



UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

SERVICIOS DE RED DEL SISTEMA DE ATENCIÓN Y
CAPACITACIÓN MÉDICA ESPECIALIZADA A
DISTANCIA (SACMED)

TESIS

PARA OBTENER EL GRADO DE
INGENIERO EN REDES

PRESENTA

LUIS ROBERTO HERNÁNDEZ GARCÍA

DIRECTOR DE TESIS

M.T.I VLADIMIR VENIAMIN CABAÑAS VICTORIA

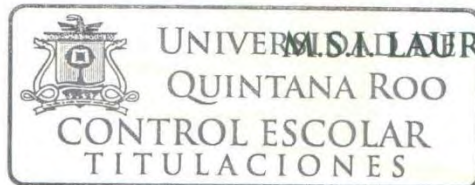
ASESORES

DR. JAIME SILVERIO ORTEGÓN AGUILAR

DR. JAVIER VÁZQUEZ CASTILLO

M.S.I. RUBÉN ENRIQUE GONZÁLEZ ELIXAVIDE

M.S.I. LAURA YÉSSICA DÁVALOS CASTILLA



CHETUMAL, QUINTANA ROO, MÉXICO, JULIO DE 2019



UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

TRABAJO DE TESIS TITULADO

“SERVICIOS DE RED DEL SISTEMA DE ATENCIÓN Y CAPACITACIÓN MÉDICA
ESPECIALIZADA A DISTANCIA (SACMED)”

ELABORADO POR

LUIS ROBERTO HERNÁNDEZ GARCÍA


BAJO SUPERVISIÓN DEL COMITÉ DE ASESORÍA Y APROBADO COMO REQUISITO
PARCIAL PARA OBTENER EL GRADO DE
INGENIERO EN REDES

COMITÉ DE TESIS

DIRECTOR:


M.T.I. VLADIMIR VENIAMIN CABAÑAS VICTORIA

ASESOR:


DR. JAIME SILVERIO ORTEGÓN AGUILAR

ASESOR:

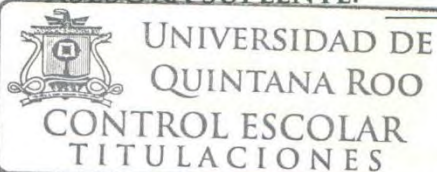

DR. JAVIER VÁZQUEZ CASTILLO

ASESOR SUPLENTE:


M.S.I. RUBÉN ENRIQUE GONZÁLEZ ELXAVIDE

ASESORA SUPLENTE:


M.S.I. LAURA YÉSSICA DÁVALOS CASTILLA



CHETUMAL, QUINTANA ROO, MÉXICO, JULIO DE 2019



Resumen

La presente tesis describe el proceso de implementación de la infraestructura de servicios de red virtualizados para la plataforma de telepresencia del Sistema de Atención y Capacitación Médica Especializada a Distancia (SACMED), el cual consiste en 16 equipos de videoconferencia distribuidos en 7 unidades médicas y 3 unidades administrativas del sector salud del estado de Quintana Roo.

Para llevar a cabo esta implementación fue necesario realizar el diseño de la infraestructura de servicios de red, destinar recurso del entorno VMware vSphere para la creación de servidores virtuales, crear cuentas de usuario en el directorio activo y cuentas de correo electrónico, configurar DNS interno/externo y generar certificados locales.

Una vez desplegada la plataforma de servicio de videoconferencias, se procede a realizar la configuración y aprovisionamiento de los endpoints así como las pruebas de comunicación de audio y video bidireccional.

Posteriormente, se realiza la distribución física a las unidades médicas que pertenecen al SACMED.

Logrando dar servicios de especialidad en zonas rurales, de esa manera no se encarece la prestación de los mismos al tener que hacer una referencia al paciente hacia otra unidad, por lo general, en el área urbana. También se pone en marcha la capacitación constante al personal de las unidades.

Cumpliendo así, que el Sistema de Atención y Capacitación Médica Especializada a Distancia (SACMED) permita brindar atención médica de especialidad y capacitación a hospitales comunitarios y clínicas rurales de la entidad, a través de Tecnologías de Información y Comunicación para optimizar los recursos humanos y materiales del sector y disminuir los costos que actualmente tiene la atención de especialidades para la población quintanarroense.

Agradecimientos

Agradezco a la vida por darme la experiencia necesaria.

Dedicatoria

A mis padres... por fin lo logré-

Contenido

| | |
|---|-------------|
| Resumen | ii |
| Agradecimientos | iii |
| Dedicatoria..... | iv |
| Lista de ilustraciones..... | vii |
| Lista de Tablas | viii |
| Capítulo 1 | 1 |
| 1.1 Introducción..... | 1 |
| 1.2 Planteamiento del problema | 1 |
| 1.3 Objetivo general..... | 2 |
| 1.4 Objetivos específicos | 2 |
| 1.5 Alcance | 3 |
| Capítulo 2 Marco teórico..... | 4 |
| 2.1 Virtualización | 4 |
| 2.1.1 Tipos de virtualización | 4 |
| Virtualización de servidores..... | 4 |
| Virtualización de redes | 5 |
| Virtualización de escritorios..... | 5 |
| Diferencias entre la virtualización y el cómputo en la nube | 5 |
| 2.1.2 Tipos de hipervisores..... | 6 |
| Hipervisor nativo | 6 |
| Hipervisor hospedado..... | 7 |
| 2.1.3 VMware vsphere | 8 |
| 2.1.4 Hyper-V | 8 |
| 2.1.4 Citrix Hipervisor..... | 9 |
| 2.2 Servicios de directorio | 9 |
| 2.2.1 Conceptos básicos | 9 |
| 2.2.1.1 Dominio | 9 |
| 2.2.1.2 Controlador de dominio | 10 |

| | |
|---|-----------|
| 2.2.1.3 Cuenta de usuario | 10 |
| 2.2.1.4 Dominio de directorio activo, árboles y bosques | 10 |
| 2.2.1.5 Gestión TCP/IP | 11 |
| 2.2.2 Active Directory | 12 |
| 2.2.3 OpenLDAP | 12 |
| 2.2.4 Apacheds | 12 |
| 2.3 DNS..... | 13 |
| 2.3.1 Canonical Name (Cname) Records | 13 |
| 2.3.2 Record A (Host Address) | 13 |
| 2.3.3 Srv (Service Location) | 14 |
| 2.3.4 Aaaa (Ipv6 Host Address)..... | 14 |
| 2.3.5 Ns (Name Server) | 14 |
| 2.4 Certificados de seguridad..... | 14 |
| Capítulo 3 Desarrollo | 16 |
| Introducción | 16 |
| 3.1 Análisis de los requerimientos de la plataforma de telepresencia | 16 |
| 3.1.1 Máquinas virtuales | 16 |
| 3.1.2 Servicios De Directorio Y DNS | 17 |
| 3.1.3 Certificados De Seguridad..... | 19 |
| 3.1.4 Cuentas de usuario de dominio y correo..... | 19 |
| 3.2 Diseño Lógico | 20 |
| 3.3 Diseño Físico | 22 |
| 3.4 Aprovisionamiento de endpoint..... | 30 |
| 3.5 Pruebas de comunicación | 43 |
| 3.6 Implementación | 45 |
| 3.6 Monitoreo..... | 46 |
| Capítulo 4 Resultados y Conclusiones | 49 |
| 4.1 Resultados | 49 |
| 4.2 Conclusiones | 51 |
| Bibliografía..... | 52 |

Lista de ilustraciones

| | |
|--|----|
| Ilustración 1.- Hipervisor nativo | 6 |
| Ilustración 2.- Hipervisor hospedado | 7 |
| Ilustración 3 Diseño Lógico de la Red de Datos SACMED | 21 |
| Ilustración 4.- Diseño Físico SACMED | 23 |
| Ilustración 5.- Panel Frontal RealPresence® Collaboration Server (RMX®) 1800 | 23 |
| Ilustración 6.- Panel Posterior RealPresence® Collaboration Server (RMX®) 1800 | 24 |
| Ilustración 7.- RealPresence Group 310 | 25 |
| Ilustración 8.- Panel Posterior RealPresence Group 310 | 26 |
| Ilustración 9.- RealPresence Group 700 | 27 |
| Ilustración 10.- Panel Posterior RealPresence Group 700 | 28 |
| Ilustración 11.- Real Presence Resource Manager (RPRM) | 30 |
| Ilustración 12. - Dashboard Real Presence Resource Manager (RPRM) | 31 |
| Ilustración 13.- Sitos | 31 |
| Ilustración 14.- Seleccionando site de Endpoints | 32 |
| Ilustración 15.- Ventana Edit Site | 32 |
| Ilustración 16.- Agregando red/subred | 33 |
| Ilustración 17.- Ventana Add Subnet | 33 |
| Ilustración 18.- Equipo conectado y encendido | 34 |
| Ilustración 19.- Pantalla inicial de configuración | 35 |
| Ilustración 20.- Accediendo a la dirección IP | 36 |
| Ilustración 21.- Pantalla de inicio de sesión | 36 |
| Ilustración 22.- Selección de idioma | 37 |
| Ilustración 23.- Acuerdo de licencia de usuario final | 37 |
| Ilustración 24.- Método de configuración del equipo. | 38 |
| Ilustración 25. Configurando servidor de aprovisionamiento. Status Pending | 38 |
| Ilustración 26.- Configurando servidor de aprovisionamiento. Status Registered | 39 |
| Ilustración 27.- Asignando nombre al equipo | 40 |
| Ilustración 28.- Mensaje de confirmación de aprovisionamiento | 40 |
| Ilustración 29.- Pantalla de administración del endpoint | 41 |
| Ilustración 30.- Campo de búsqueda | 41 |
| Ilustración 31.- System Status | 42 |
| Ilustración 32.- Escenario de pruebas | 43 |

| | |
|--|----|
| Ilustración 33.- Transmisión de audio y video del equipo 2 al equipo1 | 44 |
| Ilustración 34.- Transmisión de audio y video del equipo 1 al equipo 2 | 44 |
| Ilustración 35.- Real Presence Resource Manager (RPRM) | 46 |
| Ilustración 36. - Dashboard Real Presence Resource Manager (RPRM)..... | 47 |
| Ilustración 37.- Monitor View | 47 |

Lista de Tablas

| | |
|---|----|
| Tabla 1.- Unidades hospitalarias que integran la primera fase del SACMED..... | 3 |
| Tabla 2.- Requerimientos para las máquinas virtuales | 16 |
| Tabla 3.- Dominio Interno, Dominio Externo Y Dominio De Correo..... | 17 |
| Tabla 4.- Registros Dns Internos | 18 |
| Tabla 5.- Registros DNS Externos | 18 |
| Tabla 6.- Requerimiento De Certificados | 19 |
| Tabla 7.- Usuarios de dominio y correo para endpoints..... | 20 |
| Tabla 8.- Descripción Panel Frontal RealPresence® Collaboration Server (RMX®) 1800 | 24 |
| Tabla 9.- Descripción Panel Posterior RealPresence® Collaboration Server (RMX®) 1800..... | 25 |
| Tabla 10.- Unidades de Telemedicina | 49 |
| Tabla 11.- Unidades de Teleeducación | 50 |

Capítulo 1

1.1 Introducción

La atención médica basada en el uso de tecnologías de la información y comunicación (conocida como Telesalud) contribuye para hacer accesibles los servicios de salud de especialidad a la población alejada geográficamente. Como instrumento de equidad, logra brindar servicios médicos de calidad, independientemente de la ubicación física, tanto de los que ofrecen el servicio, como de los pacientes que lo reciben; beneficia la población más vulnerable, con menores recursos y que vive en condiciones de pobreza. La Telesalud brinda la oportunidad de usar una herramienta tecnológica por algún medio electrónico, para el intercambio de imágenes, voz, datos y video; permite el diagnóstico y opinión de especialistas en casos clínicos; da acceso a la infraestructura y equipos tecnológicos de apoyo a la consulta médica, como por ejemplo los estudios de gabinete; optimiza el costo-beneficio de estas inversiones y alienta con esto para que se siga invirtiendo aún más. En conclusión, la Telesalud permite una igualdad en el acceso a los servicios de salud, disminuye costos y evita traslado de pacientes.

1.2 Planteamiento del problema

En el estado de Quintana Roo existen carencias de servicios de especialidad en el área rural, lo cual encarece la prestación de los mismos al tener que trasladar al paciente hasta una unidad de mayor resolución, ubicada por lo general en el área urbana. Con el fin de evitar las pérdidas económicas concernientes a transporte, alojamiento y costos de la atención médica, se realizó el proyecto SACMED.

El proyecto “Diseño, implementación y puesta en marcha de un Sistema de Atención y Capacitación Médica Especializada a Distancia (SACMED), para ampliar la cobertura y aumentar la calidad de los servicios de salud en comunidades marginadas de Quintana Roo”, tiene como principal objetivo mejorar la oportunidad en la Atención Médica y en las actividades de educación en los Servicios Estatales de Salud de Quintana Roo, por medio de las Tecnologías de la Información y Comunicaciones que permitan disminuir la desigualdad de oportunidad a los servicios en la población Quintanarroense.

Con el fin de acercar los servicios médicos a las comunidades menos favorecidas y más alejadas del área urbana se ha desarrollado el concepto de Telesalud, debido a la amplia gama de actividades que se incluyen con el fin de mejorar las condiciones de salud de la población, atender las urgencias sanitarias y optimizar los recursos humanos y financieros, poniendo un mayor énfasis en la prevención de enfermedades.

La Telesalud es una modalidad de atención médica a distancia, tanto diferida como en tiempo real, que incluye actividades de capacitación para personal del área del cuidado de la salud, la cual requiere soporte de telecomunicaciones con características de fiabilidad y eficiencia.

Este proyecto pretende brindar el soporte de conectividad que requiere el sistema SACMED para llevar a cabo las actividades de atención médica especializada a distancia y de capacitación.

1.3 Objetivo general

Implementar la infraestructura de servicios de red virtualizados para la plataforma de telepresencia del Sistema de Atención y Capacitación Médica Especializada a Distancia (SACMED)

1.4 Objetivos específicos

- i. Diseñar la infraestructura de servicios de red para la plataforma de telepresencia
- ii. Configurar el entorno VMware vSphere en los Servicios Estatales de Salud para la creación de servidores virtuales.
- iii. Configurar el servidor de Máquinas Virtuales VMware vSphere
- iv. Crear cuentas de máquina y usuario en el Directorio Activo.
- v. Generar cuentas de correo electrónico para notificaciones.
- vi. Agregar un subdominio DNS para los equipos Endpoints
- vii. Crear registros DNS de tipo A y SRV.
- viii. Generar certificados digitales locales para los servidores virtuales

1.5 Alcance

Con la implementación de la plataforma de videoconferencias se pretende interconectar los sitios descritos en la tabla número uno, esto con el fin de mejorar la salud de un paciente, permitiendo la comunicación interactiva en tiempo real entre el paciente, y el médico o profesional a distancia.

Tabla 1.- Unidades hospitalarias que integran la primera fase del SACMED.

| SITIO | ÁREA |
|--|---------------------------------|
| Hospital General de Chetumal | Teleconsulta |
| Hospital General de Chetumal | Auditorio |
| Uneme Cisame de Chetumal | Sala de usos múltiples |
| Hospital Integral de José María Morelos | Consultorio |
| Hospital General de Felipe Carrillo Puerto | Consultorio de medicina interna |
| Hospital General de Felipe Carrillo Puerto | Sala de enseñanza |
| Uneme de enfermedades crónicas de Felipe Carrillo Puerto | Sala de usos múltiples |
| Hospital General de Playa del Carmen | Teleconsulta |
| Hospital General de Playa del Carmen | Auditorio |
| Hospital General de Cancún | Teleconsulta |
| Hospital General de Cancún | Auditorio |
| Jurisdicción Sanitaria Número 2 | Sala de enseñanza |
| Hospital Comunitario de Isla Mujeres | Consultorio 1 |
| Hospital Comunitario de Isla Mujeres | Aula de usos múltiples |
| Hospital Integral de Kantunilkín | Consultorio 2 |
| Hospital Integral de Kantunilkín | Aula de prospera |

Capítulo 2 Marco teórico

2.1 Virtualización

La virtualización es el proceso de crear una representación basada en software, o virtual, de algo como, por ejemplo, aplicaciones, servidores, almacenamiento y redes virtuales. Es la forma más eficaz de reducir los gastos de TI y, al mismo tiempo, impulsar la eficiencia y la agilidad para los negocios de todos los tamaños.

La tecnología de virtualización permite operar diversos sistemas operativos en una computadora al mismo tiempo y evita que las aplicaciones interfieran entre sí. Cada máquina virtual es como una máquina dentro de la computadora física y se ejecuta como si estuviera instalada en una plataforma de hardware autónoma. Cada máquina virtual se conoce como sistema operativo huésped o guest y se comunican con el hardware a través de un programa llamado hipervisor. El hipervisor es el que se encarga de virtualizar el hardware para cada máquina virtual hospedada en la máquina anfitriona o host.

2.1.1 Tipos de virtualización

Virtualización de servidores

La virtualización de servidores permite ejecutar múltiples sistemas operativos como máquinas virtuales de gran eficiencia en un único servidor físico. Entre las ventajas clave, se incluyen las siguientes:

- Aumento de la eficiencia de TI.
- Reducción de gastos operacionales.

- Implementación de cargas de trabajo más rápida
- Aumento del rendimiento de las aplicaciones
- Mayor disponibilidad del servidor
- Eliminación de la complejidad y la expansión de servidores

Virtualización de redes

Mediante la reproducción total de una red física, la virtualización de redes permite ejecutar aplicaciones en una red virtual de la misma forma que si se estuvieran ejecutando en una red física, pero con más ventajas operacionales y con toda la independencia del hardware que brinda la virtualización. La virtualización de redes brinda dispositivos y servicios de red lógicos a las cargas de trabajo conectadas.

Virtualización de escritorios

La implementación de escritorios como un servicio administrado les permite a las organizaciones de TI responder con mayor rapidez a las necesidades cambiantes del espacio de trabajo y las nuevas oportunidades. Las aplicaciones y los escritorios virtualizados también se pueden suministrar de manera rápida y sencilla a las sucursales, a los empleados en el extranjero y tercerizados, y a los empleados móviles mediante el uso de tabletas iPad y Android.

Diferencias entre la virtualización y el cómputo en la nube

Si bien ambas son tecnologías que generan muchas expectativas, la virtualización y la computación en nube no son equivalentes. La virtualización es software que genera entornos de procesamiento independientes de la infraestructura física, mientras que la computación en nube es un servicio que suministra recursos de computación compartidos (software o datos) según demanda por medio de Internet. Al tratarse de soluciones complementarias, las organizaciones pueden comenzar por

virtualizar sus servidores y luego avanzar hacia la computación en nube para obtener aún más agilidad y capacidad de autoservicio.

2.1.2 Tipos de hipervisores

Existen distintos tipos de hipervisores, pero hay una clasificación sencilla donde se separan en dos grandes categorías, nativos y hospedados.

Hipervisor nativo

Los hipervisores nativos son sistemas de software que corren directamente en el hardware del anfitrión “host” para controlar el hardware y para monitorear los sistemas operativos de los huéspedes o “guest”. En consecuencia, el sistema operativo de la máquina huésped se ejecuta en una capa separada superior a la del hipervisor.

Ejemplos de estos hipervisores son:

Oracle VM, Microsoft Hyper-V, VMware y XEN.



Ilustración 1.- Hipervisor nativo

Hipervisor hospedado

Los hipervisores hospedados están diseñados para ejecutarse dentro de un sistema operativo tradicional. En otras palabras, el hipervisor hospedado agrega distintas capas de software sobre el sistema operativo anfitrión y de esta manera el sistema operativo hospedado se vuelve una tercera capa de software sobre el hardware.

Los siguientes son ejemplos de hipervisores hospedados:

Oracle VM Virtual Box, VMware server, VMware Workstation, Microsoft Virtual PC, KVM, QEMU y Parallels



Ilustración 2.- Hipervisor hospedado

2.1.3 VMware vsphere

VMware vSphere es la plataforma de virtualización líder del sector para construir infraestructuras de cloud. Permite a los usuarios ejecutar aplicaciones críticas para el negocio con confianza y responder con mayor rapidez a las necesidades empresariales.

vSphere ofrece una base segura, flexible y potente para la agilidad del negocio que permite acelerar la transformación digital hacia la nube híbrida y el éxito en la economía digital. Con vSphere, puede brindar compatibilidad con cargas de trabajo y casos de uso nuevos y, al mismo tiempo, se adapta a la complejidad y las necesidades crecientes de su infraestructura. vSphere es la base de un centro de datos definido por software (Software-Defined Data Center, SDDC) seguro, lo que permite proteger los datos, las aplicaciones, la infraestructura y el acceso. Las capacidades de seguridad avanzadas completamente integradas en el hipervisor y con tecnología de aprendizaje automático proporcionan mejor visibilidad, mayor protección y tiempo de respuesta más rápido para las incidencias de seguridad.

vSphere le permite ejecutar, administrar, conectar y proteger sus aplicaciones en un entorno operativo común en la nube híbrida.

2.1.4 Hyper-V

Hyper-V provee una plataforma de virtualización simple y confiable que permite mejorar la utilización de los servidores al tiempo que se reducen costos. Cada máquina virtual es un equipo virtualizado y aislado que puede ejecutar su propio sistema operativo. Hyper-V proporciona todas las funcionalidades de plataforma necesarias para permitir que los clientes empresariales creen nubes privadas e implanten un modelo operativo de servicio.

2.1.4 Citrix Hypervisor

Citrix Hypervisor es una plataforma de virtualización de servidores completa con funciones de clase empresarial incorporadas para tratar fácilmente distintos tipos de carga de trabajo, sistemas operativos mezclados y almacenamiento en configuraciones de red. Para los casos prácticos de virtualización de escritorios y aplicaciones más exigentes, su escalabilidad y rendimiento líder del sector bajo carga, pueden afrontar las implementaciones de Citrix Virtual Apps and Desktops más grandes. TI recibe el beneficio de funciones únicas de Citrix Hypervisor, como gráficos virtualizados mejorados con NVIDIA e Intel, y una seguridad de carga de trabajo mejorada con APIs de Direct Inspect, lo que reducirá los costos y complejidad de la infraestructura virtual.

2.2 Servicios de directorio

Los directorios de dominio nos permiten administrar los objetos de la red y sus relaciones. En ellos administramos usuarios, servidores o máquinas de escritorio, guardamos sus informaciones personales y de oficina, les otorgamos permisos, los agrupamos y les damos seguridad. El sistema más utilizado en la actualidad es Active Directory (directorio activo de Microsoft). Pero también hay otros como Open Directory o ApacheDS.

2.2.1 Conceptos básicos

2.2.1.1 Dominio

Un dominio es una agrupación lógica de objetos que permite la administración central y el control sobre la replicación de esos objetos. Cada organización tiene al menos un dominio, que se implementa cuando se instala el directorio activo en el primer controlador de dominio.

2.2.1.2 Controlador de dominio

Los controladores de dominio de directorio activo son quizás el tipo más importante de servidor de red en una red de Windows. Los controladores de dominio también son uno de los servidores más utilizados en una red de Windows, por lo que es importante evaluar de manera realista los requisitos operativos y el rendimiento del servidor para cada uno.

2.2.1.3 Cuenta de usuario

En Windows Server 2008, puede tener una cuenta de usuario local. En un controlador de dominio, los usuarios y grupos locales están deshabilitados. En el directorio activo, la cuenta de usuario del dominio contiene el nombre de usuario, la contraseña, los grupos de los que el usuario es miembro y otra información descriptiva, como direcciones y números de teléfono, así como muchas otras descripciones y atributos de los usuarios, como seguridad y acceso remoto. Configuraciones de control.

2.2.1.4 Dominio de directorio activo, árboles y bosques

Dentro del directorio, los objetos se organizan mediante una estructura de árbol jerárquica denominada árbol de directorios. La estructura de la jerarquía se deriva del esquema y se utiliza para definir las relaciones padre-hijo de los objetos almacenados en el directorio.

Una agrupación lógica de objetos que permite la administración central de esos objetos se denomina dominio. En el árbol de directorios, un dominio se representa como un objeto. De hecho, es el objeto principal de todos los objetos que contiene. A diferencia de Windows NT 4.0, que limita el número de objetos que puede almacenar en un dominio, un dominio de Active Directory puede contener millones de objetos. Debido a esto, es probable que no necesite crear dominios de recursos y usuarios

separados, como se hizo comúnmente con Windows NT 4.0. En su lugar, puede crear un único dominio que contenga todos los recursos que desea administrar de forma centralizada.

Los dominios son solo uno de los varios bloques de construcción para implementar estructuras de Active Directory. Otros bloques de construcción incluyen los siguientes:

- Árboles de Active Directory, que son agrupaciones lógicas de dominios.
- Los bosques de Active Directory, que son agrupaciones lógicas de árboles de dominio.

Como se describió anteriormente, se utiliza un árbol de directorios para representar una jerarquía de objetos, mostrando las relaciones padre-hijo entre esos objetos. Por lo tanto, cuando hablamos de un árbol de dominios, observamos la relación entre los dominios principal y secundario. El dominio en la parte superior del árbol del dominio se conoce como el dominio raíz (piense en esto como un árbol al revés). Más específicamente, el dominio raíz es el primer dominio creado en un nuevo árbol dentro de Active Directory. Cuando se habla de bosques y dominios, se hace una distinción importante entre el primer dominio creado en un nuevo bosque, un dominio raíz del bosque, y el primer dominio creado en cada árbol adicional dentro de un bosque, un dominio raíz.

2.2.1.5 Gestión TCP/IP

Como administrador, permite que las computadoras en red se comuniquen utilizando los protocolos de red básicos integrados en Windows Server 2008. El protocolo clave que usará es el Protocolo de control de transmisión/Protocolo de Internet (TCP/IP). TCP/IP es en realidad una colección de protocolos y servicios utilizados para comunicarse a través de una red. Es el protocolo principal utilizado para las comunicaciones entre redes. En comparación con la configuración de otros protocolos de red, la configuración de las comunicaciones TCP/IP es bastante complicada, pero TCP/IP es el protocolo más versátil disponible.

2.2.2 Active Directory

Active Directory es un directorio extensible que le permite administrar los recursos de la red de manera eficiente. Un servicio de directorio hace esto almacenando información detallada sobre cada recurso de la red, lo que facilita la búsqueda y autenticación básicas. El hecho de poder almacenar grandes cantidades de información es un objetivo clave de un servicio de directorio, pero la información también debe estar organizada para que se pueda buscar y recuperar fácilmente.

2.2.3 OpenLDAP

OpenLDAP es una implementación de código abierto de Lightweight Directory Access Protocol. LDAP, es un protocolo para consultar y modificar un servicio de directorio basado en X.500 que se ejecuta sobre TCP / IP. La versión actual de LDAP es LDAPv3, como se define en RFC4510, y la implementación en Ubuntu es OpenLDAP.

El paquete de software OpenLDAP incluye un servidor independiente en SLAPD, varios clientes LDAP y una biblioteca de clientes LDAP que se utiliza para proporcionar acceso programático al protocolo LDAP. Se proporcionan APIs tanto síncronas como asíncronas. También se incluyen varias rutinas para analizar los resultados devueltos de estas mismas.

2.2.4 Apacheds

ApacheDS es un servidor de directorio extensible e integrable completamente escrito en Java, que ha sido certificado como compatible con LDAPv3 por Open Group. Además de LDAP, admite Kerberos 5 y el protocolo de cambio de contraseña. Ha sido diseñado para introducir desencadenantes, procedimientos almacenados, colas y vistas en el mundo de LDAP.

2.3 DNS

DNS es un servicio de resolución de nombres de host que puede utilizar para determinar la dirección IP de una computadora a partir de su nombre de host. Esto permite a los usuarios trabajar con nombres de host, como `http://www.msn.com` o `http://www.microsoft.com`, en lugar de una dirección IP, como `192.168.5.102` o `192.168.12.68`. DNS es el servicio de nombres principal para Windows Server 2008 e Internet.

Al igual que con las puertas de enlace, la mejor manera de configurar DNS depende de la configuración de su red. Si las computadoras usan DHCP, probablemente querrá configurar el DNS a través de la configuración en el servidor DHCP. Si las computadoras utilizan direcciones IP estáticas o si desea configurar DNS específicamente para un usuario o sistema individual, querrá configurar DNS manualmente.

2.3.1 Canonical Name (Cname) Records

Los registros de nombre canónico (CNAME) crean alias para los nombres de host. Esto permite que un host sea referenciado por varios nombres en DNS. El uso más común es cuando un host proporciona un servicio común, como el servicio World Wide Web (WWW) o File Transfer Protocol (FTP), y desea que tenga un nombre descriptivo en lugar de un nombre complejo. Por ejemplo, es posible que desee que `www.cpandl.com` sea un alias para el host `dc06.cpandl.com`.

2.3.2 Record A (Host Address)

Contiene el nombre de un host y su versión de Protocolo de Internet Dirección 4 (IPv4). Cualquier computadora que tenga red múltiple, interfaces o direcciones IP deben tener múltiples registros de dirección.

2.3.3 Srv (Service Location)

Permite encontrar un servidor que proporcione un Servicio. Active Directory utiliza registros SRV para localizar el dominio controladores, servidores de catálogo global, Lightweight Directory. Los servidores de Protocolo de acceso (LDAP) y los servidores Kerberos. SRV Los registros se crean automáticamente. Por ejemplo, Active Directory crea un registro SRV cuando configura un controlador de dominio como un catálogo global. Los servidores LDAP pueden agregar un SRV para indicar que están disponibles para manejar solicitudes LDAP en una zona particular.

2.3.4 Aaaa (Ipv6 Host Address)

Contiene el nombre de un host y su versión 6 de protocolo de internet (IPv6).

2.3.5 Ns (Name Server)

Proporciona una lista de servidores autorizados para un dominio, que permite búsquedas de DNS dentro de varias zonas. Cada nombre de dominio primario como secundario debe ser declarado a través de este disco.

2.4 Certificados de seguridad

Los certificados de seguridad son una medida de confianza adicional para las personas que visitan y hacen transacciones en su página web, le permite cifrar los datos entre el ordenador del cliente y el servidor que representa a la página. El significado más preciso de un certificado de seguridad es que con él logramos que los datos personales sean encriptados y así imposibilitar que sean interceptados

por otro usuario. Ahora es muy común ver en nuestros exploradores el protocolo de seguridad https; mediante éste, básicamente nos dice que la información que se envía a través de internet, entre el navegador del cliente y el servidor donde está alojada la página, se cifra de forma que es casi imposible que otra persona reciba, vea o modifique los datos confidenciales del cliente. Las ventajas de este sistema son visibles fácilmente, puesto que es más sencillo medir el nivel de confianza de un sitio web.

Los sitios web que cuentan con certificados de seguridad nos permiten saber quién es el dueño del mismo, saber a qué dominio pertenece, la procedencia real del responsable del sitio, la validez del certificado, así como su fecha de caducidad, y sobre todo, la empresa que ha emitido el certificado. Podemos decir que los sitios web que consideran necesario un certificado de seguridad logran garantizar mayor seguridad a los usuarios.

Tiene que elegir el certificado de seguridad más completo y así estar resguardando la seguridad del cliente, es lo más importante en la empresa. Para identificar fácilmente que navegamos en una página web segura, en nuestro explorador de internet se muestra un icono de candado, indicando que la transferencia de datos entre su computadora y el servidor no puede ser interceptado por nadie.

Capítulo 3 Desarrollo

Introducción

En este capítulo se presentaran los requerimientos para la plataforma Polycom, así como el diseño lógico y físico. Se mostrará el procedimiento para aprovisionar un equipo de videoconferencia y tener acceso a la plataforma para poder establecer videoconferencias. Con las pruebas realizadas y comunicación existente procedemos a configurar cada endpoint correspondiente a las unidades.

Posteriormente se realiza la distribución de los equipos, cabe mencionar que debemos tener lista la red VPN para cada unidad y tener un buen enlace de comunicación, la cual deberá ser proveída por el área de telecomunicaciones.

3.1 Análisis de los requerimientos de la plataforma de telepresencia

3.1.1 Máquinas virtuales

En la tabla número 2 se describe los requerimientos de HDD, memoria RAM y procesamiento necesario para cada servidor.

| SERVIDORES | REQUERIMIENTOS | | | |
|---------------------------------------|----------------|-----------|----------|----------|
| | CORES | CPU (MHz) | RAM (GB) | HDD (GB) |
| Distributed Media Application (DMA) | 8 | 6,000 | 16 | 146 |
| Real Presence Resource Manager (RPRM) | 8 | 8,000 | 16 | 160 |
| Web Suite Web Services Portal (WSP) | 8 | 20,000 | 16 | 100 |
| Web Suite Experience (MEA) | 8 | 20,000 | 16 | 100 |
| WebSuite Enhanced Content (ECS) | 4 | 10,000 | 8 | 100 |
| RP Access Director (RPAD) | 4 | 3,500 | 8 | 146 |

Tabla 2.- Requerimientos para las máquinas virtuales

3.1.2 Servicios De Directorio Y DNS

La tabla número 3 describe los requerimientos de directorio activo, tales como dominio interno, dominio externo, registros DNS de tipo A, SRV, CNAME tanto internos como externos, dominio de correo y FQDN

| Información del Sistema de Nombres de Dominio (DNS) | |
|---|-----------------|
| Internal DNS Domain: | dominio.local |
| External DNS Domain: | dominio.externo |
| Email Domain: | correo.com |

Tabla 3.- Dominio Interno, Dominio Externo Y Dominio De Correo

| Internal DNS Records | | | |
|------------------------------|-------------------------|-------------|----------------------------|
| Polycom Platform | IP Address ¹ | Record Type | FQDN |
| Resource Manager 1 | X.X.X.X | A Record | SRV-RPRM.dominio.local |
| DMA 1 | X.X.X.X | A Record | SRV-DMA.dominio.local |
| RPAD 1 management | X.X.X.X | A Record | SRV-RPAD.dominio.local |
| WebSuite WSP (scheduling) | X.X.X.X | A Record | SRV-WSP.dominio.local |
| WebSuite MEA (experience) | X.X.X.X | A Record | SRV-MEA.dominio.local |
| WebSuite WSP (scheduling) | X.X.X.X | A Record | schedule.dominio.local |
| WebSuite MEA (experience) | X.X.X.X | A Record | meetme.dominio.local |
| WebSuite Enhanced Content | X.X.X.X | A Record | SRV-ECS.dominio.local |
| RPCS 1 management | X.X.X.X | A Record | SRV-RPCS.dominio.local |
| RPCS1 media and signaling | X.X.X.X | A Record | SRV-RPCS-sig.dominio.local |
| Polycom Platform | Port ² | Record Type | FQDN single instance |
| _h323cs._tcp.dominio.externo | XXXX | SRV Record | SRV-DMA.dominio.local |
| _h323ls._udp.dominio.externo | XXXX | SRV Record | SRV-DMA.dominio.local |
| _sip._tcp. | XXXX | SRV Record | SRV-DMA.dominio.local |
| _sips._tcp. | XXXX | SRV Record | SRV-DMA.dominio.local |
| _sip._udp. | XXXX | SRV Record | SRV-DMA.dominio.local |
| _sip._tls. | XXXX | SRV Record | SRV-DMA.dominio.local |
| _cmaconfig._tcp.correo.com | XXXX | SRV Record | SRV-RPRM.dominio.local |

¹ Se omiten las direcciones IP

² Se omiten los puertos

| Recommended CNAME Records | | Record Type | FQDN single instance |
|---------------------------|---------------------------|-------------|------------------------|
| DMA | gk.dominio.externo | Cname | SRV-DMA.dominio.local |
| DMA | registrar.dominio.externo | Cname | SRV-DMA.dominio.local |
| DMA | video.dominio.externo | Cname | SRV-DMA.dominio.local |
| RPRM | dir.dominio.externo | Cname | SRV-RPRM.dominio.local |
| RPRM | prov.dominio.externo | Cname | SRV-RPRM.dominio.local |
| WSP | schedule.dominio.externo | Cname | SRV-WSP.dominio.local |
| MEA | meetme.dominio.externo | Cname | SRV-MEA.dominio.local |

Tabla 4.- Registros Dns Internos

| External DNS Records - Single RPAD | | | |
|------------------------------------|-------------------------|-------------|--------------------------|
| Polycom Platform | IP Address ³ | Record Type | FQDN |
| RPAD (firewall traversal) | X.X.X.X | A Record | video.dominio.externo |
| WebSuite WSP (scheduling) | X.X.X.X | A Record | schedule.dominio.externo |
| WebSuite MEA (experience) | X.X.X.X | A Record | meetme.dominio.externo |
| Polycom Platform | Port ⁴ | Record Type | FQDN |
| _h323cs._tcp.dominio.externo | XXXX | SRV Record | video.dominio.externo |
| _h323ls._udp.dominio.externo | XXXX | SRV Record | video.dominio.externo |
| _sip._tcp. | XXXX | SRV Record | video.dominio.externo |
| _sips._tcp. | XXXX | SRV Record | video.dominio.externo |
| _sip._udp. | XXXX | SRV Record | video.dominio.externo |
| _sip._tls. | XXXX | SRV Record | video.dominio.externo |
| _cmaconfig._tcp.correo.com | XXXX | SRV Record | video.dominio.externo |

Tabla 5.- Registros DNS Externos

En el caso de que el dominio interno y el dominio externo no sean el mismo, se procede a crear un subdominio para poder crear los registros CNAME correctamente.

³ Se omiten las direcciones IP

⁴ Se omiten puertos

3.1.3 Certificados De Seguridad

La siguiente tabla número 6 Describe los requerimientos para certificados de seguridad tanto internos como públicos tipo SANS

| REQUERIMIENTOS DE CERTIFICADOS | | | | |
|--------------------------------|----------------------------|----------|----------------|---|
| SERVIDOR | FQDN | TIPO CA | SANS REQUERIDO | SANS |
| RPRM 1 | SRV-RPRM.dominio.local | Internal | No | |
| DMA 1 | SRV-DMA.dominio.local | Internal | Yes | SRV-DMA.dominio.local video.dominio.externo |
| RPCS 1 | SRV-RPCS-sig.dominio.local | Internal | No | |
| WSP | SRV-WSP.dominio.local | Internal | No | |
| MEA | SRV-MEA.dominio.local | Internal | No | |
| RPAD 1 | SRV-RPAD.dominio.local | Public | Yes | video.dominio.externo schedule.dominio.externo meetme.dominio.externo |

Tabla 6.- Requerimiento De Certificados

3.1.4 Cuentas de usuario de dominio y correo.

Para el aprovisionamiento correcto de los endpoints, procedimiento que se describe más adelante en este documento, se requiere crear cuentas de usuario de dominio y correo para cada equipo de videoconferencia de acuerdo a los sitios descritos en la tabla 1 al inicio de este documento.

Las cuentas requeridas se describen en la siguiente tabla.

| SITIO | AREA | USUARIO |
|--|---------------------------------|---------------------|
| Hospital General de Chetumal | Teleconsulta | teleconsulta.hgch |
| Hospital General de Chetumal | Auditorio | teleeducacion.hgch |
| Uneme Cisame de Chetumal | Sala de usos múltiples | teleeducacion.sesa |
| Hospital Integral de José María Morelos | Consultorio | teleconsulta.hijmm |
| Hospital General de Felipe Carrillo Puerto | Consultorio de medicina interna | teleconsulta.hgfcp |
| Hospital General de Felipe Carrillo Puerto | Sala de enseñanza | teleeducacion.hgfcp |
| Uneme Felipe Carrillo Puerto | Sala de usos múltiples | teleeducacion.js3 |
| Hospital General de Playa del Carmen | Teleconsulta | teleconsulta.hgpc |
| Hospital General de Playa del Carmen | Auditorio | teleeducacion.hgpc |
| Hospital General de Cancún | Teleconsulta | teleconsulta.hgcan |
| Hospital General de Cancún | Auditorio | teleeducacion.hgcan |
| Jurisdicción Sanitaria Número 2 | Sala de enseñanza | teleeducacion.js2 |
| Hospital Comunitario de Isla Mujeres | Consultorio 1 | teleconsulta.hcim |
| Hospital Comunitario de Isla Mujeres | Aula de usos múltiples | teleeducacion.hcim |
| Hospital Integral de Kantunilkín | Consultorio 2 | teleconsulta.hikan |
| Hospital Integral de Kantunilkín | Aula de prospera | teleeducacion.hikan |

Tabla 7.- Usuarios de dominio y correo para endpoints.

Debido a que el servicio de Exchange está ligado al domino, las cuentas de correo son las mismas para cada endpoint.

3.2 Diseño Lógico

En la ilustración número 3 podemos observar el diseño lógico del Sistema de Atención y Capacitación Médica Especializada a Distancia (SACMED), el cual consiste en seis máquinas virtuales y un servidor físico, las primeras mencionadas deberán estar almacenadas en un servidor NAS con almacenamiento VMFS (Virtual Machine File System) y distribuidas entre los host de VMware VSphere, los cuales se encargan de proveer procesamiento y memoria RAM. Se muestra también los dispositivos de videoconferencia.

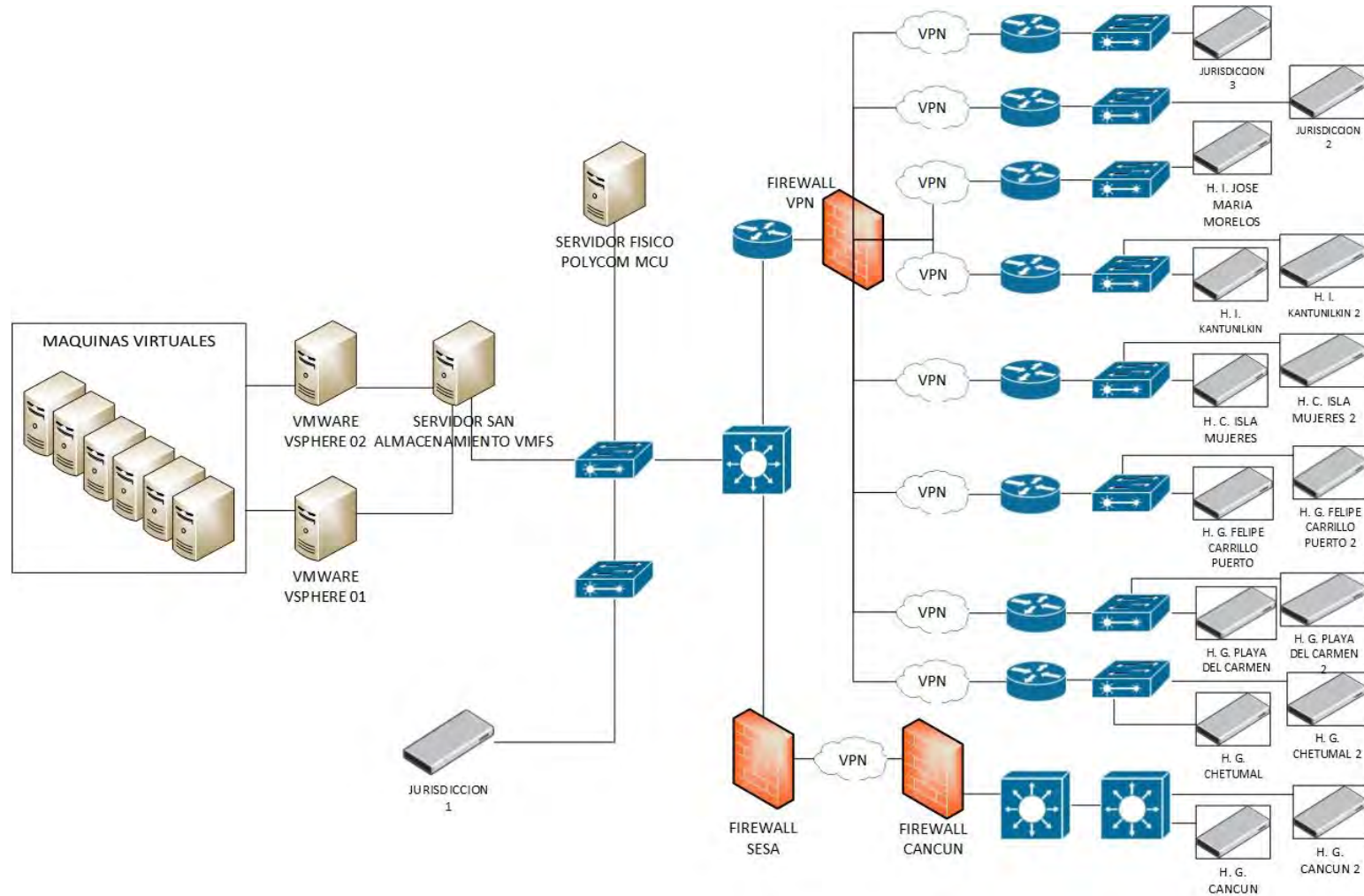


Ilustración 3 Diseño Lógico de la Red de Datos SACMED

3.3 Diseño Físico

A continuación, se describe la infraestructura en el cual fue implementado el presente proyecto.

El hardware para realizar la instalación de las maquina virtuales fue el siguiente:

- 2 Servidores UCS C220 M3 2 Procesadores 2.2GHZ E5-2660 16GB RAM
- 1 SAN IBM Storwize V3700 SFF Dual Control Enclosure 3 Discos de 600GB SAS

Podemos observar la distribución en la ilustración número

Además, tenemos que mencionar el hardware correspondiente a Polycom, los cuales son:

- 1 MCU RealPresence® Collaboration Server (RMX®) 1800.
- 9 RealPresence Group 310.
- 7 RealPresence Group 700.

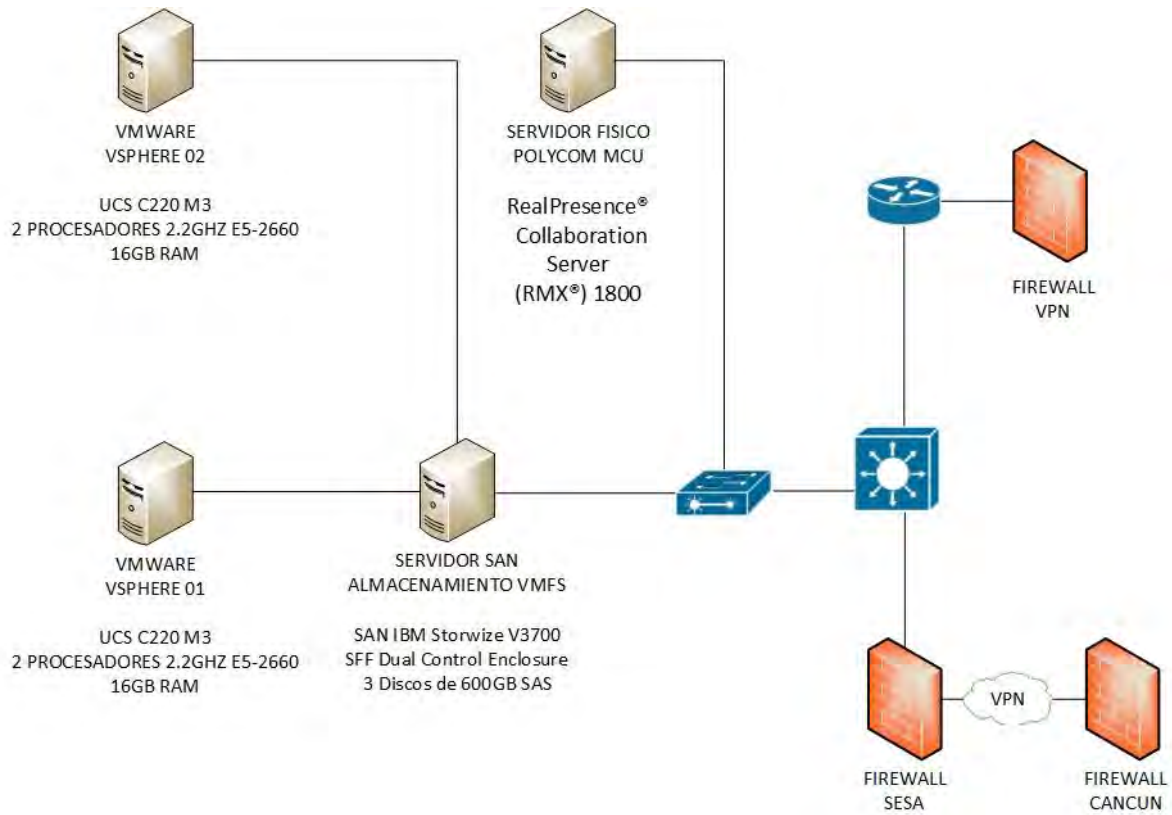


Ilustración 4.- Diseño Físico SACMED

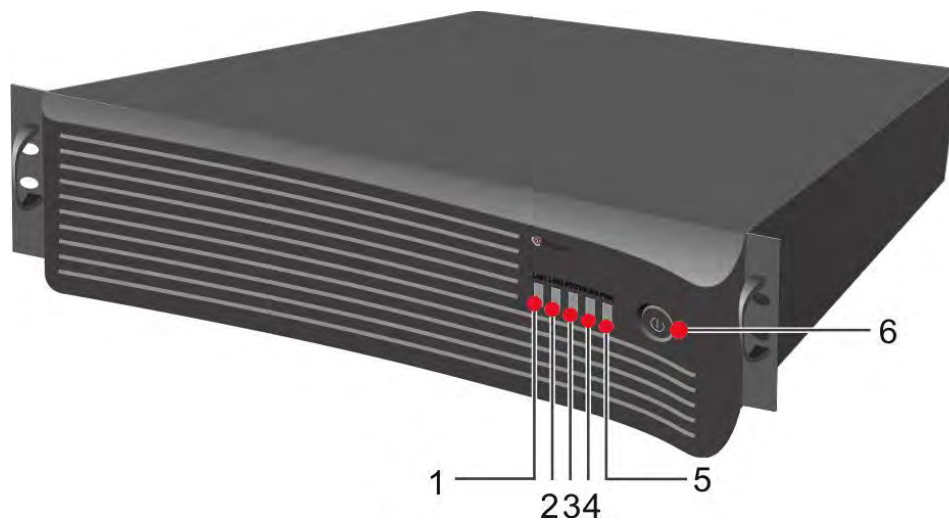


Ilustración 5.- Panel Frontal RealPresence® Collaboration Server (RMX®) 1800

| Nº | Nombre | Descripción |
|----|-------------------------------|---|
| 1 | Indicador de LED de LAN 1 | Apagado: sin conexión de red Verde: red conectada Verde destellante: en uso |
| 2 | Indicador de LED de LAN 2 | Apagado: sin conexión de red Verde: red conectada Verde destellante: en uso |
| 3 | Indicador LED de estado | Rojo: alarmas del sistema Verde: los terminales están conectados a una reunión Verde destellante: no hay alarmas del sistema ni terminales conectados a la reunión Azul destellante: se están realizando pruebas de diagnóstico Azul: las pruebas de diagnóstico se completaron. Retire la llave USB (si corresponde) y reinicie el sistema |
| 4 | Indicador LED de M/S | Azul: actualización del sistema completa, esperando el reinicio Azul destellante: actualización del sistema en progreso Verde: el sistema funciona con normalidad, ya sea en modo único o como MCU maestro en modo de respaldo dinámico Verde destellante: el sistema funciona con normalidad, como MCU esclavo en el modo de respaldo dinámico. |
| 5 | Indicador LED de alimentación | Verde: alimentación normal Rojo: alarmas de energía |
| 6 | Botón de encendido/ | Enciende o apaga el Sistema RealPresence Collaboration Server |

Tabla 8.- Descripción Panel Frontal RealPresence® Collaboration Server (RMX®) 1800

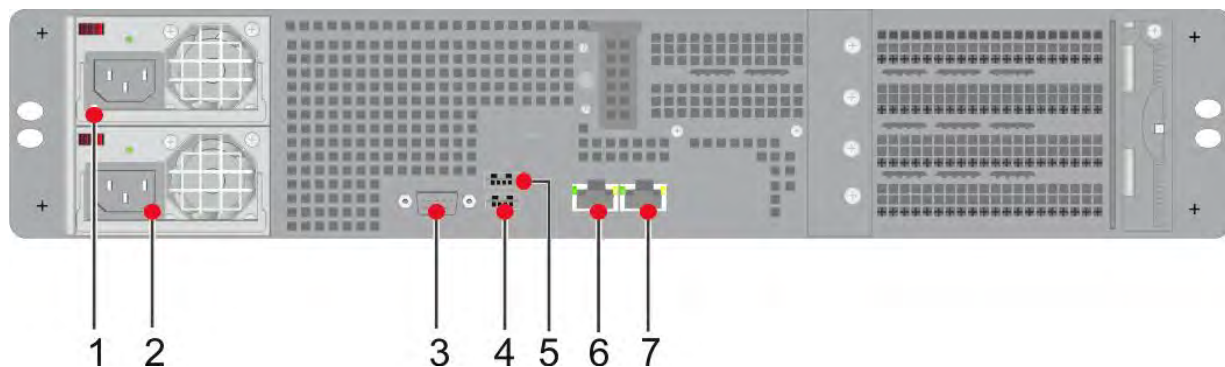


Ilustración 6.- Panel Posterior RealPresence® Collaboration Server (RMX®) 1800

| Nº | Puerto | Descripción |
|---------|-----------------------------|--|
| 1, 2 | Toma eléctrica y ventilador | Toma eléctrica y ventilador incorporados |
| 3 | Serial (RS 232) | Solo diagnósticos |
| 4 | USB 1 | Para conexión de llave USB. |
| 5 | USB 2 | Para conexión de llave USB. |
| 6 | LAN 1 | Para la conexión de red de gestión. Cuando se activa la redundancia LAN, LAN 1 se utiliza tanto para la conexión de gestión como para la conexión de red de medios y señalización. |
| 7 | LAN 2 | Para la conexión de red de medios y señalización. Cuando la redundancia LAN está activada, LAN 2 es el respaldo del puerto LAN1. |

Tabla 9.- Descripción Panel Posterior RealPresence® Collaboration Server (RMX®) 1800.



Ilustración 7.- RealPresence Group 310

- Salida de línea estéreo de 3.5 mm (x1)

Otras interfaces

- 2 x USB 2.0
- RS-232, Mini-DIN de 8 pines (x1)

Red

- Compatibilidad con IPv4 e IPv6
- Ethernet 10/100/1G (x1)

Seguridad

- Cifrado multimedia (H. 323, SIP): AES-128 y AES-256
- Acceso autenticado para los menús de administración, interfaz web, Telnet y API.



Ilustración 9.- RealPresence Group 700



Ilustración 10.- Panel Posterior RealPresence Group 700

Entrada de vídeo

- HDCI (x2)
- HDMI 1.4 (x3)
- Componente YPbPr (x1)
- RCA compuesto dual (x1)
- 1 x VGA

Salida de vídeo

- HDMI 1.3 (x3)
- VGA (x3)

Entradas de audio

- Puertos de entrada del juego de micrófonos para RealPresence Group (x2) (admite hasta 4 conjuntos)
- Compatibilidad con auriculares USB
- HDCI (x2) (cámara)
- HDMI (x3)
- Entradas de línea RCA (x2)

Salida de audio

- HDMI (para sistemas de audio en sala) (x1)
- HDMI (para dispositivo de grabación de conferencias) (x1)
- Compatibilidad con auriculares USB
- Salida de línea estéreo RCA (x1)

Otras interfaces

- USB 3.0 (posterior) (x2)
- USB 2.0 (anterior) (x1)
- RS-232 DB9 (x1)

Red

- Compatibilidad con IPv4 e IPv6
- Conmutador Ethernet 10/100/1G (x2)

Seguridad

- Cifrado multimedia (H. 323, SIP): AES-128 y AES-256
- Acceso autenticado para los menús de administración, interfaz web, Telnet y API.

3.4 Aprovisionamiento de endpoint

Para realizar el aprovisionamiento del equipo de videoconferencia necesitamos tener acceso al mismo vía web, al ser configuración inicial debemos conectarlo a una red con DHCP posteriormente se realiza el cambio a IP estática para mejorar el control y monitoreo del mismo.

Para el ejemplo de aprovisionamiento se usa una red local, para los equipos destinados a las unidades se usará redes VPN las cuales deben ser gestionadas con el área de telecomunicaciones, la cual deberá asegurar un buen enlace de comunicación.

Como primer paso tenemos que informarle al sistema de aprovisionamiento desde que red le harán una nueva solicitud, para hacer esto accedemos al servidor llamado Real Presence Resource Manager (RPRM). Accedemos al mismo con la dirección IP asignada, veremos lo siguiente:

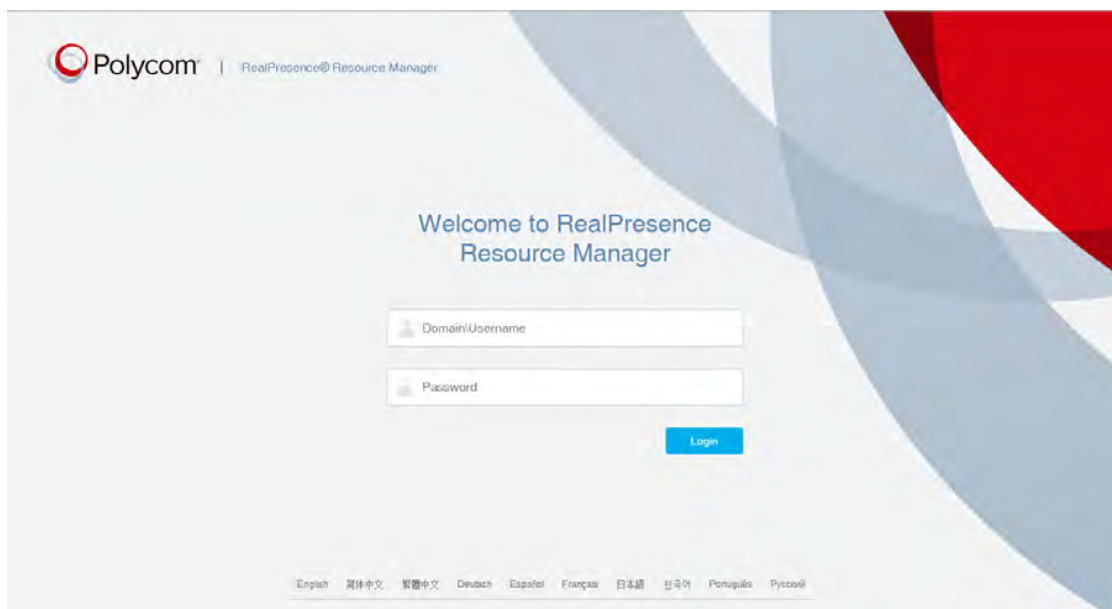


Ilustración 11.- Real Presence Resource Manager (RPRM)

Introducimos el usuario y contraseña de administrador para ver la pantalla inicial del sistema llamado dashboard.

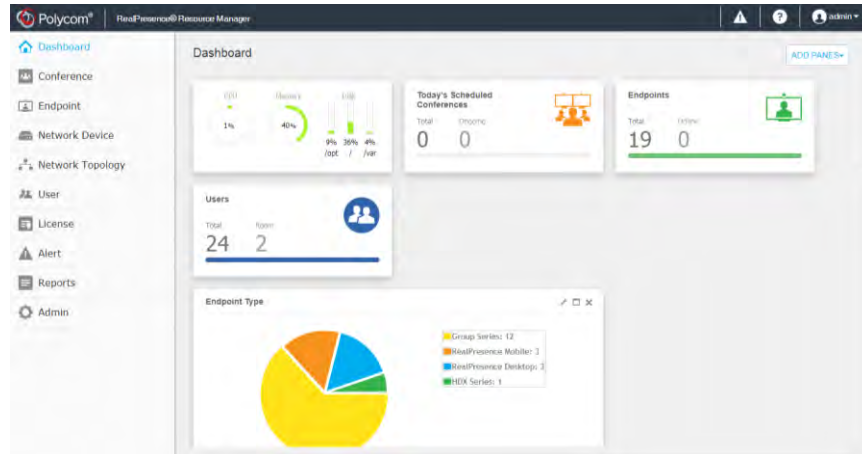


Ilustración 12. - Dashboard Real Presence Resource Manager (RPRM)

Del lado izquierdo podemos observar un menú, vamos a dar clic en la opción de **Network Topology>Sites** y veremos lo siguiente:

| Site Name | Description | Country Code | Area Code | Max Bandwidth(Mbps) | Max Bit Rate (kbps) |
|--------------|----------------------|--------------|-----------|---------------------|---------------------|
| RPAD | RPAD | | | Unlimited | Unlimited |
| Internet/VPN | Internet Placeholder | | | Unlimited | Unlimited |
| Core | SESA Core | | | Unlimited | Unlimited |
| Endpoints | Endpoints | | | Unlimited | Unlimited |

Ilustración 13.- Sites

De la lista que nos aparece debemos seleccionar la opción de **Endpoints**, posteriormente el botón de editar que se habilitará en la parte superior como se muestra en la siguiente imagen:

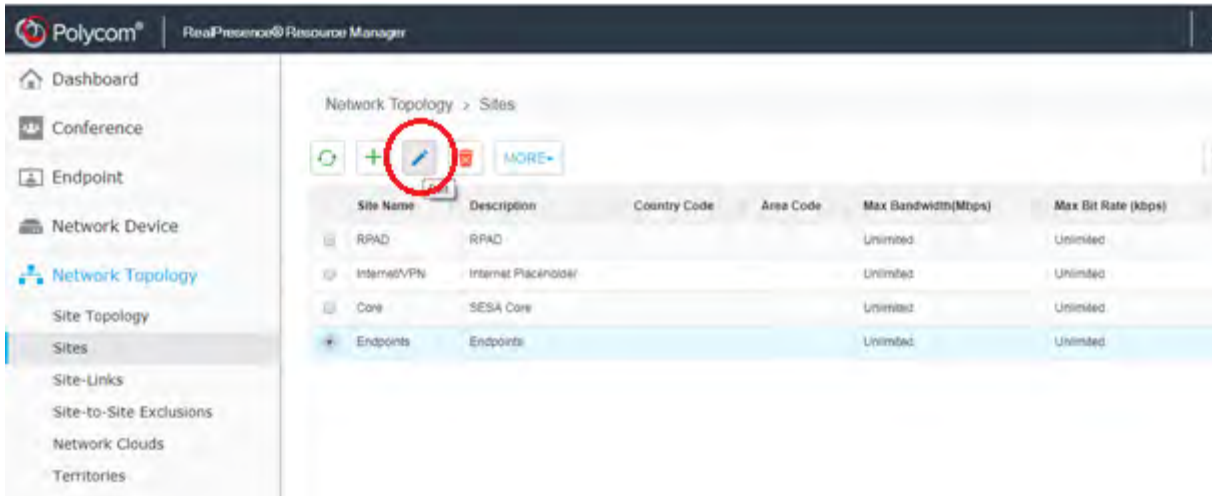


Ilustración 14.- Seleccionando site de Endpoints

A continuación, aparecerá una ventana llamada **Edit Site** (Ilustración número 15), donde seleccionaremos del lado izquierdo la opción de **Subnet**, en esta última ventana tenemos que seleccionar el icono de **+** (Ilustración número 16).

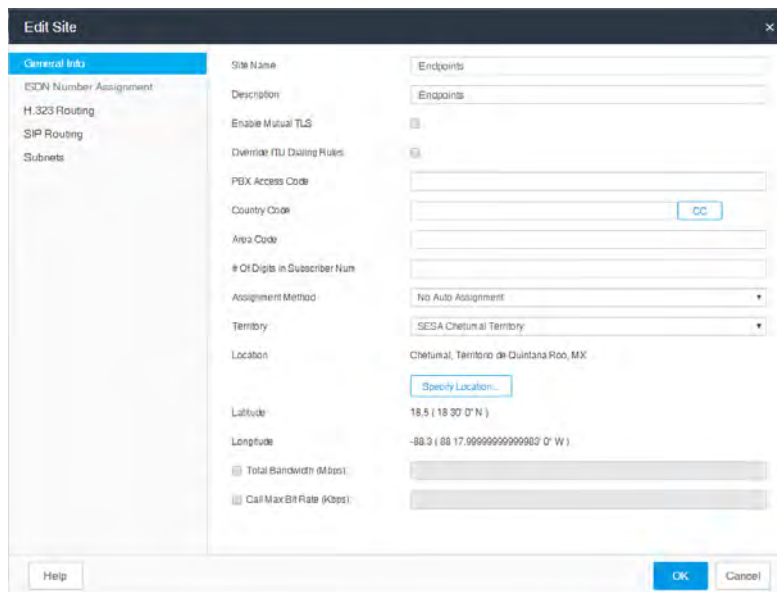


Ilustración 15.- Ventana Edit Site

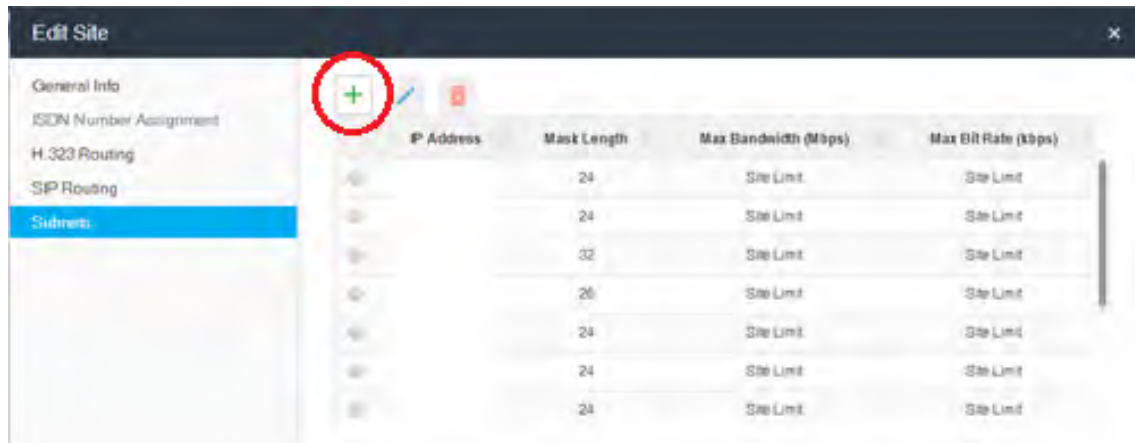


Ilustración 16.- Agregando red/subred

Seguidamente aparecerá una ventana (ilustración número 17) donde tenemos que agregar la red o subred con su respectiva mascara en la que se encuentra conectado el endpoint y dar click en OK.

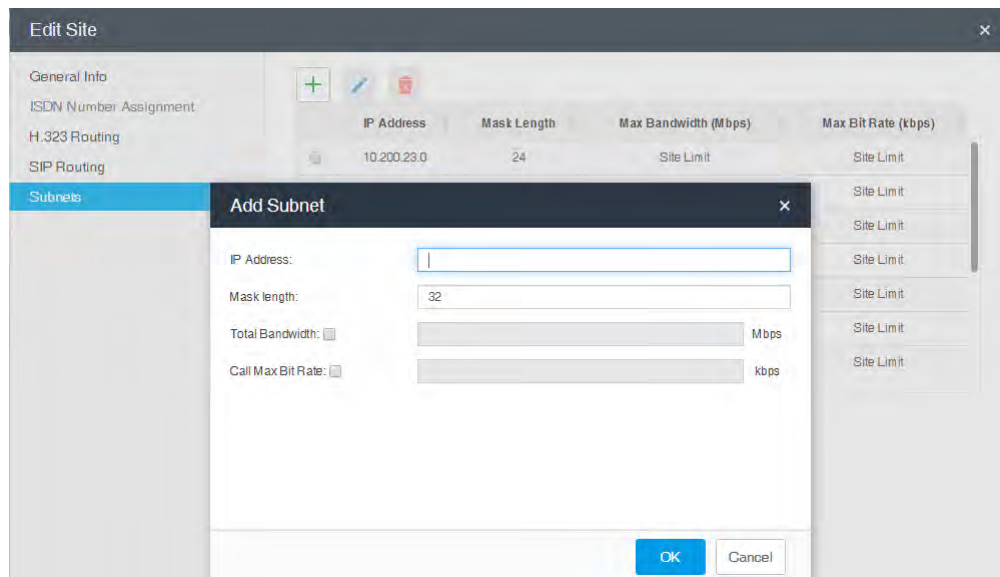


Ilustración 17.- Ventana Add Subnet

Una vez agregada la red del endpoint procedemos a conectar y encender el equipo de videoconferencia para visualizar la pantalla inicial de configuración tal como se muestra en la ilustración número 18.

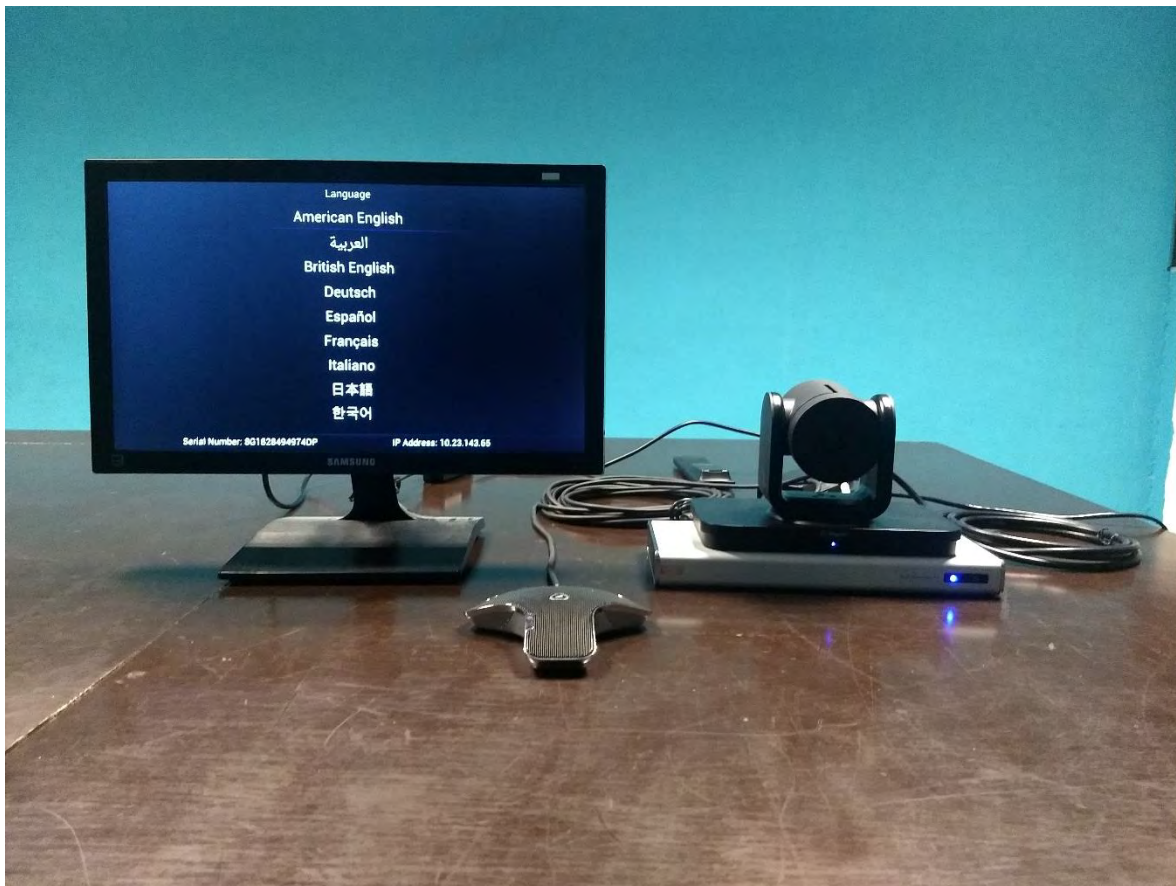


Ilustración 18.- Equipo conectado y encendido

En esta pantalla podemos visualizar la selección de idioma, el número de serie del equipo y la dirección IP que se ha configurado, lo podemos apreciar mejor en la ilustración número 19.

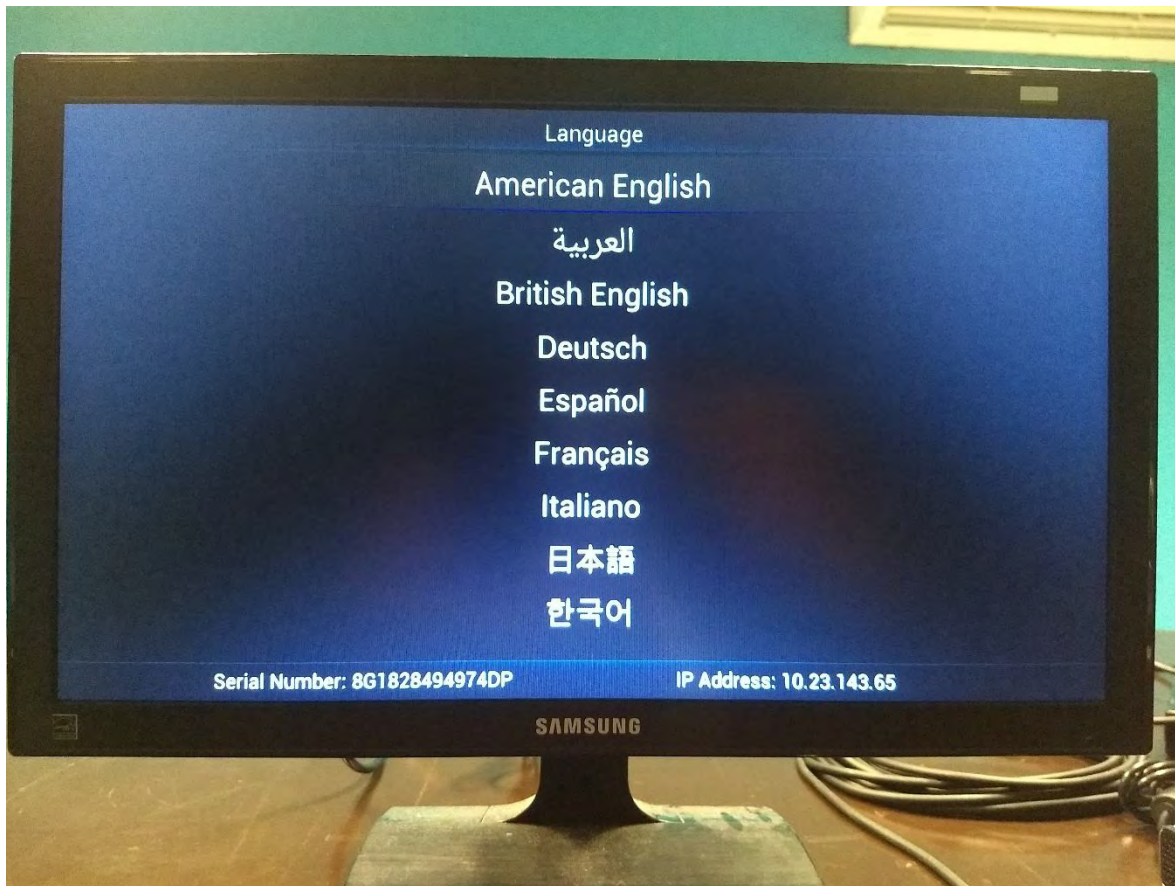


Ilustración 19.- Pantalla inicial de configuración

Mediante el navegador web accedemos a la dirección IP que aparece en pantalla, aparecerá un mensaje como se muestra en la ilustración número 20, tendremos que dar clic en opciones avanzadas y posteriormente en acceder al sitio no seguro para tener acceso a la pantalla de inicio de sesión (ilustración número 21).



La conexión no es privada

Es posible que los atacantes estén intentando robar tu información de **10.23.143.65** (por ejemplo, contraseñas, mensajes o tarjetas de crédito). [Más información](#)

NET::ERR_CERT_AUTHORITY_INVALID

Ayuda a mejorar la Navegación Segura enviando [datos del sistema y contenido de las páginas](#) a Google. [Política de Privacidad](#)

Configuración avanzada

Volver para estar a salvo

Ilustración 20.- Accediendo a la dirección IP

Admin Login

This system requires you to log in for remote access.

User Name:

Password:

For more information about configuring and using your system, go to support.polycom.com and navigate to the appropriate page for your system.

Login

support.polycom.com

Ilustración 21.- Pantalla de inicio de sesión

Para tener acceso a la administración del equipo el usuario es **admin** y la contraseña es el número de serie que podemos visualizar en la pantalla del equipo de videoconferencia o en la parte de atrás del mismo.

Por ser la primera vez que accedemos a la administración entraremos directo al asistente de configuración, como primera opción debemos elegir un idioma, se recomienda dejar por default como se muestra en la ilustración número 22 y damos clic en **Next**.



Ilustración 22.- Selección de idioma

La siguiente pantalla es el acuerdo de licencia de usuario final y damos clic en **Accept**.

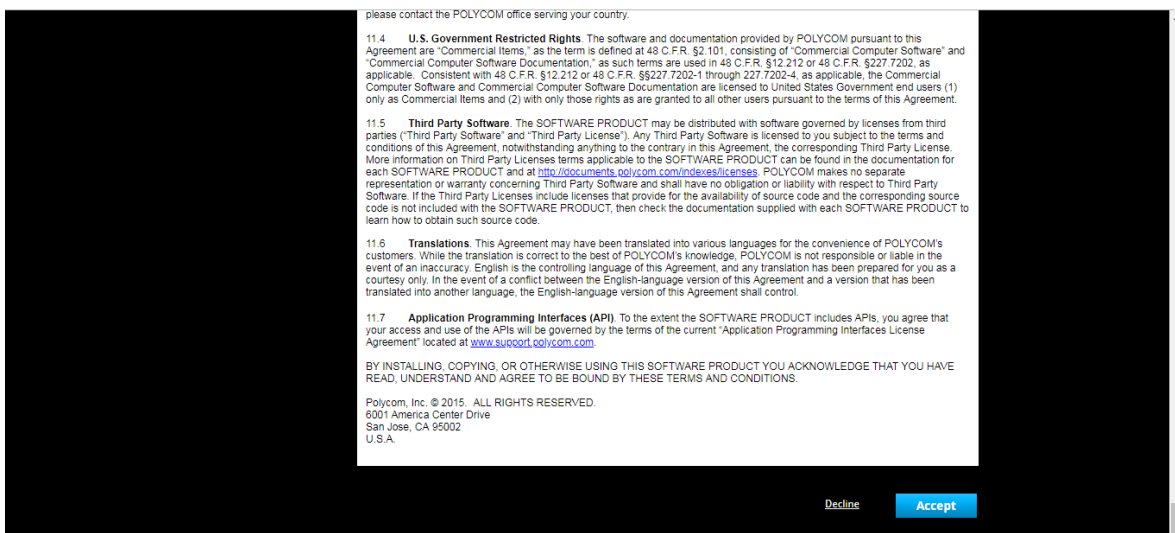


Ilustración 23.- Acuerdo de licencia de usuario final

A continuación el asistente de configuración nos dará a elegir que método queremos usar tal y como se muestra en la ilustración número 24, en este caso escogeremos la opción **Provision** y posteriormente veremos una pantalla como la ilustración número 25.

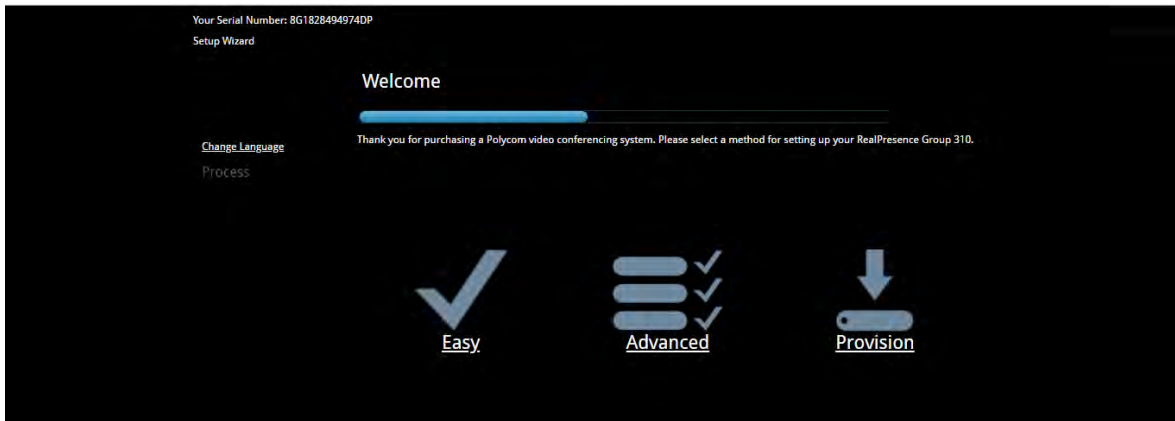


Ilustración 24.- Método de configuración del equipo.

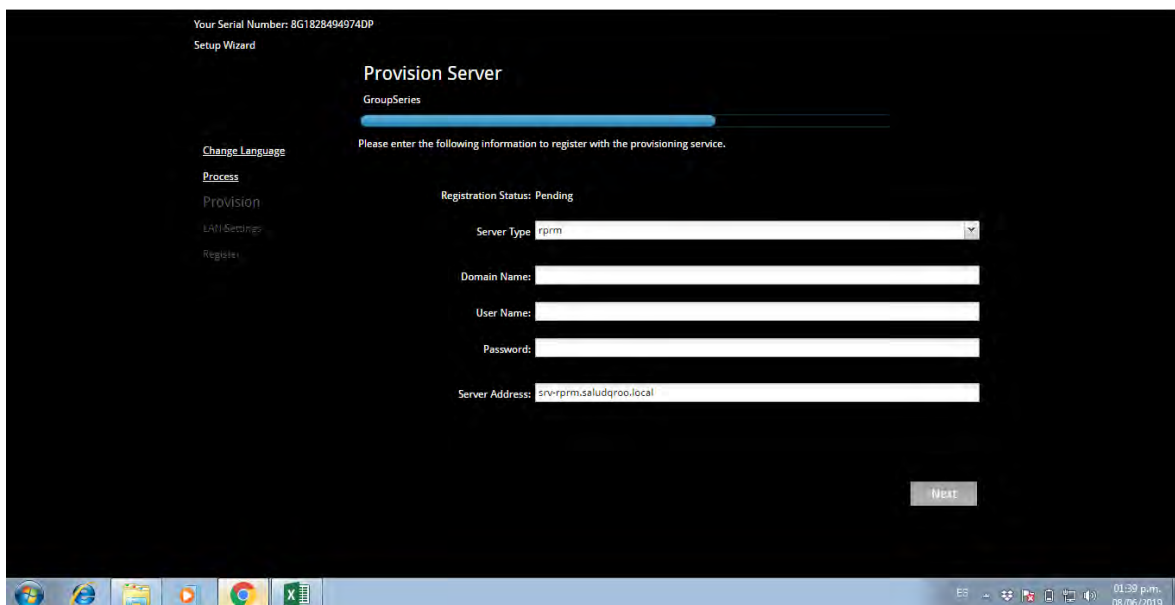


Ilustración 25. Configurando servidor de aprovisionamiento. Status Pending.

En esta última pantalla el asistente de configuración nos muestra un campo llamado **Registration Status**, el cual se encuentra en **Pending**, y un formulario que debemos llenar con información para realizar el correcto aprovisionamiento del endpoint, nos guiaremos de la tabla número 7 anteriormente mencionada para realizar el proceso de prueba.

Quedando los campos de esta manera:

- Server Type: **rprm**
- Domain Name: **dominio.interno**
- User Name: **teleeducacion.sesa**
- Password: **Preestablecida**
- Server Address: **RPRM.dominio.interno**

Una vez llenado daremos clic en **Next** y el mensaje de **Pending** en **Registration Status** deberá cambiar a **Registered**. Posteriormente debemos introducir un nombre al equipo y el correo correspondiente para finalizar dando clic en **Finish**.

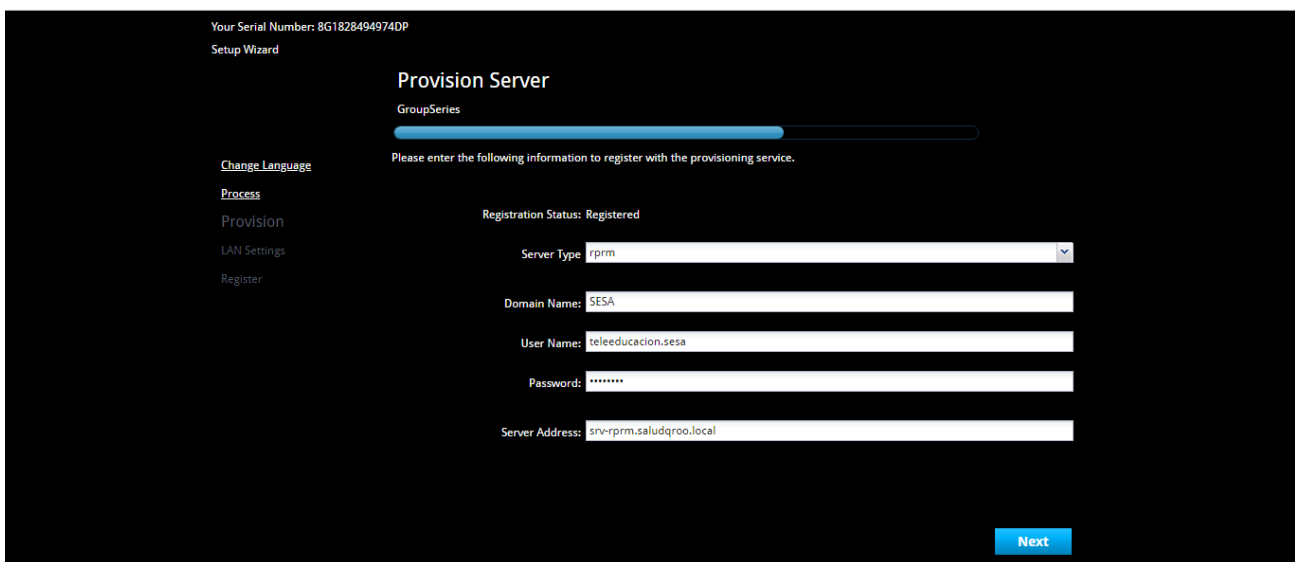


Ilustración 26.- Configurando servidor de aprovisionamiento. Status Registered

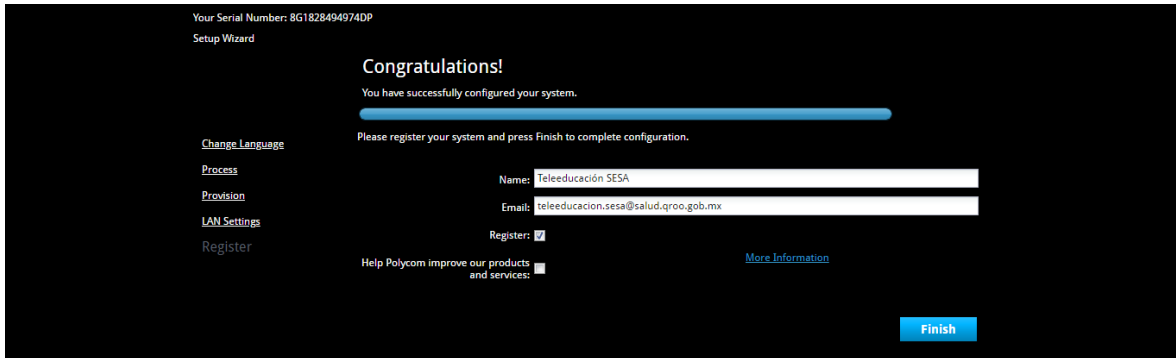


Ilustración 27.- Asignando nombre al equipo

Veremos un mensaje como el que se muestra en la ilustración número 28 y tendremos que esperar hasta ver la pantalla de administración (ilustración número 29).

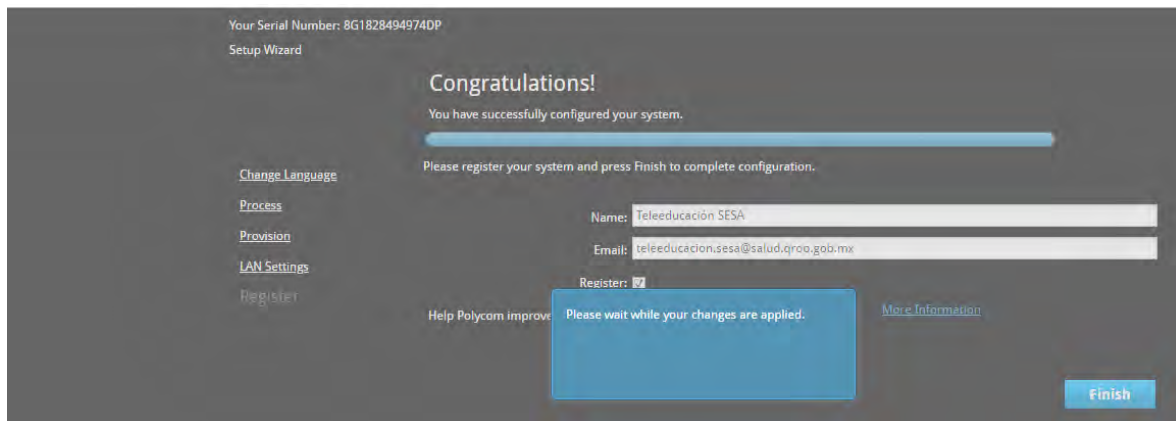


Ilustración 28.- Mensaje de confirmación de aprovisionamiento

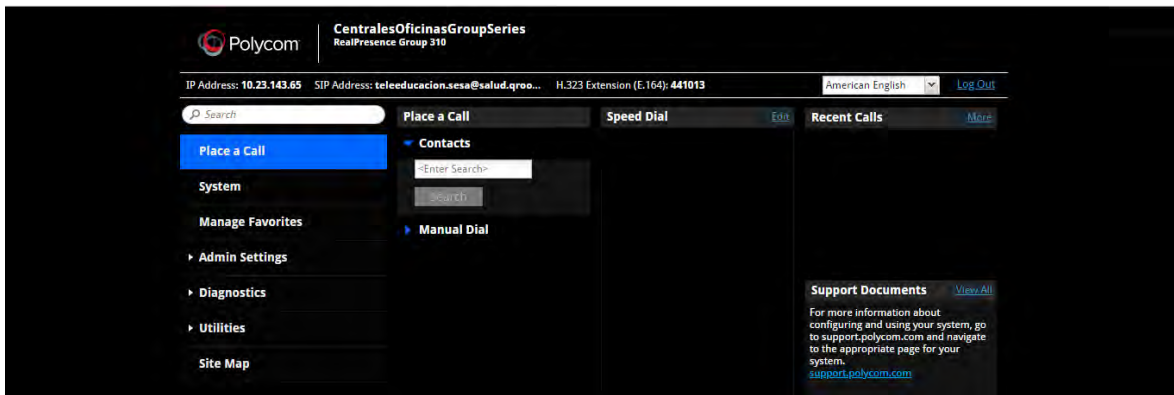


Ilustración 29.- Pantalla de administración del endpoint

En la pantalla de administración podemos observar en la parte superior información tal como dirección IP, dirección SIP y extensión H.323. Con estos datos podemos realizar las videollamadas directamente entre equipos.

Para validar que el aprovisionamiento se realizó correctamente podemos hacerlo directamente de la interfaz de administración del equipo de videoconferencia, para esto debemos escribir en el buscador la palabra status y veremos las opciones como nos muestra la ilustración número 30.

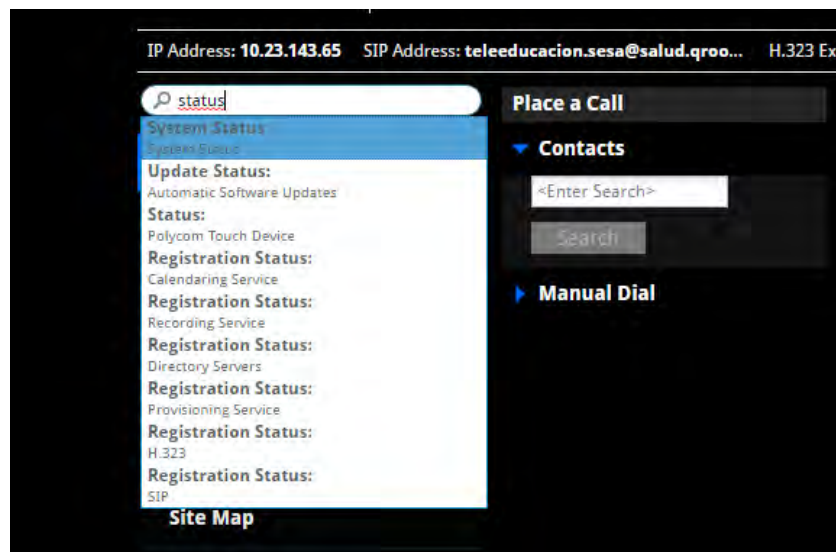


Ilustración 30.- Campo de búsqueda

Seleccionamos la opción de **System Status** y veremos lo siguiente.

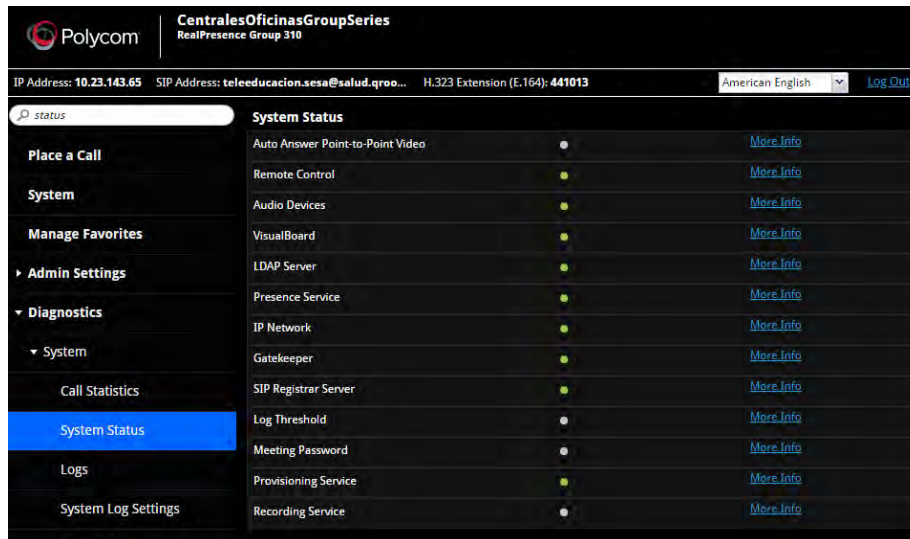


Ilustración 31.- System Status

Como podemos observar tenemos una serie de parámetros acompañados de un círculo color verde, esto significa que correcto, pero los que nos interesa para saber si es aprovisionamiento se hizo correctamente son los siguientes:

- Gatekeeper
- SIP Registrar Server (Servidor de registro SIP)
- Provisioning Service (Servicio de aprovisionamiento)
- LDAP Server (Servidor LDAP)
- Presence Service (Servicio de presencia)

Cabe mencionar que una vez realizado el aprovisionamiento el usuario y contraseña cambian a uno preestablecido en el momento de la implementación del sistema de videoconferencia.

3.5 Pruebas de comunicación

Para realizar las pruebas de comunicación se ocupó un equipo de la marca Polycom HDX 7000 que ya se tenía configurado que no es parte del proyecto SACMED, la comunicación se realiza entre el equipo antes mencionado y el equipo con el que se realizó el primer aprovisionamiento.

Ambos equipos marcaron a una sala de videoconferencia de pruebas que viene configurada en el servidor de aprovisionamiento, la cual es identificada con el número 7149983. El escenario de pruebas se muestra en la ilustración número 32, al fondo podemos observar el equipo que ya tenía una configuración, el cual llamaremos equipo 1, y sobre la mesa se encuentra el equipo recién configurado, lo llamaremos equipo 2.



Ilustración 32.- Escenario de pruebas

En la ilustración número 33 validamos la transmisión de audio y video del equipo 2 al equipo1.

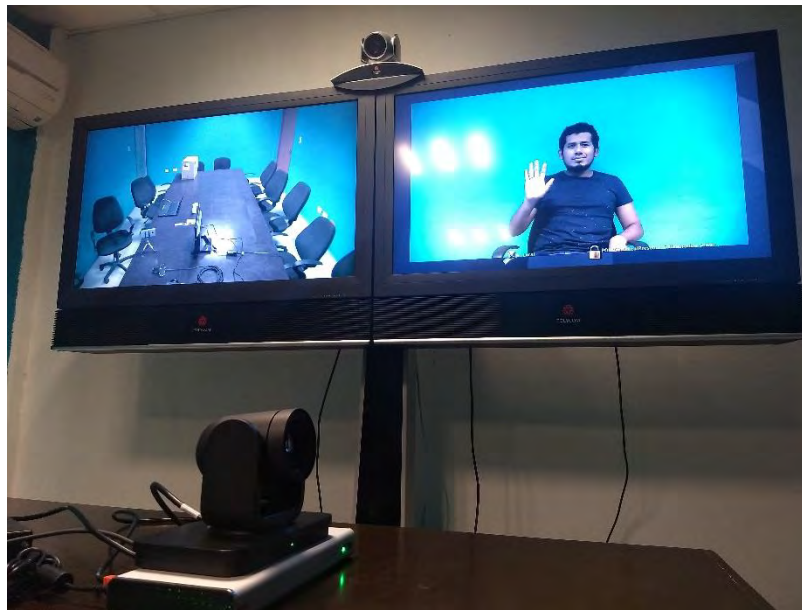


Ilustración 33.- Transmisión de audio y video del equipo 2 al equipo1

En la ilustración número 34 validamos la transmisión de audio y video del equipo 1 al equipo 2.

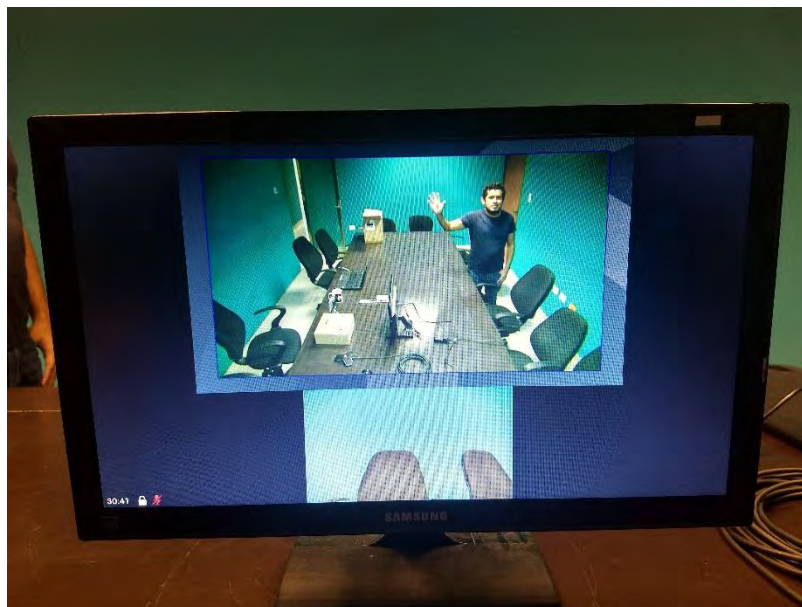


Ilustración 34.- Transmisión de audio y video del equipo 1 al equipo 2

3.6 Implementación

Con las pruebas realizadas y comunicación existente procedemos a configurar cada endpoint correspondiente a las unidades descritas en la tabla número uno presentada en el capítulo uno.

Antes de realizar la distribución de los equipos, debemos tener lista la red VPN para cada unidad y tener un buen enlace de comunicación, esto se debe gestionar con el área de telecomunicaciones. El direccionamiento obtenido debe ser agregado en el servidor de aprovisionamiento para una correcta configuración.

Se visita cada unidad para distribuir físicamente el equipamiento y con el apoyo del área técnica encargada se realiza el siguiente procedimiento:

- Se verifica el estado del equipamiento por posibles daños físicos.
- Instalamos, conectamos y encendemos el equipo.
- Verificamos conexión de red.
- Procedemos a realizar el aprovisionamiento.
- Realizamos las pruebas de comunicación, esto con el fin de detectar posibles deficiencias con los enlaces y gestionar a solución con el área de telecomunicaciones.
- Se dejan los equipos funcionando correctamente y periódicamente se realiza el monitoreo de los mismos, proceso que será descrito en la siguiente sección.
- Con ayuda del área técnica de cada unidad se verifica el estado del equipamiento por posibles daños o percances.

3.6 Monitoreo

La detección oportuna de fallas y el monitoreo de los elementos que conforman SACMED son actividades de gran relevancia para brindar un buen servicio a las unidades, médicos y pacientes. De esto se deriva la importancia de contar con un sistema de monitoreo capaz de notificar en tiempo real las fallas en los endpoints. En esta sección hablaremos sobre el servidor destinado para esta tarea.

El control de los endpoint los podemos realizar desde el servidor llamado Real Presence Resource Manager (RPRM). Accedemos al mismo con la dirección ip asignada, veremos lo siguiente:

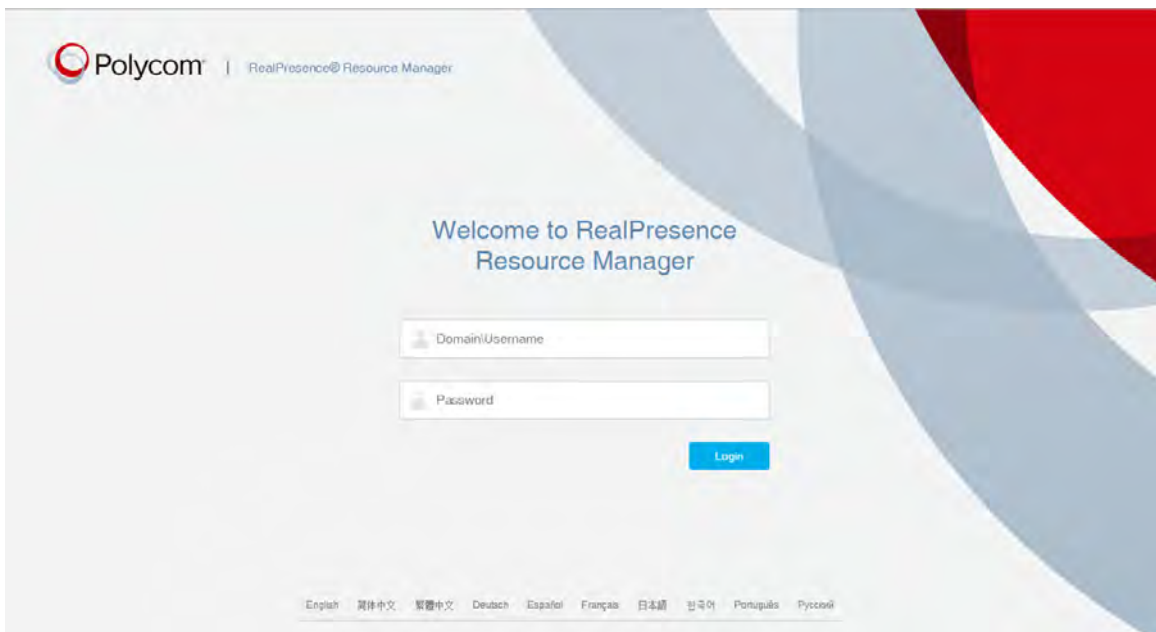


Ilustración 35.- Real Presence Resource Manager (RPRM)

Introducimos el usuario y contraseña de administrador para ver la pantalla inicial del sistema llamado dashboard.

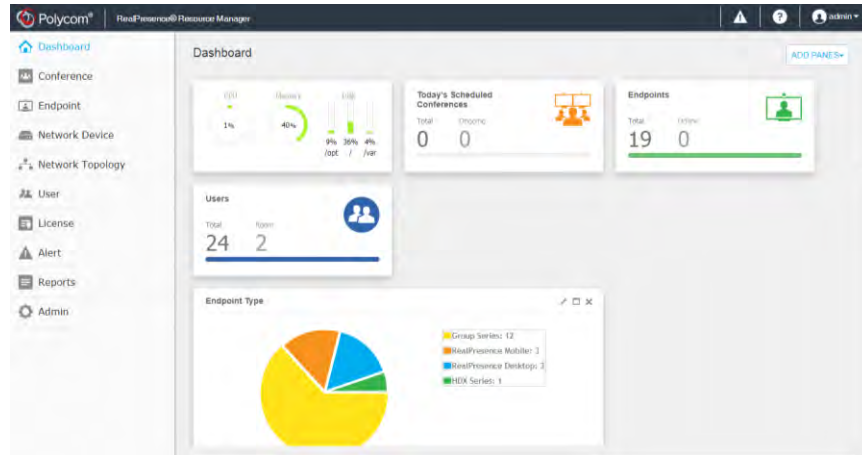


Ilustración 36. - Dashboard Real Presence Resource Manager (RPRM)





En esta pantalla inicial del sistema de monitoreo podemos observar un resumen, te muestra el procesamiento, memoria RAM y almacenamiento usado, también se puede ver la cantidad de endpoints provisionados así como los usuarios registrados.

Del lado izquierdo podemos observar un menú, vamos a dar clic en la opción de **Endpoint>Monitor View** y veremos lo siguiente:

| Status | Mode | Endpoint Name | Model | IP Address | Dial String | Site | Owner |
|--------|------|-----------------------------------|------------------------|---------------|-------------------------------------|-----------|--|
| 🟡🔴 | 📡 | Teleduccion_SESA | RealPresence Group 310 | 10.23.143.65 | teleduccion.sesa@salud.qroo.gob.mx | Endpoints | Oficinas Centrales |
| 🟡🔴🔴 | 📡 | Teleduccion_HIKAN | RealPresence Group 310 | 10.200.17.68 | teleduccion.hikan@salud.qroo.gob.mx | Endpoints | Hospital Integral de Kantunilkin 2 |
| 🟡🔴 | 📡 | Teleduccion_HGPC | RealPresence Group 310 | 10.200.23.138 | teleduccion.hgpc@salud.qroo.gob.mx | Endpoints | Hospital General de Playa del Carmen 2 |
| 🟡🔴 | 📡 | Teleduccion_HGCAN | RealPresence Group 310 | 10.23.20.213 | teleduccion.hgcan@salud.qroo.gob.mx | Endpoints | Hospital General de Cancún 2 |

Ilustración 37.- Monitor View

En esta pantalla podemos observar una lista donde nos muestra información acerca de los endpoints que se han provisionado, a continuación se describen los campos.

- Status. En este campo podemos validar si el endpoint se encuentra conectado a la red.
 - Offline 
 - Online 
 - Online con detalles de configuración 
 - Online con detalles de conexión de red 
- Endpoint Name: Nombre que fue asignado al endpoint.
- Model: Modelo del endpoint.
- IP Address: Dirección IP que tiene asignada el endpoint.

Podemos seleccionar cualquier endpoint de la lista y si se encuentra online podemos administrarlo remotamente por medio de la dirección IP.

En caso contrario, de tener un equipo offline, con el apoyo del área técnica de cada unidad procedemos a detectar el problema para dar una oportuna solución.

Capítulo 4 Resultados y Conclusiones

4.1 Resultados

Se realizó la instalación y configuración de 16 equipos de videoconferencia, de los cuales 7 son destinados a la atención médica y son capaces de transmitir audio y video bidireccional en tiempo real, así como compartir contenido desde equipo médico, tales como ultrasonido y electrocardiograma; los 9 equipos restantes destinados a capacitación médica y personal de la salud tienen las mismas capacidades.

Se instaló así un teleconsultorio en cada una de las 7 unidades médicas del SACMED, con equipo médico y con tecnología de videoconferencia especiales para Telemedicina y un teleaula/auditorio en cada una de las 3 oficinas administrativas correspondientes a las jurisdicciones sanitarias y 6 unidades médicas, equipada con un sistema de videoconferencia estándar para Tele-educación. Quedando la distribución de la siguiente manera.

| TELEMEDICINA | |
|--|--------------------|
| UNIDAD | FUNCIÓN |
| Hospital General de Chetumal | Unidad consultada |
| Hospital Integral de José María Morelos | Unidad consultante |
| Hospital General de Felipe Carrillo Puerto | Unidad consultante |
| Hospital General de Playa del Carmen | Unidad consultada |
| Hospital General de Cancún | Unidad consultada |
| Hospital Comunitario de Isla Mujeres | Unidad consultante |
| Hospital Integral de Kantunilkín | Unidad consultante |

Tabla 10.- Unidades de Telemedicina

| TELEEDUCACIÓN |
|--|
| Hospital General de Chetumal |
| Uneme Cisame de Chetumal |
| Hospital General de Felipe Carrillo Puerto |
| Uneme de enfermedades crónicas de Felipe Carrillo Puerto |
| Hospital General de Playa del Carmen |
| Hospital General de Cancún |
| Jurisdicción Sanitaria Número 2 |
| Hospital Comunitario de Isla Mujeres |
| Hospital Integral de Kantunilkín |

Tabla 11.- Unidades de Teleeducación

Con la implementación del proyecto se logró dar servicios de especialidad en zonas rurales, de esa manera no se encarece la prestación de los mismos al tener que hacer una referencia al paciente hacia otra unidad, por lo general en el área urbana. También se pone en marcha la capacitación constante al personal de las unidades.

4.2 Conclusiones

El Sistema de Atención y Capacitación Médica Especializada a Distancia (SACMED) permitirá brindar atención médica de especialidad y capacitación a hospitales comunitarios y clínicas rurales de la entidad, a través de Tecnologías de Información y Comunicación para optimizar los recursos humanos y materiales del sector y disminuir los costos que actualmente tiene la atención de especialidades para la población quintanarroense, permitiendo así la comunicación interactiva en tiempo real entre el paciente, y el médico o profesional a distancia, incrementando la capacidad y cobertura de atención especializada del sistema de salud en el Estado.

Así mismo se fortalece la infraestructura tecnológica y el recurso humano en el sector salud de Quintana Roo mediante programas de capacitación a distancia (Tele-educación) y se incrementan las acciones de protección, promoción de la salud y prevención de enfermedades para disminuir las brechas en atención médica existentes entre diferentes grupos sociales de la entidad para así lograr disminuir significativamente los índices de morbilidad y mortalidad de la población más marginada de la entidad.

Bibliografía

- Cardozo, N. L. (2014). Tecnologías de virtualización en los sistemas informáticos de las organizaciones empresariales del estado Zulia. *Revista Electrónica de Estudios Telemáticos*, 50-53.
- Certsuperior. (1 de Abril de 2019). *Certsuperior*. Obtenido de Certsuperior: <https://www.certsuperior.com/CertificadosSeguridad.aspx>
- Francis, D. (2017). *Mastering Active Directory: Understand the Core Functionalities of Active Directory Services Using Microsoft Server 2016 and PowerShell*. Packt Publishing.
- Intel Corporation. (Marzo de 2011). *Intel Corporation*. Obtenido de Intel Corporation: <https://cdrdv2.intel.com/v1/dl/getContent/599884>
- Jones, M. T. (31 de Mayo de 2009). *IBM Developer*. Obtenido de IBM Developer: <https://www.ibm.com/developerworks/ssa/library/l-hypervisor/index.html>
- Liu, C. (2006). *DNS and BIND (5th Edition)*. O'Reilly Media.
- Medina, A. L. (2010). *Análisis de la virtualización de sistemas operativos*. Barcelona, España: Facultad de Matemáticas e Informática.
- Polycom, I. (5 de Junio de 2019). *Polycom Support*. Obtenido de Polycom Support: <https://support.polycom.com/content/support/apac/china/en/support/video/group-series.html>
- Project, T. A. (18 de Agosto de 2018). *The Apache Directory™ Project*. Obtenido de The Apache Directory™ Project: <https://directory.apache.org/apacheds/>
- Project, T. O. (19 de Diciembre de 2018). *The OpenLDAP Project*. Obtenido de The OpenLDAP Project: <http://www.openldap.org>
- Salud, C. N. (29 de Abril de 2015). CONCEPTOS DE TELEMEDICINA. Ciudad de México, México. Obtenido de <http://www.cenetec.salud.gob.mx/contenidos/telesalud/conceptos.html>
- Salud, C. N. (19 de Octubre de 2017). ¿Qué es la Telesalud y la Telemedicina? Ciudad de México, México. Obtenido de <https://www.gob.mx/salud/cenetec/acciones-y-programas/que-es-la-telesalud-y-la-telemedicina>

Stanek, W. R. (2008). *Windows Server 2008 Administrator's Pocket Consultant*. Redmond, Washington: Microsoft Press.

VapourApps. (13 de Mayo de 2016). *VapourApps*. Obtenido de What is Hypervisor and what types of hypervisors are there: <https://vapour-apps.com/what-is-hypervisor/>

VMWare. (20 de Febrero de 2019). *VMWare*. Obtenido de VMWare: <https://www.vmware.com/mx/support/vsphere-hypervisor.html>