantiene la sobrecarga en un mínimo.

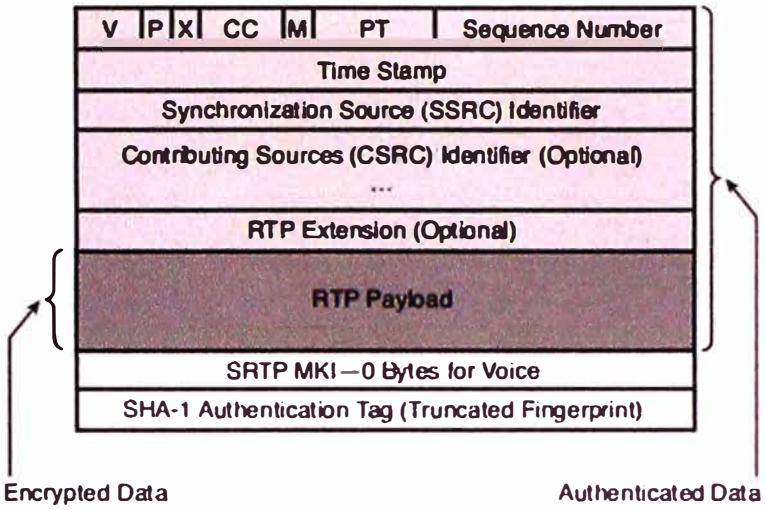


Figura 2.17 Formato de paquete SRTP

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 181)

Los campos utilizados en la cabecera RTP, como se muestra en la figura 2.17, como el tipo de carga útil, número de secuencia, marca de tiempo, y las banderas restantes se realizan en paquetes SRTP en texto plano, lo mismo que con el procesamiento de paquetes RTP.

La cabecera del paquete RTP y la carga útil RTP (voz encriptada) se autentican. Cifrado RTP se realiza antes de la autenticación RTP.

e) Consideraciones VoIP

VoIP consiste de dos componentes principales: señalización y la media, como se ilustra en la figura 2.18. Los protocolos de señalización utilizan números de puerto estáticos. Los valores por defecto son H.323 (/ puerto TCP 1720 UDP), SIP (puerto TCP / UDP 5060), MGCP (UDP / 2427), SCCP (TCP / 2000). Puertos estáticos permiten que los servidores de seguridad para identificar fácilmente el tráfico de señalización y, o bien permitir o bloquear, dependiendo de la política de seguridad.

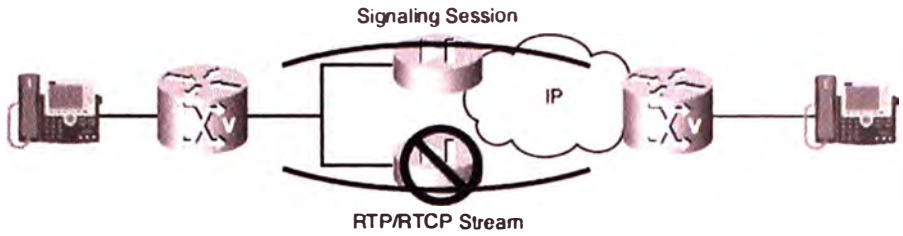


Figura 2.18 Flujo de Media y Señalización VoIP

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 181)

Flujos RTP y RTCP usan negociados dinámicamente números de puerto UDP. Los filtros de lista de control de acceso (ACL) estático no son capaces de permitir o bloquear selectivamente ciertos flujos de medios.

Equipos Cortafuegos o (*Firewalls*) rastrean la negociación de puerto RTP gestionado por el protocolo de señalización y permitir selectivamente los puertos UDP negociados si la sesión de señalización anterior fue permitida por la directiva de *Firewall*. Todos los demás puertos permanecen bloqueados y sólo los puertos actualmente negociados se pasan a través.

Esta técnica funciona bien si las sesiones RTP y RTCP fluyen sobre el mismo *Firewall* como los mensajes de señalización. Si los caminos se separan, los flujos RTP y RTCP serán reducidos o caídos por un *Firewall*, debido a que el *Firewall* no ha procesado los mensajes de señalización y por lo tanto no ha abierto los puertos UDP. Para evitar estos problemas, el diseño de la red debe garantizar que los flujos de medios toman el mismo camino que la señalización.

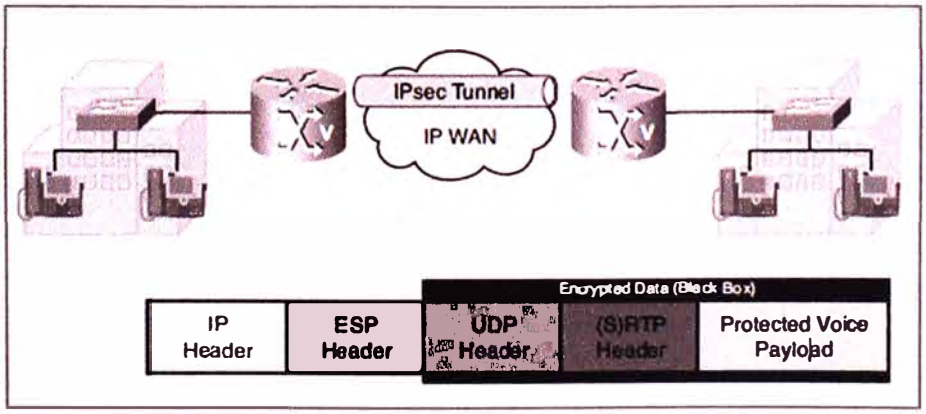


Figura 2.19 Usando IPsec para proteger la voz

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 182)

En las comunicaciones entre sitios, la empresa a menudo asegura el tráfico intercambiado entre las localidades. La tecnología VPN más común usado en estos casos es de seguridad IP (IPsec), con *Encapsulating Security Payload* (ESP) como el protocolo de cifrado y autenticación, como se muestra en la figura 2.19. ESP proporciona el mismo tipo de seguridad como SRTP.

Si ambos métodos de seguridad (SRTP y *IPsec*) están desplegados en la red, SRTP es típicamente recomendado para asegurar las llamadas, por estas razones:

- SRTP crea menos *overhead* que *IPsec*, consumiendo así menos ancho de banda y mejorar la demora.
- SRTP puede proteger a todas las otras llamadas VoIP, como de los usuarios móviles, lo que permite un enfoque más uniforme para expresar de seguridad.

2.3.6 Detección de Voz Activa

La detección de Voz Activa (*Voice Activity Detection* – VAD) es una tecnología que se basa en la naturaleza de la conversación humana, donde una persona habla mientras que otros escuchan. Esta conversación típica unidireccional se ilustra en la figura 2.20.

VAD ofrece un máximo de ahorro de ancho de banda 35 por ciento basado en un volumen promedio de más de 24 llamadas. Ahorro de ancho de banda de 35 por ciento es una cifra subjetiva, no toma en cuenta los sonidos de fondo de las conversaciones, las diferencias de idiomas, y otros factores. Cuando una red está diseñada para el ancho de banda de llamada de voz completa, todos los ahorros proporcionados por VAD pasarán a estar disponibles para las aplicaciones de datos

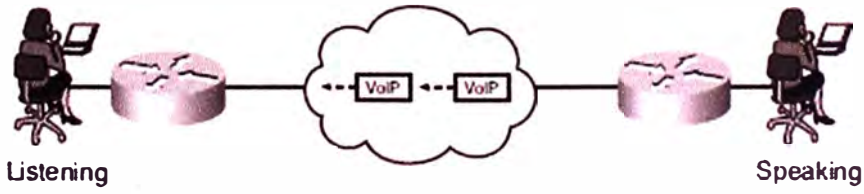


Figura 2.20 Naturaleza unidireccional de la conversación humana

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 183)

La degradación de la calidad de la voz podría ser notable cuando los sonidos iniciales se cortan después de un periodo de silencio. En tales casos, la desactivación de VAD normalmente resuelve el problema.

- **Ahorros de Ancho de Banda**

En la tabla 2.6 se indica el ahorro de ancho de banda obtenidos por VAD al

transmitir los paquetes de VoIP sobre Frame Relay enlaces. La tabla compara el ancho de banda en bruto por códec (velocidad códec) con los anchos de banda eficaces, teniendo en cuenta todo el *overhead* (Capa 2 y superior), con y sin VAD.

Tabla 2.6 Ahorro promedio de ancho de banda por VAD

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 183)

Códec	**Velocidad del Códec**	**Tamaño de muestra**	**Frame Relay sin VAD**	**Frame Relay con VAD**
G.711	64 kbps	240 bytes	76.3 kbps	49.6 kbps
G.711	64 kbps	160 bytes	82.4 kbps	53.6 kbps
iLBC	13.3 kbps	30 bytes	26.1 kbps	17.0 kbps
iLBC	15.2 kbps	20 bytes	34.4 kbps	22.4 kbps
G.729	8 kbps	30 bytes	20.3 kbps	13.2 kbps
G.729	8 kbps	20 bytes	26.4 kbps	17.2 kbps

2.3.7 Principales ventajas de VoIP

Uno de los principales impulsores de la combinación de las redes de voz y datos es ahorro monetario. Si nos fijamos estrictamente a costos minuto a minuto, los ahorros realizados por ir con VoIP podría no ser lo suficientemente grande como para justificar el gasto de despliegue de este servicio. Los ahorros de precios pueden variar en función de su ubicación geográfica. En países distintos de América del Norte, por ejemplo, una comparación minuto a minuto coste entre VoIP y PSTN tradicional (una llamada local en algunos países puede ser alrededor de $ 1 por minuto) más que para justificar el gasto de la nueva red.

2.4 Protocolo de Señalización de Voz: H.323

Gateways H.323 son los extremos de una LAN que proporcionan en tiempo real, las comunicaciones bidireccionales entre terminales H.323 en la LAN y otras terminales del UIT-T en la red. *Gateways* H.323 también pueden comunicarse con otros *Gateways* H.323. *Gateways* permiten terminales H.323 para comunicarse con terminales que no son terminales H.323 por protocolos de conversión. *Gateways* son el punto donde se codifica

una llamada por conmutación de circuitos y empaquetado de nuevo en paquetes IP. Debido *Gateways* funcionan como puntos finales H.323, proporcionan el control de admisión, la búsqueda de direcciones y la traducción y servicios de contabilidad.

2.4.1 Arquitectura H.323

H.323 es un conjunto de protocolos que la UIT definido para las conferencias multimedia sobre LANs. Fue desarrollado basado en RDSI Q.931 como un protocolo para proporcionar redes IP con funcionalidad de telefonía tradicional. H.323 es un protocolo maduro, independiente del proveedor, se encuentra actualmente como estándar de mayor despliegue basado en la voz y de vídeo estándar de conferencia de redes de paquetes conmutados.

H.323 es un protocolo de punto a punto en la que cada *Gateway* desempeña un papel igual en el proceso de señalización y debe mantener su propio plan de marcado para tomar decisiones de reenvío de llamadas. Esta característica diferencia a H.323 de protocolos de señalización servidor-cliente tales como MGCP, donde los *Gateway* son registrados en el agente de llamada (*call agent*) para recibir más instrucciones. La suite de H.323 es soportada en grandes vendedores de centrales de telefonía y videoconferencia IP como Polycom, Avaya y *Cisco Systems*.

H.323 describe una infraestructura de terminales, componentes de control común, servicios y protocolos que se utilizan para comunicaciones multimedia (voz, vídeo y datos).

Un *Gateway* H.323 es un tipo opcional de punto final que proporciona interoperabilidad entre los puntos finales H.323 y puntos finales que se encuentran en una red de circuitos conmutados (SCN), como la PSTN o una red de voz de la empresa. Idealmente, el *Gateway* es transparente tanto para el punto extremo H.323 y el punto final basado en SCN.

a) Ventajas H.323

Hay varias ventajas de utilizar *Gateways* H.323 como *Gateways* de voz:

- Plan de marcación Autosuficiente por *Gateway*: Permite procesar el enrutamiento de llamadas locales sin depender de un agente de llamada, como es el caso de MGCP.
- Las traducciones pueden ser definidos por *Gateway*: Todas las llamadas entrantes y salientes se pueden traducir directamente en el *Gateway* para cumplir con el formato de

número que se utiliza internamente.

- No hay dependencias en Agentes de llamadas o *Call Agents:* Debido a que la configuración se realiza en el *Gateway* y el soporte de H.323 es un protocolo punto a punto, no hay dependencia de versiones de software y conjuntos de características de otros componentes de señalización.
- La mayoría de interfaces de voz son soportados en los *Gateways* H.323.
- Soporte de fax: Soporte de Fax es mejor en *Gateways* H.323 que en *Gateways* MGCP debido a que H.323 soporta T.37 y T.38. Un *Gateway* H.323 puede enrutar un número de marcación interna directa (*DID:Direct Inward Dialing*) directamente a un puerto FXS (*Foreign Exchange Station*).

b) Componentes de Red H.323

En la figura 2.21 se muestra los típicos dispositivos en una red H.323. Una red H.323 incluye los siguientes componentes:

- Terminales: H.320 (RDSI), H.323, H.324 (servicio telefónico ordinario [POTS])
- *Gateways* o Puertas de Enlance
- *Gatekeeper*s o Controladores de Acceso
- Unidad de Control Multipunto (Multipoint Control Unit)
- Elemento de Borde (Session Border Control)

➢ **Terminales H.323**

Un terminal H.323 es un punto final que proporciona voz en tiempo real (y, opcionalmente, video y datos) de comunicaciones con otro punto final, tal como un terminal H.323 o MCU. Las comunicaciones se componen de control, indicaciones, audio, imágenes en movimiento de vídeo en color, o los datos entre los dos terminales. Un terminal puede proporcionar lo siguiente:

- Solo audio
- Audio y datos
- Audio y video
- Audio datos y video
- El terminal puede ser un sistema de videoconferencia basados en computadora u otro dispositivo.

- Un terminal H.323 debe ser capaz de transmitir y recibir voz que es codificada con G.711 (a-law y mu-law), y puede soportar otros formatos de voz codificados, como G.729 y G.723.1.

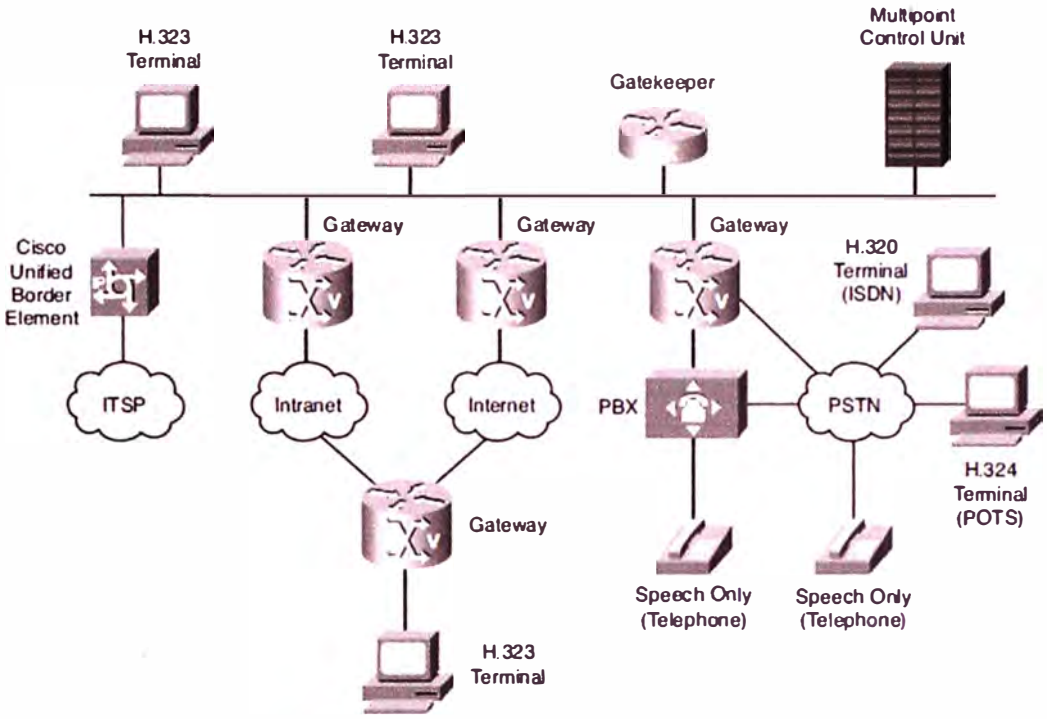


Figura 2.21 Dispositivos H.323

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 186)

➢ *Gateways* H.323

En la figura 2.22 se muestra un *Gateway* que conecta un dispositivo H.323, y un terminal que no es un terminal H.323, tales como un teléfono analógico. El dispositivo H.323 puede ser un terminal H.323, MCU, *Gatekeeper*, u otra *Gateway* H.323.

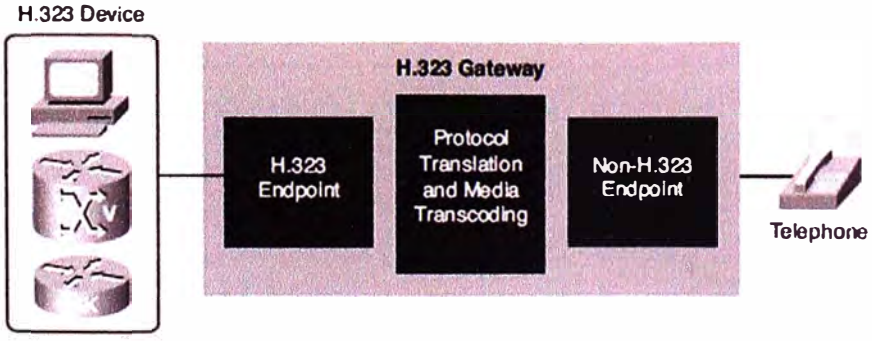


Figura 2.22 Gateway H.323

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 187)

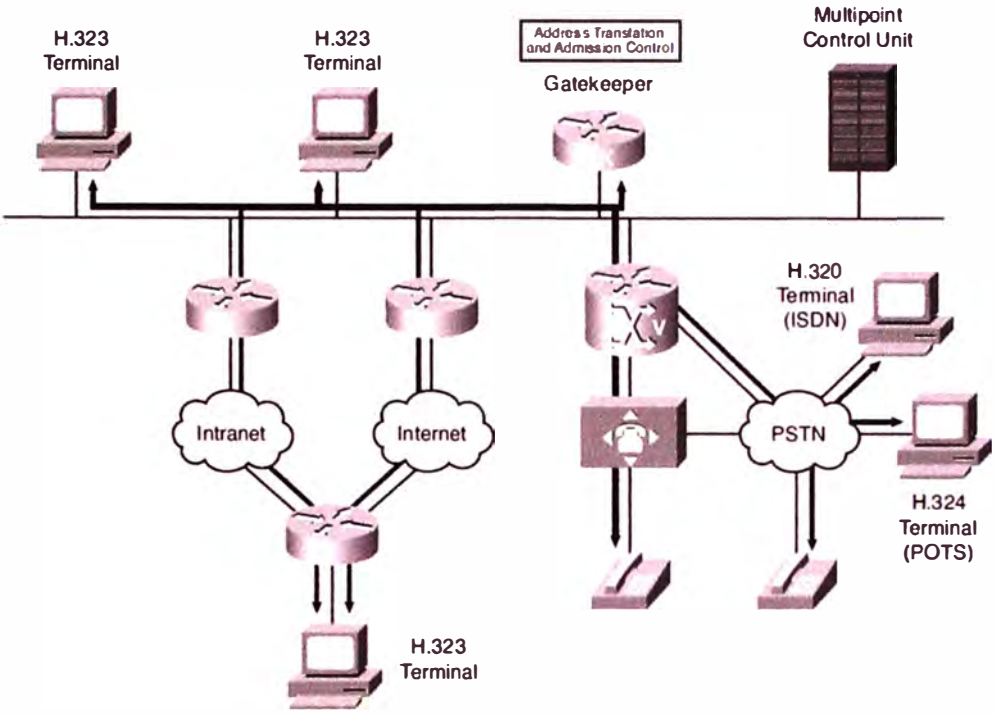


Figura 2.23 Funciones de Gatekeeper H.323

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 188)

Los *Gateways* permiten dispositivos H.323 para comunicarse con los dispositivos que ejecuten otros protocolos. Proporcionan la conversión de protocolo entre los dispositivos que ejecutan diferentes tipos de protocolos. Idealmente, el *Gateway* es transparente tanto para el punto final H.323 y el punto final no H.323.

Un *Gateway* H.323 realiza estos servicios:

- Traducción entre audio, vídeo y formatos de datos.
- La conversión entre señales y procedimientos de establecimiento de llamada.
- La conversión entre señales y procedimientos de control de la comunicación.

➢ ***Gatekeepers* H.323**

Un *Gatekeeper* H.323, como se muestra en la figura 2.23, proporciona traducción de direcciones y control de acceso para los terminales H.323, *Gateways* y MCUs. *Gatekeepers* son nodos opcionales que manejan puntos finales en una red H.323. Los puntos finales se comunican con el *Gatekeeper* utilizando el protocolo de registro de admisión y estado (*RAS: Registration, Admission, and Status*).

Los puntos finales intentan registrarse con un *Gatekeeper* en el inicio. Cuando quieren comunicarse con otro punto final, solicitan la admisión para iniciar una llamada. Si el *Gatekeeper* decide que la llamada puede proceder, devuelve una dirección IP de destino al punto final de origen. Esta dirección IP no puede ser la dirección real del punto final de destino, pero una dirección intermedia, como la dirección de un *Proxy* o un *Gatekeeper* que enruta de señalización de llamada.

Cuando se incluye un *Gatekeeper*, realiza estas funciones:

- Traducción de direcciones: Convierte una dirección de alias a una dirección IP.
- Control de admisión: Limita el acceso a los recursos de red basado en las restricciones de ancho de banda de llamada.
- Control de Ancho de Banda: Responde a las peticiones de ancho de banda y modificaciones.
- Gestión de la Zona: Proporciona servicios a los puntos finales registrados.

El *Gatekeeper* también puede realizar estas funciones:

- Autorización de llamada: Rechaza llamadas basada en la falta de autorización
- Gestión de ancho de banda: Limita el número de accesos concurrentes a recursos de red IP (control de admisión de llamadas CAC)

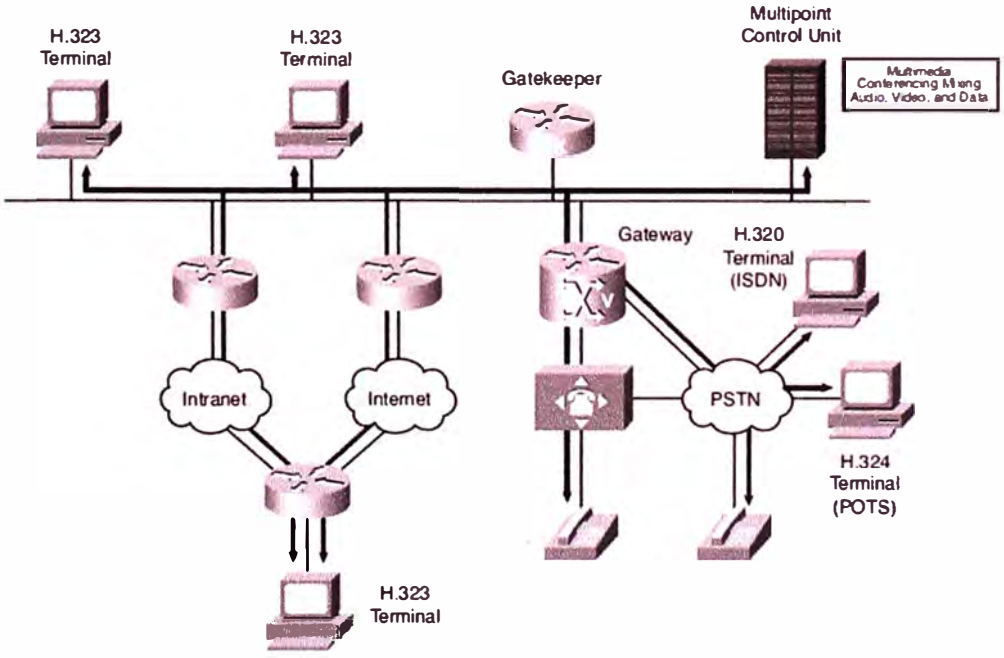


Figura 2.24 Funciones MCU H.323

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 189)

➢ **Unidades de Control Multipunto H.323 (*H.323 Multipoint Control Units*)**

Una unidad de control multipunto, como se muestra en la figura 2.24, es un punto final en la red que permite a tres o más puntos finales participar en una conferencia multipunto. Controla y mezcla de vídeo, audio y datos de los puntos finales para crear una robusta conferencia multimedia. Un MCU también puede conectar dos puntos finales en una conferencia de punto a punto, que más tarde podría convertirse en una conferencia multipunto.

Las conferencias multipunto dependen de un solo MCU para coordinar los miembros de una conferencia. Cada punto final tiene una conexión de canal de control H.245 a la MCU.

O bien el MCU o el punto final inician la configuración del canal de control. H.323 define tres tipos principales de conferencias multipunto: centralizados, distribuidos y ad hoc, como se ilustra en la figura 2.25.

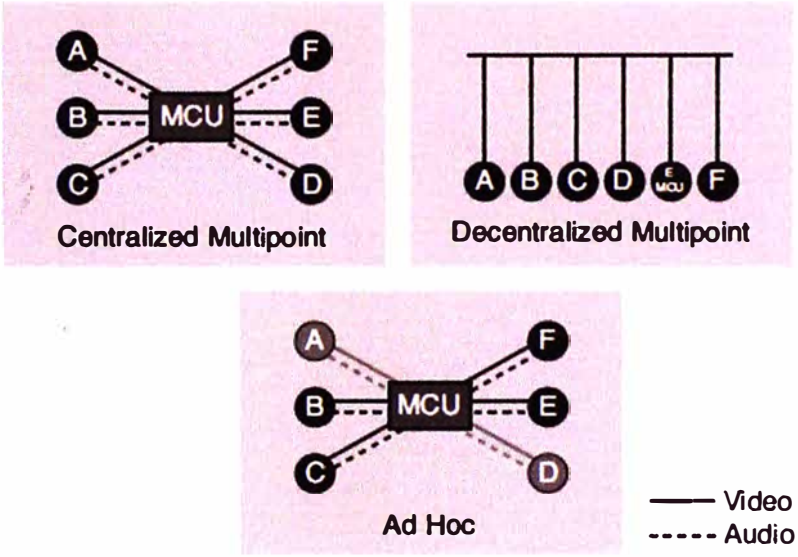


Figura 2.25 Tipos de Conferencias

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 189)

Los tres tipos principales de conferencias multipunto son:

- Conferencia multipunto Centralizada: Los puntos finales deben tener el audio, video, o canales de datos conectados a un procesador multipunto (MP). El MP realiza la mezcla y la conmutación del audio, vídeo y datos, y si el MP es compatible con la capacidad, cada punto final puede operar en un modo diferente.
- Conferencia multipunto Distribuida: Los puntos finales no tienen una conexión a un MP. En cambio, los puntos finales *multidifunden* sus audio, vídeo y flujos de datos a todos los participantes en la conferencia. Debido a que un MP no está disponible para la

conmutación y la mezcla, cualquier mezcla de las corrientes de conferencia es una función del punto final, y todos los puntos finales debe utilizar los mismos parámetros de comunicación.

- Conferencia multipunto *Ad-hoc*: Una conferencia multipunto ad hoc, es una situación híbrida, en la que los flujos de audio y vídeo son gestionadas por un único MCU, pero donde un flujo depende de la multidifusión (según el modelo distribuido) y el otro utiliza el MP (como en el modelo centralizado). Cualquiera de los dos puntos finales en una llamada puede convertir su relación en una conferencia punto a punto. Cuando se crea la conferencia de punto a punto, otros puntos finales se convierten en parte de la conferencia, al aceptar una invitación de un participante actual o el punto final pueden solicitar unirse a la conferencia.

2.4.2 Flujos de llamada H.323

En la figura 2.26 se muestran los elementos de un terminal H.323 y destaca la infraestructura de protocolo de un *endpoint* H.323.

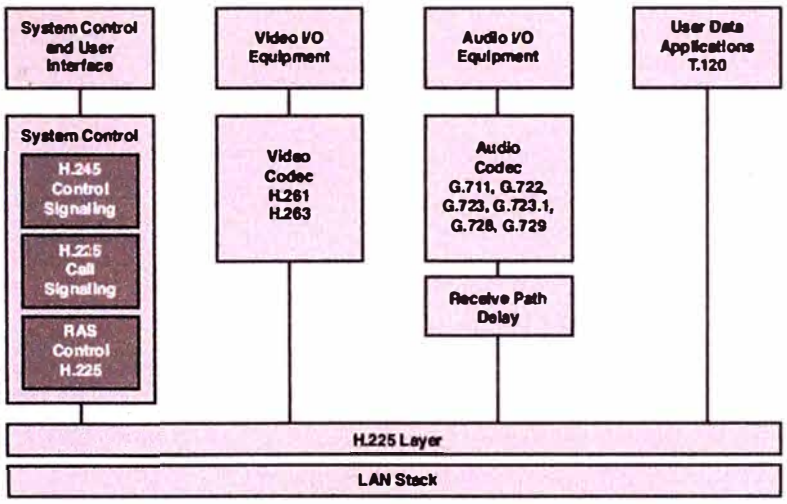


Figura 2.26 Stack de Protocolos H.323

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 192)

H.323 es considerado un "protocolo paraguas", ya que define todos los aspectos de la transmisión de llamadas, desde establecimiento de llamada a intercambio de capacidades y disponibilidad de recursos de la red. H.323 define estos protocolos:

- H.225 para el establecimiento de llamada (*call setup)*: La función de señalización de llamada permite un punto final crear conexiones con otros puntos finales. La función de señalización de llamada define los procedimientos de establecimiento de llamada que se basan en el protocolo RDSI Q.931 UIT, que permite la interoperabilidad con la red PSTN

y Sistema de Señalización 7 (SS7).

- H.225 para el registro, admisión y control de estado (*Registration, Admission, and Status RAS*): La función de señalización RAS utiliza un canal de señalización independiente para realizar el registro, admisiones, cambios de ancho de banda, el estado y desenganchar los procedimientos entre los puntos finales y un *Gatekeeper*.
- H.245 para el intercambio de capacidades: El canal de control H.245 está separado del canal de señalización de llamada y es responsable de las siguientes funciones:
  - Señalización de canal lógico: Abre y cierra los flujos de medios RTP o RTCP.
  - Intercambio de capacidades: Negocia audio, video, y las capacidades del códec.
  - Maestro: Determina qué punto final es un maestro y quien es un contestador. Se utiliza para resolver conflictos durante la llamada.
  - Solicitud de Modo: Pide un cambio en el modo, o capacidad, de la corriente de los medios de comunicación.

a) Configuración de llamadas H.323

En la figura 2.27 se muestra el inicio de un intercambio de establecimiento de llamada de H.323 entre dos *Gateways*.

El mismo procedimiento se utiliza cuando uno o ambos puntos finales son terminales H.323. La secuencia paso a paso de la comunicación es:

1.- Un punto terminal inicia una llamada.

2.- El *Gateway* de origen inicia una sesión H.225 con el *Gateway* de terminación en el puerto TCP 1720. El *Gateway* de origen determina la dirección del *Gateway* de terminación desde su configuración local.

3.- El *Gateway* de terminación reconoce la Configuración de llamadas con el mensaje de Llamada de Procedimiento (*Call Proceeding*).

4.- El *Gateway* de terminación envía la señal de llamada *(ringing signal)* en el teléfono del destinatario.

5.- El *Gateway* de terminación notifica al *Gateway* de origen sobre el timbre con el mensaje de Alerta (*Alerting message*).

6.- El *Gateway* de origen señala el tono de devolución de llamada al *endpoint* de origen.

7.- El receptor descuelga el teléfono.

8.- El *Gateway* de terminación envía el mensaje Conectar al *Gateway* de origen.

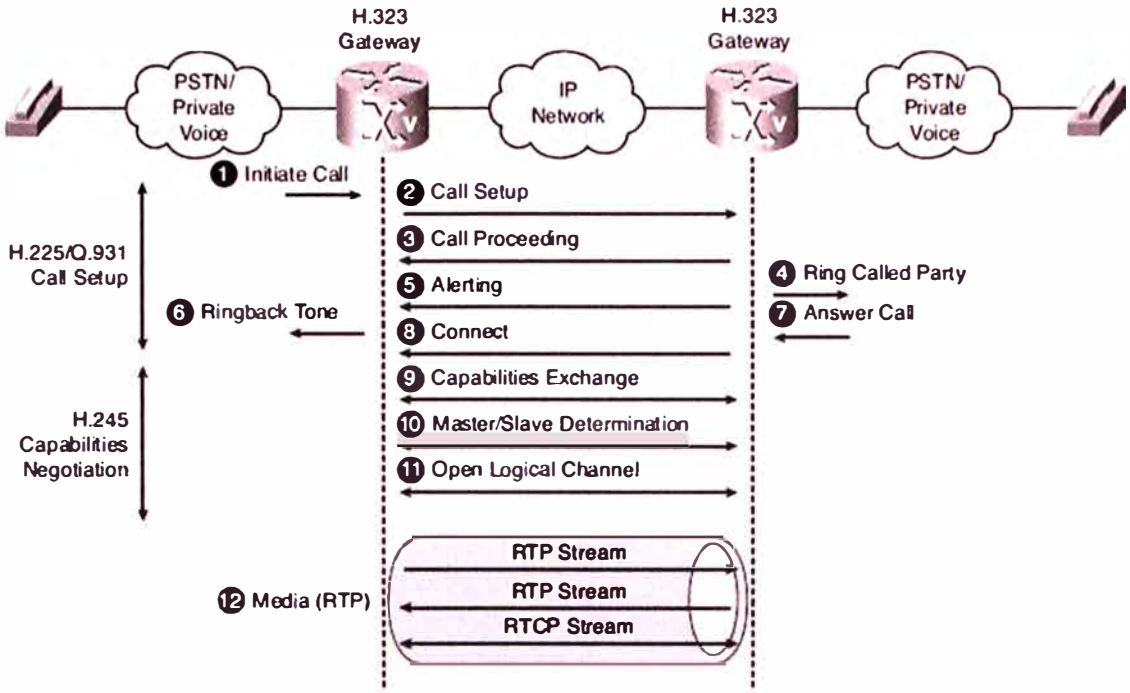


Figura 2.27 Configuración de llamada H.323

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 193)

9.- Los puntos finales abren otro canal para la función de control H.245. El H.245 tiene la función de control de negociar capacidades.

10.- La función de control H.245 determina los roles de maestro / esclavo para resolver posibles conflictos. La función de control H.245 determina los roles de maestro / esclavo para resolver posibles conflictos.

11.-La función de control H.245 intercambia mensajes OLC (*Open Logical Channel*) que describen los flujos RTP.

12.- Los *Gateways* inician la transmisión de la data multimedia sobre los canales RTP e intercambiando estadísticas de calidad de llamadas usando RTCP.

b) Terminación de llamada (*Call Teardown)* H.323

La figura 2.28 muestra una terminación de llamada entre dos *Gateways*.

La siguiente lista describe cada paso:

1.- Una de las partes que participa en la comunicación, cuelga (*hang up)*. Este ejemplo muestra al punto final detrás del *Gateway* de terminación, pero este procedimiento se refleja si el punto final detrás de la *Gateway* de origen, cuelga.

2.- El *Gateway* de terminación envía los mensajes de cerrar el canal lógico, *Close Logical Channel*, hacia el *Gateway* de Origen.

3.- El *Gateway* de origen reconoce (*acknowledges*) el mensaje.

4.- El *Gateway* de terminación envía el mensaje Comando Sesión Fin, *End Session Command*, al *Gateway* de origen.

5.- El *Gateway* de origen reconoce (*acknowledges*) el mensaje.

6.- El *Gateway* de terminación envía el mensaje de liberación completa, *Release Complete*, al *Gateway* de origen.

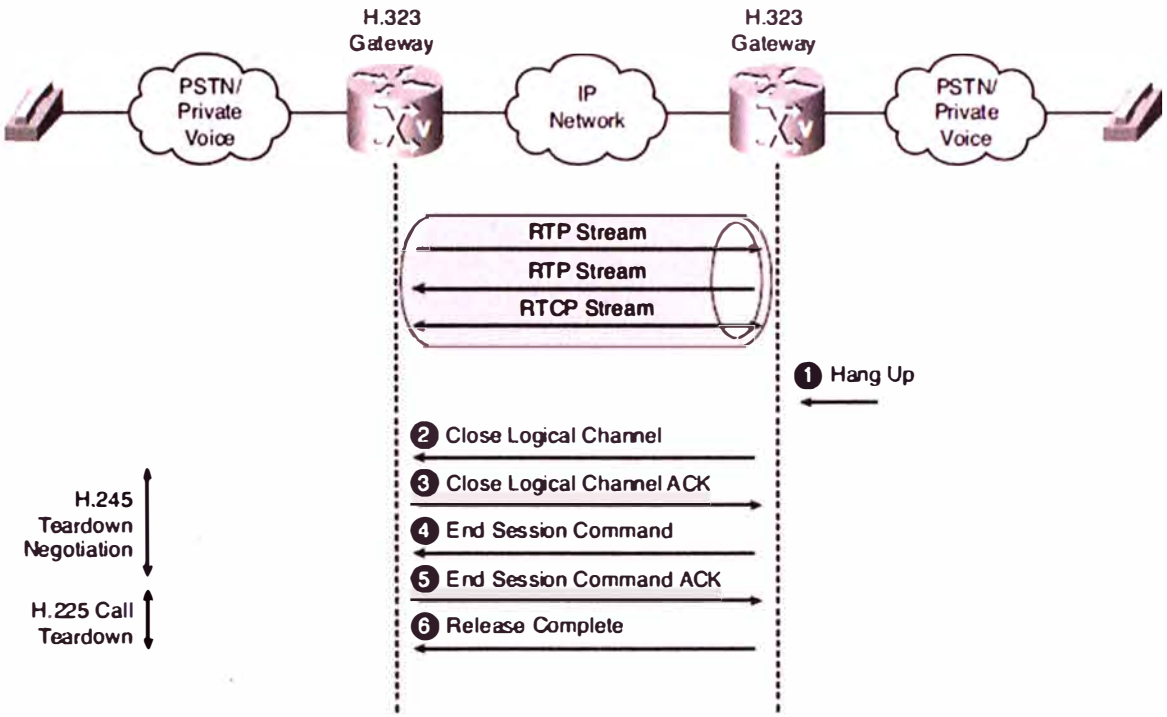


Figura 2.28 Terminación de llamada H.323

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 195)

c) Configuración de llamada RAS H.225

En la figura 2.29 se muestra un intercambio de establecimiento de llamada básica H.323 entre dos *Gateways* que están registrados en un *Gatekeeper*. El mismo procedimiento se utiliza cuando uno o ambos puntos finales son terminales H.323.

La siguiente lista describe cada paso:

1.- Un *endpoint* inicia la llamada.

2.- El *Gateway* de origen inicia una sesión H.225 con el *Gatekeeper* en el puerto registrado RAS TCP / 1719. El *Gatekeeper* escucha en el puerto TCP 1718 los mensajes de descubrimiento, y el proceso de descubrimiento debe ser completado antes de que el *Gateway* pueda enviar mensajes RAS al *Gatekeeper*. El *Gateway* envía la solicitud de Admisión (*Admisiion Request*)

3.- El *Gatekeeper* retorna la confirmación de admisión (*Admission Confirmation - ACF*) que incluye la dirección IP del *Gateway* de terminación.

4.- El *Gateway* de origen inicia una sesión H.225 con el *Gateway* de terminación en el puerto TCP/1720 usando el mensaje de configuración de llamada *Call Setup* H.225/Q.931.

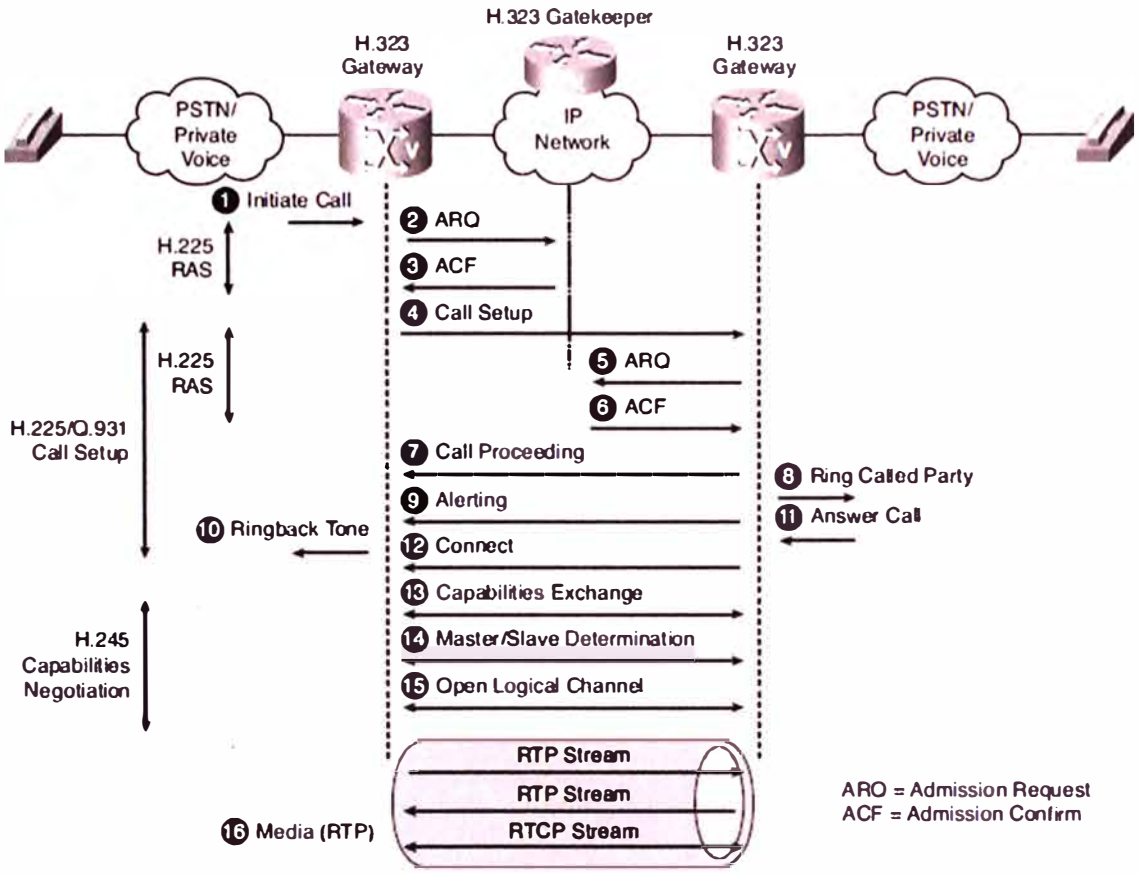


Figura 2.29 Configuración de llamada RAS H.225

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 196)

5.- El *Gateway* de terminación envía ARQ al *Gatekeeper* (TCP / 1719) solicitando permiso para aceptar la llamada.

6.- El *Gatekeeper* retorna el ACF al *Gateway* de terminación, la concesión de permiso para aceptar la llamada.

7.- El *Gateway* de terminación reconoce el *Call Setup* (Configuración de llamadas) con el mensaje de procedimiento de llamada (*Call Proceeding*) al *Gateway* de origen.

8.- El *Gateway* de terminación envía la señal de llamada al teléfono del destinatario.

9.- El *Gateway* de terminación notifica el *Gateway* de origen sobre el zumbido con el mensaje de alerta (*alerting message*).

10.- El *Gateway* de origen señala el tono de llamada de devolución al *endpoint* de origen.

11.- El receptor descuelga el teléfono.

12.- El *Gateway* de terminación envía el mensaje Conectar (*Connect*) al *Gateway* de origen.

13.- Los *endpoints* abren otro canal para la función de control H.245. La función de control H.245 negocia primero capacidades (*Capabilities Exchange*).

14.- La función de control H.245 determina los roles de maestro / esclavo para resolver posibles conflictos (*Master/Slave Determination).*

15.- La función de control H.245 intercambia mensajes OLC (*Open Logical Channel)* que describen los flujos RTP.

16.- Los *Gateways* inician la transmisión de la data multimedia sobre los canales RTP e intercambiando estadísticas de calidad de llamadas usando RTCP.

d) Terminación de llamada (*Call Teardown*) RAS H.225

En la figura 2.30 se muestra una terminación de llamada H.323 entre dos *Gateways* que están registrados a un *Gatekeeper*.

La siguiente lista describe cada paso:

1.- Una de las partes que participa en la comunicación, cuelga (*hang up*)

2.- El *Gateway* de terminación envía el mensaje Cerrar Canal Lógico (*Close Logical Channel*) al *Gateway* de origen.

3.- El *Gateway* de origen reconoce *(acknowledges*) el mensaje.

4.- El *Gateway* de terminación envía el mensaje Comando Fin de Sesión (*End Session Command*) al *Gateway* de origen.

5.- El *Gateway* de origen reconoce (*acknowledges*) el mensaje.

6.- El *Gateway* de terminación envía el mensaje de liberación completa (Release Complete) al *Gateway* de origen.

7.- Ambos *Gateways* envían mensajes petición de desenganche (*Disengage Request DRQ*) para el *Gatekeeper*.

8.- El *Gatekeeper* responde a ambos DRQs con mensajes de Confirmar Desenganche (*Disengage Confirm DCF*)

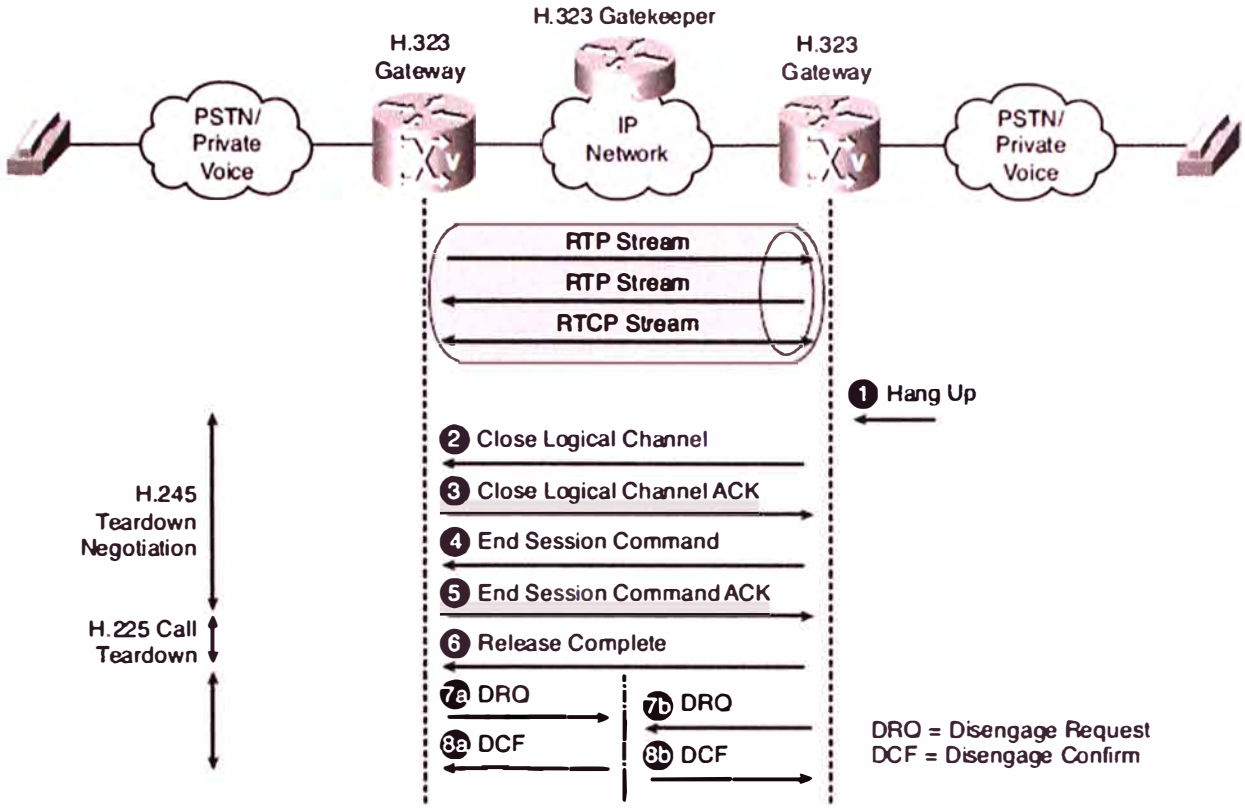


Figura 2.30 Terminación de llamada RAS H.225

(Fuente Ref. CVoice 642-437-Wallace, 2011, pág. 198)

2.5 Protocolo de Señalización de Voz: SIP

Protocolo de Inicio de Sesión (*Session Initiation Protocol - SIP*) es uno de los protocolos de señalización de voz más importantes dentro de las redes de proveedores de servicios de VoIP y es apoyado por la mayoría de los proveedores de sistemas de telefonía IP. Como tal, es un protocolo ideal para interconectar diferentes sistemas de VoIP y redes. El conocimiento de las características y funciones de los componentes SIP, y las relaciones que establecen con los componentes entre sí, es importante en la implementación de un entorno SIP escalable, flexible y seguro. Esta sección explora las características y funciones del entorno SIP, incluidos sus componentes, cómo estos componentes interactúan y cómo acomodar la escalabilidad y capacidad de supervivencia.

2.5.1 Arquitectura SIP

La *Internet Engineering Task Force (IETF)* desarrolló SIP como una alternativa a H.323. SIP es un estándar común que se basa en la lógica de la *World Wide Web* y muy sencillo de implementar. Es ampliamente utilizado con *Gateways* y servidores *Proxy* dentro de las redes de proveedores de servicios para la señalización interna y cliente final.

Al igual que otros protocolos VoIP, SIP está diseñado para atender las funciones de señalización y gestión de sesiones dentro de una red de telefonía de paquetes.

SIP funciona según el principio de las invitaciones de la sesión que se basa en un modelo de solicitud y respuesta transacción HTTP. Cada transacción consiste en una solicitud que invoca un método en particular, o de la función, en el servidor y al menos una respuesta. A través de invitaciones, SIP inicia sesiones o invita a los participantes en las sesiones establecidas. Las descripciones de estas sesiones se anuncian por cualquiera de varios medios, entre ellos el Protocolo de Anuncio de Sesión (*Session Announcement Protocol* SAP) definido en RFC 2974. SAP incorpora una descripción de la sesión de acuerdo con el Protocolo de Descripción de Sesión (*Session Description Protocol*, SDP) definido en RFC 2327.

SIP utiliza otros protocolos IETF para definir otros aspectos de sesiones VoIP y multimedia; por ejemplo, las direcciones URL para direccionar, Sistema de nombres de dominio (DNS) para la localización de servicios y Enrutamiento de Telefonía sobre IP (*Telephony Routing over IP TRIP*) para el enrutamiento de llamadas.

SIP es un protocolo punto a punto donde los *endpoints* de la Internet (llamados Agentes de usuario o *user agents [UA])* inician sesiones, similar a un punto H.323. Los UAs (Agentes de Usuarios) se descubren uno al otro y coinciden en una sesión que quisieran compartir. Para la localización de los participantes de la sesión y otras funciones. SIP permite la creación de una infraestructura de máquinas de la red (llamados servxidores *Proxy*) para que los agentes de usuario (UAs) puedan enviar registros, invitaciones a sesiones, y otras peticiones. SIP es una herramienta de propósito general ágil para crear, modificar y terminar sesiones, que funciona independientemente de los protocolos de transporte subyacentes y sin depender del tipo de sesión que se está estableciendo.

A diferencia de H.323, SIP utiliza mensajes de texto ASCII para comunicarse. Por lo tanto, permite una fácil resolución de problemas mediante el análisis del contenido de la señalización.

a) Señalización y Despliegue

SIP soporta cinco métodos para establecer y terminar las comunicaciones multimedia, que se traducen en las siguientes capacidades:

- Determina la ubicación del punto final de destino: SIP soporta resolución de direcciones, asignación de nombre, y redireccionamiento de llamadas.
- Determina las capacidades de los medios de comunicación del *endpoint* de destino:

SIP determina el nivel más bajo de los servicios comunes entre los puntos finales a través de SDP. Conferencias son establecidas utilizando sólo las capacidades de medios que pueden ser apoyadas por todos los *endpoints*.

- Determina la disponibilidad del punto final de destino: Si una llamada no puede completarse debido a que el punto final de destino no está disponible, SIP determina si la parte llamada está conectada a una llamada o no. SIP devuelve un mensaje que indica por qué el punto final de destino no estaba disponible.
- Establece una sesión entre los puntos extremos de origen y de destino: Si la llamada puede completarse, SIP establece una sesión entre los puntos extremos. SIP también es compatible con la adición de otro *endpoint* a la conferencia o el cambio de una característica de medios o códec.
- Gestiona la transferencia y terminación de las llamadas: SIP soporta la transferencia de llamadas de un extremo a otro. Durante una transferencia de llamada, SIP simplemente establece una sesión entre el cesionario y un nuevo punto final (especificado por el parte que transfiere) y termina la sesión entre el cesionario y la parte de transferencia.

b) Componentes de la Arquitectura SIP

Como se ilustra en la figura 2.31, SIP es un protocolo punto a punto. Como se mencionó anteriormente, los pares de una sesión se llaman agentes de usuario (UA). Un UA puede funcionar en una de estas dos funciones:

- Cliente de Agente de Usuario (*User agent client,* UAC): Una aplicación cliente que inicia una solicitud SIP.
- Servidor de Agente de Usuario (*User agent Server* UAS): Una aplicación de servidor que contacta con el usuario cuando una invitación SIP es recibida y luego devuelve una respuesta en nombre del usuario al originador de la invitación.

Típicamente, un UA puede funcionar como un UAC o una UAS durante una sesión, pero no tanto en la misma sesión. Si las funciones de punto final como UAC o una UAS dependen de la UA que inició la solicitud; la UAC inicia la sesión y la UAS termina la sesión.

Desde un punto de vista arquitectónico, los componentes físicos de una red SIP se agrupan en estas dos categorías:

- Clientes (*endpoints*)
  - Teléfono IP: Un teléfono IP actúa como un UAS o UAC sobre una base sesión por sesión.

o *Gateway*: Un *Gateway* actúa como UAS o UAC y proporciona soporte de control de llamadas. Al igual que en H.323, *Gateways* SIP ofrecen muchos servicios, el más común es una función de traducción entre extremos SIP y otros tipos de dispositivos, como destinos PSTN.

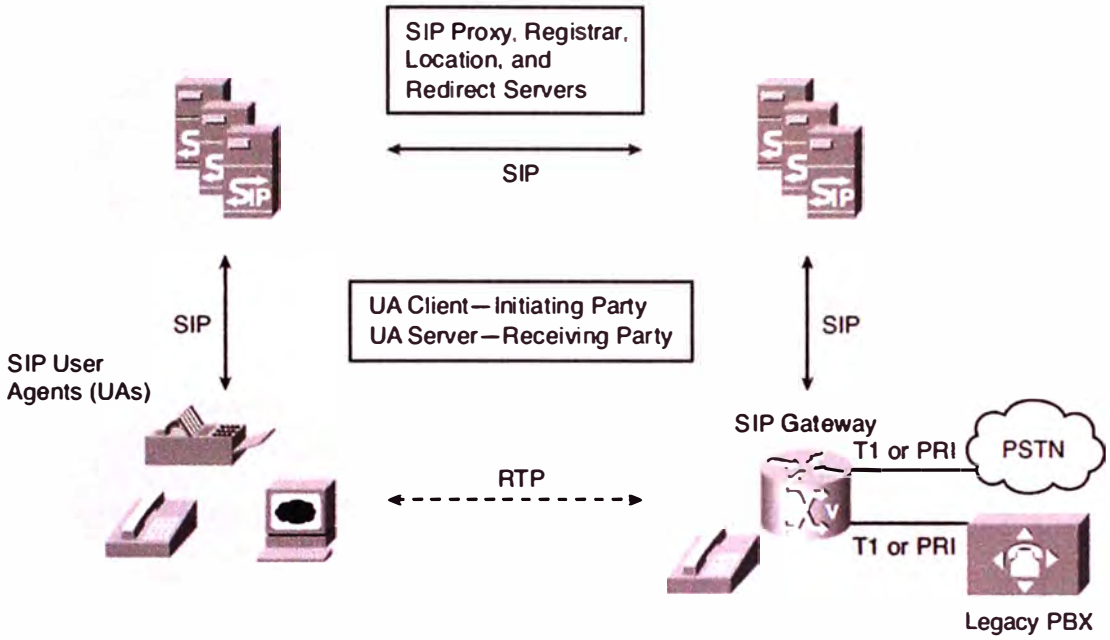


Figura 2.31 Componentes de la Arquitectura SIP

Fuente: "CVoice 642-437" (Wallace, 2011, pág. 209)

- Servidores: *Registrar*, *Proxy*, *Redirect*, y *Location*

c) Servidores SIP

Las diferentes funciones de servidor en el entorno SIP tienen estas características:

- *Registrar Server* (servidor de registro): Recibe solicitudes desde UACs para el registro de su ubicación actual. Servidores Registradores a menudo se encuentran cerca o incluso yuxtapuesto con otros servidores de red, lo más a menudo un servidor de localización (*location Server*).
- *Proxy Server* (servidor *Proxy*): Un componente intermedio que recibe solicitudes SIP de un cliente y luego reenvía las peticiones en nombre del cliente al siguiente servidor SIP en la red. El siguiente servidor puede ser otro Servidor *Proxy* o un UAS. Los servidores *Proxy* pueden proporcionar funciones tales como la autenticación, autorización, control de acceso a la red, enrutamiento, transmisiones de petición, y la seguridad.
- *Redirect Server* (Servidor de Redirección): Proporciona al cliente con información sobre el siguiente salto o saltos que un mensaje debe tomar, y luego los contactos del

cliente con el servidor del siguiente salto o UAS directamente. Cuando el servidor de redirección envía un mensaje de redirección al cliente, el cliente vuelve a enviar la invitación al servidor identificado en el mensaje de redirección. El cliente puede ser redirigido ya sea a otro servidor de red o para los UAS en el punto final de terminación.

- *Location Server* (Servidor de Ubicación): Implementa mecanismos para resolver direcciones. Estos mecanismos pueden incluir una base de datos de registros o el acceso a herramientas de resolución de uso común. Un servidor de registro puede ser modelado como un subcomponente de un servidor de localización; el servidor de registro es en parte responsable para poblar una base de datos que está asociado con el servidor de localización.

d) Ejemplos de Arquitectura SIP

En esta sección analizaremos como ejemplo a la marca *Cisco Systems*. En el mercado existen muchas marcas de centrales de procesamiento de llamadas IP como Avaya, Polycom, Mitel, etc. Específicamente tomaremos los productos de la marca *Cisco Systems*, más adelante en los capítulos 4 y 5 se sustenta porque la elección de esta marca.

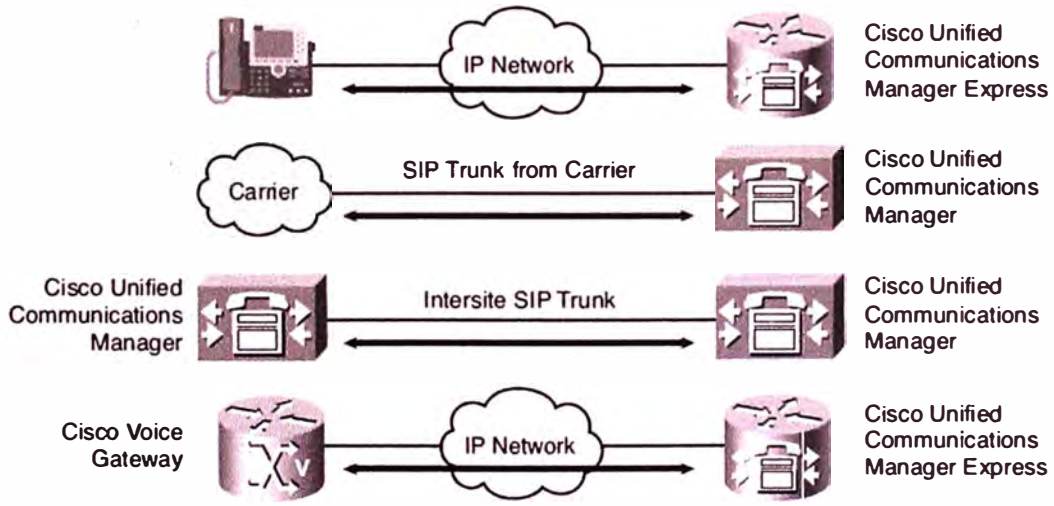


Figura 2.32 Componentes de la Arquitectura SIP

Fuente: "CVoice 642-437" (Wallace, 2011, pág. 210)

En la figura 2.32 se muestran las implementaciones de las comunicaciones unificadas de Cisco pueden desplegar SIP en los siguientes productos:

- *Cisco Unified Communications Manager.*
- *Cisco Unified Communications Manager Express*
- *Cisco Voice Gateways*

- *Cisco Unified IP Phones* corriendo firmware SIP, que se encuentren registrados al *Cisco Unified Communication Manager* o *Cisco Unified Communications Manager Express*
- *Cisco Unified IP Phones* corriendo firmware SIP y la conexión directamente a un proveedor de servicios de telefonía por Internet.
- Troncales SIP a un *carrier (*Proveedor de Servicios de Internet*)*, y entre las oficinas corporativas.

2.5.2 Flujos de Llamadas SIP

La figura 2.33 representa el establecimiento (*call setup*) y terminación (*teardown*) de la llamada directa y desmontaje entre dos *Gateways* SIP.

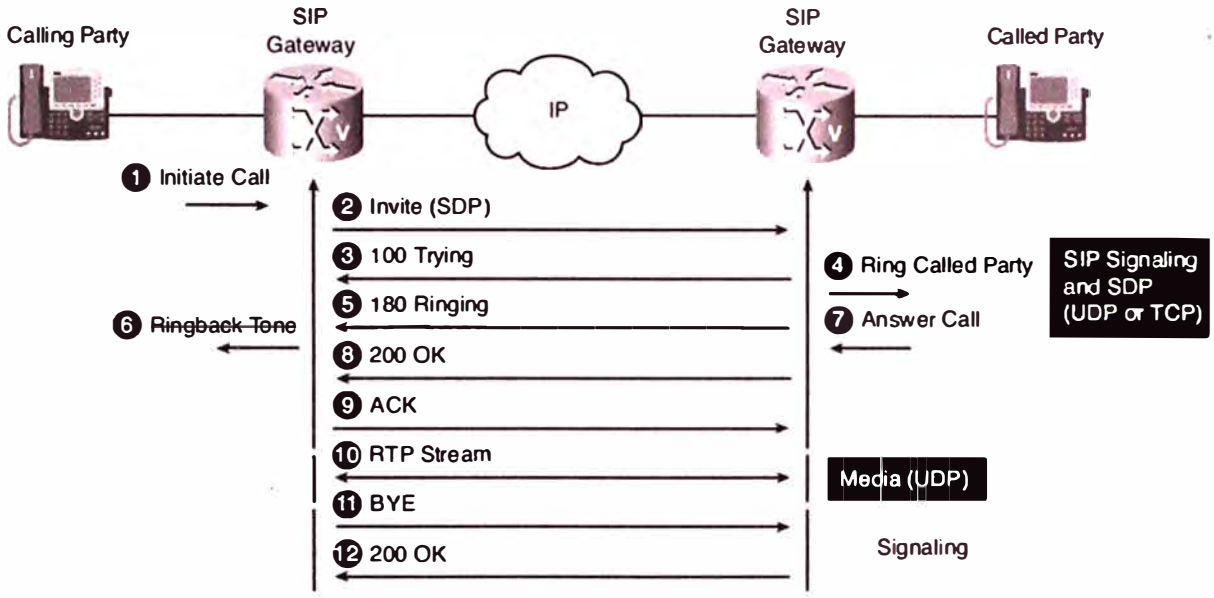


Figura 2.33 Direct Call Setup (Configuración de llamada Directa)

Fuente: "CVoice 642-437" (Wallace, 2011, pág. 211)

Cuando un UAC reconoce la dirección de un *endpoint* de terminación de la información almacenada en caché, o tiene la capacidad de resolverla por algún mecanismo interno, la UAC podría iniciar procedimientos de establecimiento de llamada directa (UAC a UAS). Si un UAC reconoce la UAS destino, el cliente se comunica directamente con el servidor. En situaciones en las que el cliente no es capaz de establecer una relación directa, el cliente solicita la ayuda de un servidor de red.

El establecimiento de llamada directa procede de la siguiente manera:

1.- Un *endpoint* inicia una llamada.

2.- El UAC de origen envía una invitación (INVITACIÓN) al UAS del destinatario.

3.- El UAS del receptor responde al mensaje *INVITE* usando el mensaje 100

Trying.

4.- El *Gateway* de terminación envía la señal de llamada a teléfono del destinatario.

5.- El destinatario UAS informa al UAC sobre la señal de llamada con el mensaje de timbre.

6.- El *Gateway* de origen envía el tono de devolución de llamada al teléfono que llama.

7.- El teléfono llamado es descolgado.

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

9.- El UAC originario emite un acuse de recibo (ACK) al UAS.

10.- En este punto, la UAC y UAS tienen toda la información que se requiere para establecer sesiones RTP entre ellos.

11.- Uno de los participantes finaliza la llamada. Su UA envía el mensaje BYE a la otra UA.

12.- El mensaje *BYE* se confirma con el mensaje 200 *OK*.

a) Establecimiento de llamada (*call setup*) SIP usando un Servidor *Proxy*

El procedimiento de Servidor *Proxy*, como esquematizado en la figura 2.34, es transparente a una UAC. El Servidor *Proxy* intercepta y reenvía una invitación a la UAS destino en nombre de su autor.

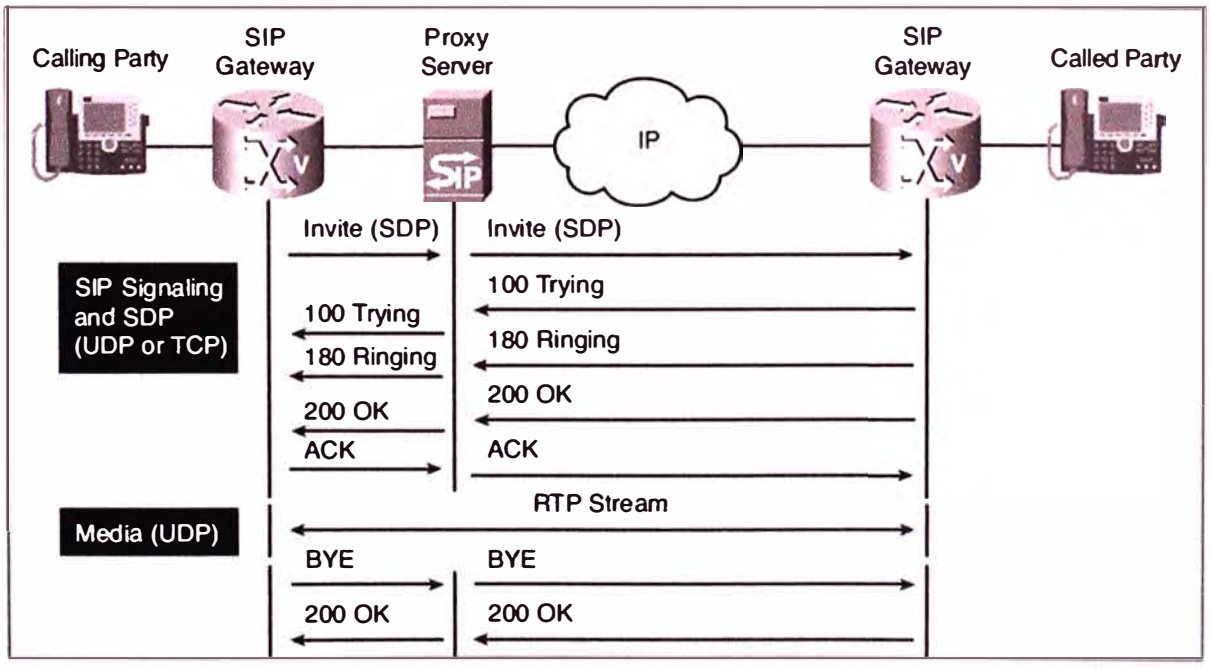


Figura 2.34 SIP Call Setup usando un Servidor Proxy

Fuente: "CVoice 642-437" (Wallace, 2011, pág. 211)

Un servidor *Proxy* responde a los problemas del método directo al centralizar el control y la gestión del establecimiento de llamada y proporciona un mayor dinamismo y hasta la capacidad de resolución de direcciones El beneficio para el UAC es que no necesita aprender las coordenadas de los UAS destino, sin embargo, todavía se puede comunicar con la UAS destino. Las desventajas de este método incluyen un aumento en la señalización y la dependencia en el servidor *Proxy*. Si el servidor *Proxy* falla, el UAC es incapaz de establecer sus propias sesiones.

Aunque el servidor *Proxy* actúa en nombre de una UA para el establecimiento de llamada, los UAs establecen sesiones RTP directamente entre sí.

b) Establecimiento de llamada (*call setup*) SIP usando un Servidor *Redirect*

Un servidor de redirección está programado para descubrir una ruta al destino. En lugar de enviar el *INVITE* al destino, el servidor de redireccionamiento informa a un UA con el destino, coordina que el UA debe intentar la próxima. El funcionamiento de un servidor de redirección SIP se representa en la figura 2.35.

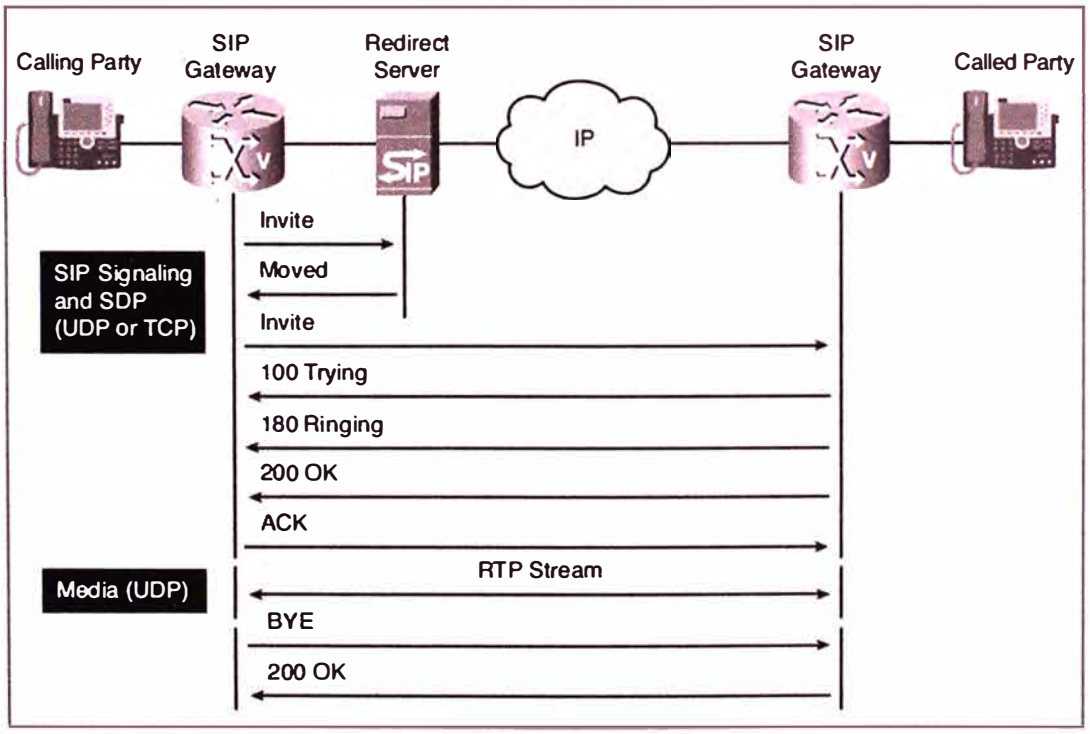


Figura 2.35 SIP Call Setup usando un Servidor de Redireccionamiento

Fuente: "CVoice 642-437" (Wallace, 2011, pág. 211)

Un servidor de redirección implementa muchas de las características del servidor *Proxy*. En el escenario de servidor de redirección, los mensajes se intercambian menos que

en el caso del servidor *Proxy*. El UAC tiene una mayor carga de trabajo, ya que debe iniciar la invitación posterior.

Cuando se utiliza un servidor de redirección, el procedimiento de establecimiento de llamada se inicia cuando el originario UAC envía un INVITE al servidor de redirección. El servidor de redireccionamiento, si es necesario, consulte al servidor de ubicación para determinar la ruta del destinatario (*location Server*) y su dirección IP. El servidor de redireccionamiento devuelve una respuesta "movido" al originario UAC con la dirección IP obtenida del servidor de ubicación. El UAC originario reconoce la redirección y continúa como se describe en el procedimiento de establecimiento de llamada directa (*direct call setup*).

2.6 Central de Telefonía IP

Una central telefónica IP hoy en día es un sistema telefónico diseñado para ofrecer servicios de comunicación a través de las redes de datos. A esta aplicación se le conoce como voz por IP (VoIP), donde la dirección IP (*Internet Protocol*) es la identificación de los dispositivos dentro de la Web. Con los componentes adecuados se puede manejar un número finito de anexos en sitio o remotos vía internet, añadir video, conectarle troncales digitales o servicios de VoIP (*SIP Trunking*) para llamadas internacionales a bajo costo. Los aparatos telefónicos que se usan les llaman teléfonos IP o SIP y se conectan a la red. Además por medio de puertos de enlaces se le conectan las líneas normales de las redes telefónicas públicas, y anexos analógicos para teléfonos estándar (fax, inalámbricos, contestadoras, etc.).

La centrales de telefonía IP proporcionan servicios consistentes a todos los empleados de una compañía, en sus lugares de trabajo, tanto si están en la oficina o conectados remotamente. La telefonía IP transmite comunicaciones de voz a través de la red mediante la utilización de los estándares del protocolo de internet. La telefonía IP de son parte integral de la solución de Centrales Telefónicas de múltiples vendedores; unifican voz, vídeo, datos, y aplicaciones móviles en redes tanto fijas como móviles, capacitando a los usuarios para comunicarse fácilmente en su lugar de trabajo a través de cualquier medio, dispositivo o sistema operativo.

Utilizando la red como plataforma, la telefonía IP de Cisco ayuda a organizaciones de todos los tamaños a conseguir mayor seguridad, resistencia, flexibilidad y escalabilidad, además de los beneficios inherentes de usar una red convergente para el transporte de datos y la interconexión.

Una central de telefonía IP puede ser catalogado como un H.323 *Gatekeeper* o un SIP *Proxy*, esto debido a que pueden soportar los protocolos H.323 y/o SIP. Los terminales o *endpoints* que pueden estar registrados a las centrales telefónicas también soportan protocolos de VoIP tales como SIP y H.323. Estos *endpoints* o terminales no solos son teléfonos IP, también pueden ser terminales de videoconferencia IP, Clientes de Software para PC, teléfonos IP inalámbricos, etc.

Existe una gran variedad de marcas en el mercado que ofrecen sistemas de telefonía IP o centrales de telefonía IP. Gartner Inc, empresa consultora y de investigación de las tecnologías de la información con sede en Stamford, Connecticut, Estados Unidos. Elabora encuestas de calidad e innovación tecnológica, el tema de la Comunicaciones Unificadas y sistemas de telefonía IP se evalúo a grandes marcas como: *Cisco Systems*, Avaya, Microsoft, Huawei, Mitel, entre otros. El siguiente diagrama "Cuadro Mágico" de Gartner muestra la posición de las marcas:

Figura 2.36 Cuadrante Mágico de Gartner para los Sistemas de Telefonía

(Fuente: Gartner 2014)

El Cuadrante Mágico de Gartner mostrado en la figura 2.36 muestra la tecnología corporativa de los vendedores y el diseño, la fabricación y distribución de soluciones de telefonía corporativa en *Datacenters* de 1.000 o más usuarios. Las soluciones de telefonía pueden ser plataformas centralizados o distribuidos, dedicados para su uso por una sola empresa, ya sea aprovisionado como soluciones independientes o como parte de una suite

de comunicaciones unificadas (UC).

"Con su red de distribución global y carteras completas de productos, Cisco es un fuerte competidor en la infraestructura de las comunicaciones de voz empresarial. Las empresas deben considerar Cisco si se inclinan hacia el uso de un único proveedor de soluciones de extremo a extremo, que incluyen equipos de red, servidores, vídeo y requisitos de colaboración". (Fuente: *Gartner* 2014)

2.7 Protocolos y características de redes

En esta sección se desarrollan los siguientes tópicos: LAN virtual (VLAN), troncales, protocolo de control de agregación de enlaces, protocolo para redundancia de capa 3, contextos, *Failover*, y protocolo de redundancia para balanceador de carga.

2.7.1 Redes de Área Local Virtuales (VLAN)

Es una agrupación lógica de ordenadores y dispositivos de red. Las VLAN se agrupan por función o por ubicación física, sin importar la ubicación real de los usuarios finales.

El flujo de datos entre las VLAN está restringido. Los *Switches* envían tráfico de datos *unicast*, multicast y *broadcast* (a un solo punto, a un grupo determinado, y a todos, respectivamente) sólo en segmentos de red que pertenezcan a la misma VLAN a la que pertenece el tráfico de datos. En otras palabras, los dispositivos que pertenecen a una VLAN sólo se comunican con los dispositivos que pertenecen a la misma VLAN.

Las VLAN mejoran el rendimiento de la red agrupando a los dispositivos y recursos de forma lógica. Las empresas a menudo usan las VLAN como una forma de garantizar que un conjunto de dispositivos se agrupen lógicamente más allá de su ubicación física. Las VLAN permiten a los usuarios finales compartir la misma ubicación física, pero pertenecer a redes diferentes, a pesar de estar usando los mismos dispositivos de red mostrados en la figura 2.37.

Por ejemplo, los usuarios del departamento de Administración se ubican en la VLAN de Administración, mientras que los usuarios del Departamento de Logística se ubican en la VLAN de Logística, a pesar de que sus miembros se encuentren en pisos y hasta edificios distintos. Las VLAN pueden mejorar la escalabilidad, seguridad y gestión de red.

2.7.2 Troncales

Una troncal es una conexión física que transporta enlaces lógicos. En el contexto

LAN, un enlace troncal es un enlace punto a punto entre dos *Switches* que soporta y transporta varias VLAN. El propósito de un enlace troncal es ahorrar puertos al crear un enlace entre dos *Switches* que implementan VLAN.

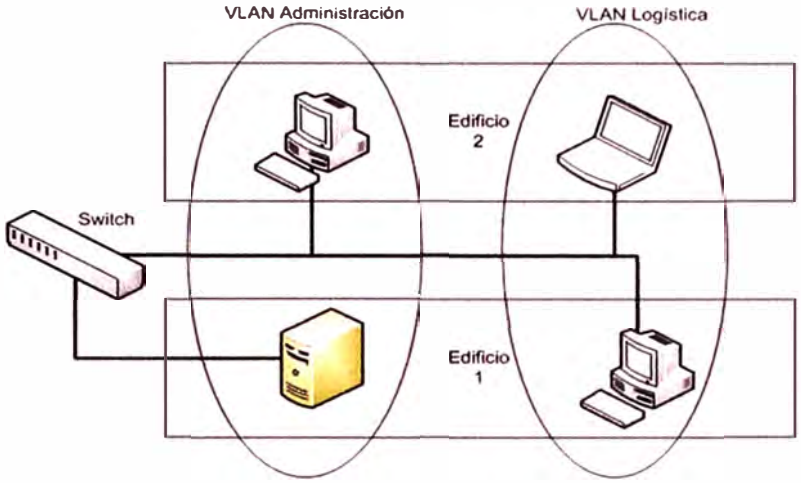


Figura 2.37 Ejemplo de VLAN

(Fuente Ref. Elaboración propia)

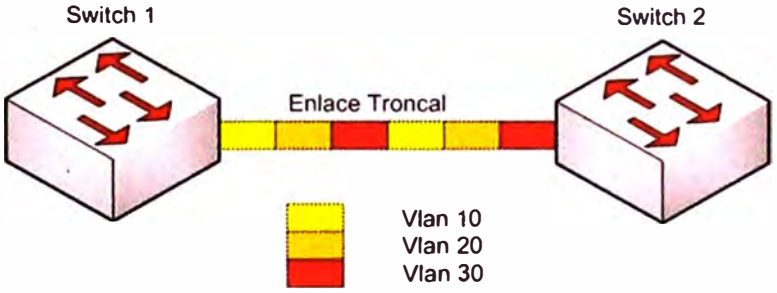


Figura 2.38 Enlace Troncal

(Fuente Ref. Elaboración propia)

2.7.3 Protocolo de agregación de enlaces (LACP)

Siglas de *Link Aggregation Control Protocol*, definido por el IEEE 802.3ad. Ofrece un método de agregación de múltiples enlaces Ethernet en un simple canal lógico, mostrado en la figura 2.39. Esta propiedad ayuda a mejorar el costo efectivo de los dispositivos, incrementando el ancho de banda acumulativo sin requerir una actualización de dispositivos. En adición, IEEE 802.3ad ofrece una capacidad de provisión dinámica, administración y monitoreo de varios enlaces de agregación y habilita la interoperabilidad entre dispositivos de diferentes marcas.

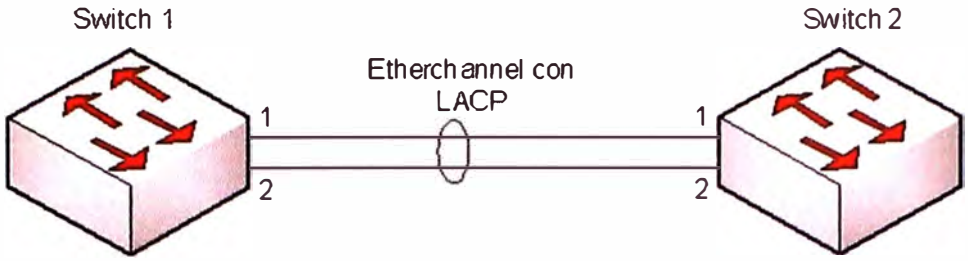


Figura 2.39 Enlace Etherchannel con LACP

(Fuente Ref. Elaboración propia)

El *Gigabit Etherchannel* es una tecnología Ethernet de alto desempeño (Cisco) que ofrece tasas de transmisión en *Gigabit* por segundo. Una agrupación *Gigabit Etherchannel* es un enlace lógico que ofrece ancho de banda agregado que llega hasta 8 enlaces físicos. Todos los puertos en cada *Etherchannel* deben tener la misma velocidad y deberán ser configurados como puertos Ethernet capa 2 o puertos capa 3.

Cuando un enlace perteneciente al *Etherchannel* falla, el tráfico previamente llevado sobre el enlace que presentó falla es redistribuido en el *Etherchannel*, también cuando ocurre una falla, se envía un mensaje que identifica el dispositivo *Etherchannel* y el enlace que falló.

El protocolo LACP soporta creación automática de *Etherchannel* intercambiando paquetes LACP entre los puertos LAN. Los paquetes LACP son intercambiados solamente entre puertos en modo pasivo y activo. El protocolo aprende la capacidad de agrupar dinámicamente puertos LAN e informar a los otros puertos LAN, después LACP identifica correctamente los enlaces Ethernet de cada extremo.

Ambos modos, pasivo y activo, permiten a LACP negociar entre puertos LAN y determinar si pueden formar un *Etherchannel*, basado en el criterio de velocidad de puertos y estado *Trunk* (troncal).

Los puertos LAN pueden formar un *Etherchannel* cuando son compatibles con el modo LACP, según los siguientes ejemplos:

- Un puerto LAN en modo activo puede formar un *Etherchannel* con otro puerto LAN en modo activo.
- Un puerto LAN en modo activo puede formar un *Etherchannel* con otro puerto LAN en modo pasivo.
- Un puerto LAN en modo pasivo no puede formar un *Etherchannel* con otro puerto LAN que es también en modo pasivo porque ninguno inicia negociación.

- La IEEE 802.3ad ofrece los siguientes beneficios:
- Incremento de la capacidad de la red sin cambiar físicamente las conexiones o actualizando los dispositivos de red.
- Ahorro de costos, resulta del uso de dispositivos existentes y funcionalidades adicionales de software.
- Es una solución estándar que habilita la interoperabilidad de los dispositivos de red.
- Puertos de redundancia sin intervención de usuarios cuando los puertos fallan.

2.7.4 Metodología para modificar direcciones de red (NAT)

Internet en sus inicios no fue pensado para ser una red tan extensa, por ese motivo se reservaron "sólo" 32 bits para direcciones, el equivalente a 4.294.967.296 direcciones únicas, pero el hecho es que el número de máquinas conectadas a Internet aumentó exponencialmente y las direcciones IP se agotaban. Por ello surgió la NAT o *Network Address Translation* (en castellano, Traducción de Direcciones de Red)

La idea es sencilla, hacer que redes de ordenadores utilicen un rango de direcciones especiales (IPs privadas) y se conecten a Internet usando una única dirección IP (IP pública). Gracias a este "parche", las grandes empresas sólo utilizarían una dirección IP y no tantas como máquinas hubiese en dicha empresa. También se utiliza para conectar redes domésticas a Internet.

NAT, que se define en RFC 3022, tiene muchos usos. Su uso es clave para conservar las direcciones IP permitiendo que las redes utilicen direcciones IP privadas. NAT traduce las direcciones no enrutables, privadas, internas en direcciones enrutables públicas. NAT es también un *Firewall* natural. Oculta las direcciones IP internas de redes externas.

Un dispositivo NAT habilitado normalmente opera en la frontera de una red de conexión. En la figura 2.39 es el *Router* de borde.

En la terminología de NAT, la red interior es el conjunto de redes que están sujetas a la traducción (todas las redes en la región sombreada en la figura 2.40). La red exterior se refiere a todas las demás direcciones.

En la figura 2.41 se muestra cómo hacer referencia a las direcciones al configurar NAT en un *Router* Cisco.

- *Inside local address*: Lo más probable es una dirección privada. En la figura, la dirección IP 192.168.10.10 asignado a PC1 es una dirección local interna.
- *Inside global address*: Una dirección pública válida que al host interior se le es

otorgado cuando sale del *Router* NAT. Cuando el tráfico de PC1 está destinado para el servidor web en 209.165.201.1, R2 debe traducir la dirección local interna a una dirección global interna, que es 209.165.200.226 en este caso.

- *Outside global address:* Una dirección IP accesible asignado a un host en Internet. Por ejemplo, el servidor web puede ser alcanzado en la dirección IP 209.165.201.1.
- *Outside local address:* La dirección IP local asignado a un host en la red exterior. En la mayoría de situaciones, esta dirección es idéntica al *outside global address* fuera de ese dispositivo exterior.

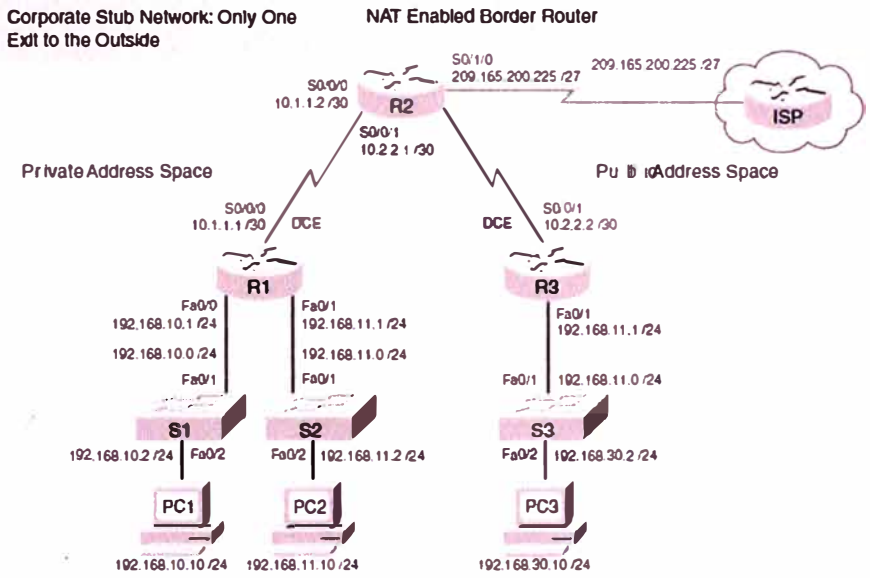


Figura 2.40 Topología NAT

(Fuente Ref. 31 Days Before Your CCNA Exam, Johnson, 2009, pág. 298)

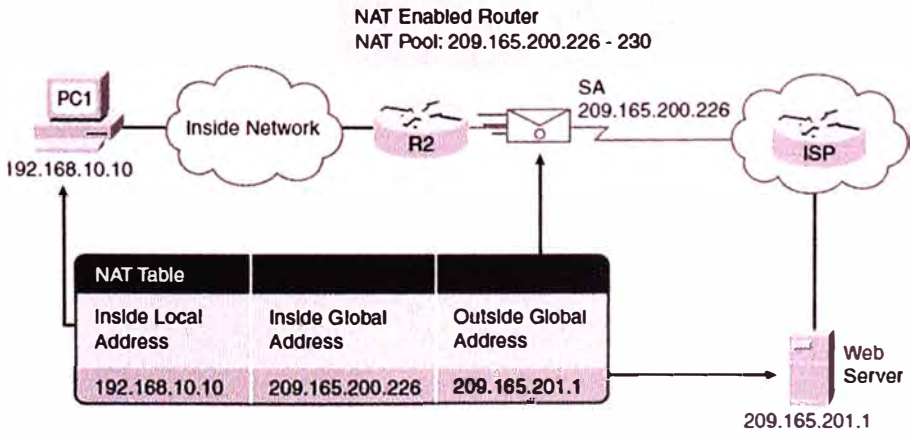


Figura 2.41 Terminología NAT

(Fuente Ref. 31 Days Before Your CCNA Exam, Johnson, 2009, pág. 298)

Los siguientes pasos muestran el proceso NAT cuando PC1 envía tráfico a Internet:

1.- PC1 envía un paquete destinado a la Internet para R1, el default *Gateway.*

2.- R1 envía el paquete a R2, según las indicaciones de su tabla de enrutamiento.

3.- R2 hace referencia a su tabla de enrutamiento e identifica al siguiente salto como el *Router* ISP. La acción siguiente es comprobar si el paquete coincide con los criterios especificados para la traducción. R2 tiene una ACL que identifica la red en el interior como un host válido para la traducción. Por lo tanto, se traduce una dirección IP local en el interior a una dirección IP global en el interior, que en este caso es 209.165.200.226. Almacena este mapeo de lo local a global de direcciones en la tabla NAT.

4.- R2 modifica el paquete con la nueva dirección IP de origen (la dirección global interna) y la envía al *Router* ISP.

5.- El paquete finalmente llega a su destino, que luego envía su respuesta en la interior dirección global *(inside global address)* 209.165.200.226.

6.- Cuando las respuestas del destino llegan de vuelta en R2, se consulta la tabla de NAT para que coincida con la dirección global interna *(inside global address)* a la correcta dirección local interna *(inside local address).* R2 y luego modifica el paquete con la dirección local interna (192.168.10.10) y lo envía a R1.

7.- R1 recibe el paquete y lo reenvía al PC1.

2.7.5 Parámetros de Calidad de Servicio (QoS)

La supervisión de llamadas VoIP, también conocido como Supervisión de Calidad *(QM quality monitoring),* utiliza soluciones de hardware y software para probar, analizar y calificar la calidad general de las llamadas realizadas a través de una red de telefonía VoIP. La supervisión de llamadas es un componente esencial para el plan de Calidad de Servicio *(QoS)* de los negocios de telecomunicaciones. Hardware y software para supervisar llamadas utilizan diversos algoritmos matemáticos para medir la calidad de una llamada VoIP y generar una calificación.

La puntuación más común se llama la puntuación media de opinión (MOS: *mean opinión score).* El MOS se mide en una escala de uno a cinco, aunque es técnicamente 4,4 les a puntuación más alta posible en una red de VoIP. Un MOS de 3,5 o superior es considerado una "buena llamada". Para obtener los MOS, el hardware y software para la supervisión de llamadas analiza diversos parámetros de calidad de la llamada, los más comunes son:

- Latencia - Este es el tiempo de retardo entre dos extremos de una conversación

telefónica de VoIP. Puede medirse, ya sea de una manera o de ida y vuelta. La latencia de ida y vuelta contribuye al "efecto de sobre conversación" experimentado durante malas llamadas VoIP, donde la gente acaba hablando por encima de la otra persona porque piensan que esta ha dejado de hablar. Una latencia de ida y vuelta con más de 300 milisegundos, se considera pobre.

- Inquietud - Es la latencia provocada por los paquetes que llegan tarde o en el orden equivocado. La mayoría de las redes de VoIP intentan deshacerse de esta fluctuación, con algo llamado un *jitter buffer* que recoge los paquetes en pequeños grupos, los coloca en el orden correcto y los entrega al usuario final todos a la vez. En las llamadas VoIP se nota una fluctuación de 50 ms o mayor.
- Pérdida de paquetes - Parte del problema con el *jitter buffer* es que a veces se sobrecarga y los paquetes que llegan tarde se "caen" o se pierden. A veces los paquetes se pierden esporádicamente a lo largo de una conversación (pérdida al azar) y a veces frases completas se dejan caer (pérdida en ráfagas). La pérdida de paquetes se mide como un porcentaje de pérdida de paquetes a los paquetes recibidos.

Hay dos tipos de supervisión de llamadas: activo y pasivo. El activo (o subjetivo) la supervisión de llamadas ocurre antes de que la empresa despliega su red de VoIP. La supervisión activa es a menudo realizada por los fabricantes de equipos y por especialistas en redes que utilizan la red de VoIP de la empresa exclusivamente para pruebas. Las pruebas activas no pueden producirse una vez a la red VoIP ha sido desplegada y que los empleados ya están utilizando el sistema. La supervisión pasiva analiza las llamadas VoIP en tiempo real mientras están siendo realizadas por los usuarios. La supervisión pasiva de llamadas puede detectar problemas en el tráfico de la red, sobrecargas del buffer y otros problemas que los administradores de red pueden arreglar cuando la red está inactiva. Otro método para supervisar llamadas es la grabación de llamadas para su posterior análisis. Este tipo de análisis es limitado, sin embargo, a lo que se puede escuchar durante la llamada, no lo que sucede en la red. Este tipo de seguimiento se realiza habitualmente por los seres humanos, no computadoras, y se llama la garantía de calidad.

- **Retardo o *Delay* aceptable**

Sector de Normalización de Telecomunicaciones de la Unión Internacional de las Telecomunicaciones (ITUT) especifica el retardo de red para aplicaciones de voz en la Recomendación G.114. Esta recomendación define tres bandas de retraso de un solo

sentido, como se muestra en la Tabla 2.7.

Tabla 2.7 Delay o Retardo aceptable G.114

(Fuente Ref. ITU G114)

Rango en Milisegundos	**Descripción**
0 a 150	Aceptable para la mayoría de las aplicaciones de usuario
150 a 400	Aceptable, son conscientes del tiempo de transmisión y su impacto en la calidad de transmisión de aplicaciones de usuario.
Superior a 400	Inaceptable para fines de planificación de la red general. (Sin embargo, se reconoce que en algunos casos excepcionales, se supera este límite)

Tabla 2.8 Cálculo del Delay

(Fuente Ref. ITU G114)

Tipo de Delay	**Fijo (ms)**	**Variable (ms)**
Delay de Codificador	18	
Packetization delay	30	
Queuing y buffering		8
Serialization (64 kbps)	5	
Network delay (public frame)	40	25
Dejitter buffer	45	

Total	138	33

La recomendación G.114 se orienta a administraciones nacionales de telecomunicaciones y, por tanto, es más estricta que las recomendaciones que normalmente se aplican en las redes de voz privadas. Cuando la ubicación y las necesidades de negocios de usuarios finales son bien conocidas para un diseñador de red, más retardo puede ser aceptable.

La recomendación G.114 es para *delay* de una vía (*one way*) y no se toma en cuenta para el *round trip delay* (delay de ida y vuelta). Los ingenieros de diseño de red deben considerar tanto *delay* variables y fijos. *Delay* Variable incluye *queuing* y *network delays* (*delays* de encolamiento y de red) y *delay* fijos que incluyen *delay* de paquetización, serialización y *buffer.*

2.7.6 Conmutación de Etiquetas Multiprotocolo (MPLS)

El problema fundamental que presentaban las diferentes soluciones de conmutación IP era la falta de interoperabilidad entre los productos de diferentes fabricantes. Además de esto, la mayoría de estas soluciones usaban ATM (*Asynchronous Transfer Mode*) como transporte, pues no podían operar sobre infraestructuras de transmisión mixtas. Se quería obtener un estándar que pudiera funcionar sobre cualquier tecnología de transporte de datos en el nivel de enlace. De aquí el Grupo de Trabajo de MPLS que se estableció en el IETF en 1977 se propuso como objetivo la adopción de un estándar unificado e interoperativo.

Los objetivos establecidos por este grupo en la elaboración del estándar eran:

- MPLS debía funcionar sobre cualquier tecnología de transporte, no sólo ATM.
- MPLS debía soportar el envío de paquetes tanto bajo demanda unidifusión (unicast) como multidifusión (multicast).
- MPLS debía ser compatible con el Modelo de Servicios Integrados del IETF, incluyendo el protocolo RSVP *(Resource Reservation Protocol).*
- MPLS debía permitir el crecimiento constante de la Internet.
- MPLS debía ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP.

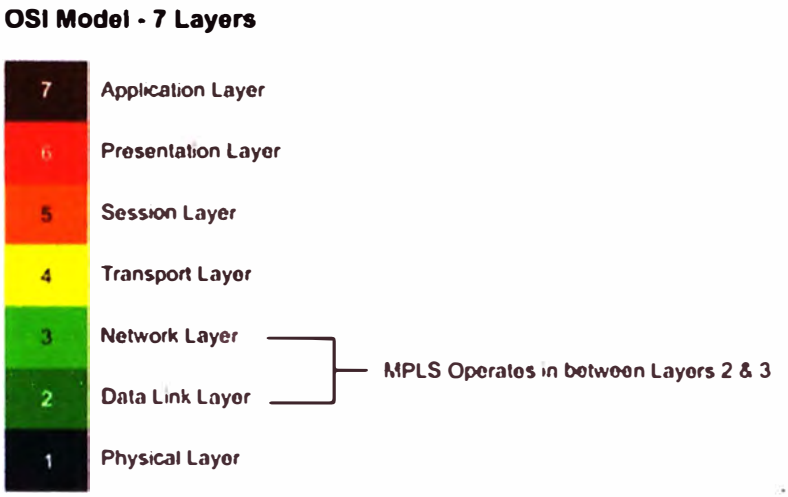


Figura 2.42 Modelo OSI con MPLS

(Fuente Ref. www.mplsinfo.org.)

MPLS se encuentra situado entre las capas de enlace de datos y de red del modelo OSI, como se muestra en la figura 2.42 se podría decir que es un protocolo de unión entre la capa de enlace y la capa de red. MPLS quiere decir Conmutación de Etiquetas Multiprotocolo (***Multiprotocol Label Switching***), es una tecnología relativamente nueva que se desarrolló para solucionar la mayoría de los problemas que existen en la técnica actual de reenvío de paquetes. La IETF cuenta con un grupo de trabajo MPLS que ha unido esfuerzos para estandarizar esta tecnología. Opera entre la capa de enlace de datos y la capa de red del modelo OSI, fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes, puede ser utilizado para transportar diferentes tipos de tráfico incluyendo tráfico de voz y de paquetes IP.

MPLS es un estándar emergente del IETF que surgió para consensuar diferentes soluciones de conmutación multinivel propuesto por diferentes fabricantes a mitad de los años noventa. Como concepto, MPLS es a veces un tanto difícil de explicar, como protocolo es bastante sencillo, pero las implicaciones que supone su implementación real son enormemente complejas. Según el énfasis (o interés) que se tenga a la hora de explicar sus características y utilidad, MPLS se puede presentar como un sustituto de la conocida arquitectura IP sobre ATM, también como un protocolo para hacer túneles (sustituyendo a las técnicas habituales de "*tunneling*"), o bien, como una técnica para acelerar el encaminamiento de paquetes. En realidad MPLS realiza un poco de todo ya que integra sin discontinuidades los niveles 2 (conmutación) y 3 (red) combinando eficazmente las funciones de control del *Routing* con la simplicidad y rapidez de la conmutación de Nivel 2.

MPLS ofrece nuevas posibilidades en la gestión de *Backbones*, así como en la provisión de nuevos servicios de valor agregado. Para entender mejor las ventajas de la solución MPLS vale la pena revisar los esfuerzos de Integración de los niveles 2 y 3 que han llevado finalmente a la adopción del estándar MPLS.

El objetivo primario de MPLS, es estandarizar una tecnología base que integre el intercambio de etiquetas durante el reenvío de paquetes con el sistema de enrutamiento actual de redes.

a) Componentes MPLS

- LSRs (*Label Switch*ing *Router*): Es un enrutador de alta velocidad especializado en el envío de paquetes etiquetados por MPLS. Participa en el establecimiento de las rutas (LSPs). Es capaz de enviar paquetes de capa 3 nativos. Los LSR, pueden ser internos o extremos, los primeros añaden o eliminan etiquetas, mientras que los segundos sustituyen unas etiquetas por otras.
- Etiqueta: es un identificador corto (de longitud fija) y con significado local, empleado para identificar un FEC. Un paquete puede tener una o más etiquetas apiladas (jerarquía). Cuando un paquete atraviesa dominios interiores a otros dominios, es cuando se produce el apilamiento de etiquetas. El LSR al recibir un paquete siempre consultará la etiqueta de nivel superior.
- FEC (Forwarding *Equivalence Class*): Agrupación de paquetes que comparten los mismos atributos (dirección destino, VPN) y/o requieren el mismo servicio (multicast, QoS). Se asigna en el momento en que el paquete entra a la red. Todos los paquetes que forman parte de la clase, siguen un mismo LSP.
- LSP (*Label Switched Path*): Es una ruta a través de uno o más LSRs en un nivel de jerarquía que sigue un paquete de un FEC en particular. Este camino puede establecerse tanto mediante protocolos de enrutamiento como manualmente.

b) Funcionamiento

El funcionamiento del protocolo MPLS debe seguir los siguientes pasos:

1) Creación y distribución de etiquetas
2) Creación de tablas en cada enrutador
3) Creación de LSPs
4) Agregar etiquetas a los paquetes con la información de la tabla.
5) Envío del paquete

Se estudiará el funcionamiento de MPLS separándolo en dos componentes:

- Envío de Paquetes
- Control de la Información

Finalmente se muestra un esquema general del funcionamiento de una red con el protocolo MPLS.

➢ Envío de Paquetes

La base del MPLS está en la asignación e intercambio de etiquetas, que permiten el establecimiento de los caminos LSP por la red. Los LSPs son unidireccionales (simplex) por naturaleza; el tráfico bidireccional (dúplex) requiere dos LSPs, uno en cada sentido. Cada LSP se crea a base de concatenar uno o más saltos (hops) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un conmutador de etiquetas (LSR) a otro, a través del dominio MPLS.

El envío se implementa mediante el intercambio de etiquetas en los LSPs. Sin embargo, MPLS no utiliza ninguno de los protocolos de señalización ni de enrutamiento definidos por el ATM Forum; en lugar de ello, se utiliza el protocolo RSVP o bien un nuevo estándar de señalización LDP (*Label Distribution Protocol).*

Pero, de acuerdo con los requisitos del IETF, el transporte de datos puede ser cualquiera. Por ejemplo, si éste fuera ATM, una red IP habilitada para MPLS es ahora mucho más sencilla de gestionar que la solución clásica IP/ATM. No es necesario administrar dos arquitecturas diferentes, lo que se haría transformando las direcciones y las tablas de enrutamiento IP en las direcciones y el enrutamiento ATM. Este problema lo resuelve el procedimiento de intercambio de etiquetas MPLS.

Un camino LSP es el circuito virtual que siguen por la red todos los paquetes asignados a la misma FEC. Al primer LSR que interviene en un LSP se le denomina de entrada o de cabecera y al último se le denomina de salida o de cola. Los dos están en el exterior del dominio MPLS. El resto, entre ambos, son LSRs interiores del dominio MPLS. Un LSR es como un enrutador que funciona a base de intercambiar etiquetas según una tabla de envío. Esta tabla se construye a partir de la información de enrutamiento que proporciona la componente de control, según se verá más adelante.

Cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondientes a cada interfaz de entrada/salida correspondientemente, que se utilizan para acompañar a cada paquete que llega por ese interfaz y con la misma etiqueta (en los LSR exteriores sólo hay una etiqueta, de salida en el de cabecera y de entrada en el de cola), en la figura 2.43 se ilustra un ejemplo del funcionamiento de un LSR del núcleo

MPLS.

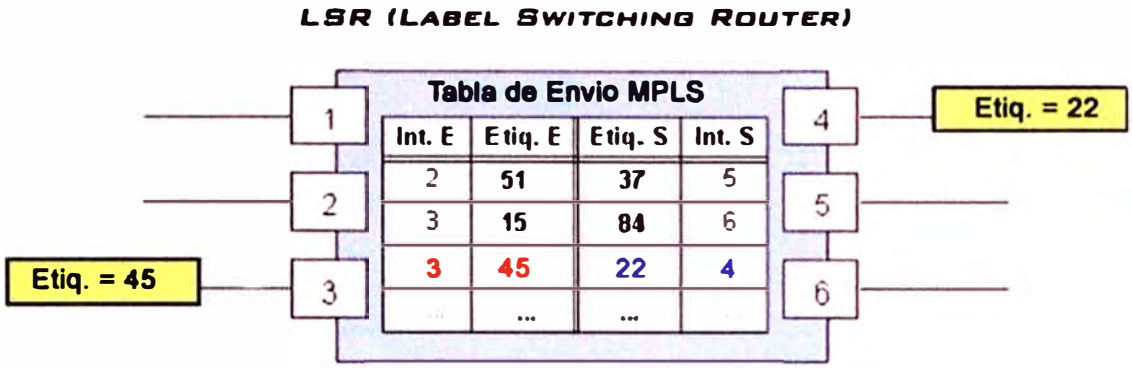


Figura 2.43 Funcionamiento de un LSR

(Fuente Ref. www.mplsinfo.org.)

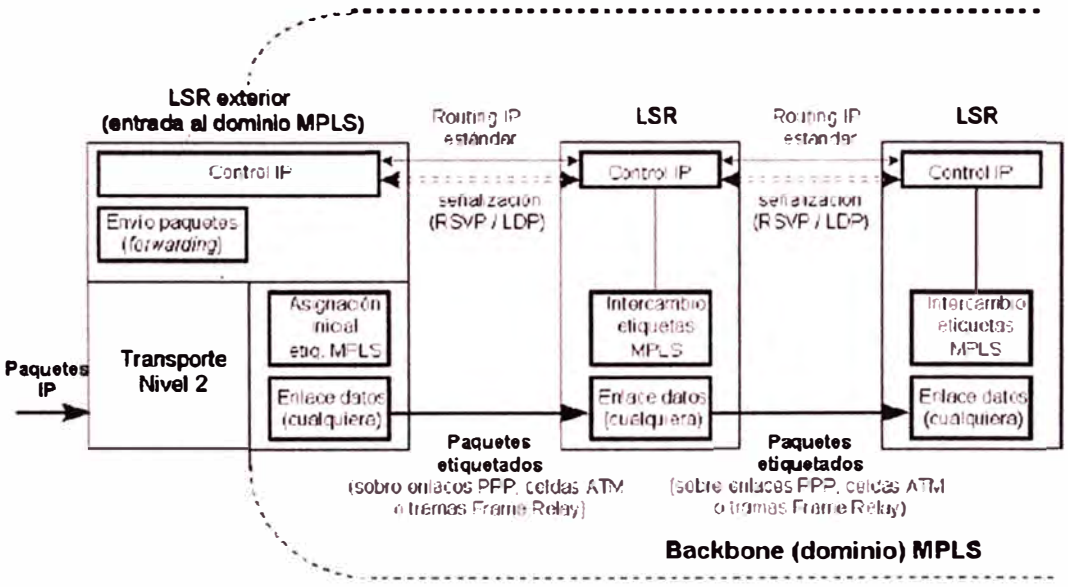


Figura 2.44 Algoritmo de intercambio de etiquetas

(Fuente Ref. www.mplsinfo.org.)

El algoritmo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para poder hacer la asignación por el LSR de cabecera. En la figura 2.44 el LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 212.95.193.1. El LSR consulta la tabla de encaminamiento y asigna el paquete a la clase FEC definida por el grupo 212.95/16. Así mismo, este LSR le asigna una etiqueta

(con valor 5 en el ejemplo) y envía el paquete al siguiente LSR del LSP.

Dentro del dominio MPLS los LSR ignoran la cabecera IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente (tabla de conmutación de etiquetas) y la reemplazan por otra nueva, de acuerdo con el algoritmo de intercambio de etiquetas. Al llegar un paquete al LSR de cola (salida), este determina que el siguiente salto va fuera de la red MPLS, por lo que al consultar la tabla de conmutación de etiquetas, remueve la etiqueta y envía dicho paquete por enrutamiento convencional. Como se ve, la identidad del paquete IP original queda enmascarada durante el transporte por la red MPLS.

Las etiquetas se insertan en cabeceras MPLS, entre los niveles 2 y 3. Según las especificaciones del IETF, MPLS debía funcionar sobre cualquier tipo de transporte: PPP, LAN, ATM, *Frame Relay*, etc. Por ello, si el protocolo de transporte de datos contiene ya un campo para etiquetas (ATM, *Frame Relay*, etc.), se pueden utilizan esos campos nativos para las etiquetas. Sin embargo, si la tecnología de nivel 2 empleada no soporta un campo para etiquetas (i.e. enlaces PPP o LAN), entonces se emplea una cabecera genérica MPLS de 4 octetos, que contiene un campo específico para la etiqueta y que se inserta entre la cabecera del nivel 2 y la del nivel 3.

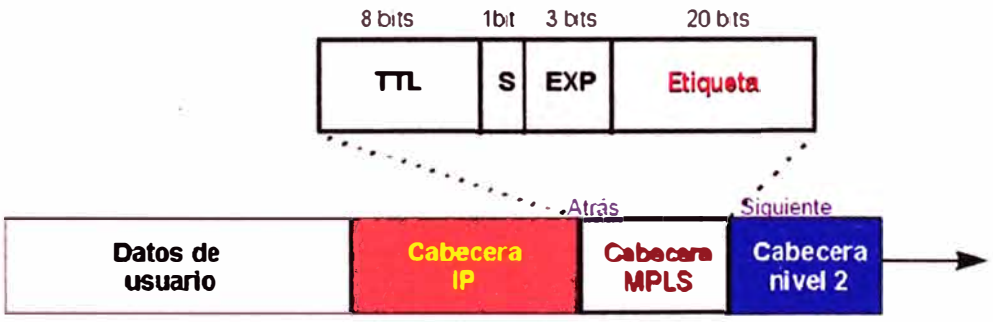


Figura 2.45 Algoritmo de intercambio de etiquetas

(Fuente Ref. www.mplsinfo.org.)

En la figura 2.45 se representa el esquema de los campos de la cabecera genérica MPLS y su relación con las cabeceras de los otros niveles. Los 32 bits de la cabecera MPLS se reparten en:

- 20 bits para la etiqueta MPLS.
- bits para identificar la clase de servicio en el campo EXP (experimental, anteriormente llamado *CoS*).
- 1 bit de pila (*stack*) para poder apilar etiquetas de forma jerárquica.
- 8 bits para indicar el TTL (*time-to-live*) que sustenta la funcionalidad estándar TTL

de las redes IP.

- **Control de Información**

Hasta ahora se ha visto el mecanismo básico de envío de paquetes en MPLS. Pero queda por ver dos aspectos fundamentales:

Cómo se generan las tablas de envío que establecen los LSPs.

Cómo se distribuye la información sobre las etiquetas a los LSRs.

Las tablas de envío se generan con la información que se tiene sobre la red, tales como topología, patrón de tráfico y características de los enlaces, entre otros. Esta información es la que manejan los protocolos internos IGP (OSPF, IS-IS, RIP) para construir sus tablas de enrutamiento. MPLS utiliza esta información de estos protocolos para establecer los caminos virtuales o LSPs.

Para cada "ruta IP" en la red se crea un camino de etiquetas, concatenando las de entrada/salida en cada tabla de los LSRs; el protocolo interno correspondiente se encarga de pasar la información necesaria.

El segundo aspecto se refiere a la información de "señalización", necesaria siempre que se quiera establecer un circuito virtual. Sin embargo, la arquitectura MPLS no asume un único protocolo de distribución de etiquetas. De hecho, se están estandarizando diferentes protocolos para tal fin. Entre los protocolos existentes que se extienden para soportar MPLS, se encuentra el protocolo RSVP y BGP en las formas conocidas como MPLS-BGP, MPLS-RSVP-TUNNELS. También se están definiendo nuevos protocolos específicos para la distribución de etiquetas, como lo es el LDP (*Label Distribution Protocol*) y CR_LPD (*Constraint Based Routing Label Protocol*). RSVP es preferido por IETF, LDP por Cisco y el CR_LPD por Nokia.

Las diferentes variaciones en el intercambio de etiquetas son:

- LDP: mapea los destinos IP (*unicast*) en etiquetas.
- RSVP, CR LDP: es usado para ingeniería de tráfico y reserva de recursos.
- BGP: para etiquetas externas (VPN).

- **Esquema General**

En la figura 2.45 se muestra el esquema global de funcionamiento de MPLS, donde quedan reflejadas las diversas funciones en cada uno de los elementos que integran la red MPLS. El núcleo MPLS proporciona una arquitectura de transporte que hace aparecer a cada par de enrutadores a una distancia de un sólo salto.

Esta unión a un solo salto se realiza por MPLS mediante los correspondientes LSPs (puede haber más de uno para cada par de enrutadores). La diferencia con topologías conectivas reales es que en MPLS la construcción de caminos virtuales es mucho más flexible y no se pierde la visibilidad sobre los paquetes IP. Esto abre enormes posibilidades a la hora de mejorar el rendimiento de las redes y de soportar nuevas aplicaciones de usuario.

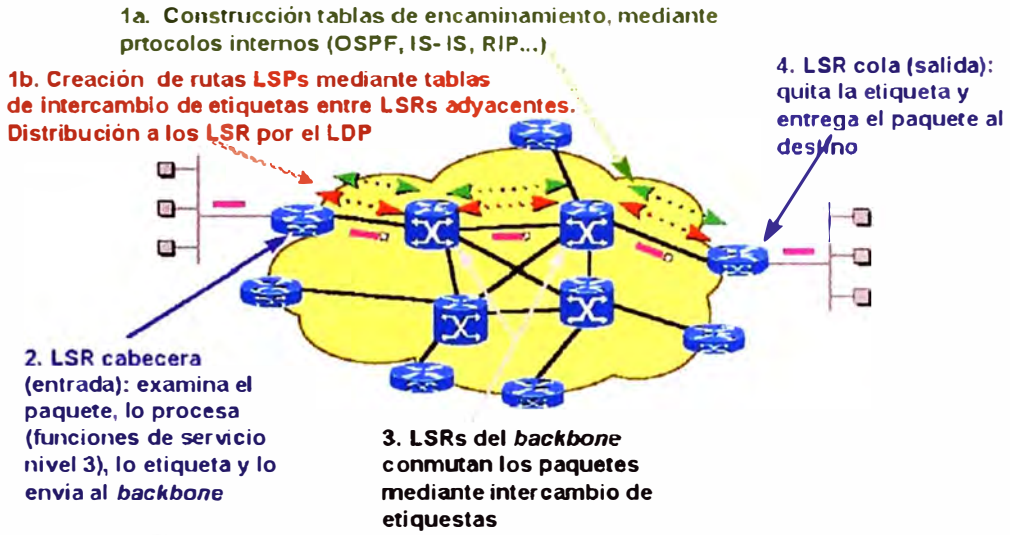


Figura 2.46 Esquema global de funcionamiento de MPLS

(Fuente Ref. www.mplsinfo.org.)

2.8 Seguridad informática

Para la comprensión de la seguridad informática, la cual también es incluida en la solución desarrollada en este informe, esta sección se divide en los siguientes ítems: Generalidades, tipos de ataque, principales metas de seguridad de red, *Firewall* (corta fuego), administración de usuarios (AAA), inspección de protocolos de aplicación y finalmente listas de acceso (ACL).

2.8.1 Generalidades

A medida que las redes crecen y se interconectan con otras redes, incluido Internet, estas redes son expuestas a un gran número de riesgos de seguridad informática. No solamente el número de potenciales atacantes ha crecido a lo largo de toda la red, sino que además las herramientas disponibles de estos potenciales atacantes se vuelven más sofisticadas.

Una red siempre es un blanco. Nuevas vulnerabilidades y nuevos métodos de ataques son descubiertas, un usuario que no posea herramientas relativamente sofisticadas

puede enviar un ataque contra una red no protegida. Los ataques de red involucran sofisticados y habilidosos métodos que evaden la detección; los ataques se vuelven cada vez más específicos y tienen mayores consecuencias financieras para sus víctimas.

2.8.2 Tipos de ataque

Al conectarse a una red externa como Internet, se introduce la posibilidad que atacantes externos aprovechen las debilidades de la red, tal vez robando información o impactando el desempeño de la red, por ejemplo, introduciendo virus; sin embargo, aun si la red estuviera desconectada de la red externa, las amenazas de seguridad seguirán existiendo.

Específicamente, acorde al *Computer Security Institute (CSI)* en San Francisco, California, aproximadamente 60 al 80% de los incidentes de red son originados desde la misma red, por consiguiente, aunque el aislamiento de la red no es factible para negocios que tienen ambientes informáticos (negocios electrónicos), incluso el aislamiento físico de la red no garantiza la seguridad de la red.

Basados en estos factores, los administradores de red deben considerar ambas amenazas: internas y externas.

a) Amenazas internas

Las amenazas internas son originadas dentro de la red, estas amenazas tienden a ser más serias que las amenazas externas. Algunas razones de la severidad de amenazas internas son:

- Los usuarios internos ya conocen la red y sus recursos disponibles.
- Los usuarios internos típicamente tienen algunos niveles de acceso por la naturaleza de su trabajo.
- Los mecanismos de seguridad de red, tales como sistemas de prevención de intruso (IPS) y *Firewall* (corta fuegos), no son efectivos contra muchos problemas de red originados internamente.

b) Amenazas Externas

Los atacantes externos probablemente no tengan conocimiento de la red, y esto es lógico porque no tienen las credenciales de acceso, sus ataques tienden a ser de naturaleza técnica.

Por ejemplo, un atacante podría realizar un barrido de comando ping en una red e identificar la dirección IP que responde a la serie de pings. Entonces, las direcciones IP podrían ser sujetas a una revisión de puertos TCP/IP de los servicios que estén abiertos de

los dispositivos descubiertos.

Si el atacante gana control del dispositivo, él podría usar ese punto como un trampolín para atacar toda la red. Afortunadamente, los administradores de red pueden mitigar muchas amenazas expuestas a atacantes externos.

2.8.3 Las tres principales metas de seguridad de red

La mayor parte de los días de una red corporativa, son en su mayoría referidas a los requerimientos y demandas del comercio electrónico y contacto con el cliente; estas dos requieren de conectividad interna entre la red externa (Internet) y red interna, desde el punto de vista de seguridad, hay dos supuestos básicos en las redes empresariales modernas, las cuales son:

- Las redes corporativas de hoy en día son grandes, se interconectan con otras redes, y corren protocolos propietarios.
- Los dispositivos y aplicaciones se conectan y usan en redes corporativas que continuamente incrementan en complejidad.
- La mayoría (si no son todas) de las redes corporativas requieren seguridad de red, se considera como las tres metas principales de la seguridad de red: la confidencialidad, la integridad y la disponibilidad. La descripción de cada una es:

a) Confidencialidad

La confidencialidad de la información implica mantener la privacidad de la información. Esta privacidad podría ser fisicamente o lógicamente de acceso restringido a la información sensible o a la encriptación de tráfico de red. Una red que ofrece confidencialidad podría hacer lo siguiente:

- 4 encriptado, de manera que el atacante no pueda descifrar cualquier tráfico que capture desde la red.

b) Integridad

La integridad de la información asegura que los datos no han sido modificados en tránsito. También se considera una solución de integridad de información la autenticación que verifica que el tráfico originado desde el origen es el enviado. Ejemplo que incluye violación de la integridad es lo siguiente:

- Modificar la página web corporativa.
- Interceptar y alterar las transacciones de comercio electrónico.
- Modificar los estados financieros que son almacenados electrónicamente.

c) Disponibilidad

La disponibilidad de la información es una medida de la accesibilidad de la data, por ejemplo, si un servidor estuviera inactivo solamente 5 minutos por año, podría tener una disponibilidad de 99.999%. Un par de ejemplos de cómo un atacante podría intentar comprometer la disponibilidad de la red:

- El envío información de formato inadecuando a los dispositivos de red, resultando un error de excepción no manejable por el dispositivo de red.
- Ataque que consista en inundar la red con una cantidad excesiva de tráfico o requerimientos. Esto consumiría procesamiento de los recursos del sistema y podría responder previniendo con varios requerimientos verdaderos. Este tipo de ataque es llamado denegación de servicio (*DoS*).

2.8.4 *Firewall* (corta fuego)

Es un dispositivo o conjunto de dispositivos diseñados para permitir o denegar direcciones de red basado en reglas y frecuentemente usado para proteger redes de acceso no autorizado mientras que permite comunicación legítima.

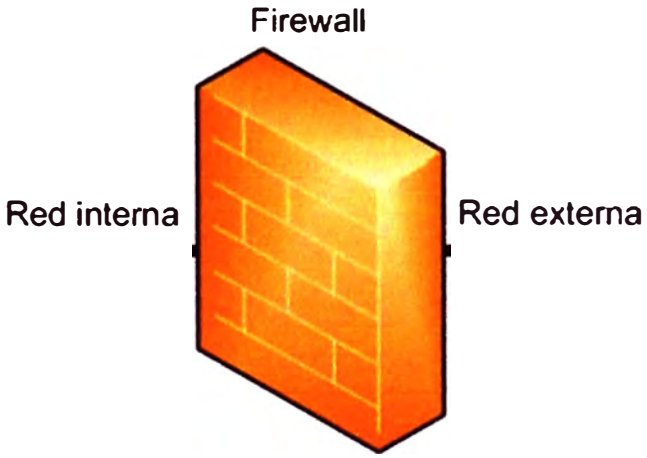


Figura 2.47 Representación de Firewall

(Fuente Ref. Elaboración Propia)

Los *Firewalls* actuales reúnen características avanzadas, sin embargo, es necesario mencionar las capacidades que tuvieron los *Firewalls* durante su evolución tecnológica.

- **Primera generación de *Firewalls* (filtrado de paquetes):**

Este tipo de filtrado de paquetes no presta atención si un paquete es parte de un flujo de tráfico. En lugar de esto, filtra cada paquete basado solamente en información contenida en su propio paquete (más comúnmente usando una combinación de paquete con dirección de origen y destino, protocolo, y el número del puerto TCP y UDP).

Los protocolos TCP (*Transmission Control Protocol*) y UDP (*User Datagram*

Protocol) constituyen a mayor comunicación sobre Internet; por convención el tráfico TCP y UDP usan puertos conocidos para un tipo de tráfico en particular.

Los *Firewalls* con filtrado de paquete funcionan principalmente en las tres primeras capas del modelo OSI.

- **Segunda generación de *Firewalls* (capa de aplicación)**

La clave del beneficio del filtrado de capa de aplicación es que puede entender ciertas aplicaciones y protocolos (tal como FTP, DNS, o Web), y puede detectar si un protocolo no deseado está oculto a través de puertos no estándares.

Un *Firewall* de aplicación es mucho más seguro y confiable comparado con *Firewalls* de filtrado de paquetes porque funciona en las siete capas del modelo OSI, desde la capa 1 (físico). Esto es similar a un *Firewall* de filtrado de paquete, pero aquí se puede filtrar información en base al contenido. Un *Firewall* de aplicación puede filtrar protocolos de capa alta como FTP, Telnet, DNS, DHCP, HTTP, TCP, UDP y TFTP.

- **Tercera generación de *Firewalls* (filtros de estado)**

Combina la primera y segunda generación de *Firewalls*, además de añadir la inspección del estado del paquete, así como al mantenimiento las conexiones que pasa a través del *Firewall*. El *Firewall* es capaz de determinar si un paquete empieza una nueva conexión, una parte de una conexión existente, o es un paquete inválido.

2.8.5 DMZ

En seguridad informática, una zona desmilitarizada (conocida también como DMZ, sigla en inglés de *demilitarized zone*) o red perimetral es una zona segura que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que en general las conexiones desde la DMZ solo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, Web y DNS. Y es precisamente estos servicios alojados en estos servidores los únicos que pueden establecer

tráfico de datos entre el DMZ y la red interna, por ejemplo, una conexión de datos entre el servidor web y una base de datos protegida situada en la red interna.

Las conexiones que se realizan desde la red externa hacia la DMZ se controlan generalmente utilizando *port address translation (PAT)*.

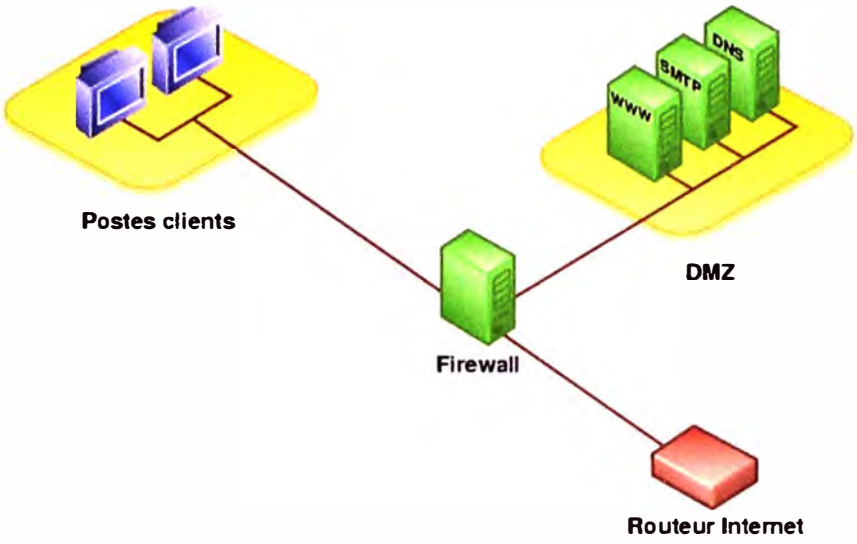


Figura 2.48 Representación de DMZ

(Fuente Ref. Elaboración Propia)

2.8.6 Inspección de protocolos de aplicación

Algunas aplicaciones requieren de un manejo especial de una porción de datos de un paquete. La inspección de los protocolos de aplicación ayuda a verificar el comportamiento de los protocolos de aplicación e identificar que tráfico malicioso no se quiere que pase a través de los dispositivos de seguridad y balanceo de carga. Basado en las especificaciones de las políticas de tráfico, el dispositivo de seguridad y balanceo de carga acepta o rechaza los paquetes asegurando que las aplicaciones y servicios estén a salvo.

Los dispositivos de seguridad y balanceo de carga inspeccionan aplicaciones como DNS, FTP, HTTP, ICMP (*Internet Control Message Protocol*), RTSP (Real Time Streaming Protocol), SCCP (*SkinnyClient Control Protocol*), ILS (Internet *Locator Service*), y SIP (*Session Initiation Protocol*).

Como primer paso antes de que los paquetes pasen al servidor destino, la inspección de aplicaciones ayuda a identificar la localización de la información embebida en las direcciones IP en el flujo TCP o UDP. Esta inspección permite al dispositivo de seguridad y balanceo de carga trasladar las direcciones embebidas y actualizar cualquier

suma de revisión u otro campo que son afectados en la traslación.

La traslación de direcciones IP embebida en el cuerpo de los protocolos es especialmente importante para el NAT y el balanceo de carga. La inspección de aplicaciones también monitorea sesiones TCP o UDP que determina el número de puertos alternativos. Algunos protocolos abiertos de TCP o UDP mejoran el desempeño. La sesión inicial de los puertos conocidos es usada para negociar dinámicamente los puertos asignados. La inspección de protocolos de aplicación tiene la función de monitorear estas sesiones, identificar el puerto dinámico asignado, y permite intercambiar información en estos puertos durante la sesión.

a. Inspección de DNS

La inspección de DNS desempeña las siguientes tareas:

- Monitorea los mensajes intercambiados de forma que aseguren que el identificador del paquete de respuesta del DNS posea una comparación correcta con el paquete de petición del DNS.
- Permite al DNS responder cada paquete de petición DNS en una conexión UDP. El dispositivo de seguridad y balanceo de carga remueve las sesiones DNS asociadas con la petición DNS tan pronto como la respuesta del DNS sea reenviada.
- Traduce el DNS a una base de grabación en la configuración del NAT (*Network Address Translation*). Solamente las búsquedas enviadas son traducidas usando NAT; el dispositivo de seguridad y balanceo de carga no administra los estados de conexión.
- Realiza la revisión del tamaño del paquete de respuesta del DNS y toma acción si sobrepasa el tamaño.
- Despliega un número de revisión de seguridad de la siguiente manera: Verifica que la longitud máxima de la etiqueta no es mayor a 63 bytes, Verifica que la longitud máxima del nombre del dominio no sea mayor 255 bytes.

b. Inspección de ICMP

La inspección de ICMP permite al tráfico ICMP tener una sesión que pueda ser inspeccionada similarmente que el tráfico TCP y UDP. Si no se usa la inspección de ICMP, se recomienda no crear listas de acceso que permitan el paso del trafico ICMP que pase a través del dispositivo de seguridad y balanceo de carga.

Sin la inspección, ICMP puede ser usada para atacar la red. La inspección ICMP asegura que hay solamente una respuesta por cada paquete de petición ICMP, y que el número de secuencia es correcto.

La inspección ICMP realiza las siguientes tareas para los paquetes de solicitud ICMP o paquetes de respuestas de mensajes ICMP:

- Crea una sesión bidireccional o estado de conexión. La clave en la búsqueda del reenvío de la dirección IP, es la dirección IP origen, dirección IP destino, tipo de protocolo ICMP, identificador ICMP, y VLAN.
- Verifica que el estado de la conexión contenga una ventana con un número de secuencia que especifique la lista de los números de secuencia de los paquetes de solicitudes pendientes de manera que los paquetes de respuesta estén pendientes.
- Verifica que los estados de conexión tengan un tiempo límite, entonces las conexiones inactivas pueden ser reusadas por otros flujos y pueden proteger la red interna contra paquetes ICMP fraudulentos.
- La respuesta del paquete es permitida solamente si una conexión es válida y previene la respuesta de paquetes que pasan a través de una ACL (lista de acceso) nuevamente si la conexión existe.
- Crea un estado de conexión para los paquetes de solicitudes y respuestas ICMP y también para los paquetes direccionados hacia o desde el dispositivo de seguridad y balanceo de carga.

2.8.7 Listas de acceso

Las listas de acceso filtran tráfico de red controlando que paquete es reenviado o bloqueado en las interfaces de un *Router*, *Switch*, dispositivo de seguridad y balanceo de carga, y *Firewall*. Los dispositivos de red determinan si se reenvía o rechaza los paquetes, basados en los criterios especificados en las listas de acceso.

El criterio de la lista de acceso podría ser por dirección origen, dirección destino, por protocolo de capa superior, o por otra información. Se debe notar que los usuarios avanzados algunas veces evaden satisfactoriamente las listas de acceso básicas, porque no se requiere autenticación.

Hay varias razones para configurar listas de acceso, por ejemplo, se puede usar listas de acceso para restringir contenido de actualización de protocolo de enrutamiento, u ofrecer control de flujo de tráfico de datos. Pero una de las más importantes razones para configurar listas de acceso es ofrecer seguridad a la red.

Se debería usar las listas de acceso para ofrecer un nivel básico de seguridad para acceder a una red. Si no se configura listas de acceso en los dispositivos de red, todos los paquetes que pasan a través de estos dispositivos podrían permitir el acceso a cualquier

parte de la red.

Por ejemplo, las listas de acceso pueden permitir que una estación acceda a una parte de la red, y previenen que otra estación acceda a la misma área. En la figura 2.49 la estación A esta permitida para acceder a la red de recursos humanos y la estación B no tiene acceso a la red de recursos humanos.

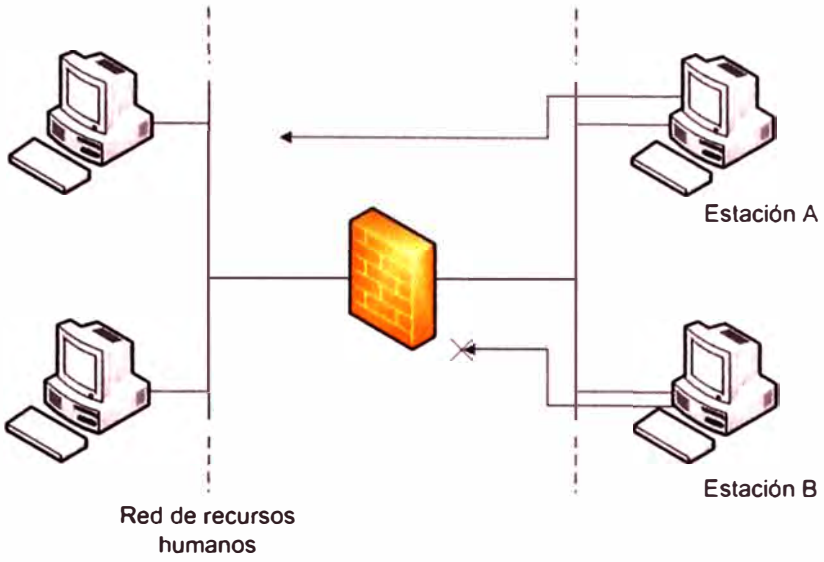


Figura 2.49 Ejemplo de listas de acceso

(Fuente Ref. Elaboración Propia)

Las listas de acceso deberían ser usadas en *Firewalls*, los cuales son colocados entre una red interna y una red externa, tal como internet. Se puede usar listas de acceso en un *Router* posicionándolo entre dos zonas de la red, para controlar el tráfico entrante o saliente en una parte especifica de la red interna.

Para aprovechar los beneficios de seguridad de la red, las listas de acceso deben ser configuradas mínimamente en los *Router*s de borde, *Router*s situados en la parte externa de la red. Esto ofrece un mayor control desde un área de menos control a la red interna o a la parte más sensible de la red.

En estos *Router*s, se debe configurar listas de acceso para cada protocolo de red configurado en las interfaces del *Router*. Se puede configurar listas de acceso con orientación de flujo entrante o con orientación de flujo saliente o en ambas direcciones.

2.9 Sistemas de Videoconferencia y características de video

Los Sistemas de videoconferencia atienden principalmente la necesidad de interacción de vídeo de alta calidad en una amplia gama de tamaños de sala de reuniones. Además de una o más pantallas de vídeo, estos sistemas permiten el intercambio de

contenidos, así como la integración con plataformas de comunicaciones unificadas (UC). Mientras los participantes se unen a las reuniones desde fuera de la sala de conferencias, estos sistemas también tienen capacidad de integrar aplicaciones de PC escritorio y puntos finales móviles (*smartphones*) al tiempo que proporciona la continuidad de la experiencia. Teniendo en cuenta la considerable base instalada de vídeo basado en estándares, estos sistemas también permiten la interoperabilidad con los criterios de valoración basados en estándares, incluyendo el Protocolo de Iniciación de Sesión (SIP) y H.323.

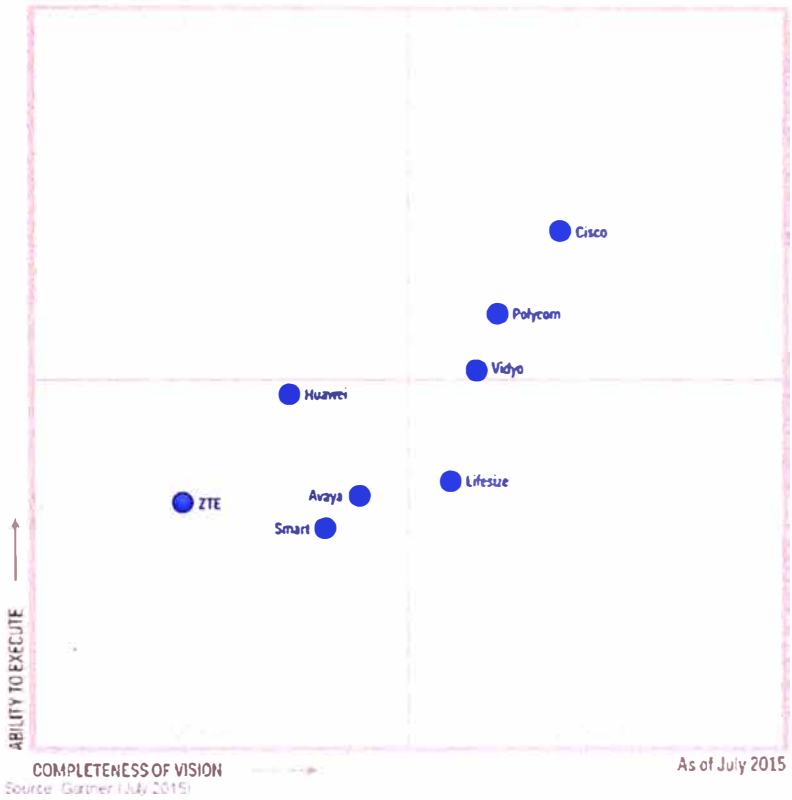


Figura 2.50 "Cuadro Mágico" de Gartner 'Fabricantes de Videoconferencia

(Fuente Ref. Gartner, julio 2015)

La figura 2.50 muestra el Cuadro Mágico del mercado de fabricantes de videoconferencia.

2.9.1 Formatos de Compresión de video y Codificación de video:

Los estudios acerca de la codificación de imágenes y video comenzaron en la década de 1950. En 1984 fue introducida la estrategia de codificación utilizando la transformada discreta de coseno (DCT), técnica ampliamente utilizada en los sistemas actuales de codificación. Las técnicas de compensación de movimiento aparecieron también en la década de 1980, obteniendo origen a las tecnologías híbridas *MC/DCT (Motion Compensation/Discrete Cosine Transform)*, utilizadas en los actuales algoritmos

MPEG.

Por otra parte, las transformadas discretas de Wavelets (DWT) comenzaron también a ser utilizadas en codificación de imágenes en la década de 1980, y fueron adoptadas más recientemente dentro de las tecnologías MPEG-4 y JPEG 2000, para la codificación de imágenes fijas.

La complejidad de codificadores y decodificadores ha ido aumentando, logrando un muy alto nivel de compresión, a expensas de requerir decodificadores y, sobre todo, codificadores muy complejos, y que requieren gran capacidad de procesamiento.

La grabación de vídeo conlleva un equilibrio entre la calidad, el tamaño del archivo y la velocidad de bits. Por lo que la técnica de compresión es esencial para reducir su tamaño y eliminar datos redundantes del video de forma que se puedan almacenar, transmitir y reproducir con eficacia, reduciendo la calidad de forma selectiva. La compresión puede ser sin pérdidas (no se descarta ningún dato de la imagen) o con pérdidas (los datos se descartan de forma selectiva).

Existen diferentes técnicas de compresión, tanto patentadas como estándar; las estándar son importantes para asegurar la compatibilidad y la interoperabilidad y tienen un papel especialmente relevante en la compresión de video, puesto que éste puede utilizar para varias finalidades y, en algunas aplicaciones de video vigilancia, debe poder visualizarse varios años después de su grabación.

Algunos codificadores utilizan varios patrones de compresión para comprimir la información. Cada codificador cuenta con su correspondiente descodificador para descomprimir e interpretar los datos de la reproducción.

2.9.2 Códec de vídeo

Es un tipo de códec que permite comprimir y descomprimir video digital, aplicando un algoritmo al video original para crear un archivo comprimido y ya listo para ser transmitido o guardado.

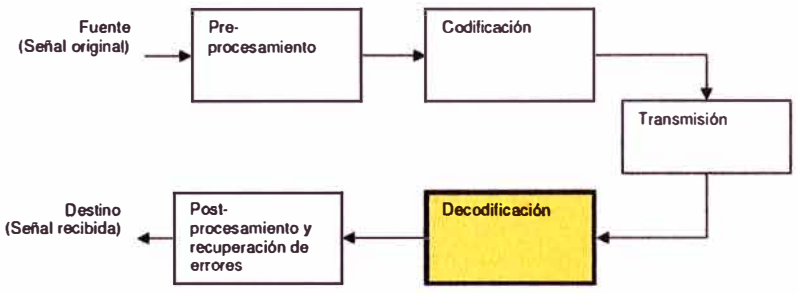


Figura 2.51 Cadena de codificación, transmisión y decodificación

(Fuente Ref. Elaboración Propia)

Para reproducir el archivo comprimido, se aplica el algoritmo inverso y se crea un video que incluye prácticamente el mismo contenido que el video original. El tiempo que se tarda en comprimir, enviar, descomprimir y mostrar un archivo es lo que se denomina "latencia". Cuanto más avanzado sea el algoritmo de compresión, mayor será a latencia. El par de algoritmos que funcionan conjuntamente se denomina códec de video (codificador/decodificador). Una cadena típica de codificación, transmisión y decodificación de video se muestra en la siguiente figura 2.51.

2.9.3 Formatos de compresión de video:

Los más difundidos estándares de compresión de video son: *Motion* JPEG, MPEG-4 Parte 2 (MPEG-4) y H.264, siendo este último el estándar más actual y eficaz.

a) Formato H.263 o MPEG-4 Parte 2

Codificación de vídeo para comunicación de baja velocidad de bits. Es una técnica de compresión de vídeo desarrollada por el *Moving Picture Experts Group* (MPEG) y basado en la Transformada de Coseno Discreta (DCT), que fue desarrollado como una mejora evolutiva basada en la experiencia del formato H.261, el estándar anterior de la ITU para la compresión de vídeo, y de los estándares MPEG-1 y MPEG-2. Su primera versión se terminó en el año 1995 y proporcionaba un sustituto adecuado para el H.261 a cualquier velocidad. Se mejoró aún más en los proyectos conocidos como H.263v2 y H.263v3.

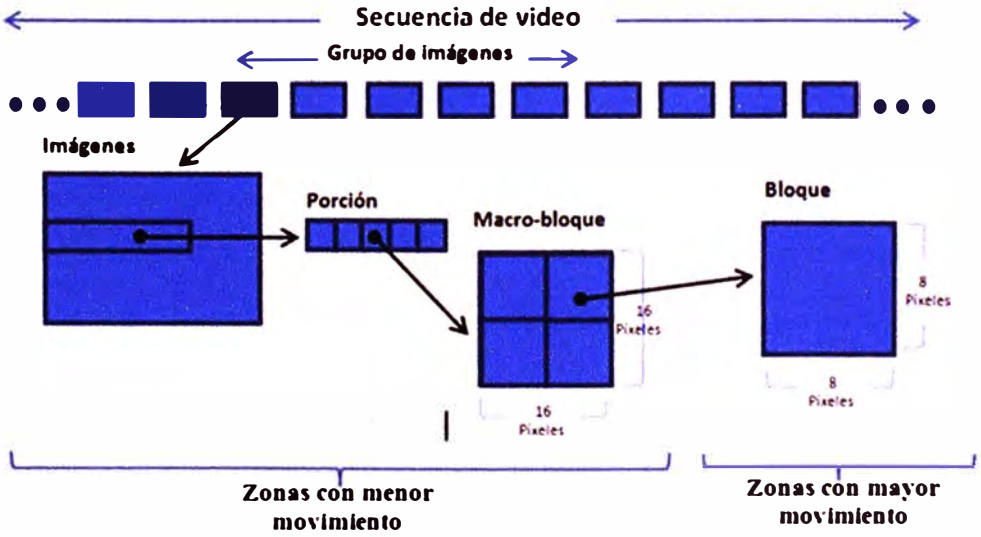


Figura 2.52 Estándares de vídeo en formato H.263

(Fuente Ref. Elaboración Propia)

En la figura 2-52 se describe la secuencia del video hasta ser codificado con

H.2634. El formato H.263 es compatible con aplicaciones de ancho de banda reducido y aplicaciones que requieren imágenes de alta calidad, sin limitaciones de frecuencia de imagen y con un ancho de banda virtualmente limitado. La mayoría de los planes de compresión de vídeo estandarizan la trama de bits, e implícitamente el decodificador, dejando el diseño del codificador a implementaciones individuales. De esta manera, las implementaciones para un perfil en particular son todas técnicamente iguales en el lado del decodificador. El perfil de un códec es un conjunto de características de este códec identificadas para cumplir con un determinado conjunto de especificaciones de las aplicaciones previstas, el H.263 tiene unos 21 perfiles, entre los que se encuentran: *Simple, Advanced Simple, Main, Core, Advanced Coding Efficiency, Advanced Real Time Simple*, etc. Los perfiles más utilizados son los de *Advanced Simple* y *Simple*, que es una parte del anterior.

Las nuevas características del H.263 son:

- Mejora la eficiencia de la codificación.
- Posibilidad de codificar datos mezclados de video, audio y voz.
- Error de resiliencia que permite una transmisión robusta.
- Posibilidad de interactuar con la escena audiovisual generada en el receptor.

b) Formato H.264 o MPEG-4 Parte 10/AAVC:

Codificación de vídeo avanzada / en movimiento para los servicios audiovisuales genéricos. Es un nuevo estándar de códec de vídeo de alta compresión, desarrollada conjuntamente por dos grupos de expertos en temas de video: el *Coding Experts Group (VCEG)* y el *Moving Picture Experts Group (MPEG)* con el propósito de crear un estándar capaz de proporcionar un vídeo de alta calidad en velocidades de bits relativamente bajas e inferiores a los estándares previos (MPEG-2, H.263 o MPEG-4 parte 2), además de no incrementarla complejidad de su diseño, la primera versión del estándar se completó en Mayo del 2003. El H.264 es un codificador de video extremadamente escalable, lo que permite entregar excelente calidad a través del entero espectro de banda ancha. Frente a las normas anteriores, H.264 propone nuevas formas de partición de bloques y una gran variedad de formas, para lo cual se asignan bloques de diferentes tamaños según la cantidad de movimiento que exista entre los distintos *frames*, para disminuir información residual y el número de vectores de movimiento. H.264 también integra un "filtro antibloques" que se aplica tanto para el codificador (antes de almacenar macro-bloques para futuras predicciones) como en el decodificador (antes de reconstruir y mostrar los

macro-bloques) para mejorar la compresión. Visualmente, este filtro suaviza los bordes de los bloques, mejorando la apariencia de los *frames* y, por tanto, también mejora la calidad de las secuencias de video. En el siguiente cuadro se muestra la variedad de particiones para la compensación de movimiento que proporciona una mayor exactitud en su estimación, a lo que se suma una precisión que puede llegar hasta un cuarto de píxel. En la figura 2.53 se describe la secuencia del video hasta ser codificado con H.264.

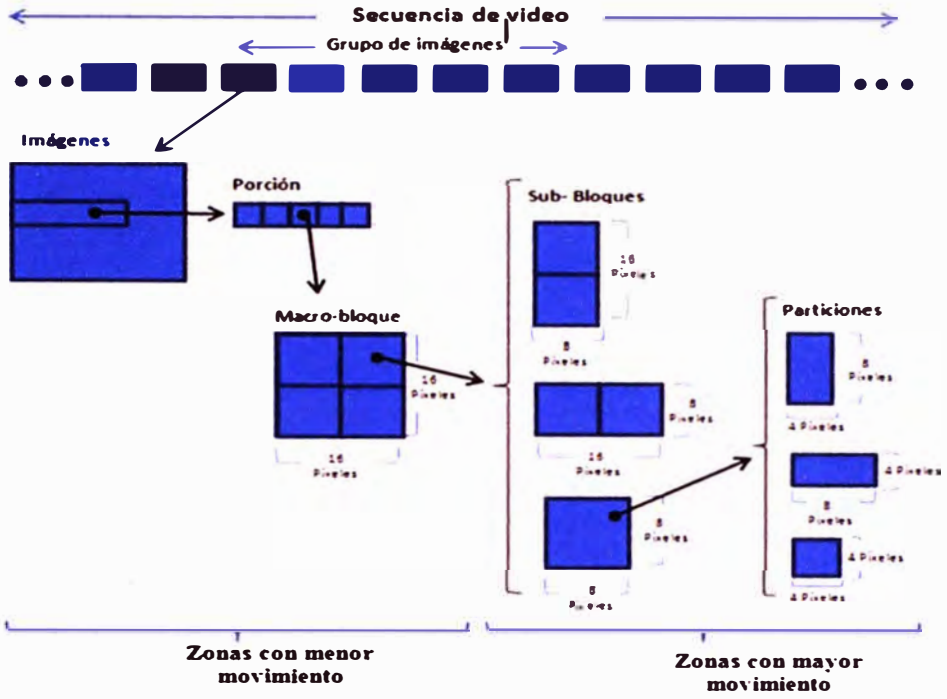


Figura 2.53 Estándar de video en formato H.264

(Fuente Ref. Elaboración Propia)

Las nuevas características del H.264 son:

- Codificación de entropía mejorada.
- Compensación / predicción de movimiento mejorada.
- Pequeños bloques para la codificación por transformada;
- Filtro "desblocking" mejorsdo.

En conclusión un codificador H.264 puede reducir el tamaño de un archivo de video digital en más de un 80% si se compara con el formato Motion JPEG, y hasta un 50% más en comparación con el estándar MPEG-4, sin comprometer la calidad (imagen, asimismo triplica la complejidad del codificador y duplica la complejida decodificador de los anteriores.

CAPÍTULO III
CASO DE ESTUDIO

En este capítulo se presenta el caso de estudio en el cual se aplica todo el contenido visto en el capítulo anterior, el marco teórico. El caso de estudio tiene como objetivo presentar el requerimiento del OSCE: el proyecto "Adquisición de un Sistema de Videoconferencia". Se hará una descripción de la necesidad para contar con tal Sistema y la situación actual tecnológica del OSCE en materias de Comunicaciones Unificadas y sistemas y/o equipamientos de redes de datos.

Actualmente el mundo empresarial, estatal y privado, necesita y requiere reestructurar la manera como los clientes internos y externos interactúan. Las empresas desean establecer comunicaciones de más impacto y más eficaces con clientes y con empresas socias; los sistemas de videoconferencia IP es la opción de más aceptación para llevar a cabo estos grandes retos.

El capítulo culmina con la presentación y descripción de un proyecto para el Banco de Crédito del Perú, en adelante BCP que tuvo por nombre: VIDEOCONFERENCIA, el cual fue diseñado por el investigador en el año 2014. Se menciona la necesidad y la finalidad del BCP para contar con este tipo de soluciones. Este es un claro ejemplo de cómo las empresas privadas requieren en la actualidad de sistemas de videoconferencia IP.

3.1 Sistema de Videoconferencia para Entidad Estatal.

El presente caso de estudio es el proyecto de telecomunicaciones del OSCE, llamado: Adquisición de un Sistema de Videoconferencia. El proyecto es una Licitación Pública identificada como: N° 002-2014-OSCE. Tuvo como valor referencial la suma de 1'935,585.59 Nuevos Soles (Fuente: Portal Web del SEACE) La fecha de otorgamiento de la buena pro fue el 10 de Noviembre del 2014, el postor ganador fue Telefónica del Perú S.A.A. En la figura 3.1 se muestra el cronograma de la licitación pública.

Cronogr ma

Etapa	Fecha Inicio	Fecha Fin
Convocatoria	29/09/2014	29/09/2014
Registro de participantes(Presencial) UNIDAD DE LOGISTICA - SEDE CENTRAL DEL OSCE	30/09/2014 08:30	29/10/2014 17:30
Formulación de consultas(Presen al) MESA DE PARTES - SEDE EDIFICIO EL REGIDOR DEL OSCE	30/09/2014 08:30	06/10/2014 16:30
Absolución de consultas UNIDAD DE LOGISTICA - SEDE CENTRAL DEL OSCE	09/10/2014	09/10/2014
Formulación de observaciones(Presencial) MESA DE PARTES - SEDE EDIFICIO EL REGIDOR DEL OSCE	10/10/2014 08:30	16/10/2014 16:30
Absolución de observaciones UNIDAD DE LOGISTICA - SEDE CENTRAL DEL OSCE	22/10/2014	22/10/2014
Integración de las Bases UNIDAD DE LOGISTICA - SEDE CENTRAL DEL OSCE	28/10/2014	28/10/2014
Presentación de propuestas(Presencial) SEDE EDIFICIO EL REGIDOR DEL OSCE	04/11/2014 10:00	04/11/2014
Calificación y Evaluación de propuestas UNIDAD DE LOGISTICA - SEDE CENTRAL DEL OSCE	05/11/2014	07/11/2014
Otorgamiento de la Buena Pro SEDE EDIFICIO EL REGIDOR DEL OSCE	10/11/2014 10:00	10/11/2014

Figura 3.1 Cronograma del proceso de Licitación Pública

(Fuente Ref. Página web del Sistema Electrónico de las Contrataciones del Estado-SEACE)

El Sistema de Videoconferencia deberá de cumplir con las especificaciones técnicas contempladas en las Bases Integradas, en el anexo A se muestra el capítulo tres de las bases integradas que hace referencia a las "Especificaciones técnicas y requerimientos técnicos mínimos".

A la fecha (Julio del 2015) el proyecto sigue siendo implementado por Telefónica del Perú S.A.A.

- **Objetivo y Requerimientos del Caso de Estudio**

El objetivo del trabajo descrito en el presente informe es dar a conocer los elementos de un sistema de videoconferencia basado en el protocolo IP para el sector empresarial y entidades públicas del Perú, mediante un diseño aplicado a la entidad estatal OSCE, de acuerdo al documento de Bases Integradas N° 002-2014-OSCE. Adicionalmente en el CAPÍTULO IV se expone y se comenta lo elementos de un sistema de

videoconferencia IP para empresas que no cuentan con ninguna base instalada o desean adquirir un sistema de videoconferencia IP en sus instalaciones.

Un resumen del requerimiento de la Infraestructura de Videoconferencia, especificado en el CAPÍTULO III "ESPECIFICACIONES TÉCNICAS Y REQUERIMIENTOS TÉCNICOS MÍNIMOS" de las bases integradas N° 002-2014-OSCE (ANEXO A) es el siguiente:

- Sistema de Telepresencia Multipunto (01 unidad): Equipo o sistema que brinde la capacidad de realizar llamadas de video multipunto. Las centradas del OSCE contarán con un terminal de videoconferencia y podrán realizar llamadas multipunto de video, estas llamadas serán provistas por el sistema de Telepresencia Multipunto de Video.
- Optimizador de recursos en el MCU (01 unidad): Sistema que actúe en conjunto con el sistema de Telepresencia Multipunto permitiendo la optimización y el manejo eficiente de los recursos de multipunto, es decir, una conferencia puede combinar videollamadas en SD, HD y Full HD sin sacrificar la experiencia de los usuarios. El OSCE desea que en una videollamada de más de dos terminales, no solo estén conectados terminales de videollamada sino también teléfonos IP, los cuales por su infraestructura de Hardware pueden contar con una cámara y pantalla de menor resolución (*SD Standard Definition*).
- *Gateway* y *Firewall* de Video: *Gateway* para el servidor de telefonía IP, que permitirá a los terminales de Telepresencia remotos, previamente registrados al sistema de telefonía IP, acceder al sistema de telefonía IP sin acceder por una conexión VPN necesariamente.
- Terminales de Telepresencia: 22 en total
- Capacitación y Entrenamiento. Dirigido al personal del OSCE como Jefes y Personal de TI
- Soporte técnico remoto y presencial, para todo el equipamiento y software instalado (Soporte correctivo por parte del proveedor) y garantía de fábrica por un periodo de tres años.

3.2 Necesidades y problemas a solucionar con los sistemas de videoconferencias

Los sistemas de Videoconferencia IP hoy en día agilizan procesos de comunicación entre clientes internos y externos de una empresa, elevando los procesos de productividad optimizando costos. La OSCE es la entidad encargada de velar por el cumplimiento de las

normas en las adquisiciones públicas del Estado peruano. Tiene competencia en el ámbito nacional, y supervisa los procesos de contratación de bienes, servicios y obras que realizan las entidades estatales (Fuente: Página Web del OSCE). Es un organismo técnico especializado adscrito al Ministerio de Economía y Finanzas, con personalidad jurídica de derecho público y constituye un pliego presupuestal. OSCE cuenta con las siguientes necesidades:

- Mejorar la toma de decisiones mediante la reducción de retardo de comunicaciones
- Construir confianza y el entendimiento entre los equipos multi-funcionales y diversos. El OSCE está en continua comunicaciones con diferentes empresas públicas o privadas que son parte del sistema de contratación públicas
- Reducir viajes de los empleados o funcionares del Tribunal de Contrataciones del Estado (Órgano resolutivo que forma parte de la estructura administrativa del OSCE. Cuenta con plena autonomía e independencia en el ejercicio de sus funciones)
- Fomentar el intercambio de conocimientos con los empleados, socios y clientes

3.3 Experiencias adicionales: Diseño de redes de videoconferencia en un Banco.

La persona que elabora esta tesina ha estado participando desde el año 2014 en proyectos relacionados a Sistemas de Videoconferencia. Dada la finalidad educativa de la presente tesina, se toma como ejemplo se hace mención a un proyecto de la entidad privada: Banco de Crédito del Perú, denominado VIDEOCONFERENCIA.

En el Anexo B se describen los términos de referencia: RFP Videoconferencia.

La solución diseñada e implementada en su momento, fue la continuación de una primera fase que tuvo lugar el año 2013. Por la cual el BCP adquirió sistemas de Videoconferencia de la marca *Cisco Systems*. Tal infraestructura fue desplegada en las sedes principales de Chorrillos y la Molina.

La figura 3.2 es una topología lógica de la infraestructura de Videoconferencia IP del BCP distribuida en las sedes de Chorrillos y la Molina. Se muestra una topología similar en cada área "*Datacenter* Chorrillos y "*Datacenter* La Molina". Cada una cuenta con

- Central de llamadas de videoconferencia Cisco Video Communication *Server* (VCS-C): Usado administrar las llamadas elaboradas por los diferentes elementos de videoconferencia presentes en las instalaciones del BCP, dentro de la red LAN y/o WAN. Estos elementos pueden ser terminales de videconferencia IP de la marca *Cisco Systems*,

Polycom y otra marca que se compatible con los protocolos estándares SIP y H.323.

- *MCUs Multipoint Control Unit*: Sistema de la marca *Cisco Systems*. Ofrece el servicio de control de llamadas multipunto de video, es el recurso en la red que realiza todo el procesamiento y transcodificación de llamadas.
- Servidores de Directorio Activo y DNS (*Domain Name Server*). Los terminales de videoconferencia son identificados mediante un nombre característico acorde a su ubicación (en una sala de reuniones) y a su uso. Es por esto que necesitan estar registrados en el directorio activo del BCP para tal fin se hace uso de un Directorio Activo y DNS mediante el sistema operativo Windows *Server* 2008 del BCP.
- Servidor NTP: Recurso en la red para sincronizar a una misma hora a todos los elementos de la red de videoconferencia.
- Sistema de Programación y Gestión de Videollamadas, *Cisco TelePresence Management Suite:* Sistema de la marca *Cisco Systems*. La gestión de las videollamadas y terminales de videoconferencia y programación de sesión de videoconferencias son funcionalidades de gran demanda para una mejor experiencia.

El proyecto de "Videoconferencia" del BCP busca adquirir terminales de videoconferencia adicionales para ser distribuidos en las sedes de La Molina y Chorrillos, adquirir un MCU adicional para tener alta disponibilidad, y sistema de control de llamada para los terminales ubicados en internet.

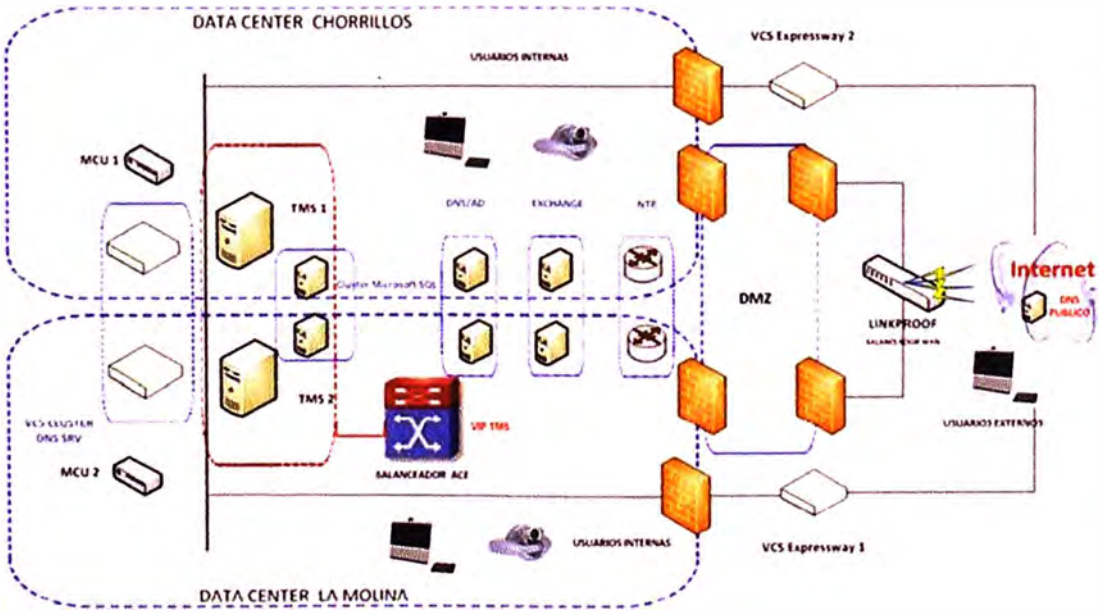


Figura 3.2 Topología de la infraestructura de Videoconferencia IP del BCP

(Fuente Ref. Telefónica del Perú)

La exposición del proyecto de "Videoconferencia" del BCP en el informe de suficiencia, es un ejemplo de los sistemas de videoconferencias IP en el sector privado. Una institución privada como un Banco siempre está en constante interacción con clientes externos o internos, la productividad de clientes internos o trabajadores de una compañía es un factor importante, los sistemas de videoconferencia IP son herramientas para contribuir en la comunicación optimizando costos de reuniones, viajes y logística.

CAPÍTULO IV
METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA

En el presente capítulo se expone solución al problema planteado en el caso de estudio del OSCE a resolver. El Objeto del presente problema es "Implementar un sistema de Videoconferencia o Telepresencia que permita fluir la comunicación entre la Sede Principal del OSCE y sus oficinas desconcentradas, ubicadas en el interior del país. El Sistema de Videoconferencia a implementar deberá poder realizar videoconferencias multipunto y de manera escalable entre las diferentes sedes, además deberá tener la capacidad de integrar otras plataformas. El sistema de Videoconferencia deberá integrarse con el sistema de telefonía IP de Cisco *Unified Communication Manager* 9.1.2 que actualmente se encuentra instalado en el OSCE, el cual provee el servicio de telefonía IP a sedes principales y oficinas desconcentradas" (Fuente: anexo a-Especificaciones técnicas y Requerimientos Técnicos mínimos)

En base a esto se hace un análisis preliminar del escenario para el problema planteado, tomando en cuenta la realidad del OSCE. Seguido se presenta una explicación de la infraestructura a usar en el desarrollo del proyecto de acuerdo a lo ofrecido por el postor ganador de la licitación pública que es a su vez la mejor opción para el OSCE.

4.1 Análisis preliminar

El OSCE en la Licitación Pública Nº 004-2013 OSCE, del año 2013 denominado "Adquisición por reemplazo del sistema de comunicaciones del OSCE". El Objeto de la licitación fue "adquirir por reemplazo la infraestructura de la red de comunicaciones (voz y datos) del OSCE, a fin de mejorar los tiempos de respuesta y niveles de disponibilidad de los procesos que cuenta; obteniendo el máximo rendimiento del hardware usado y el ahorro de recursos, en equipos de administración, eléctricos, acondicionamiento del ambiente y espacio disponible" (Fuente: Bases Integradas de la Licitación Pública N°004-2013)

En tal licitación el postor ganador o contratista fue la empresa Telefónica del Perú S.A.A. El costo del proyecto para el OSCE fue de S/. 1'889,910.23 tal como se muestra en la figura 4.1. El lugar físico de la OSCE del despliegue del proyecto fue sede la Sede El Regidor y Sede Principal (ambos ubicados en el distrito de Jesus María en Lima Metropolitana). La descripción breve de la solución propuesta, e implementada a la fecha, por Telefónica del Perú es la siguiente:

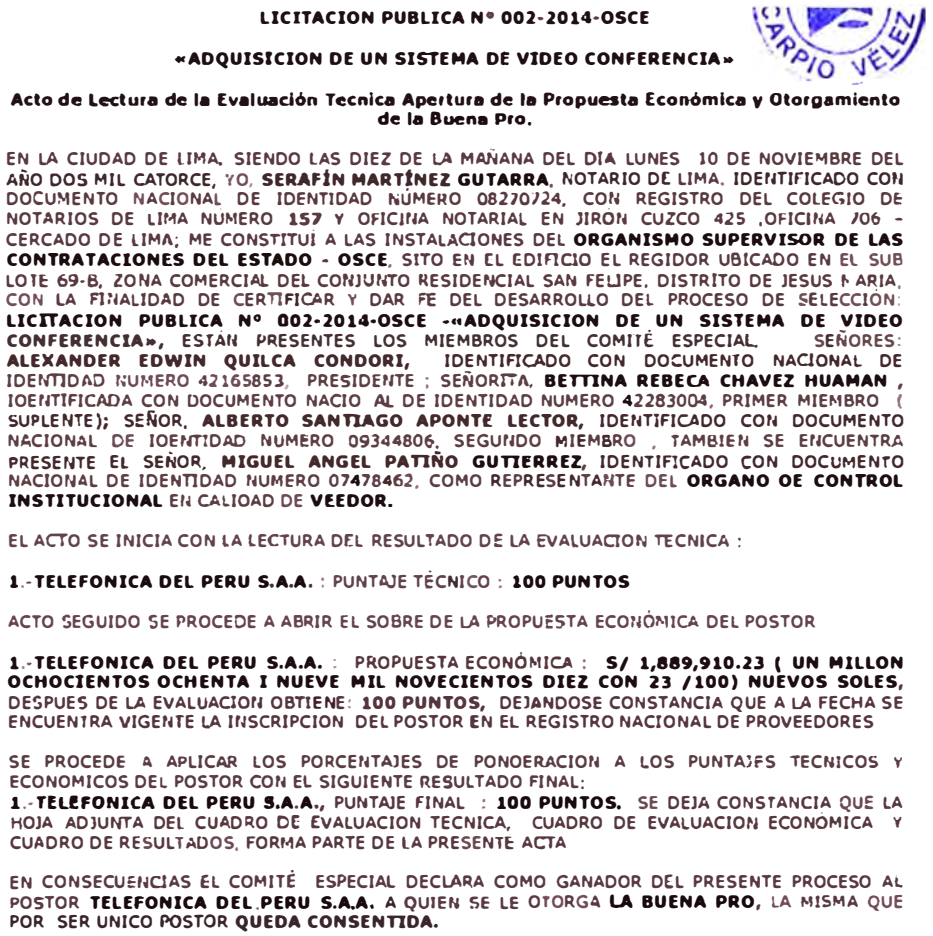
- Adquisición de equipos de comunicación: *Switches* Cisco de Acceso, *Switches* Cisco de Distribución, *Switches* Cisco de *Core*, Sistemas de puntos de acceso inalámbrico, Sistema de monitoreo y administración de la Red; todo esto de la marca *Cisco Systems*.
- Sistema de Cableado Horizontal.
- Instalación de Cableado de *Backbone*
- La renovación del centro cómputo (data center) de la sede central:
    - Climatización del Data Center.
    - Sistemas de respaldo de energía
    - Sistemas de Cableado Eléctrico.
    - Sistemas de Cableado Estructurado.
    - Sistemas de Seguridad.
    - Monitoreo Ambiental
    - Sistema de Detección y Extensión
- Plataforma de Telefonía IP: Incluye Call Center, Teléfonos IP Gerenciales, Teléfonos IP para Ejecutivos y Call Center, Teléfonos IP para la Operadora, Teléfonos IP Básicos, Teléfonos IP Privados.

La plataforma de telefonía IP que OSCE adquiere será el Sistema de Control de llamada o Central de Telefonía IP. El nombre de la "Plataforma de telefonía IP" es el Cisco *Unified Communication Manager*, el cual es un SIP *Proxy*, según lo revisado en el marco teóricio. Esta Central se encuentra actualmente desplegada en alta disponibilidad es decir OSCE cuenta con un nivel de redundancia o contingencia.

4.1.1 Alternativas de solución

En esta sección se explicará dos alternativas de solución para el caso de estudio del OSCE. La primera alternativa, denominada "Alternativa A", es acerca de ofrecer un sistema de videoconferencia y terminales de videoconferencia con la marca *Cisco Systems*, la cual es la marca de la central de telefonía IP. Esta alternativa busca destacar las ventajas operativas y tecnológicas para el OSCE.

Para la segunda alternativa, denominada "Alternativa B", los componentes para la solución no serán nombrados con una marca de fabricante en especial, sin embargo será diferente de Cisco, se mencionarán los componentes de manera genérica tomando en cuenta los estándares VoIP vistos en los capítulo además se hará mención de las ventajas y desventajas para el OSCE, al contar con una opción de otro fabricante (Marca Polycom).



LICITACION PUBLICA N° 002-2014-OSCE

«ADQUISICION DE UN SISTEMA DE VIDEO CONFERENCIA»

Acto de Lectura de la Evaluación Tecnica Apertura de la Propuesta Económica y Otorgamiento de la Buena Pro.

EN LA CIUDAD DE LIMA, SIENDO LAS DIEZ DE LA MAÑANA DEL DÍA LUNES 10 DE NOVIEMBRE DEL AÑO DOS MIL CATORCE, YO, **SERAFÍN MARTÍNEZ GUTARRA**, NOTARIO DE LIMA, IDENTIFICADO CON DOCUMENTO NACIONAL DE IDENTIDAD NÚMERO 08270724, CON REGISTRO DEL COLEGIO DE NOTARIOS DE LIMA NUMERO **157** Y OFICINA NOTARIAL EN JIRON CUZCO 425 ,OFICINA 706 - CERCADO DE LIMA; ME CONSTITUÍ A LAS INSTALACIONES DEL **ORGANISMO SUPERVISOR DE LAS CONTRATACIONES DEL ESTADO - OSCE**, SITO EN EL EDIFICIO EL REGIDOR UBICADO EN EL SUB LOTE 69-B, ZONA COMERCIAL DEL CONJUNTO RESIDENCIAL SAN FELIPE, DISTRITO DE JESUS MARIA, CON LA FINALIDAD DE CERTIFICAR Y DAR FE DEL DESARROLLO DEL PROCESO DE SELECCIÓN: **LICITACION PUBLICA N° 002-2014-OSCE -«ADQUISICION DE UN SISTEMA DE VIDEO CONFERENCIA»**, ESTÁN PRESENTES LOS MIEMBROS DEL COMITÉ ESPECIAL SEÑORES: **ALEXANDER EDWIN QUILCA CONDORI,** IDENTIFICADO CON DOCUMENTO NACIONAL DE IDENTIDAD NUMERO 42165853, PRESIDENTE ; SEÑORITA, **BETTINA REBECA CHAVEZ HUAMAN ,** IOENTIFICADA CON DOCUMENTO NACIO AL DE IDENTIDAD NUMERO 42283004, PRIMER MIEMBRO (SUPLENTE); SEÑOR, **ALBERTO SANTIAGO APONTE LECTOR,** IDENTIFICADO CON DOCUMENTO NACIONAL DE IOENTIDAD NUMERO 09344806, SEGUNDO MIEMBRO , TAMBIEN SE ENCUENTRA PRESENTE EL SEÑOR, **MIGUEL ANGEL PATIÑO GUTIERREZ,** IDENTIFICADO CON DOCUMENTO NACIONAL DE IDENTIDAD NUMERO 07478462, COMO REPRESENTANTE DEL **ORGANO OE CONTROL INSTITUCIONAL** EN CALIOAD DE **VEEDOR.**

EL ACTO SE INICIA CON LA LECTURA DEL RESULTADO DE LA EVALUACION TECNICA :

1.-TELEFONICA DEL PERU S.A.A. : PUNTAJE TÉCNICO : **100 PUNTOS**

ACTO SEGUIDO SE PROCEDE A ABRIR EL SOBRE DE LA PROPUESTA ECONÓMICA DEL POSTOR

1.-TELEFONICA DEL PERU S.A.A. : PROPUESTA ECONÓMICA : **S/ 1,889,910.23 (UN MILLON OCHOCIENTOS OCHENTA I NUEVE MIL NOVECIENTOS DIEZ CON 23 /100) NUEVOS SOLES,** DESPUES DE LA EVALUACION OBTIENE: **100 PUNTOS,** DEJANDOSE CONSTANCIA QUE A LA FECHA SE ENCUENTRA VIGENTE LA INSCRIPCION DEL POSTOR EN EL REGISTRO NACIONAL DE PROVEEDORES

SE PROCEDE A APLICAR LOS PORCENTAJES DE PONDERACION A LOS PUNTAJES TECNICOS Y ECONOMICOS DEL POSTOR CON EL SIGUIENTE RESULTADO FINAL:
1.-TELEFONICA DEL PERU S.A.A., PUNTAJE FINAL : **100 PUNTOS.** SE DEJA CONSTANCIA QUE LA HOJA ADJUNTA DEL CUADRO DE EVALUACION TECNICA, CUADRO DE EVALUACION ECONÓMICA Y CUADRO DE RESULTADOS, FORMA PARTE DE LA PRESENTE ACTA

EN CONSECUENCIAS EL COMITÉ ESPECIAL DECLARA COMO GANADOR DEL PRESENTE PROCESO AL POSTOR **TELEFONICA DEL PERU S.A.A.** A QUIEN SE LE OTORGA **LA BUENA PRO,** LA MISMA QUE POR SER UNICO POSTOR **QUEDA CONSENTIDA.**

Figura 4.1 Parte del Documento de Otorgamiento de la Buena Pro

(Fuente Ref. Página Web del SEACE)

a) Alternativa Cisco

El escenario actual del OSCE cuenta con un sistema de Telefonía IP de marca *Cisco Systems*, el nombre comercial de la Central de Telefonía IP es *Cisco Unified Communication manager* (CUCM). El CUCM es un software basado en un sistema de tratamiento de llamadas y telefonía sobre IP.

CUCM rastrea todos los componentes VoIP activos en la red; esto incluye teléfonos, *Gateways*, puentes para conferencia, recursos para transcodificación, y sistemas de mensajería de voz, entre otros. El CUCM a menudo utiliza el SCCP (*Skinny Client Control Protocol*) como un protocolo de comunicaciones para la señalización de

parámetros de hardware del sistema, tales como teléfonos IP. H.323, Media *Gateway* Control Protocol(MGCP) o SIP son usados para endosar la señalización de las llamadas a los *Gateway*. El CUCM, bajo el estándar SIP, es un SIP *Proxy*, de acuerdo al marco teórico (ver el punto 2.2.3.3 del marco teórico) es el encargado de administrar y realizar el control de acceso de una variedad de *endpoints*, de Cisco y otros fabricantes, se puede utilizar con CUCM. Los *endpoints* incluyen teléfonos IP de Cisco, *Gateways* analógicos y dispositivos de vídeo. Productos del fabricante de terceros se pueden integrar como puntos terminales SIP, sobre troncales SIP, o como terminales H.323, *Gateways*, o *Gatekeeper*s. Algunos productos de voz y de vídeo H.323 se pueden integrar a través de un *Gatekeeper*, mientras que otros serán soportados de forma nativa en el CUCM dependiendo del apoyo conjunto de características requiere. CUCM tiene un amplio apoyo para los siguientes protocolos que se utilizarán para *endpoints*: SCCP, SIP y H.323. La figura 4.2 ilustra algunas de las diversas opciones de protocolo para conectarse a CUCM. Al adquirir para este proceso

La presente alternativa busca tener al CUCM como el SIP *Proxy*. La infraestructura de videoconferencia solicitada en la parte de Especificaciones Técnicas Mínimas de las Bases Integradas, será Cisco debido a que Cisco cuenta con sistemas de videoconferencia que pueden integrarse y configurarse con el CUCM, adicionalmente Cisco cuenta con terminales de videoconferencia que cuentan con los protocolos SIP o H.323, los cuales pueden estar registrados al CUCM.

Ventajas:

- No requerir de un Sistema de Procesamiento de llamadas adicional, debido a que se usa el Sistema de Telefonía IP del OSCE para poder registrar los terminales de Videoconferencia solicitados por el OSCE. Esto evita comprar un sistema de procesamiento de llamadas exclusivamente para los 22 terminales de Videoconferencia o Telepresencia que solicita la OSCE en la Licitación Pública. Se traduce en un ahorro económico.
- Único contacto para la resolución de problemas. Al contar con infraestructura y terminales de videoconferencia de la marca Cisco, el OSCE seguirá teniendo el mismo contacto con el fabricante para la resolución de problemas o cobertura de garantía ante incidentes. Por ejemplo luego de la instalación pueden ocurrir problemas de software con el Sistema de Videoconferencia o Telepresencia Multipunto, al momento de resolver esta avería, que el contrato de garantía de

fábrica cubre, el cliente podrá tener el mismo nivel de atención, podrá realizar los mismos pasos para acceder al fabricante.

- Conocimiento de la Marca. El personal del OSCE al estar familiarizado con Cisco no tendrá problemas al recibir los nuevos conocimientos de la infraestructura de videoconferencia. Esto debido que la central telefónica IP del OSCE es de la marca Cisco.

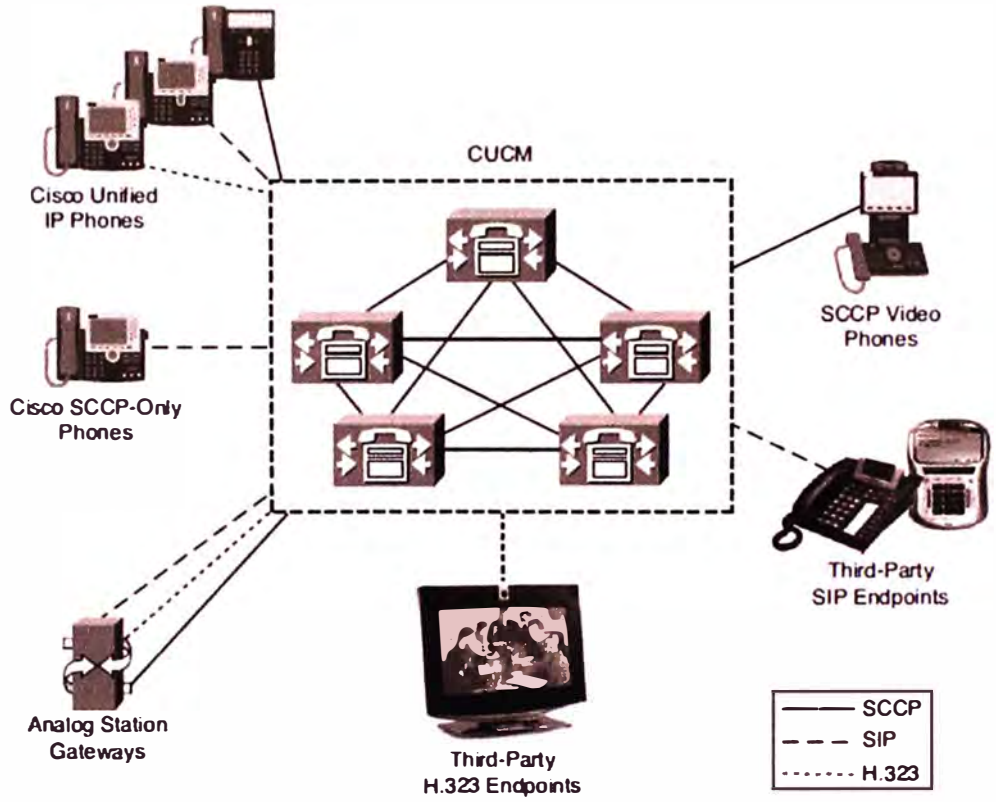


Figura 4.2 Endpoints de CUCM

(Fuente Ref. Implementing Cisco Unified Communications Manager, Part 1 (CIPT1)"- Finke, 2012, pág. 102)

b) Alternativa Polycom

En el mercado de las sistemas de videoconferencia y/o Telepresencia existen muchos fabricantes, como: Lifesize, Cisco, Polycom, Avaya, Vidyo, Huawei, entre otros. Se analiza de manera específica la alternativa con la marca Polycom

Todas las marcas antes mencionadas, también Polycom, soportan los estándares SIP y H323. Las marcas mencionadas, bajo estos estándares, ofrecen una variedad de sistemas de videoconferencia, terminales, teléfonos, software para clientes de PCs.

La alternativa B considera presentar la infraestructura de videoconferencia y

terminales de video de otra marca diferente de Cisco, la denominaremos marca "X". Presentando las siguientes características:

1.- Al proponer otra marca de Terminales de Telepresencia o Videoconferencia, de Polycom, estos no podrán ser registrados al CUCM del OSCE, por lo tanto conllevará a poner una Central o Sistema de Videoconferencia (SIP *Proxy* o H.323 *Gatekeeper*), de la misma marca de los terminales, para poder registrarlos. Esta Central de Videoconferencia tendrá las funciones de una central de terminales de videoconferencia, los terminales de videoconferencia de Polycom propuesta recibirán el control de sus llamadas y/o video llamadas por la central de Videoconferencia.

2.- Al proponer una Central de Videoconferencia de Polycom, dependiendo de cómo esté configurado como SIP *Proxy* o como H.323 *Gatekeeper* tendríamos que proponer también un *Gateway* para que pueda intercomunicarse con el CUCM del OSCE. Este *Gateway* es un elemento necesario a pesar de que no esté solicitado en las bases de la licitación. El *Gateway* tendrá configurado todas las rutas y listas de acceso que tendrán las videollamadas o llamadas de los terminales existentes (teléfonos IP del OSCE) y de los terminales Polycom de videoconferencia solicitados, vía el protocolo H.225. El *Gateway* será el elemento borde o frontera entre los dos sistemas: Sistemas de Telefonía IP Cisco del OSCE y Sistema de Videoconferencia de Polycom.

3.- Como sistema de Telepresencia o Videoconferencia Multipunto de Video se propone un MCU de Polycom. El MCU debe soportar el protocolo H.323 o SIP y será un elemento configurado mediante el protocolo SIP para el envío de la señalización hacia la central de videoconferencia IP (vía SIP *Trunk*).

4.-Sistemas con administración independiente: Proponiendo un sistema de Videoconferencia X, tendríamos dos marcas el "Sistema de Videoconferencia de Polycom" y el CUCM de Cisco para la telefonía IP.

Esta alternativa cuenta con las siguientes desventajas:

- Retardo en la resolución de problemas de tipo de garantía de fabricante.
- Personal especializado del OSCE para los dos marcas.
- Mantenimiento adicional para los sistemas Polycom.
- Capacitación de la soluciones de videoconferencia de la marca Polycom para el Personal de la OSCE

Nota: Para empresas que no tienen base instalada como la del OSCE y desean contar con soluciones de Comunicaciones Unificadas se sugiere realizar el diseño tomando

en cuenta los siguientes puntos

- Cantidad de teléfonos y cableado estructurado actuales y requeridos por SEDE que tenga la empresa:
  - Cantidad de teléfonos analógicos.
  - Cantidad de teléfonos IP
  - Protocolo de VoIP: SIP o H.323
  - Cantidad de faxes.
  - Cantidad de Operadoras.
  - Estándares de Video(H.263, H.264, etc.) o de Audio (G.729,G722,etc)
  - Categoría de cableado estructurado.
- Detallar las características que deben tener los teléfonos IP requeridos: *Headset*, Pantalla Monocromática, Pantalla a color, Manos libres (speaker), Cantidad de botones de línea, Mensajes de texto, Botonera con líneas adicionales.
- Dimensionar los servicios de Comunicaciones Unificadas que contaran en la empresa: Sistema de Telefonía IP, Sistema de Chat y Presencia corporativo, Sistema, Sistema de casilla de voz, sistema de tarificación de llamadas, sistema de IVR, etc.
- Definir la cantidad máxima de llamadas que pasarán por cada *Router* de borde.
- Dimensionamiento de la cantidad de usuarios internos y usuarios externos.
- Dimensionar los servidores y Switches LAN con calidad de servicio.
- Conectividad a la PSTN (Hunting de líneas analógicas) y WAN (ancho de banda).
- Sistema UPS, transformador de aislamiento y tablero para alimentar la solución
- Especificar las características que tendrán los *endpoints* o terminales:

4.1.2 Descripción de la topología actual

La Licitación Pública Nº 004-2013 OSCE, del año 2013 denominado "Adquisición por reemplazo del sistema de comunicaciones del OSCE" tuvo como objetivo proveer r la infraestructura de la red de comunicaciones (voz y datos) del OSCE, a fin de mejorar los tiempos de respuesta y niveles de disponibilidad de los procesos que cuenta; obteniendo el máximo rendimiento del hardware usado y el ahorro de recursos, en equipos de administración, eléctricos, acondicionamiento del ambiente y espacio disponible. La figura 4.3 muestra la topología física y lógica de la solución implementada, así como las características principales del diseño que se tienen en cuenta para la elaboración de la configuración de los equipos de red.

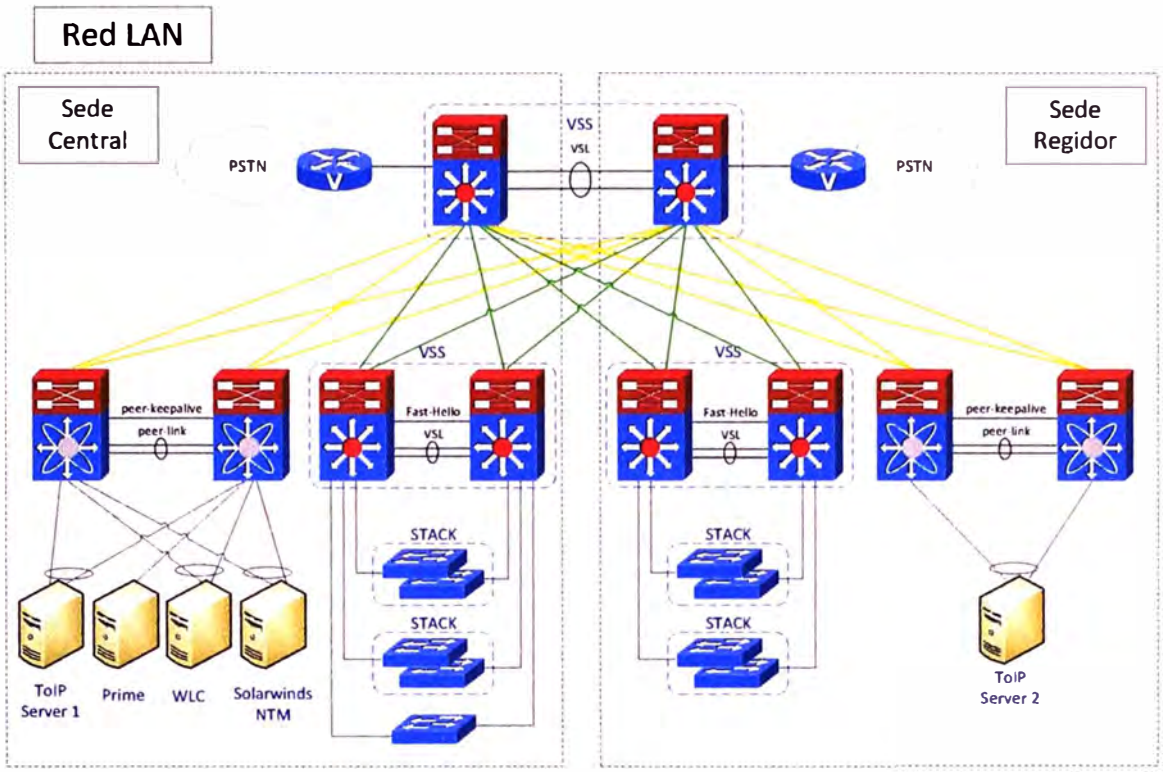


Figura 4.3 Topología Física de OSCE

(Fuente Ref. Telefónica del Perú)

El equipamiento de *Core* son dos *Switches* C4500X-32SFP+ ubicados uno en la Sede Central y el segundo en la sede Regidor. Ambos *Switches* están conectados mediante dos enlaces de 10GE y virtualizados en VSS (*Virtual Switch*ing System), de manera lógica se comportan como un solo *Switch*. VSS permite crear un clúster de dos chasis en una entidad lógica única. Esta tecnología permite la mejora en varios aspectos de la red, incluyendo el diseño, la alta disponibilidad, escalabilidad, gestión y el mantenimiento. Dicho de otra manera, dos *Switches* independientes pueden convertirse en un solo *Switch* siguiendo un procedimiento de varios pasos.

El equipamiento de distribución son cuatro *Switches* C4500X-16SFP+ ubicados dos en la Sede Central y dos en la sede Regidor. Cada par de *Switches* están conectados mediante dos enlaces de 10GE y virtualizados en VSS (Virtual *Switch*ing System), de manera lógica se comportan como un solo *Switch*.

El equipamiento de *Datacenter* son cuatro *Switches* N5K-C5548UP-FA ubicados dos en la Sede Central y dos en la sede Regidor. Cada par de *Switches* están conectados mediante dos enlaces de 10GE y con capacidad de virtualización de enlaces *Etherchannel* con *vPC (Virtual Port-Channe*l), de manera lógica se comportan como un solo *Switch*. El

virtual port cannel permite la agrupación lógica de varios enlaces físicos Ethernet, esta agrupación es tratada como un único enlace y permite sumar la velocidad nominal de cada puerto físico Ethernet usado y así obtener un enlace troncal de alta velocidad.

Cada equipo de distribución y *Datacenter* tienen dos Uplink de Fibra óptica de 10GE cada uno. Los enlaces están redundados hacia los *Switches* de *Core*, uno al de la sede Central y el otro hacia Regidor.

Los *Switches* de *Core* y de distribución están redundados con los protocolos de protección respectivos: Para el caso de los *Switches* en VSS, la protección está dada por el *Virtual Switch Link* y los protocolos *Dual Active Detection Fast-Hello* y Enhanced PagP. Para el caso de vPC, la protección está dada por el *Peer-Link* y el protocolo *Dual Active Detection Peer-Keepalive*.

La conexión entre el *Core* y *Datacenter* es en capa 2 en modo *Trunk*, dado que el cliente requiere hacer réplicas de sus servidores. La conexión entre el *Core* y los *Switches* de distribución también es en capa 2 y en modo *Trunk*, pero el enlace WAN está dado por interfaces VLAN que simulan los enlaces de capa 3. El ruteo es estático.

En la figura 4.4 se describe la distribución de los sistemas de telefonía IP finalmente implementada.

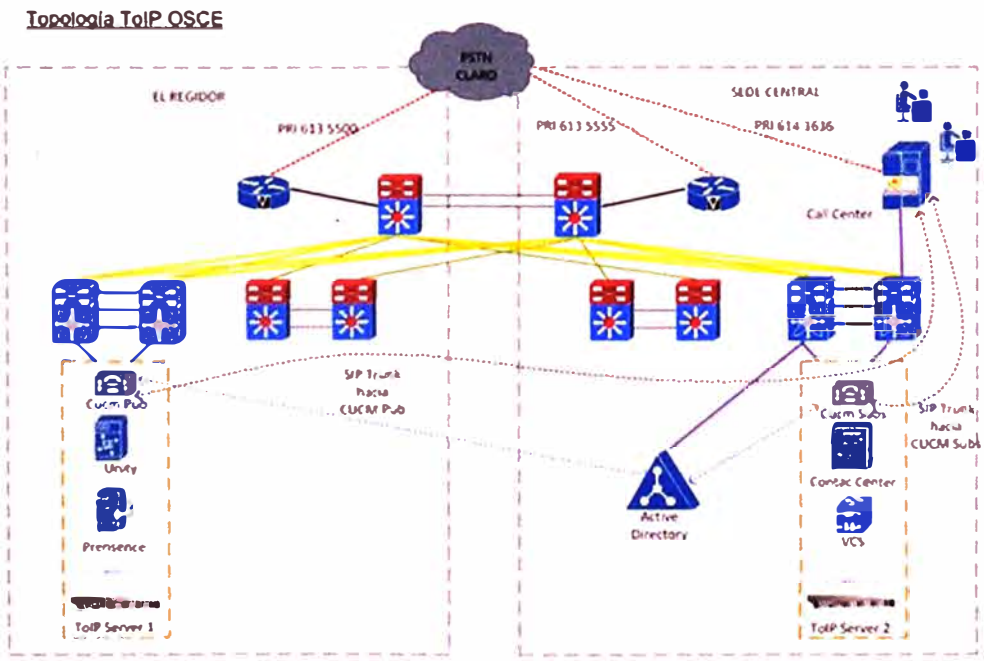


Figura 4.4 Topología del Sistema de Telefonía IP

(Fuente Ref. Telefónica del Perú)

La telefonía IP instalada en la OSCE son parte integral de la solución de

Comunicaciones Unificadas de Cisco, que unifican voz, vídeo, datos, y aplicaciones móviles en redes tanto fijas como móviles, con esta solución los usuarios de estas sedes podrán comunicarse fácilmente en su lugar de trabajo a través de cualquier medio y/o dispositivo.

Con esta solución se está utilizando la red del cliente como plataforma, para integrar los servicios desplegados en las sedes Regional y Central debido a la seguridad, resistencia, flexibilidad y escalabilidad con la que está cuenta, además de los beneficios inherentes de usar una red convergente para el transporte de datos y la interconexión.

El servidor "ToIP *Server* 1" es del modelo Cisco UCS C220 M3 cuenta con el software de virtualización de aplicaciones de la marca *VMware "Esxi"*. En este Servidor físico se han configurado los siguientes servidores Virtuales:

- *CUCM PUBLISHER* (*Cisco Unified Communication Manager*) Sistema de Telefonía IP encargado del control de admisión de las llamadas, de control y registro de los terminales de telefonía IP y video terminales El término "PUBLISHER" hace referencias a que este es el nodo principal, es el servidor virtual principal de CUCM, el CUCM "SUBSCRIBER" es el nodo secundario, ante alguna avería que tenga el PUBLISHER el SUBSCRIBER cumple el rol de CUCM principal, obteniendo como beneficio una continuidad del servicio de telefonía IP.
- *CUC PUBLISHER* (*Cisco Unity Connection*) Sistema de casilla de voz, principal, para los usuarios que cuenten con un teléfono IP,
- CUPS PUBLISHER (*Cisco Unified Presence Server*) Sistema de chat corporativo y presencia, principal, para los usuarios del OSCE

El servidor "ToIP *Server* 2" es del modelo Cisco UCS C220 M3 cuenta con el software de virtualización de aplicaciones de la marca VMware "Esxi". En este Servidor físico se han configurado los siguientes servidores Virtuales:

- *CUCM SUBSCRIBER* (*Cisco Unified Communication Manager*) Sistema de Telefonía IP encargado del control de admisión de las llamadas, de control y registro de los terminales de telefonía IP y video terminales El término "*PUBLISHER*" hace referencias a que este es el nodo principal, es el servidor virtual principal de CUCM, el CUCM "*SUBSCRIBER*" es el nodo secundario, ante alguna avería que tenga el *PUBLISHER* el *SUBSCRIBER* cumple el rol de CUCM principal, obteniendo como beneficio una continuidad del servicio de telefonía IP.
- CCX (*Cisco Conctact Center Express*) Sistema de Centro de Contactos, ofrece una

solución de gestión de interacción con clientes altamente segura, disponible, virtuales y sofisticada para un máximo de 400 agentes. La solución centro de contacto integrada y completa, está pensado tanto para los centros de contactos formales del mercado medio, sucursales de grandes empresas, y los departamentos corporativos.

La función del servidor CUCM es rastrear todos los componentes VoIP activos en la red; esto incluye teléfonos, *Gateways*, puentes para conferencia, recursos para transcodificación, y sistemas de mensajería de voz, entre otros.

El protocolo *Media Gateway Control Protocol (MGCP)* es usado para endosar la señalización de las llamadas a los *Gateways*.

Características del CUCM

Basado en tecnología de última generación, que posee una arquitectura distribuida, escalable y flexible.

- Se conecta a la PSTN a través de *Gateway* de voz usando en esta solución lineas Digitales ISDN PRI (30 canales).
- El sistema realiza video llamadas de forma nativa.
- El sistema telefónico permite asignar códigos personales para el control de las llamadas de cada usuario.
- El sistema permite la administración vía web de manera segura (https).
- El sistema de comunicaciones permite visualizar si un usuario corporativo se encuentra ocupado en una llamada.

4.1.3 Comparación de alternativas

De acuerdo a lo revisado en el punto 4.1.1 se presentaron las alternativas A y B para el desarrollo del caso de estudio. En base a un criterio de cumplimiento de las especificaciones técnicas mínimas de las bases integradas y el beneficio del OSCE se opta por elegir la alternativa A.

Tabla 2.1 Alternativas para la solución del Caso de Estudio

(Fuente Ref. Elaboración Propia)

	Alternativa A	**Alternativa B**
Integración nativa con la base instalada: Sistema	Cumple	Cumple, pero requiere de infraestructura adicional como un *Gateway*.

de Telefonía IP CUCM		
Los terminales de Videoconferencia en el CUCM	Ofrece terminales de Videoconferencia Cisco, los cuales sí pueden registrarse al Sistema de Telefonía IP CUCM	Los terminales de videoconferencia al ser de otra marca requieren de una Central de Videoconferencia.
Conocimiento Técnico de la marca por parte del OSCE	Contempla equipamiento Cisco,; debido a que el personal del OSCE cuenta actualmente con un sistema de telefonía IP de CISCO, le será de fácil entendimiento conocer la infraestructura de videoconferencia propuesta	Al proponer un sistema de videoconferencia de otra marca, el personal del OSCE deberá de conocer la arquitectura de Telepresencia o Videoconferencia propuesto, lo que se traduce a horas adicionales de capacitaciones.
Líder en Videoconferencia (Gartner 2014)	Cisco es líder en el mercado de fabricantes de videoconferencia	Dependiendo de la marca que se elija Gartner muestra los beneficios y riesgos para cada fabricante.

4.2 Infraestructura y topología de la solución

En esta sección se dará más detalle de lo mencionado en el punto 4.1.1.1 con las características de los elementos y sistemas de videoconferencia de la marca *Cisco Systems*.

4.2.1 Descripción de la infraestructura a proponer

Con la solución de videoconferencia propuesta se podrá integrar video, voz y datos en una arquitectura altamente disponible, escalable, eficiente y fácil de administrar, que permite colaboración, movilidad a los usuarios y sobre todo una reducción en el costo del servicio.

Se propone una red de videoconferencia exclusiva, capaz de integrarse de manera nativa a los servicios y aplicaciones actuales, como un *Communication Manager* 9.1.2, *IM & Presence 9.x*, del OSCE.

Componentes de la infraestructura propuesta:

- *Cisco Expressway C y E* (02 Servidores UCS)

- *Cisco TelePresence Server* 320
- *Cisco TelePresence Conductor*
- Terminal MX300G2 (2 unidades)
- Terminal Quit SX10 (20 unidades)
- Licencias de *TelePresence Room* (22)

4.2.2 Topología y descripción de la solución.

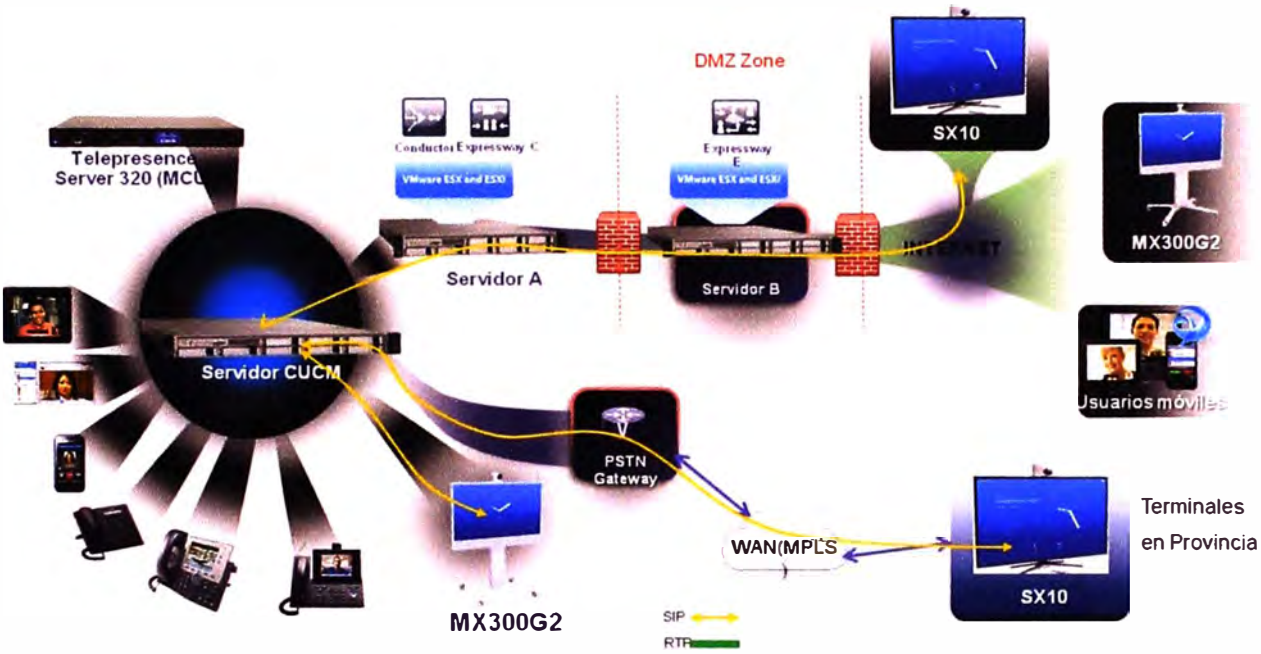


Figura 4.5 Topología de Solución Propuesta

(Fuente Ref. Telefónica del Perú)

La descripción en cuanto a funcionalidades de los componentes de la solución es la siguiente:

a) *Cisco Expressway* C y *Cisco Expressway* E

Cisco *Expressway* está diseñado específicamente para los servicios de colaboración integrales proporcionados a través de *Cisco Unified Communications Manager CUCM* (Central de Telefonía del OSCE). Cuenta con la tecnología de *Firewall*-traversal y ayuda a redefinir los límites tradicionales de colaboración empresarial, permitiendo que los terminales de Telepresencia o aplicaciones como *Cisco Jabber for Windows/iOS*, puedan realizar llamadas desde cualquier punto de la internet sin necesidad que cuenten con una VPN; esta funcionalidad es denominada "*Remote and Mobile Access*" (Acceso Remoto y Móvil).

Cisco Expressway C (Core) funciona como el *cliente* y el *Expressway E*

(Expressway) funciona como el *servidor*, tratan las llamadas entrantes desde la internet de los terminales de Telepresencia que se encuentran registrados en el CUCM.

Cisco *Expressway* C y E serán virtualizados en los servidores Cisco UCS (2) en modo de alta disponibilidad.

a) *Firewall Traversal*

El propósito de un *Firewall* es controlar el tráfico IP entrante a la red local. Los *Firewalls* generalmente bloquean las peticiones entrantes no solicitados, lo que significa que se pueden prevenir las llamadas procedentes de fuera de la red. Sin embargo, los *Firewalls* pueden configurarse para permitir solicitudes salientes a determinados destinos de confianza, y para permitir que las respuestas de esos destinos. Este principio se utiliza por la tecnología *Expressway* de Cisco para permitir el recorrido seguro de cualquier *Firewall*.

La solución *Expressway* consiste en:

- *Expressway*-E situado fuera del *Firewall* de la red pública o en la DMZ, actúa como el servidor *Firewall* tranversal.
- *Expressway*-C u otro *endpoint traversal* habilitado y situado en la red privada, que actúa como el cliente *Firewall traversal*.

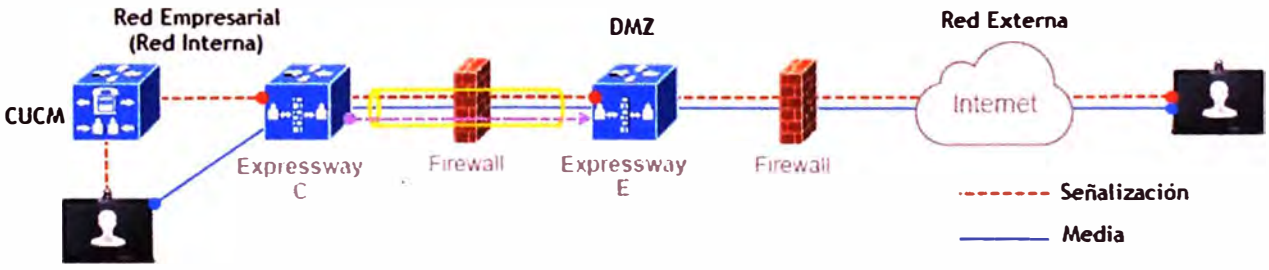


Figura 4.6 Arquitectura de Cisco Expressway y Firewal Traversal

(Fuente: www.cisco.com)

La figura 4.6 muestra la topología de Cisco Expressway y muestra el camino de la señalización y de la media. El *Firewall traversal* funciona de la siguiente manera:

i. El *Expressway E* es el servidor *traversal* instalado en la DMZ. El *Expressway C* es el cliente *traversal* instalado dentro de la red empresarial.

ii. El *Expressway C* inicia conexiones transversales de salida a través del *Firewall* para puertos específicos sobre el *Expressway E* con credenciales de acceso seguras.

iii. Una vez que la conexión se ha establecido, *Expressway C* envía *keep-alive* paquetes

al *Expressway E* para mantener la conexión.

iv. Cuando *Expressway E* recibe una llamada entrante, emite una petición de llamada entrante al *Expressway C*.

v. *Expressway C* enruta la llamada a CUCM para llegar al usuario o punto final llamado.

vi. Se establece la llamada y los medios de comunicación atraviesa el *Firewall* de forma segura a través de una conexión *traversal* existente.

➢ **Protocolos H.323 *Firewall* Traversal**

Cisco Expressway soporta dos protocolos H.323 *Firewall* traversal diferentes: El protocolo *Assent* y H.460.18/H.460.19.

- *Assent* es un protocolo propietario de Cisco.
- H.460.18 y H.460.19 son normas de la UIT que definen los protocolos para el *Firewall* transversal de la señalización y de los medios de comunicación, respectivamente. Estas normas se basan en el protocolo *Assent*.

Un *Servidor Traversal* y un cliente *traversal* deben usar el mismo protocolo para comunicarse. Cada uno de los dos protocolos usa un rango diferente de puertos.

➢ **Protocolos SIP *Firewall* Traversal**

El *expressway* soporta el protocolo *Assent* para *SIP Firewall Traversal* de la media. La señalización. La señalización se recorre a través de una conexión TCP/TLS establecida desde el cliente al servidor.

b) Cisco *TelePresence* 320

Es una solución pionera que ofrece conferencias de experiencia inmersiva para los trabajadores en la oficina y el usuario móvil. Funciona con una amplia gama de dispositivos finales, la entrega de una experiencia suave y predecible para todos los participantes de la conferencia.

Esta unidad multipunto de video, tiene como función proveer de sesiones multipunto de hasta un máximo de una sesión con 20 terminales en HD (720p) y 10 terminales en full HD (1080p).

c) Cisco TelePresence Conductor

Simplifica las comunicaciones de vídeo *multiparty*, la orquestación de los diferentes recursos que se necesitan para cada conferencia según sea necesario.

Este componente simplifica y mejora la gestión de los recursos de conferencias, haciendo conferencias fáciles de unirse y administrar. Utiliza el conocimiento de todos los

recursos de conferencia disponibles y sus capacidades para ayudar a facilitar, de forma inteligente, la utilización óptima de los recursos.

El despliegue del Conductor será de forma virtualizada en uno de los servidores UCS propuestos, ofreciendo un tratamiento de hasta máximo de 50 llamadas.

En resumen el conductor se integra con el *TelePresence Server* para la administración de las llamadas, optimizando el uso de licencias en el *TelePresence Server.* La figura 4.7 muestra el ejemplo de una llamada multipunto de video sin Conductor y con Conductor, notar que al no usar el sistema *Conductor* las licencias FHD (*Full High Definition*) son usadas y asignadas a los dispositivos que participan en la sesión multipunto, sin considerar las características de estos. Es decir un teléfono que soporta resoluciones del tipo VGA puede estar usando una licencia FHD, gracias al Conductor esta licencia FHD es "particionada" y asignada a los terminales de acuerdo al tipo de resolución que soportar, así una licencia FHD puede ser dividida para usarse con 4 terminales videoteléfonos que soportan resoluciones en SD.

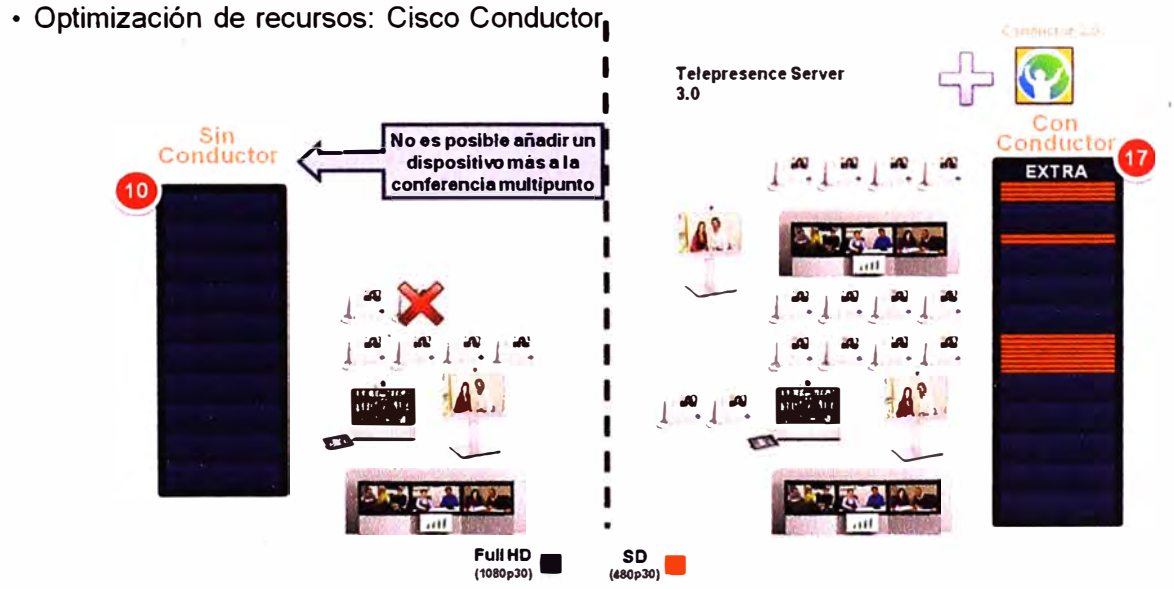


Figura 4.7 Optimación de Videollamada con Cisco Conductor

(Fuente Ref. www.cisco.com)

d) Terminales de Videoconferencia MX300

Para el modelo de terminal de videoconferencia tipo 1 solicitado por el OSCE se propone el terminal Cisco MX300 el cual cumple con las especificaciones técnicas mínimas señaladas en los términos de referencia.

e) Terminales de Videoconferencia Cisco SX10

Para el modelo de terminal de videoconferencia tipo 1 solicitado por el OSCE se propone el terminal Cisco SX10 el cual cumple con las especificaciones técnicas mínimas señaladas en los términos de referencia.

Los terminales de Telepresencia (MX300 y SX10), ubicados en las sedes remotas, al iniciar una videollamada digitando al destino, interactuarán con el CUCM de OSCE, mediante la señalización SIP. Para tal fin se registrarán en el CUCM dichos terminales mediante licencias de Telepresencia.

El CUCM verifica si los terminales de video están registrados en él. Luego la videollamada podrá tener más de 2 participantes gracias a los elementos de videoconferencia como el *TelePresence Conductor*, *TelePresence Server* 320. Este último es el terminal multipunto de video que mezcla el flujo de video (flujo RTP) de todos los participantes que participan en una llamada multipunto de video.

El *TelePresence Conductor*, optimiza los puertos licenciados del *TelePresence Server* que se usan dependiendo del terminal que participa en una videollamada.

La solución de *Expressway C* y *Expressway E* se encargan de hacer la función de *Firewall traversal* para las llamadas que acceden de terminales (*jabber for Windows, TelePresence* SX10 y MX300) ubicados en la internet. Sin la necesidad de levantar una VPN para cada conexión.

Los terminales ubicados en el internet se autentican en el *Expressway* E. El *Expressway* E estará ubicado en la DMZ por ser un recurso público.

El *expressway* E pasará las peticiones de los terminales de la internet al *Expresswway* C, este último estará instalado en la red interna e integrado al CUCM.

La solución permitirá a terminales de videoconferencia y *softclient* de telefonía interactuar mediante llamadas o videollamadas desde la internet o sedes con enlaces WAN; escalando a un videollamadas de 22 terminales participando en HD.

4.2.3 Listado de componentes

El listado de componentes y dispositivos Cisco tanto en hardware y software para la solución del caso de estudio:

Tabla 4.1 Lista de materiales

(Fuente Ref. Telefónica del Perú)

Producto	Descripción	Cantidades

BE6K-ST-BDL-K9=	Cisco BE6000 Medium Density Server Export Restricted SW	2
BE6K-SW-9X10X	Cisco Business Edition 6000 - Software App Version 9.X 10.X	2
CIT-PSU-BLKP	Power Supply Blanking Panel/Filler	2
CIT-SD-16G-C220	16GB SD Card Module for C220 Servers	2
CTI-VCSC-BE6K-PAK	Config Only E-Delivery VCS Control PAK PID	2
LIC-SW-VMVCS-K9	Software Release Key for Encrypted Virtual VCS Application	2
LIC-VCS-10+	Video Comm Server 10 Add Non-traversal Network Calls	2
LIC-VCS-GW	Enable GW Feature (H323-SIP)	2
LIC-VCSE-5+	Video Communication Server - 5 Traversal Calls	2
R2XX-RAID10	Enable RAID 10 Setting	2
UC-A03-D500GC3	500GB 6Gb SATA 7.2K RPM SFF Hot Plug/Drive Sled Mounted	8
UC-CPU-E5-2609	2.4 GHz E5-2609/80W 4C/10MB Cache/DDR3 1066MHz	4
UC-MR-1X082RY-A	8GB DDR3-1600-MHz RDIMM/PC3-12800/Dual Rank/1.35v	8
UC-PSU-650W	650W Power Supply Unit For UCSC C220 Rack Server	2
UC-RAID-9271	MegaRAID 9271-8i + Battery Backup for C240 and C220	2
VMW-VS5-HYP-K9	Cisco UC Virt. Hypervisor 5.x (2-socket)	2
VMW-VS5-SNS	Cisco UC Virt. Hypervisor 5.x - SnS	2
CAB-N5K6A-NA	Power Cord 200/240V 6A North America	2
Expressway C,E y 22 Licencias TelePresence Room		
R-CBE6K-K9	Cisco Business Edition 6000-Electronic SW Delivery-Top Level	1
BE6K-SW-9.X	Cisco Business Edition 6000 - Software Version 9.X	1
EXPWY-VE-C-K9	Cisco Expressway-C Server Virtual Edition	1
EXPWY-VE-E-K9	Cisco Expressway-E Server Virtual Edition	1
SW-EXP-8.X-K9	Software Image for Expressway with Encryption Version X8	1
LIC-EXP-AN	Enable Advanced Networking Option	1
LIC-EXP-SERIES	Enable Expressway Series Feature Set	2
LIC-EXP-E-PAK	Expressway Series Expressway-E PAK	1
LIC-EXP-TURN	Enable TURN Relay Option	1
LIC-EXP-E	Enable Expressway-E Feature Set	1
LIC-EXP-GW	Enable GW Feature (H323-SIP)	2
LIC-SW-EXP-K9	License Key Software Encrypted	2
R-UCL-UCM-LIC-K9	Top Level SKU For 9.x/10.x User License - eDelivery	1
LIC-TP-9X-ROOM	TelePresence Room Based Endpoint Single or Multi-Screen	2 2
CUCM-VERS-9.X	CUCM Software Version 9.X	1
UCM-PAK	UCM 9X/10X PAK	1
1 TelePresence 320 (Total 20 HD)		

CTI-320-TS-K9	Cisco TelePresence Server 320	1
PWR-CORD-US-C	US power cord	1
LIC-AES-TS300-K9	TelePresence Server 300 Series Encryption Key	1
CTI-5300-CAB2MCU	Cisco TelePresence MCU 5300 Series Stacking Cable	1
LIC-320-TS-K9	License Key For TS on Media 320 Software Image	1
SW-300-V4.X-K9	Software Image for TelePresence Server on media 310/320 v4.x	1
Conductor (Virtual Medium)		
R-VMCNDTRM-K9	Mid-market (Select) Virtual TP Conductor - 50 Call Sessions	1
SW-CNDTR-V2.X-K9	Cisco TelePresence Conductor base software image v2.X	1
LIC-CNDTR-C50	Conductor 50 call sessions license	1
LIC-CNDTR-CL	Conductor clustering support	1
LIC-SW-VMCNDTR-K9	Software Release Key for Virtual Conductor	1
LIC-VMCNDTR-PAK	PAK for virtual Conductor	1
Terminal TelePresence MX300G2 (2)		
CTS-MX300-K9	Cisco TelePresence MX300 55 Gen 2 PHD 1080p 8x Touch Mic	2
CTS-MX300-WBK	Cisco TelePresence MX300 Gen 2 Wheel Base	2
LIC-MX300-MS	Cisco MX300 Gen 2 MultiSite Software Feature Option	2
LIC-MX300-PR	Cisco MX300 Gen 2 Premium Resolution SW Feature Option	2
PWR-CORD-US-E	MX - Pwr cable United States 45m	2
LIC-TC-CRYPTO-K9	License key to activate sw encryption module	2
CAB-DV10-8M-	8 meter flat grey Ethernet cable for Touch 10	2
CAB-DVI-VGA-3.5MM-	SX 3.5mm ster. jack-ster.jack/DVI-VGA cab6m auto expand	2
CAB-NET-EN5M-	Ethernet cable for MX300	2
SW-S52010-TC7-K9	SW Image for SX20 and MX200/300 (2nd gen) series endpoints	2
CTS-CTRL-DVX-10+	Touch 10 auto expand	2
CTS-MX300-UNIT	MX300 Gen 2 integrated codec LCD camera speaker mic	2
CTS-QSC20-MIC+	Performance Mic - for auto expand only	4
Terminal TelePresence SX10 (20)		
CTS-SX10-K9	SX10 HD w/ int 5x Cam and mic	20
BRKT-SX10-SMK	SX10 Screen Mount Kit	20
CAB-2VGA-6M	VGA to VGA Cable 6m	20
CTS-QSC20-MIC	Performance Microphone 20	20
CAB-2HDMI-6M	HDMI to HDMI cable 6M	20
LIC-TC-CRYPTO-K9	License key to activate sw encryption module	2

		0
BRKT-SX10-WMK	SX10 Wall Mount	20
CAB-ETH-5M	Ethernet cable (5m) for auto expand	20
SW-S52030-TC7-K9	SW Image for SX10	20
CTS-RMT-TRC6	Remote Control TRC 6	20
CAB-2HDMI-2M	HDMI-HDMI oab 2m auto expand	20
PWR-SX10-AC	Power supply for SX10	20
PWR-CORD-US-A	Pwr Cord US 1.8m Black YP-12 To YC-12	20
Licencia Multipunto para el TPS320		
L-TS300-UPG-PAK	Cisco TelePresence Server 300 Series Upgrade PAK	1
L-300-1SL	Cisco TelePresence Server Screen License	10
SW-300-V4.X-K9	Software Image for TelePresence Server on media 310/320 v4.x	1

4.2.4 Configuraciones

En esta sección se detalla las actividades, operaciones y secuencias a realizar en el equipamiento Cisco propuesto para el Caso de Estudio de la Adquisición del Sistema de Videoconferencia del OSCE:

a) Terminales de Videoconferencia SX10 y MX300

- Configurar manualmente los parámetros de red: *device name* (nombre del dispositivo), IP, máscara de red, DNS, TFTP, IP del CUCM, NTP, SIP URI, etc.
- Habilitar las licencias multipunto en los MX300, las licencias multipunto son partes solicitadas por el OSCE
- Registrar los terminales al CUCM de OSCE.
- Configurar y verificar el modo aprovisionamiento para registros automáticos hacia el CUCM de OSCE.

b) Licencias de Telepresencia y del CUCM de OSCE

- Instalar de 22 licencias *Cisco TelePresence Room en* el CUCM de OSCE. Objetivo: registrar 02 MX300 y 02 SX20.
- Activar el soporte de fabricante de 3 años (PSS).
- Realizar las creaciones de los *Devices* en el CUCM de acuerdo a las

configuraciones que tenga el CUCM como *device pool, dial plans,* etc.

- Configurar 50 usuarios *devices Jabber for Windows* en el CUCM.

Expressway

- Configuración de SIP Profile para *Expressway*.
- Configuración de Regiones con apropiados anchos de banda para llamadas.
- Configuración de SIP *Profile* para teléfonos y/o terminales de videoconferencia.
- Configuración de directorio numérico para los terminales de videoconferencia (MX300 y SX10).
- Configuración de SIP *Trunk*
- Configuración de SIP *Trunk* profile.
- *Configuración* de Clúster Fully Qualified Domain Name (FQDN).
- Configuración de marcación desde teléfonos al *Expressway*. (Configuraciones en el *Call routing*).
- Marcación al dominio *Expressway* desde teléfonos Cisco.
- Configuración de SIP *Trunk*s hacia el *Cisco Telepresence Conductor*, para conferencias *Ad-Hoc y Rendezvous* (Instantánea).

c) *Expressway*-C

- Instalación de manera virtual (ova) y configurada en un UCS-C220 M3 (al cual denominaremos UCS-A). La figura 4.8 muestra el detalle de virtualización en HA.

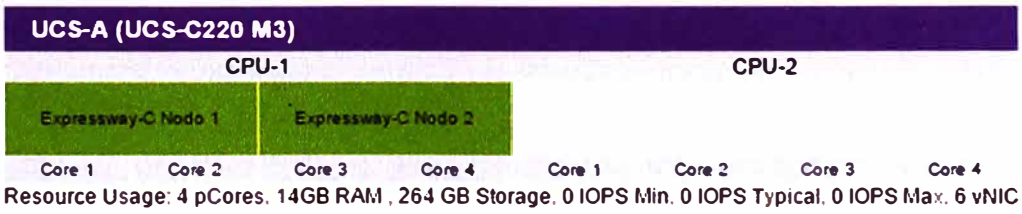


Figura 4.8 Expressway C en Servidor Cisco UCS C220

(Fuente Ref. Elaboración Propia)

- NOTA: El *Expressway*-C es un SIP *Proxy* y *Gateway* de comunicaciones para el CUCM. Es configurado con una zona *traversal*-client para comunicarse con el *Expressway*-E para permitir llamadas entrantes y salientes. Ningún dispositivo se registra en el *Expressway*-C.
- Configuración en la red interna del cliente.
- Configuración de parámetros de red: *Static* IP, Máscara de red, default *Gateway* IP, NTP.

- Configuraciones en el DNS interno del cliente, el cual el *Expressway*-C usará para realizar operaciones DNS *lookups* para resolver nombres de dispositivos internos de la red.
- Configuración de *System Name*.
- Configuración de parámetros DNS en el *Expressway*, mediante los parámetros: *System host name*, IP DNS interno y *domain name*.
- Configurar parámetros de llamadas: Pre-*search transform*, *search* rules y *transforms*. Con la intención de permitir llamadas desde dispositivos H.323 y SIP.
- Configuración de *traversal zone*, la cual define la conexión lógica entre el *Expressway* C y *Expressway* E, permite la funcionalidad de *Firewall traversal* para la señalización y media entre las dos plataformas. El *Expressway*-C es configurado con un *traversal client zone*. Configuración de *Traversal zone search rules*.
- Configuración de *neighbor zone* que contenga al CUCM de OSCE. Configuración de *search rule* para enrutar las llamadas a tal zona.
- Configuración de transform que convierta "numerodetelefonocucm"@<IP address de CUCM> a numeroexpressway@expresswaydomain.
- Configuración de certificados de seguridad entre el Expressway y CUCM.

d) *Expressway*-E

- Instalación de manera virtual (ova) y configurada en un UCS-C220 M3 (al cual denominaremos UCS-B). En la figura 4.9 se muestra el detalle de virtualización en alta disponibilidad.

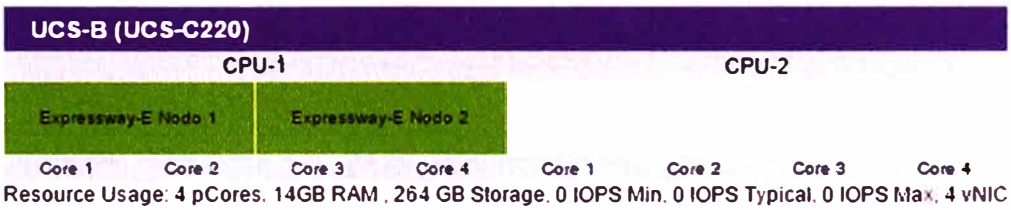


Figura 4.9 Expressway E en Servidor Cisco UCS C220

(Fuente Ref. Elaboración Propia)

- Configuración e intalación en la DMZ.
- NOTA: El *Expressway* E es un SIP *Proxy* para dispositivos que están ubicados afuera de la red interna (ejemplo: usuarios de casa o *mobile workers* registrados al CUCM a través de Internet recibiendo llamadas o haciendo llamadas desde su red empresarial). Es configurado con una zona *traversal-Server* para recibir información desde el *Expressway-C* a fin de permitir llamadas entrantes o salientes.
- El *Expressway* E es asignado con un nombre de dominio de red público, el cual será

definido en las ventanas de implementación. Por ejemplo, el *Expressway*-E es configurado con un nombre "externo solucionable": exp-e.osceperu.com (que se resuelve a una dirección IP pública por el servidor DNS público externo. Para tal fin OSCE proveerá la IP pública para el *Expressway* E.

- Configurar parámetros de red: *Públic* IP, Máscara re red, default *Gateway* IP, NTP.
- Configuración de *System Name*.
- Configuración de parámetros DNS en el *Expressway*, mediante los parámetros: System host name, IP DNS Público y domain name.
- Configurar parámetros de llamadas: *Pre-search transform, search rules y transforms.* Con la intención de permitir llamadas desde dispositivos H.323 y SIP.
- Configuración de *traversal zone*, la cual define la conexión lógica entre el *Expressway C y Expressway E*, permite la funcionalidad de *Firewall traversal* para la señalización y media entre las dos plataformas. El *Expressway-E* es configurado con un *traversal Server zone*. Configuración de *Traversal zone search* rules.
- Configuración de *DNS Zone, DNZ zone search rules.*

e) *TelePresence* Conductor

- Irá instalado de manera virtual y configurada en un UCS-C220 M3 (UCS-A). En la figura 4.10 se muestra el detalle de virtualización en alta disponibilidad.

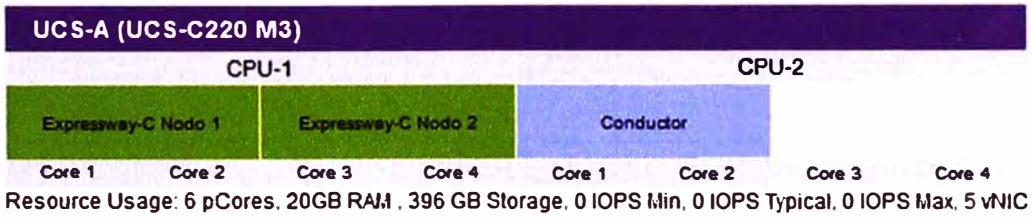


Figura 4.10 Cisco TelePresence Conductor en Servidor Cisco UCS C220

(Fuente Ref. Elaboración Propia)

- Nota: El Conductor se integra al CUCM para crear tipos de conferencias (ad hoc y *rendezvous*, los cuales serán usados por Teléfonos y Videoterminales registrados al CUCM) usando los recursos de un MCU de video o también llamado "*conference bridge*" (en este caso de estudio el *conference* bridge es el *TelePresence Server* 320).
- Configuración de *locations* para conferencias Ad-Hoc. Asignar IP para conferencias Ad-Hoc.
- Configuración de *locations* para conferencias *Rendezvous*. Asignar IP para conferencias *Rendezvous*

- C onfiguración de flujos de llamadas (*Ad-Hoc Call Flow y Rendezvous Call Flows*)
- Creación de usuario para acceso del CUCM.
- Configuración de parámetros de Red: IP, DNS, dominio, etc.
- Establecer el bridge pools, para la asignación de bridges de conferencia.

f) *TelePresence Server* 320

- Configuración de parámetros de red.
- Creación de usuario administrador para interacción con el *TelePresence* Conductor.
- Instalación de *encription key*.
- Configuración de parámetros SIP. Desahibilitar registro por H.323.
- Configuración en modo: *Remotely managed*, para que esté gestionado por el Conductor.
- Configuración licencias *Screen* (10).

g) Otros

- Procedimiento para la atención de averías (Asistencia Técnica) por un periodo de tres años.
- La asistencia técnica cubre *updates*
- Capacitación para el personal de la OSCE (personal de TI). La capacitación tendrá un máximo de 4 horas y se realizará por única vez para un máximo de 04 personas.
- Mantenimiento preventivo una vez por año, por tres años de manera presencial en la sedes de provincia, se realizarán las siguientes actividades:

➢ **Limpieza de las pantallas (TV):**

- Limpieza frecuente con un paño seco, suave y sin pelusa.
- Limpieza no frecuente con un paño humedecido con un detergente neutro.

➢ **Limpieza del lente de la cámara:**

- No se recomienda tocar el lente de la cámara con mucha frecuencia.
- En caso de realizar la limpieza, se usará un paño de micro fibra seco.

➢ **Calibración de la cámara:**

- Después de la limpieza del lente de la cámara, es necesario realizar la calibración de las cámaras.

➢ **Limpieza de las pantallas de visualización:**

- Limpieza frecuente con un paño suave con agua tibia y jabón suave para eliminar las marcas.

➢ **Limpieza de las rejillas y zona trasera de las pantallas:**

- Limpieza frecuente con un paño seco y húmedo, en caso sea necesario.

4.3 Equipamiento Cisco

En esta sección se explica las características técnicas y funcionalidades del equipamiento mencionado para la implantación del presente caso de estudio.

4.3.1 Cisco Unified Communication Manager v10.0

Es un sistema de procesamiento de llamadas que proporciona servicios de voz, vídeo, movilidad y presencia para teléfonos IP, dispositivos de procesamiento de medios, *Gateways* VoIP, dispositivos móviles y aplicaciones multimedia. Es un sistema adecuado que puede ampliarse, a la vez que mantiene la fiabilidad mediante la redundancia integrada.

Figura 4.11 Servicio de Call Control sobre terminales

(Fuente Ref. www.cisco.com)

Entre las flexibles opciones de implementación disponibles, *Cisco Unified Communications Manager* tiene la exclusiva capacidad de agrupar múltiples servidores y

gestionarlos como una entidad única, lo que permite que los clientes y los integrantes puedan optimizar la fiabilidad y la escalabilidad.

4.3.2 *Expressway Core (Expressway C) y Expressway Edge (Expressway E)*

Cisco *Expressway* está diseñado específicamente para servicios de colaboración integrales prestados a través de Cisco *Unified Communications Manager*. Proporciona tecnología de *Firewall*-traversal y ayuda a redefinir los límites tradicionales de colaboración empresarial.

Expressway puede permitir los siguientes casos de uso:

- Remoto, inicio de sesión único en el acceso a todas las cargas de trabajo de colaboración para usuarios móviles y teletrabajadores sin la necesidad de un cliente VPN
- Colaboración: Negocio-a-negocio y de empresa a consumidor.
- Interoperabilidad de vídeo con otros proveedores

4.3.3 Cisco *TelePresence Server* 320

Figura 4.12 Cisco TelePresence Server 320

(Fuente Ref. www.cisco.com)

Cisco *TelePresence Server* (TPS) conecta a usuarios de un ambiente multi-fabricante a la solución de Cisco *TelePresence*, en términos de estándar este equipo actúa como una unidad de control multipunto (MCU) de video. El Cisco TPS está basado en un chasis, descrito en la arquitectura, modelo TPS 320, el cual podrá ofrecer una videollamada multipunto con una capacidad máxima de hasta 20 participantes, cada uno en resolución 20p (HD). La figura 4.12 es la vista de la parte frontal del *TelePresence Server* 320.

- El sistema es compatible con la Central Telefónica (*CUCM*) que tiene actualmente EL CLIENTE, a fin de garantizar la compatibilidad entre todos los componentes.
- Soporta el Control automático de ganancia (AGC)
- Soporte de encriptación *Advanced Encryption Standard (AES)*
- El sistema de Telepresencia multipunto permite la combinación de terminales inmersivos, 10xFull HD (1080p30) ó 20 x HD (720p30), ó 40 x SD, ó 81 x 360 *screens*

dentro de la misma reunión virtual.

- Soporta la capacidad de realizar actualizaciones de seguridad a través de Ethernet.
- Soporta realizar una copia de seguridad de configuración.
- Soporte los siguientes códec de vídeo: H.261 (para interoperabilidad con equipos antiguos) y H.323, H.263+, H.263++ y H.264.
- Soporta en la misma conferencia formatos 16:9 como 4:3
- Soporta códec de audio tradicionales: G.711, G.722, G.723.1, G.728y G.729, así como códec de ata fidelidad: MPEG-4 AAC-LC y MPEG-4 AAC-LD, Polycom® Siren14TM y G.722.1.
- Soporta H.239/Duo Video.
- Optimiza el consumo de ancho de banda, de manera que mientras un participante está siendo visualizado en el layout pequeño, la MCU le pide a dicho terminal un ancho de banda menor. Esta funcionalidad podrá brindarse con un Hardware y/o software adicional

4.3.4 Cisco *TelePresence* Conductor

El Cisco *TelePresence* Conductor simplifica y mejora la gestión de los recursos de conferencias, haciendo fácil el unirse a las conferencias y administrarlas. Los administradores pueden especificar el nivel de servicio exacto y la experiencia requerida para cada usuario. Simplifica las comunicaciones de vídeo *multiparty*, la orquestación de los diferentes recursos que se necesitan para cada conferencia según sea necesario.

Este componente simplifica y mejora la gestión de los recursos de conferencias, haciendo conferencias fáciles de unirse y administrar. Utiliza el conocimiento de todos los recursos de conferencia disponibles y sus capacidades para ayudar a facilitar, de forma inteligente, la utilización óptima de los recursos. El despliegue del Conductor será de forma virtualizada en un servidor UCS, ofreciendo un tratamiento de hasta máximo de 2400 llamadas.

En resumen el conductor se integra con el *TelePresence Server* para la administración de las llamadas, optimizando el uso de licencias en el *TelePresence Server.*

Presenta las siguientes características:

- Es de la misma marca que el MCU (Sistema multipunto)
- Soporta la diferenciación de servicios y define determinadas clases de servicio para los asistentes de la conferencia.
- Permite la administración y gestión de los recursos de las conferencias.
- Permite seleccionar dinámicamente el más adecuado recurso para cada nueva

conferencia.

- Permite el soporte para hasta 50 sesiones de llamadas concurrentes como mínimo, pudiendo soportar más.
- Permite la asignación de recursos de acuerdo a las prioridades de cada usuario i por tipo de reunión.
- Tiene una interfaz accesible vía browser: Internet Explorer, Firefox, Chrome o Safari.
- Es compatible con los estándares de la industria tales como RS232, HTTP seguro (HTTPS), XML, Simple Network.
- Soporta los protocolos *Simple Network Management Protocol* (SNMP) y Secure Shell (SSH).
- Soporta el registro de llamadas y diagnósticos
- Soporte el registro en un servidor syslog.

4.3.5 Cisco *TelePresence* MX300

Figura 4.13 Terminal de Videoconferencia Cisco MX300

(Fuente Ref. www.cisco.com)

El equipo de videoconferencia Cisco MX300 mostrado en la figura 4.13 cuenta con las siguientes características:

- Características de diseño:
  - Kits compactos, fáciles de instalar e implementar en minutos.

- Control de la sesión vía un interfaz táctil.
- Alta fidelidad de sonido y video.
- Proporciona resoluciones de hasta 1080p a 60fps.

- Características de aplicación:
  - Comparte presentaciones y multimedia.
  - Tiene disponible la opción compartir contenido (documentos, presentaciones, etc)
  - Administración centralizada desde una interfaz táctil.
- Características de performance
  - Llamadas de hasta 6Mbps utilizando los protocolos H323 o SIP.
  - Establecer llamadas hasta con 3 puntos remotos.
  - Fácil aprovisionamiento y auto configuración desde la central de telefonía IP que tiene OSCE.
  - Soporte de funcionalidad *Firewall* Trasversal.
- Características de video:
  - Soporte de estándares H.263, H.263+, H.264.
  - *Native* 16:9 *widescreen.*
  - entradas de vídeo: 1 HDMI, 1 DVI-I (análogo y digital).
  - 1 salidas de video HDMI.
- Características de audio:
  - Parlantes integrados
  - Micrófonos integrados.
  - *Automatic Gain Control* (AGC)
  - Con reducción automática de ruido.
  - Salidas de audio, una en HDMI.
  - Estándares de audio: G.729 AB, G.711, G.722, 64 y 128 Kbps AAC-LD
- Características de red del :
  - Soporte de *QoS*
  - Soporte de NTP
  - Soporte de TCP/IP
  - Soporte de DHCP
  - Soporte de 802.1x, 802.1Q y 802.1p.
- Características de seguridad:
  - Administración vía SSH y HTTPS.

- Administración con *password* vía menú ó IP
- Interfaces de red 1 puerto *ethernet* (100/1000Mbps)
- El terminal es movible, con una base con ruedas
- Soportar funcionalidad de *ClearPath*
- Administración de sistema integrado al *TelePresence* Management Suite
- Soporte de directorio local (contactos privados) y de directorio corporativo
- Energía eléctrica de 220VAC, 50/60Hz

- Temperatura y Humedad
  - Temperatura de 0°C a 40°C
  - Humedad Relativa a 10% a 90%
- Cámara
  - 4x *Óptical* zoom
  - Campo visual horizontal 72°
  - Campo visual vertical 43.5°
- Componentes: códec, cámara HD, *display* (55"), micrófonos integrados, fuentes de alimentación.

4.3.6 Cisco *TelePresence* SX10

Figura 4.14 Terminal de Videoconferencia Cisco SX10

(Fuente Ref. www.cisco.com)

El equipo de videoconferencia Cisco SX 10, mostrado en la figura 4.14, cuenta con las siguientes características:

- Permiten la integración de un *TelePresence Management Server*
- Contiene la funcionalidad *Firewall* Traversal
- El terminal SX10 es compatible con el protocolo SIP

- Control de sesión:
  - Soporta los protocolos H.225, H.323
  - Soportar marcado URI
  - Soporte para un hunting de conferencias a través de clusters de MCU
- Características de diseño:
  - Kits compactos, fáciles de instalar e implementar
  - Control de la sesión vía touchscreen
  - Alta fidelidad de sonido y video
  - Proporcionar resoluciones de hasta 1080p a 60fps
- Características de aplicación
  - Disponibilidad de opción compartir contenido hasta una resolución WXGAp5
- Características de performance
  - Llamadas de hasta 3Mbps utilizando el protocolo SIP
  - De fácil aprovisionamiento y auto configuración con la central de telefonía IP que tiene OSCE
  - Soportar la funcionalidad *Firewall* Traversal
- Características de vídeo:
  - Soporte de estándares H.263, H.263+, H.264
  - entradas de vídeo: 1 HDMI y DVI-I (análogo y digital)
  - 1 salidas de video HDMI
- Características de audio:
  - Soportar los estándares 64kbps MPEG 4 AAC-LD, G.711, G.722, G.722.1
  - cancelares de eco
  - Automatic Gain Control (AGC)
  - Reducción automática de ruido
  - Entradas de audio: 2 micrófonos externos, 1 en la propia cámara
  - 1 salidas de audio, una en HDMI
- Características de red:
  - Soporte de QoS
  - Soporte de NTP
  - TCP/IP
  - DHCP
  - Marcado por URI

- Soporte de 802.1x, 802.1Q y 802.1p
- Características de Seguridad
  - Administración vía SSH y HTTPS
  - Administración con password vía menú o IP
- Interfaces de red ethernet (100/1000Mbps)
- Soportar funcionalidad de ClearPath
- Administración del sistema integrado al *TelePresence* Managemente Suite
- Soporte de directorio local (contactos privados) y de directorio corporativo
- Energía eléctrica
  - Alimentación energética PoE
  - Fuente de poder 220VAC, 50/60Hz
- Temperatura y Humedad
  - Temperatura de 0°C a 40°C
  - Humedad relativa 10% a 90%
- Cámara
  - 5x óptical zoom
  - Apertura vertical 51.5°
  - Apertura horizontal 83°
  - Apertura F 2.1.
- Componentes: códec, cámara HD, control remoto, micrófonos, fuente de alimentación, kit de montaje.
- Se incluyen pantallas LED con las siguientes características:
  - Tipo de pantalla
  - Tamaño de la pantalla (pulgada) 55"
  - Tipo LED
  - Resolución Full HD
  - Trumotion 120Hz
  - Panel IPS
  - Sintonizador Digital
  - Con entradas HDMI
  - Con entrada USB 3.0
  - Con entradas USB 2.0

CAPÍTULO V
VALORIZACIÓN ECONÓMICA DE UN SISTEMA DE VIDEOCONFERENCIA

En esta sección se muestra el costo total del proyecto. Los costos son mostrados en un cuadro en el que se detallan productos como equipamiento Cisco, y servicios para la puesta en marcha.

5.1 Equipamiento del Sistema de Videoconferencia

Los costos del equipamiento y servicios de ingeniería del sistema de videoconferencia disgregados por componentes. El costo total para el OSCE fue de S/1'889,910.23 nuevos soles. La empresa que vendió la solución fue Telefónica del Perú S.A.A

Tabla 5.1 Listado de Precios de todos los compontes

(Fuente Ref. Telefónica del Perú)

Código	**Descripción**	**Cantidad**	**Precio Unitario S/.**	**Precio Total S/.**
Servidores UCS				
BE6K-ST-BDL-K9=	Cisco BE6000 Medium Density *Server* Export Restricted SW	2	15,442.75	30, 885.49
BE6K-SW-9X10X	Cisco Business Edition 6000 - Software App Version 9.X 10.X	2	0.00	0.0 0
CIT-PSU-BLKP	Power Supply Blanking	2	0.00	0.0 0

	Panel/Filler			
CIT-SD-16G-C220	16GB SD Card Module for C220 Servers	2	0.00	0.00
CTI-VCSC-BE6K-PAK	Config Only E-Delivery VCS Control PAK PID	2	0.00	0.00
LIC-SW-VMVCS-K9	Software Release Key for Encrypted Virtual VCS Application	2	0.00	0.00
LIC-VCS-10+	Video Comm Server 10 Add Non-traversal Network Calls	2	0.00	0.00
LIC-VCS-GW	Enable GW Feature (H323-SIP)	2	0.00	0.00
LIC-VCSE-5+	Video Communication Server - 5 Traversal Calls	2	0.00	0.00
R2XX-RAID10	Enable RAID 10 Setting	2	0.00	0.00
UC-A03-D500GC3	500GB 6Gb SATA 7.2K RPM SFF Hot Plug/Drive Sled Mounted	8	0.00	0.00
UC-CPU-E5-2609	2.4 GHz E5-2609/80W 4C/10MB Cache/DDR3 1066MHz	4	0.00	0.00
UC-MR-1X082RY-A	8GB DDR3-1600-MHz RDIMM/PC3-12800/Dual Rank/1.35v	8	0.00	0.00
UC-PSU-650W	650W Power Supply Unit For UCSC C220 Rack Server	2	0.00	0.00
UC-RAID-9271	MegaRAID 9271-8i + Battery Backup for C240 and	2	0.00	0.00

	C220			
VMW-VS5-HYP-K9	Cisco UC Virt. Hypervisor 5.x (2-socket)	2	0.00	0.00
VMW-VS5-SNS	Cisco UC Virt. Hypervisor 5.x - SnS	2	0.00	0.00
CAB-N5K6A-NA	Power Cord 200/240V 6A North America	2	0.00	0.00
Expressway C,E y 22 Licencias *TelePresence* Room		0	0.00	0.00
R-CBE6K-K9	Cisco Business Edition 6000-Electronic SW Delivery-Top Level	1	0.00	0.00
BE6K-SW-9.X	Cisco Business Edition 6000 - Software Version 9.X	1	0.00	0.00
EXPWY-VE-C-K9	Cisco Expressway-C *Server* Virtual Edition	1	0.00	0.00
EXPWY-VE-E-K9	Cisco Expressway-E *Server* Virtual Edition	1	0.00	0.00
SW-EXP-8.X-K9	Software Image for Expressway with Encryption Version X8	1	0.00	0.00
LIC-EXP-AN	Enable Advanced Networking Option	1	0.00	0.00
LIC-EXP-SERIES	Enable Expressway Series Feature Set	2	0.00	0.00
LIC-EXP-E-PAK	Expressway Series Expressway-E	1	0.00	0.00

	PAK			
LIC-EXP-TURN	Enable TURN Relay Option	1	0.00	0.00
LIC-EXP-E	Enable Expressway-E Feature Set	1	0.00	0.00
LIC-EXP-GW	Enable GW Feature (H323-SIP)	2	0.00	0.00
LIC-SW-EXP-K9	License Key Software Encrypted	2	0.00	0.00
R-UCL-UCM-LIC-K9	Top Level SKU For 9.x/10.x User License - eDelivery	1	0.00	0.00
LIC-TP-9X-ROOM	*TelePresence* Room Based *Endpoint* Single or Multi-Screen	22	1,067.85	23,492.69
CUCM-VERS-9.X	CUCM Software Version 9.X	1	0.00	0.00
UCM-PAK	UCM 9X/10X PAK	1	0.00	0.00
1 *TelePresence* 320 (Total 20 HD)		0	0.00	0.00
CTI-320-TS-K9	Cisco *TelePresence Server* 320	1	72,285.19	72,285.19
PWR-CORD-US-C	US power cord	1	0.00	0.00
LIC-300-1SL	Cisco *TelePresence Server* Screen License	10	19,714.14	197,141.44
LIC-AES-TS300-K9	*TelePresence Server* 300 Series Encryption Key	1	0.00	0.00
CTI-5300-CAB2MCU	Cisco *TelePresence*	1	739.28	739.28

	MCU 5300 Series Stacking Cable			
LIC-320-TS-K9	License Key For TS on Media 320 Software Image	1	0.00	0.00
SW-300-V4.X-K9	Software Image for *TelePresence Server* on media 310/320 v4.x	1	0.00	0.00
Conductor (Virtual Medium)		0	0.00	0.00
R-VMCNDTRM-K9	Mid-market (Select) Virtual TP Conductor - 50 Call Sessions	1	13,134.55	13,134.55
SW-CNDTR-V2.X-K9	Cisco *TelePresence* Conductor base software image v2.X	1	0.00	0.00
LIC-CNDTR-C50	Conductor 50 call sessions license	1	0.00	0.00
LIC-CNDTR-CL	Conductor clustering support	1	0.00	0.00
LIC-SW-VMCNDTR-K9	Software Release Key for Virtual Conductor	1	0.00	0.00
LIC-VMCNDTR-PAK	PAK for virtual Conductor	1	0.00	0.00
Terminal *TelePresence* MX300G2 (2)		0	0.00	0.00
CTS-MX300-K9	Cisco *TelePresence* MX300 55 Gen 2 PHD 1080p 8x Touch Mic	2	39,264.00	78,528.01
CTS-MX300-WBK	Cisco *TelePresence* MX300 Gen 2 Wheel Base	2	0.00	0.00

LIC-MX300-MS	Cisco MX300 Gen 2 MultiSite Software Feature Option	2	5,421.39	10,842.78
LIC-MX300-PR	Cisco MX300 Gen 2 Premium Resolution SW Feature Option	2	0.00	0.00
PWR-CORD-US-E	MX - Pwr cable United States 45m	2	0.00	0.00
LIC-TC-CRYPTO-K9	License key to activate sw encryption module	2	0.00	0.00
CAB-DV10-8M-	8 meter flat grey Ethernet cable for Touch 10	2	0.00	0.00
CAB-DVI-VGA-3.5MM-	SX 3.5mm ster. jack-ster.jack/DVI-VGA cab6m auto expand	2	0.00	0.00
CAB-NET-EN5M-	Ethernet cable for MX300	2	0.00	0.00
SW-S52010-TC7-K9	SW Image for SX20 and MX200/300 (2nd gen) series *endpoints*	2	0.00	0.00
CTS-CTRL-DVX-10+	Touch 10 auto expand	2	0.00	0.00
CTS-MX300-UNIT	MX300 Gen 2 integrated codec LCD camera speaker mic	2	0.00	0.00
CTS-QSC20-MIC+	Performance Mic - for auto expand only	4	0.00	0.00
Terminal *TelePresence* SX10 (20)		0	0.00	0.00
CTS-SX10-K9	SX10 HD w/ int 5x Cam and mic	20	6,554.95	131,099.06
BRKT-SX10-	SX10	2	271.07	5,4

SMK	Screen Mount Kit	0		21.39
CAB-2VGA-6M	VGA to VGA Cable 6m	20	64.07	1,281.42
CTS-QSC20-MIC	Performance Microphone 20	20	768.85	15,377.03
CAB-2HDMI-6M	HDMI to HDMI cable 6M	20	47.64	952.85
LIC-TC-CRYPTO-K9	License key to activate sw encryption module	20	0.00	0.00
BRKT-SX10-WMK	SX10 Wall Mount	20	0.00	0.00
CAB-ETH-5M	Ethernet cable (5m) for auto expand	20	0.00	0.00
SW-S52030-TC7-K9	SW Image for SX10	20	0.00	0.00
CTS-RMT-TRC6	Remote Control TRC 6	20	0.00	0.00
CAB-2HDMI-2M	HDMI-HDMI cab 2m auto expand	20	0.00	0.00
PWR-SX10-AC	Power supply for SX10	20	131.43	2,628.55
PWR-CORD-US-A	Pwr Cord US 1.8m Black YP-12 To YC-12	20	0.00	0.00
			0.00	0.00
Soporte de Fábrica Cisco	0	0	0.00	0.00
CON-PSUP-BE6KSTBD	PRTNR SUP 24X7X4 Cisco Business Edition 6000 UCS Srv 9.0	2	1,225.13	2,450.25
CON-PSBU-RCBE6KK	PSS SWSS UPGRADES Cisco Business Editi	1	0.00	0.00
CON-PSBU-EXPWYVEC	PSS SWSS UPGRADES Cisco Expressway-C S	1	0.00	0.00
CON-PSBU-EXPWYVEE	PSS SWSS UPGRADES Cisco Expressway-E	1	0.00	0.00

	Server Virtual Editi			
CON-PSBU-RUCLUCK9	PSS SWSS UPGRADES Top Level SKU For 9.	1	0.00	0.00
CON-PSBU-LICTP9X	PSS SWSS UPGRADES *TelePresence* Room Ba	22	412.03	9,064.61
CON-PSRP-320TSK9	PRTNR TP VID 24X7X4 Cisco *TelePresence Server* 323	1	9,936.10	9,936.10
CON-PSRP-LIC3001	PRTNR TP VID 24X7X4 Cisco *TelePresence Server* Screen License	10	6,219.99	62,199.85
CON-PSRP-CTI53CAB	PRTNR TP VID 24X7X4 MCU 5300 Series Stacking Cable	1	514.31	514.31
CON-PSRU-RVMCNDK9	PRTNR TP VID SW UPG Mid-mrkt Virt TelePres Cond-50 Call Ses	1	6,503.86	6,503.86
CON-PSRP-CTSMX300	PRTNR TP VID 24X7X4 Cisco TelePres MX300 55 Gen2 PHD 1080p	2	24,291.97	48,583.94
CON-PSRN-CTSSX10	PRTNR TP VID 8X5XNBD HD w int 5x Cam and mic	20	2,259.28	45,185.50
Equipamiento Pantallas				**115 494.06**
0	Televisores LED 55" LG Model 55LB700 (20 unid)	20	5,774.70	115,494.06
Servicios de Soporte y Mantenimiento e Instalación				**717 876.62**

			0.00	
SOPORTE Y MANTENIMIENTO NO ASOCIADOS A UN CMI DE MANTENIMIENTO				
Soporte y Mantenimiento de Telefónica		3	2,728.82	8,186.47
INSTALACIONES				
Servicios profesionales de Terceros	Curso de Videoconferencia / Telepresencia	1	69,666.02	69,666.02
Servicios profesionales de Terceros	Servicios de Instalación y Configuracíon	1	213,079.07	213,079.07
Servicios profesionales de Terceros	Instalación de servicios en Lima	1	33,526.77	33,526.77
Servicios profesionales de Terceros	Riesgo por cumplimiento de tiempos	1	125,472.06	125,472.06
Servicios profesionales de Terceros	Riesgo por mantenimientos correctivos en provincia	1	83,733.20	83,733.20
Servicios profesionales de Terceros	Riesgo por instalación en 20 sedes provincia	1	50,239.92	50,239.92
Servicios profesionales de Terceros	Riesgo por sobrecosto de transporte	1	133,973.12	133,973.12
	TOTAL PROYECTO			**1,601,618.84**
	PRECIO VENTA PROYECTO (Incluido IGV)			**1,889,910.23**

5.2 Requisitos del Proveedor

El proveedor es quien ejecute el proyecto con fiel cumplimiento de las bases integradas del OSCE. El OSCE solicita algunos requisitos al proveedor para salvaguardar toda la inversión que se realice en este proyecto. Los factores y/o requisitos importantes para la realización de proyectos de esta envergadura son los siguientes:

- El proveedor debe tener autorización para brindar Servicios de Telecomunicaciones en el país.
- El proveedor cuenta con experiencia mínima de 3 años en proyectos similares de la marca ofrecida (*Cisco Systems*), considerando similares a los proyectos de los tipos: Telefonía IP, Videoconferencia, Redes o Networking). El proveedor debe acreditar con constancias, certificados, contratos en modalidad de venta o servicio con su respectiva conformidad o comprobantes de pago cuya cancelación se acredite fehacientemente.
- El proveedor debe contar con experiencia en proyectos de transmisión de audio y video en tiempo real a través de cualquier medio de transmisión (internet, redes privadas, televisión). Para acreditar esta experiencia, el proveedor, contar con constancias, certificados, contratos en la modalidad de venta o servicio con su respectiva conformidad de culminación o mediante comprobantes de pago, con la cancelación acreditada fehacientemente dentro de los últimos ocho años a la presentación de la propuesta, cumpliendo con un mínimo de 2 clientes y máximo de 10 clientes (requerimiento del OSCE).
- El proveedor debe contar con una Mesa de Ayuda (Help Desk) con un número telefónico para el reporte de fallas y gestión de incidentes 24x7. El OSCE, solicita este requerimiento para solucionar los incidentes que produzcan inoperatividad en los equipos.

CONCLUSIONES Y RECOMENDACIONES

Del presente informe se concluye lo siguiente:

1. Con los sistemas de videoconferencias, es posible organizar una reunión o una conversación cara a cara con cualquier persona en tan sólo unos minutos y eliminan la necesidad de desplazamientos y viajes. Al reducirse la necesidad de viajes produce un beneficio ecológico, en consecuencia la reducción de consumo energético y emisión de CO2.
2. La arquitectura cliente/servidor de SIP es menos compleja de implementar que H.323, al igual que sus mecanismos de seguridad y de gestión. H323 envía muchos mensajes a la red, con el riesgo potencial de crear congestión. Además, requiere de mayores procedimientos y configuraciones para la personalización.
3. La calidad de las videollamadas no se ve influenciada de manera directa por la elección de los protocolos H.323 o SIP, ya que en ambos casos, los flujos de información multimedia se transportan haciendo uso del protocolo RTP.
4. La capacitación del personal del OSCE puede ser llevada a cabo mediante los terminales que están en cada sala de Lima y Provincia. Esto trae el beneficio de ahorro de tiempo y presupuestos ya que permiten mantener reuniones y conversaciones desde cualquier lugar al ser utilizado como herramienta de comunicación para facilitar el teletrabajo.
5. El ancho de banda en las sede de Lima es mayor debido a que concentra las llamadas multipunto de video de los terminales que participan en dicha sesión.

Además se recomienda lo siguiente:

1. El OSCE al adquirir un sistema de Videoconferencia de una marca líder en tecnología, debe de capacitar al personal de ingeniería y técnicos que operarán y darán soporte a dicho sistema.
2. El uso de más terminales de videoconferencia en la sedes del OSCE implica hacer una evaluación del consumo de ancho de banda por cada sede *desconcentrada* y las

sedes de Lima del OSCE. Se recomienda evaluar el tipo de calidad de videollamada que las sedes soportarán.

3. La transferencia de contenido, como compartir escritorio remoto desde una PC conectada al terminal de videoconferencia, implica mayor ancho de banda por videollamada. Se recomienda deshabilitar esta funcionalidad en las sedes del OSCE que no lo requieran, para no tener una baja calidad de la videollamada.

ANEXO A
ESPECIFICACIONES TÉCNICAS: ADQUISICIÓN DE UN SISTEMA DE VIDEOCONFERENCIA

El presente anexo es un copia de las especificaciones técnicas y requerimientos técnicos mínimos de la Licitación Pública N° 002-2014-OSCE, elaborado por el Organismo Supervisor de las Contrataciones del Estado, con la finalidad de adquirir un sistema de videoconferencia para interconectar 21 sedes con terminales de videoconferencia y la infraestructura de red concerniente.

CAPÍTULO III
ESPECIFICACIONES TÉCNICAS Y REQUERIMIENTOS TÉCNICOS MÍNIMOS

Anexo N° 01
ESPECIFICACIONES TÉCNICAS
ADQUISICIÓN DE UN SISTEMA DE VIDEOCONFERENCIA

1. ***AREA USUARIA:***

Unida de Tecnologías de la Información

2. ***FINALIDAD PÚBLICA:***

Este requerimiento se efectúa en atención a que estos recursos brindan el apoyo tecnológico para la ejecución de los procedimientos administrativos inherentes al Sistema Nacional de la OSCE permitiendo con ello mejorar la calidad del servicio en beneficio de los ciudadanos, cuya función es promovida por toda entidad de la Administración Pública

3. ***OBJETO:***

Implementar un sistema de Videoconferencia o Telepresencia que permita fluir la comunicación entra las Sede Principal de OSCE y sus oficinas desconcentrados, ubicados en el interior del país. El Sistema de Videoconferencia a implementar deberá poder realizar videoconferencias multipunto y de manera escalable entre las diferentes sedes, además deberá tener la capacidad de integrar otras plataformas.
El sistema de Videoconferencia deberá integrarse con el sistema de telefonía IP Cisco Unified Communication Manager 9.1.2 que actualmente se encuentra instalado en el OSCE, el cual provee el servicio de telefonía IP a sedes principales y oficinas desconcentradas.

4. ***ACTIVIDAD DEL POI:***

Soporte de Sistemas a procesos internos institucionales según Desarrollo aprobado referido a los procesos internos y a usuarios.

5. ***DESCRIPCIÓN DEL BIEN:***

ITEM	*CANTIDAD*	*UNIDAD DE MEDIDA*	*DESCRIPCIÓN*
1	*01*	*01*	*SISTEMA DE VIDEOCONFERENCIA: Implementar un Sistema de VIDEOCONFERENCIA o TELEPRESENCIA que permito fluir la comunicación entra las Sede Principal de OSCE y sus oficinas desconcentrados, ubicados en el interior del país. La solución a implementar deberá permitir realizar videoconferencias multipunto y de manera escalable entre las diferentes sedes, además*

ABSOLUCIÓN A LA CONSULTA N° 01 DE TELEFONICA DEL PERÚ SAA.
En las especificaciones tecnicas no se indica que los terminales de video conferencia deben ser administrados por el call manager actual del OSCE.
Sin embargo, en los factores de evaluación se ha considerado como mejora lo siguiente:
C.2.- La solución de videoconferencia a proponer debe soportar la integración de los videotelefonos que actualmente tiene OSCE con los terminales de videoconferencia solicitados para participar en una videollamada del MCU. Además los terminales de videoconferencia deben registrarse en todo momento a la Central Telefonica del OSCE. Los terminales de Videoconferencia deben ser parte del plan de numeración telefónico actual del OSCE. Los terminales de Videoconferencia deben poder realizar llamadas encriptadas entre ellos y con los terminales de la central telefónica actual del OSCE. Esta mejora no generará costo alguno al OSCE.

			deberá tener la capacidad de integrar otras plataformas.

CARACTERÍSTICAS Y/O CONDICIONES MÍNIMAS DE BIENES Y SERVICIOS A PROVEER:

CONDICIONES MÍNIMAS

- *"Llave en mano", el proveedor ofrecerá los bienes, su instalación y puesta en funcionamiento. se deberá brindar una solución Llave en Mano de todos los componentes propuestos (en virtud de que el proveedor ofrece los bienes, su instalación y puesta en funcionamiento, incluyendo todos los accesorios, repuestos, equipamiento, servicios u otros requeridos para el correcto funcionamiento de la solución). Será la responsabilidad del portor ganador efectuar las tareas necesarias y proveer los suministros necesarios para la puesta en marcha de la solución propuesta.*
- *El postor ganador, deberá ejecutar el servicio de implementación que comprende la entrega, instalación, configuración, pruebas, integración y puesta en producción de la solución propuesta.*
- *El postor ganador presentará un procedimiento para la atención de averías.*
- *El postor ganador deberá reparar o remplazar sin costo los equipos o componentes que sean necesarios para asegurar la disponibilidad del servicio siempre y cuando la falla de estos no sea imputable al OSCE*
- *El postor ganador deberá realizar los trabajos necesarios dentro o fuera del local, incluyendo su trámite de permisos y otros necesarios sin que esto implique costo adicional para el OSCE.*
- *El OSCE garantizará la disponibilidad de las redes WAN Y LAN, de la cual es propietaria y administradora.*
- *El OSCE se compromete a brindar las facilidades de ingreso a todas las sedes del presente concurso.*
- *El OSCE será responsable de proveer solo en caso sea necesario proyectores con interface HDMI.*
- *El postor ganador será responsable de proveer e instalar para los SALAS DE VIDEOCONFERENCIA TIPO II, y las pantallas de tipo LED (PANEL IPS).*
- *El OSCE proveerá puertos disponibles en su switch LAN, tomacorrientes, energía estabilizada UPS, sistemas de protección a tierra necesarios (medición menor a 5 ohms), para los equipos que sean instalados en sus sedes en Lima (Sede Principal y Sede El Regidor) por el Postor ganador a implementar el sistema de videoconferencia, para las oficinas desconcentradas el portor deberá validar los requerimientos necesarios para asegurar el correcto funcionamiento del equipamiento a instalar, todo lo que se requiera estará a cargo del postor ganador y sin costo adicional para el OSCE.*

- ***Soporte Técnico:***

  El proveedor debe incluir soporte telefónico, envío de portes, asistencia en sitio, upgrades y updates de software, acceso a los servicios avanzados del fabricante. El soporte correctivo debe incluir:
  - *Derecho a Upgrades y Updates de Software.*
  - *Asistencia técnica telefónica, desde el principio del Periodo de Mantenimiento.*

- *Asistencia técnica presencial en Lima. En el caso de Provincias, el OSCE enviará los equipos a Lima para su revisión.*
- *Reposición automótico del equipo y/o partes de éste, si se detectan fallas propias de los equipos en el HW o SW durante el periodo de cobertura del soporte correctivo, de ser el caso el proveedor deberá proveer repuestos de fábrica. Para garantizar la continuidad operacional del servicio, el proveedor debe extender los servicios de reemplazo de partes y piezas, instalando equipos terminales mientras dure el proceso de importación.*
  El proveedor que resulte adjudicado presentará un procedimiento para la atención de averías.
  Como parte del servicio se debe de considerar los tiempos de atención y tiempo de solución a ser medidos dentro de los indicadores del servicio:
  Tiempo de Atención:
  Una vez comunicada la falla se considero un periodo aproximado de respuesta.
  - *Atención vía Telefónica : 30 minutos como máximo*
  - *Atención in-situ : 4 horas (solo Lima Metropolitana).*

- ***Capacitación y/ entrenamiento:***

  La capacitación será realizada para el personal de tecnología de la OSCE que tiene directa relación con la implementación y soporte de los equipos de infraestructura y los equipos terminales. La capacitación está considerada para ser efectuada en horario de oficina y utilizando las dependencias de la OSCE. La capacitación tendrá un máximo de 4 horas y se realizará por única vez para un máximo de 04 personas.
  Deberá de tener como mínimo los siguientes temas:
  - *Equipamiento core: operación y monitoreo de equipos.*
  - *Terminales: Configuración de elementos*
  - *Terminales: Uso del Control Remoto.*
    - *Terminales: Manejo del equipo.*
    - *Terminales: Realización de llamadas u otros requeridos.*

INFRAESTRUCTURA VIDEOCONFERENCIA

Todos los equipos deberán cumplir con las siguientes características técnicas

5.1. Sistema de Telepresencia Multipunto (01 unidad)

Se debe proveer un (01) equipo que brinde la capacidad de realizar llamadas de video multipunto, con las siguientes características:

- *El sistema deberá asegurar la compatibilidad con la Central Telefónica (Call Manager) que tiene actualmente el OSCE, a fin de garantizar la compatibilidad entre todos los componentes.*
- *Debe soportar Control automótico de ganancia (AGC).*
- *Debe soportar encriptación Advanced Encryption Standard (AES).*
- *El sistema de Telepresencia Multipunto debe permitir la combinación de terminales inmersivos, 10 x Full HD (1080p30) o 20 x HD (720p30), o 40 x SD, o 81 x 360p screens dentro de la misma reunión virtual.*
- *Debe soportar la capacidad de realizar actualizaciones de seguridad a través de Ethernet.*
- *Debe soportar realizar una copia de seguridad de configuración.*

ABSOLUCIÓN A LA CONSULTA N° 03 DE TELEFÓNICA DEL PERU SAA
Se confirma que la compatibilidad solicitada se refiere a que los componentes de la solución se integren con la central telefónica que actualmente tiene el OSCE.

- *Deben soportar los siguientes codecs de video: H.261 (poro interoperabilidad con equipos antiguos) y H.263, H.263+, H.263++ y H.264.*
- *Deben soportar en la misma conferencia formatos 16:9 como 4:3*
- *Deben soportar codes de audio tradicionales: G.711, G.722, G.723.1, G.728 y G.729, así como codecs de alta fidelidad: MPEG-4 AAC-LC y MPEG-4 AAC LD, Polycom® Siren14™ y G.722.1 Annex C.*
- *Deben soportar H.239/Duo Video.*
- *Debe optimizar el consumo de ancho de banda, de manera que mientras un participante esté siendo visualizado en un layout pequeño, la MCU le pida a dicho terminal un ancho de banda menor. Esta funcionalidad puede brindarse con un hardware y/o software adicional.*
- *Deben soportar down-speeding y recuperación de paquetes perdidos de manera que se garantice la óptima experiencia de calidad de audio y video.*

5.2. Optimizador de recursos en el MCU (01 unidad)

Se debe incluir un optimizador que actúe en conjunto con el sistema de Telepresencia Multipunto permitiendo la optimización y el manejo eficiente de los recursos de multipunto, es decir, una conferencia puede combinar sistemas en SD, HD y Full HD sin sacrificar la experiencia de los usuarios. Las especificaciones técnicas que el Optimizador de recursos debe cumplir son los siguientes:

- *Debe ser la misma marca que el MCU (Sistema multipunto).*
- *Debe soportar la diferenciación de servicios y definir determinadas clases de servicio para los asistentes de la conferencia.*
- *Debe permitir la administración y gestión de los recursos de las conferencias.*
- *Debe permitir seleccionar dinámicamente el más adecuado recurso para cada nuevo conferencio.*
- *Debe permitir soporte para hasta 50 sesiones de llamadas concurrentes.*
- *Debe permitir la asignación de recursos de acuerdo a los prioridades de cada usuario o por tipo de reunión.*
- *Debe tener una interfaz accesible vía brawer: Internet explorer, Firefox, Chrome o Safari.*
- *Debe ser compatible con los estándares de la industria tales como RS-232, HTTP seguro (HTTPS), XML, Simple Network.*
- *Debe soportar Management Protocol (SNMP) y Secure Shell (SSH) Protocolo.*
- *Debe soportar el registro de llamadas y diagnósticos.*
- *Debe soportar el registro en un servidor syslog.*

5.3. Gateway y Firewall de Video

- *Gateway para el servidor de telefonía IP, que permitirá a los terminales de telepresencia remotos, previamente registrados al sistema de telefonía IP, acceder al sistema de telefonía IP sin acceder por una conexión VPN necesariamente.*
- *Debe soportar soluciones de firewall trasversal para conectar de forma segura a otras redes de video y equipos desde lo red privado.*
- *El equipo debe integrarse nativamente con el servicio de telefonía IP.*
- *Compatible con cualquier dispositivo de videoconferencia que utilice el protocolo SIP.*
- *Debe ofrecer administración segura mediante los protocolos HTTPS, SSH y SCP.*
- *Debe soportar el protocol Transport Layer Security (TLS) para señalización SIP.*
- *El Gateway deberá permitir formar cluster entre ellos, para despliegues a futuro, hasta una capacidad de 6.*

ABSOLUCIÓN A LA CONSULTA N° 05 – 06 - 07 DE TELEFÓNICA DEL PERU SAA
Se confirma que las características del optimizador requerido deberán cumplir lo solicitado en las bases.
Se confirma que lo expresado en las bases es un requerimiento mínimo por lo tanto la solucion podria soportar más de 50 sesiones de llamadas concurrentes.

ABSOLUCIÓN A LA CONSULTA N° 08 y 09 DE TELEFÓNICA DEL PERU SAA
Los terminales de videoconferencia deben estar registrados en todo momento al Call Manager, con la finalidad de tener centralizada la gestión de estos de la misma manera como se hace con un teléfono. El Gateway y firewall de video serán los elementos de la solución que ofrezcan la funcionalidad de Firewall Traversal para dar acceso a los terminales que están en el internet sin la necesidad de una conexión VPN.
Teniendo en cuenta que la solución a implementar debe ser "llave en mano", el postor deberá considerar todos lo necesario para la implementación de estos servicios.

Se confirma que lo indicado por el postor forma parte de las caracteristicas solicitadas para el dispositivo de Gateway y Firewall de Video, y que una de sus caracteristicas debe permitir a los terminales de telepresencia remotos, previamente registrados al sistema de telefonía IP, acceder al sistema de telefonía IP sin acceder por una conexión VPN necesariamente. Así mismo el equipo debe integrarse nativamente con el servicio de telefonía IP, tal como lo señala las bases.

5.4. Terminales de Telepresencia

5.4.1. SALAS DE VIDEO CONFERENCIA TIPO I – (02 Unidades)

Se requiere implementar un total de dos (02) salas, en la Sede Principal del OSCE, en la siguiente dirección: Av. Gregorio Escobedo cuadra 7 s/n, Residencial San Felipe – Jesús María. Y en las siguientes oficinas desconcentradas del OSCE:
El equipo de videoconferencia a incluir deberá contar con las siguientes características:

- ***Características de diseño***
  - *Kits compactos, fáciles de instalar e implementar en minutos.*
  - *Control de la sesión vía uno interfaz táctil.*
  - *Alta fidelidad de sonido y video.*
  - *Proporcionar resoluciones de hasta 1080p a 60 fps.*
- ***Características de aplicación:***
  - *Compartir presentaciones y multimedia.*
  - *Debe tener disponible la opción compartir contenido (documentos, presentaciones, etc).*
  - *Administración centralizada desde una interfaz táctil.*
- ***Características de performance:***
  - *Llamadas de hasta 6Mbps utilizando los protocolos H323 o SIP.*
  - *Establecer llamadas hasta con 3 puntos remotos.*
  - *Fácil aprovisionamiento y auto configuración desde la central de telefonía IP que tiene OSCE.*
  - *Soporte de funcionalidad Firewall Trasversal.*
- ***Características de video:***
  - *Soporte de estándares H.263, H.263+. H.264.*
  - *Native 16:9 widescreen.*
  - *2 entradas de video: 1 HDMI y 1 DVI-I (análogo y digital).*
  - *1 salidas de video HDMI.*
- ***Características de audio:***
  - *Parlantes integrados.*
  - *Micrófonos integrados.*
  - *Automatic Gain Control (AGC).*
  - *Con reducción automática de ruido.*
  - *2 salidas de audio, una en HDMI.*
  - *Estándares de audio: G.729 AB, G.711, G.722.1, G.722, 64 y 128 Kbps AAC-LD.*
- ***Características de red:***
  - *Soporte de QoS.*
  - *Soporte de NTP.*
  - *TCP/IP.*
  - *DHCP.*
  - *Soporte de 802.1x, 802.1Q y 802.1p.*
- ***Características de Seguridad:***
  - *Administración vía SSH y HTTPS.*

ABSOLUCIÓN A LA CONSULTA N° 11 Y 12 DE TELEFÓNICA DEL PERU SAA
La forma de registrar el terminal de videoconferencia al CM es propia del fabricante de la solución, se confirma que deberá cumplir con lo indicado en las bases.

En las especificaciones técnicas no se indica que la base del equipo debe estar integrada o que el terminal de video conferencia sea Todo-en-uno.
Sin embargo, en los factores de evaluación se ha considerado como mejora lo siguiente:
C.3.- Sobre las Salas de Videoconferencia Tipo 1, la base del equipo deberá estar integrada a la pantalla, es decir que el terminal de videoconferencia sea todo en uno (all in one). Esta mejora no generará costo alguno al OSCE.

ABSOLUCIÓN A LA OBSERVACIÓN N° 13 DE TELEFÓNICA DEL PERU SAA
Se confirma que las salas de tipo 01 serán instaladas en el(los) local(es) del OSCE de Jesús María y se aclara que en las Oficinas Desconcentradas del OSCE se implementarán salas de Tipo 2.

- *Administración con password vía menú o IP.*

- *Interfaces de red 1 puerto ether*
- *net (100/1000Mbps).*
- *El terminal debe ser movible, con una base con ruedas.*
- *Soportar funcionalidad de ClearPath.*
- *Administración del sistema integrado al Telepresence Management Suite.*
- *Soporte de directorio local (contacto privados) y de directorio corporativo.*
- *Energía eléctrica de 220VAC, 50/60Hz.*
- ***Temperatura y Humedad:***
  - *Temperatura de 0°C a 40°C.*
  - *Humedad Relativa 10% a 90%.*
- ***Cámara:***
  - *4x Optical zoom.*
  - *Campo visual horizontal 72°.*
  - *Campo visual vertical 43.5°.*
- ***Componentes: códec, cámara HD, display (55"), micrófonos integrados, fuentes de alimentación.***

5.4.2. SALAS DE VIDEOCONFERENCIA TIPO II – (20 Unidades)

Se requiere implementar un total de veinte (20) salas, una en cada oficina desconcentrada del OSCE, las direcciones se detallan en el Anexo N°1. El equipo de videoconferencia a incluir deberá contar con las siguientes características:

- *Permitir la integración con un Telepresence Management Server.*
- *Debe contener la funcionalidad Firewall Traversal.*
- *Compatible con el protocolo SIP.*
- ***Control de sesión:***
  - *Soportar los protocolos H.225, H.323.*
  - *Soportar marcado URI.*
  - *Soporte para un hunting de conferencias a través de clusters de MCU.*
- ***Características de diseño:***
  - *Kits compactos, fáciles de instalar e implementar.*
  - *Control de la sesión vía touch screen.*
  - *Alta fidelidad de sonido y video.*
  - *Proporcionar resoluciones de hasta 1080p a 60fps.*
- ***Características de aplicación:***
  - *Disponibilidad de opción compartir contenido hasta una resolución WXGAp5*
- ***Características de performance:***
  - *Llamadas de hasta 3Mbps utilizando el protocolo SIP.*
  - *Debe ser de fácil aprovisionamiento y auto configuración con con la central de telefonía IP que tiene OSCE.*
  - *Soportar la funcionalidad Firewall Trasversal.*
- ***Características de video:***
  - *Soporte de estándares H.263, H.263+, H.264.*
  - *2 entrados de video: 1 HDMI y 1 DVI-I (análogo y digital).*
  - *1 salidas de video HDMI.*
- ***Características de audio:***

ABSOLUCIÓN A LA CONSULTA N° 10 DE TELEFÓNICA DEL PERÚ SAA

En las especificaciones técnica no se indica que los terminales de telepresencia tipo 1 y tipo 2, se registrarán al sistema de telefonía IP actual del OSCE.
Sin embargo, en los factores de evaluación se ha considerado como mejora lo siguiente:
C.2.- La solución de videoconferencia a proponer debe soportar la integración de los videoteléfonos que actualmente tiene OSCE con los terminales de videoconferencia solicitados para participar en una videollamada del MCU. Además los terminales de videoconferencia deben registrarse en todo momento a la Central Telefónica del OSCE. Los terminales de Videoconferencia deben ser parte del plan de numeración telefónico actual del OSCE. Los terminales de Videoconferencia deben poder realizar llamadas encriptadas entre ellos y con los terminales de la central telefónica actual del OSCE. Esta mejora no generará costo alguno al OSCE.

- *Soportar los estándares 64 kbps MPEG 4 AAC-LD, G.711, G.722, G.722.1*
- *2 Canceladores de eco.*
- *Automatic Gain Control (AGC).*
- *Reducción automática de ruido.*
- *Entradas de audio: 2 micrófonos externos, 1 en la propia cámara.*
- *1 Salidas de audio, una en HDMI.*

o ***Características de red:***
- *Soporte de QoS.*
- *Soporte de NTP.*
- *TCP /IP.*
- *DHCP.*
- *Marcado por URI*
- *Soporte de 802.1x, 802.1Q y 802.1p.*

o ***Características de Seguridad:***
- *Administración vía SSH y HTTPS.*
- *Administración con password vía menú o IP.*

o *Interfaces de red ethernet (100/1000Mbps).*
o *Soportar funcionolidad de ClearPath.*
o *Administración del sistema integrado al Telepresence Management Suite.*
o *Soporte de directorio local (contacto privados) y de directorio corporativo.*
o ***Energía eléctrica***
- *Alimentación energética PoE*
- *Fuente de poder 220VAC, 50/60Hz.*

o ***Temperatura y Humedad:***
- *Temperatura de 0°C a 40°C.*
- *Humedad Relativa 10% a 90%.*

o ***Cámara***
- *5x optical zoom.*
- *Apertura vertical 51.5°.*
- *Apertura horizontal de 83°.*
- *Apertura F 2.1.*

o ***Componentes: códec, cámara HD, control remoto, micrófonos, fuente de alimentación, kit de montaje.***
o ***Pantalla LED con las siguientes características***
- *Tipo de pantalla*
- *Tamaño de la pantalla (pulgada) 55"*
- *Tipo LED*
- *Resolución FULL HD*
- *Trumotion 120 Hz*
- *Panel IPS*
- *Sintonizador Digital*
- *Con entradas HDMI*
- *Con entrada USB 3.0*
- *Con entradas USB 2.0*
- *DivX*
- *Wifi*
- *Completa Navegación WEB*

ABSOLUCIÓN A LA OBSERVACIÓN N° 15 DE TELEFÓNICA DEL PERÚ SAA
Se confirma que se aceptan mejoras a las caraterísticas minimas solcitadas en bases como requerimiento tecnico minimo.

Garantía Comercial: *(36) Meses contados a partir de la entrega del informe de cumplimiento de las especificaciones técnicas por la unidad de Tecnologías de la Información del OSCE.*

6. *PRESTACIONES ACCESORIAS A LA PRESTACIÓN PRINCIPAL:*

6.1. Garantía Comercial de los bienes:

No aplica

6.2. Mantenimiento preventivo:

No aplica

7. *PLAN DE TRABAJO y ENTREGABLES:*

7.1. Plan de trabajo:

El postor deberá presentar un plan de implementación de los componentes de la solución en la sede principal de la OSCE, además del despliegue y puesta en marcha de los terminales de videoconferencia en todas las sedes solicitadas.
Fase inicial
- *El postor hará entrega del Plan de Trabajo, a los cinco (05) días contados desde el día siguiente de la firma del contrato, en el cual se incluirán todas las etapas del proyecto, tales como la entrega, instalación, configuración, puesta en funcionamiento, pruebas y todas aquellas realizadas para cada componente.*
- *El Plan de Trabajo deberá indicar con precisión la descripción de los procedimientos, recursos humanos, maquinarias, herramientas, instrumentos y otros que el postor utilizará en la instalación.*
- *Deberá contener como mínimo lo siguiente: Alcances del proyecto, Fases de la implementación, principales hitos, rutas críticas.*
- *Deberá realizar una presentación de esta fase con carácter de Transferencia de Conocimiento.*

Fase final
- *Deberá realizar una presentación técnica al finalizar la implementación, formalizando la entrega de la solución operativa.*
- *Deberá realizar una presentación de esta fase con carácter de Transferencia de Conocimiento.*

7.2. Entregables:

- *Plan de trabajo en formato escrito y digital.*
- *Documento técnico con el detalle de la solución propuesta.*
- *Informe técnico final de la solución, detalles de la operación y funcionamiento del equipamiento.*

ABSOLUCIÓN A LA CONSULTA N° 20 DE TELEFÓNICA DEL PERU SAA
Se confirma que el término "postor" se refiere al "contratista".

8. REQUISITOS DEL PROVEEDOR:

8.1. Del Proveedor:

El proveedor deberá de cumplir con los siguientes requisitos:
- *El Proveedor deberá tener autorización para brindar Servicios de Telecomunicaciones en el país, deberá adjuntar autorización del MTC.*
- *Experiencia mínima de 3 años en proyectos similares de la marca ofrecida (se considerarán proyectos similares: Telefonía IP, Videoconferencia, Redes ó Networking). Acreditar con constancias, certificados, contratos en modalidad de venta o servicio con su respectiva conformidad o comprobantes de pago cuya cancelación se acredite fehacientemente.*
- *Experiencia en proyectos de transmisión de audio y video en tiempo real a través de cualquier media de transmisión (internet, redes privadas, televisión). Para acreditar esta experiencia el postor deberá presentar constancias, certificados, contratos en la modalidad de venta o servicio con su respectiva conformidad de culminación o mediante comprobantes de pago, cuya cancelación se acredite fehacientemente dentro de los últimos ocho años a la presentación de la propuesta, con un mínimo de 2 clientes y máximo de 10 clientes.*
- *El postor deberá contar con una Mesa de Ayuda (Help Desk) con un número telefónico para el reporte de fallas y gestión de incidentes 24x7.*

8.2. Del Personal:

El postor deberá asignar o incluir en el proyecto al personal que cuente con los siguientes requisitos mínimos:
- *Un (01) El Jefe de Proyecto a cargo de la implementación del servicio deberá de ser Ingeniero Electrónico o de Sistemas, titulado, colegiado y habilitado, con un mínimo de 5 años de experiencia en implementación de servicios de redes de voz, datos o video, en proyectos de Networking o de Telefonía IP. Deberá presentar constancias o certificados que acrediten tener conocimiento en el uso de metodologías de gestión de proyectos como ITIL, PMI.*
- *Dos (02) personas que implementará el proyecto, deberán de contar con experiencia laboral de más de 5 años en proyectos de instalación y soporte técnico a redes de voz, datos o video, pudiendo ser personal con estudios técnicos o universitarios.*

9. PLAZO DE ENTREGA:

Noventa (90) días calendarios desde el día siguiente de la firma de Contrato, según lo siguiente:
- *45 días para la entrega de equipos.*
- *45 días para la instalación y pruebas en todas las salas, plazo que se computará luego de la entrega de equipos.*

ABSOLUCIÓN A LA CONSULTA N° 14 y 15 DE TELEFÓNICA DEL PERÚ SAA
- La orden de compra será considerado como un contrato en modalidad de venta y debe cumplir con lo indicado en las bases.
- Se confirma lo indicado en las bases, es decir el jefe del proyecto deberá tener conocimiento en uso de metodología de gestión de proyectos, como ITIL, PMI, es decir ambos.

ABSOLUCIÓN A LA OBSERVACION N° 03 DE TELEFÓNICA DEL PERÚ SAA
De acuerdo a la Absolución a la Consulta número 15 de Telefónica del Perú, el Jefe de Proyectos debe tener conocimiento en el uso de metodologías de gestión de proyectos tales como ITIL y PMI. En relación a los conocimientos tales como PMI, se precisa que la acreditación correspondiente puede también realizarse mediante la presentación de la certificación PMP emitida por PMI.

10. LUGAR DE ENTREGA:

Todos los bienes deben ingresar al Almacén del OSCE, antes de ser instalados en su destino final. Almacén del OSCE (Sub – Lote 69-B Zona Comercial del conjunto Residencial San Felipe Edificio El Regidor, 6to. Piso – Jesús María).

11. FORMA DE PAGO:

Previa entrega de equipos, instalación, funcionamiento y conformidad del área usuaria, según lo siguiente:
Primer Pago: 80% previa entrega de equipos y conformidad del área usuaria.
Segundo Pago: 20% al culminar la instalación y pruebas en todas las salas y conformidad del área usuaria.

12. INFORME DE CUMPLIMIENTO DE LAS ESPECIFICACIONES TÉCNICAS:

El seguimiento, control y evaluación de la prestación del servicio, así como también la conformidad de la prestación estará a cargo de la Unidad de Tecnologías de la Información del OSCE.

13. ADELANTOS:

La Entidad otorgará un adelanto directos hasta por el 30% del monto del contrato original.
El contratista conjuntamente con los documentos para la suscripción del contrato, deberá presentar a la entidad la carta fianza que garantice el adelanto solicitado, adjuntando el comprobante de pago correspondiente. De no presentar la carta fianza por adelanto, no se atenderá el adelanto.
La Entidad debe entregar el monto solicitado dentro de los quince (15) días calendarios siguientes de la presentación de la carta fianza.
En el supuesto que los adelantos no se entreguen en la oportunidad prevista, el contratista tendrá derecho a solicitar la ampliación del plazo de ejecución de la prestación por el número de días equivalente a la demora, conforme al artículo 172 del Reglamento."

14. MODALIDAD DE EJECUCIÓN CONTRACTUAL

"Llave en mano", en virtud de que el proveedor ofrece los bienes, su instalación y puesta en funcionamiento, incluyendo todos los accesorios, repuestos, equipamiento, servicios u otros requeridos para el correcto funcionamiento de la solución.

ABSOLUCIÓN A LA CONSULTA N° 13 DE TELEFÓNICA DEL PERÚ SAA
Teniendo en cuenta que la solución a implementar debe ser "llave en mano", se confirma que el traslado hacia el destino final forma parte los costos que deberá incluir el postor.

10. LUGAR DE ENTREGA:

Todos los bienes deben ingresar al Almacén del OSCE, antes de ser instalados en su destino final. Almacén del OSCE (Sub – Lote 69-B Zona Comercial del conjunto Residencial San Felipe Edificio El Regidor, 6to. Piso – Jesús María).

11. FORMA DE PAGO:

Previa entrega de equipos, instalación, funcionamiento y conformidad del área usuaria, según lo siguiente:
Primer Pago: 80% previa entrega de equipos y conformidad del área usuaria.
Segundo Pago: 20% al culminar la instalación y pruebas en todas las salas y conformidad del área usuaria.

12. INFORME DE CUMPLIMIENTO DE LAS ESPECIFICACIONES TÉCNICAS:

El seguimiento, control y evaluación de la prestación del servicio, así como también la conformidad de la prestación estará a cargo de la Unidad de Tecnologías de la Información del OSCE.

13. ADELANTOS:

La Entidad otorgará un adelanto directos hasta por el 30% del monto del contrato original.
El contratista conjuntamente con los documentos para la suscripción del contrato, deberá presentar a la entidad la carta fianza que garantice el adelanto solicitado, adjuntando el comprobante de pago correspondiente. De no presentar la carta fianza por adelanto, no se atenderá el adelanto.
La Entidad debe entregar el monto solicitado dentro de los quince (15) días calendarios siguientes de la presentación de la carta fianza.
En el supuesto que los adelantos no se entreguen en la oportunidad prevista, el contratista tendrá derecho a solicitar la ampliación del plazo de ejecución de la prestación por el número de días equivalente a la demora, conforme al artículo 172 del Reglamento."

14. MODALIDAD DE EJECUCIÓN CONTRACTUAL

"Llave en mano", en virtud de que el proveedor ofrece los bienes, su instalación y puesta en funcionamiento, incluyendo todos los accesorios, repuestos, equipamiento, servicios u otros requeridos para el correcto funcionamiento de la solución.

15. PENALIDADES APLICABLES:

1.1. ***Penalidades por mora:***

15. PENALIDADES APLICABLES:

1.1. Penalidades por mora:

De acuerdo a los establecido en el artículo 165 del reglamento de la Ley de Contrataciones del Estado.

1.2. Otras penalidades:

No aplica

16. CONFIDENCIALIDAD:

El Proveedor se compromete a mantener en reserva, y no revelar a tercero alguno sin previa conformidad escrita del OSCE, toda información que le sea suministrada por este último.
El Proveedor se compromete a no revelar ni permitir la revelación de cualquier detalle a los medios de prensa o a terceros, a no revelar que el OSCE es cliente del Proveedor, y a no usar el nombre del OSCE en cualquier promoción, publicidad o anuncio, sin previa autorización escrita del OSCE.

17. RESPONSABILIDAD POR VICIOS OCULTOS:

Un año (01), contado a partir de la conformidad otorgada. Confidencialidad y reserva absoluto en el manejo de información y documentación a la tenga acceso y que se entre relacionada con la prestación, pudiendo quedar expresamente prohibido revelar dicha información a terceros.

18. ANEXOS:

Anexo N° 1: Relación de oficinas desconcentradas del OSCE.

Vº Bº Y SELLO
JEFE DEL ÁREA USUARIA

Anexo N° 1: Relación de oficinas desconcentradas del OSCE.

	Dirección	Distrito	Provincia	Departamento
1	Jr. Morona 881, Mz. C Lt 2, Urb Las Palmeras	Iquitos	Maynas	Loreto
2	Av. Tacna 876 (CONECTAMEF)	Chiclayo	Chiclayo	Lambayeque
3	Las Geranios Mz. Ñ, Lt.9, Urb. Miraflores (CONECTAMEF)	Castilla	Piura	Piura
4	Calle Oswaldo Baca Nº 305, Cdra 2	Cusco	Cusca	Cusco
5	Jr. Zepita Nº 489	Trujillo	Trujillo	La Libertad
6	Av. República de Uruguay 540, Urb. San José de Pichus	Huancayo	Huancayo	Junín
7	Jr. Agustín Gamarra Nº 145 (CONECTAMEF)	Cercado	Huancavelica	Huancavelica
8	Calle San Cristobal Nº 112, Urb. San Carlos (CONECTAMEF)	Cajamarca	Cajamarca	Cajamarca
9	Jr. Juan Bautista Mejía Nº 879	Huaraz	Huaraz	Ancash
10	Jr. 28 de Julio 167 (CONECTAMEF)	Huamanga	Huamanga	Ayacucho
11	Jr. Damaso Beraun 1038 (CONECTAMEF)	Huánuco	Huánuco	Huánuco
12	Av. Jerónimo de Carrera 860, Urb. Luren (CONECTAMEF)	Ica	Ica	Ica
13	Jr. San Martín 621, Barrio Partido Alto (CONECTAMEF)	Tarapoto	Tarapoto	San Martin
14	Jr. Gonzales Prada Nº 347 (CONECTAMEF)	Tambopata	Puerto Maldonado	Madre de Dios
15	Calle Manscal Castilla 122 (CONECTAMEF)	Tacna	Tacna	Tacna
16	Jr. Huáscar 673 (CONECTAMEF)	Calleria	Pucallpa	Ucayali
17	Calle Francisco Navarrete 111 (CONECTAMEF)	Tumbes	Tumbes	Tumbes
18	Urb. Casa del Banco de la Nación B-3 Cercado (CONECTAMEF)	Abancay	Abancay	Apurimac
19	Jr. Independencia 170-B (CONECTAMEF)	Puno	Puno	Puno
20	Av. Lambramani Lt. 2, Urb. Santo Domingo	José Luis Bustamante y Rivero	Arequipa	Arequipa

ANEXO B

RFP SOLICITUD DE PROPUESTA - PROPUESTA: VIDEOCONFERENCIA

El presente anexo es una parte de los términos de referencia del concurso Propuesta Videoconferencia de la empresa: BANCO DE CRÉDITO DEL PERÚ, en la cual el investigador tuvo participación directa en el diseño. Se adjunta con fines educativos para apoyar la experiencia del investigador en el diseño de Sistemas de Videoconferencia.

RFP
Solicitud de propuesta

Propuesta: Videoconferencia

Fecha: 28, marzo, 2014

Tipo de Solicitud:

() Suministro
(X) Aquisición de Bienes
() Consultoría
() Tercerización de Desarrollo
(X) Servicios

Índice

1. Declaración de Confidencialidad

El postor debe observar y mantener de manera confidencial, toda la información obtenida por o de cualquier medio, fuente, modo o lugar, derivada o relacionada directa o indirectamente del presente proyecto, así como la información relacionada a los proyectos y actividades que directa o indirectamente realice El Banco.

El postor deberá limitar el acceso a la Información a sus empleados, funcionarios, ejecutivos, accionistas, socios, directores o representantes que en forma razonable sea necesario que la conozcan, haciéndoles partícipes y obligados solidarios con aquella, respecto de sus obligaciones de confidencialidad aquí especificadas. Cualquier persona que tuviere acceso a la Información, deberá ser advertida de este compromiso de confidencialidad.

Ninguna información que fuere otorgada por los representantes de El Banco podrá ser copiada o reproducida en forma alguna a no ser que existiera autorización previa y por escrito concedida por éstos.

2. Consideraciones del Servicio

2.1 Descripción del Bien o Servicio

El desarrollo y crecimiento del BCP ha elevado las necesidades de comunicación de las diversas Unidades de Negocio de El Banco. Optimizar las horas hombre así como evitar engorrosos desplazamientos para importantes reuniones han motivado el uso y crecimiento de la plataforma de videoconferencia con la que hoy en día cuenta El Banco.

Dado que esta solución viene colaborando con la eficiencia del trabajo de nuestros funcionarios se necesita crecer en infraestructura tanto a nivel de plataforma como de puntos remotos, siempre en la búsqueda de optimización de recursos. El desarrollo de la plataforma de videoconferencia les brindará a todos los colaboradores mayores posibilidades de comunicación presencial remota.

Adicionalmente, se requiere distribuir el sistema de comunicaciones Cisco Unified Communication Manager (CUCM) en cuatro sedes para aumentar las disponibilidad del servicio e integrar la voz y video en una arquitectura altamente disponible, escalable y de gestión centralizada.

2.2 Alcance del Servicio

- Implementación de equipos para brindar alta disponibilidad de los Firewall Travesal ubicados en los centros de cómputo de La Molina y Chorrillos.

- Implementación de aplicación para el control y gestión de uso de las licencias necesarios para el establecimiento de sesiones de video conferencia multipunto.

- Implementación de nuevo equipamiento para la habilitación de salas de video conferencia.

- Servicos de instalación y configuración para la distribución de 6 servidores que conforman el CUCM en las sedes de La Molina, Chorrillos, Arequipa y Trujillo.

- Habilitación de apliaciones en CUCM:

    - Attendant Console.
    - Contact Center Express.
    - Presence Server.

- Entregables del proyecto:

    - Plan de trabajo de implementación.
    - Plan de capacitacion.
    - Documentacion de cierre de proyecto

2.3 Especificaciones Tecnicas y Funcionales

- **2 equipos de Video Communication Server Expressway**

    - Debe contener la funcionalidad Firewall Traversal Avanzado, a fin de negociar la conexión con cualquier tipo de firewall, esto permitirá que nuestra red de videoconferencia pueda conectarse con plataformas externas.
    - Permitir optimización de ruteo.
    - Debe otorgar robustez de seguridad a nuestra red de videoconferencia para cuando tenga que conectarse con una red externa.
    - Compatible con cualquier dispositivo de videoconferencia que utilice los protocolos SIP o H323.
    - Manejar señalización de marcado externo.
    - Permitir el registro de endpoints remotos que se encuentren en internet.
    - Debe contener licenciamiento para llamadas de 10 equipos que se encuentran en internet.
    - Soporte para direccionamiento DNS, IPv4 e IPv6.
    - Capacidad de hasta 100 llamadas trasversal.
    - Administración segura vía HTTPS, SSH.
    - Permitir la configuración de clusters de VCS Expressway.
    - Soportar protocolos H460.18/19 y ASSENT para optimizar comunicaciones entre los equipos de control y los firewall traversal.
    - Debe poder compartir licencias dentro de un cluster.
    - Replicar configuraciones dentro de un cluster.

- **1 equipo de Telepresence Conductor**

  - Soportar de una manera simple, confiable y eficiente sesiones de Telepresencia multisite y sesiones de colaboración por videoconferencia.
  - Simplificar sesiones de videoconferencia multisite organizando los recursos necesarios para cada sesión de manera independiente.
  - Soporte e interacción con un amplio rango de MCUs y servidores de Telepresencia.
  - Soportar diferenciación de servicio que permita a los administradores definir clases de servicio a cada una de las videoconferencias establecidas.
  - Permitir el crecimiento dinámico de las conferencias aun cuando la capacidad individual de los MCUs y servidores de Telepresencia se exceda.
  - Optimización de los puertos MCU permitiendo que según el equipo de telepresencia que se conecte se le asigne un puerto por tipo de resolución del dispositivo (FullHD, HD, SD, 360 pixel o inferiores)
  - Realizar cascadas entre los equipos de MCU o TPS.

- **Licencias de Videoconferencia**

  - 20 licencias de softclient de video con funcionalidad de firewall traversal:
    - Resolución HD.
    - Protocolo de señalización SIP.
    - Identificación por SIP URI.
    - Soportar funcionalidad de ClearPath.
    - Integración nativa con Telepresence Management Suite.
  - 03 Licencias de screen para Telepresence Server 7010.

- **20 Headset Plantronics Voyager Pro UC.**

  - Responder automáticamente las llamadas con sólo colocarlo en el oído.
  - Transferir automáticamente las llamadas entre el teléfono móvil y el auricular.
  - Evita la marcación accidental mientras no se lleva puesto el auricular mediante el bloqueo del botón de llamada.
  - Doble micrófono con anulación de ruido para que ofrezca una calidad de voz nítida entre ambas partes.
  - Debe permitir escuchar transmisiones multimedia, incluidas canciones, podcasts, indicaciones de navegación y mucho más.
  - La conectividad con múltiples dispositivos permite gestionar las llamadas de ordenador y teléfono móvil desde un único auricular.
  - Sistema de alertas que anuncian el tiempo de conversación restante, el estado de conexión, el nivel de la batería y la función mute.

- **Renovación de servicio Cisco Webex.**

  - Se require la renovación del servicio Cisco Webex por 25 licencias por un periodo de 12 meses.

El proveedor debe considerar los servicios profesionales por la instalación, configuración y despliegue de los equipos antes mencionados exceptuando los headset Plantronics.

2.4 Descripción Servicios Profesionales CUCM

2.4.1 Descentralización de servidores

A continuación se detallan los servicios profesionales de configuración para la implementación de la solución propuesta:

- Actividades para mitigar los riesgos de migración:
  - Coordinación de las ventanas de trabajo.
  - Respaldo previo de toda la configuración registrada en el Communication Manager (CM).
  - Ambas versiones del CM estarán disponibles en el servidor, en caso, la nueva versión presente problemas se podrá aplicar rollback.

- Instalación y configuración de 6 servidores UCS C220 M3:
  - Verificación del hardware.
  - Configuración del sistema operativo ESXi 5.x.
  - Configuración del puerto de gestión del servidor UCS Cisco.
  - Configuración e instalación de las siguientes máquinas virtuales:
    - Servidor 1 (La Molina):
      - ✓ Máquina Virtual 1: CUCM 8.6 Publisher.
      - ✓ Máquina Virtual 2: CUCM 8.6 Subscriber 1.
      - ✓ Máquina Virtual 3: Unity Connection 1.
    - Servidor 2 (La Molina):
      - ✓ Máquina Virtual 1: CUCM 8.6 TFTP 1.
      - ✓ Máquina Virtual 2: CUCM 8.6 Subscriber 2.
    - Servidor 3 (Chorrillos):
      - ✓ Máquina Virtual 1: CUCM 8.6 Subscriber 3.
      - ✓ Máquina Virtual 2: Unity Connection 2.
    - Servidor 4 (Chorrillos):
      - ✓ Máquina Virtual 1: CUCM 8.6 TFTP 2.
      - ✓ Máquina Virtual 2: CUCM 8.6 Media Resource.
      - ✓ Máquina Virtual 2: CUCM 8.6 Subscriber 4.
    - Servidor 5 (Trujillo):
      - ✓ Máquina Virtual 1: CUCM 8.6 Subscriber 5.
    - Servidor 6 (Arequipa):
      - ✓ Máquina Virtual 1: CUCM 8.6 Subscriber 6.

- Configuración de los servidores Communication Manager 8.6
  - Back up del actual Communication Manager.
  - Copia del back up a las nuevas máquinas virtuales.
  - Configuración e implementación de las particiones, regiones y enrutamiento de llamadas de las nuevas zonas.
  - Reiniciar todos los servicios del Communication Manager.
  - Revisar que todas las aplicaciones funcionen correctamente.
  - Back up del Call Manager durante la etapa de implementación.

- Configuración y upgrade del Unity Connection:
  - Back up del actual Unity Connection 7.1.5
  - Creación de la nueva máquina virtual e instalación de nuevo Unity Connection 8.6.
  - Upgrade de las licencias actuales a través del Cisco License.
  - Registro de las nuevas licencias.
  - Copia del back up a las nuevas máquinas virtuales.
  - Integración con la nueva central Communication Manager.
  - Reiniciar todos los servicios del Unity Connection.
  - Revisar que todas las aplicaciones funcionen correctamente.
  - Back up del Unity Connection durante la etapa de implementación.

2.4.2 Aplicación Attendant Console

- Instalación y configuración de 01 servidor UCS C200M2:
  - Verificación del hardware.
  - Configuración del Sistema Operativo ESXi 4.1.
  - Configuración del puerto de gestión del servidor UCS Cisco.
  - Instalación de aplicaciones de Attendant Console.

- Instalación y Configuración de Enterprise Attendant Console 8.6:
  - Instalación y configuración del sistema operativo Windows Server 2008 y SQL 2008
  - Instalación y configuración de la aplicación Attendant Console 8.6
  - Integración con los servidores de telefonía IP CUCM 8.6.
  - Confifuración de las colas de llamadas (llamadas internas y llamadas externas).
  - Configuración de las cinco operadoras, horarios nocturnos, sobrecarga de una cola,entre otros.
  - Integración con el directorio corporativo del BCP.
  - Configuración de los números de parqueo de llamada, llamadas en esperas, estado de presencia de todos los usuarios corporativos.
  - Es responsabilidad del BCP proporcionar PC's que cumplan con los requerimientos de instalación (todas las operadoras se encontrarán fisicamente en un solo lugar).

2.4.3 Aplicación Contact Center Express

- Instalación y configuración de 01 servidor UCS C200M2:
  - Verificación del hardware.
  - Configuración del Sistema Operativo ESXi 4.1.
  - Configuración del puerto de gestión del servidor UCS Cisco.
  - Instalación de aplicaciones de Cisco Contact Center Express 8.5.

- Instalación y Configuración del Cisco Contact Center Express 8.5 (CCX 8.5):
  - Instalación y configuración del software del CCX 8.5.
  - Integración con los servidores de telefonía IP.
  - Configuración de la contestadora automática y llamadas en la cola de espera.
  - Configuración de un Auto Attendant básico (no IVR).
  - Configuración de los 9 agentes y 1 supervisora.
  - Configuración del script adecuado para el enrutamiento de las llamadas.
  - Configuración del enrutamiento de llamadas a los agentes.
  - Configuración de la aplicación para la generación de informes históricos (informes predefinidos por el sistema).
  - Backup del Cisco Contact Center durante la etapa de implementación.

- La implementación brindará las siguientes funcionalidades:
  - Contestadora automática y llamada en la cola de espera.
  - Aplicación en las PCs de dos agentes y una supervisora.
  - Enrutamientode las llamadassegún habilidades de las agentes o por disponibilidad.
  - Modificar su disponibilidad o estado.
  - Generación de informes predefinidos en el sistema Contact Center.

2.4.4 Integración de Cisco Unified Presence con plataforma de comunicaciones de voz y video

- Configuración de 1 servidor UCS C200M2 de propiedad del BCP:
  - Verificación del hardware.
  - Configuración del sistema operativo ESXi 5x.

- Configuración de la aplicación:
  - Instalación y configuración de IM&Presence 9.x.
  - Integración con los servidores de Telefonia IP CUCM 9.x.
  - Configuración del estado de presencia de los contactos que tienen teléfonos IP.
  - Configuración de 1000 terminales Jabber con funcionalidades de comunicaciones unificadas.
  - Configuración de 50 clientes Jabber en los terminales móviles (PC, MAC, Android, iphone, ipad) con funciones de voz, video, presencia y mensajería instantánea.
  - Construcción de una guía de usuario personalizada para el uso en BCP:
    - Pruebas para verificar el funcionamiento los siguientes funcionamientos:
      - ✓ Conocer el estado de otros usuarios en tiempo real.

- ✓ Realizar llamadas, transferencias y conferencias de voz por el cliente de mensajería.
- ✓ Revisión de los mensajes de correo de voz.
- ✓ Interacción instantánea y eficiente.
- ✓ Estado de presencia personalizable.
- ✓ Iniciar la comunicación usando chat, voz y video.
- ✓ Gestión de contactos con los grupos personales.
- ✓ Chat y registro de llamadas.
- ✓ Directorio Corporativo.
- ✓ Encriptación punto a punto y chat de grupo.
- ✓ Compartir contenido y video en simultáneo.

Si existiera algún licenciamiento, software o hardware no mencionado en el documento y sea indispensable para la implementación de la solución planteada considerarlo dentro de la cotización.

El Banco podrá solicitar en cualquier momento la sustentación de las certificaciones del personal del proveedor.

El postor deberá garantizar una eficiente gestión del proyecto empleando una adecuada metodología en manejo de proyectos acorde al requerimiento. Asimismo, deberá manejar la documentación apropiada, estableciendo conjuntamente con El Banco mecanismos de control, avances y entregables periódicos de acuerdo al avance del proyecto.

Las pruebas de instalación, integración, y la puesta en servicio de la plataforma de comunicaciones son responsabilidad del postor.

2.5 Servicios de Implementación, Soporte, Documentación y Capacitación

A partir de la adjudicación del proyecto el proveedor deberá garantizar que el equipamiento se entregue en un plazo no mayor a 50 días calendario y los servicios profesionales relacionados a la plataforma CUCM en un plazo no mayor a 15 días.

Por lo que luego de la adjudicación deberán enviar a El Banco en un plazo no mayor a 5 días calendario los requerimientos técnicos para la implementación de lo requerido.

a) Implementación/Migración y pruebas

En esta fase el proveedor realizará la implementación y las pruebas de acuerdo a lo definido en los documentos de Plan de Implementación y Plan de Pruebas.

b) Servicios de soporte y mantenimiento

El servicio de soporte debe ser brindado por el integrador con capacidad de involucrar al servicio de post-venta del fabricante en caso sea necesaria su participación, sin costo alguno.

Para todos los equipos que serán instalados, el mantenimiento correctivo se debe efectuar en el mismo local de la incidencia en la modalidad 24x7.

El servicio de garantía y soporte se brindará de acuerdo a los tiempos establecidos de este documento.

Asimismo debe comprender al menos las siguientes actividades:

- Atención de llamadas de El Banco relacionadas a incidentes de hardware y software de la solución provista.
- Gestión del problema reportado usando herramientas proporcionadas por el fabricante.
- Entrega de un informe en el que se detallen las causas de la avería y acciones tomadas para resolverlo.

c) Personal

El postor deberá incluir como parte del equipo que realizará el servicio de gestión, instalación, configuración e implementación de toda la solución propuesta a los siguientes recursos:

- Un (01) Jefe de proyecto: Deberá ser profesional titulado en Ingeniería Electrónica o carreras afines, colegiado y habilitado con Certificación (Project Management Professional) o una constancia de haber llevado un curso de Gestión de Proyectos (PMI) dictado por un centro de educación autorizado (REP) con una duración no menor de 40 horas. Deberá acreditar un mínimo de tres (3) años de experiencia en la gestión de proyectos, presentar certificados y/o constancias de trabajo en el que se indique el tiempo y el cargo ocupado.

- Un (01) Especialista: Deberá ser un profesional titulado y/o bachiller en Ingeniería Electrónica o carreras afines. Deberá acreditar un mínimo de tres (03) años de experiencia en implementaciones similares. Presentar certificados y/o constancias de trabajo en el que se indique el tiempo y el cargo ocupado.

- Las carreras que puedan presentarse como afines son las siguientes:
  - Ingeniería de Sistemas e Informática.
  - Ingeniería Electrónica y Telecomunicaciones.
  - Ingeniería Industrial.
  - Ingeniería Informática.
  - Ingeniería Electrónica.
  - Ingeniería de Telecomunicaciones.
  - Ingeniería Electrónica con mención en Telecomunicaciones.
  - Ingeniería de Sistemas Empresariales.
  - Ingeniería Industrial y de Sistemas.

- Ingeniería de Software.
- Ingeniería de Sistemas de Información.
- Ingeniería de Telecomunicaciones y Redes.
- Ingeniería de Computación y de Sistemas.
- Ingeniería Informática y de Sistemas.
- Ingeniería de Redes y Comunicaciones.
- Ingeniería de Seguridad Informática.
- Ingeniería de Sistemas.

El BCP podrá solicitar en cualquier momento la sustentación de las certificaciones del personal del proveedor.

El postor deberá incluir como parte de su propuesta un ingeniero residente a tiempo completo el cual laborará en las instalaciones de El Banco, quien deberá monitorear, realizar configuraciones y demás que sea necesario para el adecuado funcionamiento de la solución. Este ingeniero deberá permanecer 30 días después de la firma del acta de aceptación de la implementación. El Banco se encargará de proveer las facilidades para el desarrollo de sus funciones.

d) Documentación

Entregables del proyecto:

- Plan de Trabajo de Implementación y Migración.
- Plan de Pase a Producción.
- Plan de soporte durante Migración y Post – Producción.
- Plan de capacitación.
- Documentación de cierre de proyecto

El postor deberá entregar a la entidad una copia original de la media y otros materiales de software de instalación, configuración y administración una vez instalada la solución.

e) Capacitación

El proveedor de la solución, deberá capacitar a 4 personas en la instalación, configuración y resolución de problemas para la plataforma de videoconferencia y plataforma CUCM. La duración total del curso no debe ser menor a 24 horas efectivas y será curso ofrecido por el fabricante directamente.

Asimismo se deberá capacitar localmente a 2 personas técnicas en el empleo de las herramientas de administración de toda la plataforma de comunicaciones por un mínimo de 16 horas.

2.6 Condiciones de Entrega del Bien

La entrega de equipos deberá realizarse en un plazo no mayor a 50 días en el almacén de El Banco, sito en Av. Separadora 2493/2495, Calle los Calderos 101, Urbanizacion Vulcano en una (01) sola entrega.

El horario de atención es de lunes a viernes de 9:00am a 6:00pm.

2.7 Garantías, Soporte,cobertura

2.7.1 Garantía y Soporte

El Servicio de Mantenimiento a la solución propuesta se brindará durante el periodo de garantía (y soporte) de doce (12) meses y se iniciará desde la firma del acta de aceptación de la implementación.

El servicio de soporte debe ser brindado por el integrador, pero con capacidad de involucrar al servicio de post-venta del fabricante en caso sea necesaria su participación, sin costo alguno.

Para todos los equipos que serán instalados, el mantenimiento correctivo se debe efectuar en el mismo local de la incidencia en la modalidad 24x7.

El servicio de garantía y soporte se brindará de acuerdo a los tiempos establecidos de este documento. Asimismo, debe comprender al menos las siguientes actividades:

- Atención a llamadas de El Banco relacionadas a incidentes de hardware y software de la solución provista.
- Gestión del problema reportado usando herramientas proporcionadas por el fabricante.
- Entrega de un informe en el que se detallen las causas de la avería y acciones tomadas para resolverlo.

La garantía y soporte de los equipos se contabilizará desde la firma del acta de conformidad de la implementación final de la solución.

El postor efectuará actualizaciones de software si y sólo si dicha actualización es necesaria para dar solución a un incidente reportado.

El postor deberá poner a disposición de El Banco un número directo de reporte de llamadas en la modalidad 24x7 para la atención de los incidentes que se presenten (indisponibilidad del servicio, averías, etc.) en la solución ofertada. Este número telefónico será el único punto de contactoentre El Banco y el postor.

2.7.2 Pólizas

El proveedor deberá contratar las siguientes pólizas:

Póliza de Responsabilidad Civil

Esta Póliza cubre los daños materiales y/o personales que el personal propio y/o contratado del proveedor, puedan ocasionar a terceros (clientes del banco) durante el desarrollo de las responsabilidades encomendadas por El Banco.

- Póliza de $200,000.
- El BCP tiene que estar nombrado como asegurado adicional o tercero beneficiario.
- En la Póliza se debe incluir la Cláusula de Responsabilidad Civil Cruzada entre el BCP y el Proveedor (El BCP es Tercero para los daños que cometa el Proveedor contra el BCP).
- Debe incluir Cláusula de Responsabilidad Civil Patronal.

Póliza de Deshonestidad

La cobertura de deshonestdad cubre las pérdidas que pueda sufrir El Banco por la apropiación de dinero en efectivo, valores, mercancías, efectos, documentos realizada por un acto deshonesto de los empleados y dependientes a su servicio.

- Póliza de $20,000.
- Incluir la siguiente condición especial: "El Convenio I de la presente póliza se amplía a cubrir la apropiación ilícita y/o actos deshonestos que cometa el personal del Asegurado sobre los bienes de propiedad del Banco de Crédito del Perú, mientras efectúa operaciones, labores y/o cumplimientos del contrato entre el Asegurado y el Banco de Crédito del Perú"
- Incluir cláusula de Seguro Anterior: Se extiende a cubrir las pérdidas que, de no haber cesado o quedado cancelado el Periodo de Descubrimiento de la Póliza de Seguro inmediata anterior, hubiesen estado amparadas bajo los alcances de esa Póliza de Seguro Contra Deshonestidad inmediata anterior emitida a favor del ASEGURADO.

2.7.3 Homologación

De acuerdo a nuestras políticas de contratación de bienes y servicios, El Banco requiere que él o los proveedor(es) adjudicados inicien un proceso de homologación.
Una vez emitida la carta de adjudicación, El Banco comunicará al proveedor la empresa que realizará el proceso de homologación.
La homologación deberá estar vigente durante el servicio contratado y deberá realizarse dentro de los primeros 2 meses de otorgado el servicio.
El costo de este proceso, así como, sus renovaciones anuales correrán a cuenta del proveedor.

2.8 Niveles de Servicio y Penalidades

2.8.1 Niveles de Servicio (SLA)

El propósito del SLA es asegurar una excelente calidad del servicio con precios razonables brindados por el Proveedor. La empresa involucrada deberá hacer uso de los resultados mensuales del SLA para mejorar el servicio brindado.

El Proveedor debe administrar los servicios, empleando las mejores prácticas, con la finalidad de lograr una satisfacción comprobada de los usuarios de El Banco. El nivel de satisfacción y los mecanismos de medición, se establecerán dependiendo de cada indicador.

- **Entrega de Equipos**

  El indicador a medir es el siguiente:

  Tiempo de entrega: 50 días desde la emisión de la orden del pedido hasta que se reciben los equipos en el almacé del Banco.

- **Garantía de Equipos**

  El postor deberá garantizar los siguientes requerimientos de tiempos de respuesta para atención de fallas durante la vigencia de la garantía:

  Los indicadores a medir serán los siguientes:

  Tiempo de atención "En sitio" : Será máximo de 02 horas, transcurridos a partir de que el personal técnico de El Banco realice la llamada telefónica reportando el incidente hasta el momento en que el personal destacado por el postor se hace presente en las instalaciones de El Banco.

  Tiempo de respuesta de solución: Será máximo de 24 horas, transcurridos a partir en que el personal técnico de El Banco realice la llamada telefónica reportando el incidente, hasta el momento en que el postor resuelve el incidente. En caso de que el componente de hardware y/o software de la solución propuesta requiera una reparación mayor, éste deberá ser sustituido sin costo alguno para El Banco por un equipo igual o de mayores características durante el tiempo que demande su reparación.

- **Tiempo de servicios de instalación y configuración de equipos**

  El postor deberá garantizar que la fecha de fin de implementación del proyecto se cumpla.

- **Soporte SW**

Tiempo de Atención (TA)

Se entiende como tiempo de atención al tiempo tomado desde que la solicitud del servicio es recibida por EL PROVEEDOR hasta que el representante del servicio del PROVEEDOR se pone en contacto y a disposición del usuario correspondiente del Banco.

Indicador	Medición	Cumplimiento
Tiempo de Atención ante un incidente	2 horas	Mínimo 95%

Tiempo de Solución (TS)

Se entiende como tiempo de solución el tiempo contabilizado desde que se toma acción sobre el incidente reportado hasta que se soluciona el incidente. Este tiempo es adicional al tiempo de atención (TA).

Indicador	Medición	Cumplimiento
Tiempo de Solución ante un incidente.	24 Hr	Mínimo 95%

2.8.2 Penalidades

- **Entrega de Equipos**

Penalidad: Incumplimiento de Tiempo de Entrega

La penalidad será aplicada a los equipos que no lleguen en los 50 días, en base a:

Monto = ∑ (Monto Total de Factura del Lote a penalizar).

Cálculo de Penalidad = Monto x % Penalidad

Rango de Cumplimiento	% Penalidad
Retraso a partir de 15 días calendario	2.5%
Retraso de 30 días calendario	5%
Retraso más de 30 días calendario	10%

3. Criterios a Evaluar

- Precio por equipo.
- Cumplimiento de especificaciones técnicas mínimas.

- Costos de H-H por rol.
- Costos de licencia.
- Ratio de mantenimiento.
- Valor agregado de especificaciones técnicas y otros.
- Cumplimiento de SLA y penalidades.
- Plazos de entrega.
- Experiencia del Proveedor.
- Salud Financiera del Proveedor.

4. Consideraciones de la Licitación

El objetivo del Concurso es cotizar el servicio requerido por El Banco y que los Postores puedan ofrecer las mejores alternativas. El hecho de recepcionar y aceptar las propuestas de los Postores, no significará que El Banco estará obligado a contratar a algunos de éstos.

5. Requisitos para participar en el Evento

Los Proveedores Potenciales serán empresas registradas en el portal de ARIBA que maneja el BCP, para lo cual deberán cumplir lo siguiente:

- Aceptar todas las condiciones del presente documento.
- Conocer y comprometerse a respetar las Condiciones de Uso y las Reglas y Reglamentos del Evento publicados en el Sitio ARIBA.
- Presentar las propuestas de acuerdo a los modelos exactos definidos. Los Postores que no que utilicen otros formatos no serán tomados en cuenta para la evaluación.
- Comprometerse a enviar una propuesta técnico - comercial en los términos descritos en este documento.
- La comunicación deberá ser por medio del portal ARIBA.
- El Postor deberá enviar los documentos solicitados en el evento INFORMACIÓN BÁSICA DE PROVEEDORES que será publicado en ARIBA para continuar su participación.

5.1. Calendario de Actividades

Hito	Fecha de término
Envío de RFP por parte de El Banco.	28/03/2014
Recepción de RFP y periodo de envío de dudas sobre el RFP por parte de los postores.	28/03/2014 – 02/04/2014
Respuesta a las dudas de los postores por parte de El Banco.	03/04/2014 – 04/04/2014

Hito	Fecha de término
Fecha límite para la recepción de propuestas técnico - comerciales de los proveedores.	11/04/2014

Las fechas están sujetas a cambios, de acuerdo a necesidades de El Banco.

5.2. Licitación y Adjudicación

Las propuestas que sean colocadas en la licitación se considerarán en firme. Es decir, los proveedores se comprometen a respetarlas. En caso surgiese algún problema con la propuesta del proveedor ganador, se adjudicará como ganador al proveedor que hubiese ocupado el segundo lugar en la licitación quien deberá respetar su último precio colocado.

La postura ganadora será aquella que contemple las mejores condiciones para El Banco, tanto comerciales como técnicas. Para las condiciones técnicas El Banco podrá asignar un puntaje a la propuesta de cada proveedor, en función a su propuesta presentada y en función a un Análisis de Valor, lo que los beneficiará en el desarrollo de la licitación. El Proveedor Ganador no necesariamente será el que ofrezca los costos más bajos.

5.3. Descalificación

Un postor puede ser descalificado durante el proceso del concurso si ocurre alguno de los siguientes eventos:

a. Incumple el Compromiso de Confidencialidad.

b. Provee información falsa o tendenciosa.

c. Trata de contactar a empleados o contratistas del BCP (que no sean los autorizados por BCP) durante el proceso de selección para obtener información que pudiera generar cualquier tipo de ventaja.

d. No cumple los hitos establecidos.

e. No sigue las instrucciones del concurso.

5.4. Entregables Técnico – Comerciales

En las fechas establecidas en el numeral anterior, los Proveedores potenciales deberán enviar sus propuestas por el portal ARIBA considerando que **el viernes 11/04/2014 como fecha máxima hasta las 05:00pm hora peruana.**

No se recibirán propuestas después de la fecha y hora de entrega indicada.

La propuesta estará conformada por: Propuesta Técnica y Propuesta Económica.

Propuesta Técnica

Deberá contener la siguiente información como mínimo:

a) Siguiente información por equipo:

- Especificaciones Técnicas.
- Garantía.

b) Aceptación de SLAs y Penalidades.

c) Aceptación de las garantías requeridas.

d) Procedimiento para ejecutar la garantía de todos los componentes de los equipos durante el tiempo de garantía.

Propuesta Económica

a) Para completar esta información, se solicita que completen el archivo adjunto en formato Excel (Ver ANEXO: EXCEL DE PROPUESTA ECONÓMICA).

b) Costos de H-H.

c) Aceptación de política de viáticos, hoteles y pasajes.

b) Servicios de Valor Agregado que forman parte de la oferta.

Forma de Entrega de las propuestas

Tanto la propuesta técnica como la económica deberán ser enviada por medio del portal ARIBA. No se recibirán ninguna propuesta que sea enviada por otro medio.

Cualquier aclaración adicional contactar a:

- Contacto del BCP: Karina Martinez Díaz.
- Mail: kmartinezd@bcp.com.pe.

En caso el Proveedor decidiera no participar en el presente evento, deberá presentar una carta indicando el motivo de la no participación en la fecha señalada para la presentación de propuestas, caso contrario no será considerado para posteriores licitaciones.

5.5. Aclaración de Dudas

Los Proveedores tendrán acceso en línea a un foro de preguntas y respuestas a través del portal ARIBA para aclarar dudas con respecto al Evento y al RFP. Se podrá acudir al foro en línea para

consultar las respuestas, así como para registrar sus preguntas. Todas las respuestas serán publicadas dentro del foro en línea.

Si como consecuencia del foro de preguntas y respuestas se debe modificar o añadir algún punto al RFP, se emitirá una nueva versión de RFP considerando dichas modificaciones. Esta nueva versión de RFP será finalmente la que rija el proceso.

6. Anexos

- ANEXO 1: CONTRATO MARCO

Contrato de Compraventa de Lice

- ANEXO 2: EXCEL DE PROPUESTA ECONÓMICA

Ficha_Propuesta_Económica_Videoconfer

BIBLIOGRAFÍA

[1] Bruno, A., & Jordan, S. (2011). CCDA 640-864 Official Cert Guide. Indianapolis, USA: Cisco Press.

[2] CCNA Security 640-554 Official Cert Guide2013IndianapolisUSACisco Press

[3] Cioara, J., & Valentine, M. (2012). CCNA Voice 640-461. Indianapolis, USA: Cisco Press.

[4] Finke, J., & Hartmann, D. (2012). Implementing Cisco Unified Communications Manager, Part 1 (CIPT1) Foundation Learning Guide (Segunda ed.). Indianapolis, USA: Cisco Press.

[5] Lammle, T., & Swartz, J. (2013). Introducing Cisco Data Center Networking (Exam 640-911) Study Guide. Indianapolis, USA: Sybex.

[6] Odom, W. (2008). CCENT/CCNA ICND1 Official Exam Certification Guide (Segunda ed.). Indianapolis, USA: Cisco Press.

[7] Odom, W. (2008). CCNA ICND2 Official Exam Certification Guide (Segunda ed.). Indianapolis, USA: Cisco Press.

[8] Tribunal del OSCE Quienes Somos

[9] Wallace, K. (2011). Implementing Cisco Unified Communications Voice over IP and QoS (CVOICE) Foundation Learning Guide (Cuarta ed.). Indiniapolis, USA: Cisco Press.