IMPLEMENTACIÓN DE TECNOLOGÍA IPV6 PARA LA INFRAESTRUCTURA CONVERGENTE DE LA CLOUD EMPRESARIAL SONDA DE COLOMBIA S.A.

CHRISTIAN LEONARDO BERNAL GUTIERREZ

ESCUELA TECNOLÓGICA INSTITUTO TÉCNICO CENTRAL

INGENIERÍA DE SISTEMAS

BOGOTÁ

2015

IMPLEMENTACIÓN DE TECNOLOGÍA IPV6 PARA LA INFRAESTRUCTURA CONVERGENTE DE LA CLOUD EMPRESARIAL SONDA DE COLOMBIA S.A.

CHRISTIAN LEONARDO BERNAL GUTIERREZ

Cód. 113103

PROYECTO DE GRADO

Asesor:

Ing. CARLOS VELASQUEZ

ESCUELA TECNOLÓGICA INSTITUTO TÉCNICO CENTRAL

INGENIERÍA DE SISTEMAS

BOGOTÁ D.C. 2015

AGRADECIMIENTOS

Este proyecto de grado va dedicado principalmente a mis papas, que me han apoyado e instruido durante toda mi etapa de educación, siendo el mayor apoyo que pude tener, a mi familia que me motiva a ser cada día mejor, también nuestro asesor Ing. Carlos Velásquez quien me orientó en el transcurso de la implementación del proyecto, a los docentes que me motivaron a seguir en este camino de las telecomunicaciones sin importar la orientación de la mayoría y a Sonda de Colombia por darme la oportunidad de utilizar su infraestructura para el desarrollo del proyecto y compañeros de carrera y todas las personas allegadas que brindaron su apoyo para lograr el 100% de esta meta y sobre todo a Dios que me ha dado la vida y la sabiduría para llevar a cabo las metas que me he propuesto, como esta.

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Jurado

_____

Jurado

Bogotá D.C. ___ De Septiembre de 2015

TABLA DE CONTENIDO

LISTA DE ILUSTRACIONES

LISTA DE ANEXOS

GLOSARIO[1]

ADSL: Hace referencia a la expresión Asymmetric Digital Subscriber Line es una clase de tecnología que permite la conexión a Internet mediante el uso de la línea telefónica tradicional.

BACKBONE: Es llamado backbone al lugar físico donde se encuentran las principales conexiones troncales de Internet la cual está compuesta de un gran número de routers interconectados con la capacidad de llevar los datos a través de la red mediante fibra óptica.

DATAGRAMA: Conjunto estructurado de bytes que forma la unidad básica de comunicación del protocolo.

DIRECCIÓN: Identificador asignado a nivel de la capa de red a un interfaz o conjunto de interfaces que puede ser empleado como campo de origen o destino en datagramas IPv6.

DIRECCIÓN MAC: Es un identificador de 48 bits (3 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo. Está determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits) utilizando el Organizationally Unique Identifier.

DOMINIO: Un dominio es la parte de una URL (dirección de una página o recurso en internet) por la que se identifica al servidor en el que se aloja.

FLUJO: Una serie de datagramas intercambiados entre una fuente y un destino que requieren un tratamiento especial en los routers intermedios, y definidos por

---

[1] Glosario términos AbaNet – [En línea] http://www.abanet.net/glosario.html [Citado Agosto – 2015]

una dirección IP origen y destino específico, así como por una etiqueta de flujo con un valor distinto a 0.

FRAGMENTACIÓN: Proceso por el que se divide la carga de un datagrama IPv6 en fragmentos por la máquina emisora, de modo que todos los fragmentos tienen una MTU apropiada al camino a seguir hasta el destino.

GATEWAY: Equipo encargado de proporcionar los servicios a un host.

INTERFAZ: Una representación de un nexo físico o lógico de un nodo a un enlace. Un ejemplo de un interfaz físico es una interfaz de red. Un ejemplo de un interfaz lógico es un interfaz de un túnel.

MIP: El Protocolo MIP (Mobile Internet Protocol) suministra una serie de extensiones al protocolo IP estándar definido por la IETF, se especializa en permitir a los usuarios que se registren en redes externas y se conecten a su red propietaria a través de la combinación de un FA (Foreing Agent) y un HA (Home Agent), MIP es usado como mecanismo de movilidad en las redes no-3GPP. [2]

MPLS (MultiProtocol Label Switching) es un método de reenvío de paquetes de alta performance que se asienta en el agregado de una etiqueta al paquete IP en base a la cual se hará el reenvío de paquetes con una mínima sobrecarga por búsqueda de rutas el cual está definido en el RFC 3031.[3]

NODO: Espacio real en el que confluyen parte de las conexiones de otros espacios reales o abstractos que comparten sus mismas características y que a su vez también son nodos. Todos estos nodos se interrelacionan entre sí de una

---

[2] Protocolo MIP – [En línea] http://wikitel.info/wiki/MIP [Citado Agosto -2015]

[3] MPLS – [En linea] http://*catarina.udlap.mx/u_dl_a/tales/documentos/lis/...d_l/capitulo2.pdf* [Citado Agosto -2015]

manera no jerárquica y conforman lo que en términos sociológicos o matemáticos le llamamos red.

PAQUETE: Unidad fundamental de trasporte de información en todas las redes de cómputo. Un paquete está generalmente compuesto de tres elementos: Una cabecera (header) que contiene generalmente la información necesaria para trasladar el paquete desde el emisor hasta el receptor, el área de datos (payload) que contiene los datos que se desean trasladar, y la cola (trailer), que comúnmente incluye código de detección de errores.

PMIP: Es un protocolo de gestión de la movilidad basada en la red estandarizada por IETF y se especifica en el RFC 5213, se trata de un protocolo para la construcción de una tecnología común y acceso independiente de redes centrales móviles, con capacidad para varias tecnologías de acceso tales como WiMAX, 3GPP, 3GPP2 y WLAN arquitecturas de acceso basados. Proxy Mobile IPv6 es el único protocolo de gestión de la movilidad basada en la red estandarizada por IETF.[4]

PON: Sistema de comunicaciones por fibra óptica en el que se establece una comunicación punto-multipunto entre un router central denominado en estos montajes OLT (optical line Terminal) Terminal óptico de línea y los equipos en campo ONT (optical Network Terminal) Terminal óptico de red. Es decir, el ancho de banda no es dedicado, sino multiplexado en una misma fibra en los puntos de acceso de red de los usuarios.

POP: (*Post Office Protocol*) es utilizado por clientes de correo locales instalados en la PC para obtener los mensajes de correo electrónico almacenados en un servidor remoto y transferirlos al almacenamiento de la PC.

---

[4] PMIP [En línea] - www.cisco.com/c/en/us/.../**pmip**_20.pdf *citado [Agosto - 2015]*

PROTOCOLO: Este es el procedimiento (conjunto de pasos, mensajes, forma de los mensajes y secuencias) que se utiliza para mover la información de una localización a otra sin errores.

RFC (REQUEST FOR COMMENTS): Documento de especificaciones que se expone públicamente para su discusión.

ROUTER: Es un dispositivo hardware o software de interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras.

SWITCH CORE: Es el switch núcleo de una red, sirve como puerta de enlace para los demás switches de distribución y es el encargado de manejar el root del protocolo spanning tree de una red LAN.

TUNNELING: Encapsulado de un protocolo IPv6 dentro de un protocolo IPv4 o viceversa.

UPSTREAM PROVIDERS: Se denomina usualmente un Upstream Provider como un gran ISP proveedor de acceso a internet a otro ISP Local. [5]

---

[5] *Upstream Providers [En línea]* www.diyisp.org/dokuwiki/doku.php?id...upstream *[Citado Agosto de 2015]*

INTRODUCCIÓN

IPv4 nace como protocolo de internet en septiembre de 1981 y es definido en el RFC 791[6] por el instituto de ciencias de la información de la Universidad de California, este protocolo cuenta con una longitud de 32 bits lo que equivale a 4.294.967.296 de direcciones IP para todo el mundo. Lo que para aquella época se imaginaba que era el número ideal para todos los equipos con conexión a internet a nivel mundial que podrían llegar a existir a futuro; ya que en el momento no se contaba con la cantidad suficiente de computadores o dispositivos que se conectaran a la red, para que se agotara el número de direcciones IP, puesto que para el año de 1984 eran de aproximadamente 1000 los equipos conectados a la red.[7]

En un inicio solo los computadores podían tener acceso a la red ya que eran los únicos dispositivos con los medios físicos para poder conectarse, en el transcurso de los años y a los avances tecnológicos, diferentes dispositivos y equipos se pueden conectar a la red, en la actualidad se pueden ver smartphones, televisores, relojes entre otros dispositivos conectados a internet, este es un panorama que para el protocolo IPv4 no es favorable, ya que las direcciones IP se acabaron totalmente desde el jueves 3 de febrero de 2011 según la IANA[8] (Internet Assigned Numbers Authority) y para evitar este agotamiento de direcciones IP se ha debido utilizar una serie de estrategias como por ejemplo NAT (referenciado en el punto 2.2.1 IPv4) y subnetting. Como solución a este problema de agotamiento de direcciones IP, se creó bajo el RFC 2460 en diciembre de 1998 el protocolo de comunicaciones IPv6 el cual cuenta con 340 sextillones de direcciones IP, direcciones suficientes para todos los dispositivos que se conectan a la red a nivel mundial y que se pueden llegar a conectar en un

---

[6] [RFC-791] Jon Postel., "INTERNET PROTOCOL", RFC 791, Septiembre 1981.

[7] Information Society Breve historia de internet - Septiembre 2012 [citado Septiembre 2015]. Disponible en http://www.internetsociety.org/es/breve-historia-de-internet

futuro lejano, además del aumento de direcciones IP el protocolo IPv6 cuenta con una serie de ventajas como lo son QoS, seguridad, encriptación de los datos, asignación de dirección IP más simple, mejor capacidad de autenticación.

En Colombia son pocas las empresas que tienen su red interna con tecnología IPv6 simplemente porque algunas no han visto aun la necesidad de realizar una migración de IPv4 – IPv6, o las empresas que conocen la necesidad de la migración y las ventajas no cuentan con el conocimiento o el personal capacitado para la realización de la transición, para ver las empresas que en la actualidad cuentan con implementación de protocolo IPv6 en Colombia puede revisar a detalle en el punto 2.1 *Antecedentes.*[8]

Sonda de Colombia S.A. al ser una multinacional líder en servicios IT en busca siempre del progreso y de la innovación hacia sus clientes y servicios, se propone a través de este proyecto la implementación del protocolo de telecomunicaciones IPv6 en paralelo a IPv4 para la publicación de servicios web, gestión de equipos internos y diferentes servidores como SSH, FTP en la Cloud empresarial con el fin de permitir la comunicación con otras redes IPv6, y dar cumplimiento a las exigencias del sector del gobierno .

Para que así la nube privada de la compañía, pueda ofrecer conectividad IPv6 a todas las entidades realicen este tipo de requerimientos para futuros proyectos en el portal Colombia compra eficiente http://www.colombiacompra.gov.co/es y así no quedar en desventaja con la competencia del mercado.

Este proyecto se plantea para anteponerse al agotamiento de direcciones IPv4, y para que en el momento que se requiera una transición total de tecnología sea más fácil llevarla a cabo ya que se contara con cierta experiencia en el tema.

[8] - IPv6 Portal. ¿Quiénes implementan? [en línea]. http://portalipv6.lacnic.net/quienes-implementan/ [Citado 19 de enero de 2015].

1. PROBLEMA DE INVESTIGACIÓN

1.1 PLANTEAMIENTO

1.1.1. Descripción del Problema

El protocolo de internet IPv4 ha estado definido desde el año 1981 en el RFC 791 en esta época no se pensaba que este número de direcciones IP disponibles en algún momento se fuera a acabar, puesto que eran pocos los equipos que estaban conectados a la red, en su mayoría eran universidades, las cuales empezaron con la iniciativa de internet; pocas de estas tenían equipos o infraestructura para apoyar este proyecto.

En la actualidad donde cada persona cuenta con más dispositivos que se conectan a la red y por consiguiente ocupan más de una dirección IP como los celulares, relojes, carros entre otros; debido a este avance tecnológico las direcciones IPv4 año tras año se fueron agotando por diferentes factores como la demografía de internet, la cual ha aumentado pues la mayoría de los hogares de países industrializados cuentan con servicio a internet.

Este agotamiento de direccionamiento también fue causado por el uso ineficiente de direcciones ya que en un comienzo en los años 80 cuando se asignaron las diferentes direcciones IP a muchas compañías grandes o universidades se les entregaron bloques de direcciones clase A que cuentan con 16 millones de direcciones IP, malgastando las direcciones IP, en el año 2011 la IANA (Internet Assigned Numbers Authority) asignó los últimos bloques libres de direcciones al Registro Regional de Internet el cual está subdividido en cinco autoridades encargadas de asignar las direcciones IP a los ISP por continente, por tal motivo las últimas direcciones IP públicas ya han sido asignadas o quedan muy pocas en poder de los RIRs los cuales son el registro regional de internet quienes entregan

el direccionamiento tanto IPv4 como IPv6 a los diferentes proveedores de internet a nivel mundial.

En vista de esta problemática se plantea la siguiente versión de protocolo IP llamada IPv6 la cual contiene direcciones IP interpretadas en formato hexadecimal y nos permite aproximadamente 340 sextillones de direcciones buscando una dirección única sin necesidad de utilizar subredes para cada uno de los dispositivos en el mundo aumentando la seguridad y proporcionando diferentes ventajas en comparación a su predecesor IPv4. Además un punto a favor de la implementación de IPv6 es que no es necesario el cambio de equipos de ningún tipo en cualquier entorno en el que se requiera hacer una migración a esta nueva versión de protocolo de internet, la cual se quiera o no en pocos años va a coger más fuerza, hasta el punto en el que todos a nivel mundial utilicemos IPv6 para comunicarnos en la red.

SONDA DE COLOMBIA S.A, al implementar esta tecnología quedaría en ventaja con cualquier proveedor de nube pública y/o privada de la competencia que en el momento no cuente con este servicio, dado que puede ser un factor diferencial al momento de decidir una contratación de millones de dólares en IaaS (Infrastructure as a Service - Infraestructura como servicio).

1.1.2. Formulación del Problema

¿Cuál es la mejor manera de realizar la transición de direccionamiento IPv4 – IPv6 soportando los servicios actualmente publicados en la red Cloud de Sonda S.A.?

1.2 JUSTIFICACIÓN.

La mayoría de las redes e infraestructuras internas a nivel corporativo de las diferentes empresas en Colombia cuentan con direccionamiento IPv4 por diferentes factores y causas que facilitan tareas como mantenimiento, escalabilidad, facilidad de uso, documentación, fácil configuración, tradición de uso entre otras, además porque la utilización de direccionamiento IPv6 no es tan común o por temor, falta de conocimiento no es aplicado en las redes LAN de las empresas, por otro lado la mayoría de las empresas no conocen la necesidad de la realización de una migración IPv4 - IPv6, además se desconoce la nomenclatura que se utiliza en este tipo de protocolo, compatibilidad con los demás protocolos de conexión, seguridad de implementación y carencia de personal idóneo, con experiencia que pueda realizar la migración entre protocolos, por estos y otros motivos no se llevan a cabo migraciones y muchos cambios a nivel tecnológico en las empresas.

Pero Sonda de Colombia S.A. como empresa líder en servicios IT en busca del desarrollo tecnológico y de promover el conocimiento se interesa por cada día estar al tanto de los últimos avances tecnológicos y poder aplicar estas mejoras a su infraestructura interna para poder mostrar una mejor imagen ante sus actuales y futuros clientes, permite y motiva la migración de IPv6 en su cloud empresarial, infraestructura ubicada en el Datacenter de Level 3, buscando de alguna manera tomar la iniciativa y apoyar la migración de IPv4 a IPv6; como lo hacen algunas empresas en su red interna. Por consecuencia en el momento en que se deba realizar una migración total en la red empresarial en unos cuantos años ya existirán pruebas realizadas en ambientes real, existirá personal capacitado y documentación sobre protocolo de internet IPv6 lo cual facilitará la tarea y hará más amena y menos tediosa la migración a IPv6 y por ende con menos consecuencias y afectando de la menor manera a los clientes y redes internas.

1.3 OBJETIVOS.

1.3.1 Objetivo General

Implementar tecnología IPV6 para la red Cloud empresarial Sonda de Colombia S.A.

1.3.2 Objetivos Específicos.

- ✓ Identificar los mecanismos de migración de IPv4 a IPv6 que ayudarán a la empresa Sonda de Colombia S.A. a llevar el proceso de la mejor manera.
- ✓ Definir el direccionamiento IPv6 necesario para la configuración de los equipos involucrados en la red convergente.
- ✓ Determinar la manera en la que se va a comunicar protocolos de internet IPv4 – IPv6.
- ✓ Configuración de IPv6 en dispositivos de la red interna firewall, routers, switches, servidores.
- ✓ Verificar comunicación entre dispositivos configurados en IPv6.

1.4 DELIMITACIÓN

1.4.1 Alcance

Publicar los servicios implementados en la red Cloud de Sonda de Colombia y configurar en dos equipos de la red interna del Cloud sobre IPV6, con la infraestructura actual.

1.4.2 Limitación.

Se realizara la migración de los servicios que actualmente están funcionando sobre IPv4 en la red Cloud de Sonda S.A nombrados a continuación:

- Se debe publicar el https://portalcloud.co.sonda.com por IPV6.
- Se debe publicar la conexión SSH al Core de la red Cloud.
- Se debe realizar la publicación del portal de monitoreo Zabbix de la Cloud.
- Realizar la configuración de dos equipos de la red management mediante IPV6.
- Realizar la configuración IPV6 sin afectar el funcionamiento de las publicaciones realizadas por IPV4.

1.5 VALOR DIFERENCIAL.

Este proyecto servirá como punto de partida del proceso de migración de la Cloud de Sonda S.A. a protocolo IPv6, tomando como primer punto la red management y algunos servicios web publicados en IPv4 para esta migración, en el cual se realizaron las pruebas necesarias tanto en implementación como en desempeño y funcionamiento para obtener la experiencia necesaria y llegar a la finalidad de convertir la Cloud en proveedor de direccionamiento IPV6 público y privado ante sus clientes de servicios en la nube, y poder ofrecer en su catálogo de servicios este nuevo tipo de implementación, que abre una nueva ventana de oportunidades de ventas para la empresa.

2. MARCO REFERENCIAL.

2.1 ANTECEDENTES. [9]

ERT E.S.P S.A: Empresa de Recursos Tecnológicos tiene implementado IPv6 en su red con el prefijo IPv6: 2800:9F0::/32 el cual es anunciado en Internet a través del AS 27845, actualmente se encuentra disponible para todos los suscriptores de conectividad con E.R.T. a través de dual stack, este proyecto también incluirá a los usuarios masivos, corporativos, educativos y gubernamentales poniendo a disposición todo el conocimiento de los ingenieros.

ETB: Está anunciando IPv6 hacia Internet con varios upstream providers conectados en el POP de Miami. En una primera etapa de prueba se utilizan esquemas de túneles. Actualmente se tienen conexiones con Dual-Stack. En una etapa posterior se probará un esquema en modo nativo.
La red MPLS de ETB cuenta con soporte para IPv6 utilizando los RFC correspondientes a 6PE y 6VPE. Permitiendo a los clientes conectar dominios separados de IPv6 a través del Backbone IPv4. En una etapa posterior se probará un esquema en modo nativo

MEDIA COMMERCE TELECOMUNICACIONES: Cuenta con una gran red de fibra óptica en Colombia, brindando acceso a los clientes bajo el protocolo IP, además del transporte nacional con un robusto core MPLS en la modalidad de 6VPE. Con infraestructura que cuenta con soporte IPv6 en su modalidad “Dual Stack” en nuestros equipos de borde y de última milla, facilitando la operación de IPv4 e IPv6 de forma paralela sin inconvenientes. Media Commerce cuenta con

---

[9] IPv6 Portal. ¿Quiénes implementan? [en línea]. *http://portalipv6.lacnic.net/quienes-implementan/* [Citado 19 de enero de 2015].

varios upstream providers y se está anunciando con todos los bloques propietarios de IPv6 de la compañia. Actualmente Media Commerce provee acceso IPv6 a grandes clientes en Colombia.

Telmex Colombia (Claro Fijo Colombia): Tiene implementado y operativo IPV6 para servicios corporativos de internet con el rango 2800:480::/32 (AS 14080). El CORE de Internet soporta dual-stack con 6VPE y se tienen planes de trabajo para el despliegue IPV6 a servicios residenciales y PYMES sobre las plataformas de CABLE DOCSIS y GPON.

UNE EPM TELECOMUNICACIONES: tiene implementado IPv6 dual stack en toda su infraestructura de enrutamiento así como en todos los enlaces de interconexión locales e internacionales, siendo el prefijo: 2800:e0::/28 (AS 13489) actualmente IPv6 está disponible para todos los clientes de Acceso Dedicado (dual stack) y se está trabajando en el despliegue de IPv6 dual stack en el servicio Banda Ancha en las tecnologías ADSL, CM y PON.

LA UNIVERSIDAD PONTIFICIA BOLIVARIANA, Seccional Bucaramanga, ya tiene implementados bajo IPv6 los servicios de DNS, WEB, las configuraciones en las estaciones de trabajo y en reglas de Firewall, utilizando el rango de direcciones 2801:0:2e0::0/48. El proveedor de servicios que los anuncia a Internet es Level3.

2.2 MARCO TEÓRICO

2.2.1 IPv4. Este protocolo de internet fue diseñado para interconectar sistemas de computadores mediante una red de comunicación por medio de intercambio de paquetes y definido en el RFC0791 de septiembre de 1981, este protocolo de internet brinda los elementos necesarios para la transmisión de datagramas desde un nodo origen a un nodo destino, este protocolo también se encarga de la fragmentación de los datagramas para que pueda ser transmitido.

Este protocolo está basado en dos funciones básicas las cuales son direccionamiento y fragmentación, y en cuatro mecanismos para la utilización de su servicio, tipo de servicio la cual es usada por las pasarelas para seleccionar los parámetros de transmisión dependiendo la funcionalidad de la red, el segundo mecanismo es el tiempo de vida el cual es el límite en el que el datagrama está en internet, el tercer elemento es las opción que incluye recursos para marcas de tiempo, seguridad, encaminamiento especial y como último mecanismo encontramos suma de control de cabecera la cual verifica la información utilizada cuando se procesa un datagrama.

Hay que tener en cuenta que IPv4 no proporciona ningún mecanismo de comunicación fiable, no existen acuses de recibo ni entre extremos ni entre saltos, no hay control de errores para los datos, sólo una suma de control de cabecera, no hay retransmisiones, no existe control de flujo, entre las características más relevantes de IPv4 se encuentran:[10]

[10] - [RFC-791] Jon Postel., "INTERNET PROTOCOL", RFC 791, Septiembre 1981.

- Direcciones IPv4 privadas. Las direcciones IPv4 son aquellos tipos de direcciones que han sido reservadas para la administración de redes privadas, se caracterizan porque manejan un direccionamiento que no permite el acceso a la red pública.

Algunos rangos en el direccionamiento IPv4 fueron reservados para la operación de este tipo de redes. Manejan algo en común a las redes públicas que son únicas e irrepetibles, para permitir la conectividad de los diferentes dispositivos que se encuentren dentro de la red.

- Direcciones reservadas. Las direcciones reservadas son grupos de direcciones que han quedado para un uso específico. Las más importantes son las siguientes:

- 0.0.0.0 (o la dirección .0 de cualquier subred). Esta es la dirección para referirse a la red.
- 255.255.255.255 (o la dirección .255 de cualquier subred). Esta es la dirección de broadcast. Equivale a todos los terminales de la red.
- 127.X.X.X Este es el rango de ip's de loopback. Son para referirnos a nosotros mismos (nuestra máquina). También llamadas de diagnóstico.
- 127.0.0.1 (o local host) Es un caso particular del anterior. Es la más usada para referirnos a nuestra máquina de manera local. [11]

- NAT (Network Address Translation). Para que una red privada tenga acceso a internet, se debe realizar por medio de un dispositivo ubicado en la frontera de las dos redes, que tenga configurado NAT para la traducción de direcciones.

Este dispositivo NAT cambia y traduce la dirección origen en cada paquete de salida y el puerto de origen para que sea único. Estas traducciones de dirección se

---

[11] - [RFC-1918] Y. Rekhter. B. Moskowitz. D. Karrenberg " Address Allocation for Private Internets", RFC 1918, Febrero 1996.

almacenan en una tabla, para recordar qué dirección y puerto le corresponde a cada dispositivo cliente y así saber dónde deben regresar los paquetes de respuesta.

Esto ayuda a garantizar la seguridad, ya que cada petición saliente o entrante debe pasar por un proceso de traducción que ofrece la oportunidad de verificar y autenticar la solicitud. NAT también se conserva en el número de direcciones IP globales que una empresa necesita y permite a la empresa utilizar una única dirección IP en su comunicación con el mundo.[12]

2.2.2 IPv6. El protocolo de Internet versión 6 [RFC2460], es una tecnología que entrará poco a poco a reemplazar a la versión 4, su desarrollo contribuye en la búsqueda de soluciones a las problemáticas existentes en IPv4, esta fue diseñada como la evolución del IPv4 presentando características de seguridad y mejor funcionamiento.

IPv6 se desarrolla a la falta de direccionamiento IP, se desarrolló IPv6, que a inicios de su creación se llamó como: Ping (Protocolo de Internet de Nueva Generación), que promete dar solución a los problemas del direccionamiento, dándole un mejoramiento en capacidad del envío de la información, la seguridad, la facilidad y el rendimiento en los equipos.

La nueva versión del protocolo utiliza direcciones de 128 bits lo cual equivale a tener 2^128 = 340.283.366.920.938.463.463.374.607.431.768.211.456 direcciones IP, que es representado en formato hexadecimal, esta cantidad de nuevas direcciones, podrán ser utilizadas por miles de millones de usuarios que requieran servicios en las diferentes plataformas que necesitan las direcciones IP como, las páginas Web, los dispositivos móviles como teléfonos celulares, PDA´s, dispositivos de consumo, vehículos, nuevas tecnologías de acceso como xDSL.

---

[12] - [RFC-3022] P. Srisuresh. K. Egevang."Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, Enero 2001.

De esta manera esta versión del protocolo permite solucionar el grave problema de direccionamiento que hoy en día se debe enfrentar con la versión 4.[13]

- Capacidades de Direccionamiento Extendida. IPv6 incrementa el tamaño de dirección IP de 32 bits a 128 bits, para dar soporte a más niveles de direccionamiento jerárquico, un número mucho mayor de nodos direccionales, y una autoconfiguración más simple de direcciones. La escalabilidad del enrutamiento multienvío se mejora agregando un campo ámbito a las direcciones multienvío. Y se define un nuevo tipo de dirección llamada anycast, usada para enviar un paquete a cualquiera de un grupo de nodos.

- Simplificación del Formato de Cabecera. Se realizaron algunas modificaciones en el formato de la cabecera de IPv4, siendo para IPv6 más simple, pues posee menor cantidad de campos, sus estructuras y contenidos han sido mejorados; optimizando los recursos que utiliza, pues se han eliminado algunos campos repetitivos que ya se representaban anticuados, incrementando algunas características para hacer frente a las nuevas necesidades de las redes actuales, como comunicación en tiempo real y seguridad.

- Soporte mejorado para las extensiones y opciones. Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten un reenvío más eficiente, límites menos rigurosos en la longitud de opciones y mayor flexibilidad para introducir nuevas opciones en el futuro.

- **Capacidad de etiquetado de flujo.** Una nueva capacidad se agrega para permitir el etiquetado de paquetes que pertenecen a "flujos" de tráfico particulares para lo cual el remitente solicita tratamiento especial, como la calidad de servicio no estándar o el servicio en "tiempo real".

---

[13] - [RFC-2460] S. Deering. R. Hinden."Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, Diciembre 1998.

- Capacidades de autenticación y privacidad. Extensiones para utilizar autenticación, integridad de los datos, y (opcional) confidencialidad de los datos, se especifican para el IPv6.

- Características de movilidad. IPv6 permite que la comunicación pueda llevarse a cabo en cualquier momento y lugar con un óptimo grado de operatividad, así como de forma trasparente al usuario, permitiéndole realizar su propia gestión y control. Cuestiones de gran importancia si queremos disfrutar de servicios multimedia en los terminales móviles de última generación (VozIP y Video). Protocolos como MPI (Mobile IP) o HMIP (Hierarchical MIP) posibilitan la implantación y explotación real de estos servicios.

- Autoconfiguración de los nodos. La autoconfiguración de direcciones es más simple. Especialmente en direcciones Globales Unicast, los 64 bits superiores son asignados por un mensaje desde el router (Router Advertisement) y los 64 bits más bajos son asignados con la dirección MAC (en formato EUI-64). En este caso, el largo del prefijo de la subred es 64, por lo que no hay que preocuparse más por la máscara de red. Además el largo del prefijo no depende del número de hosts por lo tanto la asignación es más simple.

- Calidad de servicio y clases de servicios. Capacidad de una red para sostener un comportamiento adecuado del tráfico que transita por ella, cumpliendo con parámetros relevantes para el usuario final. IPv6 fue diseñado con soporte extendido a QoS. En el encabezamiento se han incluido dos campos relacionados a QoS, éstos son: Clase de tráfico e Identificador de Flujo.

- Multihoming. Es la facilidad que se da a las empresas o instituciones que desean realizar el cambio de un proveedor a otro por algún motivo, no necesitaría

cambiar de dirección, ni la realización de una nueva configuración de los equipos de comunicación. [14]

- Representación del direccionamiento IPv6. Las direcciones IPv6 tienen una forma diferente de representarse a las IPv4, como se verá a continuación.

- ✓ Forma hexadecimal: Una dirección IPv6 válida es representada por valores hexadecimales, los cuales se dividen en ocho piezas de 16 bits de dirección.

x: x : x : x : x : x : x : x

- ✓ Forma comprimida: Existen reglas que pueden ser aplicadas a las direcciones IPv6 con el objetivo de resumir un poco la sintaxis de las direcciones.

2001:0000:0000: 1234:0000:A1A0: ABEF: 0816

- ✓ Las letras pueden ser mayúsculas o minúsculas y las dirección se puede escribir como:

2001:0000:0000:1234:0000:a1a0:abef:0816

- ✓ Los ceros consecutivos son opcionales y se pueden representar en la dirección como:

2001:0:0: 1234:0:a1a0:ABEF:0816

- ✓ Los campos sucesivos de ceros pueden ser reemplazados por "::" y la dirección puede tomar la forma :

2001::1234:0:A1A0:ABEF:816

- ✓ Pero, cualquier dirección que tenga más de una vez la representación "::" será una dirección inválida ya que solamente se puede usar esa representación una sola vez.

---

[14] [RFC-2460] S. Deering. R. Hinden."Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, Diciembre 1998.

- ✓ Forma mixta. Esta forma combina las direcciones IPv4 e IPv6. Una forma alternativa que a veces es más conveniente cuando se trata de un entorno

x:x: x: x: x: x: dddd

Donde las x son los valores hexadecimales de las seis partes de 16 bits de orden superior de la dirección, y las 'd' son los valores decimales de las cuatro piezas de orden inferior de 8 bits de la dirección (representación estándar IPv4).

0:0:0:0:0:0:13.1.68.3

0:0:0:0:0: FFFF: 129.144.52.38

O en forma comprimida:

::13.1.68.3

::FFFF: 129.144.52.38.

- Unicast. Es una dirección para una sola interface, un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección, cada dirección IPv6 pertenece a un ámbito, que es un área dentro de la cual ésta puede ser utilizada como un identificador único de una o varias interfaces, en el caso de las direcciones unicast se podrían reflejar en ámbitos de diferentes tipos.[15]

- La dirección no especificada. La dirección 0:0:0:0:0:0:0:0 toma como nombre dirección no especificada, de forma abreviada se representa “0::0” o “::”. Nunca debe ser asignada a ningún nodo, pues indica la ausencia de una dirección. Un ejemplo de uso de esta dirección es en el campo dirección origen de un paquete IPv6 enviado por un host durante su proceso de inicialización, antes de que haya obtenido su propia dirección.

---

[15] - [RFC-4193] R. Hinden. B. Haberman."Unique Local IPv6 Unicast Addresses", RFC 4193, Octubre 2005.

La dirección de no especificada no puede ser usada como dirección origen para paquetes salientes, y un paquete con la dirección no especificada como destino nunca puede ser enviado fuera del nodo ni debe ser encaminado por los routers.

- Dirección Loopback o dirección de bucle invertido. La dirección unicast 0:0:0:0:0:0:0:1, se define como dirección loopback, ésta puede ser utilizada por un nodo destino para el envío de un paquete IPv6 a sí mismo, la dirección loopback no debe ser utilizada como fuente de la dirección en Paquetes IPv6 que se envían fuera de un solo nodo. Un paquete IPv6 con una dirección de destino de loopback nunca debe ser enviado fuera de un solo nodo y nunca debe ser remitido por un router IPv6.

- Anycast. Una dirección anycast es un identificador que se asigna a múltiples interfaces (típicamente pertenecen a diferentes nodos). Un paquete enviado a una dirección Anycast es entregado en una (cualquiera) de las interfaces identificadas con dicha dirección (la más próxima, de acuerdo a las medidas de distancia del protocolo de encaminamiento). Nos permite crear, por ejemplo ámbitos de redundancia, de forma que varias máquinas puedan ocuparse del mismo tráfico según una secuencia determinada por el routing si la primera cae.

Una dirección anycast es difícil de distinguir. No hay un rango de espacio dedicado a este tipo de direcciones, pues ocupan el mismo rango de direcciones Unicast. La configuración local es responsable de identificación de las direcciones de difusión ilimitada, el uso de este tipo de direcciones es brindar una identificación a un conjunto de routers que pertenecen a una organización que proporciona los servicios de internet, o para identificar un conjunto de routers conectados a una red particular las direcciones Anycast no deben de ser utilizadas como una dirección de origen de un paquete IPv6, son rangos que son asignados por el

administrador de la red o proveedor de servicios, para uso exclusivo de identificación de los router y no para asignación de los host.[16]

- Multicast. Se define en el RFC 3513, este tipo de direcciones cumple como un Identificador para un conjunto de interfaces (por lo general pertenecientes a diferentes nodos). Un paquete enviado a una dirección multicast es entregada a todas las interfaces identificadas por dicha dirección. La misión de este tipo de paquetes es evidente: aplicaciones de retrasmisión múltiple (Broadcast), teniendo en cuenta que para IPv6 no existen direcciones de Broadcast, las funciones son realizadas por direcciones multicast.[17]

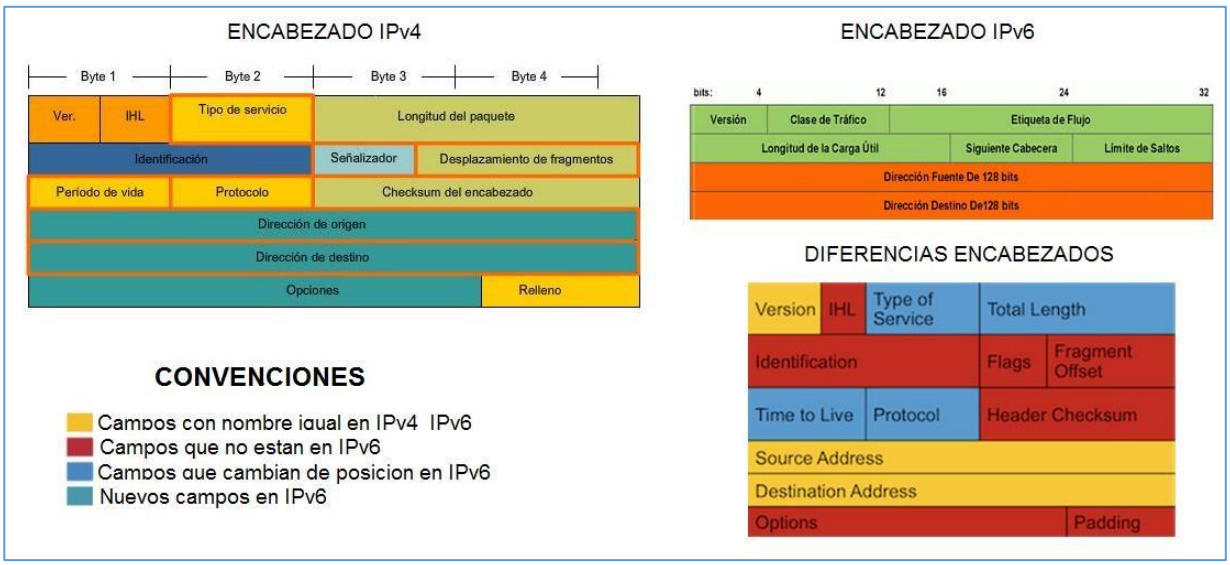
---

[16] - [RFC-4786] S. Deering., R. Hinden. "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, Diciembre 1998.

[17] - [RFC-4601] J. B. Fenner., M. Handley.H. Holbrook " Protocol Independent Multicast - Sparse Mode (PIM-SM):", RFC 4786, Agosto 2006.

2.2.3 Cabecera IPV4 vs IPV6.

Figura 1. Encabezado IPV4 Vs. Encabezado IPV6.



Fuente: https://supportforums.cisco.com– Año 2015.

Haciendo referencia a la diferencia del encabezado de paquetes entre direccionamiento IPV4 – IPV6 aclarando la Figura 1. todas las secciones que aparecen en color rojo son elementos que se eliminaron del encabezado de IPv6, las que están en color azul, cambió de nombre y posición y las que están en amarillo se mantienen de la misma manera.

Entre las secciones modificadas o nuevas en la cabecera de IPV6 con relación a IPv4 encontramos las siguientes:

- **Traffic Class (8 bits).** Tiene la misma funcionalidad que el Type of Service, sirve para almacenar la información de precedencia, DSCP o clase de servicio dependiendo de la implementación de QoS.

- **Payload Length (16 bits).** En IPv6 tenemos un encabezado fijo de 40 bytes por lo que solo necesitamos saber el tamaño de la información útil del paquete.

Esto también nos quita la necesidad de implementar rutinas de búsqueda como en IPv4. Ya estamos utilizando 4 veces el tamaño de buffers para el manejo de direcciones de 128 bits, cualquier cosa que disminuya el procesamiento extensivo de los paquetes es preferible.

- **Next Header (8 bits).** Esta sección nos puede indicar el protocolo al que pertenece la información que estamos acarreando (TCP, UDP, ICMPv6, etc.). También se utiliza para indicarnos si existe información de opciones para los datos que se transportan. En lugar de manejar Opciones en el encabezado como IPv4, éstas las integramos dentro de la carga útil de los paquetes para mantener el encabezado en un tamaño fijo. Esta sección nos indicaría si hay opciones que revisar dentro del paquete.

- **Hop Limit (8 bits).** Sirve exactamente la misma función que el TTL de IPv4. Solo se cambió el nombre ya que este parámetro es un contador de saltos (equipos capa 3) y no un contador de tiempo como parece indicar el nombre en IPv4.[18]

[18] - [RFC-2460] S. Deering. R. Hinden."Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, Diciembre 1998.

2.2.4 Cloud Computing.

La infraestructura de la Cloud de Sonda S.A tiene como finalidad ofrecer servicios de Cloud Computing a los clientes, esta tecnología nace de la necesidad de que el cliente tenga su infraestructura en un lugar que no conoce, ni le interesa la infraestructura sino que sus servicios estén disponibles en un ANS (Acuerdo de nivel de servicio) lo más cercano al 100% por este motivo algunas compañías empiezan utilizar esta serie de servicios sobre la nube por temas como seguridad, reducción de costos, evitar gastos de infraestructura de Datacenter, incrementar agilidad y rendimiento utilizando esta serie de ambientes en la nube.

Pero puntualmente que es Cloud Computing según la definición dada por el NIST (National Institute of Standards and Technology), cloud computing es un modelo tecnológico que permite el acceso ubicuo, adaptado y bajo demanda en red a un conjunto compartido de recursos de computación configurables como lo son redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y liberados con un esfuerzo de gestión reducido o interacción mínima con el proveedor del servicio, se refiere tanto a las aplicaciones entregadas como servicio a través de internet, como el hardware y software de los centros de datos que proporcionan estos servicios. [19]

Las soluciones Cloud ofrecen una serie de ventajas a las empresas de tipo económico, tecnológico ambiental, y social en diversos la consolidación de las empresas en el mercado ya que ante la competencia tener una infraestructura con niveles de servicio altos es más favorable, además la alta gama de opciones que se pueden encontrar en el mercado para la prestación de servicios Cloud como lo pueden ser empresas outsourcing con utilización de reconocidas empresas de desarrollo de tecnología de infraestructura como lo son CISCO, VMWARE,

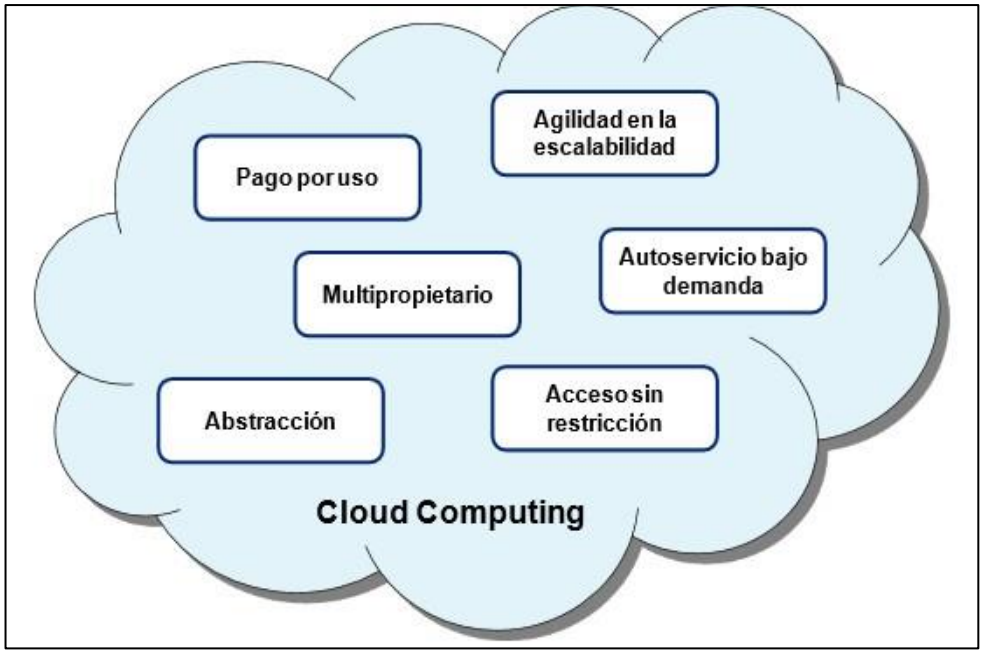
---

[19]Cisco Cloud Solutions [en línea].
http://www.cisco.com/web/solutions/trends/cloud/index.html [Citado 19 de agosto de 2015].

ORACLE, DELL entre otras pioneras en el mercado de infraestructura y soluciones tecnológicas.

Pero qué hace tan innovador y llamativo a Cloud Computing, para ver las claves que tienen tan bien posicionado este tipo de tecnología debemos ver las características más relevantes las cuales las podemos ver resumidas en la Figura 2.

Figura 2. Características asociadas al Cloud Computing.



Fuente: http://www.ontsi.red.es – Año 2015.

Pago por uso: Es el modelo de cobro en base al consumo del cliente, varía en función del uso del servicio Cloud.

Abstracción: es la característica que separa los recursos físicos contratados al proveedor de servicios Cloud, con ayuda de la virtualización de estaciones por lo cual no requiere personal que realice mantenimiento de infraestructura constante, actualización de equipos, energización, pruebas lo cual queda netamente realizado por parte del proveedor.

Agilidad en la escalabilidad: Se puede parametrizar a cada uno de los clientes por independiente aun después de entregada la solución, en función de las necesidades puntuales del cliente, esto evita la compra de recursos innecesarios en estaciones físicas.

Multiusuario: Capacidad que otorga Cloud que permite que varios usuarios se comuniquen con la infraestructura en la nube en sesiones simultáneas controlando la concurrencia de usuarios.

Auto servicio bajo demanda: la comunicación con el proveedor solo se llevaría a cabo cuando se presente alguna falla o implementación o requerimiento nuevo.

Acceso sin restricciones: la comunicación por parte del cliente a su nube virtual 24 horas 7 días a la semana, desde cualquier origen con conexión a internet ya que en ingreso a su infraestructura se realiza por una dirección IP pública, lo cual facilita el acceso para dispositivos portátiles como celulares, tablets y demás dispositivos con conexión a internet.

2.2.5 Vblock

Es una infraestructura Convergente Avanzada formada por Cisco y EMC, con inversiones de VMware e Intel, VCE representa un nivel sin precedentes de la colaboración en el desarrollo, los servicios y la habilitación de socios por cuatro establecidos líderes del mercado y la tecnología. VCE ayuda a simplificar las operaciones de TI al tiempo que ofrece un mayor valor para el negocio.

La implementación de una nueva infraestructura de múltiples proveedores ya no requiere largos ciclos de integración y pruebas. VCE integra virtualización, redes, computación, almacenamiento, seguridad y tecnologías de gestión líderes en la industria para entregar sistemas Vblock: una infraestructura única, convergente que es compatible con una amplia gama de aplicaciones críticas de negocio.

Con Vblock Systems, VCE:

- Mejora el rendimiento de las aplicaciones, el escalamiento dinámico, y la recuperación de desastres.
- Usos de normalización para garantizar la seguridad está integrada en todas las configuraciones.
- Se integra y valida las configuraciones a acelerar el despliegue.
- Reduce los costes de las instalaciones con una infraestructura densa rendimiento.
- Ofrece opciones de gestión del sistema y de apoyo para mejorar la productividad de TI.
- VCE puede ayudar a transformar TI y reducir el costo total de propiedad.

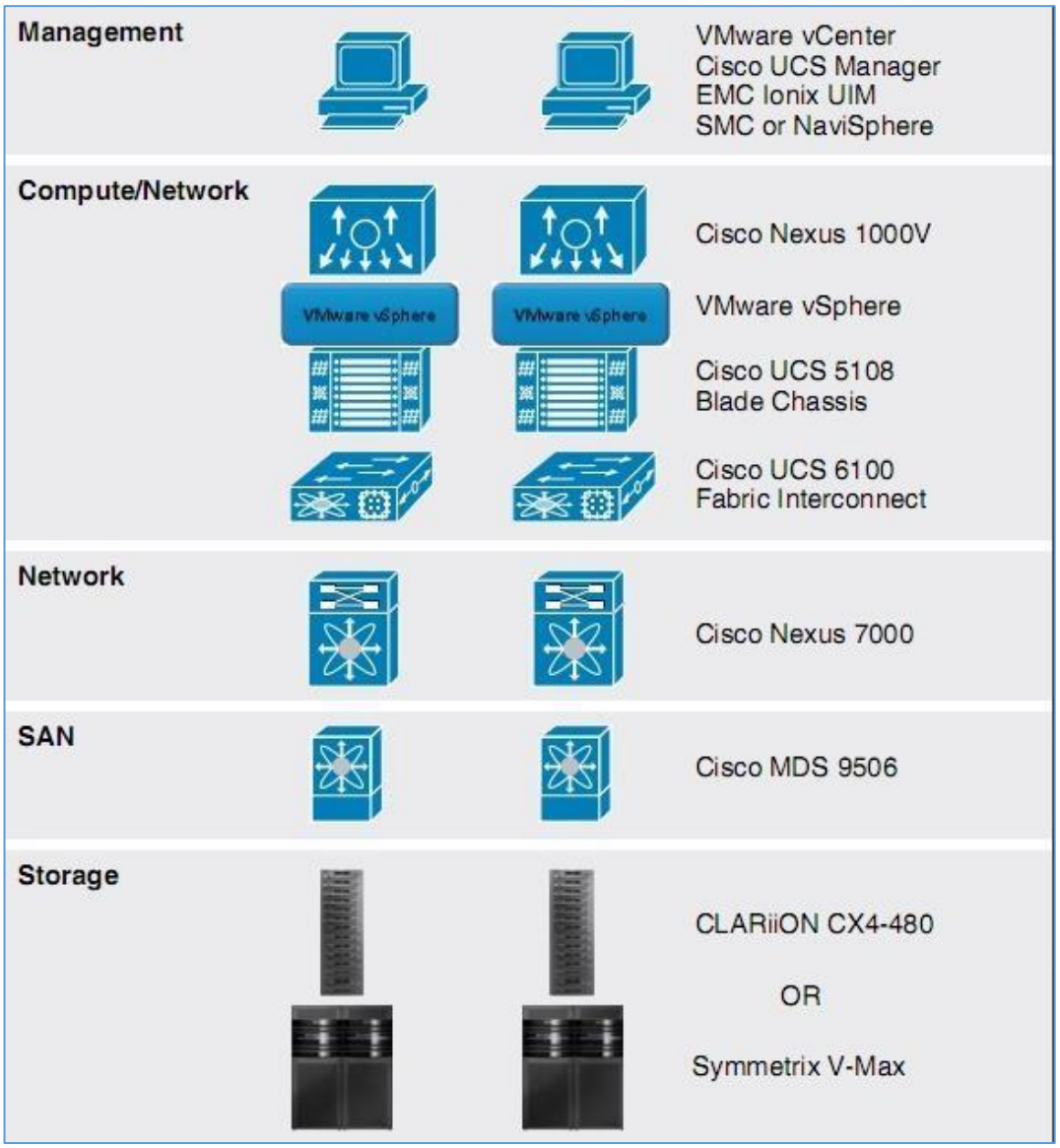
Figura 3. Tipos de familia Vblock.

Fuente: http://www.emc.com/platform/vce-vblock.htm - Año 2015.

Vblock es un paquete de infraestructura virtual completa construida en serie CX4 EMC Clariion o la EMC Symmetrix V-Max para la capa de almacenamiento, conectado a través de Cisco Nexus 1000V y Switches Cisco Multilayer direccionales (MDS) a un centro de Cisco Unified Computing Systems (UCS) blade corriendo VMware vSphere 4. Mediante el uso de una combinación fija de componentes VCE (un consorcio de VMware, Cisco y EMC) es capaz de

garantizar el rendimiento, la capacidad y la disponibilidad SLA para un número conocido de máquinas virtuales.[20]

Figura 4. Vblock Arquitecture.



Fuente: http://gabesvirtualworld.com – Año 2015.

[20] Vblock Systems Overview [En línea]. http://www.vce.com/products/converged/vblock/overview [Citado 16 de julio 2015].

En la actualidad Sonda de Colombia S.A. cuenta en su red Cloud con un V-Block 330 el cual consta de tres rack distribuidos en sus capas más importantes de la arquitectura en el primero se encuentra la capa de management con dos Cisco UCS C220 y cuatro Cisco UCS 5108 Blade Server Chassis, en el segundo rack se encuentra la capa de networking recursos explicados a detalle en el punto 4.2 (Recursos Físicos) y por último en el tercer rack se encuentra la capa de Storage compuesta por un VNX5800: 32 GB/SP, 750 Drives, FAST Cache: 3 TB, arquitectura sobre la cual están configurados y publicados los servicios sobre los cuales se desarrollarlo el proyecto de migración IPv6.

2.2.6 Estrategias De Migración IPv4 – IPv6[21]

- Dual Stack (Pila Dual). Es una de las técnicas más utilizadas en la migración de IPv4 a IPv6, ya que puede emplearse en diferentes puntos de la red: equipos clientes, servidores y routers, no habrá comunicación entre IPv4 e IPv6; sin que las aplicaciones soporten ambos modos. El desafío con dual stack es que todos los equipos de la red han de contar con la suficiente potencia de proceso y memoria, para gestionar dos pilas IP diferentes. Además, gestionar dos pilas IP supone un doble gasto en gestión y soporte, lo que incrementa los costes de TI.

- Configured Tunnels. Esta es una técnica que se define en el RFC 2893, encapsula las comunicaciones de uno de los protocolos sobre el otro, estableciendo para ello un túnel de comunicación (similar a una VPN). Para ello necesitaremos contar con dual stack en cada uno de los puntos del túnel. Los routers involucrados en este método han de ser capaces de mapear las direcciones del contrario. Este tipo de túneles point to point necesitan ser

[21] Mecanismos de migración IPv4 – Ipv6 [en línea]. http://long.ccaba.upc.es/long/050Dissemination_Activities/carlos_ralli_transitiontutorial.pdf [Citado 19 de agosto de 2015].

configurados manualmente, para el control de las rutas del túnel, y para reducir el alto nivel de ataques al servicio.[22]

- Túnel Broker. La idea básica de un Túnel Broker es permitir al usuario conectarse a un servidor web, opcionalmente permite entrar en algunos detalles de autenticación, y recibir de vuelta un pequeño script para ejecutar y establecer un túnel IPv6 en IPv4 al servidor de Túnel Broker el proveedor del servicio del Túnel Broker debe ofrecer un servidor web disponible a través de IPv4 o un router de dual-stack capaz de aceptar comandos automatizados de configuración para crear nuevos túneles a los extremos de cliente. Es posible que ambas funciones puedan servir desde una sola máquina.[23]

- Túnel 6to4. El mecanismo de transición conocido como Túnel 6to4 [RFC3056] es una forma automática de permitir la comunicación de router a router por medio del túnel, facilitando a los dominios aislados en IPv6 comunicarse con otros dominios IPv6 con una configuración mínima. La IANA asignó el prefijo IPv6 2002:: / 16 para designar un sitio donde participar, al sitio de IPv6 se le asignará un prefijo de 2002: V4ADDR::/ 48, donde V4ADDR es el rango dirección única en IPv4, configurada en la interfaz del router de salida apropiada al dominio, este prefijo tiene exactamente el mismo formato que los prefijos normales / 48 y por lo tanto permite un dominio IPv6 para utilizarlo como cualquier otro prefijo válido / 48, en el escenario donde los dominios 6to4 desean comunicarse con otros dominios 6to4.

- Túnel ISATAP. Una alternativa a 6over4 es ISATAP (Intra-Site Protocolo de direccionamiento automático de túnel). ISATAP también usa el sitio infraestructura IPv4 como un vínculo virtual, pero no utiliza IPv4 multicast, por lo que el enlace es

---

[22] - [RFC-2473] A. Conta., S. Deering. "Generic Packet Tunneling in IPv6 Specification", RFC 2473, Diciembre 1998.

[23] A. Conta, S. Deering, "RFC2473 Especificaciones genéricas de tunelización de paquetes en IPv6". [En línea]. Disponible: http://www.ietf.org/rfc/rfc2473.txt

NBMA (non-broadcast múltiple Access), ISATAP, como 6over4, crea un identificador de interfaz basado en la dirección IPv4. ISATAP es compatible con una configuración automática o manual de direcciones, pero la dirección IPv4 de la interfaz se integrará como los últimos 32

- Túnel 6over4. 6over4 se define en el RFC 2529. Interconecta hosts IPv6 aislados en un sitio a través de IPv6 en IPv4 sin encapsulación explícita de túneles. Utiliza las direcciones IPv4 como identificadores de interfaz y crea un enlace virtual usando un grupo de multidifusión IPv4 con ámbito de organización local. El método 6over4 ha caído en desuso debido a una serie de razones, incluyendo la falta general de IPv4 multicast en las redes de ISP.

- Túnel Teredo. El mecanismo de transición Teredo, es una forma de túnel automático destinado a proporcionar conectividad IPv6 con direcciones IPv4 que se encuentran detrás de un NAT [RFC1613]. Se trata de un mecanismo de túnel automático que proporciona conectividad IPv6, cuando un host de dual-stack se localiza detrás de un NAT, para encapsular paquetes IPv6 en IPv4 el usuario se basa en el Protocolo de Datagramas de Mensajes (UDP).[24]

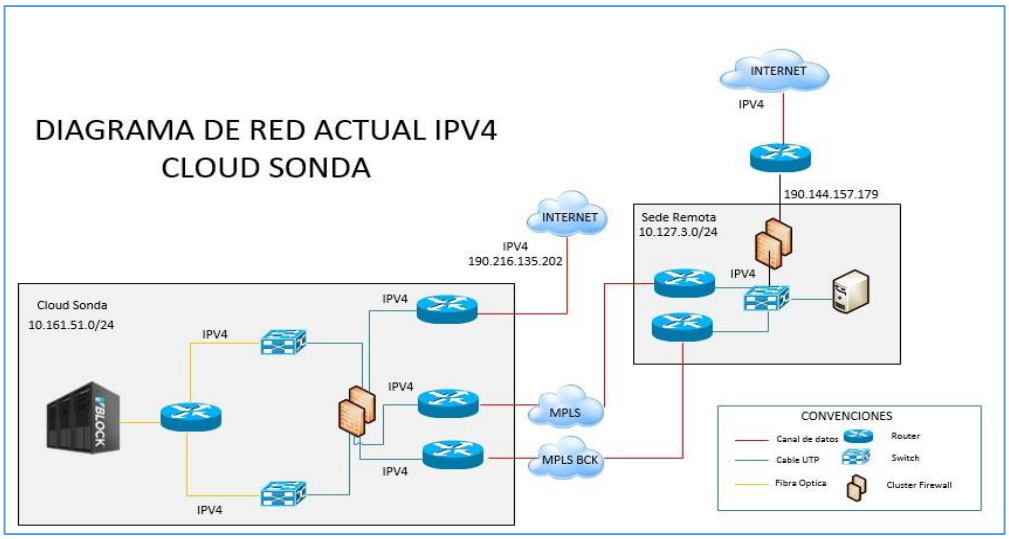
[24] - [RFC-6180] J. Arkko., F. Baker. " Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment", RFC 6180, Mayo 2011.

2.3 ESTADO ACTUAL RED CONVERGENTE SONDA CON IPv4

La infraestructura en la que esta implementada la red Cloud empresarial de Sonda S.A. está compuesta por una solución llamada VCE (Virtual Computing Environment), el cual es un sistema resultado de la unión entre Cisco, EMC Y VMware, se creó al ver el continuo movimiento y procesamiento de los centros de procesamiento de datos, y la necesidad de la flexibilidad de la infraestructura tecnológica que se veía en la diferentes compañías a nivel mundial, mediante esta solución se llegaría a los clientes en forma de paquetes de soluciones según las necesidades mediante Vblocks; en el rack Vblock de la red Cloud se encuentra a nivel físico los elementos citados en el punto 4.2 (Recursos Físicos), más el hardware de la capa de almacenamiento y administración.

En la actualidad la interconexión entre el Datacenter Level 3 y la sede remota de Sonda S.A se realiza por medio de dos canales de datos principal - back up con el proveedor Level 3 y la salida de internet del Datacenter y la red interna, se realiza por medio del protocolo IPv4 mediante el mismo proveedor el diagrama a nivel lógico de la interconexión se puede visualizar en la Figura 5.

Figura 5 Conexión actual Cloud Sonda de Colombia.



Fuente Diseño IPV4 Infraestructura Cloud – Año 2015.

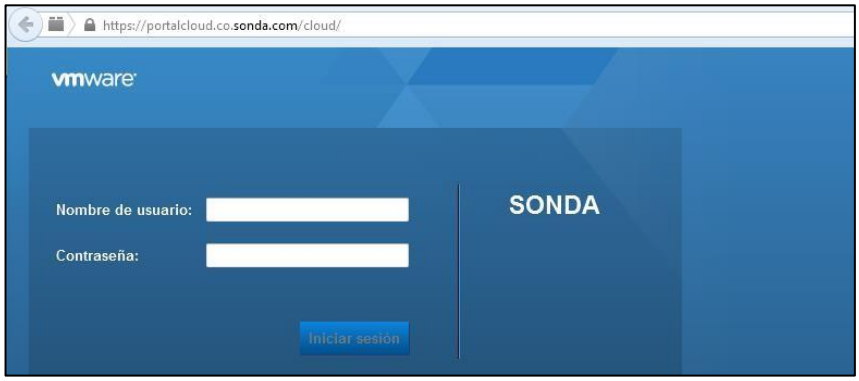
2.4 SERVICIOS ACTUALMENTE SOBRE IPv4.

En la Cloud empresarial se encuentran publicados diversos servicios a múltiples clientes y algunos de uso interno los cuales se tomarán para efectos del proyecto como punto de referencia los cuales son citados a continuación:

2.4.1 Portal Administración Cloud Empresarial

El primer servicio a revisar es el portal de administración de la Cloud empresarial de Sonda S.A. https://portalcloud.co.sonda.com es un sitio publicado en internet mediante la dirección IP 190.216.135.204 en el cual permite realizar la administración independiente de las nubes de cada cliente.

Figura 6. Portal Administración página de inicio.



Fuente: https://portalcloud.co.sonda.com – Año 2015.

Este portal es el acceso al vCloud Director la cual es una plataforma VCloud Director (VCD) es la herramienta de gestión de la computación en nube de VMware Inc. Gestiona Infraestructura como Servicio (IaaS) arquitecturas de gestión de los diferentes componentes de computación en nube, como la seguridad, la máquina virtual (VM) de aprovisionamiento, facturación y acceso de autoservicio. Se centra en las infraestructuras de computación en nube privada e híbrida.

VMware vCloud Director fue desarrollado inicialmente bajo el nombre en clave del proyecto Redwood y, en VMworld 2009, discutió informalmente el proyecto nube. En mayo de 2010, cuando VMware publicó accidentalmente información sobre el producto de cloud computing en su sitio web, más detalles emergieron. VMware anunció oficialmente el producto de gestión de cloud computing y su nombre en su conferencia anual, VMworld 2010.

VCloud Director proporciona una configuración vCD que requiere de herramientas adicionales, como una base de datos Oracle y de 64 bits de Red Hat Enterprise Linux (RHEL) 5. Y para avanzados vCloud Director de características, los usuarios deben recurrir a varios productos y proveedores:

- VShield perimetral para la seguridad
- Cloud Control de HyTrust Inc. para la federación de autenticación
- Zenoss Inc. para la supervisión y presentación de informes avanzada
- De Aria System Inc, que suministra el software de gestión de facturación.

Estos componentes interactúan con vCloud Director a través de interfaces de programación de aplicaciones (API). [25]

Figura 7 Portal Administración página de inicio 2.

Fuente: https://portalcloud.co.sonda.com/Help – Año 2015.

[25] What is VMware vCloud Director? – Foro Oficial VMware [En linea]. http://searchvmware.techtarget.com/ [Citado 18 de marzo 2015].

Este portal de administración está configurado para algunos de los clientes de la compañía los cuales tienen sus servidores o servicios publicados en la Cloud empresarial de la compañía, cada uno de los clientes tiene una red privada a su disposición en la cual pueden publicar los servidores o servicios que sean necesarios cada una de las redes son independientes por lo cual no se presenta problema de solapamiento o duplicidad de direccionamiento entre redes, de diferentes nubes corporativas ya que acceden por una única dirección ip pública y un puerto en específico definido por la necesidad del cliente ejemplo un escritorio remoto, aplicación web entre otros.

Figura 8 Vista de nubes corporativas en Cloud empresarial.

Fuente: https://portalcloud.co.sonda.com/cloud/#/orgListPage?

2.4.2 Servidor SSH de gestión de red

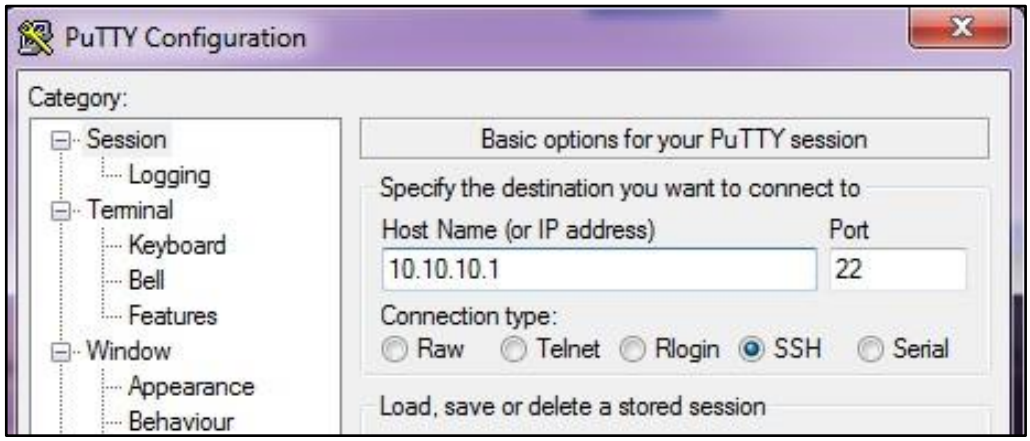
El servidor de Shell seguro o SSH (Secure SHell) es un servicio muy similar al servicio telnet ya que permite que un usuario acceda de forma remota a un sistema Linux pero con la particularidad de que, al contrario que telnet, las comunicaciones entre el cliente y servidor viajan cifradas desde el primer momento de forma que si un usuario malintencionado intercepta los paquetes de datos entre el cliente y el servidor, será muy difícil que pueda extraer la información ya que se utilizan sofisticados algoritmos de cifrado.

La popularidad de SSH ha llegado a tal punto que el servicio telnet prácticamente no se utiliza. Se recomienda no utilizar nunca telnet y utilizar ssh en su lugar.

Para que un usuario se conecte a un sistema mediante ssh, deberá disponer de un cliente ssh, como lo puede ser un putty, hyperterminal y la comunicación se debe realizar por el puerto 22 TCP especial para conexiones ssh Durante el proceso de autentificación, cuando el usuario proporciona el nombre y la contraseña, se utiliza cifrado asimétrico pero en el resto de la sesión se utiliza cifrado simétrico por su menor necesidad de procesamiento.

El servicio es el servidor SSH de gestión de red es un servidor Linux publicado desde el que se puede obtener acceso SSH a este equipo el cual está excluido de toda la red y políticas de firewall para que se pueda acceder a cualquier destino en la red Cloud en caso de perder conexión con algunos de los equipos.

Figura 9. Ejemplo conexión SSH.



Fuente: Conexión SSH – Captura Propia.

2.4.3 Acceso VPN red cloud.

Este servicio permite la administración del cluster de Firewall ASA ubicado en la red cloud de SONDA, la administración se realiza mediante la plataforma ASDM Esta administración es directamente hacia los equipos Firewall Cisco ASA 5525 Adaptive Security Appliance Platform, en donde están configuradas las reglas de firewall, QoS, administración de filtrado de contenido y demás características proporcionadas por el Cluster Firewall ASA 5525 como se ve a continuación en la Figura 10.

Figura 10. Portal de acceso Cloud Empresarial.

Captura Propia – Año 2015.

2.4.4 Portal de monitoreo equipos Cloud con ZABBIX.

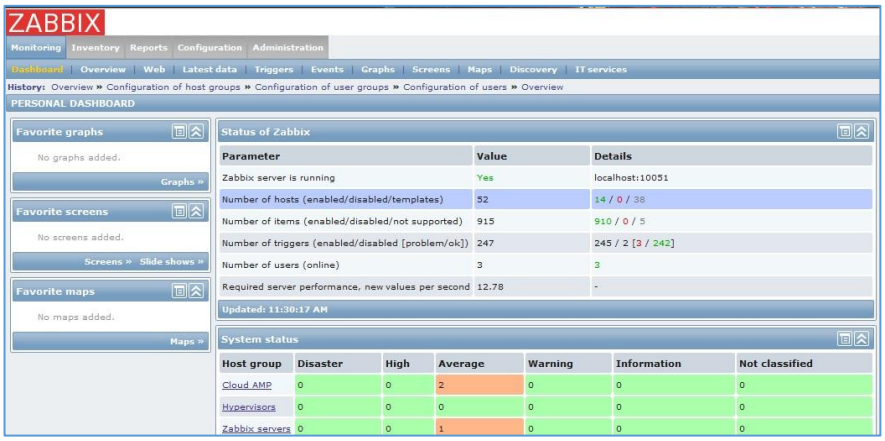
Contar con un sistema de monitorización de redes ampliamente utilizado, de código abierto, que vigile los equipos físicos y servicios según la necesidad del cliente, alertando cuando el comportamiento de los mismos no sea el deseado, como perdidas de conexión, desconexión de interfaces, apagado de equipos entre otras características, es una de las herramientas más importantes para la revisión de reportes y detalles de cualquier implementación de infraestructura.

Entre las características principales con las que debe contar un portal de monitoreo figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), independencia

de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugins específicos para nuevos sistemas.

Se trata de un software que proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables correspondientes mediante (entre otros medios) correo electrónico y mensajes SMS, cuando estos parámetros exceden los márgenes definidos por el administrador de red como se ve en la Figura 11 aplicado para algunos servidores de red.

Figura 11. Portal monitoreo ZABBIX.



Fuente: https://monitoreocloud.co.sonda.com - Año 2015.

Estas alertas también son visualmente fáciles de reconocer por la persona encargada de realizar el monitoreo según como se configure la herramienta que realice el monitoreo de la red, entre las herramientas más reconocidas encontramos SolarWinds, Nagios, Zabbix, PRTG, entre otras que se diferencian es en el modo de licenciamiento, características especiales, modo de realizar los reportes, [26]

[26] What Nagios Provides? – Página Oficial NAGIOS [En línea].

3 DISEÑO METODOLÓGICO.

3.1 TIPO DE ESTUDIO.

El tipo de estudio de este proyecto de grado es de adaptación y/o transferencia de tecnología ya que consiste en desarrollar un proceso de investigación tecnológica que tiene por objeto realizar, adaptar o transferir de protocolo de internet IPv4 a IPv6 en la red convergente de la empresa Sonda De Colombia S.A.

3.2 UNIDAD DE ANÁLISIS.

Implementación de protocolo de internet IPv6 en red convergente ubicada en Datacenter Triara de la empresa Sonda de Colombia S.A.

3.3 UNIDAD DE ESTUDIO.

Documentación protocolo de internet IPv6, tecnologías de migración de direccionamiento IPv6 a IPv4 y utilización de túneles de convergencia.

3.4 UNIDAD DE TIEMPO.

El desarrollo de este proyecto está comprendido entre agosto de 2014 y agosto de 2015.

---

http://www.nagios.org/about/overview [Citado 18 de marzo 2015].

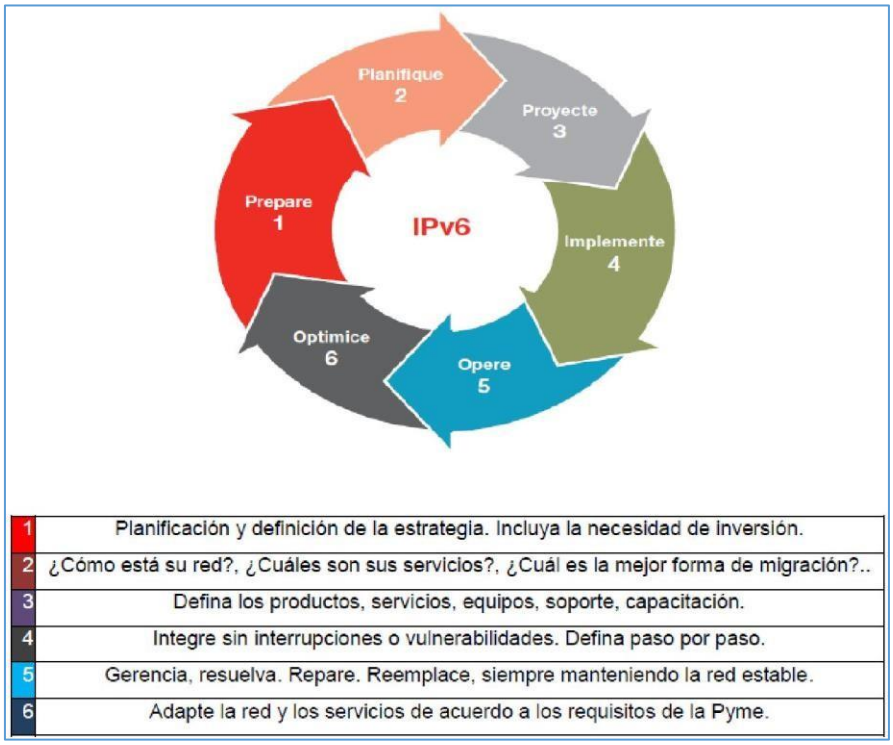
3.5 UNIDAD GEOGRÁFICA.

Esta aplicación estará funcionando en la cloud empresarial de Sonda de Colombia ubicada en el Datacenter de Level 3.

3.6 METODOLOGÍA DE LA INVESTIGACIÓN.

La metodología de investigación, consta de seis fases de un proceso cíclico, alineado con los procesos e infraestructuras y servicios existentes en el momento en la red en la Figura 12. Se explican las seis etapas las cuales se deben seguir para realizar la migración de IPv4 – IPv6

Figura 12 Fases de migración IPv4-IPv6.



1	Planificación y definición de la estrategia. Incluya la necesidad de inversión.
2	¿Cómo está su red?, ¿Cuáles son sus servicios?, ¿Cuál es la mejor forma de migración?..
3	Defina los productos, servicios, equipos, soporte, capacitación.
4	Integre sin interrupciones o vulnerabilidades. Defina paso por paso.
5	Gerencia, resuelva. Repare. Reemplace, siempre manteniendo la red estable.
6	Adapte la red y los servicios de acuerdo a los requisitos de la Pyme.

Fuente: http://www.networkworld.es.

3.6.1 Preparar. Sonda de Colombia S.A. debe revisar si la infraestructura con la que se cuenta actualmente cuenta con las características necesarias que le permitan la migración de IPv4 a IPv6 para obtener el máximo beneficio en el funcionamiento de la red, dentro de la planificación y definición de la estrategia se incluyen aspectos importantes como plantear una red que se ajuste a las exigencias de rendimiento de la compañía como son los SLA (Service Level Agreement) que se tienen con cada cliente independientemente y contemplando variables como escalabilidad de la red, incorporación de clientes nuevos, mantenimiento y administración de la red.

3.6.2 Planificar. Se plantea un conjunto de componentes los cuales deben ser identificados y deben permitir definir puntualmente el alcance del proyecto de migración, se deben incluir todos los elementos que intervengan en el proyecto tanto elementos físicos como lógicos, que se relacionen con la red a cualquier nivel como lo es todo el conjunto de la red de área local, salida a clientes por medio de red WAN en el cual se tienen que tener en cuenta tanto equipos de seguridad y de routing que permiten el enrutamiento como los protocolos de direccionamiento, tanto internos como de salida, se debe evaluar el tráfico que llega y sale de esta a cada una de sus redes conjuntas, que aplicaciones empresariales y el nivel de seguridad que se deben manejar con cada uno de los clientes involucrados, además se deben verificar las medidas de seguridad y políticas necesarias para asegurar el acceso a personal no deseado generando ambientes de prueba donde se simulen accesos a ilícito a la red.

3.6.3 Proyectar. La empresa Sonda de Colombia debe proyectar el funcionamiento de la red con direccionamiento IPv6 para permitir llevar la migración y la transición de una forma más segura y estable para la red, teniendo en cuenta cada uno de sus clientes, y pensando en la escalabilidad de la red como principio.

3.6.4 Implementar. Es necesario identificar las soluciones que se puedan necesitar para facilitar la transición de IPv4 – IPv6 sin necesidad de recurrir a compra de hardware y o que se requiera una sustitución completa o reingeniería de toda la infraestructura además se deben contar con un plan de contingencia o rollback que permita mantener la estabilidad en la prestación de los servicios a los clientes involucrados al momento de reestructurar los equipos en el proceso de migración a IPv6, evitando que se encuentre en un estado de vulnerabilidad, o falta de prestación de servicio afectando niveles de servicio y calidad del mismo.

3.6.5 Operar. Para llevar a cabo exitosamente la migración de IPv4 a IPv6, se debe realizar el proceso mediante pasos cortos para no generar alteraciones que afecten la prestación del servicio, y así poder asumir los problemas que vayan surgiendo con mayor facilidad para la empresa, se deben tener en cuenta procesos que requieran de reparaciones de equipos, reingeniería, o remplazo de infraestructura.

3.6.6 Optimizar. Sonda de Colombia S.A. al acceder a nuevas tecnologías como lo es la migración de direccionamiento de IPv4 - IPv6 en su red convergente, mejora la competitividad y optimiza los servicios con sus clientes manteniendo los niveles de servicio requeridos y generando un impacto positivo al interior de la organización, también acopla la red de acuerdo a sus exigencias, teniendo en cuenta la tecnología disponible y la capacidad de adquirir nuevos clientes gracias a la nueva implementación de tecnología.

3.7 PARTICIPANTES

Christian Leonardo Bernal Gutierrez, Tecnólogo en Sistemas de la Escuela Tecnológica Instituto Técnico Central y estudiante de XI semestre de Ingeniería de Sistemas de la misma institución.

3.8 POBLACIÓN Y MUESTRA

La población es toda la red Cloud de la empresa Sonda de Colombia S.A. y como muestra la migración se realiza en parte de la red management.

3.9 INSTRUMENTOS Y EQUIPOS

La recolección de información está dada por medio del estudio y análisis de la tecnología y la información relacionada al tema de aplicación y la aplicación de metodologías.

3.9.1 Hardware.

- ✓ Equipo portátil con capacidad de realizar conexión serial, ssh, telnet a los equipos que se requieren configurar.

3.9.2 Software.

- Putty 0.64.
- Cisco IOS Software, C3560 Software (C3560-IPBASEK9-M), Versión 15.0(2)SE5
- Windows 2008 Server Standard Edition x 64 bits.
- CISCO ASA Versión 9.0.
- Cisco Nexus 5500 Series NX-OS Software Release 7.0.
- Linux 2.6 OS.

4. RECURSOS.

4.1 RECURSOS HUMANOS

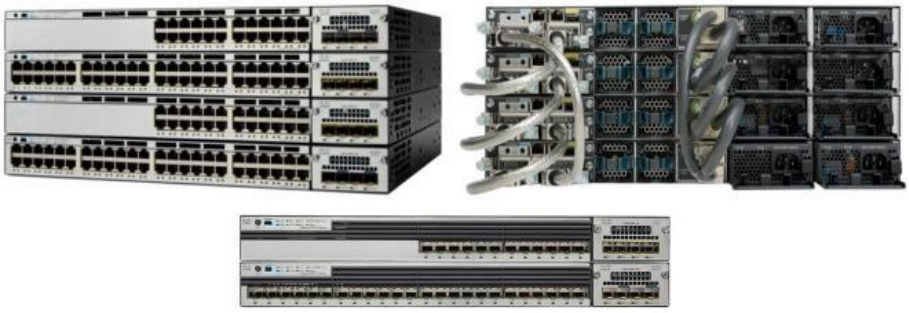
La configuración del proyecto de implementación de IPv6 en la Cloud empresarial de Sonda de Colombia S.A. será realizada por el estudiante de último semestre de Ingeniero de sistemas Christian Leonardo Bernal Gutierrez, la asesoría documental se realiza por parte del Ing. Oscar Lombana profesor de Proyecto de grado. La asesoría de proyecto será realizada por el Ing. Camilo Jaraba gerente de servicios compartidos de Sonda de Colombia S.A.

4.2 RECURSOS FÍSICOS

- Switches Cisco Catalyst 3560X-24T-S

Cisco Catalyst 3560X-24T-S cuenta con 48 puertos Ethernet 10/100/1000 con tecnología PoE (Power on Ethernet) y 1 modulo extraíble con 4 puertos Gigabit Ethernet basados en SFP (small form-factor pluggable) este equipo ocupa 1 RU (Rack Unit), cuenta con 2 puertos Stack, 1 puerto de consola, 2 fuentes redundantes, ventiladores internos, y fuentes de poder extraíbles.

Figura 13 Cisco Catalyst 3560 – X Series Switches (Front and Back).



Fuente. Cisco Catalyst 3750-X and 3560-X Series Switches Data Sheet.

Switches con funcionalidad de stack o agrupamiento en pila mediante las tarjetas de stack de cada uno de los switches, permitiendo que se puedan realizar configuraciones globales para todos los miembros de la pila, sin dejar a un lado la configuración individual de cada uno de los switches, entre la pila de switches debe haber un switch maestro, si este dispositivo no se encuentra disponible entre los demás elementos se debe escoger un switch maestro, esta funcionalidad permite mayor escalabilidad.

Figura 14 Cisco Catalyst 3560 – StackPower Connector

Fuente. Cisco Catalyst 3750-X and 3560-X Series Switches Data Sheet.

Maneja direccionamiento IPv4 – IPv6, routing multicast, manejo de QoS, Voice Vlan, TFTP (Trivial File Transfer Protocol), NTP (Network Time Protocol) y

características de seguridad avanzadas entre los puntos tecnologías más relevantes. [27]

- Firewall Cisco ASA 5525 Adaptive Security Appliance Platform

Firewall Cisco ASA 5525 Adaptive Security Appliance Platform es un dispositivo multiescala para el rendimiento en la industria, que permite la flexibilidad de servicio a ofrecer, escalabilidad, funciones entendibles, entre las características más importantes se encuentran las siguientes funcionalidades Firewall para la creación de reglas de tráfico, apertura y denegación de puertos en la red, manejo de QoS para garantizar calidad de servicio de un punto en la red a un destino, IPS como sistemas de prevención de intrusos, módulo VPN para conexiones de acceso remoto a red local, módulo de WSE (Web Security Essentials) para funcionalidades como filtrado URL.

Figura 15 Cisco ASA 5525 Series Firewall (Front and Back).

Fuente. Cisco ASA 5525-X Adaptive Security Appliance Data Sheet.

[27] CISCO. Data Sheet Cisco Catalyst 3750 - X and 3560 - X Series Switches [en línea]. http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3750-x-series switches/data_sheet_c78-584733.pdf [Citado 19 de enero de 2015].

Cuenta con un numero de nodos y de usuario ilimitados, 750 usuarios concurrentes de VPN (Virtual Private Network), permite 500000 conexiones simultaneas, con la capacidad de recibir 20000 conexiones por segundo, permite la creación de 200 interfaces virtuales VLANs (Virtual Local Area Network), permite la posibilidad de clusterizar dos equipos firewall Cisco ASA 5525 Adaptive Security Appliance Platform los cuales se comportarían de modo activo – pasivo para ofrecer alta disponibilidad y mayor seguridad e integridad de la información.

El appliance cuenta con 2 puertos USB 2.0, 8 entradas de cobre Gigaethernet, un puerto serial consola RJ-45, disco duro de 120 GB y 8GB de memoria RAM con arquitectura multibus.[28]

- Servidores UCS-FI-6248UP

Cisco Unified Computing System (UCS) unifican los recursos de informática, redes, gestión, virtualización y acceso a almacenamiento en una misma arquitectura integrada. Esta arquitectura exclusiva permite tener una visibilidad integral de servidores, gestión y control tanto en entornos físicos como virtuales, y facilita la migración al Cloud Computing y TI.

Figura 16 Cisco UCS 6248UP 48-Port Fabric Interconnect (Front and Back).

Fuente. Cisco UCS 6248UP 48-Port Fabric Interconnect Data Sheet.

[28] Data Sheet Cisco ASA 5500 - X Series Next – Generation Firewalls [en línea]. <http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-x-series-next-generation-firewalls/data-sheet-c78-729807.pdf> [Citado 20 de enero de 2015].

La serie Cisco UCS 6200 está construido para consolidar el tráfico LAN y SAN en una sola estructura unificada, el ahorro de los gastos de capital y gastos operativos asociados a múltiples redes paralelas que puedan presentarse en un mismo entorno de conectividad, además permite la conexión de fibra óptica para optimizar el proceso de cableado dentro de los bastidores.

Figura 17 Cisco Unified Data Center.

Fuente http://www.cisco.com/c/en/us/solutions/data-center-virtualization/architecture.html.

Los puertos unificados soportan y permiten módulos de expansión para apoyar conexiones directas de Cisco UCS para redes SAN (Storage Area Network) existentes.

Permite una configuración de alta disponibilidad, permitiendo interconexiones de stack para gestionar plenamente todos los elementos de Cisco UCS además permite la conectividad con el Cisco UCS chasis blade serie 5100 el cual se mantiene a través de los Cisco UCS 2100 o 2200 Series Fabric Extender en cada chasis blade. Las interconexiones de la serie Cisco UCS 6200 apoyan la administración a través de un puerto de gestión dedicado Ethernet 10/100/1000 Mbps, Cisco UCS Manager normalmente se implementan en una configuración

activa-pasiva agrupado en interconexiones redundantes conectados a través de puertos 10/100/1000 Ethernet agrupados.

Para entornos virtualizados, la serie Cisco UCS 6200 soporta redes virtualizadas y permite las interconexiones para proporcionar conectividad con las máquinas virtuales basándose en políticas de conectividad virtual, permitiendo así un modelo operativo consistente para entornos físicos y virtuales.[29]

- Switch Cisco Nexus 5500

El Cisco Nexus 5500 permite simplificar la convergencia lo que los convierte en el switch ideal para un diseño top-of-rack y realizar implementaciones tradicionales.

Figura 18 Cisco Nexus 5548UP Switch (Front and Back).

Fuente. Cisco Nexus 5548P, 5548UP, 5596UP, and 5596T Switches Data Sheet.

Permite hasta 96 puertos unificadas además permite eficiencia operativa a través de un único punto de gestión y capacidad de programación FEX, realiza

[29] Cisco UCS 6200 Series Fabric Interconnects Data Sheet [en línea]. <http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-6200-series-fabric- interconnects/data_sheet_c78-675245.html> [Citado 20 de enero de 2015].

programación de secuencias de comandos Python, scripting TCL, el Kit de Cisco Una Plataforma (onePK), y su arquitectura flexible permite satisfacer las diversas necesidades de los clientes independiente su infraestructura permite amplia conectividad incluyendo, 10 Gigabit Ethernet, 10G-BASE-T, 40 Gigabit enlaces ascendentes Ethernet, conexión canal de fibra sobre Ethernet (FCoE).

La plataforma Cisco Nexus 5500 está equipado con módulos de expansión que se pueden utilizar para aumentar el número de puertos GE a 10 Gigabit Ethernet o 40 puertos Gigabit Ethernet y FCoE para realizar conexiones a redes SAN de conexión de fibra según sea la necesidad del ambiente de conectividad.

- **Cisco Nexus 2248TP GE Fabric Extender**

Figura 19 Cisco Nexus 2148T, 2248TP, 2224TP, and 2232PP Fabric Extenders.

Fuente. Cisco Nexus 2248TP GE Fabric Extender

Los Fabric extender Cisco Nexus 2248TP GE permite un diseño de arquitectura nuevo y flexible reduciendo la complejidad de administración, permitiendo un acceso unificado a arquitecturas de cualquier escala, además facilita migraciones de ambientes virtualizados y unificados.

El appliance Nexus 2148T GE Fabric Extender cuenta con 48 puertos para conectividad de servicios independientes, 4 puertos FTP para conexión de fibra óptica y tan solo ocupando una unidad de rack, entre los beneficios que puede encontrar este equipo se puede encontrar:

Flexibilidad de arquitectura: ya que proporciona una alta gama de opciones como conectividad 100 Megabit Ethernet y 10 Gigabit Ethernet para ambientes unificados y soporte de conectividad mediante SFP, SFP+ y CX1 sobre cobre y fibra óptica, además se ajusta para organización en espacios optimizados ya sea para ToP (Top of Rack)O EoR (End of Rack), ofrece administración plug and play la cual incluye autoconfiguración, reduce costos de cableado y optimiza la forma de cablear dentro del rack de comunicaciones [30]

[31]

[30] Cisco Nexus 2000 Series Fabric Extenders [en línea]. <http://www.cisco.com/c/dam/en/us/products/collateral/switches/nexus-2000-series-fabric-extenders/at_a_glance_c45-511599.pdf > [Citado 20 de enero de 2015].

[31] Cisco ME 3600X Series Ethernet Access Switches [en línea]. <http://www.cisco.com/c/en/us/products/collateral/switches/me-3600x-series-ethernet-access- switches/data_sheet_c78-601946.pdf> [Citado 20 de enero de 2015].

4.3 COSTOS

Tabla1. Costos migración IPv6 anual Cloud Sonda S.A.

Cantidad	Recurso	Descripción	Costo Mensual	N. Meses	Costo Total
0	Recursos Físicos	La empresa Sonda de Colombia S.A. cuenta con la infraestructura necesaria en la Cloud para realizar el proceso de migración de IPv4 – IPv6.	0	6	0
1	Recursos Humanos	Ing. de sistemas que realice el proceso de migración de IPv4 – IPv6 durante el tiempo estimado del proyecto cuatro meses.	2.000.000	4	8’000.000
1	Pool de direcciones /27 publicas IPV4	Pool de direcciones publicas IPV4 ya que no hay para próximos servicios, a implementar.	1.500.000	1	1.500.000
1	Pool de direcciones /64 publicas IPV6	Pool de direcciones publicas IPV6 para publicaciones de requerimientos del sector gobierno.	1.500.000	1	1.500.000
1	DNS AAAA	Upgrade a DNS AAAA que permita configuración DNS IPV6	0	0	0
					11’000.000

5 PROCEDIMIENTO DE IMPLEMENTACIÓN IPV6.

5.1 REVISIÓN DE COSTOS POOL IPV6 vs IPV4.

Se solicita cotización de pool IPv6 a LACNIC que es el registro de direcciones de Internet para América Latina y Caribe, esta cotización se puede solicitar por dos métodos como usuario final o como proveedor ISP, la opción solicitada es por ISP ya que SONDA S.A a futuro venderá direccionamiento IPv6 a sus clientes; para este tipo de servicio LACNIC ofrece un direccionamiento mínimo de /64 que son aproximadamente 18 trillones de direcciones por un costo anual de 500 dólares en comparación de un pool IPv4 /27 público que contiene 30 direcciones el cual tiene un valor anual de 500 dolares con el proveedor Level 3.

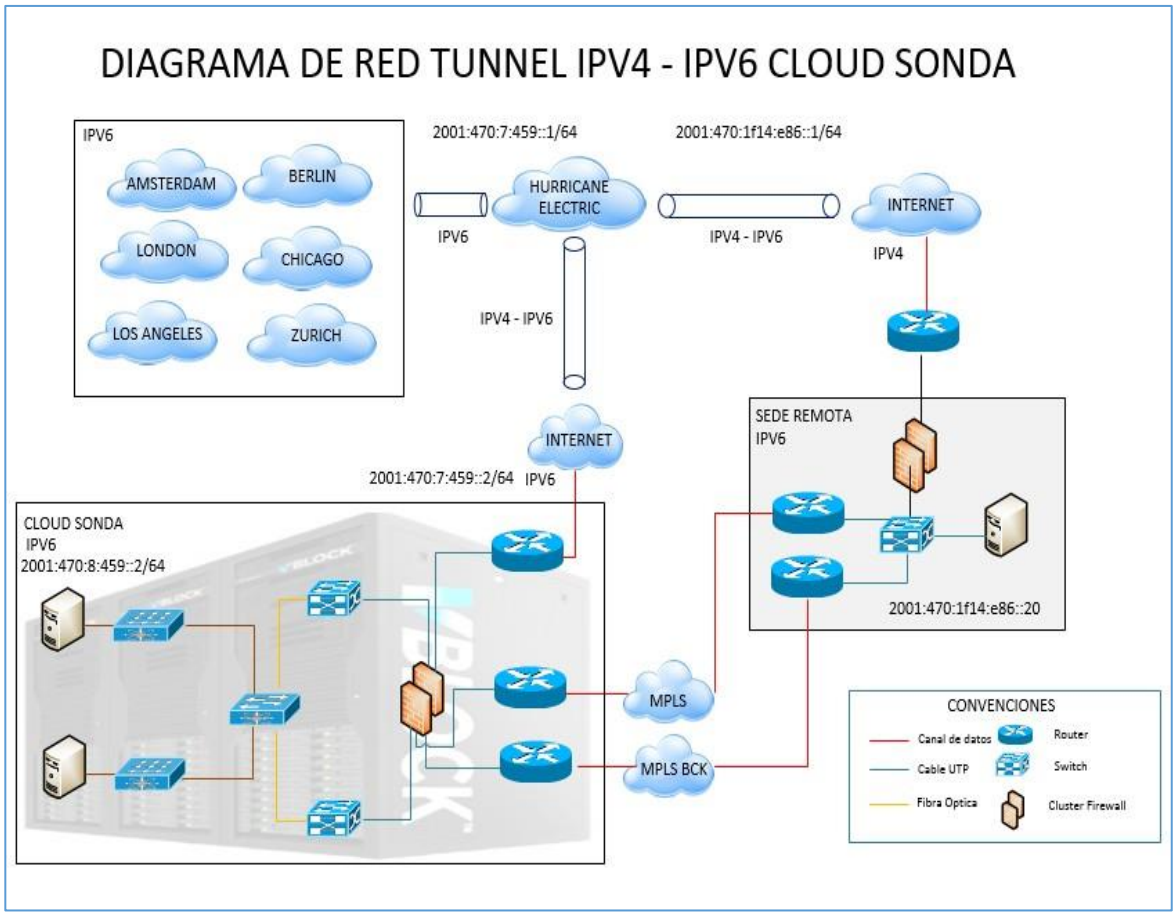
5.2 ELECCIÓN DE METODO DE MIGRACIÓN.

Revisando las diferentes estrategias de migración citadas en el punto 2.2.6 (Estrategias De Migración IPv4 – IPv6) se opta por la utilización de tunnel broker sobre las demás opciones teniendo en cuenta que los equipos tengan direccionamiento IPv4 – IPv6 simultáneamente funcionando, sin presentar afectación en los servicios ya publicados, además con tunnel broker se puede realizar la configuración de los túneles y direccionamiento directamente en los equipos finales, sin necesidad de modificar configuración de enrutamiento en los switches ofreciendo un menor impacto en caso de alguna falla de configuración en un switch o router como se debe realizar para algunos de los otros métodos de migración. TunnelBroker.com proporciona conexión a redes IPv6 mediante tráfico encapsulado sobre una infraestructura ya configurada con protocolo IPv4, en la cual un servidor de tunnel broker ofrece diferentes servidores a nivel mundial para levantar túneles independientes.

5.3 DIAGRAMA PUBLICACIÓN DE SERVICIOS.

En la Figura 20 se muestra gráficamente a detalle la forma en la que se visualiza la arquitectura de red a nivel lógico, después de ser realizada la implantación de IPV6 mediante tunnelbroker y server tunnel de Hurricane Electric en la Cloud empresarial de Sonda S.A., se evidencian las tres partes involucradas tunnel server, sede remota, y Datacenter Level 3.

Figura 20 Conexión IPV6 Cloud Sonda de Colombia.



Fuente: Diagrama propio Visio 2013 – 2015.

5.4 PROVEEDOR IPV6.

Para utilizar este servicio de tunnelbroker es necesario tener un túnel IPv6 el cual está disponible para la mayoría de los sistemas operativos o enrutadores que también tiene IPv4. Este servicio de túnel está orientado a desarrolladores y experimentadores que quieren una plataforma túnel estable.

Ventajas del uso del servicio de túnel de HE sobre otros incluyen:

- Dirigido por un ISP de negocios con 24 x 7 personal en múltiples ubicaciones y un backbone internacional.
- Capacidad para obtener su propio direccionamiento IPV6 / 48 prefijo.
- Capacidad para obtener una vista completa de la tabla de enrutamiento IPv6 BGP4 +.
- Capacidad para utilizar el túnel ahora después de un sencillo proceso de registro.
- Capacidad para crear un túnel direccionado a servidores de túneles en diferentes locaciones geográficas (Ashburn, Chicago, Dallas, Denver, Fremont, Kansas City, Los Ángeles, Miami, Nueva York, Palo Alto, Phoenix, San José, Seattle, Toronto.[32]

[32] IPv6 Tunnel Broker [en línea].
< https://tunnelbroker.net/> [Citado 20 de agosto de 2015].

5.5 CREACIÓN TUNEL IPV6 EQUIPO REMOTO.

Para la creación del pool de IPV6 necesitamos una dirección IP pública IPV4 que responda tráfico ICMP (Ping), para lo cual se utilizó una dirección IP del pool público de la sede remota y se asignó directamente al equipo Windows 7 con el que se establecerá el túnel IPV6, (190.144.157.179) para permitir el tráfico ICMP se debe crear la regla de acceso en el firewall como se ve en la Figura 21 donde se permite cualquier tráfico (Any) hacia el equipo remoto el cual se le realizó un NAT para que responda ICMP por la dirección IP pública.

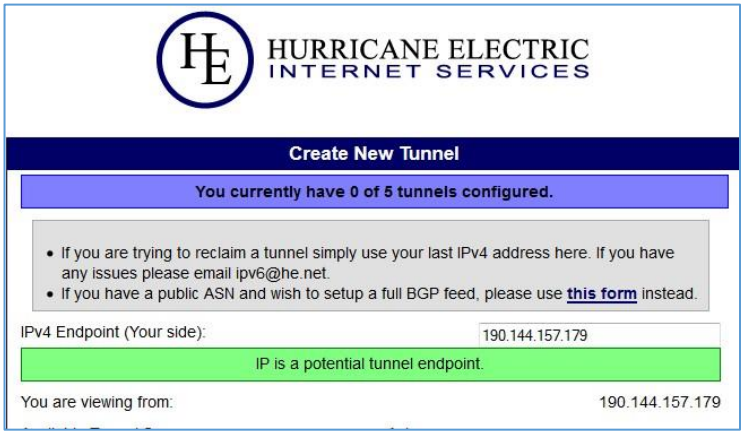
Figura 21 Creación regla Firewall CheckPoint.

Name	Source	Destination	VPN	Service	Action	Track	Install On
ICMP Publico	Any	REMOTO_IPV6	Any Traffic	Any	accept	Log	Policy Targets

Fuente: Captura Propia – 2015.

Después se procede a verificar que la dirección IP responda ping desde internet o propiamente desde la página web, ya que para levantar el tunel IPV6 es necesario la respuesta de paquetes ICMP desde la web Hurricane Electric hasta la dirección IP pública del equipo remoto, lo cual se verifica en la Figura 22.

Figura 22 Verificación ping HE.



Fuente: http://he.net/- 2015

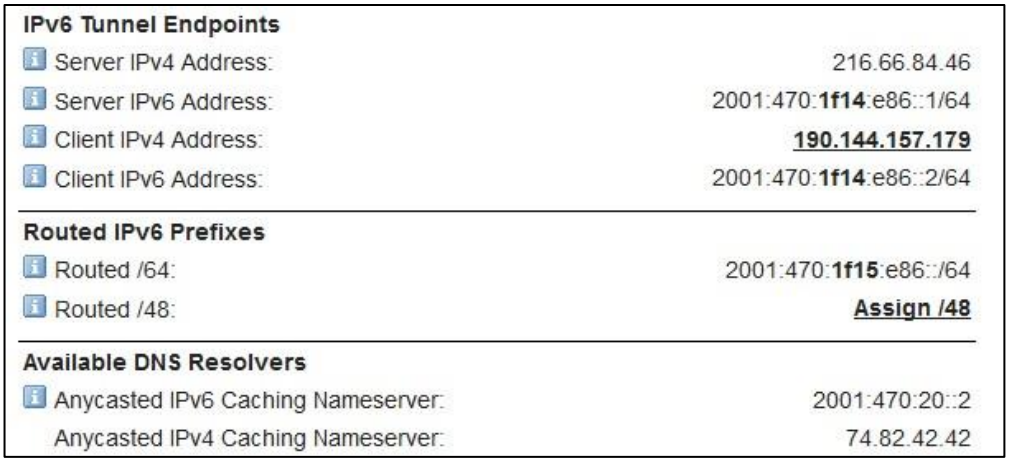
Posterior a que responda ping se procede a escoger el servidor de tunel entre los que estén disponibles.

Figura 23 Elección Tunnel Server HE.

Fuente: http://he.net/- 2015.

Una vez que se haya escogido el servidor se tendrá establecido el túnel por parte de HE y el servidor de túnel nos estregará dos pool de direcciones IPV6 uno para los endpoint que son los equipos de comunicaciones con los que se levanta directamente el tunel (2001:470:1f10:1113c::1/64) y un segmento enrutado que es de los equipos que están detrás de los endpoint como lo pueden ser equipos finales o servidores (2001:470:1f11113c::/64), los cuales nos permiten cada uno tener 18,446,744,073,709,551,616 direcciones disponibles.

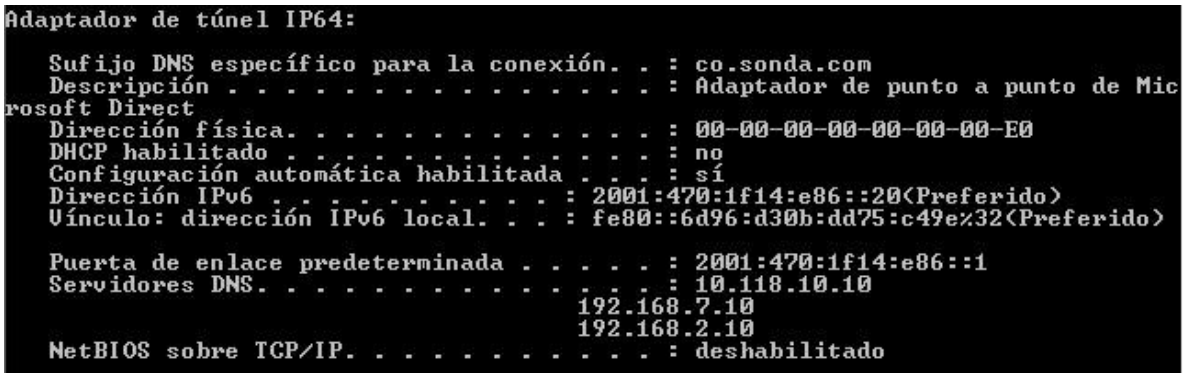
Figura 24 Verificación Tunnel IPV6 HE.



Fuente: http://he.net/- 2015.

Al realizar la anterior configuración ya se tiene levantado el peer de Hurricane Electric lo que se debe realizar a continuación es levantar el peer del equipo por medio de CLI línea de comando para poder tener el equipo con el que vamos a probar las conexiones y publicaciones IPV6 de la cloud empresarial, se procede a configurar una de las direcciones del pool tunel endpoints, y asignando de puerta de enlace predeterminada la dirección del server IP address.

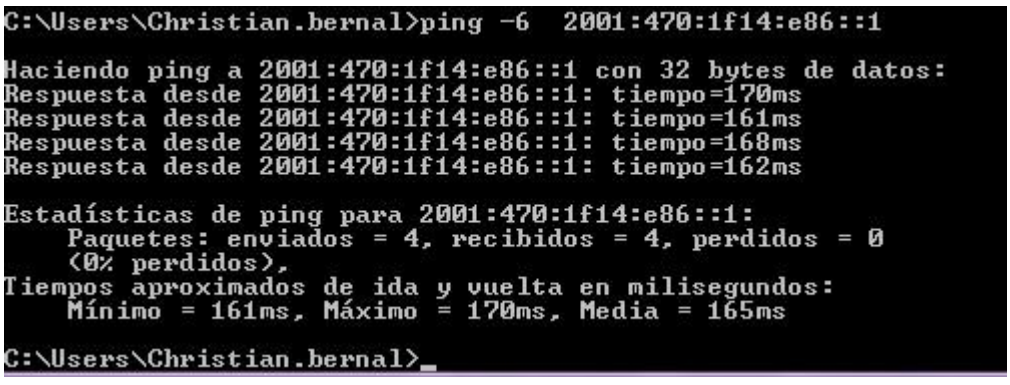
Figura 25 Verificación Tunnel IPV6 HE.



Fuente: Captura Propia – Año 2015.

Procedemos a verificar la comunicación entre los peer mediante el comando ping -6 con destino al servidor IPV6 desde el equipo de la sede remota.

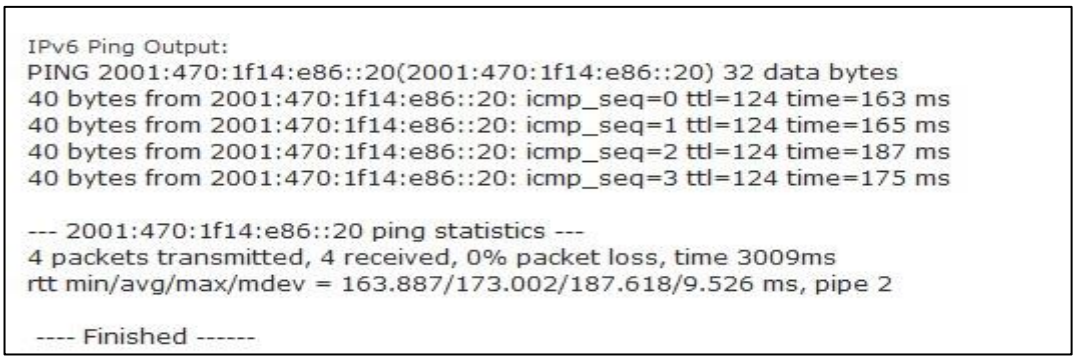
Figura 26. Verificación ping servidor Tunnel IPV6.



Fuente: Captura Propia – Año 2015.

Verificamos desde internet hacia el equipo remoto mediante la herramienta web http://www.subnetonline.com con lo cual se verifica que desde un equipo con configuración IPv6 en internet es visible el equipo remoto que se configuro previamente con la misma configuración de protocolo.

Figura 27. Verificación ping http://www.subnetonline.com.



Fuente: http://www.subnetonline.com – 2015.

5.6 CREACIÓN TUNEL IPV6 EQUIPOS CLOUD.

Ya que se tiene configurado el tunel IPV6 para el equipo con el cual se realizarán las pruebas de acceso a los aplicativos y publicaciones se procede a publicar cada uno de los servicios anteriormente nombrados dependiendo del sistema operativo de cada uno de los servidores se debe realizar la configuración de la interfaz.

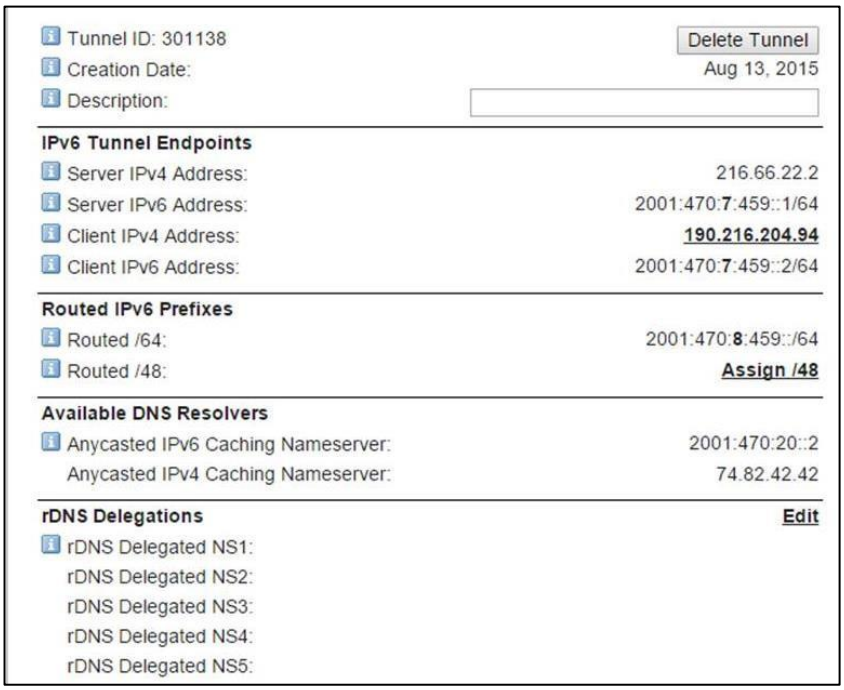
5.6.1 Configuración Tunel IPV6 Cloud.

La configuración del peer de IPV6 en la cloud se realizará en un servidor Linux el cual tiene acceso a todos los servidores que van a publicar servicios mediante IPV6, para realizar esta configuración es necesario crear un tunel exclusivo para la red de la Cloud similar a como se realizó para el equipo remoto aunque se debe tener en cuenta que el cambio de sistema operativo modifica la configuración en su totalidad.

Primero se debe publicar y permitir el tráfico ICMP a la dirección con la que se va a realizar el peer del tunel IPV6,

Luego se procede a configurar el tunel en el servidor IPV6 el cual nos entrega nuevamente dos pools totalmente diferentes a los del tunel del equipo remoto, uno para los peers y el otro para los equipos de la red que están detrás de los peers.

Figura 28 Verificación tunnel HE.

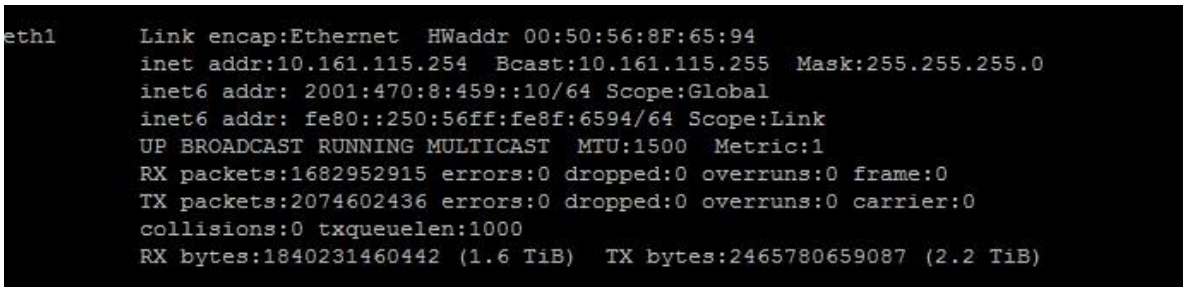


Fuente: http://he.net/- 2015

Luego de tener la dirección a la que vamos a destinar como Gateway del tunel de IPV6 se debe realizar la configuración de la interfaz en el equipo que nos servirá de peer para el tunel IPV6, se debe tener en cuenta que para los equipos de sistema operativo Linux tenemos que realizar algunas configuraciones adicionales como habilitación de servicios IPV6 creación de rutas independientes hacia los dos pool entregados por el proveedor IPV6, creación de reglas del firewall propios del server (IPTABLES), configuración del tráfico entrante y saliente para que permita los dos protocolos simultáneamente, y por último la configuración de la interfaz que utilizaremos como tunel y de la interfaz virtual que tendrá

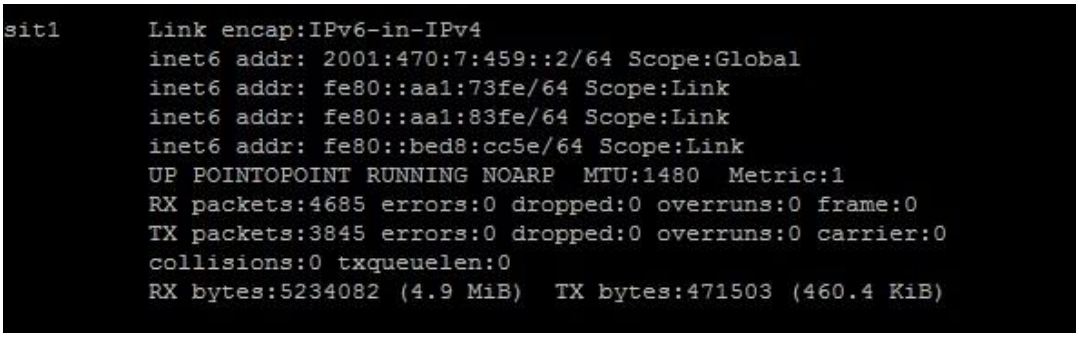
comunicación del otro segmento las cuales quedarían de la siguiente manera como se evidencia en las Figuras 29 – 30.

Figura 29 Verificación interfaz peer tunel IPV6.



Fuente Propia – Año 2015.

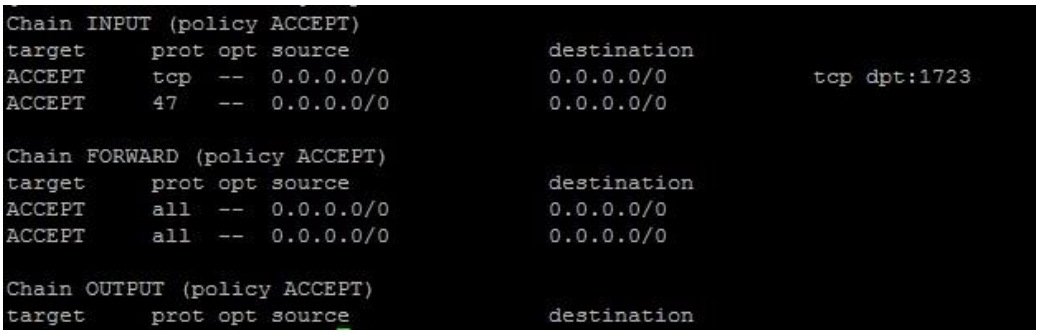
Figura 30 Verificación interfaz tunel IPV6 nivel interno.



Fuente Propia – Año 2015.

Se verifica el firewall interno del server y se configura una regla any any para permitir los diferentes puertos por los que se establece la comunicación

Figura 31 Verificación IPTables peer tunel IPV6 Cloud.



Fuente Propia – Año 2015.

Se crean y se verifican las rutas ipv6 que permiten el direccionamiento interno y externo en el peer del tunel.

Figura 32 Print rutas equipo peer tunel IPV6 Cloud.

```
fe80::/64 dev eth0  metric 256  expires -20064460sec mtu 1500 advmss 1440 hoplimit 4294967295
fe80::/64 dev eth1  metric 256  expires -20064455sec mtu 1500 advmss 1440 hoplimit 4294967295
fe80::/64 dev eth2  metric 256  expires -20064454sec mtu 1500 advmss 1440 hoplimit 4294967295
fe80::/64 via :: dev sit1  metric 256  expires 20645872sec mtu 1480 advmss 1420 hoplimit 4294967295
default dev sit1  metric 1  expires 20645873sec mtu 1480 advmss 1420 hoplimit 4294967295
```

Fuente: Captura propia - 2015

Luego se procede a permitir en el archivo **/etc/sysctl.conf** el forwarding de paquetes IPV6 hacia los demás equipos de la red.

Figura 33 Configuración forwanding peer tunel IPV6 Cloud.

```
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
net.ipv6.conf.all.forwarding=1

# Controls source route verification
net.ipv4.conf.default.rp_filter = 1
```

Fuente: Captura propia - 2015

Se verifica la salida hacia direcciones IPV6 probando con el comando ping6 a la dirección del peer indicada por HE para verificar la conexión del tunel.

Figura 34 Ping -6 peer HE.

```
PING 2001:470:1f0e:19b::1(2001:470:1f0e:19b::1) 56 data bytes
64 bytes from 2001:470:1f0e:19b::1: icmp_seq=0 ttl=60 time=105 ms
64 bytes from 2001:470:1f0e:19b::1: icmp_seq=1 ttl=60 time=105 ms
64 bytes from 2001:470:1f0e:19b::1: icmp_seq=2 ttl=60 time=107 ms
64 bytes from 2001:470:1f0e:19b::1: icmp_seq=3 ttl=60 time=106 ms
64 bytes from 2001:470:1f0e:19b::1: icmp_seq=4 ttl=60 time=109 ms
64 bytes from 2001:470:1f0e:19b::1: icmp_seq=5 ttl=60 time=106 ms
64 bytes from 2001:470:1f0e:19b::1: icmp_seq=6 ttl=60 time=106 ms
64 bytes from 2001:470:1f0e:19b::1: icmp_seq=7 ttl=60 time=106 ms

--- 2001:470:1f0e:19b::1 ping statistics ---
```

Fuente: Captura Propia 2015.

5.6.2 Publicación acceso SSH.

La publicación de este servidor es indispensable ya que es el que permite el acceso SSH a los equipos de red de la Cloud incluso estando el canal MPLS entre la Cloud y la sede remota caído, ya que tiene una conexión directa a los equipos de borde de la Cloud, este server tiene sistema operativo GNU/Linux 2.6.18 sin entorno gráfico y la configuración de la interfaz IPV6 se debe realizar de manera similar al servidor anterior pero sin involucrar la configuración que va hacia el tunel IPV6 como se ve en la Figura 35.

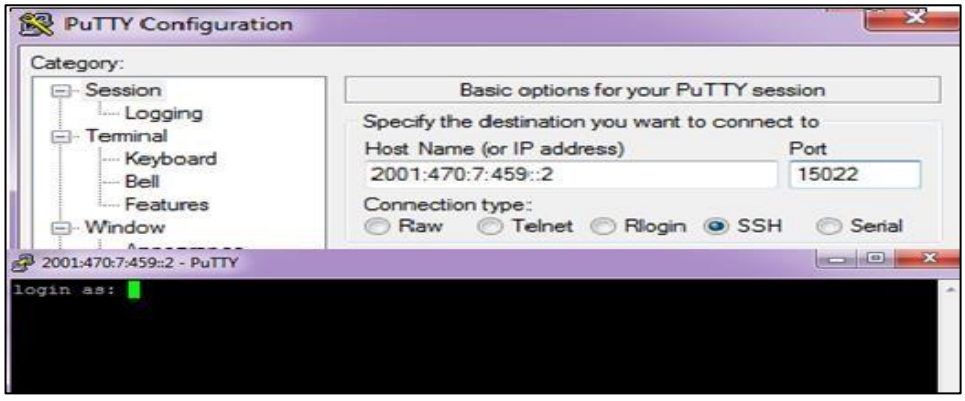
Figura 35. Verificación interfaz server SSH.

```
eth1      Link encap:Ethernet  HWaddr 00:50:56:8F:65:94
          inet addr:10.161.115.254  Bcast:10.161.115.255  Mask:255.255.255.0
          inet6 addr: 2001:470:8:459::10/64 Scope:Global
          inet6 addr: fe80::250:56ff:fe8f:6594/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1683500287 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2074603681 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1840267474176 (1.6 TiB)  TX bytes:2465780905852 (2.2 TiB)
```

Captura Propia – 2015.

Una vez realizada la configuración se procede a verificar desde la sede remota la cual tiene salida a direcciones IPV6, verificando mediante el acceso SSH a este equipo previamente configurado como se evidencia en la Figura 36.

Figura 36 Verificación ingreso server SSH.



Captura Propia – Año 2015.

5.6.3 Publicación portales web.

Los portales web a publicar están montados en servidores GNU/ Linux 2.6 por lo cual la configuración es similar a la del server anterior que permite el ingreso SSH a continuación se encuentran las pruebas de acceso por navegador web a estos portales anteriormente publicados en las figuras 37 y 39.

El portal de monitoreo de la herramienta Zabbix de los equipos de la cloud está publicado por la dirección 190.216.135.204 el cual responde al URL https://cloudmonitor.co.sonda.com/zabbix/ el cual a su vez está configurado con la dirección pública IPV6 2001:470:8:459::11.

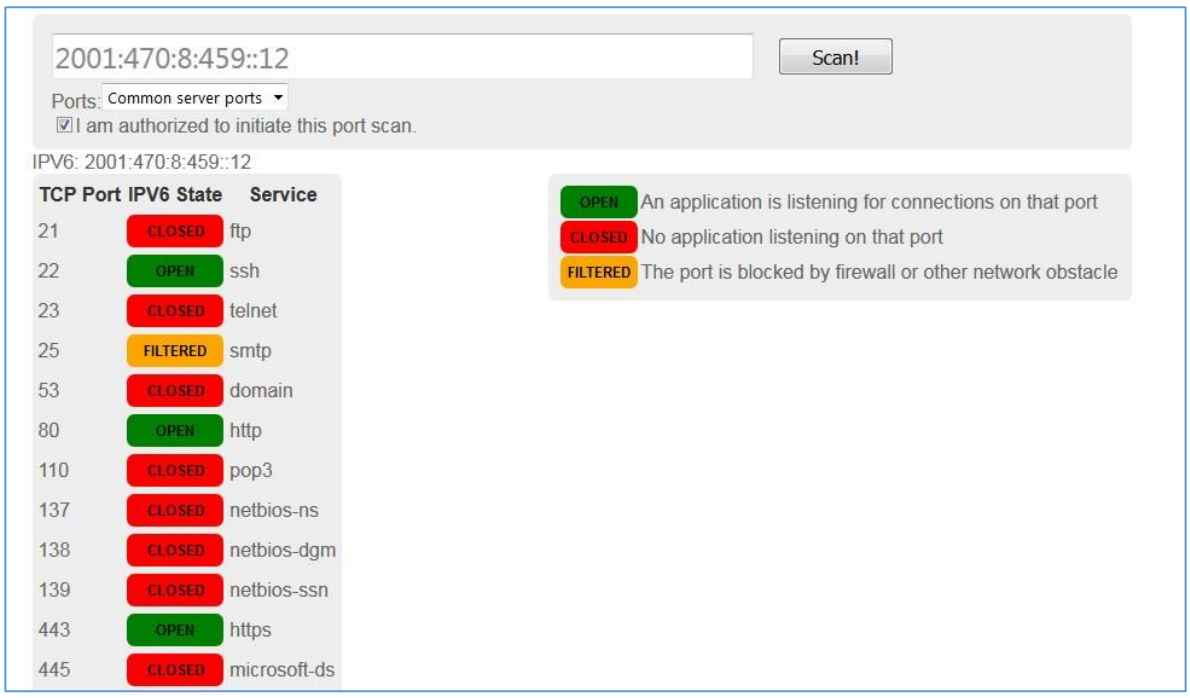
Se procede a realizar pruebas desde el navegador web ingresando por la dirección IPV6 para lo cual hay que tener en cuenta que se debe colocar la dirección IPV6 dentro de corchetes cuadrados [2001:470:8:459::11] para que el navegador lo interprete y permita el ingreso, se verifica y responde correctamente la página principal publicada.

Figura 37 Verificación ingreso portal Zabbits.

Fuente: Captura Propia – Año 2015.

Al realizar un Scan Port con la herramienta online http://www.ipv6scanner.com encontramos que desde internet se puede acceder a la URL y vemos los puertos que se encuentran abiertos como lo son el 80 – 443 para la publicación web y el 22 para el acceso SSH.

Figura 38 Verificación puertos con ipv6scanner.

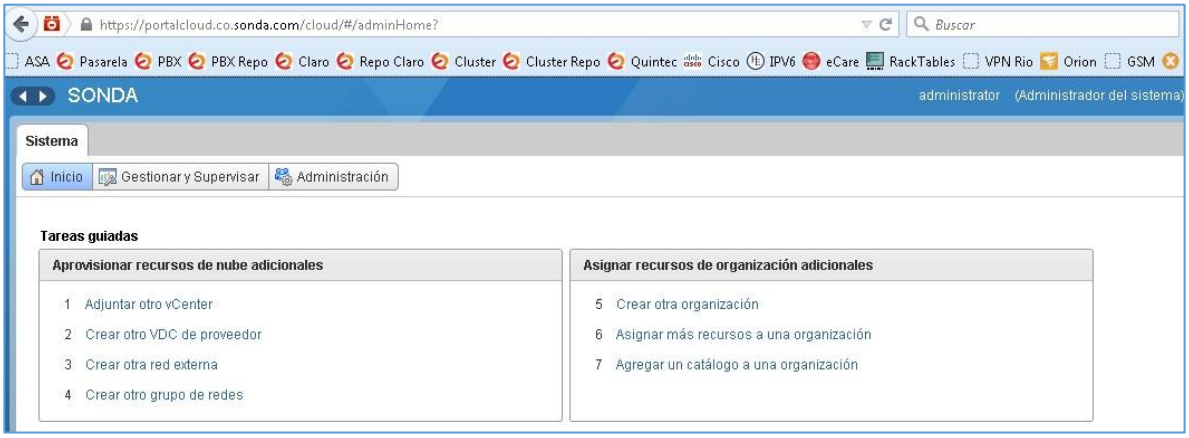


Fuente Propia – Año 2015.

Los cuales eran los resultados esperados ya que por lo puertos TCP que aparecen abiertos es por lo que se tiene acceso al portal web y a la administración del server desde internet IPV6.

Igualmente se realizan las pruebas para el portal web portalcloud.co.sonda.com el cual responde a la dirección IP IPV6 [2001:470:8:459::12] y se realiza el logueo correspondiente para verificar el funcionamiento del mismo. Figura 39

Figura 39 Verificación ingreso portalcloud.co.sonda.com IPV6.



Fuente: portalcloud.co.sonda.com – Año 2015.

5.6.4 Servidor JUMP Windows

Similar al servidor SSH montado en Linux previamente publicado es necesario la publicación del servidor de salto el cual esta tiene sistema operativo Windows server 2008 R2 el cual tiene la función de compartir el escritorio remoto para la administración de algunos equipos de clientes, desde consolas internas.

Para este servidor en específico es necesaria la validación que en el firewall perimetral y en el firewall interno se permita la conexión al puerto TCP 3389 para que las conexiones externas sean permitidas.

Luego de realizar las validaciones correspondientes se procede a configurar la interfaz virtual que permitirá la conexión al server por medio de IPV6, para esto se verifica una de las direcciones disponibles del pool de equipos finales y se procede a la configuración similar como se realizó con el equipo de la sede remota aunque con algunas variables ya que a pesar de ser Windows existen algunas diferencias en la configuración al ser un equipo Windows 7 y el otro Windows server.

Se procede a la configuración de la interfaz asignando la dirección 2001:470:8:459::15 a la cual se debe agregar el puerto de conexión al momento de realizar las validaciones correspondientes en caso de que se diferente al 3389 que se tiene por defecto.

Figura 40 Verificación ingreso escritorio remoto.

Captura Propia – Año 2015

En la Figura 40 se evidencia la correcta conexión del equipo destino bajo su direccionamiento IPv6.

6. PRUEBAS INFRAESTRUCTURA IPV4-IPV6.

6.1 PRUEBA IPV6TEST.COM IPV4.

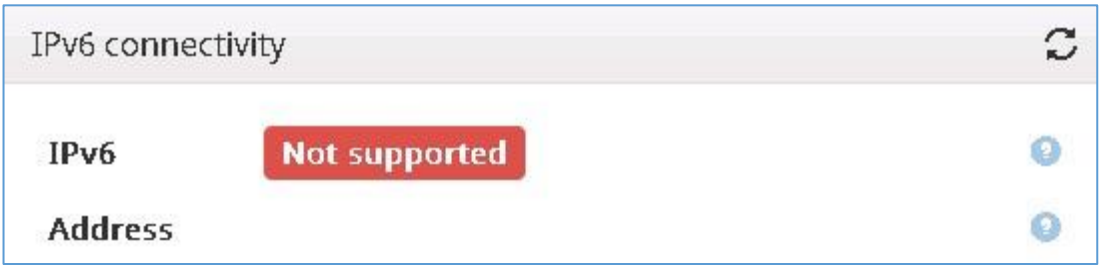
Se realizan las pruebas de conectividad y verificación de conexión antes de realizar la implementación de IPV6, desde un equipo de la LAN 10.161.115.0/24 perteneciente a la red Cloud de Sonda S.A, obteniendo los siguientes resultados Figura 41, 42 y 43.

Figura 41 Verificación conectividad IPV4 Datacenter.

Fuente: http://ipv6test.com – Año 2015

En la Figura 43 se verifica la conexión actual se realiza por conexión IPV4 mediante la dirección IP pública 190.216.135.203 entregada por el ISP Level 3, además se revisa que las conexiones vía IPV6 en el momento no se encuentran activas, ni hay ninguna configuración funcional para este servicio.

Figura 42 Verificación conectividad IPV6 Datacenter.



Fuente: http://ipv6test.com – Año 2015

La configuración de los DNS en el momento solo se encuentra configurada y funcional para el protocolo IPV4 como se evidencia en la Figura 43.

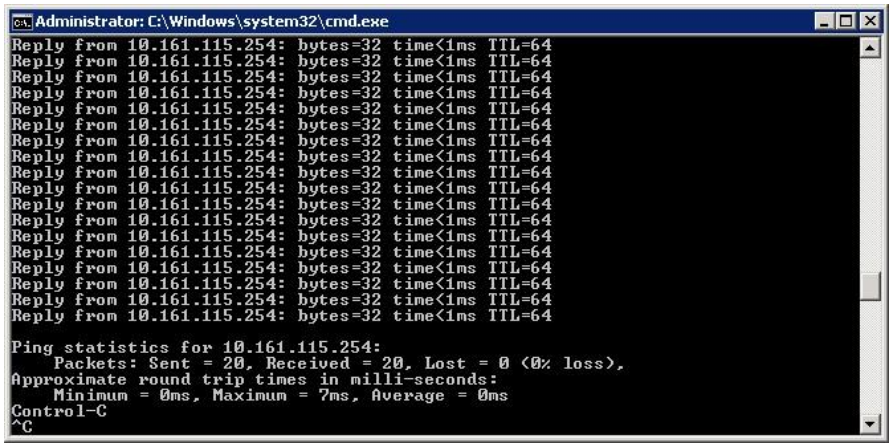
Figura 43 Verificación configuración DNS Datacenter.

Fuente: http://ipv6test.com – Año 2015

6.2 PRUEBAS DE TIEMPO DE RESPUESTA NIVEL LAN IPV4.

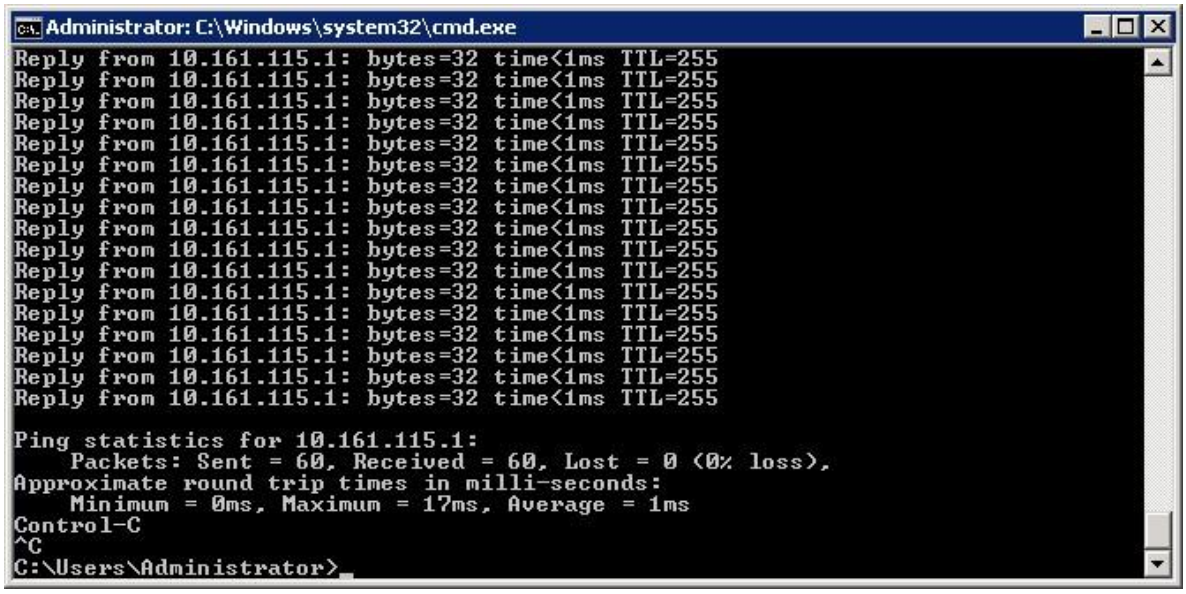
Antes de realizar cualquier configuración sobre los equipos de la cloud se realizan pruebas de tiempo de respuesta a nivel interno teniendo dos puntos de referencia que son un host en la misma LAN y la puerta de enlace de la LAN que es la interfaz física del Cluster Firewall ASA como se evidencia en las figuras 44 y 45.

Figura 44 Verificación ping server en la misma red.



Captura Propia – Año 2015

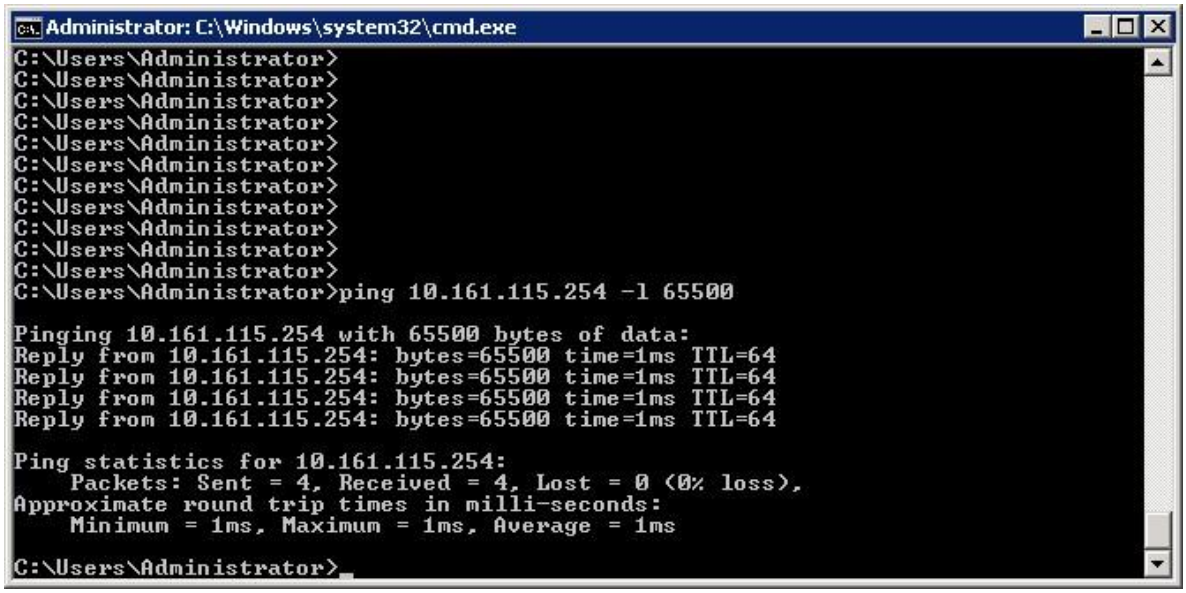
Figura 45 Verificación ping puerta de enlace de la red.



Captura Propia – Año 2015

Se realizan pruebas del mismo ping a nivel interno con más peso de bytes con el tamaño máximo permitido por el CDM 65500bytes y se observan tiempos de respuesta iguales a 1 ms como se evidencia en la Figura 46.

Figura 46 Verificación ping con mayor peso.

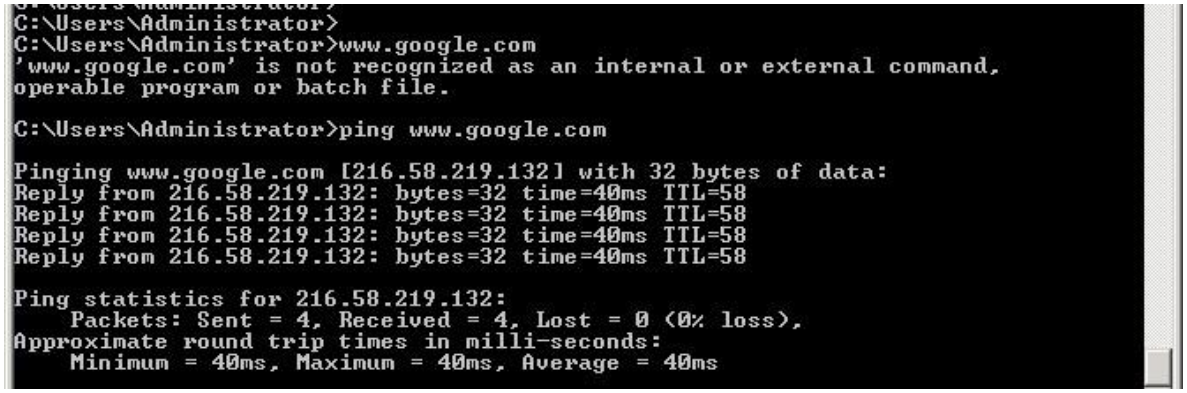


Captura Propia – Año 2015

6.3 PRUEBAS DE TIEMPO DE RESPUESTA NIVEL WAN IPV4.

Es necesario realizar pruebas a nivel WAN verificando tiempos de respuesta hacia una página externa como lo es www.google.com en la cual se ven tiempos estándar de 40ms independiente el número de paquetes enviados como se evidencia en la Figura 47.

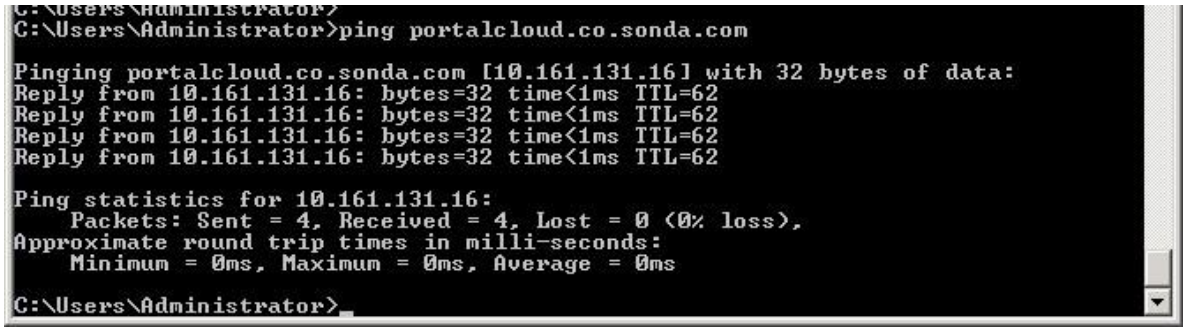
Figura 47 Verificación ping a google.



Captura Propia – Año 2015

Se verifica tiempos de respuesta a portalcloud.co.sonda.com y los tiempos de respuesta son mucho mejores ya que no necesita salir a internet para resolver esta URL, porque la encuentra a nivel interno lo cual se puede visualizar en la Figura 48.

Figura 48 Verificación ping portalcloud.co.sonda.com



Captura Propia – Año 2015

6.4 PRUEBA IPV6TEST.COM IPV6.

Se realizan las pruebas previamente realizadas en el punto 6.1 luego de realizar la configuración de IPV6 y la configuración del tunel previamente realizada, verificando que los equipos tienen salida por el servidor tunel IPV6 de Hurricane Electric, con la dirección asignada en la interfaz del equipo remoto como se evidencia en la Figura 49.

Figura 49 Verificación conectividad IPV6 sede remota

Fuente: http://ipv6test.com – Año 2015

Entre las pruebas realizadas se verifica que el navegador permita resolver url de direcciones IPV6 lo cual se evidencia en la Figura 50.

Figura 50 Verificación conexión Browser IPV6.

Fuente: http://ipv6test.com – Año 2015

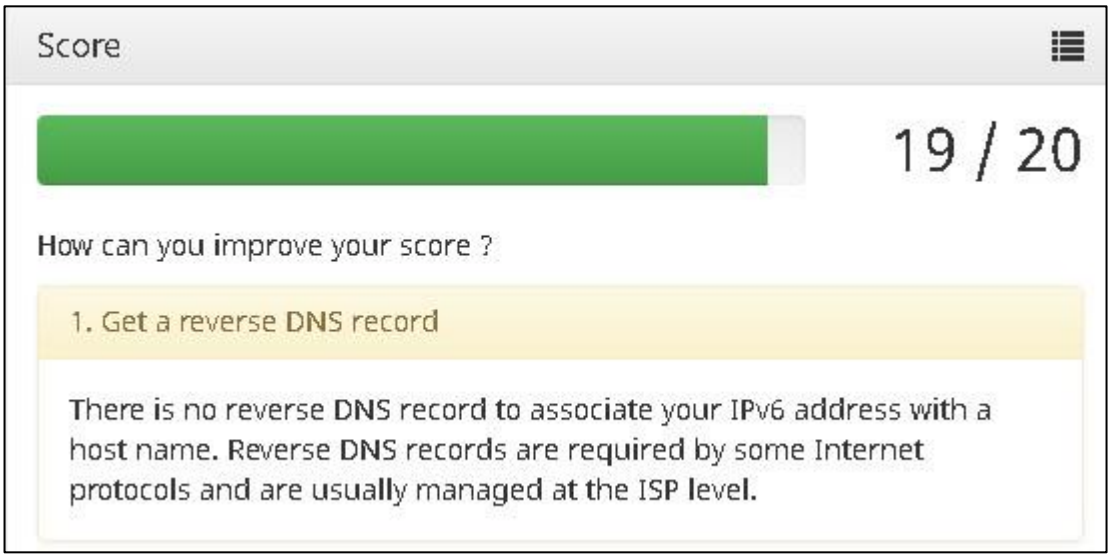
Se verifica configuración de DNS tanto para IPV4 como para IPV6 lo que evidencia en la Figura 51 que permite la resolución de nombres a nivel de IPV6

Figura 51 Verificación DNS IPV6.

Fuente: http://ipv6test.com – Año 2015

En general IPV6 test realiza un análisis final de la configuración total en la cual se obtiene un score de 19 sobre 20 como se evidencia en la Figura 52 ya que los portales publicados no tienen un servidor DNS público que soporte IPV6 en la actualidad.

Figura 52 Verificación resultados finales IPV6 Test

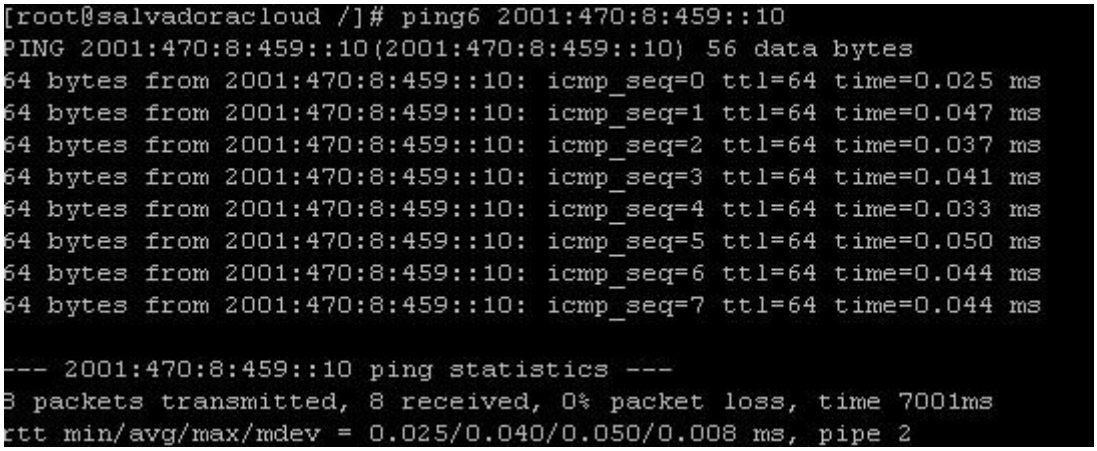


Fuente: http://ipv6test.com – Año 2015

6.5 PRUEBA CONEXIÓN LAN IPV6.

Al realizar pruebas de conexión LAN se evidencian tiempos menores a los realizados con direccionamiento IPV4 de 1ms ver Figura 53.

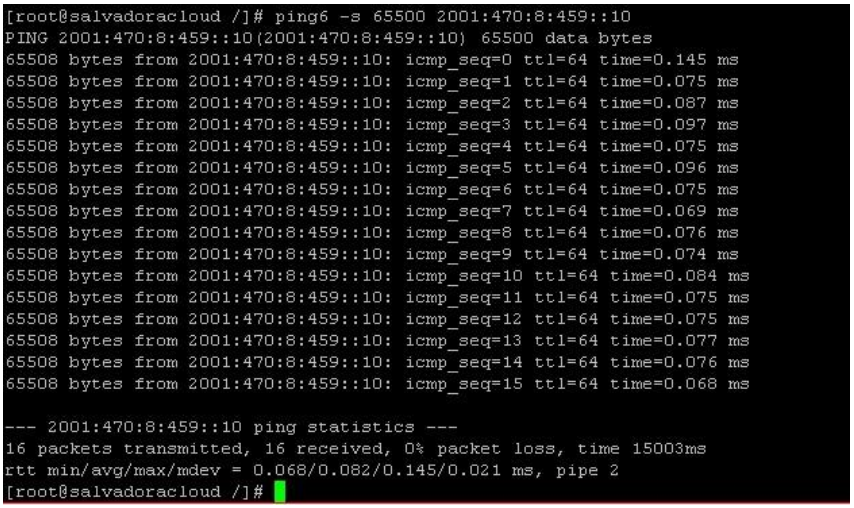
Figura 53 Verificación ping con destino server interno.



Captura Propia – Año 2015

Al realizar pruebas de ping con el peso mayor permitido de 65500 bytes se evidencia el mismo comportamiento que el la Figura 54 con un tiempo de respuesta menor.

Figura 54 Verificación ping con peso server interno.

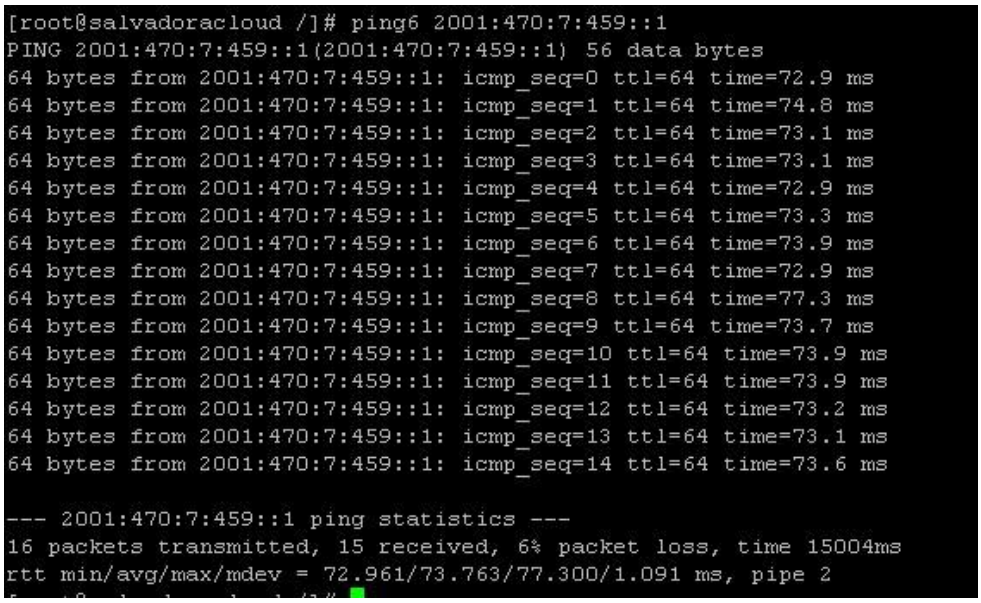


Captura Propia – Año 2015

6.6 PRUEBA CONEXIÓN WAN IPV6.

Al realizar pruebas de ping al peer de IPV6 indicado por el tunel server de HE se evidencia un promedio de tiempo de respuesta de 73.763 ms con un 6% de pérdida de paquetes ya que por razones de rutas a nivel de IPV6 el primer paquete se pierde en la mayoría de casos como se ve en la figura 55 y 56.

Figura 55 Verificación ping -6 peer HE.



Captura Propia – Año 2015

Figura 56 Verificación ping -6 a google.com.

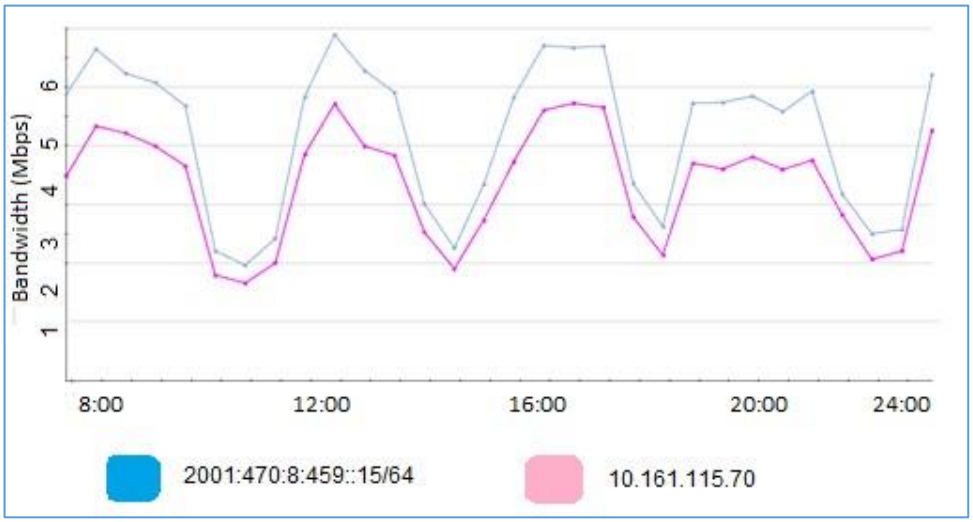
Captura Propia – Año 2015

7. ANÁLISIS DE RESULTADOS.

Después de realizar la correcta publicación de los servicios nombrados en el alcance a excepción de la VPN configurada por el cluster ASA, ya que por motivos de configuración del servidor tunel de Hurricane Electric entre las configuración que están a su alcance no está soportada el IOS del cluster ASA, por tal motivo para este proyecto no fue posible la configuración del mismo.

Luego de la configuración se procedió a realizar pruebas en dos equipos cada uno configurado en un protocolo diferente y se realizó la misma operación en los dos durante el día que fue realizar traspaso de archivos con un peso total de 30 GB al portal Mega.nz y se realizaron las configuraciones correspondientes en el cluster ASA para verificar el tráfico de los dos equipos durante el trascurso del día y verificar el ancho de banda utilizado por cada uno de los equipos, después de realizada la prueba se encuentra que el equipo con direccionamiento IPv6 consume más ancho de banda que cuando el equipo tiene direccionamiento IPv4 como se evidencia en la Figura 57.

Figura 57 Grafica de consumo de red.



Fuente: ASA 5525 Monitoring Module

Al verificar la infraestructura se comprueba que la infraestructura con la que cuenta el Datacenter a nivel de VBlock y Networking es óptima para la configuración de los servicios que se tienen actualmente publicados y los que se tienen a nivel interno configurados, sin ninguna degradación de los mismos; ya que el protocolo IPV6 es un avance en las comunicaciones hacia lo cual las grandes compañías desde hace varios años han estado predispuestas al cambio y por tal motivo su infraestructura se presta para este tipo de configuraciones y de migraciones.

En comparación con los servicios publicados se observa un comportamiento óptimo y competitivo contra los tiempos de respuesta a nivel IPV4 realizados en las verificaciones anteriores, se evidenció que es posible el acceso a portales web, diferente comunicación de servicios por diferentes puerto TCP – UDP como lo son sesiones remotas, servicio FTP, acceso SSH, y configuración de red interna con direccionamiento IPV6, sin ningún problema de compatibilidad o de afectación de los servicios a publicar, o de las publicaciones ya realizadas con el protocolo IPV4, la configuración del protocolo IPV6 con un proveedor de servicios varía en pocos parámetros ya que las condiciones son similares se recibe un pool de direcciones privado y público para realizar según los requerimientos de los servicios y de la red destino.

Tabla 2.Comparacion servicios en la red Cloud SONDA S.A.

Servicio	IPv4	IPv6	Observaciones
PortalCloud	190.216.135.204	2001:470:8:459::11/64	Es posible realizar la publicación por IPv6 y se prueba el acceso a la plataforma de virtualización pública.
Zabbix	10.161.115.28	2001:470:8:459::12/64	Es posible realizar la publicación por IPv6 y se prueba el acceso al portal de monitoreo.
Escritorio Remoto	10.161.115.70	2001:470:8:459::15/64	Es posible la conexión vía IPv6 al escritorio remoto como se realizaba usualmente.
Server SSH	10.161.115.254	2001:470:8:459::10/64	Es posible la conexión de manera SSH al servidor Linux e ingreso a su CLI.
Servidor Tunnel	10.161.115.254	2001:470:7:459::2/64	Es posible la creación del tunnel broken desde un server Linux permitiendo tiempos de respuesta menores de 1 ms a nivel externo e interno.
Server FTP	10.161.115.230	2001:470:8:459::20/64	Es posible el acceso a los archivos compartidos en el server FTP mediante el Client FTP.
Portal VPN	10.172.10.12	N/A	No es posible la configuración ya que el IOS de ASA no es compatible con los comando de creación de tunnel de HE.
PC	10.161.115.0/24	2001:470:8:459::25/64	Se configura un equipo a nivel interno con ningún servicio publicado con el que se realizan pruebas de navegación y acceso a los demás servicios.

Al revisar a nivel general desde el equipo de pruebas mediante IPV6test.com se encuentra que el servidor DNS público no es capaz de resolver direcciones IPV6 ya que co.sonda.com como servidor DNS no cuenta con el módulo AAAA que permite la validación DNS para direcciones IPV6, pero por lo contrario en las demás pruebas se encuentra total funcionalidad a nivel de verificación de puertos, tiempos de respuesta y configuración de servicios.

IPv6 entre sus ventajas vistas en la implementación en la Cloud permite manejar múltiples direcciones por interfaz de dispositivo haciendo la ruta simple y eficiente contrario a IPV4 en donde las direcciones tienen muy poca o ninguna conexión con los caminos de enrutamiento, por lo que los enrutadores deben mantener las tablas de enrutamiento para cada uno de los destinos mientras que en IPV6 los enrutadores mantienen pequeñas tablas de prefijos que permiten que la fuente envíe los paquetes al destino correcto.

El protocolo de Internet versión 6 permite coexistir con su antecesor IPV4 en la misma red, como se evidenció en la implementación realizada, las implementaciones de este nuevo protocolo empiezan a estar disponibles, y gracias a su compatibilidad permiten a los administradores de redes revisar la configuración, parametrización, costos, alcance, ventajas, desventajas de esta implementación que para algunas personas o compañías es un tema nuevo o que por el momento no se tiene en cuenta, grandes proveedores de comunicaciones o entidades como LACNIC el cual es el encargado del registro de direcciones para Latino América y el Caribe prestan de manera gratuita certificaciones, cursos online, guías y avances de implementación de algunas empresas para tomar de punto de referencia e incursionar de manera fácil en el mundo de IPV6, también se encuentra Hurricane Electric el cual es un backbone global de internet (ISP) especializado en IPV6 que constantemente está en la incentivación del conocimiento de IPV6 a nivel mundial mediante aplicaciones móviles informativas del agotamiento IPV4, cursos a nivel académico, profesional y experto gratuitos

certificables online, con la intención de educar a los usuarios interesados, e incentivar a la migración de servicios IPV4 a IPV6.

Verificando los antecedentes de migración de IPV6 en diferentes empresas colombianas se encuentra en muchas de ellas un avance significativo con respecto a Sonda S.A. por lo tanto al ser una empresa líder en tecnologías y prestadora de servicios IT, se debe estar al tanto de las nuevas tecnologías e infraestructuras y siempre dispuesta al cambio; como lo puede ser en este caso la migración de la red Cloud a direccionamiento IPV6 el cual permitiría a la empresa la oportunidad de presentarse en licitaciones del sector gobierno por medio del portal Colombia compra eficiente.

CONCLUSIONES.

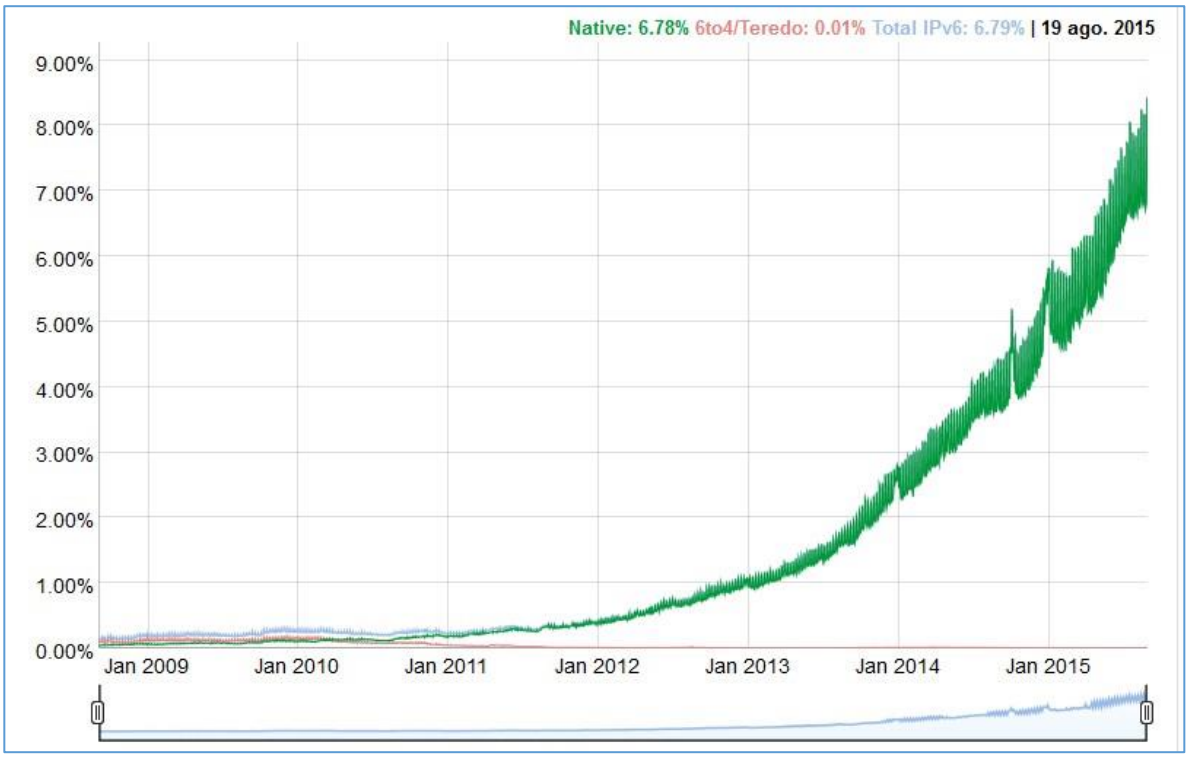
IPv6 como protocolo de internet ofrece una cantidad de características y ventajas por las cuales es razonable pensar en un proceso de migración en un futuro cercano, luego de realizar este proyecto como punto de partida se puede evidenciar que de manera sencilla se puede obtener comunicación con equipos IPv6 con casi cualquier tipo de infraestructura existente, como se pudo evidenciar al momento de realizar la configuración de IPv6 en el Datacenter de Level 3 y en la sede remota de Sonda en donde las infraestructuras son totalmente diferentes en cuanto arquitectura, equipos, marcas, proveedores; pero obteniendo resultados similares al ver que el direccionamiento IPv6 tanto para una red interna, como para realizar publicación de servicios funciono de manera óptima y con los resultados esperados.

Luego de verificar diferentes métodos de migración IPv4 – IPv6 en base a los requerimientos del proyecto en el cual hay que buscar la estrategia de migración más adecuada para que tanto la publicación por IPv4 como por IPv6 funcionen simultáneamente se optó por la utilización de dual stack como estrategia de migración en conjunto con tunelbroker.com como servidor de túnel IPv6 para fines del proyecto de grado, con él cual se define el direccionamiento para cada uno de las redes involucradas como para el Datacenter como para la sede remota de Sonda .S.A, con la que se realizó la configuración de los equipos involucrados en el proceso de migración ; pero que para fines de Sonda S.A. las condiciones más optimas serian la compra de un pool de direcciones IPv6 /64 propio con alguno de los proveedores que actualmente ofrecen este servicio para Colombia como Level3 o LACNIC ya que de esta manera se puede obtener un soporte más cercano y fiable para la configuración IPv6 para la empresa.

Este tipo de configuraciones a nivel empresarial abren una serie de ventanas para mejorar la imagen ante la competencia y futuros clientes ya que evidencia que la empresa siempre está buscando mejorar su portafolio de servicios, con la utilización de nuevas tecnologías.

IPv6 como tecnología a nivel mundial ha tenido más acogida e implementación en algunos países que en otros, pero a medida que se ha venido realizando procesos de migración, poco a poco se ha aumentado el número de empresas que están realizando procesos o planes de migración de protocolo de enrutamiento, como se evidencia en la Figura 58 en donde con comparación al año 2009 se ha aumentado en un 9% el acceso a internet desde redes que bajo alguna estrategia de migración se comunican desde una red IPv6.

Figura 58. Crecimiento IPv6 nivel mundial 2015



Fuente: http://www.google.com/intl/es/ipv6/statistics.html

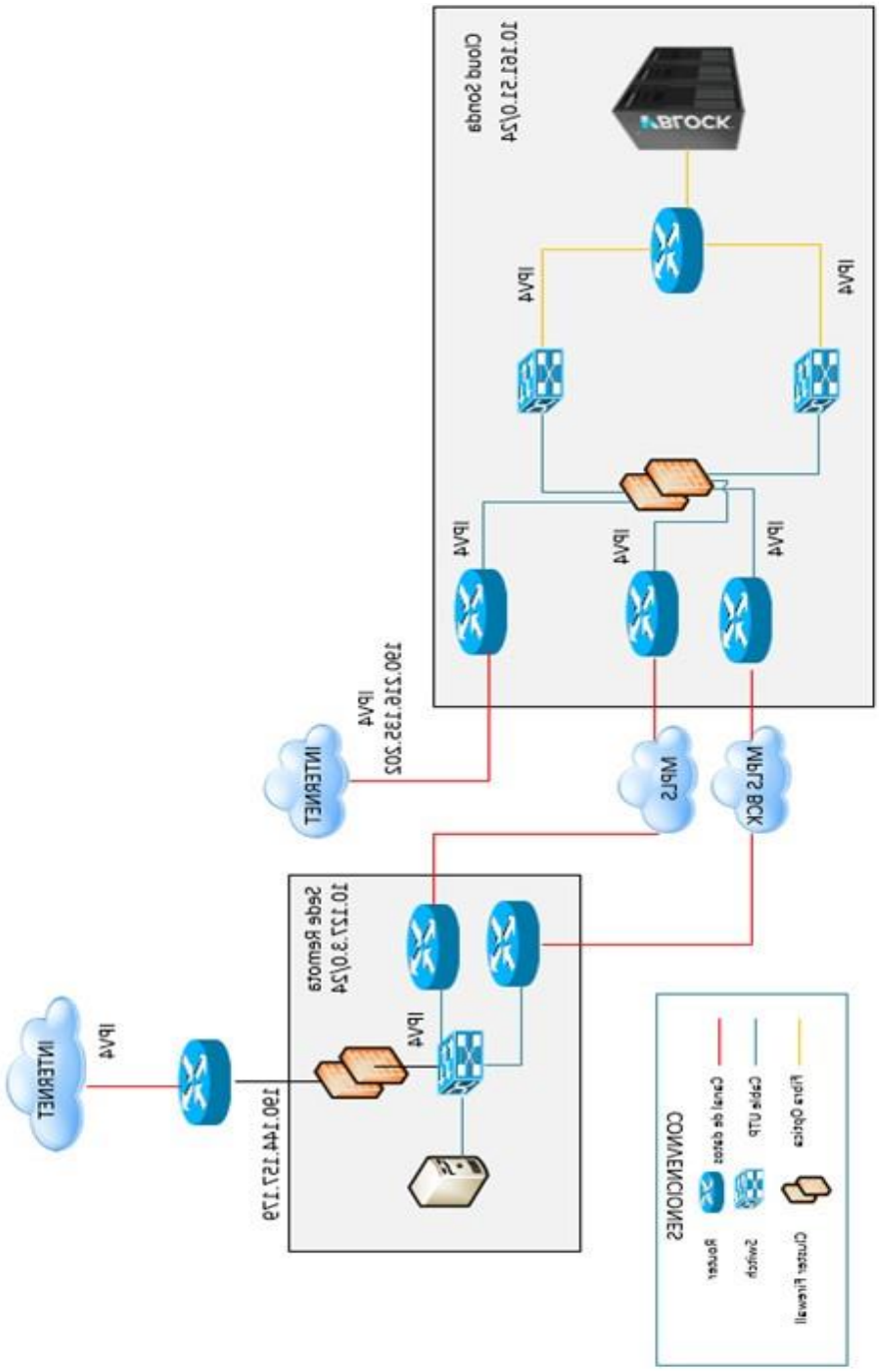
En Colombia son contadas las empresas que están en proceso o ya tienen implementada la red con direccionamiento IPv6 por lo cual es una oportunidad personal de conocer y capacitarse en nuevas tecnologías que en futuro cercano solicita gran demanda de implementación, soporte, capacitación a medida que los procesos de migración sigan avanzando

BIBLIOGRAFÍA.

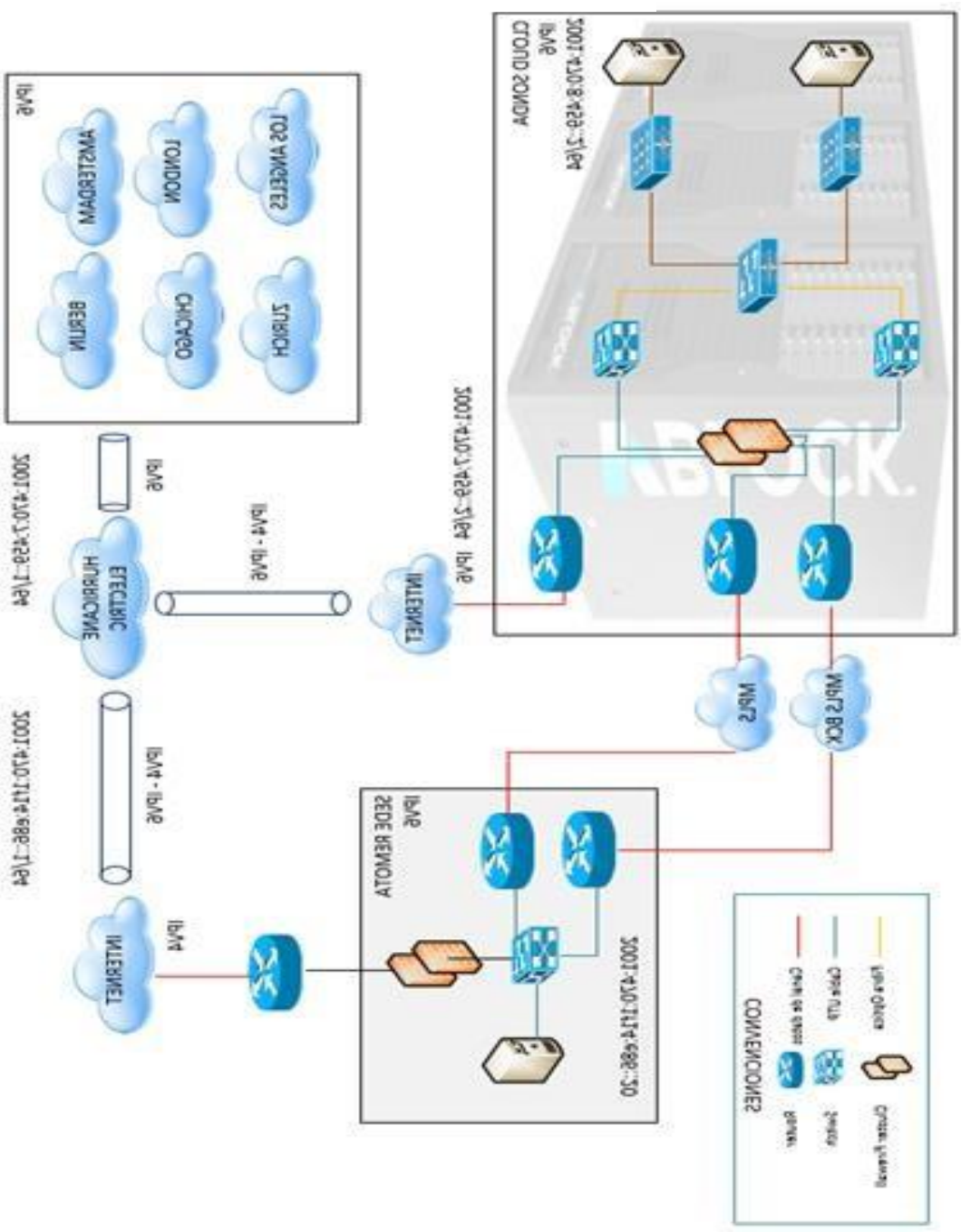
- ✓ Proyecto migración del protocolo IPv4 a IPv6, [Citado Mayo de 2015 – En línea], Disponible en http://www.auben.net/index.php/ipv6-tecnicas-de-migracion.
- ✓ IPv6 / Técnicas de Migración, [Citado Julio de 2015 – En línea], Disponible en http://www.izt.uam.mx/newpage/contterior/n79ne/ipv6.pdf.
- ✓ Propuesta de migración universidad Simón Bolívar, [Citado Julio de 2015], Disponible en http://www.mintic.gov.co/gestionti/615/transicion_IPV4.pdf.
- ✓ Guía de transición de IPv4 a IPv6 para Colombia, [Citado Marzo de 2015], Disponible en http://159.90.80.55/tesis/000130687.pdf.
- ✓ [RFC-4786] J. Abley., K. Lindqvist. "Operation of Anycast Services", RFC 4786, Diciembre 2006.
- ✓ [RFC-791] Jon Postel., "INTERNET PROTOCOL", RFC 791, Septiembre 1981.
- ✓ [RFC-4601] J. B. Fenner., M. Handley.H. Holbrook " Protocol Independent Multicast - Sparse Mode (PIM-SM):", RFC 4786, Agosto 2006.
- ✓ [RFC-4786] J. Abley., K. Lindqvist. "Operation of Anycast Services", RFC 4786, Diciembre 2006.
- ✓ [RFC-4786] S. Deering., R. Hinden. "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, Diciembre 1998.
- ✓ [RFC-2473] A. Conta., S. Deering. "Generic Packet Tunneling in IPv6 Specification", RFC 2473, Diciembre 1998.
- ✓ [RFC-6180] J. Arkko., F. Baker. " Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment", RFC 6180, Mayo 2011.
- ✓ Informe LACNIC. (2014). "Distribuciones/Asignaciones IPv4, espacio disponible y pronósticos". [Citado Julio de 20145 - En línea]. Disponible: http://www.lacnic.net/sp/registro/espacio-disponible-ipv4.html.
- ✓ Upstream Providers [En línea] .www.diyisp.orstream *[Citado Agosto de 2015]*
- ✓ RFC3513 Internet Protocol Version 6 (IPv6) Addressing Architecture. [Citado Julio 2015 - En línea]. Disponible: http://www.ietf.org/rfc/rfc3513.txt.

- ✓ [RFC-791] Jon Postel., "INTERNET PROTOCOL", RFC 791, Septiembre 1981.
- ✓ IPv6 Portal. ¿Quiénes implementan? [en línea]. http://portalipv6.lacnic.net/quienes-implementan/ [Citado enero de 2015].
- ✓ Information Society Breve historia de internet - Septiembre 2012 [citado Septiembre 2015]. Disponible en http://www.internetsociety.org/es/breve-historia-de-internet
- ✓ [RFC-1918] Y. Rekhter. B. Moskowitz. D. Karrenberg " Address Allocation for Private Internets", RFC 1918, Febrero 1996.
- ✓ [RFC-3022] P. Srisuresh. K. Egevang."Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, Enero 2001.
- ✓ [RFC-2460] S. Deering. R. Hinden."Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, Diciembre 1998.
- ✓ [RFC-4193] R. Hinden. B. Haberman."Unique Local IPv6 Unicast Addresses", RFC 4193, Octubre 2005.
- ✓ IPv6 Servicio de Información y Soporte. [Citado Julio de 2015 - En línea]. Disponible: http://www.6sos.org.
- ✓ Características principales de IPv6, [Citado Julio de 2015 – En línea], Disponible en http://docs.sun.com/app/docs/doc/820-2981/ipv6-overview-8?l=es&a=view.
- ✓ Como se representan las direcciones URL en IPv6, [Citado Julio de 2015- En línea], Disponible en http://eduangi.com/tag/ipv6/.
- ✓ ICMP v6, [Citado Julio de 2015 – En línea], Disponible en http://worldlingo.com/ma/enwiki/es/ICMPv6/1.
- ✓ Protocolo MIP – [En línea] http://wikitel.info/wiki/MIP [Citado Agosto -2015]
- ✓ PMIP [En línea] - www.cisco.com/c/en/us/.../pmip_20.pdf *citado [Agosto - 2015]*

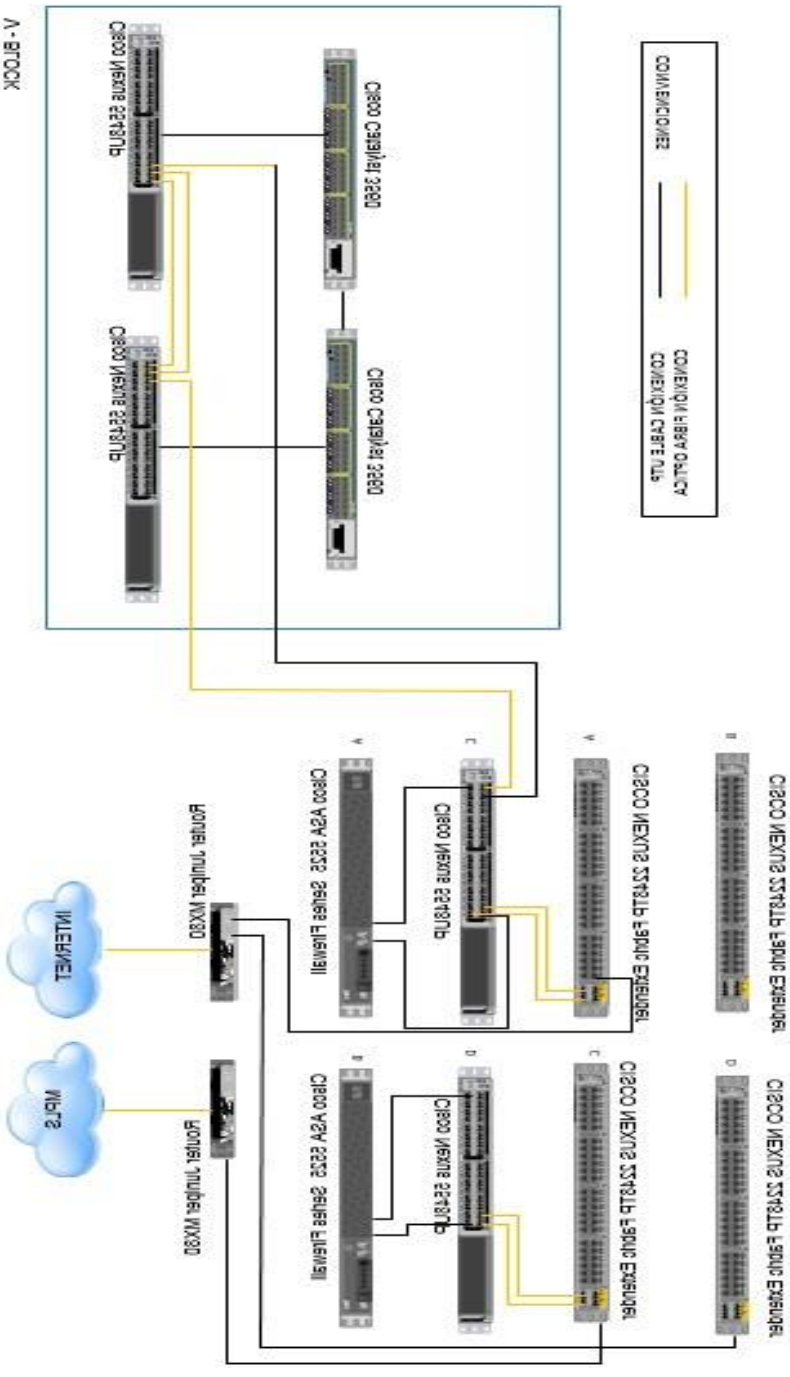
ANEXO A


Cloud Sonda
10.191.151.0\24
IPv4
IPv4
IPv4
IPv4
IPv4
190.216.135.202
INTERNET
MPLS
MPLS BCK
Sede Remota
10.127.3.0\24
IPv4
IPv4
INTERNET
190.144.157.179
CONVENCIONES
Router
Switch
Cluster Firewall
Canal de datos
Cable UTP
Fibra Optica

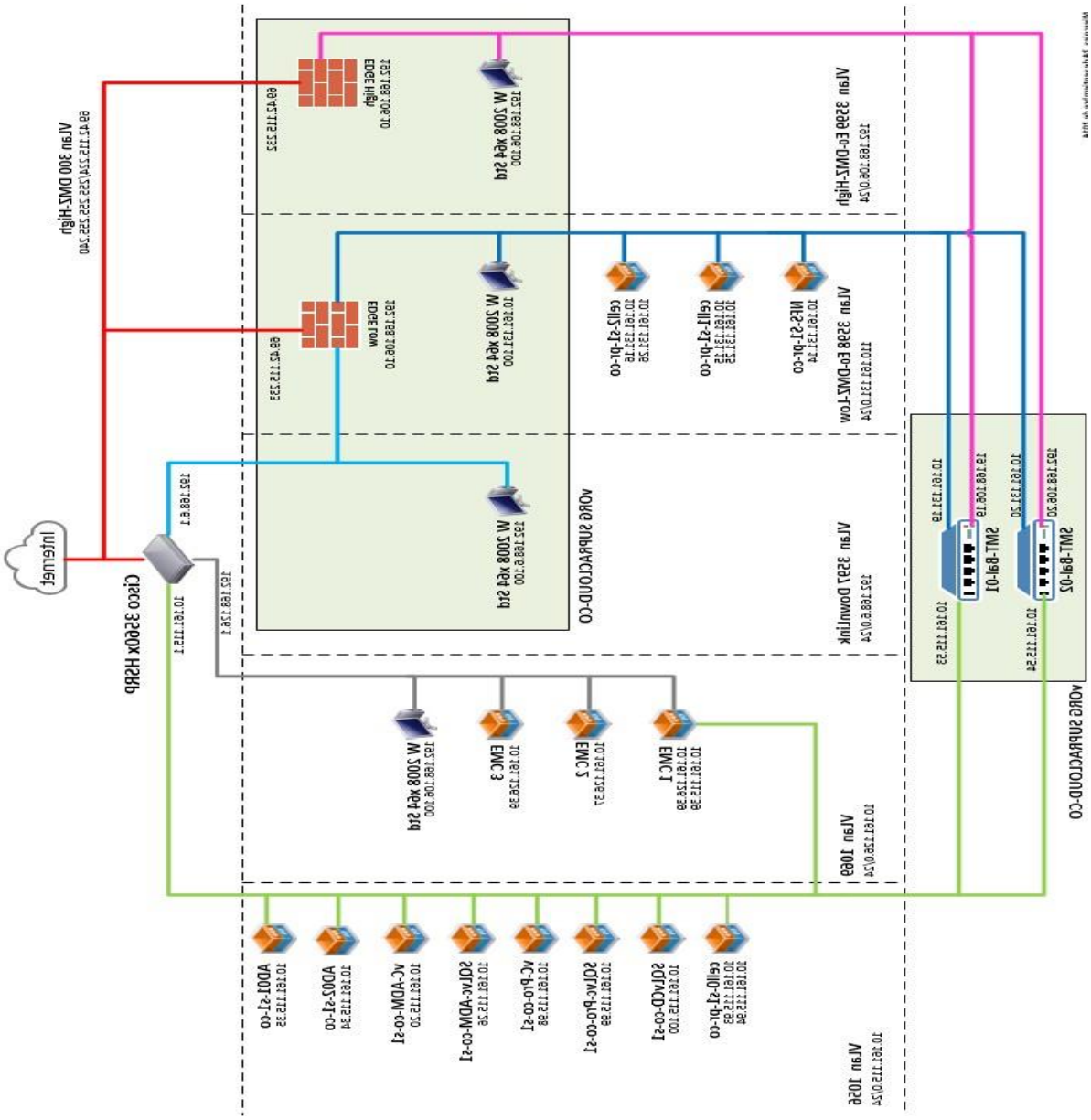
ANEXO B



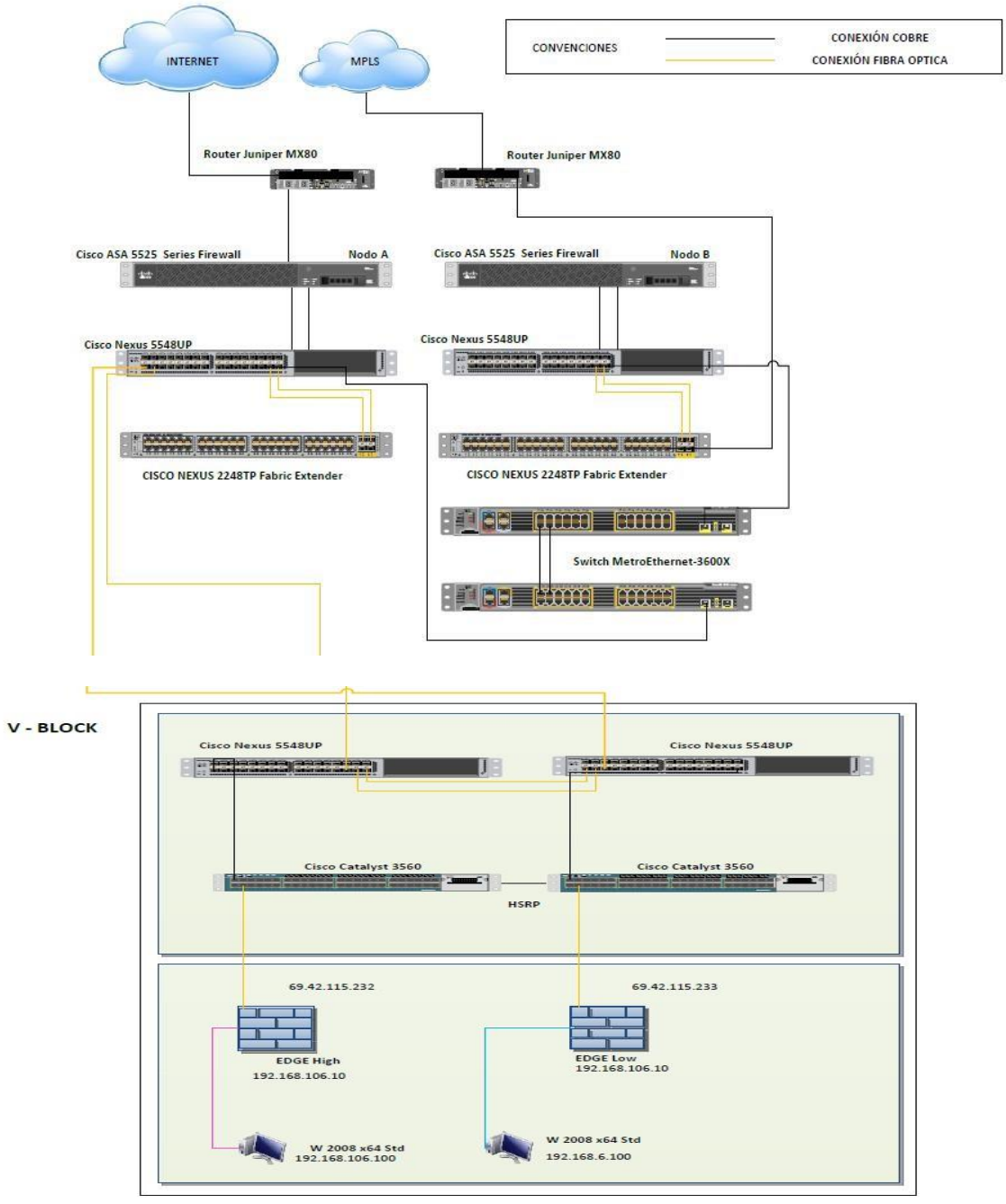
ANEXO C


INTERNET
MPLS
Router Juniper MX80
Router Juniper MX80
Cisco ASA 5525 Series Firewall
Cisco ASA 5525 Series Firewall
Cisco Nexus 5548UP
Cisco Nexus 5548UP
CISCO NEXUS 2248TP Fabric Extender
CISCO NEXUS 2248TP Fabric Extender
CISCO NEXUS 2248TP Fabric Extender
CISCO NEXUS 2248TP Fabric Extender
Cisco Catalyst 3560
Cisco Catalyst 3560
Cisco Nexus 5548UP
Cisco Nexus 5548UP
V - BLOCK
CONEXIÓN FIBRA OPTICA
CONEXIÓN UTP

ANEXO D


Internet
Cisco 3560X HSRP
Vlan 300 DMZ-High
Vlan 3239 Eo-DMZ-High
Vlan 3238 Eo-DMZ-Low
Vlan 3237 Downlink
Vlan 1069
Vlan 1050
VORA SUPRACLOUD-CO
SMT-B9I-01
SMT-B9I-02
EDGE High
EDGE Low
W 2008 x64 Std
EMC 1
EMC 2
EMC 3
MC-S1-pr-co
cell1-s1-pr-co
cell2-s1-pr-co
cell0-s1-pr-co
SQLWCD-co-s1
SQLw-pro-co-s1
MC-pro-co-s1
SQLw-ADM-co-s1
MC-ADM-co-s1
ADO2-s1-co
ADO1-s1-co

ANEXO E


INTERNET
MPLS
CONVENCIONES
CONEXIÓN COBRE
CONEXIÓN FIBRA OPTICA
Router Juniper MX80
Router Juniper MX80
Cisco ASA 5525 Series Firewall
Nodo A
Cisco ASA 5525 Series Firewall
Nodo B
Cisco Nexus 5548UP
Cisco Nexus 5548UP
CISCO NEXUS 2248TP Fabric Extender
CISCO NEXUS 2248TP Fabric Extender
Switch MetroEthernet-3600X
V - BLOCK
Cisco Nexus 5548UP
Cisco Nexus 5548UP
Cisco Catalyst 3560
Cisco Catalyst 3560
HSRP
69.42.115.232
69.42.115.233
EDGE High
192.168.106.10
EDGE Low
192.168.106.10
W 2008 x64 Std
192.168.106.100
W 2008 x64 Std
192.168.6.100

ANEXO F

Escuela Tecnologica Instituto Tecnico Central	CRONOGRAMA DEL PROYECTO
NOMBRE DEL PROYECTO	**IMPLEMENTACIÓN DE TECNOLOGÍA IPV6 PARA LA INFRAESTRUCTURA CONVERGENTE DE LA CLOUD EMPRESARIAL SONDA DE COLOMBIA S.A.**
DURACIÓN DE LA EJECUCIÓN DEL PROYECTO EN MESES	**12 Meses Inicio Agosto 2014**

N°	ACTIVIDAD	MES											
		1	2	3	4	5	6	7	8	9	10	11	12
1	Definición de proyecto de grado												
2	Contextualización con la empresa del proyecto de grado												
3	Definición de alcance y objetivos												
4	Contextualización del proyecto con el asesor												
5	Verificación de equipos involucrados												
6	Verificación de servicios afectados												
7	Documentación de servicios asociados a publicar												
8	Revisión de implementaciones similares de migración de IPV6												
9	Revisión de software involucrado en la implementación.												
10	Solicitud de permisos para ingreso a datacenter Level 3.												
11	Revisión documentación laboratorios redes IPV6.												
12	Revisión de enrutamiento IPV4 en Datacenter.												
13	Revisión de configuración de equipos involucrados en la migración.												
14	Diagramación de direccionamiento red Cloud con IPV6												
15	Revisión de beneficios empresariales de la configuración de IPV6.												
16	Revisión de precios de arrendamiento de pool IPV6 con level3 y LACNIC												
17	Verificación de alternativas de direccionamiento IPV6												
18	Realización de implementación de infraestructura de pruebas con HE.												
19	Solicitud de pool IPV6 público con HE.												
20	Solicitud 2 pool de direcciones IPV6 para pool remoto												
21	Habilitación de permisos a nivel de firewall para permitir tráfico ICMP												
22	Asignación de direcciones públicas a equipos finales para permitir ICMP.												
23	Verificación de documentación en HE para realización de tunnel sede remota												
24	Implementación peer IPV6 sede remota												
25	Verificación conectividad IPV6 sede remota												
26	Verificación de configuración de IPV6 para Linux 2,6												
27	Configuración de peer datacenter equipo Linux												
28	Verificación peer to peer HE												
29	Configuración de accesos y permisos internos de publicación a nivel ASA												
30	Configuración de interfaz tunel Linux												
31	Creación de rutas de salida IPV6												
32	Configuración forwarding e IPTABLES de server Linux												
33	Verificación de conectividad IPV6 Cloud												
34	Verificación conectividad IPV6 Cloud - Sede remota												
35	Publicación de servidores requeridos en el alcance												
36	Verificación de servicios implementados												
37	Verificación de pruebas IPV6.NET												
38	Verificación de pruebas y comparación con análisis IPV4												
39	Conclusiones												