

RED WAN VOIP CON PROTOCOLO OSPFv2 BASADA EN TECNOLOGÍA CISCO PARA LA EMPRESA EQUIMAVENCA

(Red Wan Voip with Protocol OspfV2 Based in Cisco Technology for Company
Equimavenca)

Recibido: 05/05/2016 Aceptado: 23/05/2017

Díaz, Alfredo

Universidad del Zulia, LUZ, Venezuela

alfredojodp@hotmail.com

Fuenmayor, Jonathan

Coordinador de IT en la empresa EQUIMAVENCA, Venezuela

jfuenmayor05@gmail.com

RESUMEN

El objetivo de esta investigación fue proponer una red WAN VoIP con protocolo OSPFv2 basada en tecnología CISCO para la empresa EQUIMAVENCA, la cual tuvo como propósito lograr la reducción de gastos en telefonía convencional, permitiendo la comunicación mediante voz entre las tres sedes con las que cuenta la empresa ubicadas en Ciudad Ojeda, Maracaibo y El Tigre, a través del uso de la misma infraestructura de red. Con una población y muestra de (3) personas que laboraban en el departamento de IT. Las bases teóricas se fundamentaron por diversos autores como Odom (2016), Ariangelo y Barrientos, (2011), Huidobro (2010), entre otros. Así como también Información contenida en libros, consultas electrónicas y trabajos de grado, desde los cuales se sustentaron las fases metodológicas en la tecnología CISCO. El tipo de investigación se consideró aplicada por su corte tecnológico bajo la modalidad de proyecto factible, y de campo. La recolección de datos se realizó mediante revisión documental, observación directa, entrevistas no estructuradas, listas de cotejo y entrevistas no estructuradas. Como resultado de la misma, se realizó el diseño de topología WAN de la red, conteniendo los diseños tanto físicos como lógicos de la red, así como la estructuración de las subredes para cada sede.

Palabras clave: Red WAN, VoIP, OSPFv2, tecnología CISCO.

ABSTRACT

The objective of this research was to propose a VoIP WAN network over OSPFv2 routing protocol based on CISCO technology for the EQUIMAVENCA Company, achieving cost reduction in conventional telephony, allowing voice communication between it three branch offices. The company was located in Ciudad Ojeda, Maracaibo and El Tigre, through the same network infrastructure. The information was obtained over a population of three people working at the IT department using a population census. The theoretical bases were founded by various authors such as Odom (2016), Ariangelo y Barrientos,

(2011), Huidobro (2010), among others. As well as Information contained in books, electronic consultations and degree works, from which the methodological phases in CISCO technology were sustained. The type of research was considered applied by its technological cutting under the modality of field and feasible project. Data collection was done through document review, direct observation, unstructured interviews, checklists and unstructured interviews. As a result, the network WAN topology was designed, containing both the physical and logical designs of the network, as well as the structuring of the subnets for each site.

Keywords: WAN, VoIP, OSPFv2, and CISCO technology.

INTRODUCCIÓN

A nivel global, la tecnología de la información (IT), ha venido evolucionando de tal forma que se ha vuelto imprescindible la implementación de redes informáticas en las organizaciones, ya que estas al momento de almacenar, procesar, y transmitir datos, aportan beneficios tales como automatización de procesos, flexibilidad, seguridad, velocidad, entre otros factores, permitiendo de esta manera un desempeño óptimo en las empresas. En las últimas décadas en Latinoamérica, el sector empresarial ha venido creciendo, por lo tanto también sus redes, motivo por el cual estas se han visto en la necesidad de adquirir nuevas tecnologías que cumplan con las exigencias que demandan los usuarios.

Asimismo, en las empresas, las redes de servicios de telefonía convencional han mantenido su popularidad debido a su accesibilidad, dicho servicio sigue siendo el preferido, pero esto conlleva al pago de costosos planes mensuales para poder hacer uso de la telefonía. Tal es el caso de la empresa EQUIMAVENCA, ubicada en Venezuela, la cual en los últimos años ha venido experimentando un aumento considerable en los gastos de telefonía, de igual manera cuenta con una infraestructura de red independiente de la red de telefonía

Gracias a la innovación por parte de grandes empresas pioneras en la fabricación de dispositivos para networking, ya no es necesario implementar una red por cada servicio que se tenga en una organización, es decir, telefonía, video, datos, entre otros, sino que es posible que todos los servicios mencionados funcionen bajo la misma infraestructura de red, logrando así una convergencia. Este es un tema de suma importancia al tratarse de redes convergentes y tecnología VoIP, ya que en la actualidad gran parte de las organizaciones están implementando dicho servicio, permitiendo de esta manera reducir gastos y a su vez administrar todos los servicios a través de la misma red.

PROBLEMÁTICA

Una red es un conjunto de elementos informáticos conectados entre sí a través de medios físicos, inalámbricos, dispositivos intermediarios, los cuales están compuestos tanto por hardware como software, con la finalidad de administrar, compartir y almacenar información, incluso cuando estos se encuentren separados geográficamente, permitiendo

tiempos de respuesta acordes a las exigencias demandadas actualmente por las organizaciones al momento de intercambiar información entre dispositivos.

Esto permite que en una organización se lleve a cabo la comunicación de manera eficaz. En la actualidad las redes se han vuelto indispensables para el sector empresarial, ya que es necesario mantener la comunicación en las organizaciones aunque estas se encuentren separadas por varios kilómetros. Actualmente, en muchas empresas de Latinoamérica las infraestructuras de red se encuentran separadas de la red telefónica. Hoy en día se están implementando nuevas tecnologías en las organizaciones que permiten la transmisión de voz a bajo costo, haciendo uso de la misma infraestructura de red con la que se realiza la transmisión de datos.

La empresa EQUIMAVENCA (Equipos y Manufacturas Venezolanas C.A), en la actualidad cuenta con tres sedes ubicadas en Venezuela: Base Operativa Occidente, ubicada en la Av. Intercomunal, entre carreteras "O" y "P", Sector Tasajeras, Ciudad Ojeda - Edo. Zulia. Base Operativa Oriente, ubicada en la Av. Fernández Padilla N° 226, San José de Guanipa – Edo. Anzoátegui. Oficinas Administrativas, ubicadas en la Av. 2 El Milagro No. 86 A-27 Edificio Ven Mex Piso 1 y 2 Sector Santa Lucia, Maracaibo – Edo. Zulia. Estas sedes mantienen una constante comunicación mediante líneas telefónicas convencionales y correo electrónico.

El correo electrónico es utilizado con el propósito de suministrar información a empleados, clientes y proveedores. Los teléfonos convencionales son utilizados entre las sedes con el fin de realizar consultas e informar sobre el estado de las operaciones con las oficinas administrativas. Este es el sistema más utilizado por la empresa, ya que por este medio se obtiene respuesta inmediata a la información solicitada por los empleados ubicados en los galpones, talleres y oficinas administrativas. Esto convierte la telefonía en un recurso indispensable para mantener el funcionamiento óptimo en la empresa, permitiéndole ofrecer servicios de calidad.

A partir del año 2007 se ha producido un aumento considerable de las operaciones, generando un incremento en las llamadas entre sucursales, esto ha llevado a la empresa a realizar gastos en telefonía mayores a los realizados anteriormente, los cuales son posibles reducir mediante otra alternativa o tecnología que permita la comunicación entre las sucursales por medio de la transmisión de voz.

En los últimos años, la empresa EQUIMAVENCA ha venido realizando grandes inversiones en tecnología para mejorar la calidad de las comunicaciones entre las sedes y así seguir funcionando de manera óptima, adquiriendo dispositivos intermediarios de alto desempeño con características de hardware y software capaces de manejar tecnología VoIP, la cual, hoy en día no ha sido implementada, aún cuando dichos dispositivos son capaces de manejar esta tecnología.

Al mismo tiempo, realizó la inversión de centrales telefónicas (PBX), las cuales poseen compatibilidad con los dispositivos intermediarios. Con base en lo expuesto anteriormente y tomando en cuenta el factor económico y la factibilidad, dicha problemática se puede solventar con la siguiente propuesta que lleva como nombre Red WAN VoIP con protocolo

OSPFv2 basada en tecnología CISCO para la empresa EQUIMAVENCA. Esta cuenta con dispositivos de red marca CISCO que soportan funciones VoIP (Voz sobre Protocolo de Internet) y posee enlaces VPN (Red Privada Virtual) entre las sedes a través del ISP (Proveedor de Servicios de Internet) y conexiones mediante otros proveedores, los cuales brindan un ancho de banda elevado para la transmisión de voz en enlaces con los que cuenta la red WAN, que puede ser de gran utilidad para disminuir los gastos en telefonía.

Dicha propuesta consta de un diseño de la topología lógica y física de la red que permite activar funciones VoIP, asimismo, las configuraciones pertinentes referentes a segmentación de la red por VLAN (Red de Área Local Virtual) y VLSM, (Máscara de Subred de Longitud Variable) enlaces troncales, configuraciones de seguridad, acceso remoto a los dispositivos intermediarios con el uso del protocolo SSH (Intérprete de Ordenes Seguro), configuración de servidor DHCP (Protocolo de Configuración Dinámica de Host) para los hosts y teléfonos VoIP, QoS (Calidad de Servicio), redundancia de capa 2, entre otras configuraciones básicas y avanzadas.

La propuesta tiene un impacto positivo en la organización a un corto plazo, al utilizar la red de datos para transportar voz disminuyendo el costo de las comunicaciones considerablemente y a largo plazo porque con el pasar del tiempo las tarifas de telefonía seguirán aumentando, situación que no será un problema para la organización debido a la tecnología que se está proponiendo. Esto aporta beneficios en cuanto a innovación se refiere, hoy en día la convergencia de la comunicación en las empresas (voz, datos y video), en una única red IP, resulta una tendencia en crecimiento.

A través de la arquitectura de red propuesta, se producirán ahorros en llamadas, simplificación en la infraestructura de comunicaciones, optimización de la gestión y unificación del sistema de telefonía entre redes, tomando en cuenta aspectos como son la fiabilidad, seguridad y calidad de servicio. La red cuenta con escalabilidad, dando capacidad de crecimiento a la red para satisfacer demandas de rendimiento cada vez mayores y permitiendo agregar equipos sin modificar las configuraciones.

También aporta confiabilidad, es decir, la red posee tolerancia a fallas a través de redundancia de hardware, permitiendo el funcionamiento con total normalidad si un dispositivo llega a fallar. Otro factor importante es la disponibilidad, esto se refiere al porcentaje de tiempo en que un sistema realiza las funciones para las que fue diseñado. Asimismo, cuenta con calidad de servicio que permite dar prioridad de tráfico a la transmisión de voz sobre la transmisión de datos pero manteniendo ambos servicios en un estado de funcionamiento apropiado para una excelente calidad en cuanto a envío y recepción de información se refiere.

Realizadas las consideraciones anteriores, se establece que el propósito de esta investigación es desarrollar una propuesta que le permita a la empresa EQUIMAVENCA solventar la problemática referente al gasto excesivo en servicios de telefonía convencional, y a su vez hacer uso de la infraestructura de red con la que cuenta para lograr la transmisión de voz y datos, logrando de esa manera que todas sus sedes puedan comunicarse por medio de la tecnología de voz sobre protocolo de Internet. Cabe destacar que la misma se desarrolló en el municipio Maracaibo del estado Zulia, en la

empresa EQUIMAVENCA, ubicada en la Av. 2 El Milagro No. 86 A-27 Edificio Ven Mex Piso 1 y 2 Sector Santa Lucia, Maracaibo – Edo. Zulia. La misma se realizó en el período comprendido entre los meses de Abril y Julio del 2015.

FUNDAMENTACIÓN TEÓRICA

De acuerdo a lo expuesto por Odom (2016a) las redes de área extensa (WAN, Wide Área Networks) son infraestructuras de red que abarcan un área geográfica extensa. Las WAN interconectan LAN a través de áreas geográficas extensas, por ejemplo, entre ciudades, estados, provincias, países o continentes. En ese sentido, las redes WAN se conciben como la conexión de varias redes de área local (LAN). Una red de área extensa está conformada por la interconexión de redes de área local, proporcionando conectividad entre ellas sin importar la ubicación geográfica.

Por su parte, Huidobro (2010) indica que la voz sobre IP es una tecnología utilizada para transportar conversaciones voz sobre una red de datos usando el protocolo IP. Asimismo, VoIP es un protocolo que permite que la voz analógica de llamadas telefónicas sea digitalizada y después encapsulada en paquetes IP, quienes a su vez son transmitidos a través de una red. VoIP es el método o técnica que permite la transmisión de voz a través del protocolo de internet.

Ahora bien, resulta oportuno mencionar a Ariangelo y Barrientos (2011) quienes definen OSPF (Open Shortest Path First) como un protocolo de enrutamiento estándar definido en la RFC 2328. Utiliza el algoritmo SPF (Shortest Path First) para encontrar las mejores rutas hacia los diferentes destinos y es capaz de converger muy rápidamente. De igual forma Odom (2016b) determina que el protocolo OSPF es un protocolo de enrutamiento de estado de enlace, desarrollado como reemplazo del protocolo de vector distancia RIP, siendo este sin clase, que utiliza el concepto de áreas para realizar la escalabilidad. En tal sentido, OSPF es un protocolo de enrutamiento dinámico de estado de enlace que permite la rápida convergencia entre dispositivos determinando la mejor ruta a través de su algoritmo SPF.

Con base en los aportes citados anteriormente, a efectos de la presente investigación, los autores definen la red WAN VOIP, como la interconexión de varias redes LAN a través de enlaces VPN, Frame Relay, Última Milla, entre otros, que permiten la transmisión de voz a través del protocolo IP, sin importar la ubicación geográfica de las mismas. Lo que se busca lograr con estas redes es la convergencia entre todos los servicios como voz, datos y video, dentro de la misma infraestructura de red perteneciente a cada LAN, logrando una administración centralizada de dicha plataforma.

En tal sentido, Odom (2016b) establece para OSPF las siguientes características: Por su diseño es un protocolo sin clase, de modo que admite VLSM y CIDR. Es eficaz ya que los cambios de topologías originan actualizaciones de enrutamiento (no hay actualizaciones periódicas). Usa algoritmo SPF para elegir la mejor ruta hacia las redes destino. Es de convergencia rápida, ya que asume y propaga rápidamente los cambios que se realizan a la red. Resulta escalable debido a que funciona adecuadamente en redes de gran envergadura. Se pueden agrupar los enrutadores en áreas para

implementar una red jerárquica. Asimismo, es un protocolo seguro porque admite la autenticación de síntesis del mensaje 5 (MD5). Cuando están habilitados en los enrutadores OSPF, solo aceptan actualizaciones de enrutamiento encriptados de aquellos pares quienes poseen una clave compartida previamente.

Por otra parte, Ariangelo y Barrientos (2011) mencionan una serie de características del protocolo OSPF. Los mismos indican que es un protocolo sin clase, el cual permite sumarización y a su vez rápida convergencia. Es estándar, lo que permite configurarlo en un escenario con diferentes tipos de fabricantes, aprovechando el ancho de banda disponible. Por otra parte, implementa tráfico y multidifusión en vez de difusión, en el cual además sus actualizaciones son incrementales, basado en su costo como métrica.

Adicionalmente, según (Ob. Cit), indican que los protocolos vector - distancia anuncian rutas hacia sus pares, pero los de estado de enlace, anuncian distintas listas hacia todos sus vecinos. Cuando se pierde un enlace se envían LSA (Link-State Advertisement), hacia los vecinos, como así también una base topológica LSDB (Link-State Database). Las LSA se identifican con un número de 0x8000 001 al 0xFFFF FFFF. Cuando los enrutadores convergen poseen una misma LSDB, a partir de ese momento, SPF es capaz de determinar la mejor ruta hacia las distintas redes destino. La tabla de topología es la visión que tiene el enrutador de la red circunscrita en el área donde se encuentra.

Por otro lado, Odom (2016b) indica que cuando se habilita OSPF en una interfaz el enrutador debe determinar si existen otros vecinos OSPF en sus enlaces. Para hacerlo, el mismo reenvía un paquete de saludo con su ID por todas las interfaces con OSPF habilitado, es decir, el utiliza la ID del enrutador para diferenciarlo en cada área exclusivamente. Cuando un enrutador vecino con OSPF habilitado, recibe un paquete de saludo con un ID de otro que no figura en su lista de vecinos, intenta establecer una adyacencia con el enrutador que inició la comunicación.

METODOLOGÍA

La presente investigación se considera de tipo aplicada y de corte tecnológico, ya que la propuesta sobre la implementación de la tecnología VoIP busca afrontar la problemática existente, propuesta que puede ser implementada en el momento que se desee. Hernández y otros (2014) informan que a la investigación aplicada también se le denomina activa o dinámica, ya que depende de sus descubrimientos y aportes teóricos. Busca confrontar la teoría con la realidad. Es el estudio y la aplicación de la investigación a problemas concretos, en circunstancias y características concretas. La presente investigación se fundamentó en una propuesta que permite aplicar los conocimientos adquiridos por medio de la teoría consultada de diversas fuentes y de esa hacer frente a la problemática antes mencionada.

En cuanto a la modalidad del estudio, puede catalogarse como proyecto factible y a su vez de campo, ya que esta propuesta está destinada a dar solución a una problemática, se considera que es de campo porque la recolección de los datos para dicha propuesta se efectuó en la empresa Equimavenca, mismo lugar donde se presenta la problemática. Tal como lo define Fideas (2012) que la investigación de campo consiste en la recolección de

datos directamente de la realidad donde ocurren los hechos, sin manipular o controlar variable alguna. A la vez, la investigación está ubicada en el proyecto factible, Fidias (2012) lo define como una propuesta de acción para resolver un problema práctico o satisfacer una necesidad. Es indispensable que dicha propuesta se acompañe de la demostración de su factibilidad o posibilidad de realización.

Según Hernández y otros (2014) la población es la totalidad de un fenómeno de estudio, incluye la totalidad de unidades de análisis o entidades de población que integran dicho fenómeno y que debe cuantificarse para un determinado estudio, integrando un conjunto N de entidades que participan de una determinada característica, y se le denomina población por constituir la totalidad del fenómeno adscrito a un estudio o investigación. Se tomó como población las tres (3) personas encargadas del departamento de tecnología de la información (IT) de EQUIMAVENCA. Por otro lado, dado el tamaño y accesibilidad a la población objeto de estudio, se consideró la muestra como un censo poblacional.

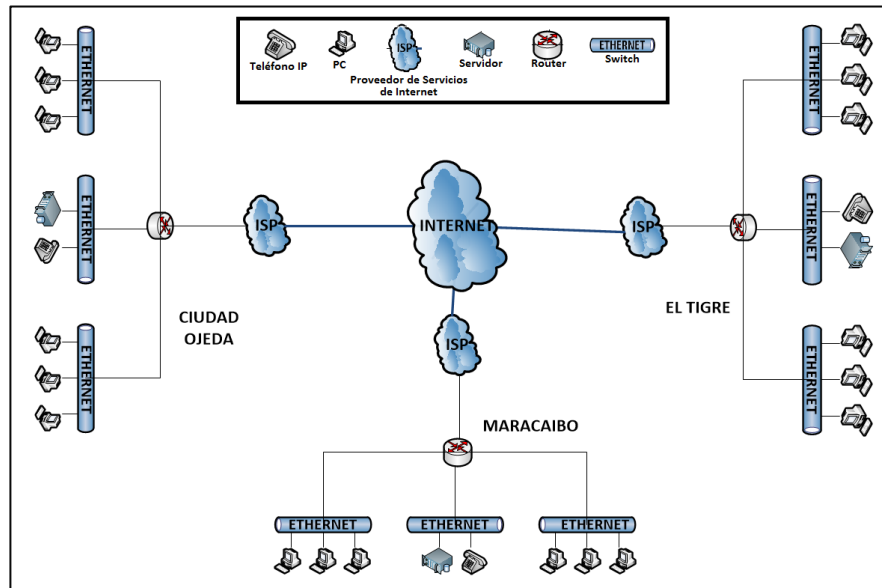
En ese orden de ideas, las técnicas e instrumentos utilizados fueron la observación directa, entrevista no estructurada y revisión documental. En ese sentido, según Hernández y otros (2014) la observación directa es aquella en la cual el investigador puede observar y recoger datos mediante su propia observación. Existe la observación intersubjetiva, basada en el principio de que observaciones repetidas de las mismas respuestas por el mismo observador deben producir los mismos datos. La misma se llevó a cabo en el departamento de IT de la empresa Equimavenca, ya que es allí donde se encuentra instalada la red de telefonía y de datos.

Por su parte, Fidias (2012) establece que la entrevista no estructurada es una técnica basada en un dialogo o conversación cara a cara, entre el entrevistador y el entrevistado acerca de un tema previamente determinado, de tal manera que el entrevistador pueda obtener la información requerida. Para este tipo de entrevistas, normalmente no se sigue un esquema previo. El contenido, el orden y la formulación dependen del orientador. Exige un alto nivel de calidad del entrevistador. Esta fue aplicada al personal de IT de la empresa Equimavenca ya que son las personas que cuentan con los conocimientos necesarios para llevar de manera correcta el desarrollo de la propuesta.

DISEÑO DE LA RED PROPUESTA

Para la propuesta planteada se determinó que la red cuenta con un diseño de topología lógico y físico, con el fin de comprender la manera en que los hosts se comunican entre sí, a través de los medios físicos. La topología lógica utilizada en dicho diseño está fundamentada sobre la tecnología Ethernet, donde cada host envía los datos a los demás en lo que se conoce como acceso por contienda, atendiendo al primer dispositivo que accede al medio, en otros términos por orden de llegada. (Ver figura 1).

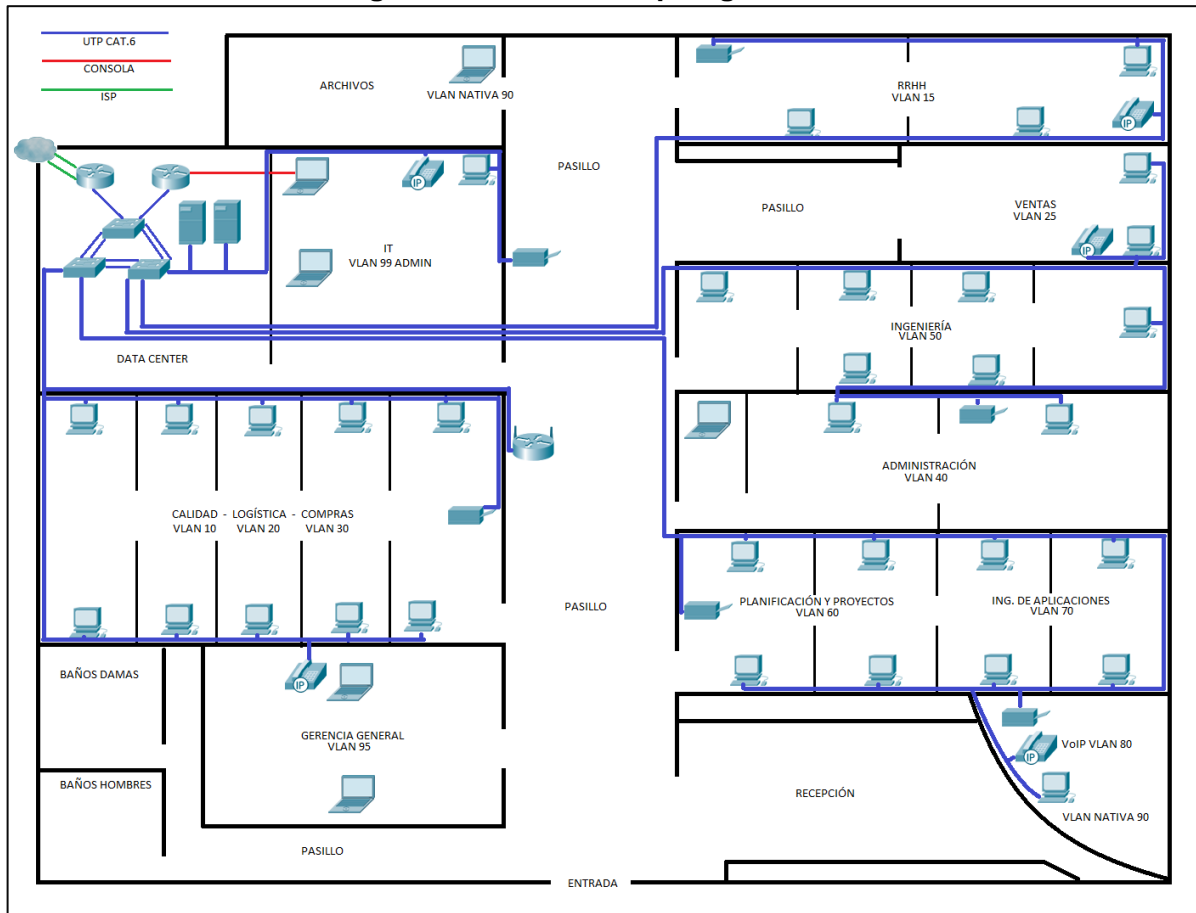
Figura 1. Diseño de Topología lógica



Fuente: Elaboración propia (2015).

En el caso del diseño de la topología física se considera de tipo híbrida, ya que esta es una de las más frecuentes y se deriva de varios tipos de topologías de red, como por ejemplo: árbol, estrella – estrella, bus – estrella, entre otras. En este caso se le considera como híbrida porque está compuesta de varias topologías en estrella, en la cual todos los nodos se conectan a un nodo central y en el caso de que un nodo falle la red sigue funcionando, excepto si el nodo central llega a fallar. (Ver figura 2).

Figura 2. Diseño de Topología física



Fuente: Elaboración propia (2015).

De igual forma, la red cuenta con un conjunto de protocolos que se configuraron para que esta funcione de manera adecuada, mitigando las tormentas de difusión, proporcionando redundancia de capa 2 y capa 3, seguridad, administración remota, ahorro de ancho de banda, velocidad de transmisión, enrutamiento y servicios que permiten que la red funcione de manera eficiente. Las configuraciones realizadas son las mismas para cada sede de la empresa Equimavenca, ya que en sus tres sedes esta cuenta con la misma topología y misma cantidad de dispositivos intermedios, tales protocolos y configuraciones se mencionan a continuación:

(VTP) VLAN Trunking Protocol: Es un protocolo de mensajería de capa 2 que permite reducir la administración en una red conmutada. Cuando se configura una VLAN en un switch que previamente ha sido configurado como servidor VTP, automáticamente esta se distribuye por todos los switches del dominio, reduciendo la necesidad de configurar la misma VLAN en cada uno de los switches, para esto se debe configurar el resto de los switches como clientes VTP. Esto permite agilizar la gestión de los mismos debido a que

se mantiene una coherencia en la administración a través de un dominio de administración común, permitiendo suprimir o realizar cambio de nombres de las VLAN'S por medio de un switch principal.

Asimismo, se ha utilizado el STP o Spanning Tree Protocol: El protocolo de árbol de expansión el cual será configurado bajo el protocolo (PVST+ rápido) Rapid Spanning Tree Protocol, basado en el estándar IEEE 802.1w. El mismo brinda una mayor velocidad de convergencia que otros protocolos y proporciona a la red redundancia controlada de capa 2, es decir, crea una sola ruta lógica entre los destinos de la red y bloquea de forma intencional las rutas redundantes con el fin de evitar bucles en la red. En este protocolo se debe configurar un switch como root-bridge o puente raíz, el cual será utilizado como punto de referencia para realizar los cálculos de las rutas.

De esta manera se pueden controlar los inconvenientes que surgen de la redundancia, como son la duplicidad de tramas, debido a que existen dos medios para la transmisión y ambos se encuentran en uso, lo que genera que se dupliquen. Inconsistencia en la tabla de direcciones MAC, lo que se produce debido a que se tienen varios medios de envío y recepción para las tramas, el switch mantiene un cambio constante en la tabla MAC, lo que produce una inconsistencia y por último las tormentas de difusión, que son generadas cuando existe un bucle en la red, provocando daños severos.

Hot Standby Routing Protocol (HSRP): El protocolo de enrutamiento de reserva activa utiliza enrutador en estado activo y otro de reserva, cuando el activo falla el de reserva toma el control, de esta manera ofrece redundancia de capa 3. Implementado mayormente en la capa de distribución de los modelos jerárquicos. HSRP utiliza una dirección IP y una dirección MAC virtual donde el enrutador de respaldo o reserva asume el control, en caso de que el enrutador principal o activo falle, asimismo, cuando el activo restablece su funcionamiento, el de reserva asume su estado de reserva nuevamente.

Etherchannel: Consiste en agrupar varios enlaces físicos y convertirlos en un solo enlace lógico o canal de puertos, esto con la finalidad de proporcionar balanceo de carga, redundancia y mayor ancho de banda, etherchannel permite agrupar hasta 8 puertos en los que se suma la velocidad nominal de cada puerto físico, lo que permite obtener un enlace troncal de alta velocidad.

En la topología propuesta, se configuró solo 2 puertos Fast Ethernet de 100 Mbps c/u entre cada switch lo que da como resultado un enlace lógico de 200 Mbps en cada enlace troncal. Esta configuración se realizó a través del protocolo Link Aggregation Control Protocol (LACP), del estándar IEEE 802.3ad, el cual es un protocolo de agregación de enlaces abierto, es decir, que puede ser configurado en dispositivos intermediarios de capa 2 de fabricantes distintos a CISCO.

Skinny Call Control Protocol (SCCP): A través de este protocolo propietario de CISCO se realizó la configuración de los servicios de telefonía IP y Call Manager en el enrutador en el cual un cliente skinny (teléfono VoIP CISCO 7960), utiliza TCP/IP para conectarse y para el tráfico de datos, es decir, flujo de datos de audio en tiempo real son utilizados los protocolos RTP/UDP/IP.

Seguidamente, se procedió con la activación del servicio de telefonía por medio de (CME) Cisco Unified Call Manager Express, debido a que esta es una versión más ligera que basada en servidores. (CM es utilizado en servidores dedicados mientras que CME se utiliza en enrutadores). Luego se dio inicio a la creación de los números de directorio seguido de la configuración de los teléfonos.

Open Shortest Path First (OSPFv2): Es el protocolo de enrutamiento dinámico que permitirá a la red de la empresa comunicarse con redes remotas, y una de sus ventajas que más resalta es que es un protocolo abierto, lo que permite que pueda haber convergencia entre enrutadores de distintos proveedores. En el proceso de configuración se inició activando el proceso OSPF y asignándole un número de proceso, cuyo número debe ser el mismo en todos los enrutadores que conforman la topología, luego se realizó la configuración de interfaces pasivas, lo que permite que el enrutador no envíe paquetes de propagación de redes a través de las interfaces que no se encuentran conectadas a otras redes remotas. Asimismo, se declararon las redes conectadas al enrutador donde se especificó la dirección de la red, seguida de su wildcard y el área a la que pertenecía.

Este procedimiento se realizó en todos los enrutadores que conformaban la topología WAN para una efectiva convergencia entre los dispositivos y que pudieran establecer adyacencias entre ellos, es decir, reconocerse como vecinos. Aunado a esto se configuró una autenticación denominada MD5, permitiendo intercambiar paquetes de OSPF, entre los dispositivos con la misma contraseña.

Por consiguiente, se aplicó el NAT (Network Address Translation): El cual, permitió la traducción de direcciones IP internas (privadas) hacia externas (públicas), empleando aquellas direcciones suministradas por los proveedores de servicios de internet (ISP). Dicha configuración se realizó con la finalidad de que los dispositivos finales (hosts, teléfonos VoIP, servidores, entre otros) pudieran conectarse a internet mediante la dirección IP privada (asignada por el servidor DHCP) a través de una dirección IP pública.

En el caso de la empresa, contaba con cuatro (4) direcciones IP que fueron arrendadas al ISP, por lo tanto, debido a la poca cantidad de direcciones se configuró un NAT con sobrecarga (PAT - Port Address Translation, por sus siglas en inglés). Esto permitió que direcciones IP privadas pudiesen utilizar mediante los números de puertos, utilizar una dirección pública para distintas conexiones a internet.

Secure Shell (SSH): Permite realizar conexiones remotas a dispositivos de manera segura, debido a que este protocolo utiliza cifrado en la comunicación, lo que proporciona mayor seguridad a diferencia de telnet que es un protocolo que también permite las conexiones remotas pero ha sido sustituido por SSH a causa de que este no proporciona seguridad en la comunicación. En la topología se configuró SSH con la finalidad de brindar acceso remoto a los enrutadores y switches que conformaban la red WAN, lo que otorgó flexibilidad y seguridad en la administración de los mismos.

Adicionalmente, como complemento a los servicios y protocolos configurados en la topología, un factor importante en una red es la segmentación, ya que esta permite mejorar el tráfico de la red, agrupando un grupo de hosts en segmentos, lo que da como

resultado que cuando un host intente comunicarse con otro host que se encuentre dentro de la misma red, el paquete solo será retransmitido a los dispositivos pertenecientes a ese segmento, evitando de esa manera la propagación por toda la red de dicho paquete consumiendo ancho de banda de manera innecesaria.

En la topología propuesta se realizó la segmentación a través de VLAN, lo que permite a su vez tener un mejor control sobre los hosts que conforman la red. Para que pueda existir comunicación entre VLAN'S distintas se debe contar con un dispositivo intermediario de capa 3 (capa de red del modelo OSI), en donde dicho dispositivo procede a realizar un encapsulamiento del paquete proveniente de una VLAN, en dicho encapsulamiento se le agrega un etiquetado donde indica que el paquete debe ser reenviado a una VLAN en específico, ignorando al resto de las VLAN'S, esto es posible haciendo uso del estándar IEEE 802.1Q el cual se configuró con el fin de crear enlaces troncales para la comunicación entre VLAN'S.

Asimismo, se realizó en el router la configuración de un método para enrutamiento entre VLAN'S denominado Router-on-a-Stick. Este método consiste en utilizar una interfaz del enrutador y configuración sub-interfaces lógicas, según a la cantidad de VLAN'S con las que cuente la topología, permitiendo de esta manera realizar el enrutamiento del tráfico con etiqueta (tráfico perteneciente a una VLAN) y el tráfico sin etiqueta (tráfico que pertenece a la VLAN nativa). Dicho método tiene como desventaja el consumo de recursos en el dispositivo, mientras mayor sea la cantidad de sub-interfaces mayor será el uso de recursos, sin embargo es el método de enrutamiento más utilizado debido a su vigencia, disminución de los costos asociados a interfaces reales y efectividad.

Luego de haber culminado la segmentación, se realizó un esquema de direccionamiento que permite asignar la cantidad de direcciones IP necesarias con el fin de no desperdiciar las mismas y tener un control de estas. Para ello se hizo uso de Máscara de Longitud Variable (VLSM), donde se realizó el cálculo de la máscara de subred de cada segmento determinando que cantidad de direcciones serán asignadas a dichos segmentos. (Ver cuadro 1).



Cuadro 1. VLSM. Distribuci n de subredes

-	VLAN 10	VLAN 20	VLAN 30
Red	172.16.10.0/28	172.16.20.0/28	172.16.30.0/28
Primera	172.16.10.1	172.16.20.1	172.16.30.1
�ltima	172.16.10.12	172.16.20.12	172.16.30.12
Broadcast	172.16.10.13	172.16.20.13	172.16.30.13
Hosts	16-2=14	8-2=6	8-2=6
-	VLAN 40	VLAN 50	VLAN 60
Red	172.16.40.0/28	172.16.50.0/28	172.16.60.0/28
Primera	172.16.40.1	172.16.50.1	172.16.60.1
�ltima	172.16.40.12	172.16.50.12	172.16.60.12
Broadcast	172.16.40.13	172.16.50.13	172.16.60.13
Hosts	16-2=14	16-2=14	16-2=14
-	VLAN 70	VLAN 80	VLAN 90
Red	172.16.70.0/28	172.16.80.0/28	172.16.90.0/28
Primera	172.16.70.1	172.16.80.1	172.16.90.1
�ltima	172.16.70.12	172.16.80.12	172.16.90.12
Broadcast	172.16.70.13	172.16.80.13	172.16.90.13
Hosts	16-2=14	16-2=14	16-2=14
-	VLAN 95	VLAN 99	VLAN 15
Red	172.16.10.0/28	172.16.10.0/28	172.16.10.0/28
Primera	172.16.95.1	172.16.99.1	172.16.15.1
�ltima	172.16.95.12	172.16.99.12	172.16.15.12
Broadcast	172.16.95.13	172.16.99.13	172.16.15.13
Hosts	16-2=14	16-2=14	16-2=14
-	VLAN 25		

Red	172.16.25.0/28	/28 = 255.255.255.240	
Primera	172.16.25.1		
Última	172.16.25.12	Sumarizadas = 172.16.0.0 /17	
Broadcast	172.16.25.13		
Hosts	16-2=14	/17 = 255.255.128.0	

Fuente: Elaboración Propia (2015).

Para proporcionar seguridad a la red se realizó la configuración de lista de control de acceso (ACL), lo que permite controlar el flujo de tráfico entre los enrutadores y switches. El objetivo principal de una ACL es filtrar el tráfico de red, permitiendo o denegando el mismo de acuerdo a las sentencias o instrucciones que sean anexadas a la lista. En el caso de la topología presentada se configuró una lista de control de acceso extendida, denegando la comunicación a través del protocolo ICMP, es decir, denegar PING por parte de equipos pertenecientes a redes remotas hacia los hosts pertenecientes a la red y a los servidores de las mismas. Sin embargo, se permitirá el acceso a los servidores web a través del protocolo HTTP por medio del puerto 80, asimismo, será posible conectarse a redes externas, (Internet). Para esto se utilizaron listas de control de acceso extendidas.

Como complemento a las configuraciones de las políticas de seguridad, se tomó la decisión de proteger el acceso a la consola de los dispositivos intermediarios, asignándole una contraseña a cada línea vty (virtual) de los enrutadores y switches, lo que significa que para acceder a la interfaz de línea de comandos (CLI), se debe ingresar un nombre de usuario y una contraseña que solo el personal del departamento de IT debe conocer.

La configuración se hizo con el fin de dar a conocer los comandos necesarios para lograr dicha característica de seguridad, haciendo uso de una contraseña y nombre de usuario elegidos al azar, sin embargo, esta puede estar sometida a cambios por parte del personal de IT con el fin de conservar la privacidad de la misma. Luego de realizar las configuraciones de protección de consola, se procedió a encriptar el usuario y contraseña con el fin de que estos datos no puedan ser descifrados por algún usuario externo.

Como medida de seguridad física a los dispositivos intermediarios se activó la función de seguridad de puertos que permite desactivar los puertos del switch que tengan configurado port-security, en este caso se realizó la configuración con el fin de que el switch a través de un puerto se aprenda la dirección MAC de un host y luego, si se llega a conectar un host distinto al puerto configurado este se desactiva, impidiendo que equipos no autorizados accedan a la red, haciendo más robusta las políticas de seguridad de la red.

VIABILIDAD DE LA PROPUESTA

La propuesta es técnicamente factible debido a que cada dispositivo cuenta con un sistema operativo totalmente compatible con las funciones, servicios y protocolos ya mencionados, los dispositivos intermediarios cuentan con IOS versión 12.4, los dispositivos finales tales como PC's y servidores cuentan con sistemas operativos de Windows lo que permite hacer uso los recursos de la red y sacar el mayor provecho a los dispositivos, asimismo, permite la interconexión ente los mismos.

Es factible a nivel operativo debido a que el manejo de los dispositivos continúa siendo el mismo, es decir, simple para el usuario que ya labora en la empresa. En el caso de los dispositivos de networking, el personal del departamento de IT recibió las configuraciones de cada dispositivo las cuales se muestran en las páginas anteriores, permitiendo de esa manera la posibilidad de estudiar y mejorar las configuraciones realizadas con el fin de mejorar los servicios de la red.

La propuesta es factible económicamente, ya que no es necesario realizar una inversión elevada, ventaja que tiene la empresa al contar con mayor parte de los dispositivos a utilizar, entre ellos enrutadores, switches y dispositivos finales, permitiendo poner en funcionamiento la red WAN solo manteniendo el costo del arrendamiento de los enlaces que interconectan las sucursales y que conforman dicha red. Sin embargo, se muestra a continuación el costo de la inversión en caso de no contar con los dispositivos.

Cuadro 2. Costo por cada sede

Cantidad	Tipo	Modelo	Precio BsF	Sub-Total
02	Router	CISCO 9800	70.000	140.000
03	Switch	CISCO catalyst 2960	65.000	195.000
05	Teléfono IP	CISCO 7960	39.999	199.995
Total = 534.995				

Fuente: Elaboración propia (2015).

Cuadro 3. Costo total (3 sedes)

Cantidad	Tipo	Modelo	Precio BsF	Sub-Total
06	Router	CISCO 9800	70.000	420.000
09	Switch	CISCO catalyst 2960	65.000	585.000
15	Teléfono IP	CISCO 7960	39.999	599.985
Total = 1.604.985				

Fuente: Elaboración propia (2015).

CONCLUSIONES

En la actualidad, las medianas y grandes organizaciones poseen plataformas tecnológicas robustas que les permiten el manejo de información de manera rápida,

estable y segura, permitiendo así brindar servicios de calidad y funcionar de manera óptima. Los dispositivos de red que conforman dichas plataformas pueden ser configurados con la finalidad de brindar redundancia, control en la transmisión de datos, seguridad, acceso remoto, entre otros beneficios tales como los que fueron mencionados en la investigación.

Se logró caracterizar el protocolo OSPFv2 de CISCO a fin de determinar sus fortalezas en virtud de ser utilizado para la transmisión de voz y datos entre cada una de las sucursales de la empresa objeto de estudio. Se observó que el mismo provee la arquitectura necesaria para soportar el tráfico de paquetes entre las sedes; brindando estabilidad y eficiencia a la red de la organización.

Mediante un software simulador provisto por Cisco (Packet Tracer V. 6.0) para representar el comportamiento de la red propuesta; logrando establecer comunicación tanto de voz como datos entre los nodos de la misma, de acuerdo a las tablas VLSM. Debe notarse la existencia de las VLANS que permiten dividir lógicamente la red, reduciendo los tamaños de difusión, favoreciendo la administración de la misma. Por consiguiente, la distribución en subredes se ha realizado de forma tal que se optimice el tráfico de paquetes, dejando holguras para la inclusión de hosts en casos de expansión de las unidades funcionales de la empresa.

Como complemento a lo anterior, se presentó una propuesta totalmente funcional, con características de estabilidad, escalabilidad, seguridad y confiabilidad, requeridas para un entorno de red WAN. Asimismo, se evidenció el uso de tecnología actualizada, dentro de los estándares más recientes del mercado, dentro de las posibilidades del contexto venezolano. Lo anterior se evidencia a través del estudio de factibilidad realizado en las tres sedes involucradas. Igualmente, se recomienda la implementación del diseño de red que se ha presentado, ya que se reducirán costos en telefonía convencional, brindando grandes ventajas tales como automatización de procesos críticos de la organización, mayor seguridad, optimización de la velocidad de procesamiento, entre otros factores, permitiendo de esta manera un desempeño adecuado en las sedes que han sido objeto de estudio.

REFERENCIAS BIBLIOGRÁFICAS

- Ariangelo, E. y Barrientos, E. (2011). Redes CISCO CCNP, Guía de Estudios para certificación CCNA 640.802. México. RA-MA, S.A. Editorial y Publicaciones.
- Fidias, A. (2012). El Proyecto de Investigación. Introducción a la metodología científica. Venezuela. Editorial Episteme.
- Hernández, R. Fernández, C. y Baptista, P. (2014). Metodología de la Investigación. Venezuela. McGraw-Hill Education.
- Huidobro, J. (2010). Telecomunicaciones: Tecnologías, redes y servicios. México. RA-MA, S.A. Editorial y Publicaciones.



Odom, W. (2016a). CCENT/CCNA ICND1 100-105 Official Cert Guide. United States of America. Cisco Press.

Odom, W. (2016b). CCNA Routing and Switching ICND2 200-105 Official Cert Guide. United States of America. Cisco Press.