ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ANÁLISIS DE OPCIONES DE ACCESO DESDE INTERNET AL SERVICIO DE COMUNICACIONES UNIFICADAS CON CISCO

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

WINSTON ALEXANDER SÁNCHEZ MALDONADO
winston-sanchez@hotmail.com

DIRECTOR: PABLO WILLIAM HIDALGO LASCANO MSc.
pablo.hidalgo@epn.edu.ec

Quito, agosto 2018

AVAL

Certifico que el presente trabajo fue desarrollado por Winston Alexander Sánchez Maldonado, bajo mi supervisión.

PABLO HIDALGO MSc.
DIRECTOR DEL TRABAJO DE TITULACIÓN

DECLARACIÓN DE AUTORÍA

Yo, Winston Alexander Sánchez Maldonado, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

WINSTON ALEXANDER SÁNCHEZ MALDONADO

DEDICATORIA

Dedico este trabajo a mi mamá, Aracely Maldonado y a mi hijo Matías Sánchez, son lo mejor de mi vida y por ustedes quiero seguir adelante.

AGRADECIMIENTO

En primero lugar quiero agradecer a mi madre Aracely Maldonado y mi hermano Ricardo Sánchez, por su apoyo incondicional en todo momento. Gracias por creer en mí y darme la oportunidad de seguir mis estudios en la Escuela Politécnica Nacional.

A mi familia por su apoyo y consejos en todo momento, siempre pude contar con ustedes.

A mi novia María del Cisne Sarmiento, por su apoyo en todo momento, me diste fuerza y motivación para poder terminar este proyecto.

A mis compañeros de la EPN, que hicieron más llevadera la etapa universitaria.

Al Ingeniero Pablo Hidalgo, muchas gracias por su paciencia, su guía, por su dedicación y en especial por creer en mí.

ÍNDICE DE CONTENIDO

RESUMEN

El presente proyecto parte de una revisión de conceptos sobre Comunicaciones Unificadas (UC), sus componentes y protocolos. Luego se pasa a una explicación de la solución de Comunicaciones Unificadas con Cisco, principalmente en las características de Movilidad y Acceso Remoto.

En el capítulo 2 se define una empresa ficticia con un giro de negocio que demande movilidad en una solución de Comunicaciones Unificadas. Sobre la empresa definida se realiza el diseño de Comunicaciones Unificadas con Cisco, el mismo que sirve de base para la elaboración del prototipo UC.

El capítulo 3 es la implementación del prototipo de Comunicaciones Unificadas. El prototipo es implementado con los elementos necesarios para ofrecer las dos opciones de acceso desde Internet a servicios de Comunicaciones Unificadas corporativas.

Las pruebas del prototipo y análisis de resultados se presentan en el capítulo 4. Se realizan pruebas de funciones desde un cliente de *software* de Comunicaciones Unificadas; el análisis se lo establece en relación con el uso de las funciones de Comunicaciones Unificadas a través de dos métodos de acceso desde Internet, para poder determinar el mejor método.

El capítulo 5 corresponde a conclusiones y recomendaciones. En este capítulo se indican las conclusiones que surgieron del: diseño de la solución de Comunicaciones Unificadas para la empresa ficticia, la implementación del prototipo y la ejecución de pruebas. También cuenta con recomendaciones basadas en la elaboración del presente trabajo y en la experiencia con la solución de Comunicaciones Unificadas con Cisco.

En los anexos se presenta el proceso de instalación de cada elemento del prototipo de Comunicaciones Unificadas y el funcionamiento de VPNs de acceso remoto.

PALABRAS CLAVE: Cisco, Comunicaciones Unificadas, Cisco *Jabber*, *Expressway.*

ABSTRACT

The present project begins with a review of concepts on Unified Communications (UC), its components and protocols. Then it presents an explanation of the Unified Communications solution with Cisco, mainly on the characteristics of Mobility and Remote Access.

Chapter 2 defines a fictitious company with a business line that requires mobility in a Unified Communications solution. About the company defined a design with Cisco Unified Communications is performed, and serves as a basis for the development of the prototype UC.

Chapter 3 is the prototype implementation of Unified Communications. The prototype is implemented with the necessary elements to offer the two options of access from the Internet to corporate Unified Communications services.

The prototype tests and results analysis are performed in chapter 4. Function tests are performed from a Unified Communications software client, and the analysis is performed in relation to the use of the Unified Communications functions through the two methods access from the Internet and determine the best method.

Chapter 5 corresponds to conclusions and recommendations. This chapter presents the conclusions that emerged from: the design of the Unified Communications solution for the fictional company, the implementation of the prototype and test execution. It also has recommendations based on the preparation of this work and the experience with the Unified Communications solution with Cisco.

The process of installing each element of the Unified Communications prototype and the operation of remote access VPNs is presented in the annexes.

KEYWORDS: Cisco*, Unified Communications*, Cisco *Jabber*, *Expressway.*

1. INTRODUCCIÓN

1.1 Objetivos

1.1.1 Objetivo General

- Analizar las opciones de acceso desde Internet a servicios de Comunicaciones Unificadas con Cisco.

1.1.2 Objetivos Específicos

- Describir cómo se conforma una solución de Comunicaciones Unificadas con Cisco, y las opciones que ofrece para el acceso desde Internet a los servicios de comunicaciones unificadas.
- Diseñar un escenario que ponga a prueba las opciones de acceso soportadas en Comunicaciones Unificadas con Cisco.
- Implementar el prototipo de Comunicaciones Unificadas que sirva como escenario de prueba para evaluar las opciones de acceso soportadas por Cisco, a partir del diseño correspondiente.
- Analizar los resultados obtenidos a partir de la ejecución del protocolo de pruebas elaborado, sobre el funcionamiento de las dos opciones de acceso desde Internet al servicio de Comunicaciones Unificadas, implementadas en el prototipo de pruebas.

1.2 Alcance

En el presente proyecto, se parte de los fundamentos teóricos sobre Comunicaciones Unificadas, sus características y la solución de Comunicaciones Unificadas con Cisco. Se revisa el funcionamiento de dos métodos de acceso desde Internet hacia una solución de Comunicaciones Unificadas corporativa.

Se realiza el diseño de Comunicaciones Unificadas con Cisco para una empresa ficticia, el mismo que será tomado como base para la implementación del prototipo de Comunicaciones Unificadas. Los elementos del prototipo serán los mínimos y necesarios para probar los métodos de acceso desde Internet a la solución de Comunicaciones Unificadas corporativa.

Para el prototipo se contará con recursos para realizar su implementación con características de Comunicaciones Unificadas mínimas y ejecutar los dos métodos de acceso; con ello se podrá recolectar la información resultante de las pruebas del prototipo.

Las pruebas realizadas se complementarán con los resultados de una encuesta dirigida a usuarios técnicos y no técnicos que utilicen servicios de Comunicaciones Unificadas con Cisco. El resultado de la encuesta nos da información sobre la experiencia del usuario en cuanto al uso de la solución de Comunicaciones Unificadas.

1.3 Comunicaciones Unificadas [1]

Al considerar la definición de Comunicaciones Unificadas (UC), los líderes de la industria típicamente lo describen como las comunicaciones que se están integrando para optimizar los procesos de negocio. Esto significa que una organización puede integrar o unificar sin problemas sus procesos empresariales típicos con comunicaciones en tiempo real (como mensajería instantánea / chat, información de presencia, telefonía / VoIP, control de llamadas y videoconferencia) y comunicaciones que no son en tiempo real (como mensajería unificada - buzón de voz integrado, correo electrónico, SMS[1] y fax).

A menudo se supone que UC es un solo producto, pero en realidad UC se compone de un conjunto de productos que proporciona una interfaz de usuario coherente y unificada, y la experiencia del usuario a través de múltiples dispositivos y tipos de medios. En su sentido más amplio, la UC puede abarcar todas las formas de comunicaciones que se intercambian a través de la red TCP / IP (*Transmission Control Protocol/Internet Protocol*).

1.3.1 Componentes de una Solución de Comunicaciones Unificadas [2]

Entre los principales componentes de Comunicaciones Unificadas se encuentran: Control de Llamadas (IP PBX), Presencia, Mensajería Instantánea, Mensajería Unificada y Movilidad.

Control de Llamadas (IP PBX)

El Control de Llamadas se refiere al servicio de Telefonía y Video IP, que permite a los usuarios iniciar y mantener una comunicación de voz o video entre dos o más dispositivos finales.

Presencia

El servicio de Presencia permite a un usuario conocer la disponibilidad de otro usuario mediante aplicaciones y/o dispositivos que forman parte de la solución de Comunicaciones Unificadas (Teléfonos IP, *Softphones*, etc.).

[1] SMS: *Short Message Service*

Mensajería Instantánea

Es el componente que permite el intercambio de mensajes de texto mediante aplicaciones de software en tiempo real. La Mensajería Instantánea normalmente está complementada con el servicio de presencia que permite al usuario conocer la disponibilidad de otro usuario mediante la aplicación de envío de mensajes de texto.

Mensajería Unificada [3]

Se refiere a un buzón integrado donde el usuario puede acceder a distintos mensajes desde diferentes medios de comunicación. El buzón único por lo general es el buzón de correo electrónico, y comúnmente realiza la integración para poder recibir mensajes de voz y mensajes de FAX como adjuntos en un correo electrónico. Actualmente existe mayor desarrollo en las aplicaciones de Comunicaciones Unificadas para obtener el mensaje de voz desde cualquier dispositivo cliente sin tener que pasar por el acceso al correo electrónico.

Movilidad

En Comunicaciones Unificadas el componente de Movilidad ayuda a que los usuarios puedan utilizar los servicios de la solución desde cualquier lugar con acceso a la Red Corporativa.

Las soluciones de Comunicaciones Unificadas cuentan con productos que se integran con dispositivos móviles como *smartphones, laptops, tablets,* etc*,* y permiten que el usuario permanezca conectado.

Existen componentes que permiten a los usuarios utilizar el cliente software de Comunicaciones Unificadas para poder acceder a sus servicios desde fuera de la red corporativa.

1.3.2 Protocolos de Comunicaciones Unificadas

En Comunicaciones Unificadas, existen varios protocolos de comunicación que se utilizan para la correcta operación de cada elemento de la solución. Entre los principales se tienen a los siguientes:

Session Initiation Protocol (SIP) [4]

SIP es un protocolo, definido en el RFC 3261, que utiliza un esquema solicitud – respuesta, que permite establecer una llamada o sesión entre dos o más dispositivos finales.

En los mensajes que se intercambian en SIP, los usuarios son identificados con un formato de dirección, que es un formato similar a las direcciones de correo electrónico*, sip:<userID>@<domain>*. En la red de Telefonía IP, los usuarios SIP son contactados mediante el uso de un plan de marcado, en el cual se asigna un número de extensión que dirige la petición de inicio de sesión a una o varias cuentas SIP disponibles.

En una red SIP se identifican los siguientes componentes:

- SIP *Proxy Server*. - El servidor *Proxy* funciona como un dispositivo intermedio que recibe peticiones SIP de un cliente y luego reenvía las solicitudes en nombre del cliente. Los servidores *Proxy* pueden proporcionar funciones tales como autenticación, autorización, control de acceso a la red, enrutamiento, retransmisión de solicitud confiable y seguridad.
- *Redirect Server*. - El servidor de redireccionamiento proporciona al cliente información sobre el siguiente salto o saltos que debe llevar un mensaje, para que a continuación el cliente contacte directamente con el servidor del siguiente salto.
- *Registrar Server*. - El servidor procesa solicitudes de clientes SIP para el registro de su ubicación actual en la red. Los servidores de redirección o *Proxy* a menudo contienen servidores de registro.
- *User Agent* (UA). - UA comprende una combinación de agente de usuario cliente (UAC) y agente de usuario servidor (UAS) que inicia y recibe llamadas. Un UAC inicia una petición SIP, luego un UAS, contacta al usuario cuando recibe una petición SIP. El UAS responde entonces en nombre del usuario. En una solución de Comunicaciones Unificadas un dispositivo puede actuar como un servidor y como cliente y se denomina *Back-to-Back User Agent* (B2BUA).

H.323 [5]

La Unión Internacional de Telecomunicaciones (UIT) desarrolló la norma H.323 para las comunicaciones multimedia a través de redes de paquetes. Como tal, el protocolo H.323 representa un estándar de la UIT y proporciona interoperabilidad *multi - vendor*. El protocolo H.323 especifica todos los aspectos de los servicios de aplicaciones multimedia, señalización y control de sesión sobre una red de paquetes subyacente. Aunque el audio es estándar, en las redes H.323, se puede escalar para incluir vídeo y datos.

Media Gateway Control Protocol (MGCP) [4]

MGCP permite a un agente de llamadas controlar y administrar remotamente dispositivos de comunicación de voz y datos en el borde de la red IP. Debido a su arquitectura centralizada, MGCP simplifica la configuración y administración de *Gateways* de voz y admite múltiples agentes de llamada (redundantes) en una red. MGCP no proporciona mecanismos de seguridad como encriptación o autenticación de mensajes.

Skinny Client Control Protocol (SCCP) [4]

SCCP utiliza mensajes propietarios de Cisco para comunicarse entre dispositivos IP y una central de control de llamadas. SCCP coexiste fácilmente en un entorno de protocolos múltiples. Durante el registro, el teléfono IP recibe su línea y todas las demás configuraciones desde la central del control de llamadas en una solución de Comunicaciones Unificadas. Después de registrarse, el sistema lo notifica de nuevas llamadas entrantes, y puede realizar llamadas salientes. SCCP se utiliza para la señalización de llamadas VoIP y características mejoradas como el indicador de mensaje en espera (MWI).

Extensible Messaging and Presence Protocol (XMPP) [6]

XMPP es un conjunto de tecnologías para mensajería instantánea, presencia, llamadas de voz y video, colaboración y enrutamiento generalizado de datos XML.

XMPP fue desarrollado originalmente en la comunidad de código abierto de *Jabber* para proporcionar una alternativa abierta y descentralizada a los servicios de mensajería instantánea cerrados en ese momento.

1.3.3 Principales Empresas Fabricantes de Comunicaciones Unificadas [7]

De acuerdo con el cuadrante mágico de Gartner publicado en julio de 2017, las marcas líderes en Comunicaciones Unificadas son: Cisco, Microsoft y Mitel (ver Figura 1-1). En la publicación "*Magic Quadrant for Unified Communications*" se definen las siguientes fortalezas de cada una de las empresas fabricantes.

Cisco

Cisco es una empresa pública con sede en San José, California, Estados Unidos. Ofrece un conjunto interrelacionado de soluciones de UC (recientes y maduras) que abarca opciones de implementación locales, híbridas y en la nube.

Figura 1-1 *Magic Quadrant for Unified Communications* [7].

- **Fortalezas**
  - Cisco ofrece una *suite* de UC completa globalmente escalable, con una experiencia de usuario de calidad en todos los dispositivos móviles líderes, además de una sólida telefonía y capacidades de conferencia líderes en el mercado.
  - *Cisco Prime Collaboration* proporciona una gestión unificada de las redes de voz y vídeo: despliegue automatizado y acelerado; aprovisionamiento; monitoreo en tiempo real; solución proactiva de problemas; gestión de licencias; tendencias a largo plazo y análisis.

Microsoft

Microsoft es una compañía global con sede en *Redmond, Washington,* EE. UU., que ofrece una solución amplia de UC bajo la marca de *Skype for Business* (SfB). La solución UC *on-premises*[2] es *Skype for Business Server* (SfBS) y la solución UC

[2] *On-premise:* Se refiere a soluciones que se instalan localmente, o en instalaciones que pertenecen a la organización.

en la nube es *Skype for Business Online* (SfBO), que se licencia como parte de la cartera de Office 365. Un despliegue de SfBS, con significativamente más capacidades de telefonía que la solución SfBO, se ha puesto a prueba en el reemplazo de PBX de muchas organizaciones, y es crítico para diseños distinguir entre las dos soluciones cuando se considera reemplazar un sistema de telefonía tradicional. Microsoft también tiene algunas configuraciones adicionales de UC, especialmente *Skype for Business Hybrid*.

- **Fortalezas**
  - Microsoft puede agrupar *Skype for Business* con una amplia gama de productos empresariales, de colaboración y de oficina bien establecidos, lo que le permite aprovechar su dominio en las soluciones empresariales de IT y de oficina.
  - Microsoft ofrece un atractivo camino de soluciones que incluye *on-presmises, cloud* e híbridos. También cuenta con una sólida red de socios para abordar la diversa gama de requisitos empresariales a nivel mundial.

Mitel

Mitel es una compañía global con sede en *Ottawa, Ontario*, Canadá. Ofrece la *suite MiCollab de* UC*,* como la solución UC común a través de sus múltiples plataformas de administración de llamadas. Las plataformas principales de gestión de llamadas de Mitel son *MiVoice Business*, que apunta a las medianas o grandes empresas y *MiVoice MX-ONE* (del patrimonio de Aastra *Technologies*), que apunta a grandes y muy grandes empresas.

- **Fortalezas**
  - Mitel ha aumentado su competitividad global en EMEA (*Europe, the Middle East and Africa*) y Norteamérica durante los últimos dos años.
  - Con la adquisición de Maven (*Mitel Mobile*) en abril de 2015, que ofrece una solución de red basada en software para los operadores móviles, Mitel se posiciona dentro de las adyacencias de mercado para ofrecer servicios de comunicaciones de valor agregado para operadores móviles a medida que *VoLTE (Voice over Long-Term Evolution*) llega al mercado.
  - Las soluciones Mitel *MiCollab, MiVoice, MiTeam, MiContact Center* y *MiCloud* ofrecen una completa suite de software. Se basan en una arquitectura de software común y una experiencia de usuario consistente que se puede distribuir o centralizar en un centro de datos.

1.4 Comunicaciones Unificadas con Cisco

Los siguientes componentes pertenecen a una solución de Comunicaciones Unificadas con CISCO:

- *Cisco Unified Communications Manager* (CUCM).
- *Cisco Unity Connection* (CUC).
- *Cisco Unified IM and Presence* (CUCMIMP).
- *Gateway* de Voz Cisco.
- Dispositivos Finales de Comunicaciones Unificadas Cisco.

1.4.1 *Cisco Unified Communications Manager* (CUCM)

CUCM es el núcleo de la solución de Comunicaciones Unificadas con Cisco. Es el componente de control de llamadas, que ofrece servicios para la gestión de sesiones de voz, video, mensajería, movilidad y conferencias web.

CUCM soporta interoperabilidad con soluciones de otros fabricantes a través del manejo de comunicación con protocolos estándar; incluso soporta el registro de dispositivos finales SIP de terceros. Una solución con CUCM puede escalar hasta 40000 usuarios y soporta una extensión de hasta 80000 usuarios.

1.4.2 *Cisco Unity Connection* (CUC)

El componente CUC combina mensajería integrada y unificada, reconocimiento de voz, y transferencia de llamadas bajo una sola consola de administración. Dependiendo del tipo de despliegue de la solución puede soportar hasta 100000 usuarios. *Unity Connection* puede ser configurado para ofrecer solo correo de voz o mensajería integrada o solo mensajería unificada.

Mensajería integrada se refiera al acceso al correo de voz por vía telefónica y por clientes de software de mensajería. La mensajería unificada combina la mensajería de voz y la mensajería del correo electrónico en un buzón de correo al que se puede tener acceso desde muchos dispositivos diferentes. [8]

1.4.3 *Cisco Unified Communications Manager IM and Presence* (CUCMIMP) [9]

El servicio de Mensajería Instantánea y Presencia de *Cisco Unified Communications Manager* proporciona mensajería instantánea empresarial (IM) basadas en estándares nativos, y presencia sobre la red como parte de la solución de Comunicaciones Unificadas con Cisco.

Este servicio está estrechamente integrado con clientes de presencia y mensajería instantánea de escritorio y móviles, de Cisco, siendo compatible con aplicaciones de terceros. El servicio permite a los clientes realizar diversas funciones adicionales a mensajería instantánea y presencia, como *click-to-call*, control de teléfonos, comunicación de voz y video, correo de voz, y colaboración web.

1.4.4 *Gateway* de Voz Cisco [10]

Los *Gateways* proporcionan una serie de métodos para conectar una red de dispositivos finales de colaboración con la PSTN, de una PBX tradicional o a sistemas externos. Cisco cuenta con los siguientes tipos de *Gateways* de Voz:

- *Gateways* TDM y Serial. - *Gateways* de voz que soportan conexiones entre dispositivos de Telefonía IP hacia o desde líneas analógicas (FXS *Foreign Exchange Subscriber*, FXO *Foreign eXchange Office*) o digitales (T1, E1).
- *Gateways* para Videotelefonía. – Los *Gateways* de video se diferencian de los de voz porque deben interactuar con la ISDN (*Integrated Services Digital Network*) o enlaces seriales que soporten video y convierten la llamada de voz a una videollamada sobre una red IP utilizando protocolos como H.323 o SIP.
- *Gateways* IP. – *Gateways* que proporcionan comunicación entre redes de voz y video IP ofreciendo interoperabilidad, seguridad, y garantía del servicio. Las comunicaciones pueden darse entre empresas con soluciones de telefonía IP, hacia la PSTN, y hacia Internet para poder conectar con usuarios móviles y remotos sin el uso de VPN (*Virtual Private Network*).

1.4.5 Dispositivos Finales de Comunicaciones Unificadas Cisco [11]

La solución de Comunicaciones Unificadas de Cisco soporta el uso de una gran variedad de dispositivos finales, los cuales se clasifican de la siguiente manera:

- Dispositivos Analógicos

  Pueden ser teléfonos o centrales analógicas que se conectan a la solución de Comunicaciones Unificadas utilizando *Gateways* de Voz, que cuentan con puertos adecuados para estas integraciones (FXS y FXO).
- Dispositivos IP de escritorio

  Cisco cuenta con una gran variedad de teléfonos IP para estaciones de trabajo fijas, y pueden ser registrados mediante SCCP o SIP.
- Dispositivos de Video IP

  Los dispositivos finales de Video de Cisco proveen características de videotelefonía similares a las características de telefonía de voz, ofreciendo

al usuario la posibilidad de realizar videollamadas de tipo punto a punto y punto a multipunto.

- Dispositivos basados en *software* [12]

  Es una aplicación instalada en un equipo de escritorio (*Windows* o MAC) que registra y se comunica con las plataformas de procesamiento de llamadas de Cisco para servicios de voz y video. Estas aplicaciones pueden proporcionar funciones y servicios de colaboración como mensajería, presencia, acceso a directorios y conferencias.

- Dispositivos inalámbricos

  Se basan en una infraestructura LAN inalámbrica 802.11 (WLAN) para conectividad de red y proporcionar funcionalidades y características de telefonía IP. Este tipo de dispositivos es ideal para usuarios móviles que se mueven dentro de una sucursal o entre varias sucursales de la empresa o entornos donde no se cuenta con un adecuado cableado estructurado.

- Dispositivos móviles

  Son dispositivos basados en software que pueden ser instalados en dispositivos móviles del usuario tales como *smartphones* y *tablets*. Proporcionan funciones y servicios de colaboración como mensajería, presencia, acceso a directorios y conferencias.

- Teléfonos IP de terceros

  Se puede ofrecer funciones básicas de telefonía IP a equipos finales de terceros que trabajen con el protocolo SIP y H323.

***Cisco Jabber* [13]**

Es un cliente de *software* para usuarios finales, y permite utilizar los servicios de Comunicaciones Unificadas instalados. A través de Cisco *Jabber* un usuario puede acceder a todos los servicios de Comunicaciones Unificadas tales como: Presencia, Telefonía IP, Mensajería Instantánea, Correo de voz, Directorio Corporativo, etc. El Cliente de software puede ser instalado en: *Android, IPhone, IPad,* Mac y Windows.

1.5 Movilidad en Comunicaciones Unificadas con Cisco [14]

Las soluciones y aplicaciones de movilidad proporcionan características y funcionalidades del entorno de Comunicaciones Unificadas empresariales a los trabajadores móviles dondequiera que se encuentren. Con las soluciones de colaboración móviles, los usuarios pueden manejar las llamadas de negocios desde una variedad de dispositivos y

aplicaciones de acceso de la empresa, moviéndose alrededor del edificio, entre edificios, o entre ubicaciones geográficas fuera de la organización.

La movilidad y acceso remoto en soluciones corporativas de Comunicaciones Unificadas, se refiere a usuarios móviles en ubicaciones alejadas de la empresa, pero aun así conectadas a la infraestructura de la red empresarial a través de conexiones seguras sobre Internet. Existen dos tipos de accesos seguros para usuarios remotos de Comunicaciones Unificadas:

- Conectividad remota segura con VPN.
- Conectividad remota segura sin VPN.

1.5.1 Conectividad remota segura con VPN

Las conexiones a través de VPN habilitan un túnel seguro en capa tres entre la red corporativa y la red remota o el dispositivo remoto. Los dos tipos de despliegue comunes para VPN de acceso remotos son: acceso remoto con VPM desde *Router* y acceso remoto con cliente VPN desde dispositivo final.

Acceso Remoto con VPN desde *Router*

En un escenario con túneles VPN basados en *Router*s. El *router* implementado en el sitio remoto es responsable de levantar y proteger un túnel VPN de capa 3 contra la red empresarial; esto amplía el límite de la red empresarial a la ubicación remota del sitio. La ventaja de este tipo de conectividad es que varios dispositivos finales pueden ser desplegados en el sitio remoto, ya que los dispositivos finales no son responsables de la conexión segura y por lo tanto no requieren *software* o configuración especial. En su lugar, estos dispositivos simplemente se conectan a la LAN del sitio remoto y aprovechan el túnel VPN desde el enrutador del sitio remoto hasta el servidor de VPN corporativo, tal y como se muestra en la Figura 1-2.

Acceso Remoto con cliente VPN desde Dispositivo Final

La conexión VPN en el escenario basado en cliente, es establecida a través de una aplicación instalada en el dispositivo final, así el dispositivo final y el *software* son responsables de la creación de la conexión VPN hacia el concentrador corporativo (ver Figura 1-3). Este escenario extiende el límite de la red hasta el dispositivo remoto.

La ventaja de este tipo de conexiones es que existe un amplio rango de ubicaciones remotas, incluyendo redes públicas donde una VPN basada en *Router* no es una solución práctica.

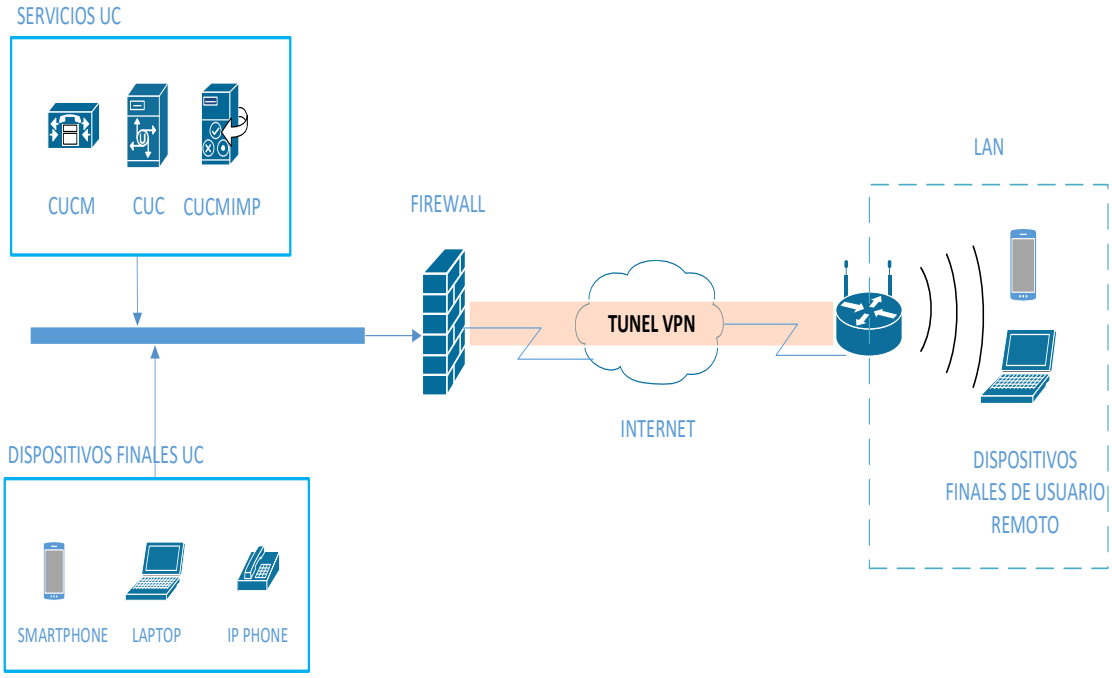

Figura 1-2 Acceso remoto desde VPN con *Router.*

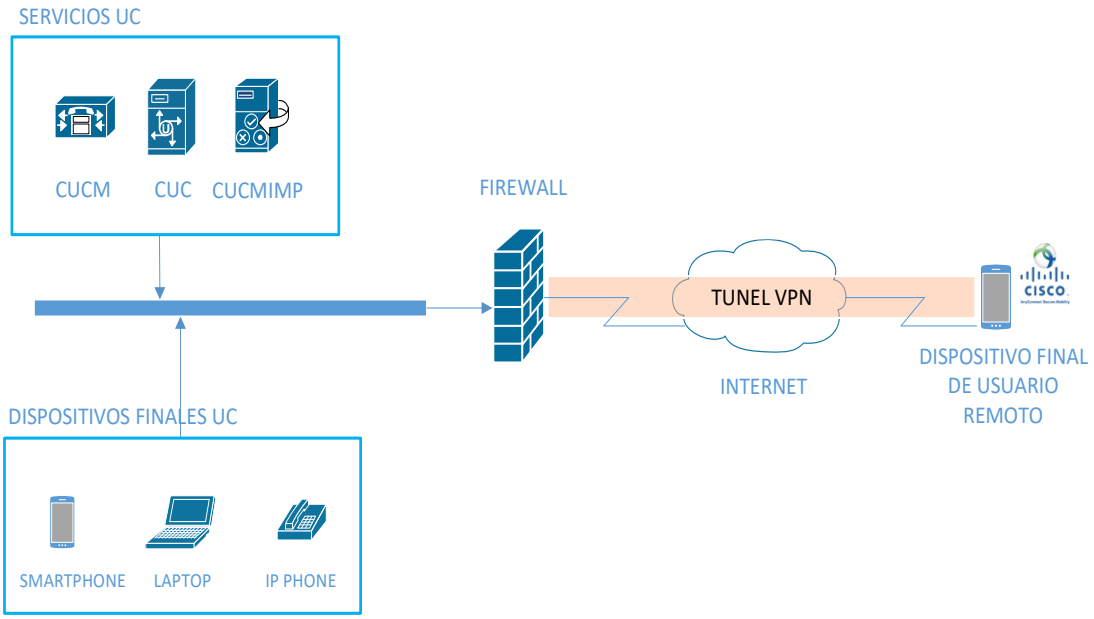

Figura 1-3 Acceso remoto con Cliente VPN desde dispositivo Final.

1.5.2 Conectividad Remota segura sin VPN

Las conexiones remotas sin el uso de VPN habilitan túneles seguros TLS (*Transport Layer Security*) entre los servicios de Comunicaciones Unificadas y el dispositivo remoto. Usando la comunicación sin VPN, extiende el límite de la red empresarial hasta el dispositivo o la aplicación cliente. La solución en Cisco para este tipo de accesos se denomina Cisco *Expressway*.

Cisco Expressway

La solución de movilidad y acceso remoto con Cisco *Expressway*, permite a los usuarios remotos y a sus dispositivos finales, el acceso y consumo de las aplicaciones y servicios de una solución de Comunicaciones Unificadas empresarial.

La solución de Cisco *Expressway* se compone de dos elementos: *Expressway*-E (*Expressway Edge*) y *Expressway*-C (*Expressway Core*), tal y como se muestra en la Figura 1-4. Estos componentes trabajan en conjunto con los servicios internos de Comunicaciones Unificadas con Cisco para proveer movilidad y acceso remoto seguro.

El nodo *Expressway*-E provee en el borde de la red una interfaz segura hacia los dispositivos móviles y remotos. Este nodo normalmente está ubicado en una DMZ (*Demilitarized Zone*) de la red corporativa y crea un túnel TLS con el nodo *Expressway*-C.

El nodo *Expressway*-C hace el trabajo de *proxy* para el registro seguro de los dispositivos remotos a los servicios internos de Comunicaciones Unificadas (CUCM, CUC, CUCMIMP, Directorio Corporativo). El tráfico de voz, video, señalización y cualquier otro tráfico de colaboración desde los dispositivos registrados desde Internet, pasa por el nodo *Expressway*-C.

A diferencia del acceso a los servicios mediante el uso de VPN de acceso remoto, en Cisco *Expressway* se provee comunicación segura sólo para el tráfico de Comunicaciones Unificadas.

1.6 Funcionamiento de las opciones de Movilidad Remota con Cisco para soluciones de Comunicaciones Unificadas

1.6.1 Funcionamiento de opción de acceso remoto con cliente VPN desde dispositivo final

Para brindar acceso remoto a una solución de Comunicaciones Unificadas mediante el uso de VPN, conviene utilizar el método basado en el cliente VPN sobre el dispositivo final del usuario. El método basado en *Router* no es una opción práctica en una solución de Comunicaciones Unificadas si se da el caso de que varios usuarios requieran el servicio de acceso remoto.

Un usuario remoto que tiene instalado Cisco *Jabber*[3] en su dispositivo final *(laptop, smartphone, Tablet*), deberá contar con el cliente software VPN en su dispositivo final para poder usar el servicio de Comunicaciones Unificadas desde una ubicación remota a través de Internet.

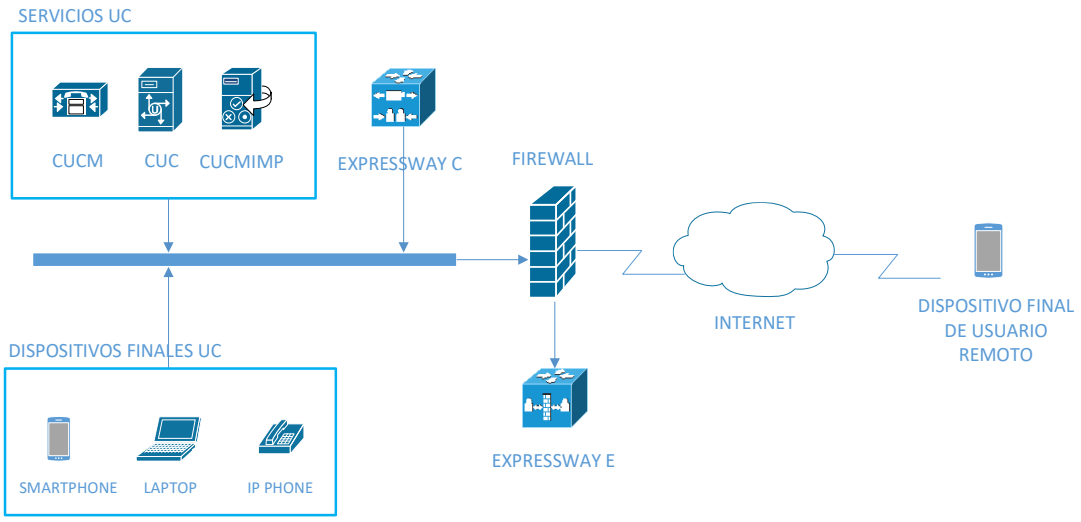

Figura 1-4 Conexión remota segura sin VPN con Cisco *Expressway*.

Cuando un usuario abre una sesión VPN usando el cliente de VPN de Cisco, éste se conecta al *Firewall* ASA (*Adaptive Security Appliance*) mediante SSL (*Socket Secure Layer*) o IPSec, dependiendo del tipo de cliente VPN. El usuario se autentica con el ASA y éste le asigna una dirección IP de una subred definida en la configuración del *Firewall* para VPNs de acceso remoto.

[3] Cliente en software de Comunicaciones Unificadas que ofrece mensajería instantánea, llamadas de voz y video, acceso a correo de voz, compartición de escritorio y presencia. [13]

VPN de Acceso Remoto IPSec

IPSec es un *framework* de capa tres independiente del protocolo, que permite proveer servicios de seguridad de datos en una red IP. IPSec permite proveer confidencialidad, integridad, autenticación, y servicios *anti-replay* al tráfico de red.

IPSec consta de dos fases principales. La principal responsabilidad de la Fase 1 es la autenticación de los dispositivos finales involucrados en la comunicación; y, que la comunicación entre estos dispositivos sea segura para poder iniciar la Fase 2. La Fase 2 son los túneles que se crean para proveer los servicios de confidencialidad e integridad al tráfico de red entre dos dispositivos finales.

El proceso cuando se levanta una conexión VPN de acceso remoto con IPSec es el siguiente:

1. Desde el cliente VPN de acceso remoto se inicia una conexión hacia el *Gateway* de VPNs remotas, por ejemplo, un *Firewall* ASA.
2. Inicia la Fase 1 cuando el cliente VPN y el *Gateway* VPN negocian cómo van a proteger la administración de la conexión.
3. Se utiliza Diffie-Hellman para compartir de manera segura las claves de los algoritmos de encriptación y funciones HMAC (*Hash-based Message Authentication Code*) para la administración de la conexión.
4. Se realiza la autenticación del dispositivo a través de la conexión segura de administración.
5. Se realiza la autenticación de usuario utilizando autenticación extendida (XAUTH); con XAUTH el *Gateway* VPN solicitará al usuario sus credenciales de acceso (nombre de usuario y contraseña).
6. El *Gateway* VPN aplica políticas de conexión al cliente VPN; entre las principales se tienen: dirección IP interna, nombre de dominio, direcciones IP de servicios de DNS, y políticas de *Firewall*.
7. La Fase 1 termina para dar paso a la Fase 2. El cliente y el *Gateway* VPN negocian los parámetros y la información de claves de encriptación a través de la conexión segura de administración, para proteger las conexiones de datos.
8. Las conexiones de datos SA (Asociaciones de Seguridad) se establecen y con esto la Fase 2 culmina. El *Gateway* VPN puede a partir de ese momento proteger el tráfico de usuario a través de las conexiones de datos.

VPN de Acceso Remoto SSL

SSL (*Secure Sockets Layer*) fue desarrollado por *Netscape Communications* para crear conexiones seguras en ambientes WEB. La meta de diseño fue proveer confidencialidad, integridad, autenticación y ser utilizado para asegurar otros protocolos de comunicación.

- SSL versión 1 (SSLv1).
- SSL versión 2 (SSLv2).
- SSL versión 3 (SSLv3).
- *Transport Layer Securit*y (TLS versión 1.0, 1.2).

La primera versión puesta en escena fue SSLv2 (la versión 1 nunca fue publicada) en 1995 y fue rápidamente reemplazada por SSLv3 en 1996, luego de que algunas vulnerabilidades hayan sido detectadas en la versión 2. TLS fue presentada en 1999 como una nueva versión de SSL basada en SSLv3, pero no compatibles.

SSL se sitúa entre la capa de Aplicación y la capa de Transporte. La unidad básica en SSL se denomina *record*. Cada *record* está conformado por una cabecera de 5 bytes seguido de la parte de datos. El protocolo realiza los siguientes pasos para poder armar un *record* SSL con los datos que se obtienen desde la capa Aplicación:

1. Fragmenta la información que baja desde la capa Aplicación en bloques de máximo 2^{14} *bytes*.
2. Opcionalmente realiza compresión de los datos y añade un código de autenticación de mensaje (MAC: *Message Authentication Code*).
3. Cifra los datos de acuerdo con la especificación que se acuerda en la negociación SSL.
4. Se añade la cabecera SSL.

Existen cuatro tipos de *records*: de saludo (*Handshake*), de cambio de especificación de cifrado (*Client Key Exchange*), de alertas, de datos de aplicación.

- *Record* de Saludo (*Handshake*), se utiliza en el intercambio de mensajes entre los pares SSL para negociar la versión SSL, algoritmos de cifrado, y parámetros de conexión. También se realiza autenticación entre los pares SSL y la generación de la clave secreta para el cifrado utilizando técnicas de claves públicas.
- *Record* de cambio de especificación de cifrado (*Client Key Exchange*), es utilizado para indicar el inicio de la comunicación segura entre el cliente y el

servidor, y para poder señalizar una transición o cambio en la estrategia de cifrado para la comunicación. Este tipo de *record* contiene un dato de longitud de un *byte*.

- *Record* de tipo Alerta, es utilizado para enviar información de errores, problemas o advertencias sobre la conexión entre los pares SSL.
- *Record* de datos de aplicación, el *record* contiene los datos de la aplicación que son fragmentados, comprimidos, y encriptados basados en el estado actual de la conexión.

1.6.2 Funcionamiento de opción de Acceso Remoto con Cisco *Expressway* [15]

Una solución con *Cisco Expressway* provee movilidad remota y segura a usuarios para que puedan consumir servicios empresariales de Comunicaciones Unificadas sin necesidad de clientes VPN en sus dispositivos finales.

Cisco Expressway está conformado de dos componentes: el nodo *Cisco Expressway C* y el nodo *Cisco Expressway E,* estos dos componentes trabajan en conjunto con CUCM principalmente para ofrecer el servicio de Comunicaciones Unificadas a usuarios remotos.

El nodo *Expressway C* se instala en la red corporativa Interna, usualmente en el mismo segmento de red de los servicios internos de Comunicaciones Unificadas, mientras que el nodo *Expressway E* se ubica en una DMZ del *Firewall*, tal y como se especifica en la Figura 1-4.

Expressway C crea una conexión segura TLS con el nodo *Expressway E,* y sirve de proxy hacia el CUCM para el registro seguro de dispositivos remotos. El nodo *Expressway C* contiene un agente B2BUA (*Back to Back User Agent*) con el cual provee capacidades de terminación de *media*.

Expressway C y *Expressway E* fueron diseñados para que trabajen juntos en una solución de *Firewall traversal,* que es el componente principal para la comunicación de usuarios remotos desde Internet con servicios de Comunicaciones Unificadas.

Expressway C ubicado en el interior de la red corporativa, actúa como un cliente de tránsito para todos los dispositivos internos de Comunicaciones Unificadas (dispositivos finales y servicios), y resuelve el problema de dispositivos que utilizan un gran rango de puertos de media multiplexándolos a un número significativamente bajo de puertos abiertos para comunicaciones salientes. *Expressway C* mantiene una conexión segura y autenticada

desde el interior de la red corporativa hacia la red externa, con el envío de *keep-alive* para la zona de tránsito desde el nodo *Expressway C* al *Expressway E.*

Expressway E se sitúa en el borde de la red, en una DMZ, mantiene la señalización y el enrutamiento de *media* para SIP, H323 y XMPP. Modifica las cabeceras y direcciones IP de los paquetes para procesar la voz y/o video, y señalización en nombre de los dispositivos finales y servidores de aplicación que están en la red interna.

Expressway C y *Expressway E* proveen funciones de *Firewall traversal* y funciona de la siguiente manera:

1. *Expressway E* es el servidor de recorrido (*traversal*) instalado en la DMZ. *Expressway C* es el cliente de recorrido y está instalado en red INSIDE del *Firewall*.
2. *Expressway C* inicia una conexión a través del *Firewall* hacia puertos específicos sobre *Expressway E,* con las credenciales seguras de inicio de sesión.
3. Una vez que la conexión ha sido establecida, *Expressway C* envía periódicamente paquetes *keep-alive* hacia el *Expressway E* para mantener la conexión.
4. Cuando el servidor *Expressway E* recibe una llamada u otra solicitud de servicio de colaboración, ejecuta una solicitud de inicio hacia el servidor *Expressway C.*
5. *Expressway C* enruta la solicitud hacia el servicio de Comunicaciones Unificadas correspondiente.
6. La conexión se establece y el tráfico de aplicación a traviesa el *Firewall* de manera segura sobre una conexión transversal existente.

La Figura 1-5 describe cómo funciona el proceso *Firewall Traversal.* Es necesaria la configuración de una zona *Firewall Traversal Client* en el servidor *Expressway C,* y una zona *Firewall Traversal Server* en el servidor *Expressway* E.

Cuando un dispositivo final es registrado a través de Internet con Cisco Expressway, no puede ser administrado remotamente por los servicios de Comunicaciones Unificadas internos, esto se da porque la dirección IP del dispositivo final es dinámicamente traducido y está detrás de un dispositivo de seguridad (Firewall).

Expressway C tiene la característica de *proxy* reverso que provee provisión, registro, y detalles de servicio a los clientes conectados desde Internet, estando al frente de los servicios de Comunicaciones Unificadas tales como CUCM, Presencia y Mensajería Instantánea, y *Unity Connection.* La provisión para los clientes se lleva a cabo por HTTPS mientras que el registro por SIP y XMPP.

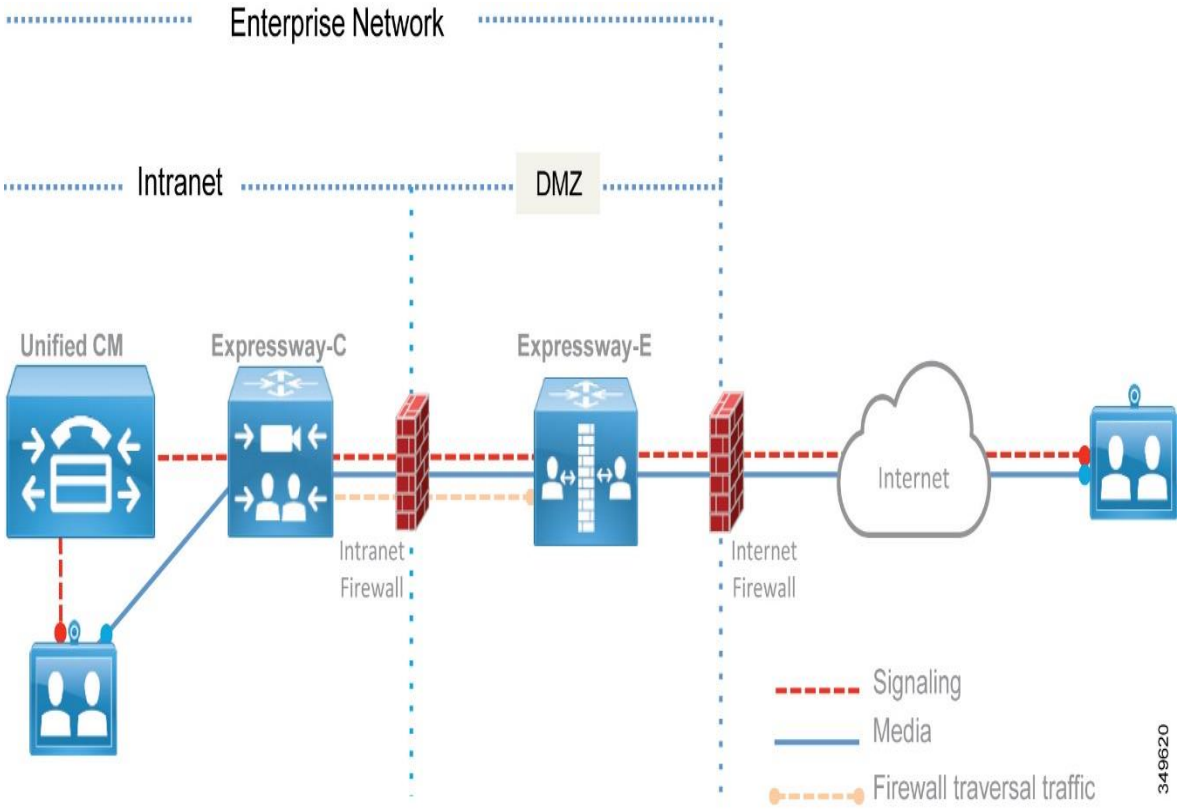

Figura 1-5 *Cisco Expressway: Firewall Traversal*. [15]

Cuando un usuario inicia sesión desde *Cisco Jabber* o un dispositivo de Telepresencia, utiliza el FQDN (*Fully Qualified Domain Name*) de su usuario, por ejemplo "user1@example.com". El cliente consulta al servidor de DNS público por registros SRV específicos:

- *_cisco_uds._tcp.example.com*, este registro se configura solo en el DNS corporativo.
- *_collab-edge._tls.example.com*, el cual es configurado solo en un DNS público y resuelve con la dirección pública del servicio de *Expressway E*.

Si el cliente está conectado desde Internet, no tendrá respuesta desde el servidor DNS público para el registro _cisco-uds._tcp, pero sí para el registro SRV _collab-edge._tls. Una vez que el cliente conoce el nombre de DNS del servidor *Expressway E* puede comenzar con el proceso de provisión y registro.

El proceso de aprovisionamiento a través de *Expressway* contiene los siguientes pasos:

1. El cliente inicia con una solicitud "*GET_edge_config"*, por ejemplo:

   https://Expressway_e_name.example.com:8443/ZeW50LXBhLmNvbQ/GET_edge_config?service_name=_cisco-uds&service_name=_cuplogin

Junto con la solicitud el cliente envía las credenciales del usuario, lo cual *Expressway E* reenvía al servidor de *Expressway C.*

2. Desde el servidor *Expressway C* se envía una solicitud al CUCM para poder determinar el *cluster* al cual pertenece el usuario. Este paso es esencial para esquemas *multi-cluster:*
GET cucm.example.com:8443/cucm-uds/clusterUser?username=user1

3. Una vez que se identifica el *cluster* al cual pertenece el usuario, se envía una respuesta el servidor *Expressway C* que incluye la dirección de todos los servidores del *cluster*.
4. *Expressway C* solicita al *cluster* CUCM identificado la información de aprovisionamiento realizando los siguientes métodos de solicitudes:
   GET /cucm-uds/user/user1/devices, para recibir la lista de dispositivos asociados al usuario.
   GET /cucm-uds/servers, para recibir la lista de servidores que conforman el *cluster* CUCM.
   ***GET* /cucm-uds/user/user1**, para recibir la configuración de usuario y extensión o línea.
   En las respuestas a las solicitudes el CUCM envía también la información del nodo o nodos CUCM con el servicio de TFTP.

Las solicitudes subsecuentes son hacia el nodo TFTP a través de HTTP, y así se completaría el proceso de aprovisionamiento y toda la información recolectada es reenviada al cliente remoto para poder iniciar el proceso de registro. El proceso de registro consiste en dos acciones:

1. Inicio de sesión con el servicio CUCMIMP, el cual se ejecuta con la funcionalidad XCP *Router (Extensible Communications Platform Router)* en *Expressway C.* El enrutador XCP consulta sobre *clusters* CUCMIMP configurados en *Expressway C* para encontrar el *cluster* asociado al usuario, y con esto el cliente Cisco *Jabber* es capaz de iniciar sesión con el servicio de Presencia y Mensajería Instantánea.
2. Registro con CUCM utilizando los mensajes *SIP REGISTER,* los cuales son atendidos por la función de SIP *proxy* de *Expressway.*

2. METODOLOGÍA

2.1 Diseño de una solución de Comunicaciones Unificadas

2.1.1 Información de la Empresa[4]

Descripción de la Empresa

Fue fundada en 1997 con el firme propósito de suplir las necesidades de la salud de los ecuatorianos. Representante de importantes marcas internacionales y con cobertura a nivel nacional, ha ido creando estrategias y soluciones para brindar un servicio personalizado; lo que le ha permitido llegar a constituirse una empresa líder en el mercado médico nacional. Tiene sedes en Quito, Cuenca, Guayaquil, Loja, Ambato y El Coca.

Misión

"Satisfacer las necesidades de nuestros clientes, ofreciendo Productos de alta calidad y Equipos con tecnología de punta, con la vocación y calidad de servicio de nuestro equipo humano, manteniendo una atención personalizada, integral y eficiente."

Visión

"Consolidarnos como empresa líder en excelencia y calidad de servicio, dentro del mercado nacional, proporcionando seguridad y bienestar a todos nuestros clientes mediante la innovación y capacitación, manteniendo una mejora continua en todos los procesos de la organización."

Productos

Se ofrecen los siguientes productos:

- Anestesia y Ventilación.
- Terapia Respiratoria.
- Electrocirugía.
- Gasas y Apósitos.
- Guantes.
- Emergencia y Resucitación.

[4] La información de la empresa ficticia, misión, visión, productos y servicios fue tomada como referencia de GIMPROMED CIA. LTDA (https://www.gimpromed.com/empresa.html), para el diseño del presente proyecto.

- Catéteres.
- Cuidado del Paciente.
- Protección Quirúrgica.
- Cirugía.
- Urología.

Servicios

La empresa ofrece los siguientes servicios:

- Asesoría sobre productos y nuevas tendencias.
- Servicio de Capacitación.
- Soporte Técnico especializado.

Situación actual

Actualmente la empresa mantiene una infraestructura de Red sólida que permite a los usuarios de todas las sedes, acceder a los servicios internos de la organización a través de enlaces WAN. Con el proveedor de servicios mantiene el contrato de una WAN MPLS para la comunicación de todas las sucursales.

La empresa cuenta con dos centros de datos; principal y alterno, en los cuales alojan servicios internos como: servicio de dominio, correo electrónico, facturación electrónica y CRM. Cada sucursal cuenta con un sistema de telefonía analógica; en las sedes principales, Quito y Guayaquil, tienen una línea E1; el resto de las sedes cuentan con tres líneas analógicas cada una, para la comunicación desde y hacia la PSTN. Las llamadas entre las sucursales se realizan a través de la PSTN.

La empresa cuenta con 177 empleados en total, y su distribución sobre las sucursales se presenta en la Tabla 2-1.

Tabla 2-1 Número de empleados por sucursal.

Sucursal	Número de empleados
Quito	80
Guayaquil	67
Cuenca	7
Ambato	9
Loja	8
El Coca	6

En la organización existe un equipo de ventas altamente capacitado que visita clientes de manera frecuente. Debido a que los vendedores pasan la mayor parte del tiempo fuera de la oficina, cuentan con un teléfono celular con plan corporativo de voz y datos. Los vendedores solo pueden ser localizados a su número celular, y esto genera un gasto a la empresa cuando la llamada es realizada desde cualquier oficina de la organización.

2.1.2 Diseño de alto de nivel (HLD, *High-Level Design*)

Requerimientos

La empresa demanda un sistema de Comunicaciones Unificadas que cumpla con los siguientes requisitos:

- El servicio de Telefonía IP entre sucursales deberá realizarse a través de la WAN, lo cual reduciría gastos de llamadas a la PSTN. Con el sistema de telefonía actual, las llamadas entre sucursales se realizan a través de la PSTN y genera un costo considerable a la organización.
- Las líneas analógicas no permiten llamadas concurrentes, si una línea es utilizada para una llamada saliente, las misma no puede ser utilizada hasta que la llamada en curso termine. La solución por instalarse debe permitir la conexión de troncales SIP, que permite obtener el número de llamadas concurrentes a un número telefónico de acuerdo con el número de canales que se contrate con el proveedor de servicios. Se prevé la contratación de troncales SIP en todas las sucursales.
- Una solución de telefonía analógica no cuenta con facilidades para soporte remoto, cada Centra Telefónica debe ser administrada localmente, esto genera tiempos de respuesta muy altos a los requerimientos de soporte de Telefonía. Es necesario contar con administración centralizada y accesible desde cualquier ubicación dentro de la red de la organización, permitiendo al administrador del sistema atender de manera ágil los requerimientos de todas las sucursales.
- Con el sistema tradicional, cuando un usuario de una sede cambia de puesto, es necesario mover las conexiones de cableado telefónico para que pueda mantener su número de extensión. Existe personal que en ocasiones deben viajar a otras sucursales por varios días, ya sea por procesos de auditoría interna o capacitación, y durante esos días pierde llamadas dirigidas a su extensión. Se requiere que el usuario pueda mantener su extensión y permisos de llamada desde cualquier puesto de trabajo de la organización.

- La asignación de dispositivos finales se realizará de acuerdo con las características que se requiere para cada usuario. En la Tabla 2-2 se detalla el requerimiento de dispositivos de Comunicaciones Unificadas para usuarios finales.

Descripción de la Solución

Los servicios de Comunicaciones Unificadas que permitirán cumplir con los requerimientos de la empresa son los siguientes:

a) Telefonía IP

La Telefonía IP utiliza la red de datos IP para proporcionar comunicaciones de voz a toda la empresa. La solución contempla la instalación de los servicios de telefonía en Quito y Guayaquil para proveer redundancia del servicio y balanceo de carga en el manejo de extensiones.

Tabla 2-2 Requerimiento de dispositivos finales por sucursal.

Sucursal	Número de usuarios por sucursal	Total de dispositi-vos	Teléfonos físicos con capacidades de Voz y Video	Teléfonos físicos con capacidades de Voz	Número de usuarios con correo de Voz	Número de salas de reunio-nes	Número de teléfo-nos de opera-dora
Quito	80	83	4	75	80	3	1
Guayaquil	67	69	2	64	67	2	1
Cuenca	7	7	1	6	7	0	0
Ambato	9	9	1	8	9	0	0
Loja	8	8	1	7	8	0	0
El Coca	6	6	1	5	6	0	0

b) Movilidad

Es una característica que permite al usuario utilizar el servicio de Comunicaciones Unificadas desde cualquier ubicación con acceso a la Red corporativa.

Para completar la solución de Comunicaciones Unificadas, los siguientes servicios se incluirán en el diseño porque aportan con características que ayudan a mejorar la productividad de la empresa.

a) Correo de Voz

Es una característica que está de la mano con el servicio de Telefonía IP, y consiste en ofrecer la opción de grabar un mensaje de voz cuando el destino de la llamada no está disponible. El mensaje se guarda en una casilla virtual y está disponible para el usuario.

b) Mensajería Unificada

Consiste en la integración de los servicios de Correo de Voz y Correo Electrónico, para que el mensaje de voz esté también disponible en el buzón de Correo Electrónico del usuario.

c) Mensajería Instantánea y Presencia

Es un servicio de gran valor para las empresas, es un canal de comunicación ágil, y funciona en combinación del servicio de Presencia, el cual presenta estados telefónicos en la interfaz de la aplicación de mensajería instantánea.

d) Supervivencia de Llamada

La solución de Comunicaciones Unificadas se concentrará en los dos sitios principales: Quito y Guayaquil, y si existe alguna falla de enlace WAN en alguna sucursal ésta perderá el servicio de Telefonía local. Para que la sucursal continúe al menos con el servicio de Telefonía IP es necesario realizar la configuración del servicio de Supervivencia de Llamada.

Componentes de la Solución

Se definen los siguientes componentes para la solución de Comunicaciones Unificadas con Cisco:

a) *Cisco Unified Communications Manager* (CUCM)

CUCM es punto central para la implementación de una solución de Comunicaciones Unificadas; administra las comunicaciones de Voz y Video, administra las cuentas de usuarios para la solución, ofrece servicios de movilidad y genera archivos de registro de llamadas (CDR, *Call Detail Record*).

Productos de Comunicaciones Unificadas con Cisco como *Unity Connection* y *Cisco Unified Communications Manager IM and Presence,* se integran al CUCM para poder ofrecer sus servicios al usuario.

b) *Cisco Unified Communications Manager IM and Presense* (CUCMIMP)

Maneja servicios de presencia y mensajería instantánea. Este producto se integra desde la instalación con el CUCM, porque se asocia como un nodo de *cluster* y así mantiene sincronizadas sus bases de datos con la información de usuarios del CUCM.

En CUCMIMP se configura la información del administrador de llamadas y servidor TFTP (*Trivial File Transfer Protocol*) para los archivos de configuración, ambos roles están incluidos en el CUCM. Esta configuración tiene el fin de habilitar los servicios de llamadas a la aplicación de usuario Cisco *Jabber.* Cisco *Jabber* es un cliente de *Software* que permite al usuario tener principalmente funciones de *softphone,* mensajería instantánea, presencia y correo de voz. La característica de presencia no se limita a solo los usuarios conectados a la aplicación de Cisco *Jabber,* también se reciben estados de presencia desde teléfonos IP físicos a través de la integración del CUCMIMP y CUCM que se realiza con la configuración de un troncal SIP entre los servidores indicados.

c) *Cisco Unity Connection* (CUC) [16]

CUC brinda servicios de correo de voz, mensajería unificada y operadora automática. Se integra con CUCM para el renvío de las llamadas a los buzones de voz y al servicio de operadora automática. La integración también permite la creación de buzones de correo de voz por usuario, desde el CUCM se indica que usuario tiene el servicio. CUC es compatible con Cisco *Jabber,* para que los mensajes de voz estén disponibles en el cliente de *software;* esta configuración se la aplica desde el CUCM.

En CUC es posible realizar la configuración de los buzones para que los mensajes de voz sean enviados al correo electrónico del usuario. La configuración es compatible con *Microsoft BPOS Dedicated, Microsoft Office 365, Google Mail,* IBM *Lotus, VMWare Zimbra, y Novell GroupWise.* La integración con los productos *Microsoft* es directa desde CUC, el resto de los productos requieren el uso de *software* adicional de terceros (No Cisco).

d) *Cisco Unity Express* (CUE)

Es un módulo de servicio instalado dentro del *Gateway* de voz y provee servicios de correo de voz y operadora automática. Elemento orientado para

implementaciones multi-sitio, con una capacidad máxima de hasta 500 buzones de correo de voz y hasta 32 llamadas simultáneas, para acceso al buzón y para el servicio de operadora automática.

En el diseño, cumple su función en las sucursales pequeñas de la organización, solo con el servicio de operadora automática. Los buzones de correo de voz para los usuarios de la organización se configurarán en CUC. CUE completa la característica de supervivencia de llamada, al continuar con el servicio de operadora automática luego de que la sucursal quede aislada por falla en el acceso a la WAN. CUE no es compatible con Cisco *Jabber,* por esta razón los buzones de voz se configuran en CUC, si el usuario tiene un nuevo mensaje de voz durante el evento de falla del enlace WAN, el mensaje aún llegará a su cuenta de correo electrónico.

e) *Cisco Prime Collaboration* (CPC)

Es un componente con el cual se administran los servicios que forman parte de una solución de Comunicaciones Unificadas. La administración se realizaría desde una sola interfaz, y cuenta con características de monitoreo y reportería. El monitoreo es de rendimiento de los elementos y para medir la disponibilidad de la solución.

Este producto es de gran valor para usuarios que no están familiarizados con la administración de cada elemento de la solución de Comunicaciones Unificadas con Cisco, facilita la administración con el uso de *templates* y *wizards* de configuración.

f) *Endpoints*

Los dispositivos finales en Comunicaciones Unificadas se eligen de acuerdo con la necesidad del cliente. En Cisco existe una gran variedad de dispositivos finales, y se resume de acuerdo con el literal 1.4.5 de la sección 1.4. La elección se recomienda hacerla en base a características o funciones que se desea proveer a un usuario en su espacio de trabajo. Se contempla el uso de Cisco *Jabber* adicional al teléfono IP para cada usuario, para aprovechar las características de movilidad en la red corporativa.

g) *Voice Gateways* (VGW)

Es un dispositivo, comúnmente un *router,* con licenciamiento y módulos en *hardware* para el manejo de capacidades de Voz sobre IP. Sirve de interfaz entre un sistema VoIP y la PSTN o un sistema PBX tradicional o dispositivos

analógicos como por ejemplo máquinas de FAX. También contiene recursos DSP (*Digital Signal Processor*) adicionales para el uso de *transcoding* y conferencias de voz. Cada una de las sucursales, incluyendo la matriz, contará con un *Gateway* de voz para la comunicación con la PSTN mediante el uso de una troncal SIP; adicional a esto cada *Gateway* dispondrá de recursos DSP para uso de su correspondiente sucursal. Si una llamada necesita *transcoding,* utiliza al *Gateway* local para esta función y el *Gateway* entra a funcionar como *proxy* de la llamada.

h) Licencias [17]

Cisco maneja tres niveles de licencias, las cuales se basan en el uso de la solución por usuario, esto significa que, si un usuario tiene un teléfono IP y Cisco *Jabber* en su PC, *Smartphone* y *Tablet,* estaría consumiendo solo una licencia de un cierto tipo (ver Tabla 2-3). Los niveles de licencias actuales son los siguientes:

- *Cisco Unified Workspace Licensing (UWL) Meetings Edition*
    - Esta licencia es para una solución completa de Comunicaciones Unificadas con capacidades avanzadas de Video. Ofrece las mismas capacidades de la licencia UWL *Standard* más las opciones de video conferencia y colaboración web con Cisco *Webex.*
- *Cisco UWL Standard Edition*
    - Incluye control de llamada, mensajería de voz, mensajería instantánea, presencia, Cisco *Expressway,* y clientes de *software* (Ejemplo: Cisco *Jabber)*. Usuarios con más de dos dispositivos asociados a su cuenta, consumen este tipo de licencia.
- *Cisco User Connect Licensing* (UCL)
    - Depende del tipo y número de dispositivos que se requiera, este tipo de licencia se clasifica en: *Essential, Basic, Enhanced,* y *Enhanced Plus.*
    - Las licencias *Essential* y *Basic,* soportan hasta un dispositivo por usuario, y Cisco *Jabber* solo en modo de mensajería instantánea. La licencia *Essential* aplica para dispositivos analógicos conectados a un *Gateway,* y teléfonos IP modelos 3905 y 6901. La licencia *Basic* aplica para teléfonos IP 7811 y 7821.

- La licencia *Enhanced,* aplica en la asignación de hasta un dispositivo de cualquier modelo, que no sean de video conferencia, y los específicos para licencias *Essential* y *Basic.* Esta licencia aplica para el uso de Cisco *Jabber* con capacidades completas, pero si es un único dispositivo para un usuario.
- La licencia *Enhanced Plus,* aplica para la asignación de hasta dos dispositivos de Comunicaciones Unificadas por usuario. Incluye todos los modelos de dispositivos de Comunicaciones Unificadas, pero no incluye los dispositivos de video conferencia.

Tabla 2-3 Resumen de licencias en Comunicaciones Unificadas con Cisco. [17]

License Type	***UWL Meetings***	***UWL Standard***	***UCL Enhanced Plus/Enhanced***	***UCL Basic***	***UCL Essential***
Personal Multiparty Plus (incl Cisco Meeting Server)	Ok	N/A	N/A	N/A	N/A
Cisco WebEx conferencing–customer premises equipment	Ok	*Optional add-on*	*Optional add-on*	*Optional add-on*	*Optional add-on*
Cisco Unity Connection	Ok	Ok	*Optional add-on*	*Optional add-on*	*Optional add-on*
Cisco Expressway firewall traversal	Ok	Ok	Ok	N/A	N/A
Cisco Jabber unified communications	Ok	Ok	Ok	N/A	N/A
Cisco Jabber instant messaging and presence	Ok	Ok	Ok	Ok	Ok
Cisco Prime™ Collaboration	Ok	Ok	Ok	Ok	Ok
Number of devices supported	Multiple	Multiple	2/1	1	1

Esquema propuesto

En la Figura 2-1 se observa el diseño propuesto, con las siguientes consideraciones:

- Los servicios de Comunicaciones Unificadas: CUCM, CUCMIMP y CUC, serán *clusters* de dos elementos. Cada miembro del *cluster* será instalado en Quito y Guayaquil y la réplica entre los nodos será a través de la WAN. Con este esquema si el acceso a la WAN desde Quito llega a fallar, todas las sucursales trabajarán con los servicios instalados en Guayaquil y viceversa. Con esta configuración, cuando exista falla en el acceso a la WAN desde Quito o Guayaquil, las sucursales no pasan a modo de Supervivencia de Llamada.
- Todas las sucursales cuentan con un *Gateway* de voz para el acceso a la PSTN, pero solo las sucursales de Cuenca, Loja, Ambato y El Coca tienen la configuración de SRST (*Survivable Remote Site Telephony*) y CUE que permite Supervivencia de Llamada. Cada una de las sucursales tiene salida independiente a la PSTN, y contarán con su propio esquema de operadora automática, gracias a la implementación de *Unity Connection* y *Unity Connection Express*.
- El acceso a la PSTN de cada sucursal será mediante el uso de troncales SIP, debido a que los proveedores de servicio cuentan con este protocolo disponible para el acceso a la PSTN.
- No se considera redundancia para el servidor *Prime Collaboration.* Cada servicio de la solución tiene su propia interfaz de configuración, y puede ser accedida de manera directa en caso de pérdida del servicio Cisco *Prime Collaboration.*

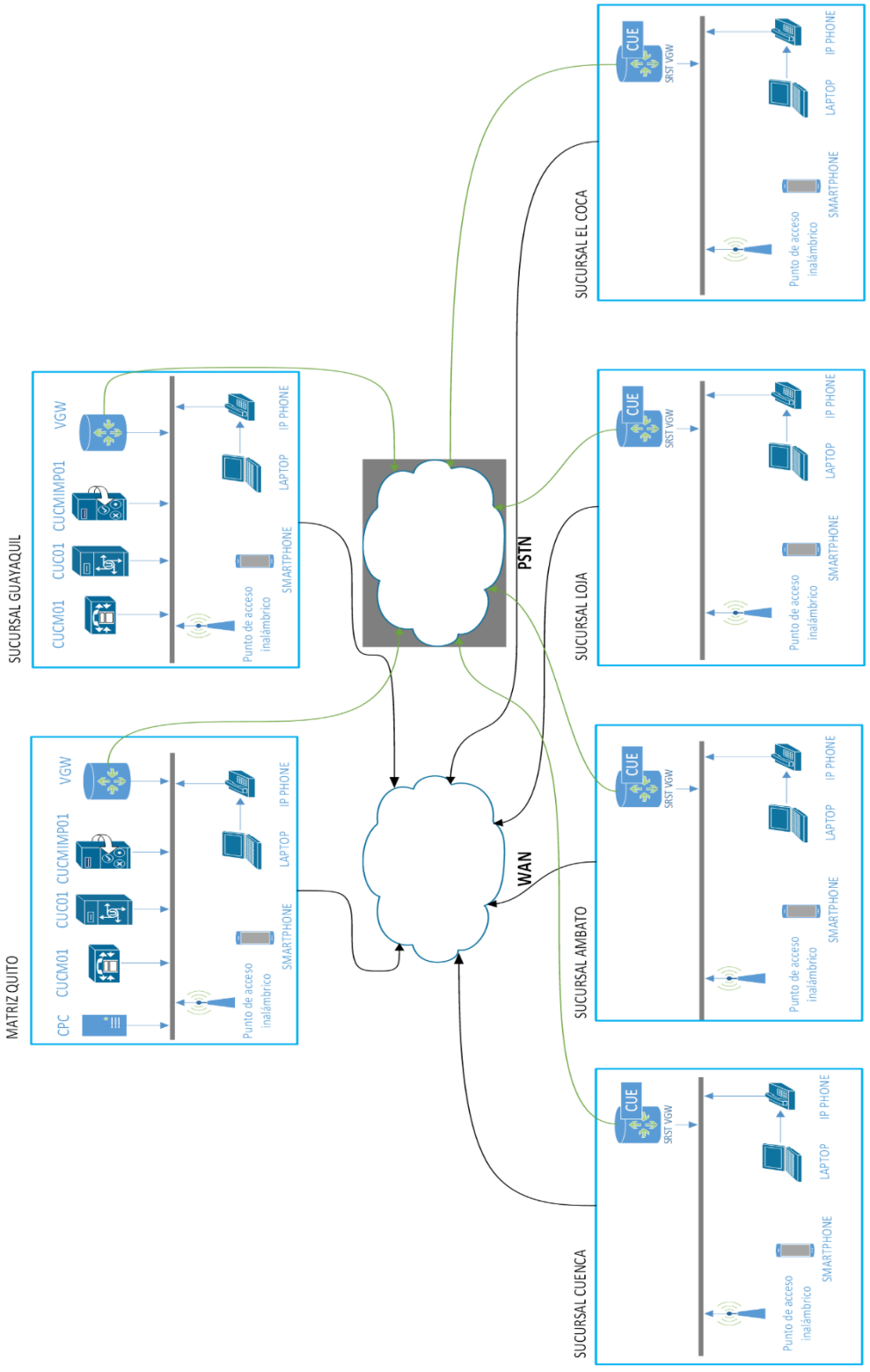

Figura 2-1 Diagrama lógico de solución propuesta.

2.1.3 Diseño de bajo nivel (LLD, *Low-Level Design*)

Requisitos de Instalación de servicios UC

Los siguientes son requisitos para la instalación de la solución de Comunicaciones Unificadas:

- DHCP (*Dynamic Host Configuration Protocol*), a través de este servicio los teléfonos IP obtienen la información IP de los servidores CUCM para poder obtener su configuración. Es necesario configurar la opción 150[5] con la información de los CUCM, en el servicio de DHCP. Para las sucursales el servicio DHCP puede ser configurado en el *Gateway* de voz.
- DNS (*Domain Name Servers*), durante la instalación los servicios UC validan la configuración de su nombre de dominio en el servidor DNS que se especifique.
- NTP (*Network Time Protocol*), los servicios a instalarse deben estar sincronizados contra un servidor NTP. Si no se cuenta con este servicio en la organización, es una opción válida configurar NTP en el *Gateway* de Voz.
- VLAN de Voz, se debe definir una VLAN para los dispositivos de usuario de Comunicaciones Unificadas y configurarla en los puertos de acceso de los *switches* LAN de cada sucursal.
- Direccionamiento IP para servicios y equipos de usuarios de Comunicaciones Unificadas. Se debe definir el direccionamiento que van a utilizar los teléfonos IP en cada sucursal.

Direccionamiento IP

En la organización no se estima un crecimiento del número de empleados mayor al 15% en 10 años, por esta razón el administrador de TI (Tecnologías de la información) designó los rangos de direcciones IP de tal manera que con el tercer octeto pueda identificar la sucursal. El plan de direccionamiento IP a utilizar se detalla en la Tabla 2-4.

El servicio DHCP para cada sucursal funcionará desde el *router Gateway* de Voz, y la configuración contará con la opción 150 en la cual se especifica la dirección IP del servidor CUCM que tiene activo el servicio TFTP para la descarga de configuración de los teléfonos IP.

---

[5] Cuando un Teléfono IP de Cisco inicia, y no tiene configurada la información IP y la dirección del servidor TFTP, envía una solicitud al servidor DHCP con la opción 150, para obtener una lista de servidores TFTP para la descarga de configuración.

Los servidores en Quito y Guayaquil estarán en la red de servidores del cliente, para Quito está dentro del rango 192.168.50.0/24, y en Guayaquil está en la red 192.168.51.0/24. La asignación de direcciones IP para cada servidor se indica en la Tabla 2-5.

Tabla 2-4 Plan de direccionamiento IP.

Sucursal	Número de dispositivos físicos para UC	Dirección de Red / Máscara	Dirección de *Gateway* de Red
Quito	84	192.168.240.0/24	192.168.240.1
Guayaquil	70	192.168.241.0/24	192.168.241.1
Cuenca	7	192.168.242.0/24	192.168.242.1
Ambato	9	192.168.243.0/24	192.168.243.1
Loja	8	192.168.244.0/24	192.168.244.1
El Coca	6	192.168.245.0/24	192.168.245.1

Tabla 2-5 Direcciones IP asignados a servidores UC.

Servidor	Dirección IP
CUCM Quito	192.168.50.10
CUCM Guayaquil	192.168.51.10
CUCMIMP Quito	192.168.50.11
CUCMIMP Guayaquil	192.168.51.11
CUC Quito	192.168.50.12
CUC Guayaquil	192.168.51.12

La red de servidores está detrás de un *firewall* y el *Gateway* de la red es 192.168.50.1 y 192.168.51.1, para Quito y Guayaquil respectivamente.

Cisco Business Edition

Cisco Business Edition 6000M es un producto orientado a PYMES, personalizado y con servicios precargados listos para la configuración inicial. El diseño incluye dos servidores físicos en los cuales tiene preinstalado los sistemas operativos de cada elemento de una solución de Comunicaciones Unificadas con Cisco. Cisco *Business Edition* está conformado con servicios UC de configuraciones mínimas, el producto está orientado a instalaciones menores a mil usuarios.

La configuración disponible para BE6000M se detalla en la Tabla 2-6. De acuerdo con la documentación de Cisco, los recursos virtuales necesarios para cada producto y soportados por BE6000M se detallan en la Tabla 2-7.

Tabla 2-6 Configuración física de servidor BE6M-M5-k9. [18]

Cantidad	Cisco *Part Number*	Descripción
1	UCSC-C220-M5SX	*UCS C220 M5 SFF 10 HD w/o CPU, mem, HD, PCIe, PSU*
1	UCS-CPU-4114	*2.2 GHz 4114/85W 10C/13.75MB Cache/DDR4 2400MHz*
3	UCS-MR-X16G1RS-H	*16GB DDR4-2666-MHz RDIMM/PC4-21300/single rank/x4/1.2v*
6	UCS-HD300G10K12N	*300GB 12G SAS 10K RPM SFF HDD*
1	UCSC-RAID-M5	*Cisco 12G Modular RAID controller with 2GB cache*
1	R2XX-RAID5	*Enable RAID 5 Setting*
1	UCSC-RAILB-M4	*Ball Bearing Rail Kit for C220 & C240 M4 & M5 rack servers*
1	UCSC-PSU1-770W	*Cisco UCS 770W AC Power Supply for Rack Server*
4	UCSC-BBLKD-S2	*UCS C-Series M5 SFF drive blanking panel*
1	UCSC-PSU-BLKP1U	*Power Supply Blanking Panel for C220 M4 servers*
1	CBL-SC-MR12GM52	*Super Cap cable for UCSC-RAID-M5 on C240 M5 Servers*
1	UCSC-SCAP-M5	*Super Cap for UCSC-RAID-M5, UCSC-MRAID1GB-KIT*
1	UCSC-HS-C220M5	*Heat sink for UCS C220 M5 rack servers 150W CPUs & below*
1	CIMC-LATEST	*IMC SW (Recommended) latest release for C-Series Servers.*
1	C1UCS-OPT-OUT	*Cisco ONE Data Center Compute Opt Out Option*

Tabla 2-7 Configuración de archivos OVA para productos UC en BE6000M.

Producto	Capacidad de usuarios	vCPU	vRAM	vDisk	vNIC
CUCM	1000 usuarios	2	6 GB	1 x 80 GB	1
CUCMIMP	1000 usuarios	1	4 GB	1 x 80 GB	1
CUC	1000 usuarios	1	4 GB	1 x 160 GB	1
Expressway-C / *Expressway-E*	*SMALL*: Hasta 2500 registros como *proxy* de CUCM.	2	4 GB	1 x 132 GB	1 / 2 (1 GB)
CPC	3000 dispositivos finales	1	2 GB	1 x 90 GB	1

Configuración de reglas en *Firewall* de Quito y Guayaquil

Los servicios de Comunicaciones Unificadas estarán detrás de un *firewall*, por esta razón se deben configurar reglas de control de acceso de acuerdo con la información de las Tablas 2-8, 2-9 y 2-10.

Tabla 2-8 Uso de puertos TCP/UDP para los servicios de UC. (Parte 1 de 3).

Descripción Origen	Descripción Destino	Puertos TCP o UDP Destino	Descripción
CUCM (Base de Datos)	CUCM (Base de Datos)	TCP/1500,1501,1510, 1511	Comunicación de base de datos entre miembros del *cluster*.
CUCM (Base de Datos)	CUCM (Base de Datos)	TCP/1515	Replicación de bases de datos entre nodos, durante el proceso de instalación.
CUCM	Dispositivos finales de usuario	ICMP	Comunicación en ambos sentidos entre los dispositivos finales de UC y el CUCM.
CUCM	Servidor SFTP	TCP/22	Comunicación desde el CUCM para el envío de *backups* de configuración y CDRs (*Call Detail Records*).
Dispositivos finales de usuario y *Gateway* de Voz	CUCM	UDP/69	Descarga de *firmware* y archivos de configuración mediante TFTP.
Dispositivos finales de usuario y *Gateway* de Voz	CUCM	TCP/6970	Descarga de *firmware* y archivos de configuración desde servidor TFTP sobre TCP.
CUCM, CUC, CUCMIMP	Servidor NTP	UDP/123	Conexión con servicio NTP.
Dispositivos finales de usuario	CUCM	TCP/8443	Consultas de directorio mediante servicio UDS (*User Data Services*)
CUCM	LDAP externo	TCP/ 389, 636, 3268, 3269	Consultas hacia LDAP (*Lightweight Directory Access Protocol*) externo.
*Web Browse*r	CUCM, CUC, CUCMIMP	TCP/22	Administración vía SSH.
*Web Browse*r	CUCM, CUC, CUCMIMP	TCP/80,8080,443,8443,	Administración *Web* en protocolos HTTP y HTTPS.

Tabla 2-9 Uso de puertos TCP UDP para los servicios de UC. (Parte 2 de 3).

Descripción Origen	Descripción Destino	Puertos TCP o UDP Destino	Descripción
Teléfono IP y *Gateway* de Voz	CUCM	TCP/2000	SCCP (*Skinny Client Control Protocol*).
Teléfono IP	CUCM	TCP/2443	SCCPS (*Secure Skinny Client Control Protocol*)
Teléfono IP	CUCM	TCP/2445	Servicio de verificación de servidor confiable.
Teléfono IP y *Gateway* de Voz	CUCM	TCP-UDP/5060	Teléfonos SIP, comunicación en ambos sentidos.
Teléfono IP y *Gateway* de Voz	CUCM	TCP/5061	Teléfonos con uso de SIP seguro, la comunicación es en ambos sentidos.
Teléfono IP	CUCM	TCP/8080	Servicios *Web* para teléfonos IP.
Gateway de Voz	CUCM	TCP/1720	Señalización H.225 para *gateways* H323. Comunicación en ambos sentidos.
Gateway de Voz	CUCM	TCP/2427,2428	Control MGCP (*Media Gateway Control Protocol*)
Teléfono IP y *Gateway* de Voz	CUCM	UDP /16384 - 32767	RTP (*Real-Time Protocol*) y SRTP (*Secure Real-Time Protocol*). Este rango se utiliza cuando el CUCM está como *proxy* en la llamada. Por ejemplo, cuando ofrece recursos de *software* para conferencias.
CUC	CUC	TCP/22000, 20500, 20501, 20502, 19003, 1935	Comunicación entre nodos de *cluster* CUC.
CUC	CUC	TCP-UDP/22001	*Heartbeat* entre nodos CUC de *cluster*.
CUC	CUC	TCP/5007	Servicio *web* habilitado entre nodos del *cluster* CUC.
CUC	CUC	TCP/1515	Replicación de bases de datos entre nodos CUC.
Teléfono IP	CUC	TCP/21000–21512	Comunicación con aplicaciones desde *Unity Connection.*
CUC	CUC	TCP/1500,1501	Comunicación de base de datos entre nodos del *cluster* CUC.

Tabla 2-10 Uso de puertos TCP UDP para los servicios de UC. (Parte 3 de 3).

Descripción Origen	Descripción Destino	Puertos TCP o UDP Destino	Descripción
Dispositivos finales de usuario	CUC	TCP-UDP/5060–5199	Control de tráfico SIP desde CUC.
CUC	CUC	TCP/1502, 1503	Comunicación de base de datos entre servidores CUC.
Dispositivos finales de usuario	CUC	UDP/16384–21511	Comunicación de audio hacia los servidores CUC.
Servidores de Correo	CUC	TCP/7080,7443	Intercambio de notificaciones entre CUC y servidores *Exchange.*
CUC	CUCM	TCP/2000	Conexión SCCP con CUCM.
CUC	CUCM	UDP/69	Conexión para descarga de certificados digitales.
CUC	Directorio Activo o *Domain Controller*	TCP/53, 389 ó 636	Utilizado en configuración de Mensajería Unificada con *Microsoft,* Los puertos 389 y 636 cuando se utiliza LDAP para la comunicación con los controladores de dominio.
CUC	CUCM	TCP/80, 443, 8080, and 8443	Sincronización de usuarios a través de HTTP y HTTPS con CUCM.
CUC	*Microsoft Exchange servers*	TCP/25, 143, 993	Comunicación para Mensajería Unificada.
Cisco *Jabber*	CUC	TCP/80, 443,143,993	Conexión entre Cisco *Jabber* y CUC.
Cisco *Jabber*	CUCM	TCP/2748	Control de función de teléfono para usuarios desde CUCM.
Clientes IM de terceros	CUCMIMP	TCP/8082,8083	Servicio HTTP por *default* en servidor IM *and Presence* para clientes *software* de terceros.
Cliente de chat por XMPP	CUCMIMP	TCP/5222	Puerto de acceso a cliente *software* de chat.

Dispositivos UC para usuarios

Todos los usuarios de la organización podrán utilizar Cisco *Jabber* en al menos un dispositivo. El uso de Cisco *Jabber* se realizará en base a las necesidades de comunicación para los usuarios relacionado con las necesidades del negocio. Por ejemplo; para el negocio es importante que un vendedor pueda ser contactado en todo momento.

Para la organización, el equipo de ventas, jefes de sucursal y gerentes, tendrán Cisco *Jabber* en dos dispositivos: el computador portátil y un *smartphone.* El resto de los usuarios de la organización dispondrán de Cisco *Jabber* en su computador portátil.

La distribución de teléfonos IP en los puestos de trabajo, se realiza de acuerdo con la información de la Tabla 2-2. Los teléfonos IP físicos con capacidades de video están destinados a gerentes y jefes de área. Los modelos que se contemplan en el diseño son los indicados en la Tabla 2-11.

Tabla 2-11 Cantidad y tipo de Teléfonos IP.

Modelo de Teléfono IP	Número de dispositivos	Descripción
Cisco IP Phone 7861	2	Teléfonos de operadora.
Cisco IP Conference Phone 7832	5	Teléfonos para salas de reuniones.
Cisco IP Phone 8845	10	Teléfonos con capacidad de Video telefonía.
Cisco IP Phone 7841	165	Teléfonos IP básicos

a) *Cisco IP Phone 7861*

Teléfono IP que dispone de 16 botones programables, que pueden ser utilizados para configuración de líneas adicionales o para marcado rápido con opción de monitoreo de estados de telefonía de las extensiones programadas (ver Figura 2-2).

Figura 2-2 *Cisco IP Phone 7861*.

b) *Cisco IP Conference Phone 7832*

Teléfono para sala de reuniones, orientado a conferencias de audio (ver Figura 2-3). Cuenta con la capacidad de brindar servicio a salas de reuniones de hasta 16 metros cuadrados.

Figura 2-3 Cisco *IP Conference Phone 7832*.

c) *Cisco IP Phone 8845*

Teléfono IP con capacidades de voz y video. Cuenta con una cámara de video 720p HD H.264 AVC (ver Figura 2-4).

Figura 2-4 *Cisco IP Phone 8845*.

d) *Cisco IP Phone 7841*

Teléfono IP orientado a usuarios con actividad moderada de llamadas, cuenta con cuatro botones programables alrededor de la pantalla (ver Figura 2-5).

Figura 2-5 *Cisco IP Phone 7841*.

Licencias

En base a la información del diseño, se requieren las licencias que se indican en la Tabla 2-12.

Tabla 2-12 Licencias para solución de Comunicaciones Unificadas.

Licencia	Número de licencias (Necesidad actual)	Número de licencias (Crecimiento en 5 años)	Descripción de usuarios
Cisco UWL *Standard*	20	5	Gerentes, jefes de área, y equipo de ventas
Cisco *Enhanced Plus*	157	30	Usuarios en general
Cisco *Enhanced*	5	0	Salas de reuniones
Cisco *Basic Messaging – Unity Connection*	157	30	Buzones de voz para usuarios en general.

Configuración general para dispositivos finales de Comunicaciones Unificadas

En el servicio CUCM, para el correcto funcionamiento de los dispositivos finales de Comunicaciones Unificadas, se debe configurar un colector denominado *Device Pool,* el cual se aplica en cada dispositivo final. Se configura un *Device Pool* por cada sucursal, y la configuración se detalla en la Tabla 2-13.

Plan de Marcado

La configuración de plan de marcado en CUCM, consiste en los siguientes elementos:

- Patrón de marcado, conjunto de símbolos que representan los dígitos que se marcan desde un dispositivo final de Comunicaciones Unificadas.
- *Partition,* se denomina a la etiqueta que se da a un patrón de marcado.
- *Calling Search Space* (CSS), conjunto de *partitions* con el cual se define un perfil o permiso de llamadas.

El patrón de marcado puede contener dígitos del 0 al 9, *, #, y caracteres *wilcards* en el patrón, en la Tabla 2-14 se describen algunos *wilcards* soportados por CUCM.

Los *partitions* son etiquetas que se dan a los patrones configurados, con esto se clasifica el patrón, por ejemplo: [23]XXXXXX coincide con la marcación de números locales en Quito, entonces se puede colocar la etiqueta o *partition* “pt_local_uio”

para poder clasificarlo. Del mismo modo se puede definir el patrón 09XXXXXXXX y colocar el *partition* pt_celular.

Tabla 2-13 Configuración inicial para dispositivos finales.

Parámetro	Descripción	Valor
Servers	En esta opción se muestran los servidores que son parte del *cluster* CUCM. Los nodos también incluyen al servidor de presencia que es parte del clúster desde la versión 10 de la solución de Cisco CUCM. Estos parámetros aparecen ya configurados luego de la instalación.	192.168.50.10 192.168.51.10
CM *Group*	Grupos de servidores CUCM con servicio de *Call Manager* activo para poder ofrecer alta disponibilidad a los dispositivos finales.	Para Quito, Cuenca, Ambato: CMG_1: 192.168.50.10 Para Guayaquil, Loja, El Coca: CMG_2: 192.168.51.10
Phone NTP *Reference*	Se ingresa la dirección IP del servidor NTP al cual los dispositivos finales se van a conectar. Adicional a la dirección IP se configura el modo de conexión, el cual se recomienda colocarlo como *Unicast.*	IP *Address*: 192.168.50.5 *Mode: Unicast*
Date / Time Group	En esta sección se configura la zona horaria, y el formato de fecha y hora que se mostrará en el *display* del teléfono IP. En esta sección se selecciona la referencia NTP que se configura en la sección anterior; se pueden configurar varios para poder ponerlos en orden para alta disponibilidad.	Time Zone: GMT-5:00 America/Guayaquil. Separator: / (Slash). Date Format: M/D/Y. Time Format: 24-hour. Phone NTP reference: 192.168.50.5
SRST	Es la información del dispositivo que va a brindar el servicio de supervivencia de llamada.	IP *Address*: Dirección IP del *Gateway* de cada sucursal. *Port*: 2000 *SIP Network/IP Address*: Dirección IP del *Gateway* de cada sucursal. SIP *Port*: 5060

Tabla 2-14 *Wildcards* para configuración de patrones de marcado.

Símbolo	Descripción	Ejemplo
X	Cuando se utiliza la X en el patrón, coincide con cualquier dígito simple entre el 0 y el 9.	El patrón de marcado 9XXX tiene coincidencias con el rango de números del 9000 al 9999.
!	Coincide con uno o más dígitos del 0 al 9.	El patrón 91! coincide con todos los dígitos entre 910 y 9199999999999999999
?	Tiene coincidencia con cero o más dígitos del *wildcard* precedente.	91X?, coincide con el rango del 91 al 9199999999999999999
+	Tiene coincidencia con uno o más dígitos del *wildcard* precedente.	91X+, coincide con el rango desde el 910 al 9199999999999999999
[ ]	Los dígitos que se encierran entre los corchetes son opciones de un solo espacio en el patrón.	907[12]0, representa los siguientes números: 90710 y 90720.
-	Es utilizado en conjunto con los corchetes para indicar que las opciones de dígitos están dentro de un rango.	9071[1-5], representa los números dentro del rango 90711 al 0715.
\+	El *backslash* sirve como escape para el símbolo +. Se utiliza para poder configurar patrones que usen en + como dígito de números internacionales.	Para poder coincidir con el número internacional +1 800 721 7549, se utiliza el patrón: \+1XXXXXXXXXX.
.	El punto sirve para poder separar uno o varios dígitos del patrón configurado utilizando la opción *"predot".*	El patrón 9.2XXX, luego de la opción *predot* solo se enviará 2XXX.

Como ya se indicó un CSS es un conjunto de *partitions*, y con esto se define cuál es el conjunto de patrones que se debe tomar en cuenta cuando desde un

dispositivo un usuario realiza una marcación. Por ejemplo: se tiene CSS_LOCAL que contiene solo el *partition* pt_local_uio, y cuando a un dispositivo se aplica este CSS entonces el usuario no podrá marcar otro número que no coincida con el patrón [23]XXXXXX.

La configuración de *partitions* y CSS se definen en la Tabla 2-15.

Tabla 2-15 Plan de marcado: CSS y *Partitions*.

PARTITIONS / **CSS**	**PT_911**	**PT_INTERNAS**	**PT_SERV**	**PT_LOCAL**	**PT_NACIONAL**	**PT_CELULAR**	**PT_EXTERIOR**
CSS_INTERNAS	X	X					
CSS_INTER_SERV	X	X	X				
CSS_LOCAL	X	X	X	X			
CSS_LOC_NAC	X	X	X	X	X		
CSS_LOC_NAC_CEL	X	X	X	X	X	X	
CSS_LOC_NAC_CEL_EXT	X	X	X	X	X	X	X

Los prefijos por utilizar en las extensiones de cada sucursal se definen en base al código de área de cada provincia. Las extensiones serán de 4 dígitos y los patrones para la asignación de extensiones se especifica en la Tabla 2-16.

El prefijo 1 no se utiliza en el plan de extensiones, porque coincide con los números de servicio del proveedor de la PSTN, por ejemplo, el número 140 para el *call center* de citas médicas del IESS.

El prefijo 8 se utilizará para números de extensión internos. Estos números se utilizan para la integración de CUCM con CUC en la función de número piloto de correo de voz y operadora automática.

Las llamadas hacia la PSTN se realizarán anteponiendo el prefijo 9. Los patrones para la configuración de llamadas hacia la PSTN se muestran en la Tabla 2-17.

Se utiliza un solo patrón para las llamadas locales y nacionales, y dependiendo de la sucursal la llamada saldrá por el *Gateway* local. A esta característica se la denomina *Local Route Group,* y se especifica la troncal SIP o grupo de puertos

analógicos que un teléfono IP debe utilizar para llamadas externas dentro de la configuración del *Device Pool.*

Tabla 2-16 Patrones para extensiones telefónicas por sucursal.

Patrón de número de extensión	Descripción
2XXX	Extensiones de matriz Quito.
4XXX	Extensiones de sucursal Guayaquil.
71XX	Extensiones de sucursal Cuenca.
31XX	Extensiones de sucursal Ambato.
72XX	Extensiones de sucursal Loja.
61XX	Extensiones de sucursal El Coca.

Tabla 2-17 Patrones de marcado.

Patrón	*Partition*	Descripción
1XX	PT_SERV	Números de servicio de la operadora, por ejemplo: 104.
911	PT_911	Número de emergencias
9.911	PT_911	Número de emergencias[6]
9.[23]XXXXXX	PT_LOCAL	Números locales en cada sucursal.
9.0[2-7]XXXXXXX	PT_NACIONAL	Números Nacionales
9.09XXXXXXXX	PT_CELULAR	Números celulares
9.00X!	PT_EXTERIOR	Números internacionales
9.\+!	PT_EXTERIOR	Números internacionales

Configuración de Usuarios

Todos los usuarios contarán con los servicios de telefonía IP, mensajería instantánea, correo de voz y presencia. Para asociar los servicios a cada usuario es necesario configurar un perfil de servicios, para ello se debe definir cada servicio

[6] Se recomienda configurar el patrón de números de emergencia con y sin prefijo de salida.

UC en la página de configuración *Cisco Unified CM Administration -> User Management -> User Settings -> UC service,* de acuerdo con lo que se detalla en la Tabla 2-18.

Tabla 2-18 Servicios UC para aplicar a usuarios.

Servicio UC	Descripción	Parámetros	
IM *and Presence*	Servicio de presencia y mensajería instantánea.	Producto	*Unified CM (IM and Presence)*
		Nombre	CUCMIMP
		Dirección IP	192.168.50.11, 192.168.51.11
Voicemail	Servicio de Correo de Voz.	Producto	*Unity Connection*
		Nombre	CUC
		Dirección IP	192.168.50.12, 192.168.50.12
		Puerto	443
		Protocolo	HTTPS
CTI (*Computer Telephony Integration*)	Servicio para control de teléfonos IP.	Producto	CTI
		Nombre	CUCM_CTI
		Dirección IP	192.168.50.10, 192.168.50.10
		Puerto	2748
		Protocolo	TCP

Al momento de crear el usuario se deben seleccionar las opciones *Home Cluster, Enable User for Unified CM IM and Presence*, y escoger el perfil de servicio UC en la casilla *UC Service Profile,* para que el usuario pueda utilizar el servicio de mensajería instantánea y presencia.

Servicio de Presencia y Mensajería Instantánea

Para configurar los servicios de Presencia y Mensajería instantánea se debe realizar la integración entre el servidor CUCM y CUCMIMP, para lo cual se deben completar las tareas descritas en la Tabla 2-19.

Tabla 2-19 Tareas previas para configuración de presencia y mensajería unificada.

Tarea	Descripción
Configurar los dispositivos telefónicos IP y asignarle un DN (*Directory Number*) a cada uno.	Esta configuración se realiza en la página de administración del CUCM, en la ruta *Cisco Unified CM Administration -> Device -> Phone.* En la configuración de cada teléfono IP se debe activar la opción *Allow Control of Device from CTI,* para permitir al teléfono la interoperabilidad con el cliente Cisco *Jabber*.
Configurar los usuarios y asociar un dispositivo a cada uno.	La configuración se realiza en sección *Cisco Unified CM Administration -> User Management -> End User.*
Configurar la sección *line appearance* para el usuario con respecto a los dispositivos asociados.	Esta configuración puede realizarse desde la página de usuarios (*Cisco Unified CM Administration -> User Management -> End User*) y también de la página de teléfonos (*Cisco Unified CM Administration -> Device -> Phone*).
Añadir a los usuarios al grupo de privilegios *CTI enabled user group.*	Esto se realiza para habilitar el control del teléfono de escritorio*. Cisco Unified CM Administration -> User Management -> User Group*

Tabla 2-20 Configuración de Troncal SIP para presencia.

Parámetro	Valor	
Tipo de Troncal	SIP *Trunk*	
Protocolo del dispositivo	SIP	
Tipo de servicio de la Troncal	Ninguno	
Nombre	CUPS-SIP-*TRUNK*	
Device Pool	DP_UC	
Dirección de destino	192.168.50.11	
Puerto de destino	5060	
Perfil SIP	*Standard SIP Profile*	
SIP *Trunk Security Profile*	Nombre	CUP *Trunk*
	Device Security Mode	*Non Secure*
	Incoming Transport Type	TCP+UDP
	Outgoing Transport Type	TCP
	Habilitar los siguientes ítems	*Accept Presence Subscription* *Accept Out-of-Dialog REFER* *Accept Unsolicited Notification* *Accept Replaces Header*

Luego de ejecutadas las tareas de la Tabla 2-19, del lado del CUCM resta crear una troncal SIP hacia el servidor CUCMIMP. La troncal SIP se debe configurar en el menú *Cisco Unified CM Administration* > *Device* > *Trunk.* En la Tabla 2-20, se muestran los parámetros a utilizar para la troncal SIP entre CUCM y CUCMIMP.

En el servidor CUCMIMP se deben activar los siguientes servicios en la página de configuración *Cisco Unified IM and Presence Serviceability -> Tools -> Service Activation*:

- *Cisco SIP Proxy*
- *Cisco Presence Engine*
- *Cisco XCP Connection Manager*
- *Cisco XCP Authentication Service*

Tabla 2-21 Información para integración entre CUCM y CUC.

Parámetro	Descripción	Valor
Partition	*Partition* para los números de extensión de cada puerto de conexión con *Unity Connection.*	PT_VMPORT
	Partition para número piloto del grupo de líneas o puertos de conexión con *Unity Connection.*	PT_VMPILOT
CSS	CSS que incluye solo el *partition* PT_VMPORT.	CSS_VMPORTS
Device Pool	*Device Pool* para los puertos de conexión con *Unity Connections.*	DP_VMPORTS
Número de puertos	Número de conexiones virtuales concurrentes entre CUCM y CUC.	10
Piloto de Correo de Voz	Número piloto para la conexión con *Unity Connection* para servicio de Correo de voz	8100
Piloto para operadora automática	Número piloto para la conexión con *Unity Connection* para el servicio de Operadora automática.	8101
Número de extensión para WMI *on* (*Message Waiting Indicator*)	Número de extensión que utiliza el sistema para poder encender el led de notificación de mensaje de voz.	8102
Número de extensión para WMI *off* (*Message Waiting Indicator*)	Número de extensión que utiliza el sistema para poder apagar la notificación de mensaje de voz.	8103
Rango de números de extensión para puertos de *Unity Connection*	El sistema creará el número de puertos que se indique en el *wizzard* de configuración, y asignará un número de extensión a cada puerto de acuerdo con el rango que se defina.	8104-8128

Correo de voz

Antes de realizar la integración entre el servidor CUCM y Cisco *Unity Connection,* los usuarios deben tener configurado el parámetro *Primary Extension,* adicional al perfil de servicios UC. El parámetro *Primary Extension* se relaciona al dispositivo asociado al usuario, y aparece como una opción no editable para seleccionar. En base a este parámetro se crea el buzón de correo de voz luego de importar las cuentas del CUCM desde *Unity Connection.*

Para la integración entre *Cisco Unified Communications Manager y Cisco Unity Connection* es necesario contar con la información y definiciones descritas en la Tabla 2-21.

Tabla 2-22 *Gateways* de Voz para sucursales.

Sucursal	*Gateway* de Voz	Supervivencia.	Unity Express
Quito	Cisco 4321 *Integrated Services Router*	No	No
Guayaquil	Cisco 4321 *Integrated Services Router*	No	No
Cuenca	Cisco 4321 *Integrated Services Router*	Si	Si
Ambato	Cisco 4321 *Integrated Services Router*	Si	Si
Loja	Cisco 4321 *Integrated Services Router*	Si	Si
El Coca	Cisco 4321 *Integrated Services Router*	Si	Si

Tabla 2-23 Licencias de supervivencia por sucursal.

Sucursal	Número de Teléfonos IP	Licencias
Quito	84	No Aplica
Guayaquil	70	No Aplica
Cuenca	7	2 licencias FL-CME-SRST-5=
Ambato	9	2 licencias FL-CME-SRST-5=
Loja	8	2 licencias FL-CME-SRST-5=
El Coca	6	2 licencias FL-CME-SRST-5=

Gateway de Voz

El Gateway de Voz que se asigne a cada sucursal depende del número de usuarios que deben recibir servicio en modo supervivencia y del número de llamadas simultáneas que se estima recibirá la operadora automática de CUE.

El número de licencias definen el número de teléfonos IP que el *Gateway* soportará en modo supervivencia. Las licencias de producto se compran en números de parte para 5 (FL-CME-SRST-5=) y 25 (FL-CME-SRST-25=) dispositivos finales en modo supervivencia.

Utilización de canal de datos por llamada

Para el cálculo de ancho de banda por llamada, se utiliza la fórmula que se indica en la Ecuación 2-1.

Tamaño de *payload* [*Bytes*] = (códec *bit rate*) * Intervalo de muestreo [milisegundos]

Tamaño de paquete de voz = (Cabecera IP (20 *bytes*) /UDP (8 *bytes*) / RTP (12 *bytes*)) + (Tamaño de *payload*).

Tamaño de la trama de voz = (Cabecera Capa 2) + Tamaño de paquete de voz.

Paquetes por segundo = (*codec bit rate*) / (Tamaño de *payload*).

Ancho de Banda (AB) Capa 3 = (Tamaño de paquete de voz) * (Paquetes por segundo)

Ancho de Banda (AB) Capa 2 = (Tamaño de trama de voz) * (Paquetes por segundo)

Ecuación 2-1 Fórmula para cálculo de ancho de banda por llamada. [19]

CUCM soporta tres códecs: G.711, G.729 y G.723, el tamaño del *payload* de voz por paquete es configurable en los parámetros del sistema, y su valor se ingresa en milisegundos (Intervalo de muestreo). El valor por defecto de tasa de muestreo para G.711 es 20 milisegundos que equivalen a 160 *bytes* de *payload* por paquete de voz de acuerdo con su *bit rate* de 64Kbps, y el valor por defecto para G.729 es también de 20 milisegundos, pero el *bit rate* de G.729 es de 8 Kbps que da como resultado 20 *bytes* de *payload* de voz por paquete. En el diseño se contempla el uso de G.711 para llamadas dentro de la sucursal y G.729 para llamadas entre sucursales.

El siguiente es un ejemplo de cálculo para el códec G.729 en una red *Ethernet,* utilizando los valores por defecto para CUCM.

Tamaño de *payload* [*Bytes*] = (8 Kbps) * (20 ms) = 20 *bytes.*

Tamaño de paquete de voz = (40 *bytes*) + (20 *bytes*) = 60 *bytes*.

Tamaño de la trama de voz = (14 *bytes header* + 4 *bytes CRC*) + (60 *bytes*) = 78 *bytes*.

Paquetes por segundo = (8 Kbps) / (20 *bytes*) = 50 pps.

AB Capa 3 = (60 *bytes*) *** (**50 pps**) =** 3 KBps * 8 *bits/Byte* = **24 Kbps.**

AB Capa 2 = (78 *bytes*) *** (**50 pps**) =** 3.9 KBps * 8 *bits/Byte* = **31.2 Kbps**

Ecuación 2-2 Ejemplo de cálculo de ancho de banda con códec G.729.

Las tablas 2-24 y 2-25 son extraídas de la documentación de Cisco, y muestran la información de consumo de ancho de banda por códec en Capa 2 y 3.

Tabla 2-24 Capa 2: Consumo de ancho de banda por códec. [19]

CODEC	Header Type and Size						
	Ethernet 14 Bytes	PPP 6 Bytes	ATM 53-Byte Cells with a 48-Byte Payload	Frame Relay 4 Bytes	MLPPP 10 Bytes	MPLS 4 Bytes	WLAN 24 Bytes
G.711 and G.722-64k at 50.0 pps	85.6 kbps	82.4 kbps	106.0 kbps	81.6 kbps	84.0 kbps	81.6 kbps	89.6 kbps
G.711 and G.722-64k (SRTP) at 50.0 pps	87.2 kbps	84.0 kbps	106.0 kbps	83.2 kbps	85.6 kbps	83.2 kbps	N/A
G.711 and G.722-64k at 33.3 pps	78.4 kbps	76.3 kbps	84.8 kbps	75.7 kbps	77.3 kbps	75.7 kbps	81.1 kbps
G.711 and G.722-64k (SRTP) at 33.3 pps	79.5 kbps	77.4 kbps	84.8 kbps	76.8 kbps	78.4 kbps	76.8 kbps	N/A
iLBC at 50.0 pps	36.8 kbps	33.6 kbps	42.4 kbps	32.8 kbps	35.2 kbps	32.8 kbps	40.8 kbps
iLBC (SRTP) at 50.0 pps	38.4 kbps	35.2 kbps	42.4 kbps	34.4 kbps	36.8 kbps	34.4 kbps	42.4 kbps
iLBC at 33.3 pps	27.7 kbps	25.6 kbps	28.3 kbps	25.0 kbps	26.6 kbps	25.0 kbps	30.4 kbps
iLBC (SRTP) at 33.3 pps	28.8 kbps	26.6 kbps	42.4 kbps	26.1 kbps	27.7 kbps	26.1 kbps	31.5 kbps
G.729A at 50.0 pps	29.6 kbps	26.4 kbps	42.4 kbps	25.6 kbps	28.0 kbps	25.6 kbps	33.6 kbps
G.729A (SRTP) at 50.0 pps	31.2 kbps	28.0 kbps	42.4 kbps	27.2 kbps	29.6 kbps	27.2 kbps	35.2 kbps
G.729A at 33.3 pps	22.4 kbps	20.3 kbps	28.3 kbps	19.7 kbps	21.3 kbps	19.8 kbps	25.1 kbps
G729A (SRTP) at 33.3 pps	23.5 kbps	21.4 kbps	28.3 kbps	20.8 kbps	22.4 kbps	20.8 kbps	26.2 kbps

Tabla 2-25 Capa 3: Consumo de Ancho de Banda por códec. [19]

CODEC	Sampling Rate	Voice Payload in Bytes	Packets per Second	Bandwidth per Conversation
G.711 and G.722-64k	20 ms	160	50.0	80.0 kbps
G.711 and G.722-64k (SRTP)	20 ms	164	50.0	81.6 kbps
G.711 and G.722-64k	30 ms	240	33.3	74.7 kbps
G.711 and G.722-64k (SRTP)	30 ms	244	33.3	75.8 kbps
iLBC	20 ms	38	50.0	31.2 kbps
iLBC (SRTP)	20 ms	42	50.0	32.8 kbps
iLBC	30 ms	50	33.3	24.0 kbps
iLBC (SRTP)	30 ms	54	33.3	25.1 kbps
G.729A	20 ms	20	50.0	24.0 kbps
G.729A (SRTP)	20 ms	24	50.0	25.6 kbps
G.729A	30 ms	30	33.3	18.7 kbps
G.729A (SRTP)	30 ms	34	33.3	19.8 kbps

Sobre el diseño, el peor caso es que todas las extensiones de cada sucursal estén en una llamada con una extensión de otra sucursal, y que cada uno de los teléfonos tengan una llamada en espera. Con esto se puede tener un estimado de consumo de canal de acceso a la WAN por sucursal, que se detalla en la Tabla 2-26.

Tabla 2-26 Consumo máximo de ancho de banda por sucursal.

Sucursal	Número máximo de llamadas entre sucursales	Consumo de ancho de banda por llamada con G.729 en MPLS	Consumo total de ancho de banda
Quito	168	25.6 Kbps	4.3008 Mbps
Guayaquil	140	25.6 Kbps	3.584 Mbps
Cuenca	14	25.6 Kbps	358.4 Kbps
Ambato	18	25.6 Kbps	460.8 Kbps
Loja	16	25.6 Kbps	409.6 Kbps
El Coca	12	25.6 Kbps	307.2 Kbps

Presupuesto referencial

La Tabla 2-27 presenta los valores cotizados para cada elemento del diseño descrito. El valor de cada ítem incluye los servicios de mantenimiento de *software.*

Tabla 2-27 Presupuesto referencial.

Producto	Número de parte	Cantidad	Precio Unitario (USD)	Subtotal (USD)
Business Edition 6000	BE6M-M5-k9	2	12,500.50	25,001.00
Teléfono CP-7861	CP-7861-3PWNAK9-RF	2	288.00	576.00
Teléfono CP-7832	CP-7832-K9=	5	1,116.00	5,580.00
Teléfono CP-8845	CP-8845-K9=	10	599.75	5,997.50
Teléfono CP-7841	CP-7841-K9=	165	378.15	62,493.75
Unified Workspace Licensing v. 11.x	CUWL-11X-K9	25	382.50	9,562.50
UCL *Enhanced Plus*	LIC-UCM-11X-ENHP-A	187	349.05	65,272.35
UCL *Enhanced*	LIC-CUCM-11X-ENH-A	5	247.95	1,239.75
Cisco *Basic Messaging – Unity Connection*	UNITYCN11-STD-USR	187	92.25	17,250.75
ISR4321/K9	ISR4321/K9	6	2,527.20	15,163.20
FL-CME-SRST-5=	FL-CME-SRST-5=	8	170.00	1,360.00
			TOTAL (USD)	209,496.8

Diagrama LLD

Una vez definidos los elementos del diseño y su rol dentro de la Solución de Comunicaciones Unificadas, se elabora un diagrama con más detalle para facilitar la operación y mantenimiento de la Solución de Comunicaciones Unificadas.

Los servicios de Comunicaciones Unificadas se ubican en una red de servidores en los centros de datos de Quito y Guayaquil. Para que los servicios sean alcanzados por los dispositivos de usuario, es necesario que el *firewall* cuente ya con la configuración de permisos de acuerdo con la Tabla 2-1. La Figura 2-6, describe la topología que se va a implementar en la organización.

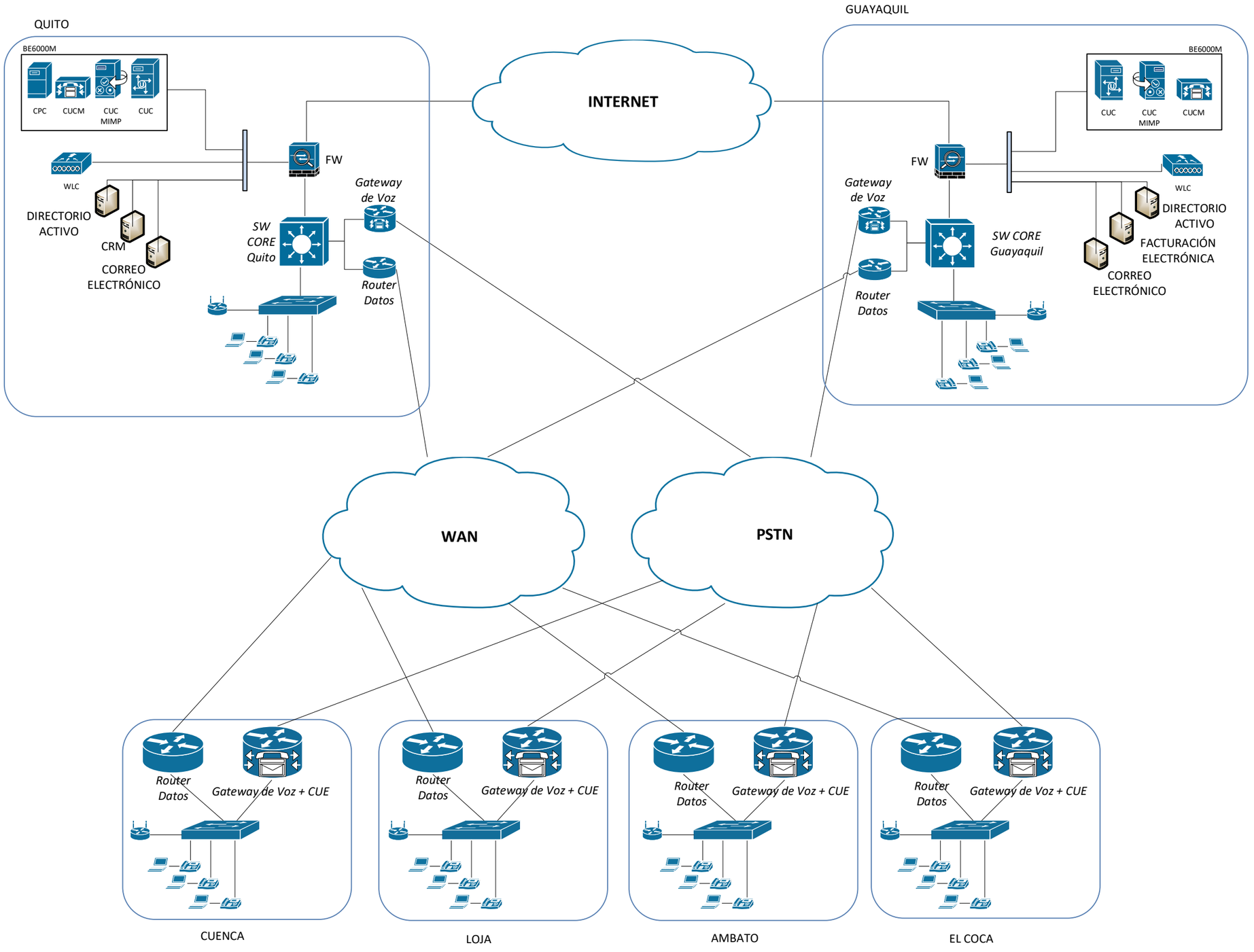

Figura 2-6 Diagrama LLD.

2.2 Implementación de Prototipo de Comunicaciones Unificadas

Descripción del prototipo de Comunicaciones Unificadas

El prototipo por implementar debe permitir realizar las pruebas necesarias sobre los métodos de acceso desde Internet a una solución de Comunicaciones Unificadas con Cisco. En el prototipo se utilizará el cliente de *software Cisco Jabber,* el cual, con todas sus funciones permitirá probar los servicios de Comunicaciones Unificadas. Para el correcto funcionamiento de *Cisco Jabber*, una solución debe contener como mínimo los siguientes servicios implementados:

- *Cisco Unified Communications Manager*.
- *Cisco Unified Communications Manager IM and Presence.*

Al prototipo se va a añadir el servicio *Cisco Unity Connection,* para probar el comportamiento del acceso al correo de voz desde Internet.

El prototipo contendrá servicios no Cisco, que permitan al usuario de prueba utilizar adecuadamente los servicios de Comunicaciones Unificadas. Los servicios no Cisco son los siguientes:

- DHCP (*Dynamic Host Configuration Protocol*).
- DNS (*Domain Name Servers*) interno y externo.
- CA (*Certification Authorities*).
- NTP (*Network Time Protocol*).

El servicio DNS se implementa en la red interna, así como en la red que emula al Internet, y adicionalmente en la sección de Internet se instalará un emulador de canal para poder dar complejidad a las conexiones desde esa sección del prototipo. El emulador de canal se instala entre el *firewall* e Internet, tal y como se muestra en la Figura 2-7.

La configuración de cada servicio se realizará en base a una dimensión mínima para poder cumplir con las pruebas de las opciones de acceso a los servicios de Comunicaciones Unificadas desde Internet. Cada usuario de prueba iniciará sesión en el servicio de Comunicaciones Unificadas desde la red Interna y la externa, y en cada caso se recolectará información relevante para poder efectuar el análisis.

El análisis de las pruebas será complementado con el resultado de una encuesta dirigida a usuarios, no técnicos, de Comunicaciones Unificadas con Cisco para poder evaluar la experiencia de uso del servicio.

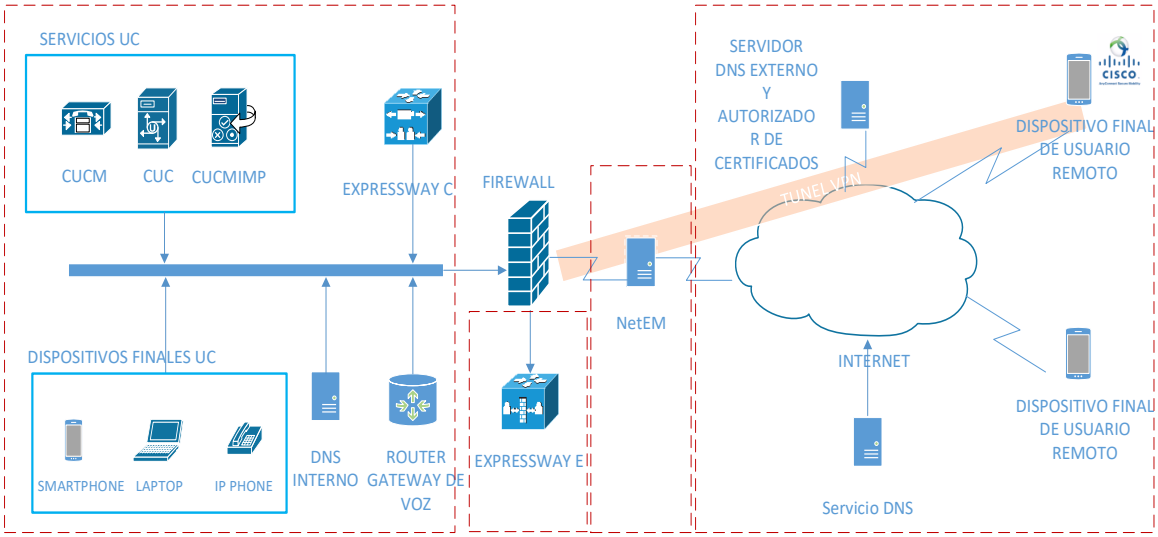

Figura 2-7 Diagrama Lógico del prototipo de Comunicaciones Unificadas.

Elementos del Prototipo de Comunicaciones Unificadas

Para la instalación del prototipo de Comunicaciones Unificadas se dispone de los siguientes elementos:

- Computador portátil Alienware 17 R3, Intel Core i7-6700HQ CPU @ 2.60GHz, 32GB RAM.
- Un Switch Catalyst 2960 de 24 puertos 10/100.
- Un Firewall PIX 515E.
- Cisco *Router* 2801 con licencia UC.
- Dos *Access Points*.

En el computador portátil se instala *VMware Workstation Pro,* sobre el cual se levanta una máquina virtual con *VMware VSphere ESXi,* que es soportado para la instalación de productos de Comunicaciones Unificadas con Cisco. [20]

a) Información de Máquinas Virtuales

Para el funcionamiento del prototipo de Comunicaciones Unificadas, se instalarán los servicios indicados en la Figura 2-7. En la Tabla 2-28 se describen cada una de las máquinas virtuales del prototipo de Comunicaciones Unificadas.

Para la creación de los servidores virtuales del prototipo, se considera el uso de recursos mínimos de CPU, memoria RAM y disco. En la Tabla 2-29 se detallan los recursos mínimos necesarios para el funcionamiento de cada máquina virtual del prototipo de Comunicaciones Unificadas.

Tabla 2-28 Máquinas Virtuales.

Servidor Virtual	Descripción
CUCM	Servidor para el control de llamadas.
CUCMIMP	Servidor de Presencia y Mensajería Instantánea.
CUC	Servidor de cuentas de correo de voz.
Expressway-C	Servidor interno para servicio de acceso a Comunicaciones Unificadas desde Internet sin VPN.
Expressway-E	Servidor de borde para servicio de acceso a Comunicaciones Unificadas desde Internet sin VPN.
Windows Server	Servidor DNS Interno.
Windows Server	Servidor DNS externo y CA.
Servidor Linux Centos	Emulador de canal de datos.

Tabla 2-29 Recursos para máquinas virtuales.

Servidores Virtuales	CPU virtual	RAM virtual (GB)	Espacio en disco virtual (GB)
CUCM	2	4	80
CUCMIMP	1	2	80
CUC	1	4	160
Expressway-C	2	4	132
Expressway-E	2	4	132
Windows Server	1	4	160
Servidor Linux Centos	1	2	40

b) Direccionamiento IP

El prototipo se implementará con diferentes rangos de direcciones IP, sobre una única VLAN, ya que las limitaciones de la tarjeta de red del computador portátil en donde se instala *VMware* ESXi, no permite utilizar 802.1Q. El direccionamiento IP utilizarse se detalla en la Tabla 2-30 y las direcciones IP para los elementos del prototipo se detalla en la Tabla 2-31.

Al aumentar la información definida de direccionamiento IP, el diagrama lógico quedaría de la forma indicada en la Figura 2-8.

Tabla 2-30 Direccionamiento IP definido.

Nombre de la red	Dirección de Red	Máscara	*Gateway* por defecto
Red Interna	192.168.236.0	255.255.255.0	192.168.236.1
Red DMZ	192.168.237.0	255.255.255.0	192.168.237.1
Red de acceso a Internet	6.0.0.0	255.255.255.252	6.0.0.1
Internet	5.0.0.0	255.255.255.224	5.0.0.1

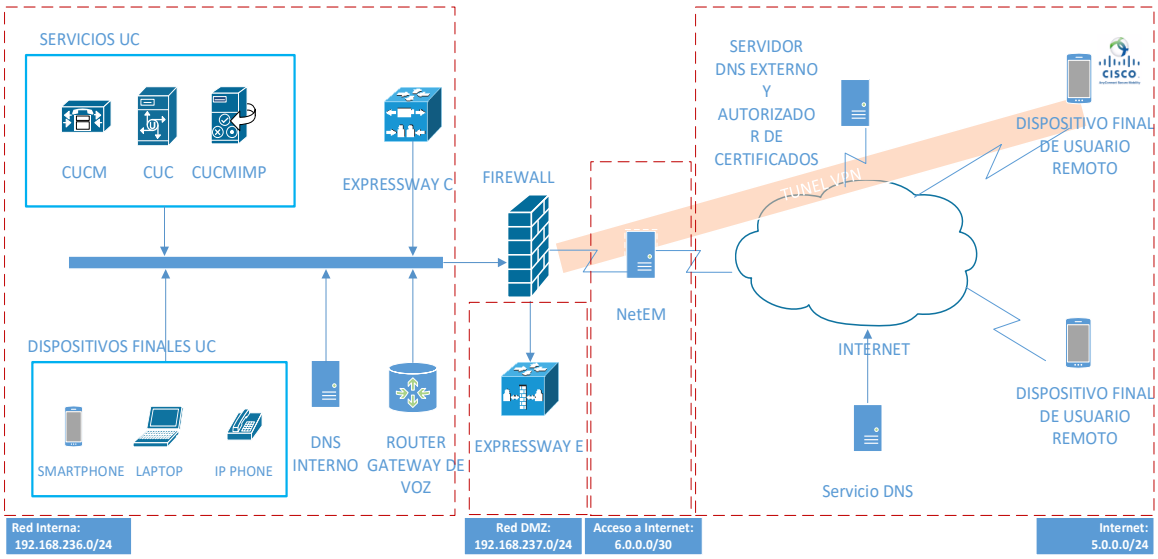

Figura 2-8 Diagrama lógico de red.

Tabla 2-31 Direcciones IP de elementos del prototipo.

Servicio	Nombre de *host*	Dirección IP	Máscara de subred	*Gateway* por defecto
CUCM	Cucm	192.168.236.2	255.255.255.0	192.168.236.1
CUCMIMP	Cucmimp	192.168.236.3	255.255.255.0	192.168.236.1
CUC	Cuc	192.168.236.4	255.255.255.0	192.168.236.1
Gateway de Voz	Vgw	192.168.236.254	255.255.255.0	192.168.236.1
Expressway C	Collabc	192.168.236.5	255.255.255.0	192.168.236.1
Expressway E	Collabe	192.168.237.2	255.255.255.0	192.168.237.1
DNS Interno	Interno	192.168.236.6	255.255.255.0	192.168.236.1
DNS Externo	Externo	5.0.0.10	255.255.255.224	5.0.0.1
NetEM nic01	Netem	6.0.0.1	255.255.255.252	
NetEM nic02	Netem	5.0.0.1	255.255.255.224	
Firewall inside	fw_tesis	192.168.236.1	255.255.255.0	
Firewall DMZ	fw_tesis	192.168.237.1	255.255.255.0	
Firewall Outside	fw_tesis	6.0.0.2	255.255.255.252	6.0.0.1

Requisitos de instalación para cada elemento virtual del Prototipo

a) *VMware ESXi* [21]

En el prototipo se utiliza un computador personal con los recursos necesarios para poder instalar las máquinas virtuales. *VMware* ESXi se instala sobre *VMware Workstation*, la cual es una configuración soportada y recomendada por el fabricante para laboratorios de certificación.

En la Tabla 2-32, se listan los requerimientos mínimos para la instalación de *VMware* ESXi.

Tabla 2-32 Recursos disponibles para ESXi.

Requerimientos	Valor Actual
Procesador x86 de 64 bits como mínimo de doble núcleo	Intel® Core ™ i7-6700HQ CPU @ 2.60 GHz
Memoria RAM de mínimo 4 GB	32 GB de RAM
Una o más tarjetas de red	Tarjeta de red Gigabit Ethernet
Espacio en disco sin particionar para creación de máquinas virtuales.	Disponible 800 GB de espacio en disco sin partición.

Todos los servidores del prototipo serán virtualizados sobre una máquina virtual de ESXi. Para los servicios de Comunicaciones Unificadas con Cisco se utilizan archivos OVA (*Open Virtual Appliance*) con las configuraciones estándar de acuerdo con el número de usuarios que soporta.

b) *Cisco Unified Communications Manager*, *Cisco Unified Communications Manager IM & Presence*, *Cisco Unity Connection*

Para la instalación de las máquinas virtuales de CUCM, CUCMIMP y CUC, en las tablas 2-33, 2-34 y 2-35 se presentan las especificaciones de los archivos OVA de acuerdo con el número de usuarios que el prototipo podría soportar de acuerdo con los recursos definidos en la Tabla 2-29.

Tabla 2-33 Configuración de archivos OVA para CUCM.

Capacidad	vCPU	vRAM	vDisk	vNIC
150	2	4 GB	1 x 80 GB	1

Tabla 2-34 Configuración de archivos OVA para CUCM IMP.

Capacidad	vCPU	vRAM	vDisk	vNIC
500	1	2 GB	1 x 80 GB	1
1000	1	2 GB	1 x 80 GB	1

Tabla 2-35 Configuración de archivos OVA para CUC.

Capacidad	vCPU	vRAM	vDisk	vNIC
200	1	4 GB	1 x 160 GB	1

c) *Expressway C* y *Expressway E*

El archivo OVA para *Expressway*, se utiliza tanto para *Expressway* C y E. Para *Expressway* se considera el tamaño de la instalación al momento de desplegar el archivo OVA. Los tipos de instalación considerados son: *Small, Medium,* y *Large. Small* y *Medium* tienen los mismos requisitos de recursos para la creación de la máquina virtual, la diferencia radica en que el tipo de despliegue *Small* se aplica en un producto orientado a pequeñas y medianas empresas, el producto se denomina *Business Edition*. El tipo de instalación para el prototipo se detalla en la Tabla 2-36.

Tabla 2-36 Tipo de despliegue para Cisco *Expressway*.

Tipo de instalación	Característica de operación
Small / Medium	Hasta 2500 registros como *proxy* de CUCM. Hasta 100 videollamadas o 200 llamadas de audio.

De acuerdo con el tipo de instalación, los recursos a utilizar de acuerdo con la configuración del archivo OVA se especifican en la Tabla 2-29.

d) *Windows Server* (Servicio DNS Y CA)

El servicio DNS y la Autoridad Certificadora, se instalarán en un servidor *Windows* virtual. Se consideran los recursos mínimos para este prototipo, que se indican en la Tabla 2-37.

Tabla 2-37 Recursos mínimos para máquina virtual de *Windows Server*.

Componente	Valor mínimo
CPU	Procesador mono núcleo de 64 bits de mínimo 1.4 Ghz
Memoria RAM	4 GB
Espacio en Disco	160 GB

e) Servidor CentOS (NETEM)

NETEM provee la funcionalidad de emulación de red para pruebas de protocolos y aplicaciones emulando las propiedades de una WAN. Los recursos mínimos para la creación del servidor virtual CentOS, se detallan en la Tabla 2-38

Tabla 2-38 Valores recomendados de recursos para instalación de servidor CentOS.

Componente	Valor mínimo
CPU	1 vCPU
Memoria RAM	2 GB
Espacio en Disco	40 GB

Configuración inicial para cada elemento del Prototipo

a) Configuración inicial de productos CUCM, CUCMIMP y CUC

Para la instalación de los servicios CUCM, CUCMIMP y CUC se necesita definir usuarios y contraseñas para las distintas interfaces de administración de producto. La Tabla 2-39 contiene la información de usuarios a configurar en el momento de la instalación.

Como parte del proceso de instalación en los productos indicados se deben configurar los parámetros para el certificado de seguridad de cada servidor. Por defecto se genera un certificado *selfsigned,* que puede ser reemplazado por un certificado emitido por un CA confiable. Los datos de la Tabla 2-40 utiliza el servidor en la generación del CSR (*Certificate Signing Request*).

La configuración de red necesaria para la instalación de los servicios UC del prototipo de Comunicaciones Unificadas con Cisco, está ya definida en la Tabla 2-31. En el proceso de instalación el sistema realiza una prueba de conectividad contra el *Gateway* de la red, si la prueba no es exitosa no permite continuar el proceso. Igual a la validación del *Gateway* de la red, el *wizard* de instalación comprueba los parámetros descritos en la Tabla 2-41.

Tabla 2-39 Información de credenciales para productos Cisco UC [22].

Parámetros de configuración	Descripción	Parámetro por configurar
Usuario administrador	Usuario de administración del sistema operativo.	administrador
Contraseña de administrador	Contraseña para cuenta administrador.	Tesis.2017
Nombre de usuario de aplicación	Usuario de las aplicaciones instaladas en el sistema, por ejemplo: el usuario de la aplicación web para administración.	Appadmin
Contraseña de usuario de aplicación	Especifica la contraseña para las aplicaciones del sistema.	Tesis.2017
Contraseña de seguridad de CUCM	Los servidores en un clúster utilizan esta contraseña para poder establecer la comunicación entre ellos. Esta contraseña define en el nodo principal del clúster (*Publisher*), y se ingresa en los servidores adicionales para el clúster. El servidor IM and *Presence* se considera un nodo del clúster CUCM, por ende, requiere este parámetro para poder continuar con el proceso de instalación.	cisco.cucm

Tabla 2-40 Parámetros de Certificado Digital.

Parámetros de configuración	Descripción	Parámetro por configurar
Organization	Utilizado para crear certificado auto firmado.	TESIS
Unit	Utilizado para crear certificado auto firmado.	IT
Location	Utilizado para crear certificado auto firmado.	QUITO
State	Utilizado para crear certificado auto firmado.	PICHINCHA
Country	Utilizado para crear certificado auto firmado.	EC

Tabla 2-41 Datos de acceso a servicio NTP y DNS.

Parámetros de configuración	Descripción	Parámetro por configurar
Servidor DNS primario	CUCM contacta a este servidor DNS primero para intentar resolver un nombre de host.	5.0.0.10
Dominio	Representa el nombre de dominio en donde el servicio está localizado.	tesis.com
Zona horaria	Zona horaria local del sitio de la instalación.	América/Guayaquil
Servidor NTP	Durante la instalación del nodo principal CUCM se debe especificar la dirección IP de un servicio NTP. El resto de los nodos pueden configurar para que tomen al equipo CUCM principal como servidor NTP.	192.168.236.254

b) Configuración inicial para *Expressway C* y *Expressway E*

Los servicios *Expressway* C y *Expressway* E, se instalan con el mismo archivo OVA y luego de la configuración inicial se determina el rol del servidor al ingresar las licencias. Al momento de la instalación se requiere la información de usuario y contraseña especificada en la Tabla 2-42.

Tabla 2-42 Credenciales para Cisco *Expressway* C y E.

Parámetros de configuración	Descripción	Parámetro por configurar
Usuario administrador	Usuario de administración del sistema operativo.	Admin
Contraseña de administrador	Contraseña para cuenta administrador.	Tesis.2017

Los parámetros de red están definidos en la Tabla 2-30,y los parámetros adicionales para la instalación son los especificados para CUCM, CUCMIMP y CUC en las tablas 2-40 y 2-41.

c) Configuración inicial de *Gateway* de Voz y *Firewall*

La configuración inicial en el *Gateway* de voz se la realiza mediante línea de comandos al igual que la configuración del *Firewall.* En el *Firewall* del prototipo, luego de la configuración inicial, será posible ingresar a la

configuración por una interfaz gráfica denominada ASDM. Las tablas 2-43 y 2-44 detallan la configuración inicial del *Gateway* de Voz, y la Tabla 2-45 la del *Firewall* del prototipo.

Tabla 2-43 Configuración inicial de *Gateway* de Voz. (Parte 1 de 2).

Parámetros de configuración	Descripción	Parámetro por configurar
Banner	Mensaje que se presenta cuando un usuario ingresa al equipo por conexión de consola o SSH.	*banner motd #* ********** *VGW_UC* *Acceso Restringido a Personal autorizado* ********** *#*
Configuración AAA Local	Usuarios locales para administración del *Gateway* de Voz.	*aaa new-model* *aaa authentication login LOGIN_LOCAL local* *aaa authorization console* *aaa authorization exec default local* *aaa authorization exec LOGIN_LOCAL local*
Configuración de acceso por consola y remoto	Configuración de opciones de acceso remoto a la administración del *router*.	*line console 0* *exec-timeout 5 0* *logging synchronous* *login authentication LOGIN_LOCAL* *line vty 0 4* *exec-timeout 5 0* *logging synchronous* *login authentication LOGIN_LOCAL* *transport input telnet*
Interfaz LAN	Interfaz con direccionamiento IP dentro de la red Corporativa de Comunicaciones Unificadas.	*interface FastEthernet0/0* *ip address 192.168.236.254 255.255.255.0* *duplex auto* *speed auto* *no shutdown* *exit*

Tabla 2-44 Configuración inicial de *Gateway* de Voz (Parte 2 de 2.).

Parámetros de configuración	Descripción	Parámetro por configurar
Hostname	Nombre del *Router*	*hostname VGW_UC*
Nombre de usuario	Usuario de administración del equipo.	*username gwadmin secret cisco123* *username gwadmin privilege 15*
Configuración de servicio NTP	El *Gateway* de voz será el servidor NTP para la instalación de los servicios UC Cisco	*ntp master 1*
Configuración de Dominio	Nombre de dominio para el equipo.	*ip domain name tesis.com*

Tabla 2-45 Configuración inicial del *Firewall*.

Parámetros de configuración	Parámetro por configurar
Hostname	*hostname FWTESIS*
Nombre de usuario	*username fwadmin password cisco123*
Configuración de Dominio	*domain-name tesis.com*
Configuración de Interfaz V_INTERNA	*interface Ethernet0* *nameif INSIDE* *security-level 100* *ip address 192.168.236.1 255.255.255.0* *no shutdown*
Configuración de Interfaz V_DMZ	*interface Ethernet1* *nameif DMZ* *security-level 50* *ip address 192.168.237.1 255.255.255.0* *no shutdown*
Configuración de Interfaz V_OUTSIDE	*interface Ethernet2* *nameif OUTSIDE* *security-level 0* *ip address 6.0.0.2 255.255.255.0*
Configuración de acceso *web* para aplicación ASDM	*http server enable* *http 0.0.0.0 0.0.0.0 INSIDE* *aaa authentication http console LOCAL*
Configuración de acceso SSH	*ssh 0.0.0.0 0.0.0.0 INSIDE*
Configuración de usuarios locales para acceso por SSH	*aaa authentication ssh console LOCAL*
Configuración de servicio NTP	*ntp server 192.168.236.254 source INSIDE*

d) Configuración inicial de Servidor *Windows*

Los servidores *Windows* se instalarán con la información de las tablas 2-46 y 2-47, luego se realizará la configuración respectiva de los roles de cada servidor para el prototipo de Comunicaciones Unificadas.

Tabla 2-46 Información inicial para instalación de servidor externo *Windows*.

Dirección IP	5.0.0.10
Máscara	255.255.255.0
Default *Gateway*	5.0.0.1
Dominio	tesis.com
Nombre host	Externo
Usuario	*Administrator*
Contraseña	Cisco123

Tabla 2-47 Información inicial para instalación de servidor interno Windows.

Dirección IP	192.168.236.6
Máscara	255.255.255.0
Default *Gateway*	192.168.236.1
Dominio	tesis.com
Nombre host	Interno
Usuario	*Administrator*
Contraseña	Cisco123

e) Emulador de Canal de Datos

Este servicio se implementa en servidor virtual CentOS, al cual se le asignarán dos tarjetas de red virtuales para que pueda ejercer la función enrutador y poder generar retardos cuando pasa a través de él. La información necesaria para la instalación de servidor virtual se detalla en la Tabla 2-48.

Tabla 2-48 Información inicial para instalación de servidor Linux CentOS.

Dirección IP Interfaz 1	6.0.0.1
Máscara Interfaz 1	255.255.255.252
Dirección IP Interfaz 2	5.0.0.1
Máscara Interfaz 2	255.255.255.224
Dominio	tesis.com
Nombre host	*Router*_netem
Usuario	Root
Contraseña	Tesis.2017

Instalación de elementos del Prototipo de Comunicaciones Unificadas

a) Instalación de servidor *VMware ESX*

La implementación del prototipo inicia con la instalación del servidor *VMware* ESX en el equipo designado. El servidor ESX se lo instala sobre *VMware Workstation* utilizando los recursos definidos en la Tabla 2-32.

En la página de administración de *VMware Workstation* nos dirigimos al menú *File -> New Virtual Machine,* luego de eso se mostrará el *wizard* o *setup assistant* para la creación de la nueva máquina virtual, donde se realizan los siguientes pasos:

1. Se escoge *Typical* en el tipo de *wizard* de instalación.
2. Se selecciona la imagen .iso del sistema operativo ESX.
3. Se escoge el sistema operativo y la versión.
4. Se configura el nombre de la máquina virtual su ubicación en el equipo físico.
5. Se ingresa el valor de espacio de disco necesario para el servidor ESX.
6. Luego aparece el resumen para la creación de la máquina virtual, y se puede editar los valores de memoria RAM y CPU para cumplir con los valores definidos.
7. Se da clic en finalizar y el sistema creará la máquina virtual.
8. Una vez creada la máquina virtual, se enciende para que inicie el proceso de instalación del sistema operativo, se ingresan los parámetros de instalación ya definidos.

VMware ESX puede ser administrado desde *VMware Workstation*, pero para la creación de las máquinas virtuales utilizando los archivos OVA de Cisco, es necesario utilizar la aplicación *Web* o el cliente de escritorio *VMware VSphere.*

b) Instalación de servidores virtuales Cisco

Una vez instalado *VMware ESX,* se accede a la administración desde el cliente *VSphere* (ver Figura 2-9) para poder instalar las máquinas virtuales del prototipo. Las máquinas virtuales de la solución de Cisco de Comunicaciones Unificadas se instalan utilizando archivos OVA (*Open Virtualization Application/Appliance*).

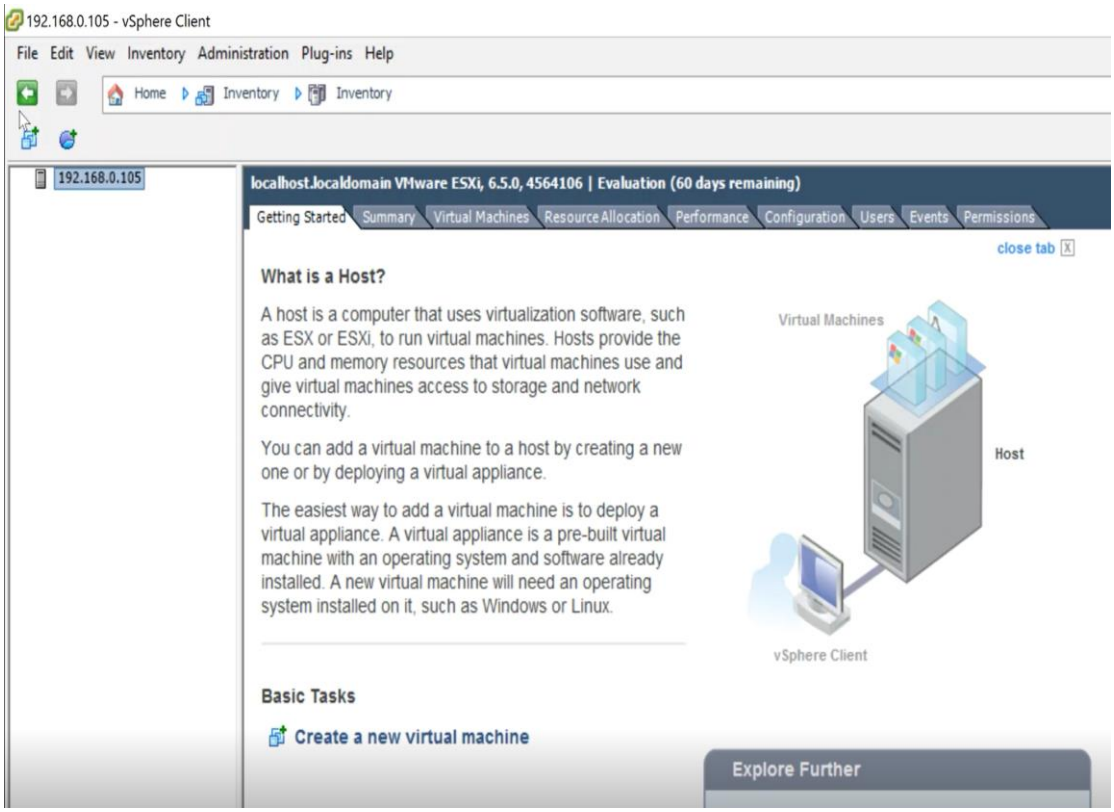

Figura 2-9 *VMware VSphere.*

Para desplegar el archivo OVA del servicio CUCM se realiza los siguientes pasos:

1. Desde *vsphere client* se dirige al menú *File -> Deploy OVF Template,* para iniciar el *wizard* de instalación.
2. En el *wizard* de instalación se escoge el archivo OVA que vamos a instalar en ESX.
3. Luego de seleccionar el archivo OVA, en la siguiente sección se muestra la información de la máquina que se va a instalar.
4. Se especifica el nombre de la máquina virtual.
5. Se elige el tipo de instalación basándonos en el número de usuarios a soportar. Para el prototipo se elige la opción más baja, y en la pantalla se muestra los recursos que se van a utilizar para la máquina virtual.
6. Para el formato de disco, se deja la opción que está por defecto. La recomendación de Cisco para los servicios de Comunicaciones Unificadas es que todos los recursos sean asignados de manera estática y no en modo *Thin Provision* que aumenta el tamaño del disco a medida que se va utilizando hasta llegar al máximo configurado.

7. Al final se muestra un resumen sobre la configuración de la máquina virtual. Si se requiere realizar algún cambio, se lo hace sobre la máquina creada utilizando cualquiera de los clientes de administración de *VMware.*

El procedimiento descrito, aplica también para la creación de las máquinas virtuales de los servicios Cisco *Unity Connection* y Cisco *Unified Communications Manager IM and Presence.* Cisco *Expressway* utiliza el mismo archivo OVA para instalar el servicio *Core* o *Edge,* el tipo de servicio se define al momento de activar las licencias. Para el archivo OVA de Cisco *Expressway* se tiene un procedimiento diferente al *wizard* de instalación de un OVA de CUCM. El tipo de instalación a elegir en el archivo OVA de *Expressway* está ya definido en la Tabla 2-36, y el detalle de su instalación se describe en el ANEXO I.

En el caso de Cisco *Expressway,* el sistema operativo es instalado con el despliegue del archivo OVA. Luego de realizar los pasos descritos, se ingresa mediante la consola de *VMware* al sistema para iniciar sesión utilizando las credenciales por defecto del producto: "*admin*" como nombre de usuario y "*TANDBERG*", esto inicia un pequeño *wizard* en el cual se ratifica la configuración IP del equipo. Cuando se confirma la información estará disponible el acceso a la administración web.

c) Instalación de servidores virtuales Linux y *Windows*

Para ambos servidores la creación se la realiza desde *VMware Workstation*. Para *Windows Server* se realizan los siguientes pasos:

1. En la primera ventana del *wizard* de configuración, se escoge la opción *typical.*
2. Se elige el sistema operativo *Windows Server* 2012 de acuerdo con la imagen de instalación disponible.
3. Se ingresa un nombre a la máquina virtual.
4. Se especifica el espacio en disco definido para la máquina virtual.
5. Al final se mostrará un resumen de los recursos que se crearán en la máquina virtual.

Para la creación del servidor Linux Centos se realizan los siguientes pasos:

1. En la primera ventana del *wizard* de configuración, se escoge la opción *typical.*
2. Se elige el sistema operativo Linux 7 (64-bit).
3. Se ingresa el nombre de la máquina virtual.
4. Configuración de espacio de disco virtual para máquina virtual.
5. Finalmente se muestra un resumen de la configuración con la que se creará la máquina virtual.

Instalación de sistemas operativos

Para instalar el sistema operativo de los servidores virtuales se utilizó el cliente *VSphere,* en él se siguen los siguientes pasos para poder iniciar el servidor en las opciones del BIOS:

1. Primero se selecciona la máquina virtual desde el cliente *VSphere* y se da clic en la opción *Edit virtual machine settings.*
2. En la pestaña *Options* se selecciona la opción *Boot Options* del panel izquierdo de la ventana, y se marca el *checkbox* dentro del recuadro *Force BIOS Setup.*

Luego de aplicar los pasos descritos, al encender la máquina virtual se mostrarán las opciones de BIOS, y en estas opciones se cambia el orden de arranque para que inicie desde el CDROM. Es necesario seleccionar la imagen de instalación antes de guardar los cambios de BIOS y reiniciar el servidor, y así el equipo iniciará el *wizard* de instalación del sistema operativo.

Para cada servicio se sigue paso a paso el *wizard* de instalación utilizando la información ya definida para el prototipo.

a) Instalación de Sistema Operativo de productos Cisco UC

Los servicios de Cisco: CUCM, CUC y CUCMIMP tienen procedimiento similar de instalación de sistema operativo, a continuación, se detalla el *wizard* de instalación:

1. En cada máquina virtual se configura el uso de la imagen de instalación.
2. Se enciende la máquina virtual, y debido a la configuración de opciones de arranque, inicia en el menú de BIOS, donde se cambia el orden de *Boot*, guardamos la configuración y reiniciamos el servidor.
3. El *wizard* de instalación empieza con la pantalla en la cual se puede realizar una validación de la imagen de instalación.
4. Se selecciona el producto a instalar.

5. Confirmación de la versión de software a instalar.
6. Inicio de *wizard* de instalación. En los tres servicios se muestra la misma pantalla de opciones.
7. Introducción a la instalación del servicio, luego de seleccionar *Proceed* en el paso anterior.
8. Se selecciona la zona horaria o *time zone* adecuado para la instalación.
9. En las opciones de configuración de tarjeta de red, se deja por defecto la configuración de MTU, y en la opción de escoger DHCP para la configuración IP, se selecciona no.
10. Se ingresa la configuración IP.
11. Se configura el usuario y contraseña de sistema operativo.
12. Se completa el formulario de información de certificado digital.
13. En el prototipo se creará un nodo para cada servicio. En los servicios de CUCM y CUC, se indica que es el primer nodo, pero en el servicio CUCMIMP el nodo es siempre secundario y forma parte del clúster CUCM.
14. Se configura la información del servidor NTP.
15. Se configura una contraseña de seguridad que se utiliza en el momento que se añaden nuevos nodos al clúster.
16. Se muestra la pantalla para la configuración de un servidor SMTP, esta configuración es opcional.
17. Configuración de usuario de administración.
18. Luego de ingresada la información solicitada en el *wizard*, se confirma esta información para que inicie el proceso de instalación.

Tal y como se indicó en el paso 13, al servicio CUCMIMP se configura como nodo secundario, porque forma parte del clúster CUCM, y es necesario que el servicio CUCM esté ya instalado.

b) Instalación de Sistema Operativo para servidores *Windows* y Linux

Para la instalación del sistema operativo *Windows Server* se realiza el siguiente procedimiento:

1. Cuando inicia el servidor virtual desde la imagen de instalación, aparecerá una pantalla, en la cual damos clic en “Instalar ahora”.
2. Se selecciona el sistema operativo a instalar.
3. Se aceptan los términos de licencia para continuar con la instalación.

4. Se selecciona el espacio de *storage* para el servidor *Windows Server*.
5. Luego de la selección de espacio de *storage*, se inicia el proceso de instalación de sistema operativo.
6. Una vez que finaliza la instalación, el equipo se reinicia y presenta la pantalla para la configuración de la contraseña del usuario administrador.

El servidor Linux se lo instala realizando los siguientes pasos:

1. Al cargar la imagen de instalación, se mostrará la pantalla inicial del *wizard* en la cual seleccionamos la opción "*Install* CentOS Linux 7".
2. Se selecciona el lenguaje para la instalación.
3. Se valida que todos los ítems de la pantalla de resumen de instalación estén listos.
4. Se selecciona el disco virtual para la instalación de sistema operativo y continuamos con él *wizard*.
5. Mientras el proceso de instalación continúa, el sistema permite configurar la contraseña para el usuario *root*.

Configuraciones de Servicios del prototipo de Comunicaciones Unificadas

a) Configuración general para dispositivos finales de Comunicaciones Unificadas

En el servicio CUCM se deben realizar las siguientes configuraciones esenciales para el correcto funcionamiento de los dispositivos finales de Comunicaciones Unificadas.

Todas las configuraciones descritas en la Tabla 2-49 se ingresan en un colector denominado *Device Pool,* el cual se configura en cada dispositivo final.

Luego de realizadas las configuraciones generales, es necesario que los siguientes servicios estén activos en Cisco *Unified Communication Manager*:

- *Cisco CallManager,* es el servicio de administración de llamadas.
- *Cisco TFTP,* a través de este servicio los dispositivos finales descargan los archivos de configuración.
- *Cisco CTIManager,* servicio para control remoto del dispositivo final.

- *Cisco AXL Web Service,* servicio para integración y sincronización de información entre CUCM y otro producto de Comunicaciones Unificadas con Cisco, por ejemplo, CUCMIMP.
- *Cisco CAR Web Service,* servicio para extracción de los archivos de detalle de llamada.
- *Cisco Dialed Number Analyzer Server,* esta característica permite probar el plan de marcado.
- *Cisco Dialed Number Analyzer,* interfaz para utilizar *Cisco Dialed Number Analyzer Server*.

Tabla 2-49 Configuración inicial para dispositivos finales.

Parámetro	Descripción	Valor
Servers	En esta opción se muestran los servidores que son parte del clúster CUCM. Los nodos también incluyen al servidor de presencia que es parte del *cluster* desde la versión 10 de la solución de Cisco CUCM. Estos parámetros aparecen ya configurados luego de la instalación.	192.168.236.2 192.168.236.3
CM *Group*	Grupos de servidores CUCM con servicio de *Call Manager* activo para poder ofrecer alta disponibilidad a los dispositivos finales.	CMG_1: 192.168.236.2
Phone NTP Reference	Se ingresa la dirección IP del servidor NTP al cual los dispositivos finales se van a conectar. Adicional a la dirección IP se configura el modo de conexión, el cual se recomienda colocarlo como *Unicast*.	IP *Address*: 192.168.236.254 *Mode: Unicast*
Date / Time Group	En esta sección se configura la zona horaria, y el formato de fecha y hora que se mostrará en el display del teléfono IP. En esta sección seleccionamos la referencia NTP que se configura en la sección anterior, se pueden configurar varios para poder ponerlos en orden para alta disponibilidad.	*Time Zone*: GMT-5:00 America/Guayaquil. *Separator*: / (Slash). *Date Format*: M/D/Y. *Time Format*: 24-hour. *Phone* NTP *reference*: 192.168.236.254
SRST	Es la información del dispositivo que va a brindar el servicio de supervivencia de llamada.	IP *Address*: 192.168.236.254 *Port*: 2000 SIP *Network*/IP *Address*: 192.168.236.254 SIP *Port*: 5060

Para poder activar los servicios es necesario ingresar a la página de configuración *Cisco Unified Serviceability,* y al menú "*Tools -> Service Activation"* luego se selecciona el nodo al cual se activan los servicios.

b) Plan de marcado

Para el plan de marcado se utilizará el definido en la Tabla 2-15, para el diseño expuesto. Los patrones de llamada se configuran igual que en el capítulo. Los patrones por configurar están descritos en la Tabla 2-16.

c) Configuración de Usuarios

Los usuarios del prototipo serán locales, y la configuración se detalla en la Tabla 2-50.

Tabla 2-50 Usuarios de prueba para el prototipo.

Apellido	Nombre	Nombre de Usuario	Contraseña	Correo electrónico	Número de extensión
Sánchez	Winston	wsanchez	12345	wsanchez@tesis.com	2001
Sánchez	Matías	msanchez	12345	msanchez@tesis.com	2002
Salcedo	Alex	Asalcedo	12345	asalcedo@tesis.com	2003
Sarmiento	Cisne	csarmiento	12345	csarmiento@tesis.com	2004

Todos los usuarios contarán con los servicios de telefonía IP, mensajería instantánea, correo de voz y presencia. Para asociar los servicios a cada usuario es necesario configurar un perfil de servicios, para ello se debe definir cada servicio UC en la página de configuración *Cisco Unified CM Administration -> User Management -> User Settings -> UC service,* de acuerdo con la Tabla 2-51.

El perfil de servicios se crea en *Cisco Unified CM Administration -> User Management -> User Settings -> Service Profile* (ver Figura 2-10).

Tabla 2-51 Servicios UC para aplicar a usuarios.

Tipo de servicio UC	Descripción	Parámetros	
IM *and Presence*	Servicio de presencia y mensajería instantánea.	Producto	CUCMIMP
		Nombre	CUCMIMP
		Dirección IP	192.168.236.3
Voicemail	Servicio de Correo de Voz.	Producto	*Unity Connection*
		Nombre	CUC
		Dirección IP	192.168.236.4
		Puerto	443
		Protocolo	HTTPS
CTI (*Computer Telephony Integration*)	Servicio para control de teléfonos IP.	Producto	CTI
		Nombre	CUCM_CTI
		Dirección IP	192.168.236.2
		Puerto	2748
		Protocolo	TCP

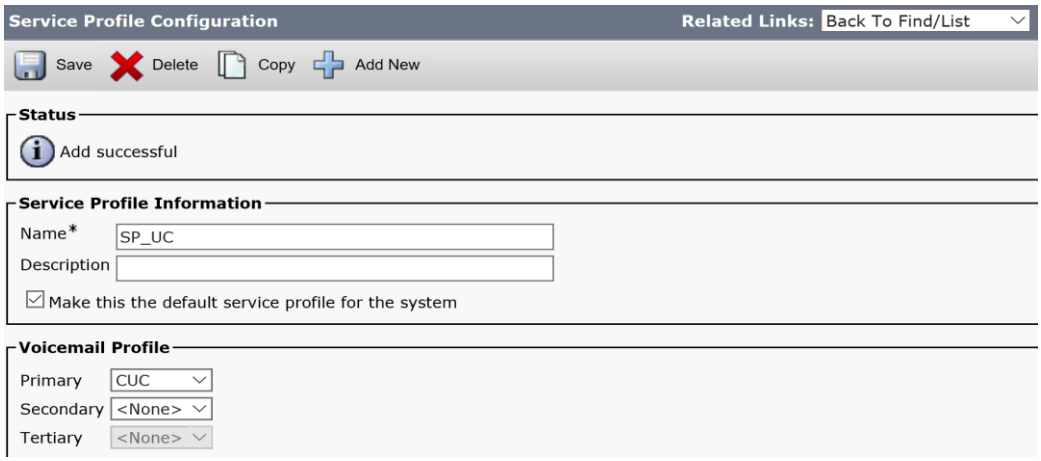

Figura 2-10 Ejemplo de configuración de perfil de servicios.

En el perfil creado se selecciona la opción de perfil por defecto, tal y como se indica en la Figura 2-10, ya que será el único perfil para el prototipo.

d) Configuración del servicio de Presencia y Mensajería Instantánea

Para configurar los servicios de Presencia y Mensajería instantánea se debe realizar la integración entre el servidor CUCM y CUCMIMP, para lo cual se deben completar las tareas previas descritas en el capítulo dos, en la Tabla 2-19.

Luego de configurar los servicios con la información de la Tabla 2-19, se crea una troncal SIP con los parámetros descritos en la Tabla 2-52.

En el servidor CUCMIMP se debe validar si están activos los siguientes servicios:

- *Cisco SIP Proxy*
- *Cisco Presence Engine*
- *Cisco XCP Connection Manager*
- *Cisco XCP Authentication Service*

Tabla 2-52 Configuración de Troncal SIP para presencia.

Parámetro	**Valor**	
Tipo de Troncal	SIP *Trunk*	
Protocolo del dispositivo	SIP	
Tipo de servicio de la Troncal	Ninguno	
Nombre	CUPS-SIP-*TRUNK*	
Device Pool	DP_UC	
Dirección de destino	192.168.236.3	
Puerto de destino	5060	
Perfil SIP	*Standard SIP Profile*	
SIP *Trunk Security Profile*	Nombre	CUP *Trunk*
	Device Security Mode	*Non Secure*
	Incoming Transport Type	TCP+UDP
	Outgoing Transport Type	TCP
	Habilitar los siguientes ítems	*Accept Presence Subscription* *Accept Out-of-Dialog REFER* *Accept Unsolicited Notification* *Accept Replaces Header*

e) Configuración de buzones de voz

Cada usuario del prototipo debe tener configurado el parámetro *Primary Extension,* adicional al perfil de servicios UC. En base a este parámetro se crea el buzón de correo de voz luego de importar las cuentas desde CUCM a *Unity Connection.*

Para la integración entre *Cisco Unified Communications Manager y Cisco Unity Connection* es necesario contar con la información y definiciones descritas en la Tabla 2-53.

f) Configuración de *Gateway* de Voz desde CUCM

Es necesario contar con la información de los modelos de tarjeta que contiene el *Gateway* de voz, esta información se la obtiene del comando *show inventory.* La configuración del *Gateway de voz* se la realiza en *Cisco Unified CM Administration > Device > Gateway,* y se añade uno con la información de la Tabla 2-54.

Tabla 2-53 Información para integración entre CUCM y CUC.

Parámetro	Descripción	Valor
Partition	*Partition* para los números de extensión de cada puerto de conexión con *Unity Connection.*	PT_VMPORT
	Partition para número piloto del grupo de líneas o puertos de conexión con *Unity Connection.*	PT_VMPILOT
CSS	CSS que incluye solo el *partition* PT_VMPORT.	CSS_VMPORTS
Device Pool	*Device Pool* para los puertos de conexión con *Unity Connections.*	DP_VMPORTS
Número de puertos	Número de conexiones virtuales concurrentes entre CUCM y CUC.	10
Piloto de Correo de Voz	Número piloto para la conexión con *Unity Connection* para servicio de Correo de voz	8100
Piloto para operadora automática	Número piloto para la conexión con *Unity Connection* para el servicio de Operadora automática.	8101
Número de extensión para WMI *on* (*Message Waiting Indicator*)	Número de extensión que utiliza el sistema para poder encender el led de notificación de mensaje de voz.	8102
Número de extensión para WMI *off* (*Message Waiting Indicator*)	Número de extensión que utiliza el sistema para poder apagar la notificación de mensaje de voz.	8103
Rando de números de extensión para puertos de Unity Connection	El sistema creará el número de puertos que se indique en el *wizzard* de configuración, y asignará un número de extensión a cada puerto de acuerdo al rango que se defina.	8104-8113

Una vez añadido el *Gateway* de voz, aparece la sección *Configured Slots, VICs and Endpoints,* en donde se selecciona la única opción de tarjeta que se muestra para el modelo 2801, y en el *SLOT 0* se escoge la tarjeta VIC2-2FXO.

Tabla 2-54 Configuración de *Gateway* de Voz.

Parámetro	Valor
Gateway Type	Cisco 2801
Protocolo	MGCP
Domain Name	VGWUC.tesis.com
Cisco Unified Communications Manager Group	CUCM_G

Cuando se da clic en guardar la configuración, aparecen dos íconos de puertos analógicos, éstos se configuran para poder utilizar el puerto para la conexión a la PSTN.

Desde el *Gateway* de voz se deben ejecutar dos comandos: *ccm-manager config server* 192.168.236.2, *ccm-manager config.* Luego de ejecutar el segundo comando, el *Gateway* de voz se comunica con el servidor CUCM configurado y descarga el archivo de configuración para poderlo aplicar[7].

g) Configuración de Supervivencia de Llamada

Para poder contar con Supervivencia de Llamada se debe configurar la característica MGCP *Fallback* (Solo en *Gateway* de Voz) y configurar SRST (*Survivable Remote Site Telephony*) en CUCM y *Gateway* de voz.

Cuando se configura MGCP *Fallback* y Cisco *Unified SRST*, se deben seguir los siguientes pasos:

[7] El nombre del archivo que solicita el *Gateway* de voz está conformado por el nombre de host y el dominio configurado, por esta razón se recomienda que el nombre de *host* no contenga caracteres especiales.

1. Definir la referencia SRST que usarán los teléfonos en la página de administración del CUCM.
2. Configurar la característica *Call Forward Unregistered* (CFUR), colocando el número telefónico al cual las llamadas serán redirigidas para alcanzar al sitio remoto. Es decir, cuando el sitio remoto pierde conexión WAN, desde el CUCM las extensiones de ese sitio se verán como no registradas, y en la línea de cada extensión existe la configuración que captura el estado no registrado de la extensión. Entonces cuando un usuario marca el número de extensión del sitio remoto, el sistema va a redirigir la llamada al número configurado en la línea.
3. Habilitar y configurar MGCP *fallback* y Cisco *Unified* SRST en el *Gateway* de voz.
4. Implementar un plan de marcado para ser utilizado en el sitio remoto cuando está en modo SRST. Se configura un plan de marcado simple ya que funcionará hasta recuperar la conexión a la WAN.

La configuración de referencia SRST está ya descrita en las configuraciones generales del CUCM para dispositivos finales, en la Tabla 2-55 se describen los pasos para realizar las configuraciones de SRST en el *Gateway* de voz.

Para habilitar las llamadas en el *Gateway* MGCP mientras se encuentra en modo SRST, se configura MGCP *fallback* para permitir que el *Gateway* MGCP en modo SRST asuma el control sobre los puertos de voz y sobre el procesamiento de llamadas. Los comandos que se deben aplicar en el *Gateway* son los siguientes:

1. *call-manager-fallback.*
2. *application.*
3. *global.*
4. *service alternate default.*

Luego de la activación de SRST y la configuración de MGCP *fallback,* es necesario configurar un plan de marcado en el *Router* para poder manejar llamadas en modo SRST. El plan de marcado se describe en las Tablas 2-56 y 2-57.

Tabla 2-55 Configuración SRST en *Gateway* de voz.

Actividad	Comando
Ingresar al modo de configuración *call-manager-fallback* para activar el modo SRST.	*call-manager-fallback*
Definir la dirección IP y el puerto al cual se conectará para el servicio SRST.	*ip source-address* 192.168.236.254 *port* 2000
Definir el número máximo de líneas o números de extensión que va a soportar.	*max-dn* 6
Definir el número máximo de teléfonos IP permitidos.	*max-ephones* 10
Definir un intervalo de *keepalive* hacia los teléfonos.	*keepalive* 20

Tabla 2-56 Plan de marcado para supervivencia de llamadas. (Parte 1 de 2)

Tipo de llamada	Configuración
Llamadas Locales	dial-peer voice 2 pots description Llamadas locales preference 1 destination-pattern 9[23]..... port 0/1/0 forward-digits 7 dial-peer voice 5 pots description Llamadas locales preference 2 destination-pattern 9[23]..... port 0/1/1 forward-digits 7

Tabla 2-57 Plan de marcado para supervivencia de llamadas. (Parte 2 de 2)

Tipo de llamada	Configuración
Llamadas Nacionales	dial-peer voice 1 pots description Llamadas Nacionales preference 1 destination-pattern 90[2-7]..... port 0/1/0 forward-digits 9 dial-peer voice 4 pots description Llamadas Nacionales preference 2 destination-pattern 90[2-7]..... port 0/1/1 forward-digits 9
Llamadas Celulares	dial-peer voice 3 pots description Llamadas a Celular preference 1 destination-pattern 909..... port 0/1/0 forward-digits 10 dial-peer voice 6 pots description Llamadas a Celular preference 2 destination-pattern 909..... port 0/1/1 forward-digits 10
Llamadas Internacionales	dial-peer voice 8 pots description Llamadas Internacionales preference 1 destination-pattern 900.T prefix 00 port 0/1/0 dial-peer voice 9 pots description Llamadas a Celular preference 2 destination-pattern 900.T prefix 00 port 0/1/1

h) Configuración de *Firewall* para uso de VPN de acceso remoto

De acuerdo con la configuración inicial, es posible acceder al *Firewall* a través de la aplicación ASDM, en la cual se puede ejecutar el *wizard* de configuración de VPNs. En el *wizard* de configuración se necesita la información descrita en la Tabla 2-58.

Tabla 2-58 Información para creación de VPN de acceso remoto.

Parámetro	Valor
VPN *Tunnel Type*	*Remote Access*
VPN *Tunnel Interface*	*OUTSIDE*
VPN *Client Type*	Cisco VPN *Client, reléase 3.X or higher*
Pre-shared Key	cisco123
Tunnel Group Name	VPNTESIS
Users	*fwadmin, user1, user2*
Pool de direcciones IP	Nombre: vpnpool
	Dirección inicio: 192.168.238.100
	Dirección fin: 192.168.238.200
	Máscara de red: 255.255.255.0
DNS *Server*	192.168.236.6
Domain Name	tesis.com
IKE *Policy*	*Encryption:* 3DES
	Authentication: SHA
	Diffie-Hellman Group: 2
IPSec *Rule*	*Encryption:* 3DES
	Authentication: SHA
	Perfect Forwarding Secrecy (PFS): enabled
	PFS *Diffie-Helman Group:* 1
Dirección de red para excepción de NAT	192.168.236.0/24, 192.168.237.0/24

i) Configuración de *Firewall* para Cisco *Expressway*

En el *Firewall* es necesario configurar las siguientes reglas para el correcto funcionamiento de la solución de Cisco *Expressway*:

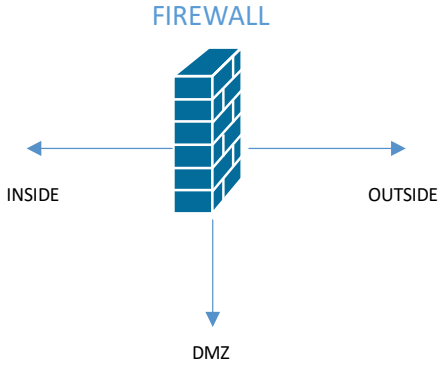

Figura 2-11 *Firewall* de Prototipo.

Tabla 2-59 ACLs para funcionamiento de Cisco *Expressway.*

Interfaz Origen	Interfaz Destino	IP Origen	IP Destino	Puertos TCP/UDP
INSIDE	DMZ	Redes internas	192.168.237.2	TCP/80, TCP/443, TCP/22, UDP/161
DMZ	INSIDE	192.168.237.2	192.168.236.254	UDP/123
DMZ	OUTSIDE	192.168.237.2	5.0.0.10	UDP/53
INSIDE	DMZ	192.168.236.5	6.0.0.3	TCP/7400, TCP/2222, TCP/7001, UDP/36000, UDP/36001, UDP/3478 – 3483
OUTSIDE	DMZ	Cualquier dirección de red (*any)*	6.0.0.3	TCP/5222, TCP/8443, TCP/5061, UDP/36002 – 59999, UDP/3478 – 3483, UDP/24000-29999

El servicio de *Expressway* E será alcanzable desde Internet a través la configuración de NAT estático. *Expressway* C levanta una comunicación hacia el servidor *Expressway* E utilizando como dirección destino la dirección del NAT estático del servidor *Expressway* E; este modo de uso de la configuración NAT se denomina NAT *reflection*. NAT *reflection* debe ser configurado para que funcione solo en la comunicación entre *Expressway* C y *Expressway* E, para no afectar al NAT configurado para la comunicación desde Internet.

j) Configuración de Cisco *Expressway C* y *Expressway E*

A continuación, se presenta un resumen de la configuración requerida los servidores *Expressway* E y *Expressway* C:

- Asegurar que en cada servidor *Expressway* tienen configurado nombre de *host,* nombre de dominio, y la sincronización con el servidor NTP.
- Configurar el modo de Comunicaciones Unificadas a *Mobile and remote Access.*
- Configurar los servidores CUCM y CUCIMP en *Expressway* C.

- Configurar los dominios en *Expressway* C a los cuales se enrutará el servicio hacia el CUCM interno.
- Configurar un *traversal zone* seguro entre *Expressway* E y *Expressway* C.

Para la configuración de *traversal zone* se utiliza la información de la Tabla 2-60.

Tabla 2-60 Parámetros para configuración de túnel entre servidores *Expressway.*

Parámetro	*Expressway C*	*Expressway E*
Nombre	*Traversal zone*	*Traversal zone*
Tipo	*Unified Communications traversal*	*Unified Communications traversal*
Nombre de usuario	Redadmin	Redadmin
Contraseña	Cisco.123	Cisco.123
Puerto	7001	7001
Dirección IP de *peer*	collabe.tesis.com	No aplica
TLS *verify subject name*	No aplica	El valor del parámetro *Subject Alternate Name* o del parámetro *Subject Common Name* del certificado digital del servidor.

La configuración de la Tabla 2-61 debe ser aplicada en el servidor DNS externo para que los dispositivos finales puedan descubrir el servidor de *Expressway* E, para su uso en movilidad y acceso remoto. De igual manera es necesario configurar en el DNS interno el registro SRV que se detalla en la Tabla 2-62 para el uso de Cisco *Jabber* en la LAN.

Tabla 2-61 DNS *record* externo para implementación de *Expressway.*

Dominio	Servicio	Protocolo	Prioridad	Peso	Puerto	Objetivo
tesis.com	*_collab-*	tls	10	10	8443	collabe.tesis.com

Tabla 2-62 DNS *record* interno para el inicio de sesión de Cisco *Jabber*.

Dominio	Servicio	Protocolo	Prioridad	Peso	Puerto	Objetivo
tesis.com	*_cisco_uds*	tcp	10	10	8443	cucm.tesis.com

2.3 Prueba del Prototipo de Comunicaciones Unificadas

2.3.1 Definición de Pruebas de prototipo

Primero se realizarán pruebas de funcionamiento de la solución de Comunicaciones Unificadas, sobre la LAN. Con esto será posible recolectar información para que sirva como base para la comparación de los métodos de acceso.

En la Tabla 2-64 se indican las pruebas que se realizarán sobre la solución de Comunicaciones Unificadas, y se completará con la información de si la prueba pudo ser realizada o no, colocando los valores “Cumple” y “Falló” respectivamente.

Las pruebas descritas en la Tabla 2-64, se ejecutarán sobre las extensiones que se registren con los dos métodos de acceso remoto descritas en el presente proyecto. Para emular el canal de acceso a Internet se implementa un servidor Linux, tal y como se muestra en la Figura 2-8, configurado para que realice reenvío de paquetes a través de sus interfaces y a través del comando “tc” poder colocar retardo en la comunicación de voz y video. La ITU (*International Telecommunication Union*) considera los retardos de la red para aplicaciones voz en la Recomendación G.114, en esta recomendación se definen tres rangos sobre los retardos, como se observa en la Tabla 2-63.

En base a la información de la Tabla 2-63, se pueden definir los escenarios en función del tipo de retardo configurado en el enlace, tal y como se describe en la Tabla 2-65.

Tabla 2-63 Retardos de red sobre comunicación de voz y video. [23]

Rango en milisegundos	Descripción
0-150	Aceptable para la mayoría de las aplicaciones.
150-400	Aceptable con condición de que los administradores están conscientes del tiempo de transmisión y el impacto que tiene sobre la calidad de transmisión de las aplicaciones de usuario.
Mayor a 400	No aceptable para propósitos generales en la planificación de la red.

Tabla 2-64 Pruebas de funcionamiento del prototipo

Prueba	Cumple	Falló
Inicio de sesión con Cisco *Jabber.*		
Videollamada entre extensiones internas con Cisco *Jabber*.		
Llamada entre extensiones internas, dejando correo de voz.		
Acceso al correo de voz.		
Mensajería instantánea entre usuarios de Cisco *Jabber.*		
Transferencia de archivos desde chat con Cisco *Jabber.*		
Compartir pantalla durante video llamada en Cisco *Jabber.*		
Durante una llamada entre dos extensiones con Cisco *Jabber*, revisar el estado de presencia desde una tercera extensión.		
Comentario sobre calidad de la llamada en pruebas.		

Tabla 2-65 Valores de emulación de problemas de canal de comunicación para escenarios de prueba.

Escenarios	Valores
1	400 ms ± 10 ms de retardo
2	450 ms ± 10 ms de retardo
3	500 ms ± 10 ms de retardo

Los valores de retardo pueden ser configurados en el servidor Linux utilizando el comando: *tc qdisc add dev eth0 root netem delay 100ms,* que aumenta 100 milisegundos al retardo actual de la comunicación que pasa por la interfaz *eth0.* El retardo generado por el comando indicado es constante, para obtener retardos variados que se aproximen al comportamiento de un enlace real, se utilizan parámetros adicionales para variar de manera aleatoria el retardo y que la variación no sea uniforme, que varíe en base a una curva de distribución normal. Estos cambios se realizan aumentando tres parámetros al comando; el primero indica el tamaño de la variación aleatoria, el segundo es un porcentaje con el cual cambia la

variación basándose en el último valor aplicado, y el tercero es la sentencia *distribution normal* con el cual la variación no será uniforme. Un ejemplo del comando sería el siguiente*: tc qdisc change dev eth0 root netem delay 100ms 20ms distribution normal.* [24]

El objetivo de aplicar los cambios en el emulador del canal es poner a prueba cada método de acceso remoto a la solución de Comunicaciones Unificadas, con esto se puede validar qué método es más tolerante a la calidad del canal de datos.

2.3.2 Pruebas de funcionamiento

Para iniciar las pruebas del prototipo, se realiza el registro de tres dispositivos Cisco *Jabber,* dos serán de *smartphones* y el tercero desde una portátil con sistema operativo Windows 10, tal y como se muestra en la Figura 2-12.

Las pruebas definidas en el capítulo anterior se realizarán inicialmente en la LAN, para poder tomar datos iniciales con los cuales poder comparar, principalmente la calidad de los servicios de voz y video.

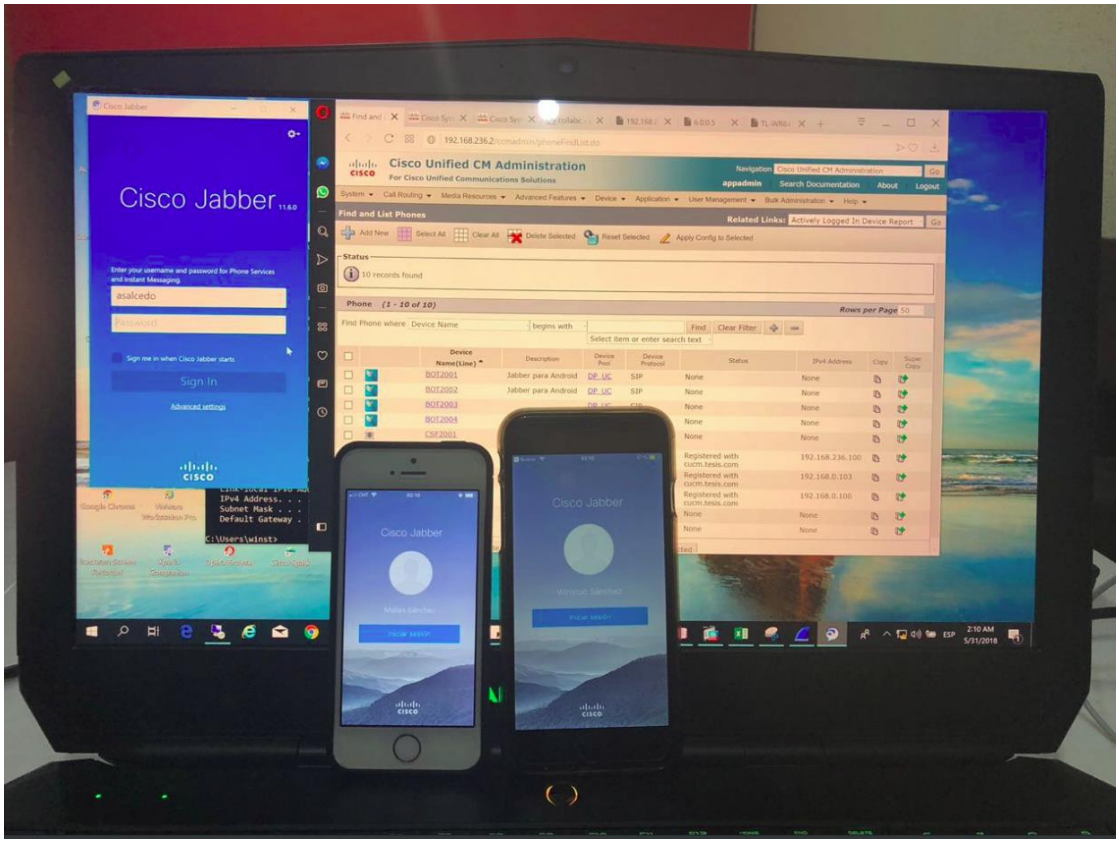

Figura 2-12 Dispositivos con Cisco *Jabber* para pruebas del prototipo.

2.3.3 Escenario de prueba 1: Comunicación dentro de la LAN

Inicio de sesión con *Cisco Jabber*

En la aplicación Cisco *Jabber* ingreso el nombre de usuario y contraseña, la aplicación encuentra el servicio a través de los registros SRV configurados en el DNS.

En la Figura 2-13 se muestran los dispositivos *IPhone* registrados a los servicios de Mensajería Instantánea, CUCM y CUC.

Videollamada entre extensiones internas con *Cisco Jabber*

En la Figura 2-14 se puede apreciar una videollamada entre las extensiones Cisco *Jabber* configuradas en IPhone. No existieron problemas en la calidad de voz y video.

Llamada entre extensiones internas, dejando correo de voz

Se realiza una llamada desde la extensión 2001 (*IPhone*) a la extensión 2003 (*Windows*), y se rechaza la llamada desde la extensión 2003 para que pueda ser transferida al sistema de Correo de Voz. Una vez finalizado el mensaje queda guardado en el buzón de voz, y por el registro desde Cisco *Jabber,* el mensaje se descarga en la aplicación tal y como se muestra en la Figura 2-15

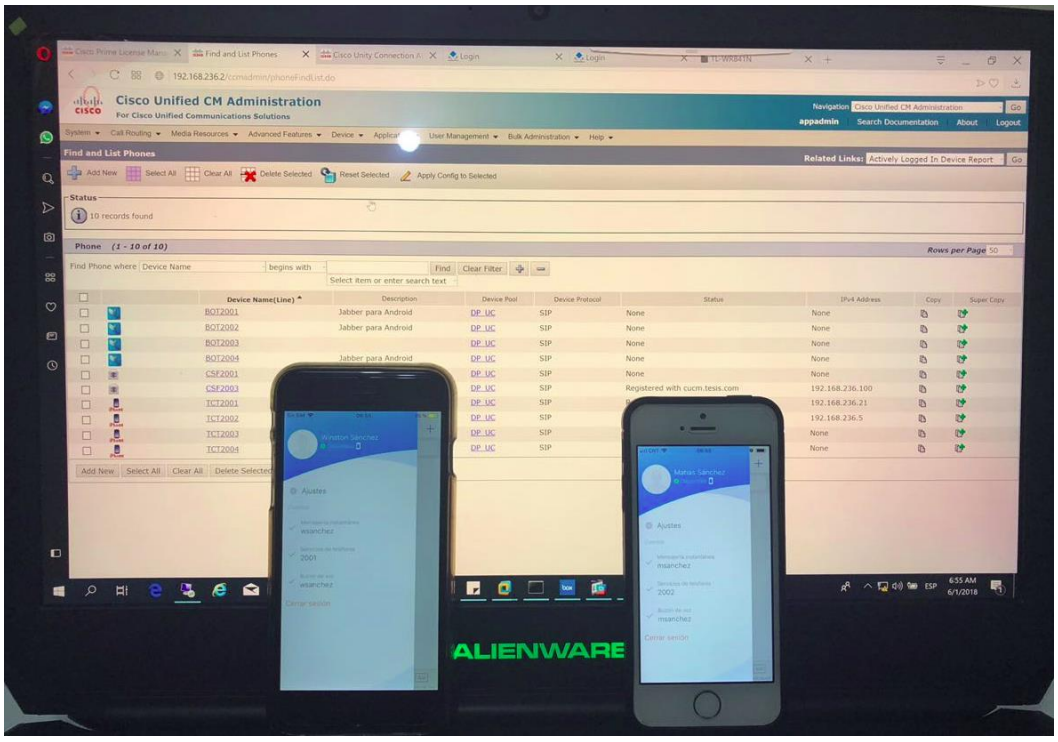

Figura 2-13 Inicio sesión con Cisco *Jabber.*

Acceso al correo de voz

La notificación de un nuevo mensaje de voz aparece en la aplicación Cisco *Jabber,* como muestra la Figura 2-15. Al ingresar en la opción *Voice Messages* se observa el nuevo mensaje de voz, el mismo que puede ser reproducido desde Cisco *Jabber* sin tener que llamar al sistema de Correo de Voz.

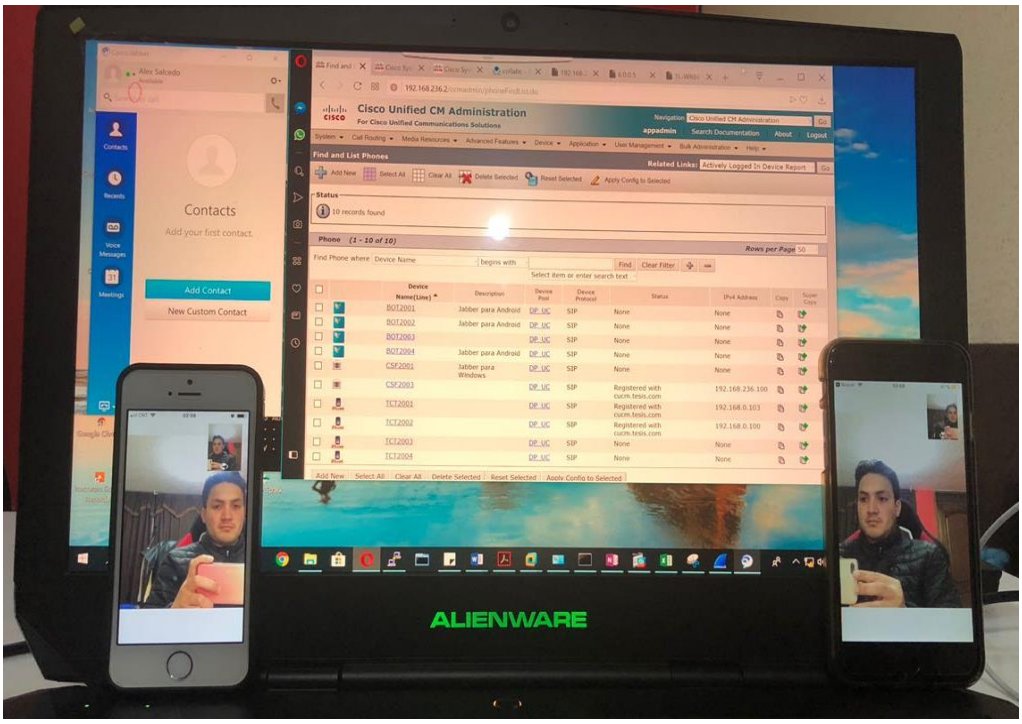

Figura 2-14 Video Llamada entre extensiones internas.

Figura 2-15 Correo de voz en Cisco *Jabber.*

Figura 2-16 Acceso a Correo de Voz desde Cisco *Jabber*.

Mensajería instantánea entre usuarios de *Cisco Jabber*

La prueba de esta función se realiza con el fin de validar si se mantiene luego de usar los métodos de acceso desde Internet.

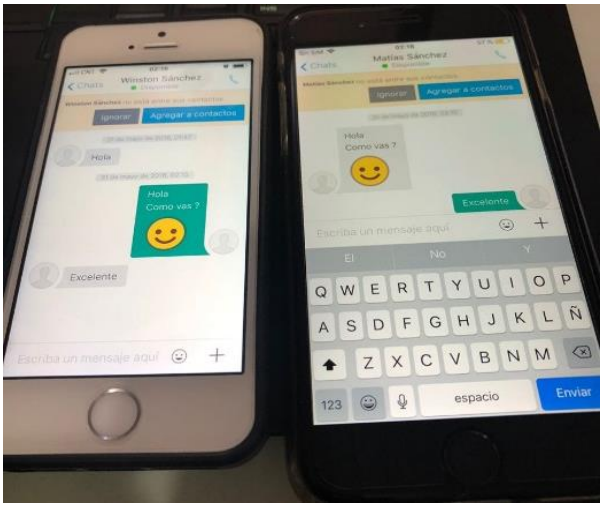

Figura 2-17 Mensajería Instantánea entre dispositivos con Cisco *Jabber*.

Transferencia de archivos desde *chat* con *Cisco Jabber*

Al igual que en la característica de mensajería instantánea, la finalidad de esta prueba es validar su funcionamiento en los escenarios de prueba. La transferencia de archivos entre extensiones Cisco *Jabber* es una comunicación *peer to peer* a través del protocolo XMPP. En la Figura 2-18 se muestra un ejemplo del envío de archivos entre dos dispositivos con Cisco *Jabber*.

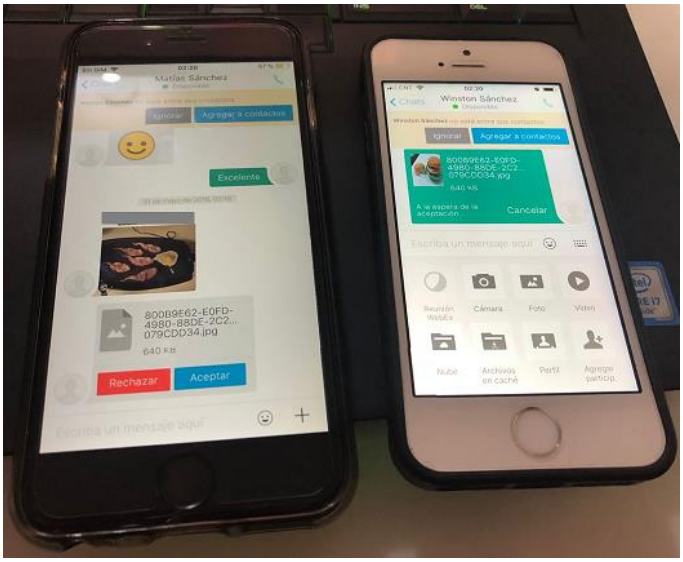

Figura 2-18 transferencia de archivos entre dispositivos con Cisco *Jabber.*

Compartir pantalla durante video llamada en *Cisco Jabber*

La función para compartir la pantalla es una opción que está disponible cuando dos dispositivos con Cisco *Jabber* están en una videollamada y es una característica sensible al retardo. La Figura 2-19 muestra la prueba de compartir la pantalla durante una videollamada sobre LAN.

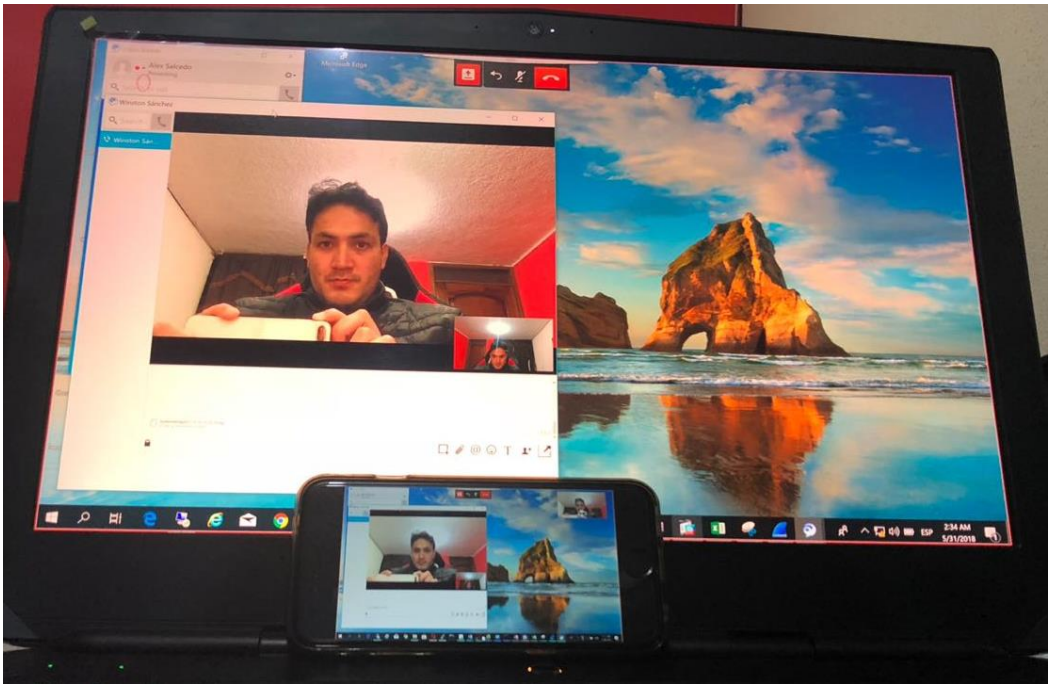

Figura 2-19 Cisco *Jabber Share Screen*.

Estado de presencia desde una tercera extensión

Los estados de presencia de extensión se envían desde el CUCM, a través de una troncal SIP con el servidor CUCMIMP. Se probará si la opción se mantiene desde las opciones de acceso remoto a la solución de Comunicaciones Unificadas. En la Figura 2-20 se puede apreciar que en la ventana de chat de la portátil *Windows* se muestra el estado *"On a call"* para la extensión del usuario wsanchez que mantiene una llamada con la extensión del usuario msanchez.

Comentario sobre calidad de la llamada en Escenario 1

La comunicación dentro de la LAN fue nítida y sin errores. La videollamada y la función de pantalla compartida no presentaron problemas de calidad de imagen y fue posible realizar transferencia de archivos entre dispositivos con Cisco *Jabber*. Las pruebas en el Escenario 1 sirve de base para el resto de Los escenarios de Prueba.

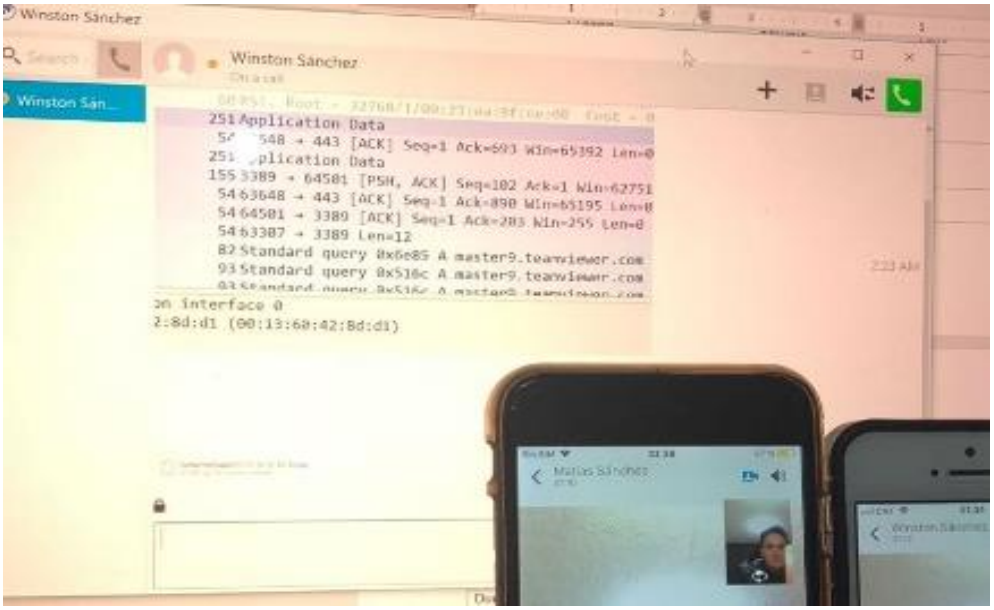

Figura 2-20 Estado de presencia.

2.3.4 Escenario de prueba 2: Comunicación con extensión remoto utilizando *Cisco Expressway*

Inicio de sesión con *Cisco Jabber*

En el escenario de Cisco *Expressway,* la aplicación busca los registros SRV externos luego de perder comunicación con los servicios internos. En la Figura 2-21 se observa la dirección IP del registro del dispositivo Cisco *Jabber,* y una de las

extensiones está registrada dese la IP 192.168.236.5 que es la dirección IP de Cisco *Expressway* C.

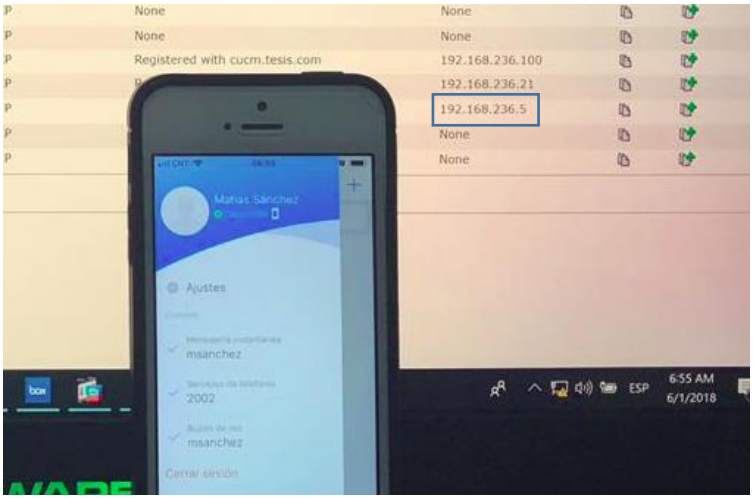

Figura 2-21 Inicio sesión con Cisco *Jabber.*

Videollamada entre extensiones internas con *Cisco Jabber*

En el escenario del acceso a través de Cisco *Expressway,* se realiza la prueba de llamada utilizando la configuración del emulador de retardos descrita en la Tabla 2-65, todas las configuraciones de retardo tienen variación de 10 ms, y se obtienen los siguientes resultados:

a) Prueba de videollamada con retardo de 400 milisegundos

En esta prueba la comunicación de voz no presentó errores. Tal y como se muestra en la Figura 2-22, la comunicación de video presenta fallas en la imagen, esto fue visible cuando se generaban movimientos en el video que se estaba transmitiendo.

Figura 2-22 Videollamada entre extensiones internas con retardo de 400 ± 10 ms.

b) Prueba de videollamada con retardo de 450 milisegundos

Existen pequeños errores en la comunicación de voz, y la calidad de la imagen disminuye tal y como se muestra en la Figura 2-23.

c) Prueba de videollamada con retardo de 500 milisegundos

Los errores de la comunicación de voz son más notorios, y mayor degradación de imagen en cuando existe movimiento en la videollamada. En la Figura 2-24 se muestra el resultado de la prueba a 500 ms.

Figura 2-23 Videollamada con retardo de 450 ± 10 ms.

Figura 2-24 Videollamada con retardo de 500 ± 10 ms.

Llamada entre extensiones internas, dejando correo de voz

La notificación del nuevo correo de voz llega sin problemas a la extensión remota, y el archivo de audio se descarga sin problema, como se aprecia en Figura 2-25.

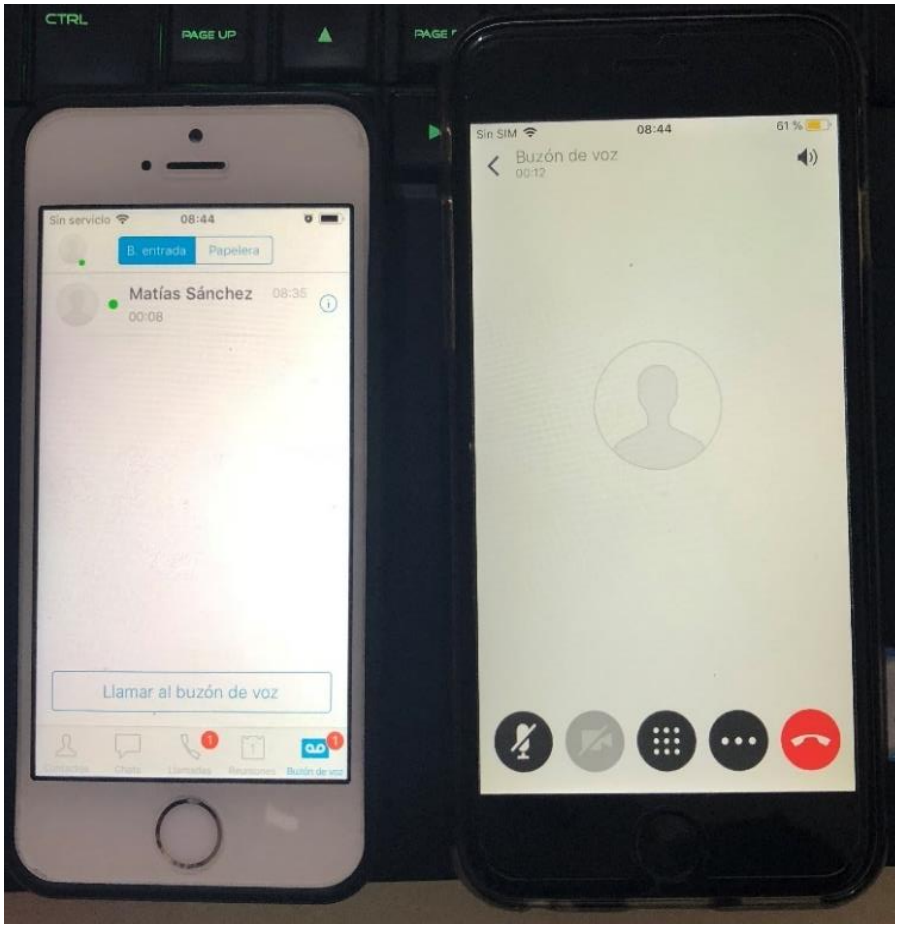

Figura 2-25 Correo de voz en Cisco *Jabber.*

Acceso al correo de voz

Los mensajes de voz están disponibles para poder reproducirlos sin necesidad de llamar al sistema de Correo de Voz. La Figura 2-26 muestra los mensajes de voz que recibe la extensión remota.

Mensajería instantánea entre usuarios de *Cisco Jabber*

La función de mensajería instantánea funciona correctamente con la opción de acceso remoto Cisco *Expressway,* tal y como se aprecia en Figura 2-27.

Transferencia de archivos desde *chat* con *Cisco Jabber*

La opción de transferencia de archivos se desactiva cuando se inicia sesión a través de Cisco *Expressway.* En la Figura 2-27 se puede observar que en ambos

dispositivos están desactivadas las opciones relacionadas con transferencias de archivos.

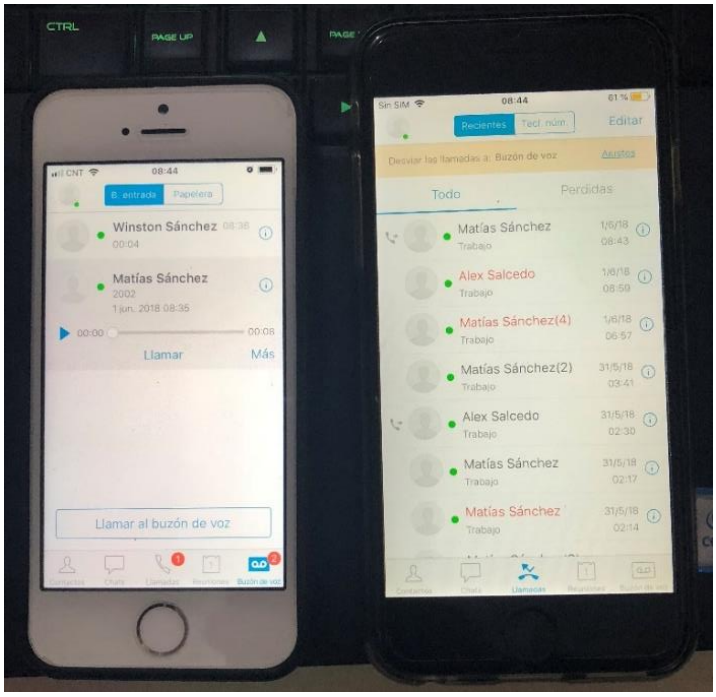

Figura 2-26 Acceso al contenido del buzón de voz con *Cisco Jabber.*

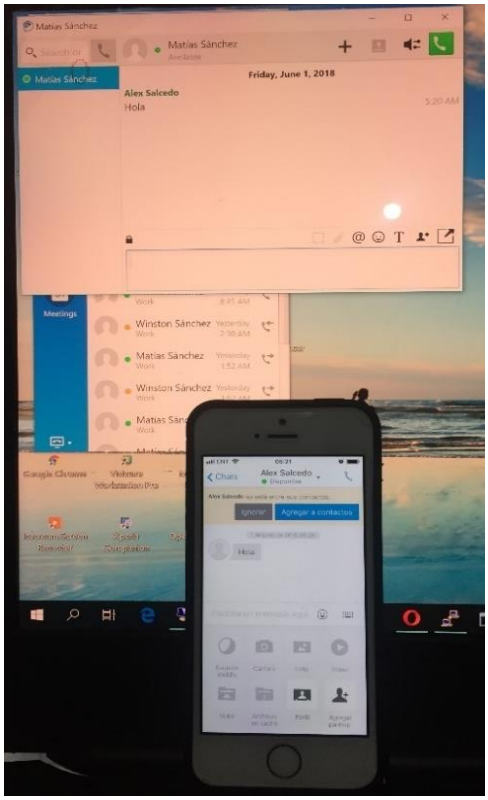

Figura 2-27 Mensajería Instantánea entre dispositivos con *Cisco Jabber.*

Estado de presencia

En la Figura 2-28 se muestra el estado de presencia del usuario Winston Sánchez, el estado es *On a call.*

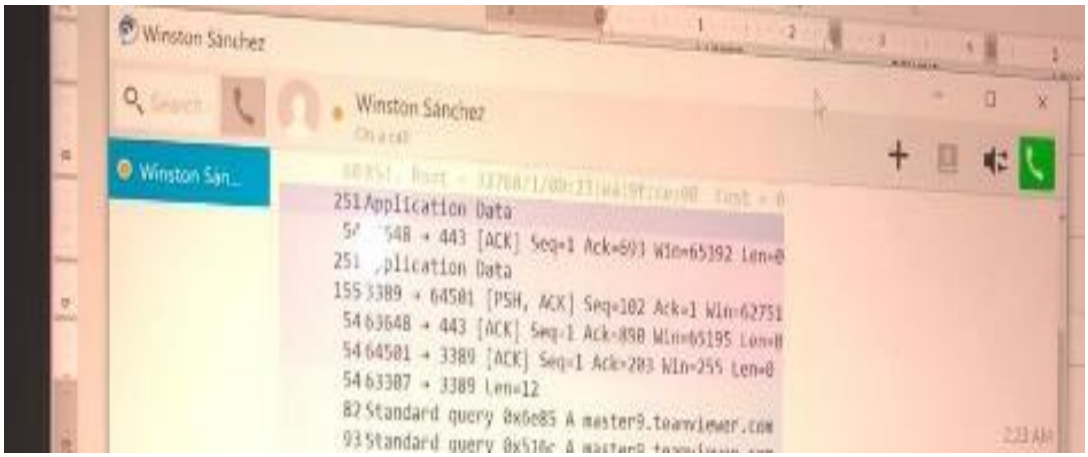

Figura 2-28 Estado de presencia en cliente *Jabber* de Windows.

Comentario sobre calidad de la llamada en Escenario 2

En las pruebas, la calidad de la voz fue cambiando a medida que se aumentaba el retardo en las conexiones remotas. Se pudo apreciar en la videollamada la imagen se congelaba o se distorsionaba, estos errores se notan fácilmente en la video llamada. Los errores de audio eran de tipo distorsión de la voz y ausencia de voz.

2.3.5 Escenario de prueba 3: Comunicación con extensión remota utilizando VPN de acceso remoto

Inicio de sesión con *Cisco Jabber*

Con el uso de una VPN de acceso remoto, la aplicación busca los registros SRV internos para alcanzar los servicios de Comunicaciones Unificadas. En la Figura 2-29 se observa la dirección IP del registro del dispositivo Cisco *Jabber,* una de las extensiones está registrada dese la IP 192.168.238.100 que es parte del rango configurado para la VPN de acceso remoto.

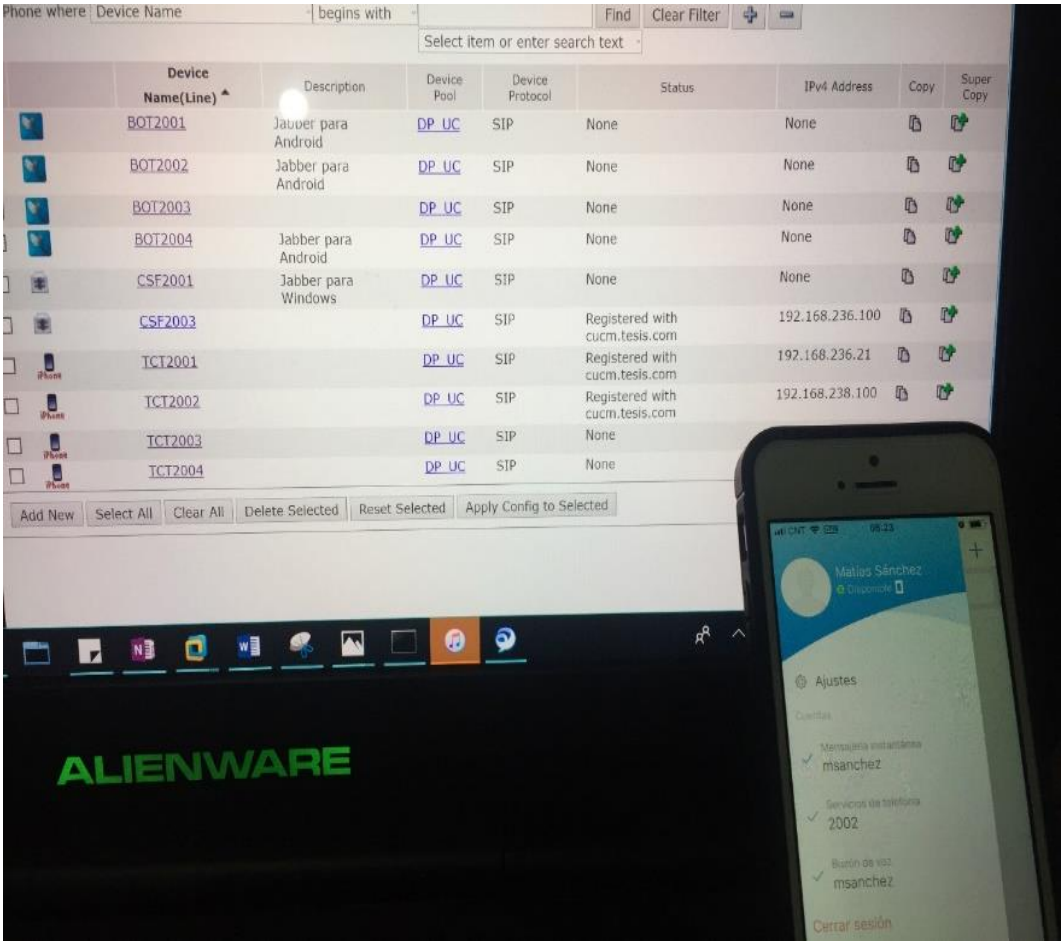

Figura 2-29 Inicio sesión con *Cisco Jabber* desde VPN de acceso remoto.

Videollamada entre extensiones internas con *Cisco Jabber*

En el escenario del acceso a través de VPN de acceso remoto, se realizó la prueba de llamada utilizando la configuración del emulador de retardos descrita en la Tabla 3-38, todas las configuraciones de retardo tienen variación de 10 ms, y se obtuvieron los siguientes resultados:

a) Prueba de videollamada con retardo de 400 milisegundos

En esta prueba no se mostraron errores en la comunicación de voz. En la Figura 2-30, la comunicación de video no presenta fallas graves en la imagen, con los movimientos del video la imagen perdió un poco de resolución.

b) Prueba de videollamada con retardo de 450 milisegundos

La comunicación de voz aún es entendible, aunque se presentan pequeños errores. La resolución del video se mantiene a la capturada en la prueba anterior, a pesar del movimiento en la transmisión (ver Figura 4-20).

Figura 2-30 Videollamada entre extensiones internas a través de VPN con retardo de 400 ± 10 ms.

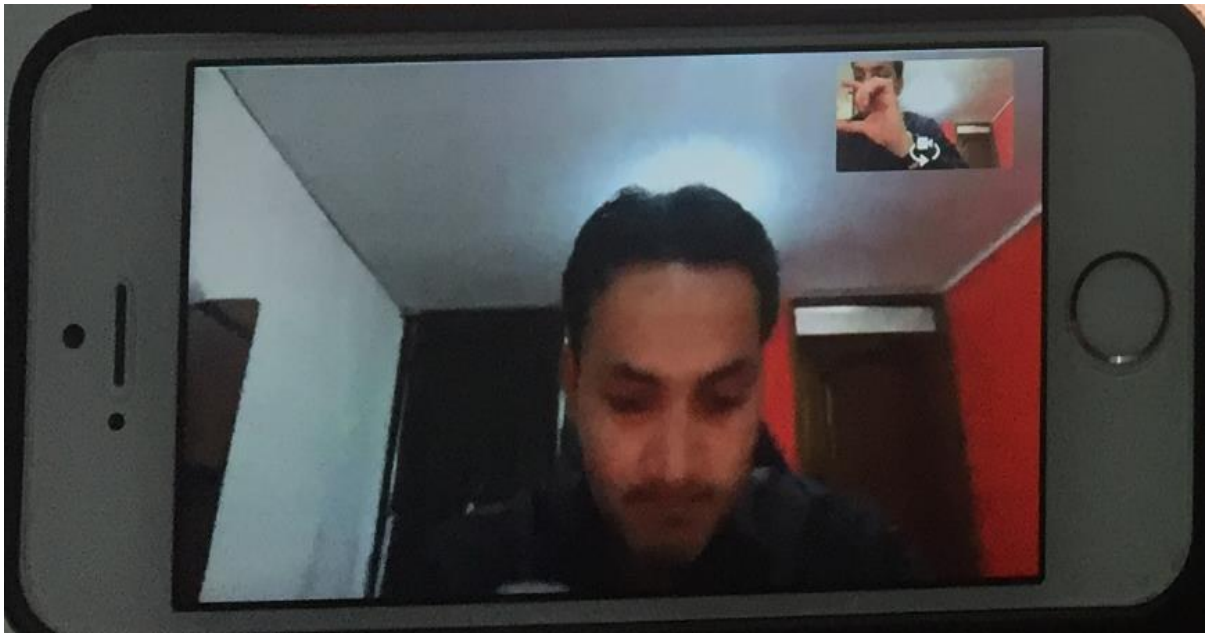

Figura 2-31 Videollamada a través de VPN con retardo de 450 ± 10 ms.

c) Prueba de videollamada con retardo de 500 milisegundos

Se presenta una comunicación de voz con mayor frecuencia de errores. El video se degrada tal y como se muestra en la Figura 2-32.

Figura 2-32 Videollamada a través de VPN con retardo de 500 ± 10 ms.

Llamada entre extensiones internas, dejando correo de voz

La notificación del nuevo correo de voz llega sin problemas a la extensión remota (ver Figura 2-33).

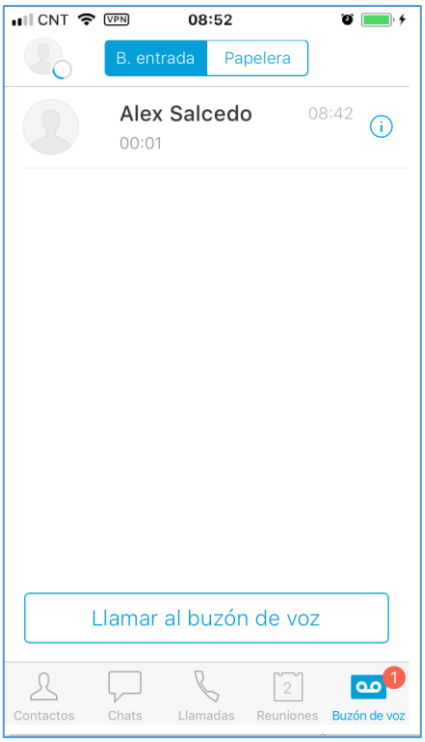

Figura 2-33 Correo de voz en *Cisco Jabber* desde VPN de acceso remoto.

Acceso al correo de voz

El mensaje de voz se descarga correctamente en el dispositivo remoto con Cisco *Jabber* (ver Figura 2-34).

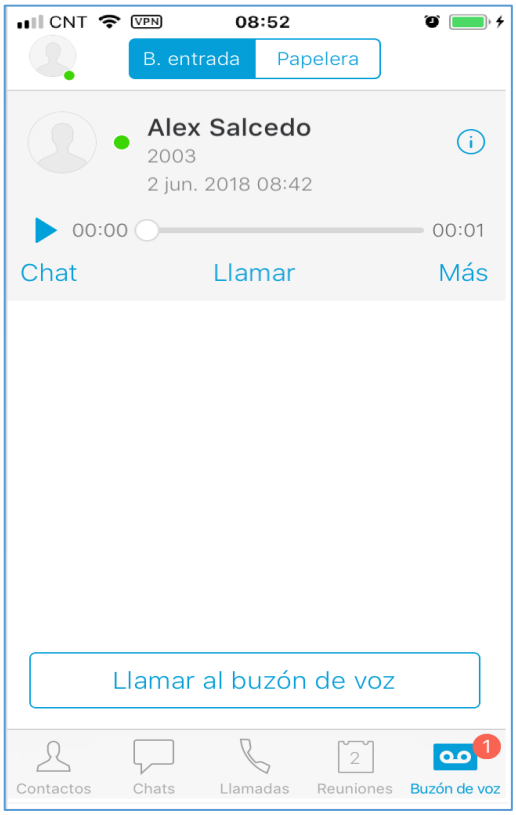

Figura 2-34 Acceso al contenido del buzón de voz con *Cisco Jabber*.

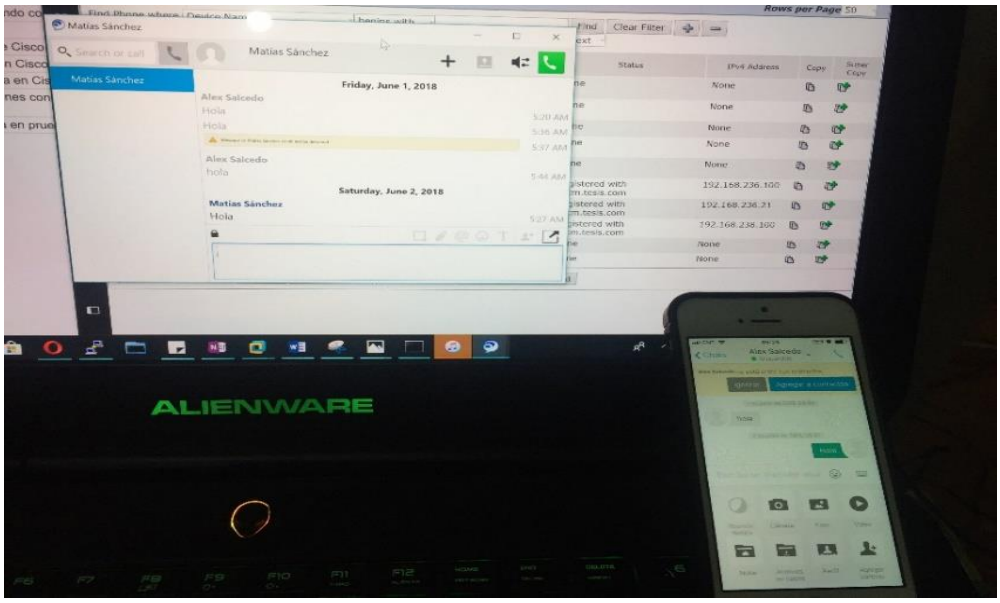

Figura 2-35 Mensajería Instantánea entre dispositivos con Cisco *Jabber* a través de VPN.

Mensajería instantánea entre usuarios de *Cisco Jabber*

La función de mensajería instantánea funciona correctamente con la opción de acceso remoto con VPN, los mensajes se entregan sin problemas al destinatario (ver Figura 2-35).

Transferencia de archivos desde *chat* con *Cisco Jabber*

De acuerdo con la prueba, es posible transferir archivos entre dispositivos con Cisco *Jabber,* en la Figura 2-35 se observa que las opciones de envío de archivos y capturas de pantalla están habilitadas en la ventana de *chat.*

Compartir pantalla durante video llamada en *Cisco Jabber*

Es posible compartir la pantalla en una videollamada, Figura 2-36 ,entre dispositivos Cisco *Jabber,* a través de la VPN. Esta función, al igual que la de transferencia de archivos, la cual es *peer to peer.*

Figura 2-36 Cisco *Jabber Share Screen* a través de VPN.

Estado de presencia desde una tercera extensión

Se observa en Figura 2-37 que la función de presencia se mantiene en la conexión a través de la VPN.

Figura 2-37 Presencia a través de VPN.

Comentario sobre calidad de la llamada en pruebas

La calidad de llamadas se mantuvo con pocos errores, entrecortes de voz, hasta los 450 ms. Al configurar el retardo en 500 ms, la calidad de voz y video se vio afectada; los entrecortes de audio fueron más frecuentes y el video se distorcionó más con el movimiento en la imagen.

3. RESULTADOS Y DISCUSIÓN

En las tablas 3-1, 3-2 y 3-3 se resumen los resultados de cada escenario de pruebas.

Tabla 3-1 Resultado de pruebas en Escenario 1.

Prueba	Cumple	Falló
Inicio de sesión con Cisco *Jabber.*	X	
Videollamada entre extensiones internas con Cisco *Jabber*.	X	
Llamada entre extensiones internas, dejando correo de voz.	X	
Acceso al correo de voz.	X	
Mensajería instantánea entre usuarios de Cisco *Jabber.*	X	
Transferencia de archivos desde chat con Cisco *Jabber.*	X	
Compartir pantalla durante video llamada en Cisco *Jabber.*	X	
Durante una llamada entre dos extensiones con Cisco Jabber, revisar el estado de presencia desde una tercera extensión.	X	
Comentario sobre calidad de la llamada en pruebas.	Excelente calidad de videollamadas	

Tabla 3-2 Resultado de pruebas en Escenario 2.

Prueba	Cumple	Falló
Inicio de sesión con Cisco *Jabber.*	X	
Videollamada entre extensiones internas con Cisco *Jabber*.	X	
Llamada entre extensiones internas, dejando correo de voz.	X	
Acceso al correo de voz.	X	
Mensajería instantánea entre usuarios de Cisco *Jabber.*	X	
Transferencia de archivos desde chat con Cisco *Jabber.*		X
Compartir pantalla durante video llamada en Cisco *Jabber.*		X
Durante una llamada entre dos extensiones con Cisco Jabber, revisar el estado de presencia desde una tercera extensión.	X	
Comentario sobre calidad de la llamada en pruebas.	En las video llamadas, la voz fue afectada en menor grado. Se notaron fallas grandes en la parte de video.	

Tabla 3-3 Resultado de pruebas en Escenario 3.

Prueba	Cumple	Falló
Inicio de sesión con Cisco *Jabber.*	X	
Videollamada entre extensiones internas con Cisco *Jabber*.	X	
Llamada entre extensiones internas, dejando correo de voz.	X	
Acceso al correo de voz.	X	
Mensajería instantánea entre usuarios de Cisco *Jabber.*	X	
Transferencia de archivos desde chat con Cisco *Jabber.*	X	
Compartir pantalla durante video llamada en Cisco *Jabber.*	X	
Durante una llamada entre dos extensiones con Cisco Jabber, revisar el estado de presencia desde una tercera extensión.	X	
Comentario sobre calidad de la llamada en pruebas.	En comparación al escenario de pruebas 2, la calidad de la videollamada fue mejor.	

3.1 Encuestas a usuarios

La presente encuesta está dirigida a personal técnico y no técnico de empresas en las que se conoce tienen implementada una solución de Comunicaciones Unificadas, y cuentan con al menos una de las dos opciones de acceso remoto.

3.1.1 Contenido de la Encuesta

Se incluyen íconos en la encuesta, por facilidad del usuario para que pueda entender los servicios que dispone. Las preguntas que forman parte de la encuesta se detallan a continuación:

1. ¿Tiene instalado en su *smartphone* Cisco Jabber  para uso corporativo? Responda Si o No.
2. ¿Utiliza su cliente de Comunicaciones Unificadas desde fuera de la oficina? Responda Si o No.
3. En caso de responder Si en la pregunta 2: Para iniciar sesión en su cliente de Comunicaciones Unificadas, ¿Utiliza dos aplicaciones; Cisco *Anyconnect*  y Cisco *Jabber*  , o solo una aplicación  ?

4. En caso de utilizar dos aplicaciones;  y  , califique su experiencia en base a las siguientes opciones:
    a. Mala
    b. Buena
    c. Muy Buena

5. En caso de utilizar solo una aplicación,  , califique su experiencia en base a las siguientes opciones:
    a. Mala
    b. Buena
    c. Muy Buena

6. Cuando inicia sesión al sistema de Comunicaciones Unificadas desde fuera de la oficina, ¿cuál de los siguientes métodos utiliza más a menudo?
    a. Red del hogar.
    b. Red de datos celular (Ej.: 4G, LTE, 3G, etc.).
    c. Redes gratuitas en sitios públicos (Ej. Restaurant, parques, etc.).

7. Para los usuarios que utilizan dos aplicaciones. En base a su experiencia, ¿Cuál de las siguientes opciones describe mejor su interés en cambiar a una sola aplicación para el acceso remoto de Comunicaciones Unificadas?
    a. No estoy interesado.
    b. Medianamente interesado.
    c. Muy interesado.

3.1.2 Resultados de las encuestas

La encuesta fue aplicada a una muestra de treinta y tres personas, y los resultados se detallan en la Tabla 3-4.

En las figuras 3-1, 3-2, 3-3, 3-4, 3-5, 3-6, y 3-7 se muestran los porcentajes para cada respuesta. Los porcentajes son calculados en base a número de personas que responde cada pregunta.

Tabla 3-4 Resultados de la encuesta.

Pregunta	Opciones de respuesta	Número de respuestas
1	Si.	25
	No.	8
2	Si.	13
	No.	12
3	Dos aplicaciones.	5
	Una aplicación.	8
4	Mala.	0
	Buena.	4
	Muy Buena.	1
5	Mala.	0
	Buena.	3
	Muy Buena.	5
6	Red del hogar.	3
	Red de datos celular	6
	Redes gratuitas en sitios públicos.	4
7	No estoy interesado.	0
	Medianamente interesado.	1
	Muy interesado.	4

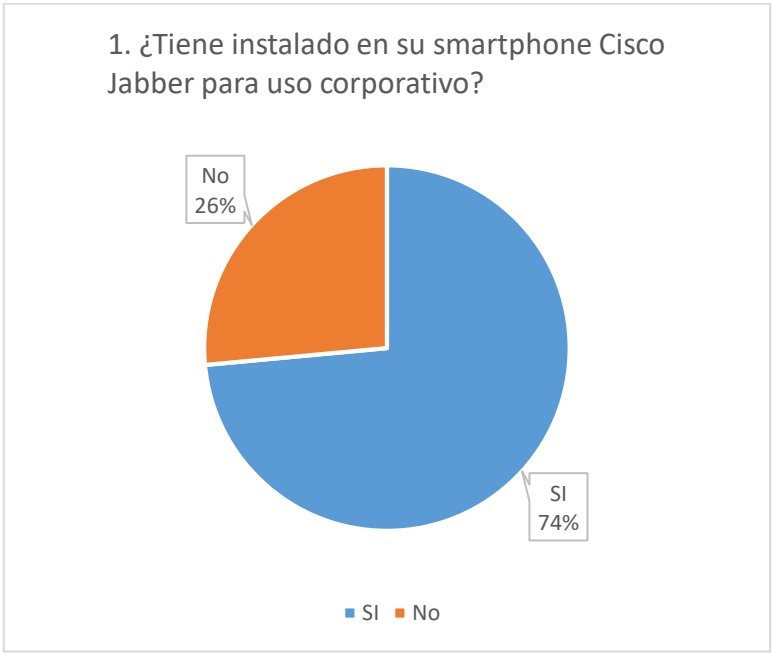

Figura 3-1 Resultados de la pregunta 1.

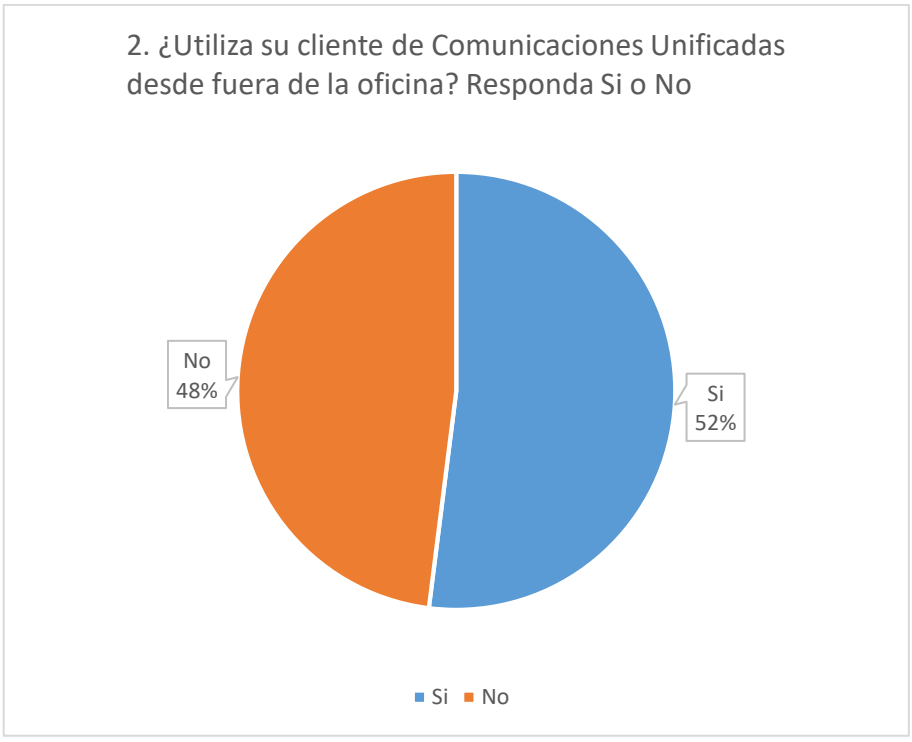

Figura 3-2 Resultados de la pregunta 2.

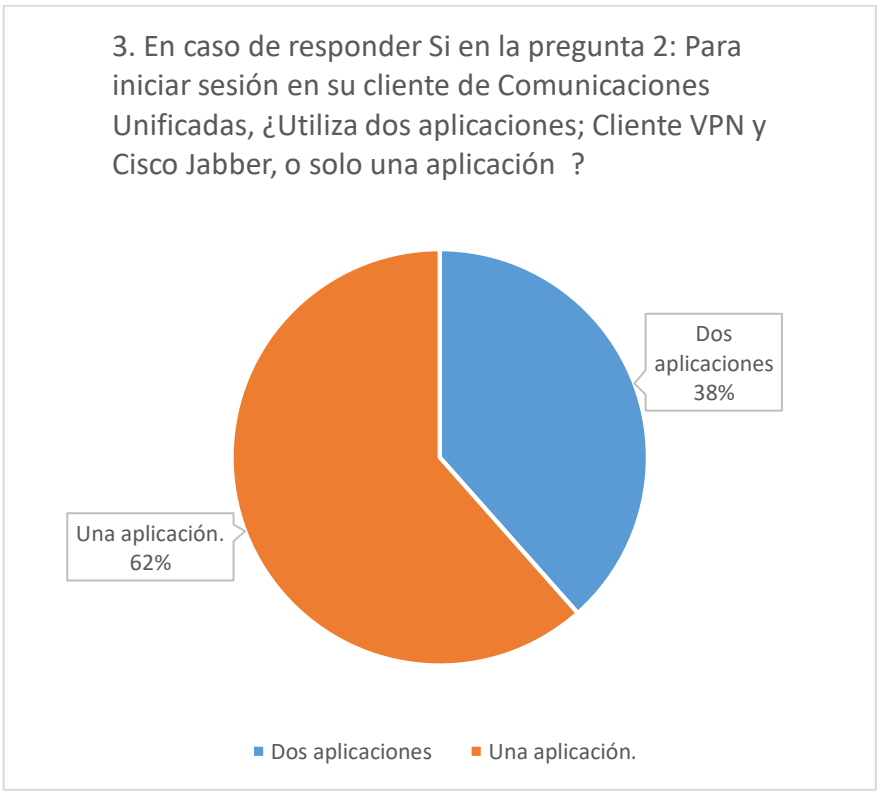

Figura 3-3 Resultados de la pregunta 3.

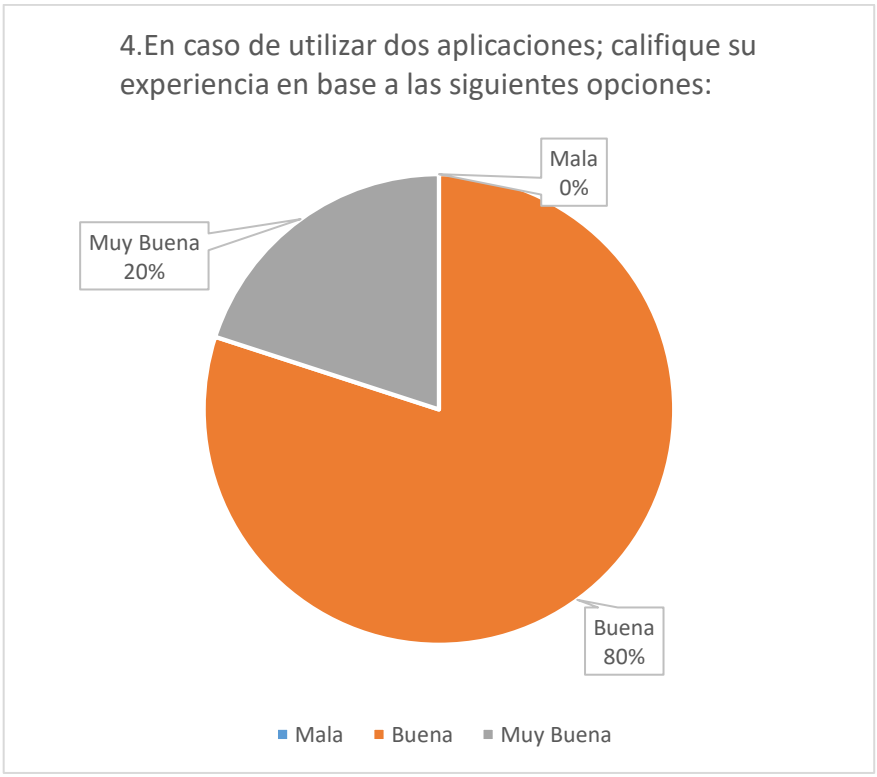

Figura 3-4 Resultados de la pregunta 4.

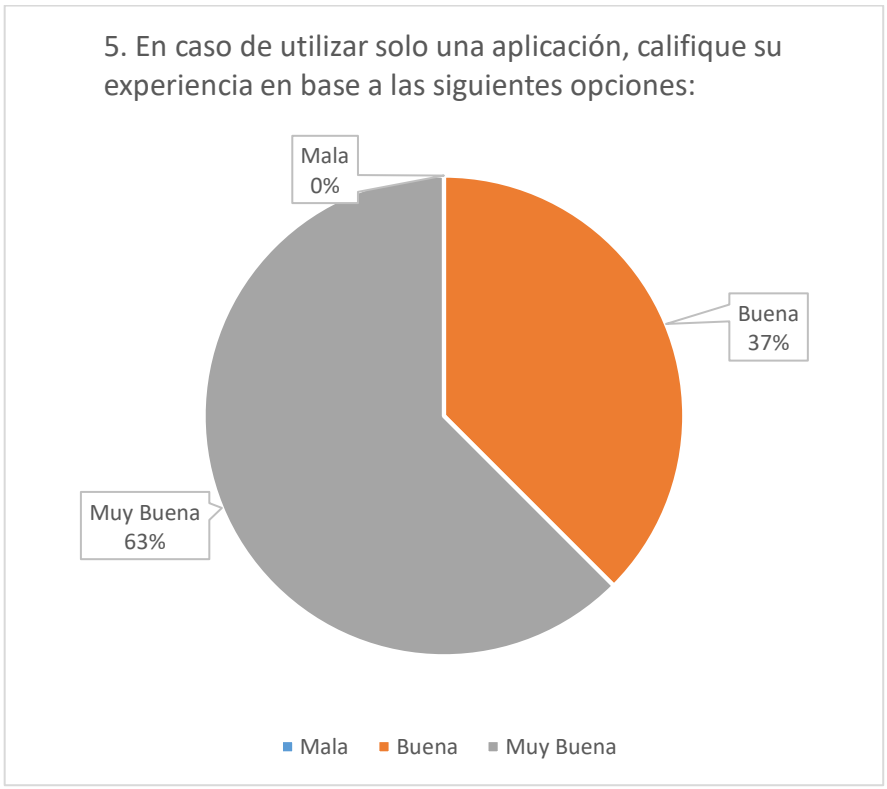

Figura 3-5 Resultados de la pregunta 5.

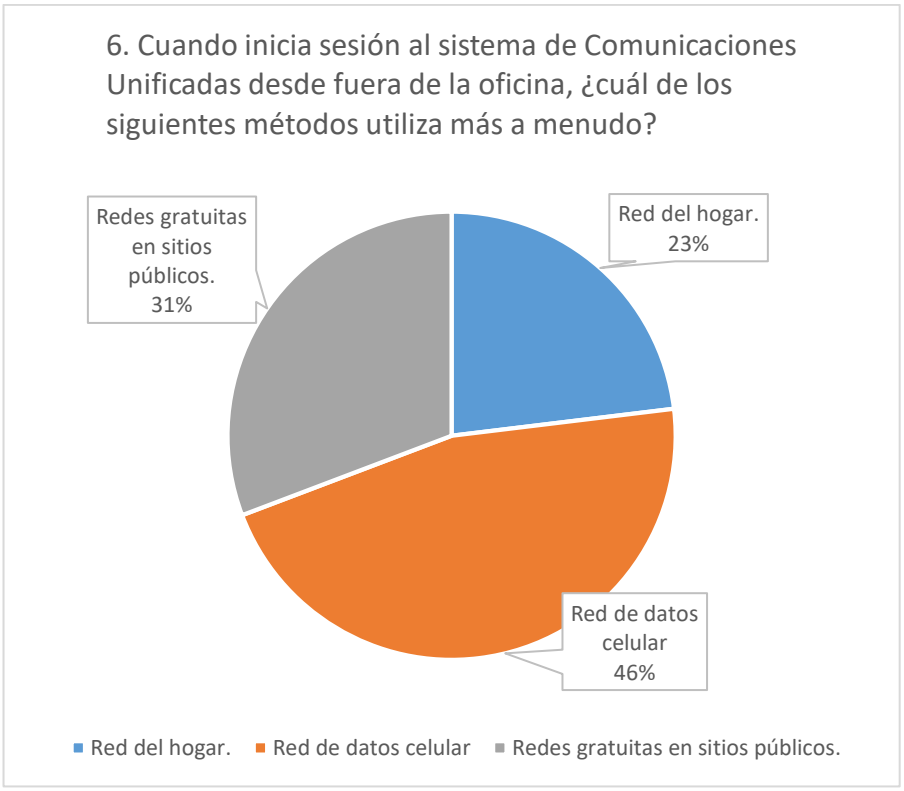

Figura 3-6 Resultados de la pregunta 6.

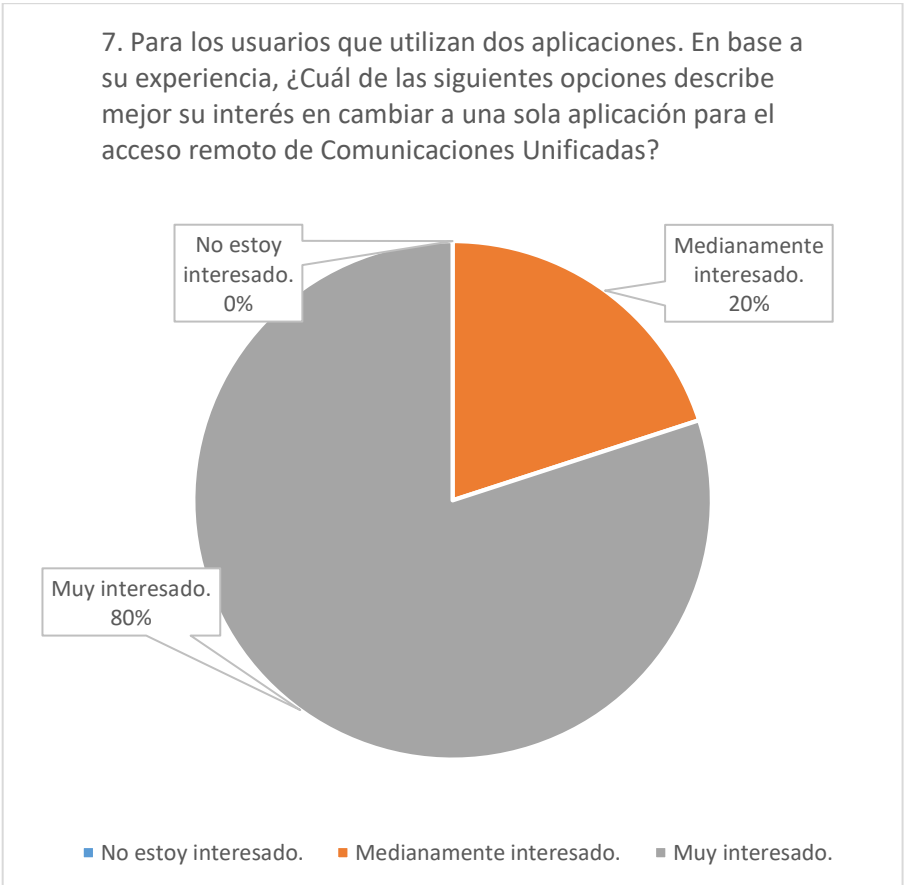

Figura 3-7 Resultados de la pregunta 7.

De acuerdo con los resultados de la encuesta, se observa que existe una tendencia al uso de una sola aplicación para el acceso desde Internet a la solución de Comunicaciones Unificadas, esto se puede apreciar en la representación gráfica de cada pregunta de la encuesta, la mayoría vota por el uso de solo una aplicación, lo que implica el uso de Cisco *Expressway*. De acuerdo con los encuestados no técnicos, utilizar solo Cisco *Jabber* es mejor que encender y autenticarse en una aplicación adicional (vpn *client*) y luego en Cisco *Jabber.*

Las personas que respondieron a la pregunta 4, el 80% está conforme con la solución de acceso mediante VPN de acceso remoto. Existe el 20% califica la solución con VPN como “Muy Buena”, este porcentaje no tiene problemas con la doble autenticación para acceder al servicio. El manejo de la VPN da una sensación de seguridad al usuario, y mediante la sesión segura puede ingresar a servicios internos adicionales.

4. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Para los usuarios finales, el uso de VPNs de acceso remoto del tipo SSL presenta mayor facilidad de acceso que el uso de VPN de acceso remoto IPSec, debido a que el cliente de VPN SSL se conecta con el *Firewall* o concentrador de VPNs, a través del puerto TCP 443, y es un puerto que normalmente está abierto para navegación a Internet. Esto es una ventaja cuando la conexión se la realiza desde un hotel o desde alguna red pública con protección; con IPSec es necesario solicitar que permitan el tráfico saliente hacia el puerto UDP 500.

- La solución de Comunicaciones Unificadas diseñada para la empresa ficticia, cuenta con los productos base para poder escalar a servicios de Videoconferencia y Colaboración *Web*. También es posible instalar una solución de *Contact Center*, la cual se integra con el servicio CUCM y ofrece características de manejo de Colas de Servicio, aplicaciones para agentes y supervisores, Servicio de Campañas, IVR (*Interactive Voice Response*), etc.

- El manejo de licencias en la solución de Comunicaciones Unificadas se dimensiona por tipo de usuarios, es decir un usuario que necesita llevar su extensión en varios dispositivos consume una sola licencia de tipo CUWL.

- El CUCM de Quito es el nodo Publisher, si este nodo falla o se pierde conexión, no es posible realizar cambios de configuración desde el CUCM de Guayaquil, debido a que las bases de datos del nodo *subscriber* pasan a modo *read-only*.

- Publicar una solución de Comunicaciones Unificadas, sin el uso de uno de los métodos de acceso revisados en el presente proyecto, implica exponer la seguridad. Los servicios quedarían expuestos a diversos tipos de ataques como, por ejemplo; ataques de denegación de servicio (DOS).

- La solución de Comunicaciones Unificadas con Cisco soporta integración con servicios y dispositivos finales de otras marcas, siempre y cuando la integración se maneje a través de protocolos estándar, por ejemplo, SIP, H.323, XMPP, etc. Este soporte es solo para funciones básicas de Telefonía IP y Mensajería Instantánea. Cisco trabaja con productos de otros fabricantes que son parte de Cisco *Developer Network* y que desarrollan soluciones que aprovechan las capacidades del CUCM.

- Cuando una de las sucursales pasa a modo SRST debido a falla en el enlace de datos, la sucursal cuenta en ese momento con funciones básicas de Telefonía IP. Un usuario puede seguir conectado a los servicios de Comunicaciones Unificadas a través de cualquiera de los dos métodos de acceso desde Internet: Cisco *Expressway,* VPN de acceso remoto.

- Las funciones de Cisco *Jabber* para el envío de archivos, envío de captura de pantalla, compartir pantalla, etc., es comunicación *peer to peer* entre los dispositivos finales. Estas funciones están disponibles en la opción con VPN de acceso remoto y no están disponibles en la solución con Cisco *Expressway*.

- Cisco *Jabber* brinda al usuario una opción de acceso rápido a los mensajes de voz, permitiendo a través de su interfaz reproducir los archivos de mensaje de voz sin tener que llamar al IVR del correo de voz.

- Mantener la característica de Presencia desde Internet, es de gran importancia porque así el usuario remoto puede revisar el estado de su compañero de trabajo antes de poder comunicarse, y así elegir mejor su vía de comunicación. Es decir, si un usuario necesita comunicarse con su compañero de trabajo, y observa que en Cisco *Jabber* mantiene un estado “en reunión” con un color ámbar, la elección para comunicarse puede ser mediante un mensaje de texto. Pero si el estado es “presentando” en color rojo, es posible que su compañero esté compartiendo su pantalla para una presentación, y con esto el usuario puede elegir una mejor manera de comunicarse o intentarlo en otro momento.

- En las pruebas de funcionamiento, la opción con Cisco *Expressway* presentó problemas de calidad en videollamadas, más que la opción de acceso a través de VPN. Pero en los resultados de las encuestas, la opción de *Expressway* es más aceptada por los usuarios por su facilidad de uso al momento de acceder al servicio de Comunicaciones Unificadas desde Internet.

- La solución Cisco *Expressway* es más atractiva para el usuario final, porque para ellos es transparente el acceso a los servicios de Telefonía IP, Correo de Voz, Presencia y Mensajería Instantánea.

4.2 Recomendaciones

- Si se requiere incluir un servicio de software libre, por ejemplo, Asterisk, en la solución de comunicaciones unificadas con Cisco, es necesario que este servicio cuente con todas las configuraciones de seguridad para que no se convierta en un expuesto de seguridad.

- Cisco *Expressway* no acepta conexiones si uno de los nodos o ambos, *Expressway* C o *Expressway* E, pierde acceso al servicio NTP. Es por esta razón que lo recomendable es levantar este servicio en un equipo con alta disponibilidad y que pueda ser alcanzable desde los dos servidores.

- Cisco *Expressway* funciona sin problemas con certificados digitales firmados por un servidor local. Es recomendable que los certificados de los elementos internos de la solución de Comunicaciones Unificadas con Cisco y de Cisco *Expressway* E, sean emitidos por un CA público, para que los usuarios que usan la aplicación desde Internet no reciban notificaciones de conexión a un servicio inseguro.

- Para implementaciones o migraciones de Telefonía tradicional a Comunicaciones Unificadas con Cisco, se recomienda realizar charlas dirigidas a personal técnico y no técnico sobre el uso de la solución, y así aprovechar todas las características implementadas.

- Si el plan de marcado de una organización define que para las llamadas a la PSTN se debe marcar un prefijo, es recomendable que la configuración del patrón 911 se configure con y sin prefijo.

- Si la opción de acceso remoto a utilizar es mediante VPN, se recomienda el uso de VPN SSL para asegurar que el usuario pueda conectarse desde cualquier sitio, ya que la VPN levanta la conexión utilizando puerto TCP 443 que es comúnmente utilizado para navegación web por medio de HTTPS.

- Si se requiere el uso de servicios de terceros para integrarlos con la solución de Comunicaciones Unificadas con Cisco, se recomienda que estos servicios sean soportados para evitar problemas de incompatibilidad.

- Se recomienda realizar procesos periódicos de *backups*, utilizando la administración de cada elemento de la solución de Comunicaciones Unificadas con Cisco.

- Por recomendación es necesario detener la réplica de bases de datos entre los nodos de un *cluster* de Comunicaciones Unificadas, cuando sea necesario apagar servidores virtuales de la solución UC. Una base de datos consistente es importante para el servicio.

- Cisco *Business Edition* 6000, es una solución diseñada y probada para implementaciones de hasta mil usuarios. Para diseños mayores la opción es utilizar el producto *Business Edition* 7000 o configuraciones personalizadas de servidores Cisco para alojar más servicios y mayor número de nodos en el *cluster* de CUCM. Cuando se requiere implementar un *cluster* CUCM de varios nodos, se recomienda distribuir la carga de trabajo, por ejemplo, un megacluster CUCM consta de 21 nodos: 16 nodos subscriptores para manejo de llamadas, 2 nodos con servicio TFTP, 2 servidores para proveer *music on hold* (MoH), y un servidor con el rol de *Publisher* que lidera las bases de datos de CUCM. Los 16 nodos subscriptores se agrupan en 8 pares en modo activo – *stand by* para ofrecer redundancia 1:1 para un máximo de 80000 dispositivos.

5. REFERENCIAS BIBLIOGRÁFICAS

[1] «Unified Communications,» Diciembre 2016. [En línea]. Disponible: https://www.kmlcs.com/voice-services/unified-communications/. [Último acceso: 15 Julio 2017].

[2] «Overview of Cisco Collaboration System Components and Architecture,» 13 Febrero 2017. [En línea]. Disponible: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab11/collab11/ovarchit.html. [Último acceso: 15 Julio 2017].

[3] «What is the difference between unified communications and unified messaging?,» 10 Mayo 2018. [En línea]. Disponible: http://searchunifiedcommunications.techtarget.com/answer/What-is-the-difference-between-unified-communications-and-unified-messaging. [Último acceso: 30 Mayo 2018].

[4] CISCO, «Session Initiation Protocol,» 21 Abril 2016. [En línea]. Disponible: http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/9_0_1/ccmsys/CUCM_BK_CD2F83FA_00_cucm-system-guide-90/CUCM_BK_CD2F83FA_00_system-guide_chapter_0101000.html#CUCM_TP_S57EBDA6_00. [Último acceso: 10 Febrero 2018].

[5] «IP Telephony Protocols,» 17 Noviembre 2017. [En línea]. Disponible: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/9_0_1/ccmsys/CUCM_BK_CD2F83FA_00_cucm-system-guide-90/CUCM_BK_CD2F83FA_00_system-guide_chapter_0100111.html#CUCM_RF_S698E703_00. [Último acceso: 10 Febrero 2018].

[6] «An Overview of XMPP,» [En línea]. Disponible: https://xmpp.org/about/technology-overview.html. [Último acceso: 15 Mayo 2018].

[7] «Magic Quadrant for Unified Communications,» 19 Julio 2017. [En línea]. Disponible: https://www.gartner.com/doc/reprints?id=1-46VDGVD&ct=170719&st=sb. [Último acceso: 21 Julio 2017].

[8] «Mensajería unificada,» 9 Diciembre 2016. [En línea]. Disponible: https://technet.microsoft.com/es-es/library/jj150478(v=exchg.150).aspx.

[9] CISCO, «Collaboration Instant Messaging and Presence,» 13 Febrero 2017. [En línea]. Disponible: http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab11/collab11/presence.html#pgfId-1124383. [Último acceso: 14 Junio 2017].

[10] CISCO, «Gateways,» 13 Febrero 2017. [En línea]. Disponible: http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab11/collab11/gateways.html#39374. [Último acceso: 10 Noviembre 2017].

[11] CISCO, «Collaboration Endpoints version 11,» 13 Febrero 2017. [En línea]. Disponible: http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab11/collab11/endpnts.html#16036. [Último acceso: 10 Noviembre 2017].

[12] CISCO, «Collaboration Endpoints,» 13 Febrero 2017. [En línea]. Disponible: http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab11/collab11/endpnts.html#34680. [Último acceso: 15 Noviembre 2017].

[13] CISCO, «Cisco Jabber,» Mayo 2018. [En línea]. Disponible: https://www.cisco.com/c/en/us/products/unified-communications/jabber/index.html. [Último acceso: 30 Mayo 2018].

[14] «Mobile Collaboration,» 13 Febrero 2017. [En línea]. Disponible: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab11/collab11/mobilapp.html. [Último acceso: 15 Octubre 2017].

[15] CISCO, «Collaboration Edge,» 3 Abril 2017. [En línea]. Disponible: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/enterprise/11x/collbcvd/edge.html#pgfId-1111665. [Último acceso: 10 Noviembre 2017].

[16] CISCO, «Cisco Voice and Unified Messaging Products Feature Comparison (Unity Express, Unity Connection, Unity),» 20 Octubre 2016. [En línea]. Disponible: https://www.cisco.com/c/en/us/products/collateral/unified-communications/unity/product_data_sheet0900aecd806bfc37.html. [Último acceso: 10 Mayo 2018].

[17] CISCO, «Cisco Unified Communications 11.x and 10.x Licensing,» 10 Enero 2018. [En línea]. Disponible https://www.cisco.com/c/dam/en/us/products/collateral/unified-communications/unified-communications-licensing/C45_523902_11_9_licensing_aag_v5a_1.pdf. [Último acceso: 30 Mayo 2018].

[18] CISCO, «Collaboration Virtualization Hardware,» Enero 2018. [En línea]. Disponible: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-hardware.html#bomC220M5SXTRC1. [Último acceso: 10 Febrero 2018].

[19] CISCO, «Network Infrastructure,» 13 Abril 2016. [En línea]. Disponible: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab10/collab10/netstruc.html#24007. [Último acceso: 10 Mayo 2018].

[20] «Virtualization Software Requirements - Required vs. Supported Vendors, Products, Versions and Feature Editions,» Noviembre 2017. [En línea]. Disponible: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-software-requirements.html#software_requirements.

[21] «ESXi Hardware Requirements,» 7 Octubre 2016. [En línea]. Disponible: https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.install.doc/GUID-DEB8086A-306B-4239-BF76-E354679202FC.html. [Último acceso: 12 Noviembre 2017].

[22] «Installation Guide for Cisco Unified Communications Manager,» 9 Noviembre 2017. [En línea]. Disponible: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/install/11_0_1/CUCM_BK_IDF93684_00_installing-cucm_1101/Installation_planning.html#CUCM_RF_R538E881_00. [Último acceso: 15 Diciembre 2017].

[23] «Understanding Delay in Packet Voice Networks,» 2 Febrero 2006. [En línea]. Disponible: https://www.cisco.com/c/en/us/support/docs/voice/voice-quality/5125-delay-details.html. [Último acceso: 10 Mayo 2018].

[24] «Use Linux Traffic Control as impairment node in a test environment,» 24 Noviembre 2014. [En línea]. Disponible: https://www.excentis.com/blog/use-linux-traffic-control-impairment-node-test-environment-part-2. [Último acceso: 15 Octubre 2017].

[25] CISCO, «SSL Introduction with Sample Transaction and Packet Exchange,» 7 Abril 2017. [En línea]. Disponible: https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-socket-layer-ssl/116181-technote-product-00.html. [Último acceso: 15 Julio 2017].

[26] [En línea]. Disponible: https://www.digium.com/solutions/unified-communications/what-is-unified-communications.

ANEXO I. IMPLEMENTACIÓN DE ELEMENTOS DEL PROTOTIPO DE COMUNICACIONES UNIFICADAS

Instalación de servidor *VMware ESX*

En la página de administración de *VMware Workstation* se debe dirigir al menú *File -> New Virtual Machine,* luego de eso se mostrará el *wizard* o *setup assistant* para la creación de la nueva máquina virtual, donde se realizan los siguientes pasos:

1. Se escoge *Typical* en el tipo de *wizard* de instalación (ver Figura I-1).

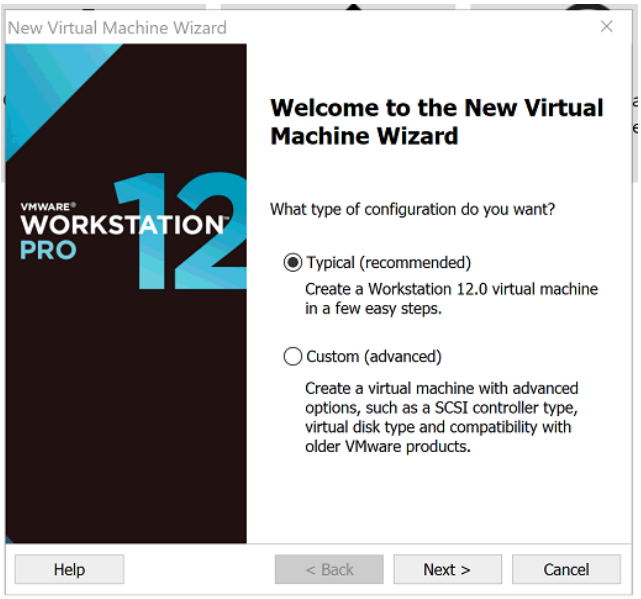

Figura I-1 Inicio de *wizard* de instalación.

2. Se selecciona la imagen .iso del sistema operativo ESX (ver Figura I-2).

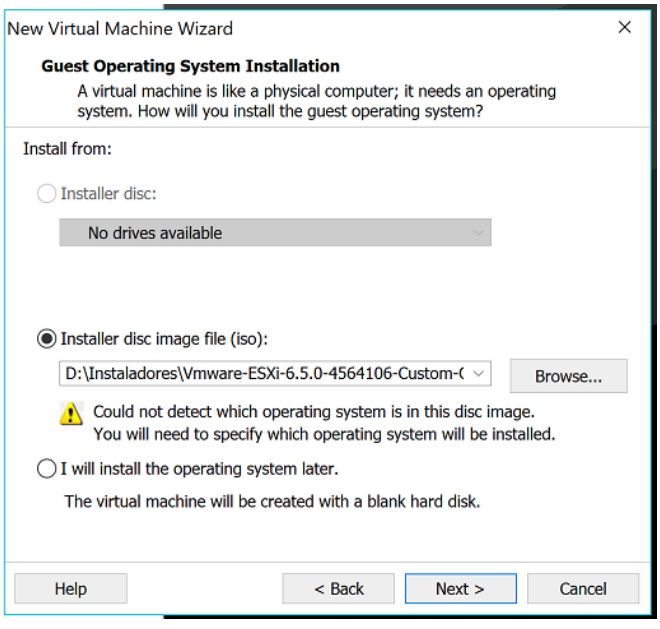

Figura I-2 Selección de archivo .iso para instalación de máquina virtual.

3. Se escoge el sistema operativo y la versión, tal y como se indica en la Figura I-3.

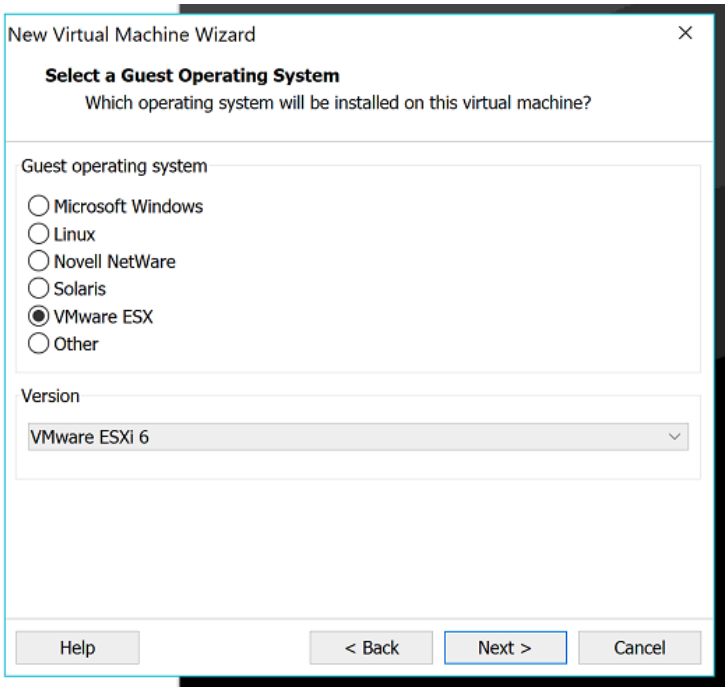

Figura I-3 Sistema operativo de máquina virtual.

4. Se configura el nombre de la máquina virtual su ubicación en el equipo físico (ver Figura I-4).

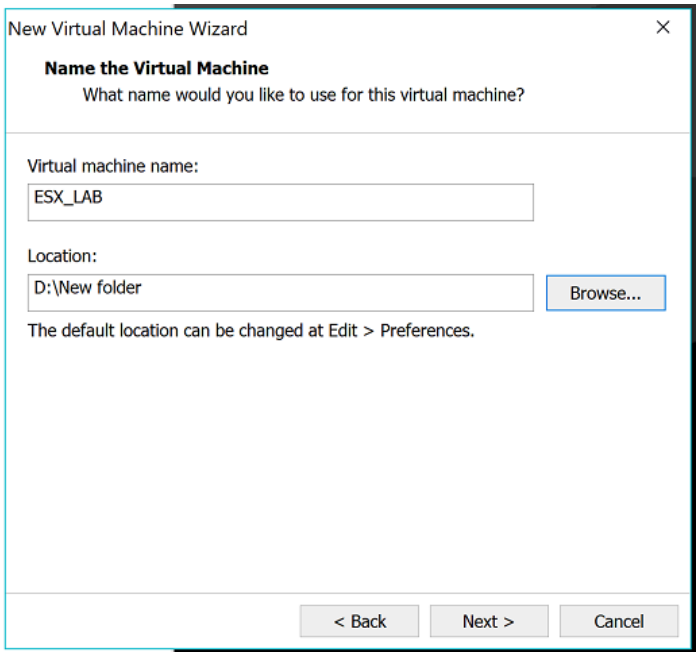

Figura I-4 Nombre y ubicación de máquina virtual.

5. Se ingresa el valor de espacio de disco necesario para el servidor ESX (ver Figura I-5).

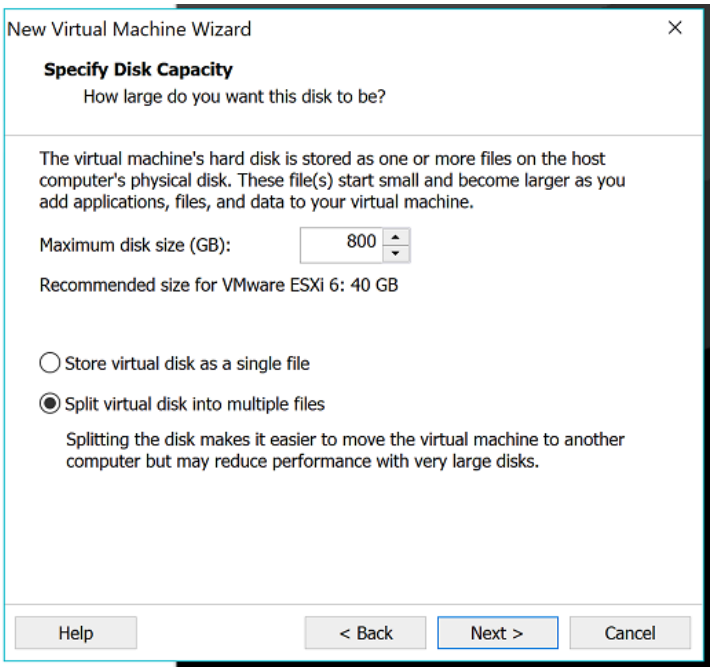

Figura I-5 Definición de capacidad de disco virtual.

6. Luego aparece el resumen para la creación de la máquina virtual, y es posible editar los valores de memoria RAM y CPU para cumplir con los valores definidos (ver Figura I-6).

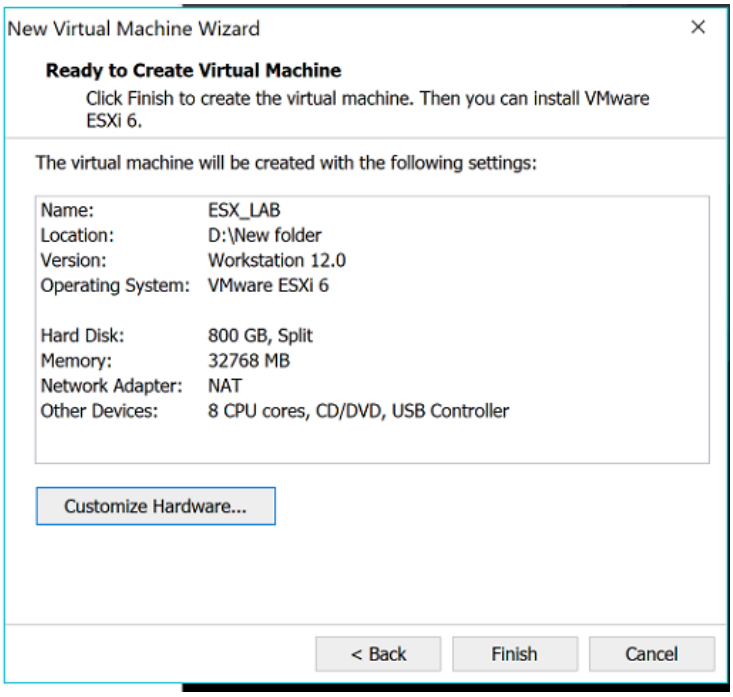

Figura I-6 Resumen de recursos para instalación de máquina virtual.

7. Se selecciona finalizar y el sistema creará la máquina virtual.
8. Una vez creada la máquina virtual, se procede a encenderla para que inicie el proceso de instalación del sistema operativo, y se ingresa los parámetros de instalación ya definidos (ver Figura I-7).

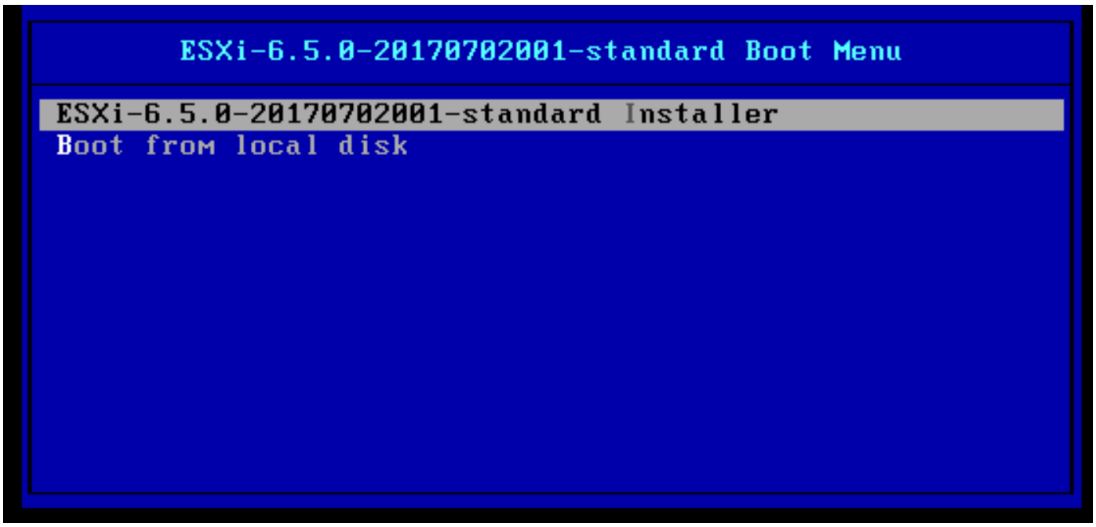

Figura I-7 *Wizard* de instalación de sistema operativo.

VMware ESX puede ser administrado desde *VMware Workstation*, pero para la creación de las máquinas virtuales utilizando los archivos OVA de Cisco, es necesario utilizar la aplicación *Web* o el cliente de escritorio *VMware VSphere.* En el presente proyecto la instalación se realizó con el cliente de escritorio de VMware.

Instalación de servidores virtuales Cisco

Una vez instalado *VMware ESX,* se accede desde el cliente *VSphere* (ver Figura I-8) para poder instalar las máquinas virtuales del prototipo. Las máquinas virtuales de la solución de Cisco de Comunicaciones Unificadas se instalan utilizando archivos OVA (*Open Virtualization Application/Appliance*).

Para desplegar el archivo OVA del servicio CUCM se realizan los siguientes pasos:

1. Desde *vsphere client* se selecciona *File -> Deploy OVF Template,* para iniciar el *wizard* de instalación tal y como se indica en la figura I-9.

2. En el *wizard* de instalación se escoge el archivo OVA para instalar en el ESX (ver Figura I-10).

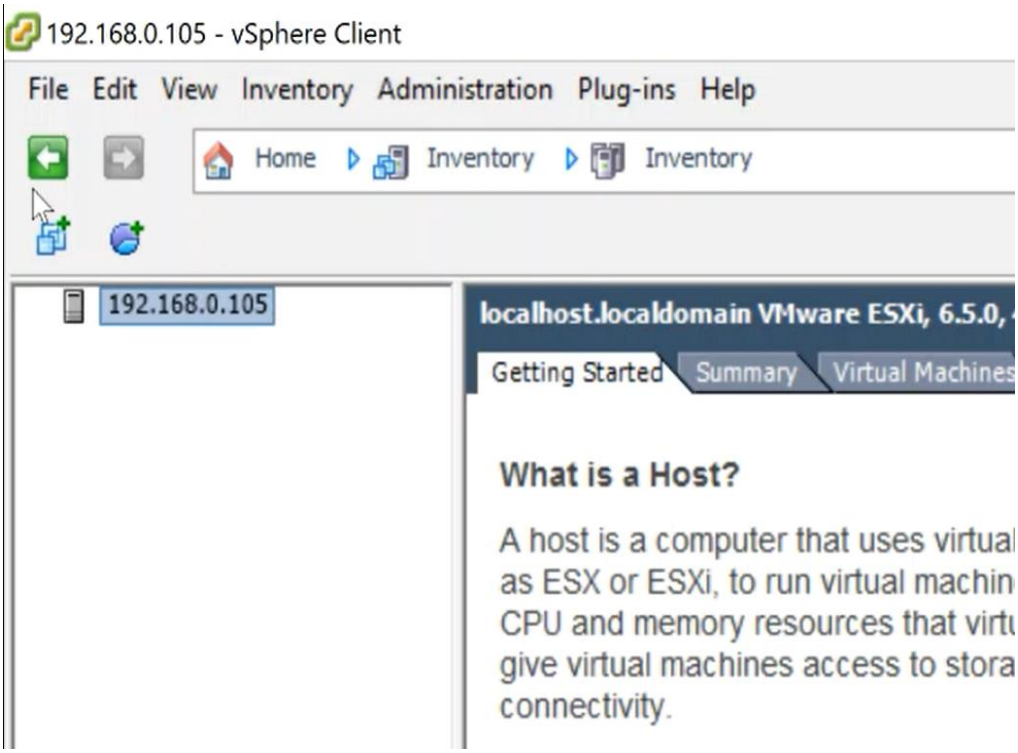

Figura I-8 *VMware VSphere.*

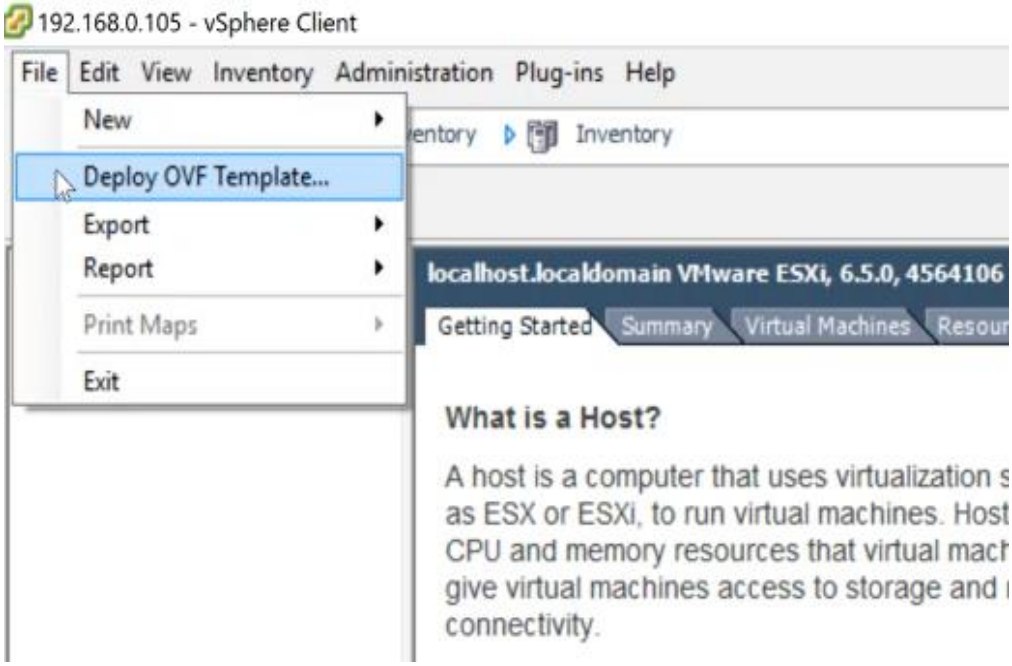

Figura I-9 Instalación de servicio CUCM desde archivo OVA.

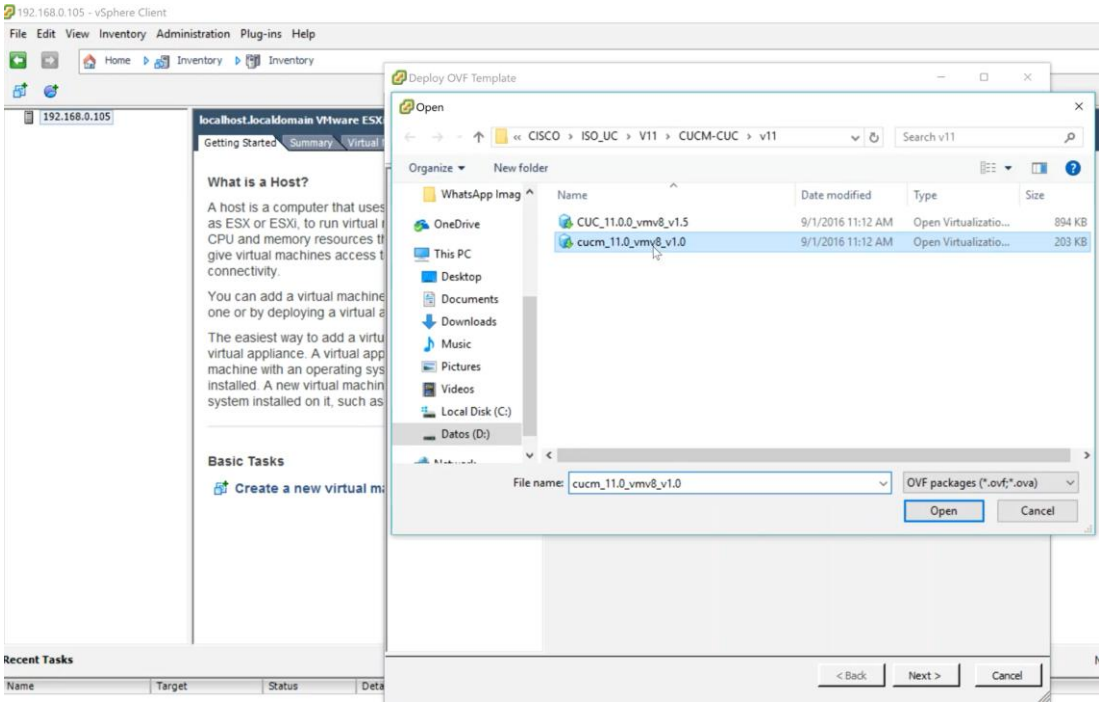

Figura I-10 Selección de archivo OVA desde wizard de instalación.

3. Luego de seleccionar el archivo OVA, en la siguiente sección se muestra la información de la máquina que se va a instalar (ver Figura I-11).

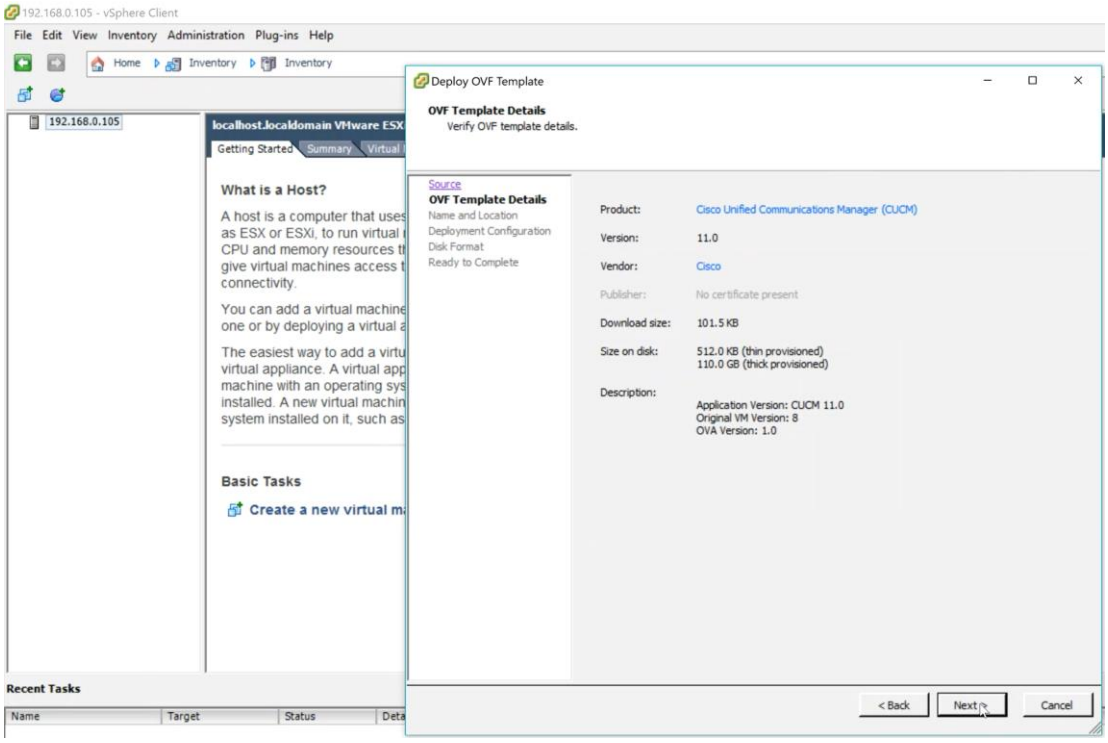

Figura I-11 Información de archivo OVA del servicio CUCM.

4. Se especifica el nombre de la máquina virtual, tal y como se muestra en la Figura I-12.

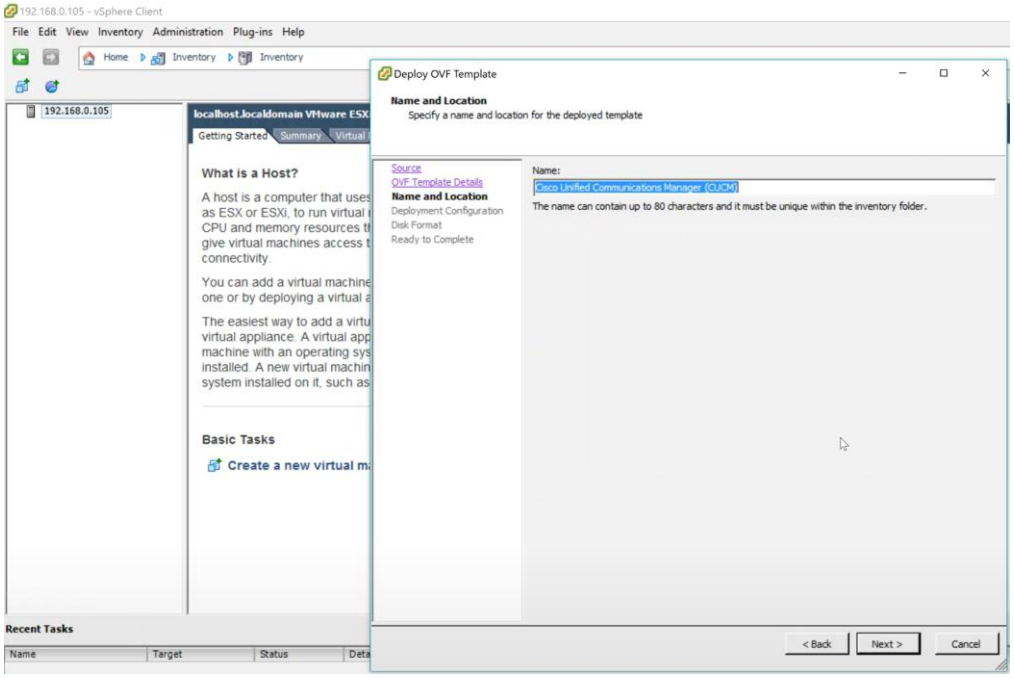

Figura I-12 Configuración de nombre de máquina virtual.

5. Se selecciona el tipo de instalación basándose en el número de usuarios a soportar. Para el prototipo se elige la opción más baja, y en la Figura I-13 se muestra la información de recursos que se va a utilizar para la máquina virtual.

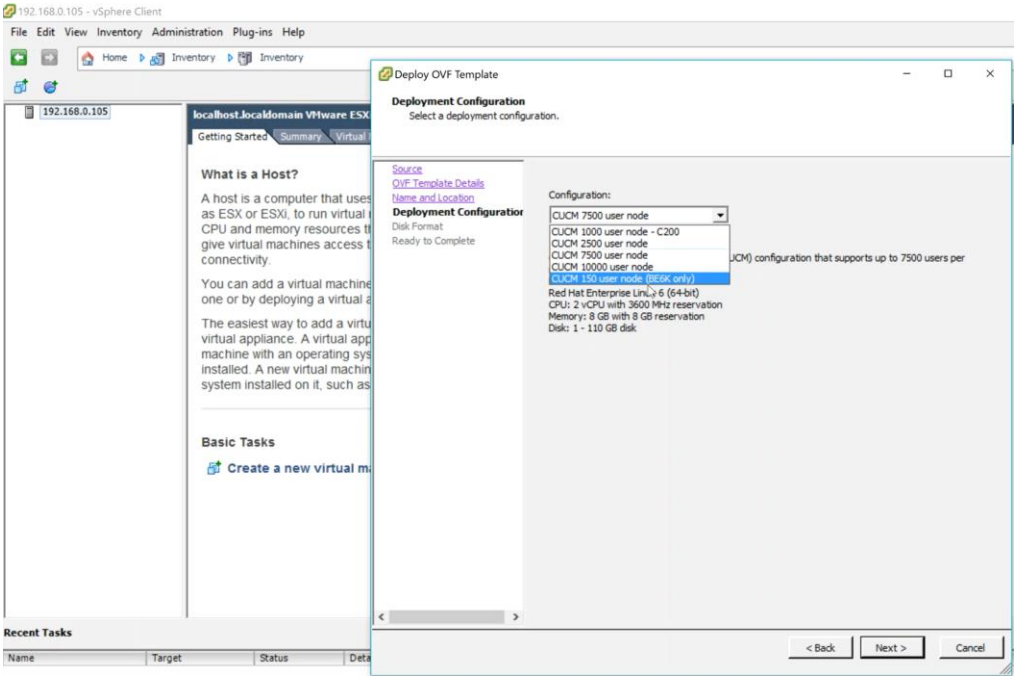

Figura I-13 Selección de tipo de instalación.

6. Para el formato de disco, se deja la opción que está por defecto. La recomendación de Cisco para los servicios de Comunicaciones Unificadas es que todos los recursos sean asignados de manera estática y no en modo *Thin Provision* que aumenta el tamaño del disco a medida que se va utilizando hasta llegar al máximo configurado (ver Figura I-14).

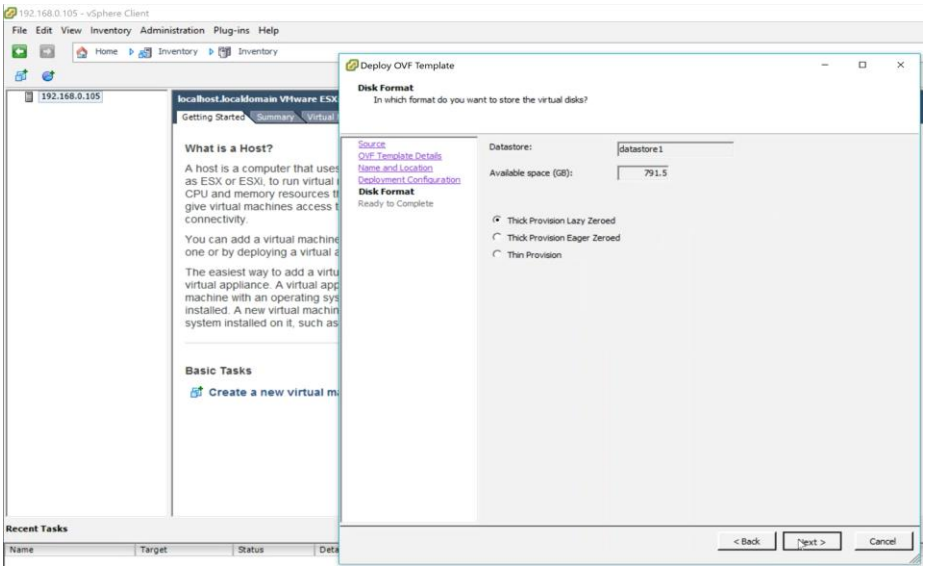

Figura I-14 Selección de formato de disco virtual.

7. Al final se muestra un resumen sobre la configuración de la máquina virtual (ver Figura I-15). Si se requiere realizar algún cambio, se lo hace sobre la máquina creada utilizando cualquiera de los clientes de administración de *VMware.*

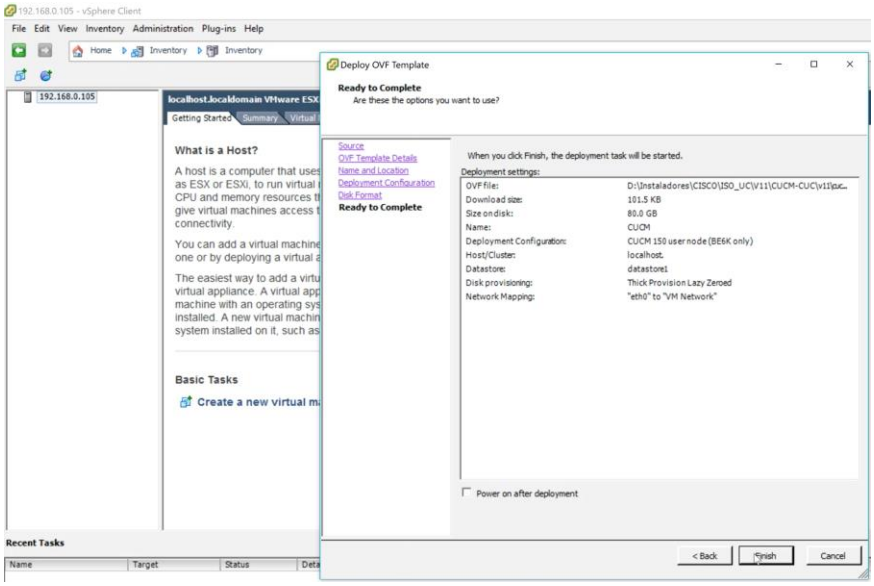

Figura I-15 Resumen de configuraciones de la máquina virtual.

El procedimiento descrito, aplica también para la creación de las máquinas virtuales de los servicios Cisco *Unity Connection* y Cisco *Unified Communications Manager IM and Presence.* Cisco *Expressway* utiliza el mismo archivo OVA para instalar el servicio *Core* o *Edge,* el tipo de servicio se define al momento de activar las licencias. Para el archivo OVA de Cisco *Expressway* se tienen las siguientes pantallas (figuras I-16 hasta I-20), diferentes al *wizard* de instalación de un OVA de CUCM.

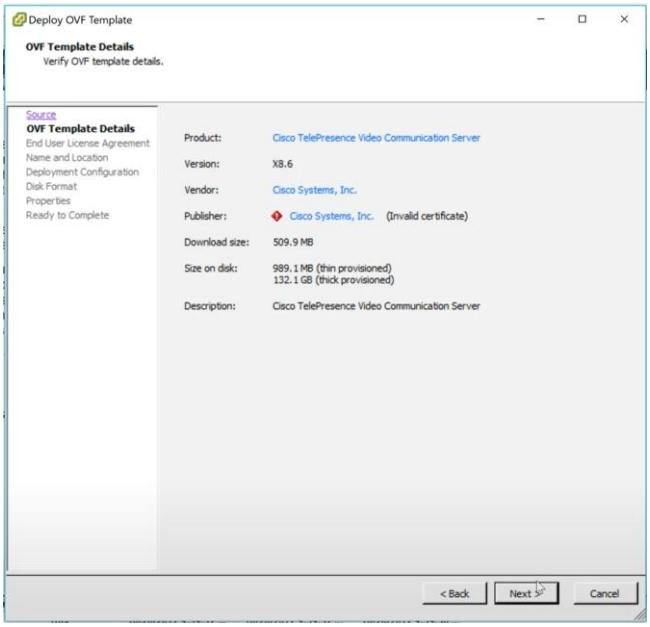

Figura I-16 Información de archivo OVA para Cisco *Expressway*.

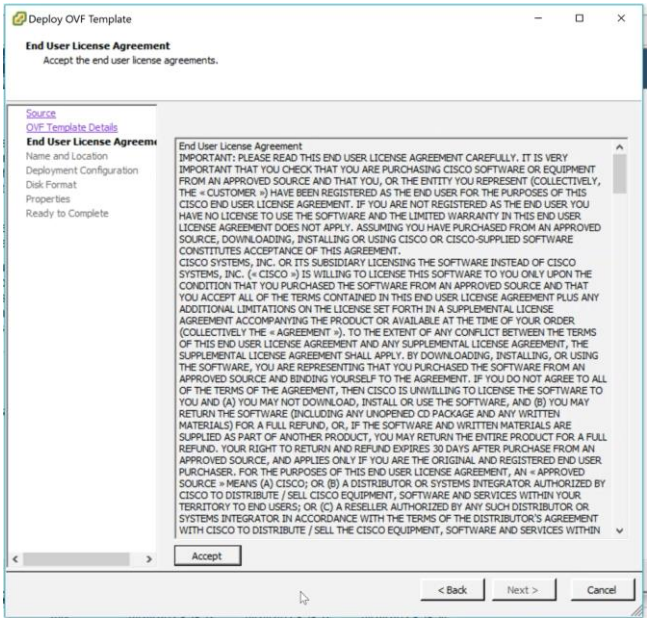

Figura I-17 Aceptación de acuerdo de licencia de usuario final.

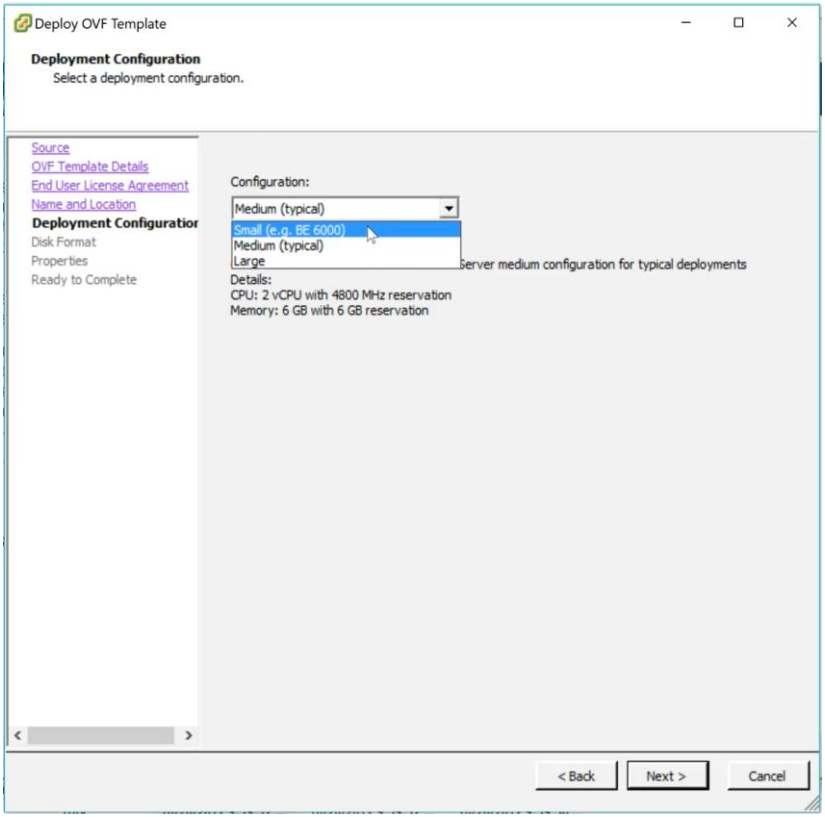

Figura I-18 Tipo de instalación.

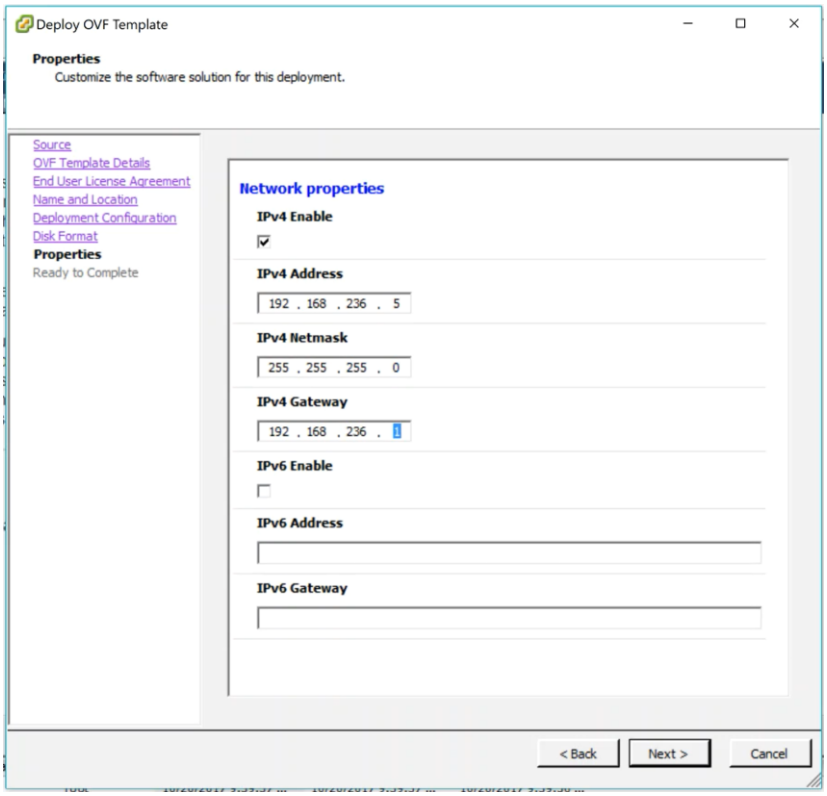

Figura I-19 Dirección IP de administración.

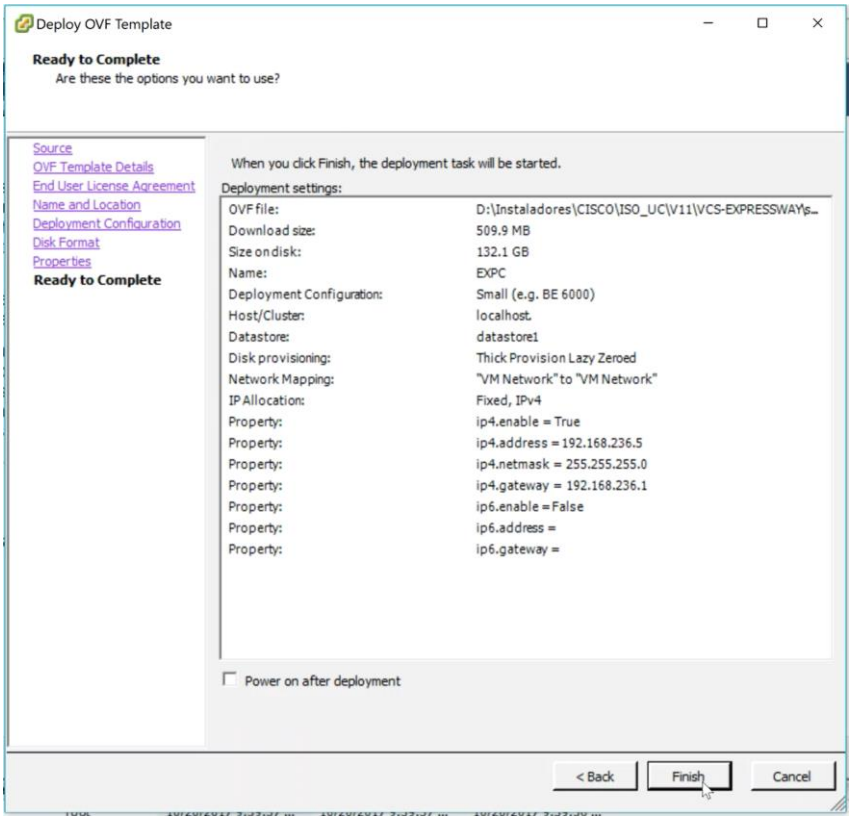

Figura I-20 Resumen de instalación de máquina virtual.

En el caso de Cisco *Expressway,* el sistema operativo es instalado con el despliegue del archivo OVA. Luego de realizar los pasos descritos, se ingresa mediante la consola de *VMware* al sistema y se inicia sesión utilizando las credenciales por defecto del producto: "*admin*" como nombre de usuario y "*TANDBERG*", esto inicia un pequeño *wizard* en el cual se ratifica la configuración IP del equipo. Cuando se confirma la información estará disponible el acceso a la administración web.

Instalación de servidores virtuales Linux y Windows

Para ambos servidores la creación se la realiza desde *VMware Workstation*. Para *Windows Server* se realizan los siguientes pasos:

1. En la primera ventana del *wizard* de configuración, se escoge la opción *typical* (ver Figura I-21).
2. Se selecciona el sistema operativo *Windows Server* 2012 de acuerdo con la imagen de instalación disponible (ver Figura I-22).

Figura I-21 Inicio de *wizard* de instalación.

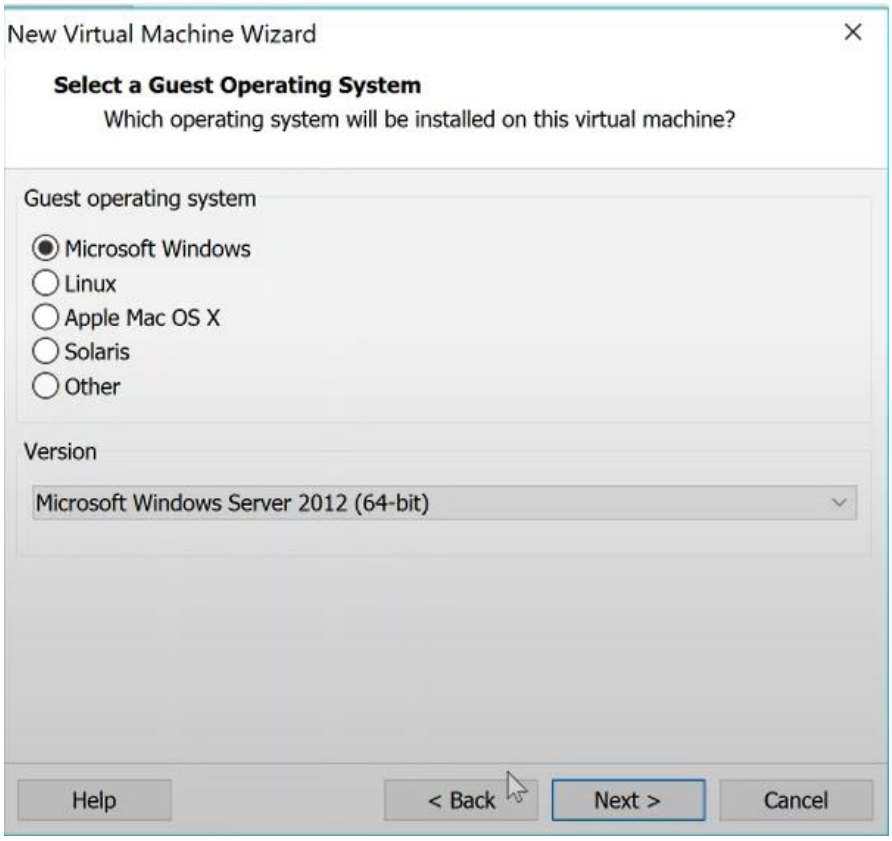

Figura I-22 Selección de sistema operativo.

3. Se configura un nombre a la máquina virtual (ver Figura I-23).

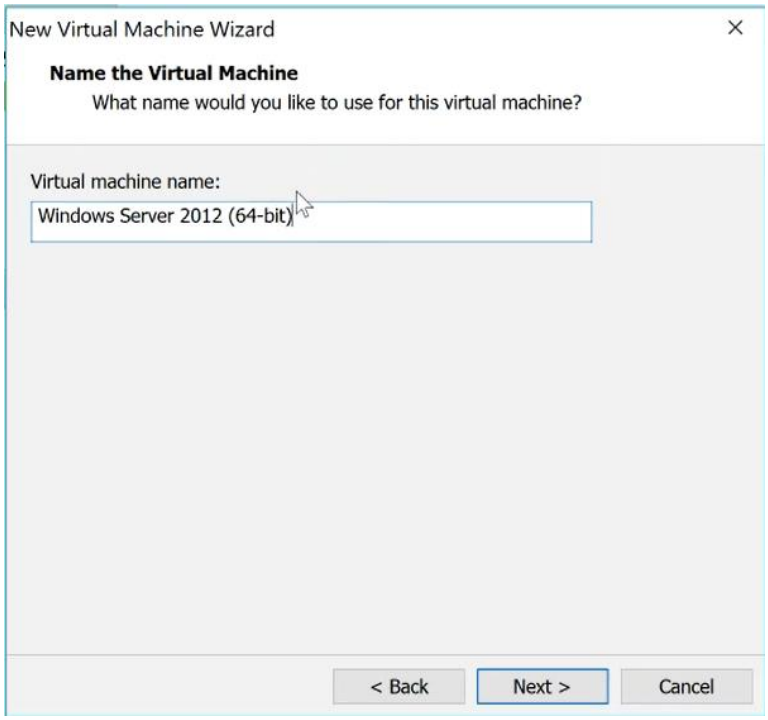

Figura I-23 Configuración de nombre de máquina virtual.

4. Se configura el espacio en disco definido para la máquina virtual (ver Figura I-24).

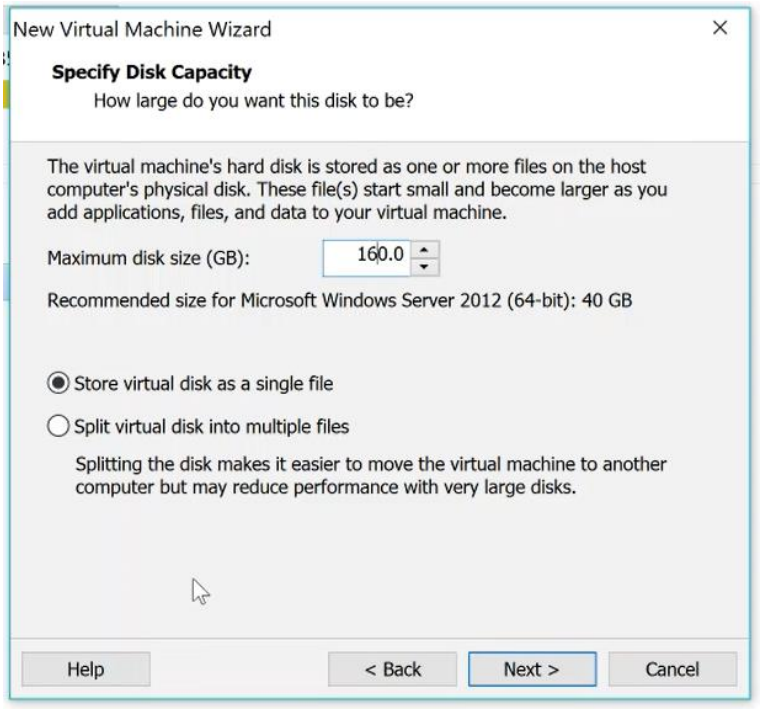

Figura I-24 Configuración de disco virtual.

5. Al final se mostrará un resumen de los recursos que se crearán en la máquina virtual (ver Figura I-25).

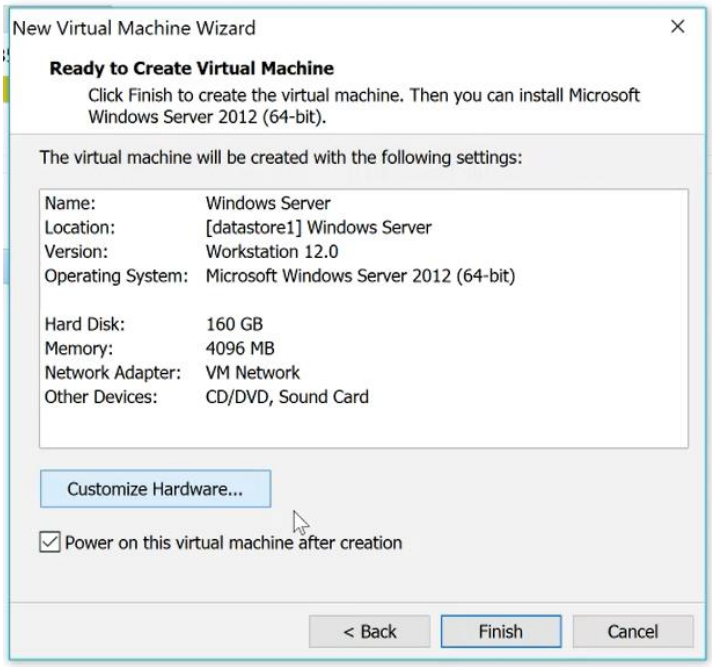

Figura I-25 Resumen de máquina virtual.

Para la creación del servidor Linux Centos se realizan los siguientes pasos:

6. En la primera ventana del *wizard* de configuración, se escoge la opción *typical* (ver Figura I-26).

Figura I-26 Inicio de *wizard* de instalación.

7. Se selecciona el sistema operativo Linux 7 (64-bit) (ver Figura I-27).

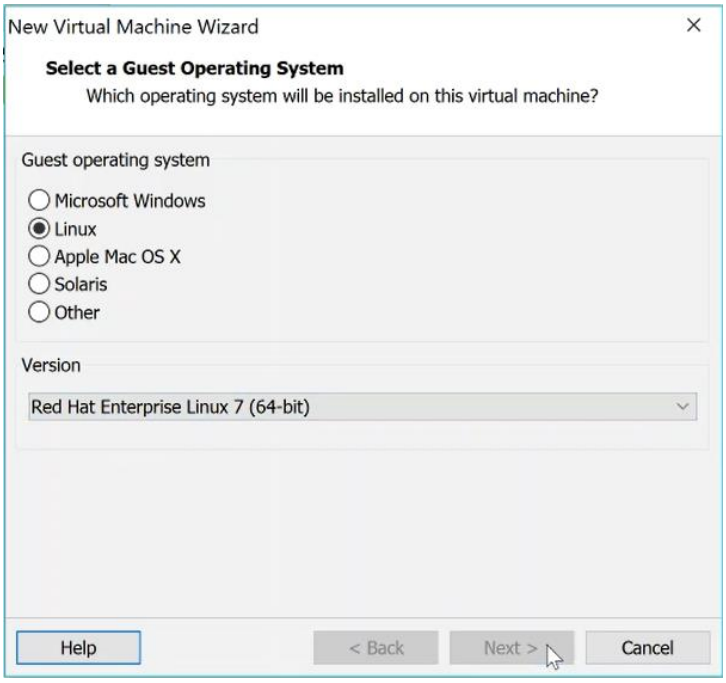

Figura I-27 Selección de sistema operativo.

8. Se ingresa el nombre de la máquina virtual (ver Figura I-28).

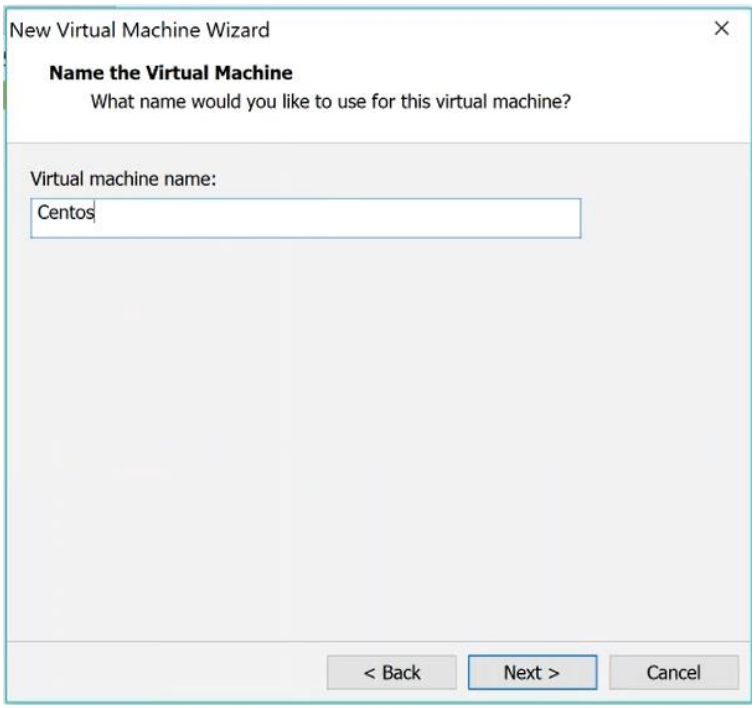

Figura I-28 Nombre de máquina virtual.

9. Se configura de espacio de disco virtual para máquina virtual (ver Figura I-29).

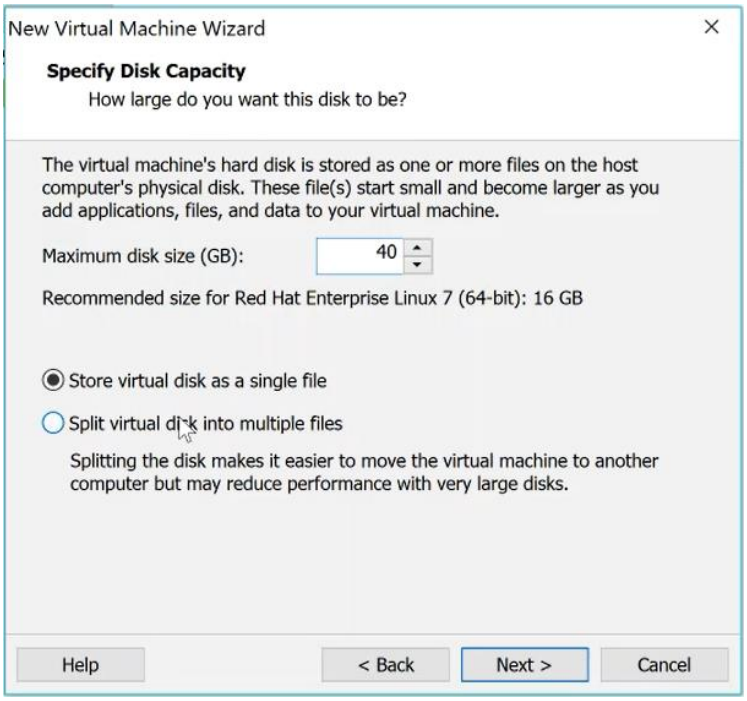

Figura I-29 Capacidad de disco virtual.

10. Finalmente se muestra un resumen de la configuración con la que se creará la máquina virtual (ver Figura I-30).

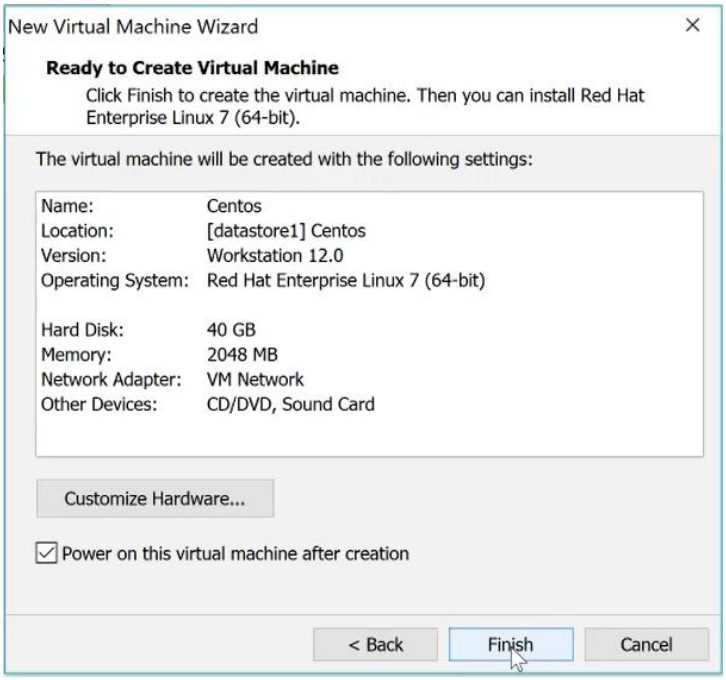

Figura I-30 Resumen de máquina virtual.

Instalación de sistemas operativos

Para instalar el sistema operativo de los servidores virtuales se utilizó el cliente *VSphere,* en él se siguen los siguientes pasos para poder iniciar el servidor en las opciones del BIOS:

1. Primero se selecciona la máquina virtual desde el cliente *VSphere* y se da clic en la opción *Edit virtual machine settings* (ver Figura I-31).

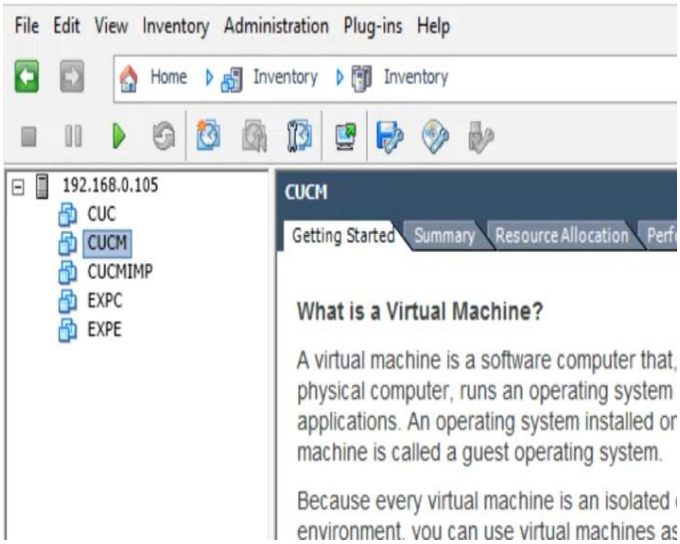

Figura I-31 Opciones de máquina virtual desde VSphere.

2. En la pestaña *Options* se selecciona la opción *Boot Options* del panel izquierdo de la ventana, y se marca el *checkbox* dentro del recuadro *Force BIOS Setup.*

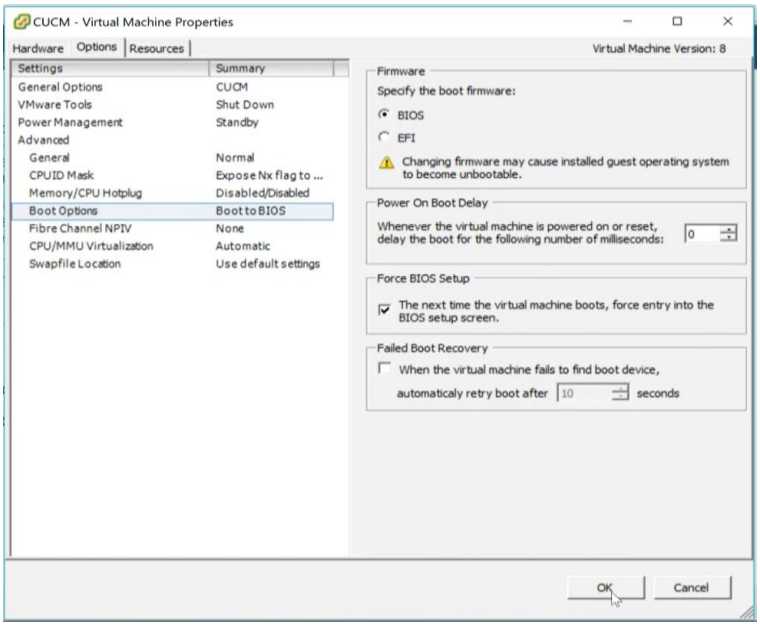

Figura I-32 Opciones de encendido de máquina virtual.

Luego de aplicar los pasos descritos, al encender la máquina virtual se mostrarán las opciones de BIOS, y en estas opciones se cambia el orden de arranque para que inicie desde el CDROM. Es necesario seleccionar la imagen de instalación antes de guardar los cambios de BIOS y reiniciar el servidor, y así el equipo iniciará el wizard de instalación del sistema operativo.

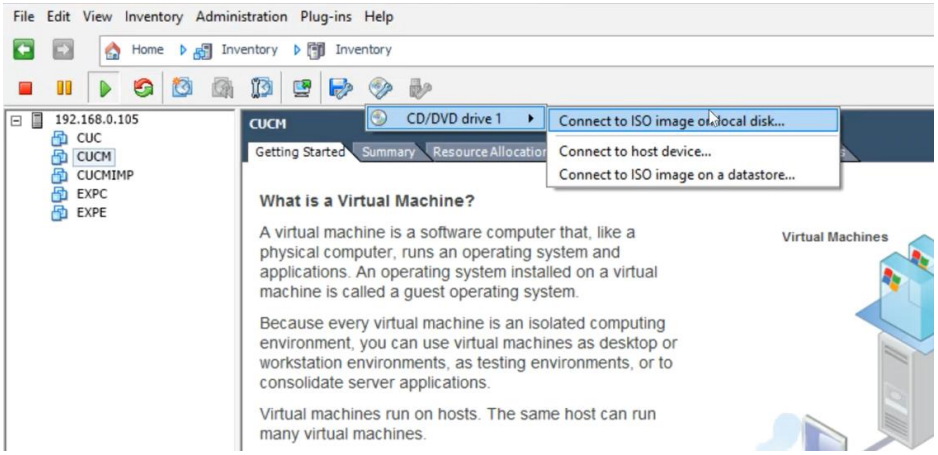

Figura I-33 Seleccionar imagen de instalación.

Para cada servicio se sigue paso a paso el *wizard* de instalación utilizando la información ya definida en el diseño de bajo nivel.

Los servicios de Cisco: CUCM, CUC y CUCMIMP tienen procedimiento similar de instalación de sistema operativo, a continuación, se detalla el *wizard* de instalación:

1. En cada máquina virtual se configura el uso de la imagen de instalación (ver Figura I-34).

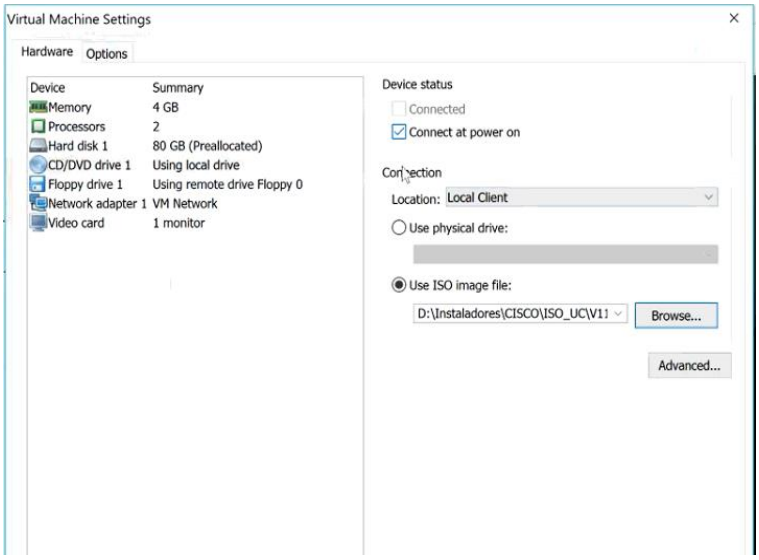

Figura I-34 Selección de imagen de instalación.

2. Se enciende la máquina virtual, y debido a la configuración de opciones de arranque, inicia en el menú de BIOS (ver Figura I-35), donde se cambia el orden de *Boot*, se guarda la configuración y se reinicia el servidor.

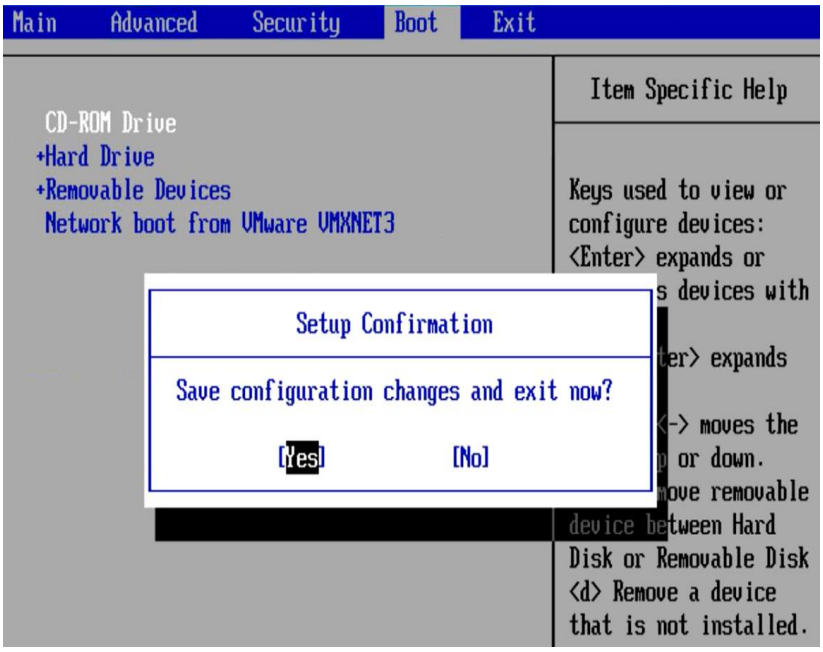

Figura I-35 Orden de *Boot*.

3. El *wizard* de instalación empieza con la pantalla en la cual se puede realizar una validación de la imagen de instalación (ver Figura I-36).

Figura I-36 Validación de la imagen de instalación.

4. Se selecciona el producto a instalar. Para cada imagen de instalación las opciones son diferentes (ver Figura I-37, I-38, I-39).

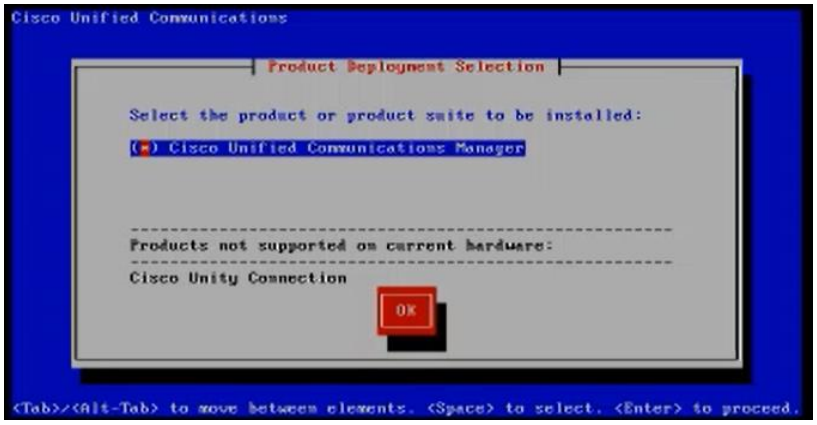

Figura I-37 Selección de producto para instalación de CUCM.

Figura I-38 Selección de producto para instalación de *Unity Connection*.

Figura I-39 Selección de producto para instalación de CUCMIMP.

5. Confirmación de la versión de software a instalar (ver Figura I-40).

Figura I-40 Versión de *software* a instalar.

6. Inicio de *wizard* de instalación. En los tres servicios se muestra la misma pantalla de opciones (ver Figura I-41).

Figura I-41 Inicio de *wizard* de instalación en CUCM.

7. Introducción a la instalación del servicio (ver Figura I-42), luego de seleccionar *Proceed* en el paso anterior.

Figura I-42 Introducción a la opción de instalación básica.

8. Se selecciona la zona horaria o *time zone* adecuado para la instalación (ver Figura I-43).

Figura I-43 Configuración de uso horario.

9. Las siguientes figuras: I-44, I-45 y I-46, son tres opciones rápidas de configuración de tarjeta de red. Por defecto la configuración de MTU no se modifica, y en la opción de escoger DHCP para la configuración IP, se selecciona no.

Figura I-44 Confirmación de negociación de tarjeta de red.

Figura I-45 Configuración de MTU.

Figura I-46 Configuración IP dinámica o estática.

10. Se ingresa la configuración IP en la pantalla representada por la Figura I-47.

Figura I-47 Configuración IP estática.

11. Se configura el usuario y contraseña de sistema operativo (ver Figura I-48).

Figura I-48 Credenciales de usuario de sistema operativo.

12. Se completa el formulario de información de certificado digital, como se indica en la Figura I-49.

13. En el prototipo se creará un nodo para cada servicio. En los servicios de CUCM y CUC, se indica que es el primer nodo, pero en el servicio CUCMIMP el nodo es siempre secundario y forma parte del clúster CUCM (ver Figura I-50).

14. Se configura la información NTP (ver Figura I-51).

Figura I-49 Información de certificado digital.

Figura I-50 Definición del primer nodo en el clúster.

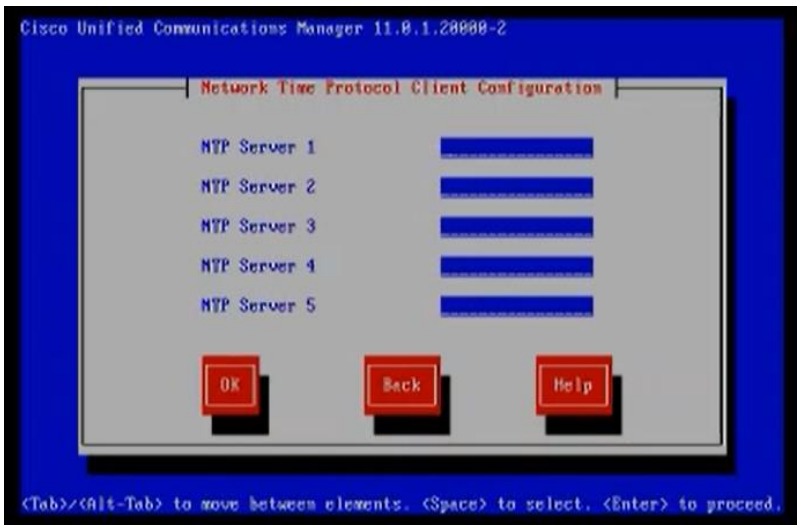

Figura I-51 Configuración NTP.

15. Se configura una contraseña de seguridad que se utiliza en el momento que se añaden nuevos nodos al clúster (ver Figura I-52).

Figura I-52 Configuración de contraseña de seguridad.

16. Se muestra la pantalla para la configuración de un servidor SMTP (Figura I-53), esta configuración es opcional.

Figura I-53 Confirmación para agregar la información de servicio SMTP.

17. Configuración de usuario de administración web (ver Figura I-54).

Figura I-54 Configuración de usuario de administración web.

18. Luego de ingresada la información solicitada en el *wizard*, se confirma la información ingresada para que inicie el proceso de instalación (ver Figura I-55).

Figura I-55 Confirmación para continuar con la instalación del sistema operativo.

Tal y como se indicó en el paso 8, al servicio CUCMIMP se configura como nodo secundario, porque forma parte del clúster CUCM, y es necesario que el servicio CUCM esté instalado ya (ver Figura I-56).

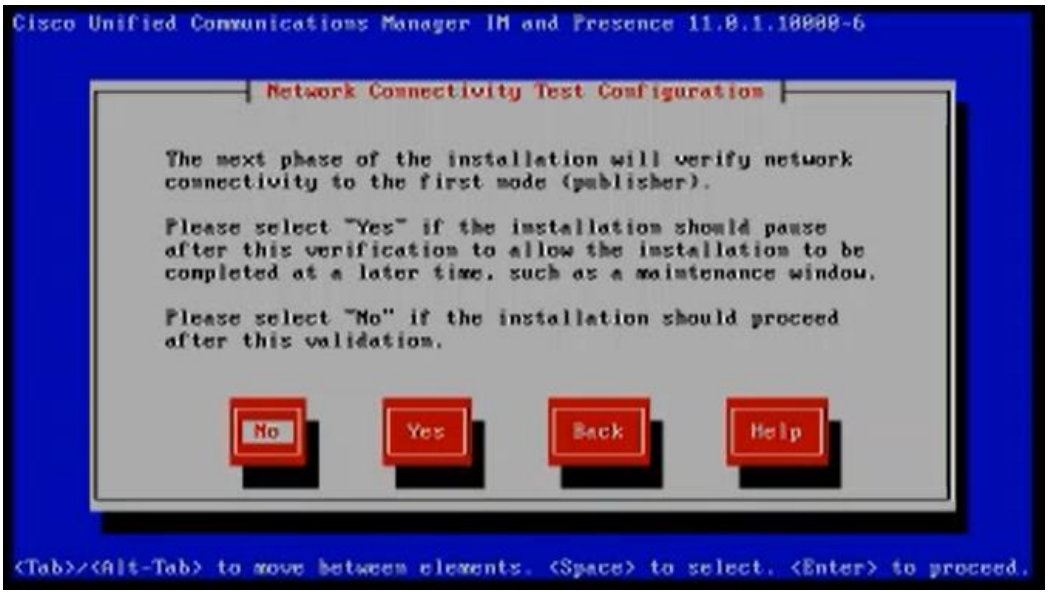

Figura I-56 CUCMIMP como parte del clúster CUCM.

Figura I-57 Configuración para conectividad con el primer nodo de CUCM.

Para la instalación del sistema operativo *Windows Server* realizamos el siguiente procedimiento:

1. Cuando se inicia el servidor virtual desde la imagen de instalación, aparecerá la pantalla de la Figura I-58, en la cual se selecciona “Instalar ahora”.

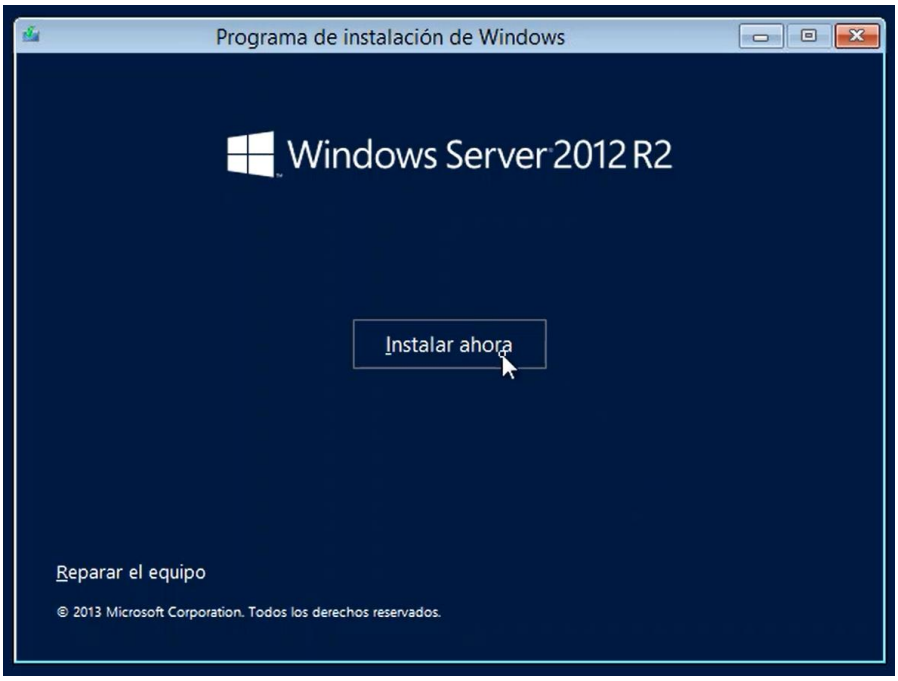

Figura I-58 Inicio de wizard de instalación de Windows Server.

2. Se selecciona el sistema operativo a instalar (Figura I-59).

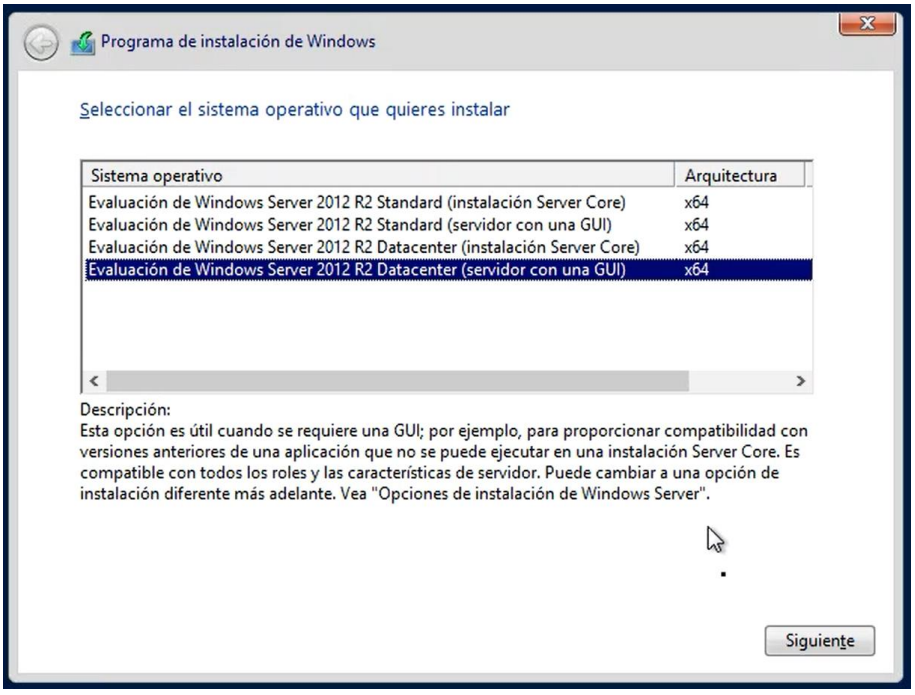

Figura I-59 Selección de sistema operativo.

3. Se aceptan los términos de licencia para continuar con la instalación.

Figura I-60 Términos de licencia de software.

4. Se selecciona el espacio de *storage* para el servidor *Windows Server* (ver Figura I-61).

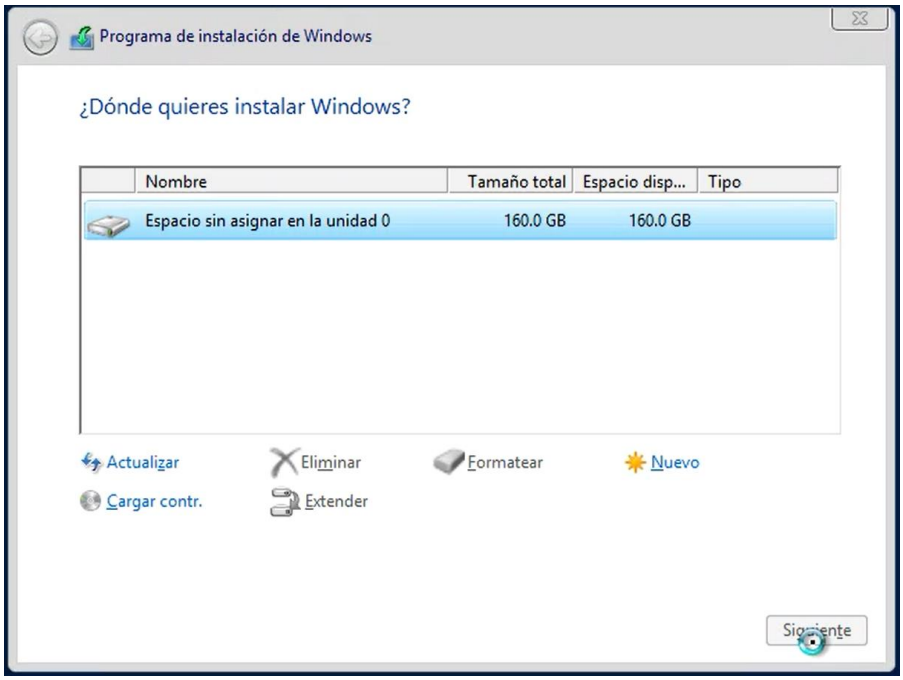

Figura I-61 Asignación de espacio para instalación.

5. Luego de la selección de espacio de *storage*, inicia el proceso de instalación de sistema operativo (Figura I-62).

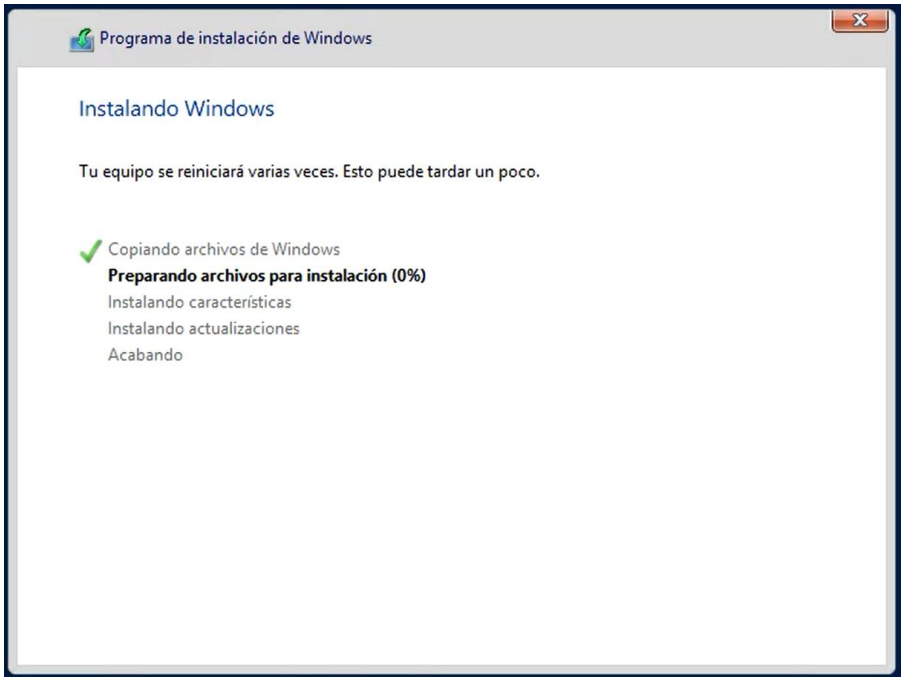

Figura I-62 Inicio de instalación del sistema operativo.

6. Una vez que finaliza la instalación, el equipo se reinicia y presenta la pantalla para la configuración de la contraseña del usuario administrador (Figura A-63).

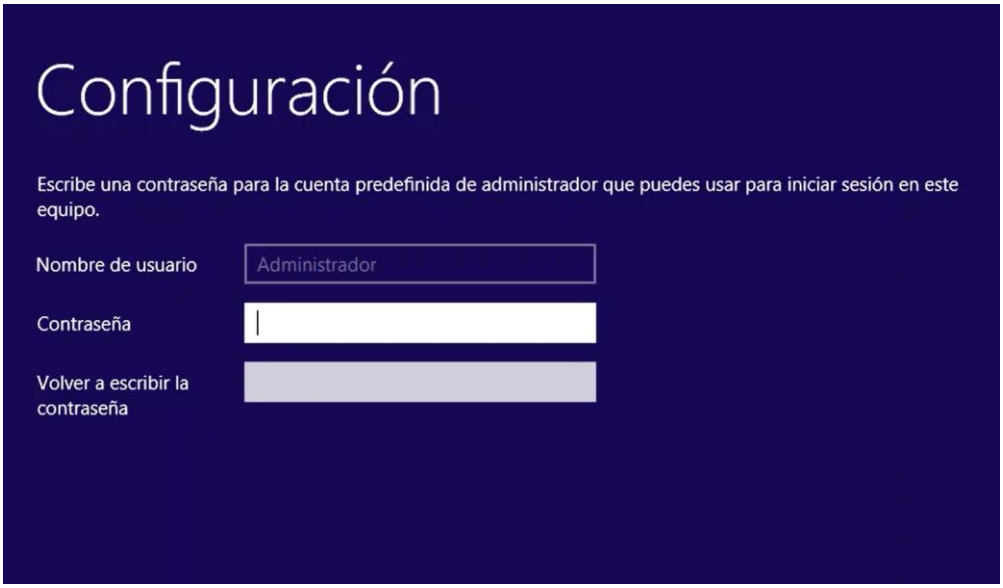

Figura I-63 Configuración de contraseña de administrador.

El servidor Linux se instala realizando los siguientes pasos:

1. Al cargar la imagen de instalación, se mostrará la pantalla inicial del *wizard* en la cual se selecciona la opción *"Install CentOS Linux 7"* (ver Figura I-64).

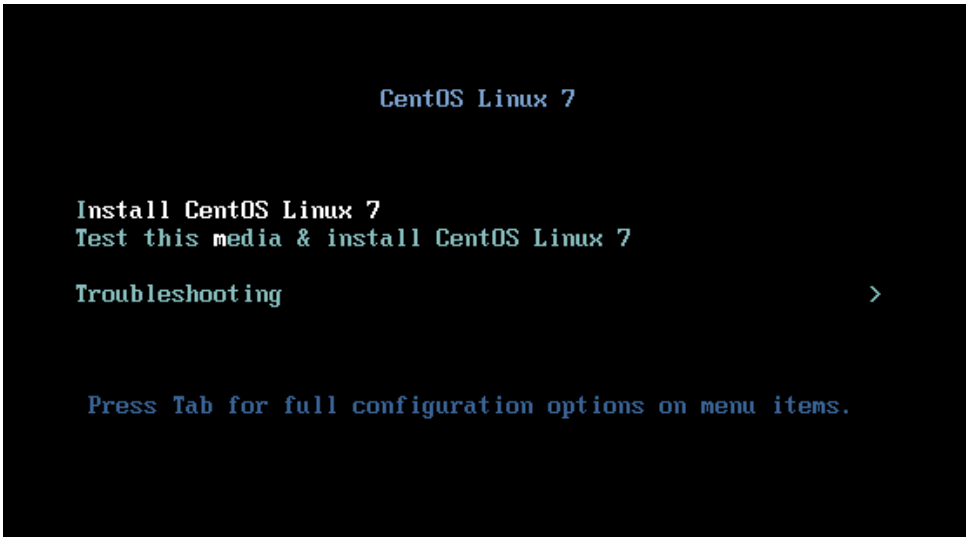

Figura I-64 Inicio de instalación de sistema operativo CentOS.

2. Se selecciona el lenguaje para la instalación (Figura I-65).

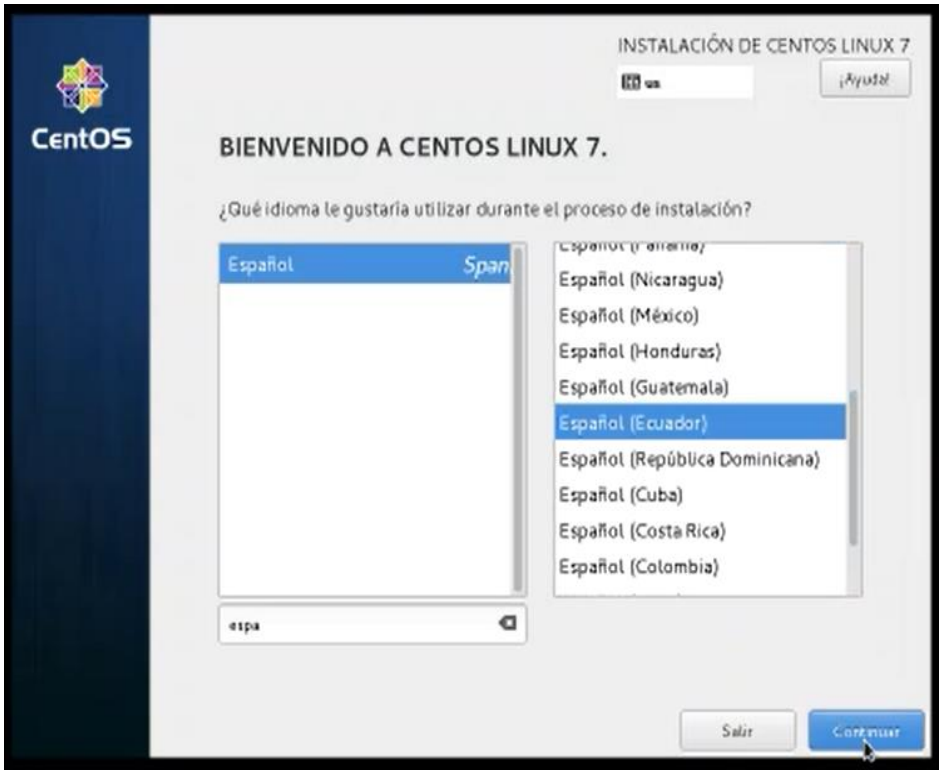

Figura I-65 Lenguaje de instalación.

3. Se valida que todos los ítems de la pantalla de resumen de instalación estén listos (Figura I-66).

Figura I-66 Resumen de instalación.

4. Se selecciona el disco virtual para la instalación de sistema operativo y se continúa con él *wizard* (Figura I-67).

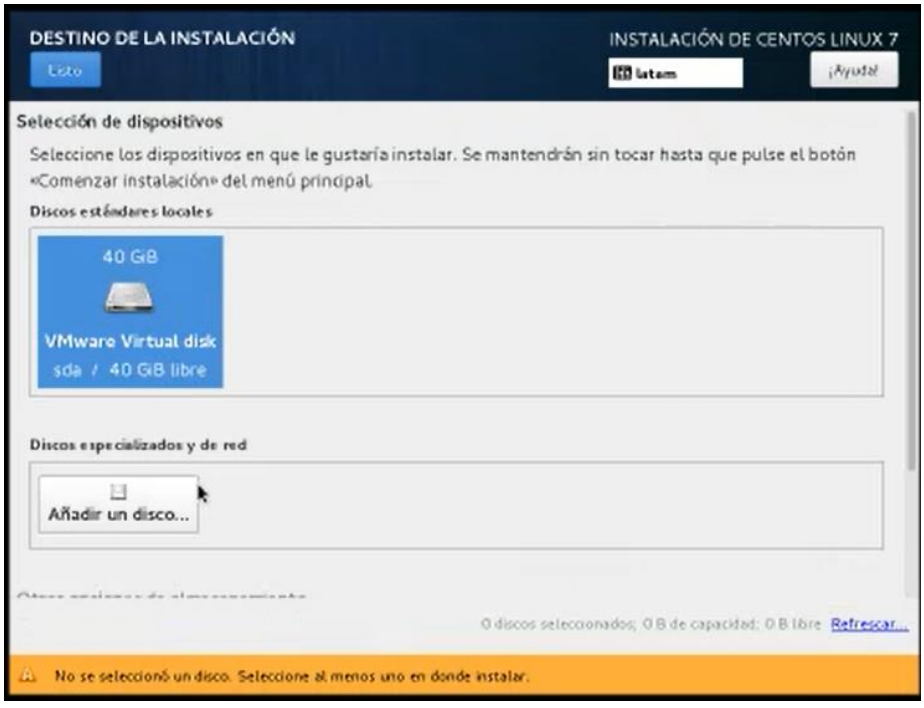

Figura I-67 Selección de destino de instalación.

5. Mientras el proceso de instalación continúa, el sistema permite configurar la contraseña para el usuario *root* (ver Figura I-68).

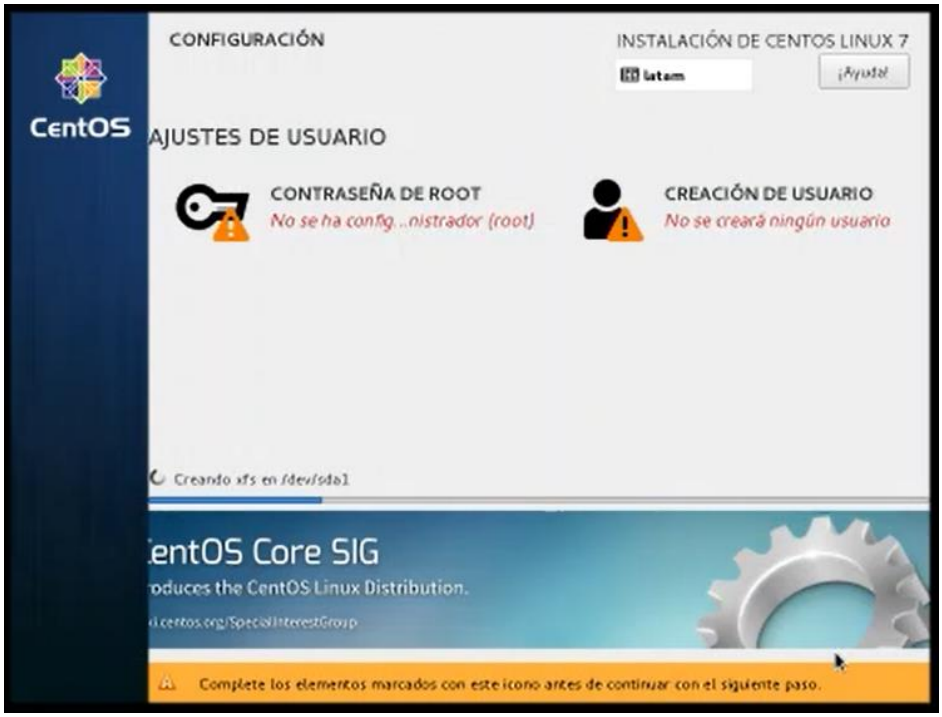

Figura I-68 Ajuste de usuario *root*.

ANEXO II. FUNCIONAMIENTO DE VPN DE ACCESO REMOTO

VPN de Acceso Remoto IPSec

IPSec: Fase 1

ISAKMP (*Internet Security Association and Key Management Protocol*) e IKE (*Internet Key Exchange*) trabajan en conjunto para poder establecer una conexión segura entre dos dispositivos. ISAKMP define el formato del mensaje, los mecanismos para el protocolo de intercambio de claves, y el proceso de negociación para crear las conexiones. IKE define la creación de las claves, el intercambio y administración de las mismas para proteger las conexiones seguras.

a) La Conexión de Administración

La conexión de administración se establece en la Fase 1. Esta conexión utiliza el puerto UDP 500, la conexión es bidireccional y ambos pares de la comunicación pueden utilizar esta conexión para el intercambio de mensajes IPSec. La conexión de administración se asegura utilizando políticas ISAKMP/IKE.

Las políticas ISAKMP/IKE también son conocidas como propuestas (ISAKMP/IKE *Proposal*), y es una lista de medidas de seguridad que deberían ser usadas para proteger la conexión de administración.

ISAKMP/IKE *Proposal* contiene:

- El algoritmo de encriptación a usar: DES, 3DES, o AES.
- La función HMAC a usar: MD5 o SHA-1
- El tipo de autenticación de dispositivo: clave pre-compartida (Simétrico), *nonces* cifrados RSA (clave pre-compartida con método asimétrico), firmas RSA (Certificados Digitales).
- El grupo de claves/llaves Diffie-Hellman: Cisco soporta únicamente los grupos 1,2,5,7.
- El tiempo de vida de la conexión de administración.

El dispositivo que inicia la comunicación IPSec envía una lista ordenada por prioridad de políticas ISAKMP/IKE al dispositivo remoto. Las prioridades de la lista de políticas son configurables en el *Gateway* VPN. El *peer* remoto compara la lista recibida de manera ordenada con su propia lista de políticas ISAKMP/IKE hasta encontrar una coincidencia y continuar con el procedimiento, y en caso de no haber coincidencia la conexión fallará.

Protocolo de Intercambio de Llaves: *Diffie-Hellman* (DH)

DH es utilizado para crear una clave/llave secreta compartida. Los pares de la comunicación IPSec generan una combinación de clave privada y pública, y comparten sus claves públicas entre ellos. Luego se utiliza la clave privada y la clave pública del par remoto para ejecutar una función que da como resultado una clave secreta, la cual es la misma en ambos pares de comunicación.

La clave secreta resultante luego se emplea para cifrar cualquier información adicional para la conexión de administración propuesta, como lo es la clave del algoritmo de encriptación y la clave de la función HMAC.

Los grupos de claves DH son utilizados para poder aplicar diferentes niveles de complejidad en el proceso de encriptación. Existen algunos grupos DH que pueden ser usados, y Cisco soporta los siguientes:

- Grupo DH 1, 768-bit.
- Grupo DH 2, 1024-bit.
- Grupo DH 5, 1536-bit.
- Grupo DH 14, 2048-bit.
- Grupo DH 15, 3072-bit.
- Grupo DH 16, 4096-bit
- Grupo DH 19, 256-bit con algoritmo de curva elíptica.
- Grupo DH 20, 384-bit con algoritmo de curva elíptica.
- Grupo DH 24, 2048-bit DH con firma digital.

Autenticación de Dispositivo

En la Fase 1 de IPSec con el modo agresivo, la negociación DH y la verificación de la identidad ocurre en un paso, y en el modo principal (*Main Mode*) el proceso toma tres pasos. En el tercer paso del modo principal de IPSec, se realiza la autenticación de dispositivo utilizando la conexión segura que se generó al compartir las claves de encriptación y HMAC. Los elementos que necesiten compartir entre los dos pares de la comunicación para poder realizar la autenticación entre ellos se enviarán a través de la conexión segura de administración.

En IPSec existen tres métodos básicos para poder realizar la autenticación de dispositivos:

- Claves pre-compartidas simétricas.
- Claves pre-compartidas asimétricas.

- Certificados Digitales.

El método por utilizarse entre los pares de IPSec lo negocian cuando intercambian las políticas ISAKMP/IKE de la Fase 1. Para el caso de VPN de acceso remoto se utiliza otro tipo de clave pre-compartida y se denomina de grupo. Cuando un cliente VPN de acceso remoto realiza autenticación de dispositivo, el dispositivo cliente debe enviar el nombre de grupo y la clave pre-compartida del grupo.

Pasos adicionales para VPN de Acceso Remoto

Para una VPN *site-to-site* con la autenticación de dispositivo terminaría la Fase 1, pero en una sesión de VPN de acceso remoto con cliente Cisco se realizan los siguientes pasos adicionales:

1. Autenticación de usuario (XAUTH).
2. Aplicación de políticas de grupo al usuario o grupo de usuarios (Configuración de Cliente IKE).

Autenticación de usuario con XAUTH

La autenticación de dispositivo permite al *Gateway* VPN y al cliente de acceso remoto autenticarse entre ellos, pero para controlar quien puede hacer uso de la VPN autenticada se utiliza una propiedad del *Gateway* VPN denominada XAUTH (Autenticación extendida), que permite autenticar al usuario que está utilizando el dispositivo cliente al solicitarle sus credenciales (nombre de usuario y contraseña).

El *Gateway* puede validar las credenciales contra un dispositivo externo como un servidor AAA o un Directorio Activo, o puede validarlas contra las credenciales almacenadas en su base local.

Políticas de grupo (*VPN GROUP POLICIES*)

En este paso el *Gateway* VPN aplica algunos parámetros al cliente VPN. Las políticas pueden incluir:

- Una dirección IP interna o lógica, que se aplica en el dispositivo cliente y que sirve solo para la comunicación a través del túnel. Esta dirección IP es adicional a la que mantiene el dispositivo remoto en su LAN.
- Nombre de dominio del servicio DNS.
- Dirección IP del servidor DNS.
- Dirección IP del servidor WINS.

- Políticas *Split Tunneling,* que define qué comunicación el dispositivo cliente va a dirigir a través del túnel VPN y qué comunicación lo dirigirá hacia la LAN.

IPSec: Fase 2

En la Fase 2 se define cómo se construyen conexiones seguras de datos de usuario entre dos pares IPSec. En la Fase 2 se crean dos conexiones de datos unidireccionales entre los pares IPSec, es decir el par A tiene una conexión de datos hacia el par B, y el par B tiene una conexión de datos aparte hacia el par A.

a) Protocolos de seguridad en la Fase 2

IPSec utiliza dos protocolos para la Fase 2: AH (*Authentication Header*) y ESP (*Encapsulating Security Payload*).

El protocolo AH provee un mecanismo para realizar solo autenticación. Provee integridad de datos, autenticación del origen de datos, y opcionalmente protección contra ataques de tipo *data-replay*. La integridad de datos se valida con el uso de resúmenes generados con MD5 o SHA. La autenticación del origen de datos se asegura utilizando la calve secreta compartida para crear el resumen del mensaje (MD5 o SHA). La protección contra ataques de tipo *data-replay* se realiza usando números de secuencia en la cabecera de AH.

ESP provee confidencialidad de datos (encriptación) y autenticación. ESP puede ser usado para brindar solo confidencialidad, solo autenticación, o ambos confidencialidad y autenticación. ESP usa los mismos algoritmos que AH pero la diferencia radica en la cobertura, AH autentica el paquete IP entero mientras que ESP solo autentica los datos del paquete IP.

Modos de conexión

Existen dos modos: modo transporte y modo túnel.

El modo túnel es utilizado para cifrar el tráfico entre *Gateways* IPSec (VPN *site-to-site*), o desde un dispositivo cliente hacia un *Gateway* IPSec (VPN de acceso remoto). El modo transporte es utilizado entre dispositivos finales que soportan IPSec.

Transformaciones en Fase 2

Una transformación define cómo las conexiones de datos deben ser protegidas. Al igual que las políticas ISAKMP/IKE de la Fase 1, en la Fase 2 las transformaciones

de datos deben coincidir en los pares IPSec. Un conjunto de transformaciones de datos contiene la siguiente información:

- El protocolo de seguridad: AH y/o ESP.
- El modo de conexión para los protocolos de seguridad: modo túnel o transporte.
- Para ESP, la información de encriptación: sin encriptación, DES, 3DES, AES-128, AES-192, o AES-256.
- La autenticación de paquetes y verificación por función HMAC: MD5 o SHA-1 (en ESP esta parte es opcional).

Asociaciones de seguridad (SA)

En IPSec una asociación de seguridad agrupa todos los componentes de seguridad necesarios para una correcta comunicación con el par IPSec. Se tienen SA de datos por dirección de la comunicación y por protocolo de seguridad utilizado, es decir que si entre dos pares IPSec se utiliza únicamente ESP entonces se tendrá un SA por par IPSec, y en el caso de que se usen ambos protocolos entonces se tendrán dos SA por cada par IPSec. El par IPSec receptor utiliza un parámetro denominado SPI (*Security Parameter Indexes*) para identificar el SA al cual un paquete entrante está vinculado.

En el SA de datos se puede encontrar la siguiente información:

- El protocolo de seguridad.
- El valor del SPI para AH y/o ESP.
- El modo de conexión para AH y/o ESP.
- El tiempo de vida, en segundos, del SA.
- La función HMAC de autenticación y verificación de integridad de paquete y las claves simétricas MD5 o SHA-1.
- El algoritmo de encriptación y la clave simétrica usada si se emplea ESP.
- PFS (*Perfect Forward Secrecy*).

PFS se usa para poder compartir entre los pares IPSec las claves simétricas de HMAC y encriptación, por defecto este parámetro está desactivado ya que la conexión de administración de la Fase 1 es utilizada para este fin. Cuando se utiliza la opción PFS se realiza el proceso con los grupos Diffie-Hellman.

VPN de Acceso Remoto SSL

Intercambio de mensajes en SSL [25]

En la Figura B-1 se puede apreciar un ejemplo del intercambio de mensajes en el protocolo SSL.

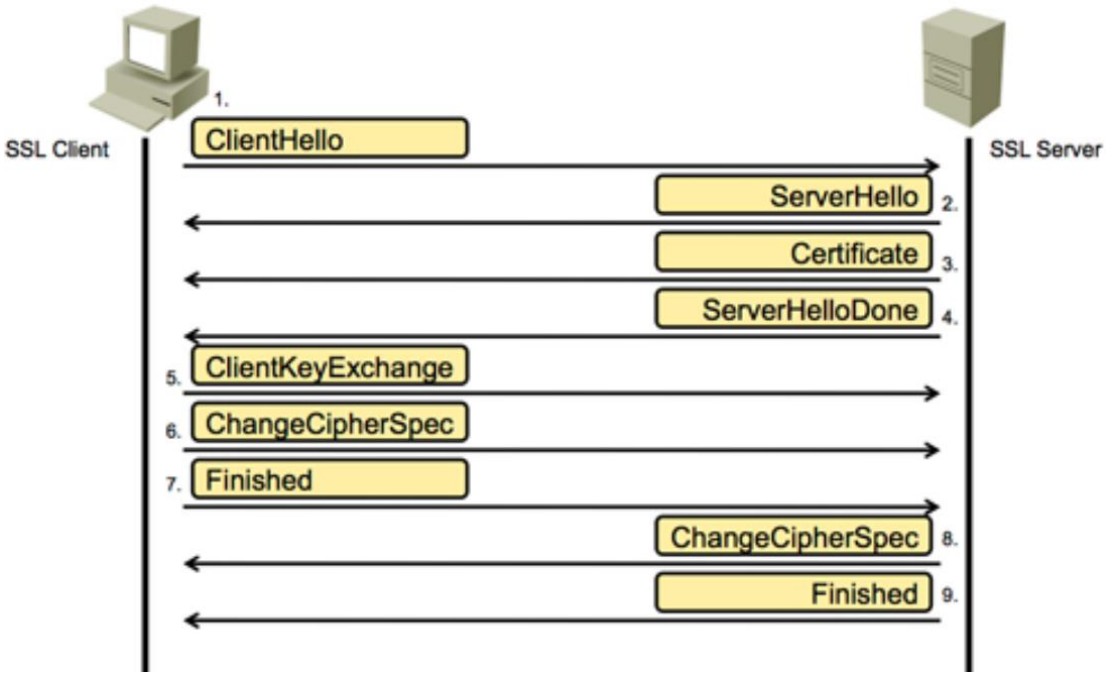

Figura II-1 Ejemplo de intercambio de mensajes en SSL. [25]

a) Intercambio de mensajes "*Hello*" (*Hello Message Phase*)

El cliente envía un mensaje de "*Client Hello*" al servidor, que debe responder con un mensaje de "*Server Hello*" o la conexión falla. Los mensajes "*Client Hello*" y "*Server Hello*" se utilizan para establecer capacidades de mejora de seguridad entre el cliente y el servidor.

El mensaje "*Client Hello*" tiene los siguientes parámetros:

- Versión de Protocolo: La versión SSL que el cliente requiere utilizar en la sesión.
- ID de sesión: Es el identificador de la sesión que define el cliente en el primer mensaje "*Client Hello*".
- *Suite* de Cifrado: Contiene las combinaciones de algoritmos de cifrado que el cliente soporta. Cada *suite* de cifrado define el algoritmo de intercambio de claves y especificaciones de cifrado. El servidor elige una *suite* de cifrado, pero en el caso de no encontrar *suites* de cifrados aceptables cerrará la conexión.

- Método de compresión: Incluye una lista de algoritmos de compresión soportados por el cliente, y deberá coincidir con al menos un método soportado por el servidor. El parámetro puede ser "*null*".

El servidor responde con los siguientes parámetros en el mensaje "*Server Hello*":

Versión de Protocolo: La versión de SSL escogida de acuerdo con la soportada por el cliente.

- ID de sesión: Es el identificador de la sesión. Si el ID de sesión enviada por el cliente no es un parámetro vacío, entonces el servidor busca una coincidencia en el caché de sesiones. Si existe una coincidencia, entonces el servidor establece la nueva conexión utilizando el estado de conexión especificado y responde al cliente con el mismo valor de ID de sesión. Este caso indica una sesión reanudada y las partes proceden directamente a los mensajes de Fin.
- *Suite* de Cifrado: La respuesta contiene la *suite* de cifrado que el servidor eligió.
- Método de compresión: El método de compresión seleccionado por el servidor de la lista enviada por el cliente.
- Solicitud de certificado: El servidor envía al cliente una lista de los certificados configurados, y permite al cliente seleccionar el certificado que utilizará para la autenticación.

Inmediatamente después del mensaje "*Server Hello*", el servidor envía su información de su certificado en un mensaje, en donde se encuentra la clave pública. Luego el servidor envía el mensaje "*Server Hello* Done", con lo cual indica el fin de los mensajes de saludo y mensajes asociados. Luego de la recepción del mensaje "*Server Hello* Done", el cliente verifica el certificado provisto por el servidor, y los parámetros del mensaje "*Server Hello*".

Intercambio de claves por parte del Cliente (*Client Key Exchange*)

El contenido del mensaje "*Client Key Exchange*" depende del algoritmo de clave pública seleccionado entre los mensajes "Cliente Hello" y "*Server Hello*". El cliente utiliza el algoritmo RSA (*Rivest-Shamir-Addleman*) o DH para el intercambio de claves y autenticación. Si la autenticación y el intercambio de claves se realiza con RSA, el cliente genera un código de 48 bytes denominado *pre_master_secret*, lo encripta con la clave pública del servidor y lo envía al mismo. El servidor utiliza la

clave privada para descifrar el *pre_master_secret*. Ambos pares de la comunicación luego convierten el *pre_master_key* en la clave secreta (*master_secret*).

Cambio de especificación de Cifrado (*Client Key Exchange*) y Mensajes de terminado (*Finished Messages*)

Los mensajes "*Client Key Exchange*", existen para señalizar transiciones en las estrategias de cifrado. El mensaje es enviado tanto por el cliente como el servidor para poder notificar al receptor que los siguientes récords serán protegidos con las más recientes especificaciones de cifrado y claves negociadas. Inmediatamente después del mensaje "*Client Key Exchange*", el par de la comunicación SSL envía un mensaje "*Finished Message*" para verificar que el intercambio de claves y el proceso de autenticación fue exitoso; este mensaje es el primero que utiliza las especificaciones de cifrado y claves más recientes. El mensaje "*Finished Message*" no necesita un acuse de recibo, el par SSL puede empezar a enviar los datos cifrados inmediatamente después del envío del mensaje "*Finished Message*".

ORDEN DE EMPASTADO