PROPUESTA DE SOLUCIÓN DE RED CON ALTA DISPONIBILIDAD PARA LA TRANSICIÓN DE IPV4 A IPV6 EN UNA ENTIDAD DEL ESTADO.

BERNAL SANTOS RODRIGO

CARVAJAL QUINTERO WILLIAM GERMAN

RICO BELLO JERONIMO

Trabajo de Grado

Director
CARLOS RENÉ SUAREZ SUAREZ

UNIVERSIDAD EL BOSQUE
FACULTAD DE INGENIERÍA ELECTRÓNICA
ESPECIALIZACIÓN EN DISEÑO DE REDES TELEMATICAS
BOGOTÁ, COLOMBIA
2020

TABLA DE CONTENIDO

Pág.

1. RESUMEN 11

2. INTRODUCCIÓN 12

3. DESCRIPCIÓN GENERAL DEL PROYECTO 14

3.1 DEFINICIÓN DEL PROBLEMA 14
3.2 ASPECTOS A SOLUCIONAR 16
3.3 SOLUCIÓN PROPUESTA 16

4. ESTADO DEL ARTE 17
4.1 EL PROTOCOLO IPV6 17
4.2 IMPLEMENTACIÓN DE IPV6 EN COLOMBIA 19
4.3 MÉTODOS DE TRANSICIÓN A IPV6 21
4.3.1 Doble Pila(Dual Stack) 21
4.3.2 Tunelización 22
4.3.3 Teredo 22
4.3.4 Nat64 23

5. HERRAMIENTAS DE SIMULACIÓN DE REDES 24
5.1 SIMULADOR PACKET TRACERT 24
5.2 SIMULADOR GNS3 25
5.3 SIMULADOR OPNET 26
5.4 SIMULADOR EVE-NG 28

6. JUSTIFICACIÓN 30

7. OBJETIVOS 31

7.1. GENERAL 31
7.2. ESPECÍFICOS 31

8. REQUERIMIENTOS 32

9. METODOLOGÍA 33

10. DESARROLLO 35

10.1 PLAN PARA LA TRANSICIÓN A IPV6 EN LA ENTIDAD 35
10.1.1 Análisis de la topología actual de la red 38

10.1.1.1 Inventario de TI para la red actual 38
10.1.1.2 Servicios 40
10.1.1.3 Análisis de capacidad de soporte de Ipv6 del ISP y Terceros 41
10.2 DISEÑO Y MEJORAS EN LA RED PARA MIGRAR A IPV6 43
10.2.1 Adquisición y Segmentación de pool IPv6 propuesto para las sedes 44
10.2.2 Aplicación de métodos de transición a IPv6 en la entidad 48
10.2.3 Redundancia en sedes capitales para mejorar la disponibilidad 51
10.2.4 Servidor DHCP centralizado con gestión. 52
10.2.5 Gestión y Monitoreo de la red. 53
10.3 SIMULACIÓN COMO HERRAMIENTA EN EL DISEÑO 54
10.3.1 Simulación de conectividad Ipv4 61
10.3.2 Simulación de conectividad Ipv6 64
10.3.3 Simulación de conectividad Ipv6 por medio de Túnel sobre IPv4 66
10.3.4 Comparación de desempeño delos tres escenarios simulados 69

11. RESULTADOS 71

12. DISCUSIÓN 72

13. CONCLUSIONES 73

14. REFERENCIAS 74

ANEXOS

LISTA DE FIGURAS

Pág.

Figura 1. Encabezado Ipv6 18
Figura 2. Implementación de Ipv6 en Colombia a hoy 20
Figura 3. Topología Dual-Stack 21
Figura 4. Túnel Ipv4 to Ipv6 22
Figura 5. Técnica Teredo 22
Figura 6. Método NAT64 23
Figura 7. Simulador Packet Tracert 25
Figura 8. Simulador GNS3 26
Figura 9. Simulador Opnet 27
Figura 10. Simulador EVE-NG 28
Figura 11. Plan propuesto para la transición de IPv4 a IPv6 de la Entidad 36
Figura 12. Ejemplo de Modelo de Infraestructura actual en la entidad 38
Figura 13. Distribución de proveedores de servicios en la entidad 42
Figura 14. Cantidad de equipos por sede 44
Figura 15. Segmentación Ipv6 por categoría 45
Figura 16. Segmentación Ipv6 para sedes Inspecciones 45
Figura 17. Segmentación Ipv6 para vlan en las sedes de Inspecciones 46
Figura 18. Segmentación Ipv6 para sedes Territoriales 46
Figura 19. Segmentación Ipv6 para sedes Capitales 47
Figura 20. Segmentación Ipv6 para los equipos de DataCenter 47
Figura 21. Segmentación Ipv6 Wan en las sedes 47
Figura 22. Topología para implementación de Dual-Stack en la entidad 49
Figura 23. Topología para implementación de Túnel 6to4 en la entidad 50
Figura 24. Topología propuesta para mejorar disponibilidad 51
Figura 25. Servidor DHCP configurado actualmente sobre el router 52
Figura 26. Elementos seleccionados en las topologías de simulación 54
Figura 27. Presentación de aplicaciones 55
Figura 28. Perfiles estándar para todos los escenarios 55
Figura 29. Perfil generado Lan y Wlan 56
Figura 30. Perfil multimedia 56
Figura 31. Configuración de perfil para maquina multimedia 57
Figura 32. Configuración Bss Id y velocidad sobre ap y cliente 58
Figura 33. Configuración de perfil para servidor web “fuente” 58
Figura 34. Topología simulada de una sede tipo inspección 59
Figura 35. Topología simulada de una sede tipo territorial 59
Figura 36. Topología simulada de una sede tipo central 60
Figura 37. Configuración de direccionamiento ipv4 en máquinas terminales 61
Figura 38. Configuración de direccionamiento ipv4 router sede 61
Figura 39. Muestra de configuración en mpls 62
Figura 40. Configuración de direccionamiento ipv4 router datacenter 62

LISTA DE FIGURAS (Continuación)

Pág..

Figura 41. Resultado de consumo Ipv4 para Territoriales,Inspecciones 63
Figura 42. Configuración de direccionamiento ipv6 en terminales 64
Figura 43. Configuración de direccionamiento ipv6 en enrutadores 64
Figura 44. Consumo ipv6 en las sedes Inspecciones,Territoriales y central 65
Figura 45. Configuración Ipv4 Wan 66
Figura 46. Configuración de extremos Ipv4 del Túnel 67
Figura 47. Configuración de Interfaces en los enrutadores en Ipv6 67
Figura 48. Gráfico de consumo túnel 6 to 4 en Inspecciones y Territoriales 68
Figura 49. Trafico Inspección “Ipv4 vs Ipv6 vs tunnel 6 to 4” 69
Figura 50. Trafico territorial “Ipv4 vs Ipv6 vs tunnel 6 to 4” 69
Figura 51. Trafico central “Ipv4 vs Ipv6 vs túnnel 6 to 4” 70

LISTA DE TABLAS

Pág.

Tabla 1. Progreso en la implementación de Ipv6 en Colombia 20
Tabla 2. Comparación de características de los simuladores 29
Tabla 3. Inventario de recursos tecnológicos en la red actual 39
Tabla 4. Relación de soporte de Ipv6 nativo por los operadores de UM 43

LISTA DE ANEXOS

ANEXO A. LISTADO DE SEDES EN EL TERRITORIO NACIONAL

ANEXO B. RELACION DE DIRECCIONAMIENTO IPV6 ASIGNADO

ANEXO C. CARTA PRESENTACION ESTUDIANTES PGC-F1

ANEXO D. CARTA ACEPTACION PROYECTO DE GRADO - PGC-F2

ANEXO E. CARTA APROBACION DEL TRABAJO DE GRADO - PGC-F3

ANEXO F. CARTA SOBRE DERECHOS DE AUTOR PGC-F5

GLOSARIO

CIDR: (Classless Inter-Domain Routing)estrategia para la asignación de direcciones IPv4 de 32 bits con miras a conservar el espacio y limitar la tasa de crecimiento [9].

DUAL STACK: (Pila doble) permite la implementación completa de ambas versiones del Protocolo de Internet. Mediante la tunelización proporciona un medio para transportar paquetes IPv6 sobre infraestructuras de enrutamiento IPv4.

FAST ETHERNET: familia de especificaciones de capa física para lograr una operación de 100 Mb/s [17].

FCAPS: Método de gestión ampliamente utilizado en redes de comunicaciones grandes, que detecta fallas y cambios en la topología mientras realiza también configuraciones.

IOT: (internet of things) infraestructura global para la sociedad, permitiendo servicios avanzados mediante la interconexión de cosas (físicas y virtuales) basadas en tecnologías de información y comunicación interoperables existentes y en evolución [18].

IP: (Internet Protocol) el Protocolo de Internet está diseñado para identificar un dispositivo en sistemas interconectados en redes de comunicación informática con conmutación de paquetes. se utiliza para transmitir bloques de datos llamados datagramas desde las fuentes a destinos, donde las fuentes y los destinos son hosts identificados por direcciones de longitud fija [4].

IPV4: (Internet Protocol version 4) protocolo de direccionamiento IP (IPv4) con una longitud fija de cuatro octetos (32 bits). Una dirección comienza con un número de red, seguido de la dirección local [4].

IPV6: (Internet Protocol version 6) el protocolo IP versión 6 (IPv6) es la nueva versión del Protocolo Internet, diseñado como el sucesor para el IP versión 4 (IPv4) [RFC-791]. Los cambios del IPv4 al IPv6 trae bastantes mejoras [5].

NAT: (Network Address Translation) la operación básica consiste en permitir que las direcciones IP dentro de un dominio puedan ser reutilizadas por cualquier otro dominio. Por ejemplo, una dirección de Clase A podría ser utilizada por muchos dominios.[7]

ROUTER: las funciones de un enrutador son leer la dirección de destino marcada

en un paquete IP entrante, consultar su información interna para identificar un enlace saliente al que se reenviará el paquete [19].

SWITCH: el switch es un dispositivo que divide la red en segmentos más pequeños, por lo que el tráfico de broadcast puede reducirse y más hosts pueden comunicarse en al mismo tiempo [33].

WAN: las tecnologías WAN se utilizan principalmente para conectar redes que están geográficamente apartadas. Por ejemplo, una sucursal remota ubicada en la ciudad A que se conecta a la oficina central en la ciudad B [33].

1.RESUMEN

Este proyecto tiene como finalidad dar una propuesta de solución para la transición del protocolo IPv4 a IPv6 en una entidad del gobierno, ya que la versión 6 del nuevo protocolo permite la conexión de un gran número de máquinas a la red posibilita el crecimiento sin restricciones, además trae consigo otros grandes beneficios como: calidad de servicio, evitar mayores costos si se desea adquirir un nuevo pool de direccionamiento IPv4 y seguridad; por otro lado le permite cumplir con el requerimiento de transición a Ipv6 exigido por el Ministerio de las Tecnologías de la información (Min Tic) en la circular 2710 del 3 de octubre del 2017.

En el proyecto se hace un análisis de la topología actual de la red en la entidad permitiendo realizar una recopilación y registro de los elementos y operadores que conforman su infraestructura, de esta manera poder utilizar las técnicas apropiadas y así poder proponer los pasos para la transición a IPv6 de manera que la entidad no se vea afectada con indisponibilidad en su red, además se sugirieren algunas mejoras que le permitieran una mayor eficiencia y alta disponibilidad en sus recursos. Por último con un sistema computacional se simula una topología de red que representa las sedes de la entidad antes y después de la transición para confirmar su correcto funcionamiento y poder presentar los resultados con el fin de que la entidad los tenga en cuenta para su posible implementación.

Palabras Clave: Transición,Ipv6,Migración,Plan,Diseño,Direccionamiento.

1.ABSTRACT

This project was made as a proposal for the solution of the transition from protocol ipv4 to ipv6 in an entity of the government. It is well known that the version 6 of the new protocol permits making many connections to a big number of machines in the network, and gives a scalability without restrictions. This also comes with huge benefits such as QoS, avoiding costs if it was wished to acquire a new pool of public addresses, security, among others. On the other hand, it pretended to accomplish the requirements of the MinTic .

In the project it was made an analysis of the entity network current topology permitting to do a collection and a record of the elements and service providers that are part of the infrastructure, that way it is possible to perform the transition to ipv6 without affecting the entity's network availability. Furthermore some improvements were suggested in order to get a major efficiency and a high availability of its resources. To confirm the correct performance, the entity's network was simulated before and after the migration through a computational system and therefore making it possible to show the results to take into account for the possible implementation. to be able to present the results to take into account for its possible implementation.

Keywords: Transition,ipV6,Migration,Plan,Design, Addressing.

2. INTRODUCCION

El protocolo IPv4 está basado en direcciones compuestas por 32 bits, esto implica que existan 2^32 (4.294.967.296) de direcciones disponibles, lo que en sus inicios parecía un gran número, con la creación de Internet y su rápida expansión estas direcciones se fueron agotando por las malas políticas en la asignación, como fue el caso de las grandes empresas y organizaciones a las que se les asignaron bloques de direcciones que no fueron devueltas, debido a esto se crearon métodos que extendieron la vida útil del protocolo como por ejemplo el NAT, afectando el rendimiento de los dispositivos de red.

Para eliminar las falencias presentadas por IPv4 la Internet Engineering Task Force diseñó el protocolo IPv6, que se compone por direcciones de 128 bits que incrementa el espacio de direcciones disponibles elevando considerablemente el número de dispositivos conectados a la red, permitiendo así que internet pueda crecer sin limitaciones, además este protocolo presenta grandes ventajas como lo son la calidad del servicio y la seguridad embebidos en él, por esta razón se viene hablando de la necesidad de adoptar el protocolo IPv6 a nivel mundial para satisfacer la actual y futura demanda de direccionamiento ip que requiere la gran cantidad de dispositivos, es evidente que es ahora cuando se hizo oficial el agotamiento del direccionamiento Ipv4 que las entidades deben hacer su mayor esfuerzo por migrar sus redes a Ipv6, garantizando la continuidad de los servicios que ofrecen mejorando la calidad con las nuevas tecnologías.

En este proyecto se realiza el diseño de un plan de la transición de una red Ipv4 a Ipv6 en una entidad del estado, asegurando que no se vea afectada la calidad y continuidad de sus servicios además de permitir la escalabilidad en la red. Para llegar a ello en el proyecto se analiza la información de la infraestructura de red actual entregada por el departamento de TI de la entidad, con esto se puede identificar la cantidad de sedes con su respectiva caracterización y se determina los métodos de transición que permitan la coexistencia de los protocolos Ipv4 e Ipv6 mientras se migra completamente la red a Ipv6, además se evalúa el comportamiento del diseño con un software computacional que confirme mediante los resultados de una simulación el correcto funcionamiento y posteriormente se presenten los resultados y conclusiones además de las recomendaciones a tener en cuenta si se decide su implementación para mejorar el desempeño de la red.

En el capítulo 3 se presenta una descripción detallada de la problemática que llevó al desarrollo de este proyecto, se estudian las razones por las que no se realizó antes la migración y los cambios positivos que obtendrá la entidad con la implementación.

En el capítulo 4 se realiza un estudio del protocolo IPv6 mostrando las ventajas de

su implementación ,también se analiza el avance de su implementación en Colombia y los métodos de transición que pueden ser utilizados en la migración hacia IPv6.

En el capítulo 5 se explican diferentes métodos computacionales que pueden ser utilizados en el análisis de redes mediante la ejecución de simulaciones, se hace también un comparativo entre ellos.

En el capítulo 6 se encuentra la justificación social y académica donde se muestra la relevancia de la realización del proyecto dando a conocer el impacto positivo que obtiene la entidad objeto de la migración y el beneficio en el ámbito profesional de los autores del proyecto.

En el capítulo 7 se presentan los objetivos generales y específicos que permiten definir el alcance del proyecto .

En el capítulo 8 se muestran los requerimientos del proyecto, se indican los requisitos mínimos necesarios que deben cumplirse al realizar el proyecto.

En el capítulo 9 se presenta la metodología scrum, utilizada para prevenir retrasos al cumplir con los objetivos propuestos en el proyecto, incentivando el trabajo en equipo.

En el capítulo 10 se encuentra el desarrollo del diseño para la migración a IPv6 ,aquí se levanta la información actual y se definen los métodos de transición más adecuados para cada sede de la entidad, además se realiza la simulación del diseño en el simulador de redes OPNET.

En el capítulo 11 se encuentran los resultados, donde se analizan los datos obtenidos en la simulación y se valida el funcionamiento del diseño realizado.

En el capítulo 12 se presentan las discusiones donde de una forma crítica se comparan los resultados obtenidos anteriormente con la teoría disponible sobre la conectividad en el protocolo IPv6.

En el capítulo 13 se presentan las conclusiones, aquí se expone el aprendizaje nuevo adquirido mediante la ejecución del proyecto de migración a IPv6 en esta entidad.

Luego, se encuentra la documentación de referencias, aquí se pueden consultar las fuentes de información literarias y electrónicas utilizadas durante la formulación de este proyecto.

Por último se presentan los Anexos, donde se encuentra la información de soporte generada durante el desarrollo del diseño, como la relación de direccionamiento IPv6 y el listado de las sedes.

3. DESCRIPCION GENERAL DEL PROYECTO

En respuesta a la necesidad de implementar Ipv6 en la entidad y de cumplir con la circular 2710 del 3 de octubre del 2017 [27] expedida por Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTIC), que establece como plazo máximo el 31 de Diciembre de 2020 para la implementación de Ipv6 en las entidades territoriales del país, se realiza para una entidad del estado el diseño de red para la migración de Ipv4 a Ipv6 mediante el levantamiento de información de la topología actual que permita caracterizar los perfiles de usuarios y la infraestructura con que se cuenta, con esto se definen los métodos de transición que se utilizan en las diferentes sedes para la migración como Dual Stack, Teredo o tunelización en algunos casos.

Se realiza una segmentación del direccionamiento Ipv6 /48, que es asignado por el Registro de direcciones de Internet para América Latina (LACNIC) con la finalidad de ofrecer conectividad global a todas sus sedes sin necesidad de hacer uso de procesos de traslaciones de Ip (NAT), como se hace actualmente con Ipv4 y consecuentemente con ello disminuir la carga de procesamiento de los equipos mientras se mejora la calidad de las comunicaciones, además del aumento en la seguridad que ya ofrece implícitamente el protocolo Ipv6, este diseño es analizado en un sistema computacional por medio de la simulación la cual permite la visualización del comportamiento futuro mediante la obtención de datos estadísticos, que son estudiados para confirmar la viabilidad o efectividad del diseño realizado, estos resultados son presentados a la entidad que será quien determine la implementación del diseño.

3.1 DEFINICION DEL PROBLEMA

La entidad responsable del registro de direcciones de Internet para América Latina y el Caribe (LACNIC) anunció el 10 de junio de 2014 que el último segmento de direcciones públicas IPV4 está entrando en fase de agotamiento gradual. Además la mala planificación en la asignación y el crecimiento exponencial de la red de internet hizo que el direccionamiento IPV4 se agotara antes de lo esperado; dado que se considera que el direccionamiento de red es un recurso importante para el crecimiento económico, científico y tecnológico para un país, se ha hecho necesario que las entidades encargadas tomen las medidas necesarias para encaminarse hacia la acogida del nuevo protocolo IPV6.

En Colombia la entidad encargada de reglamentar y regular el proceso de transición es el Ministerio de las Tecnologías de la información y las Comunicaciones MinTIC, con la intención de impulsar y promover la migración a IPV6 esta entidad emitió la

resolución 2710 de Octubre de 2017 [27] donde se informa que las entidades territoriales tienen como plazo máximo el 31 de Diciembre de 2020 para efectuar la transición del protocolo IPV4 al protocolo IPV6, actualmente la entidad del estado cuenta con 32 direcciones territoriales en Colombia, aproximadamente una por departamento, de estas se desprenden algunas inspecciones ubicadas en los municipios del país, además se suma el punto de Datacenter donde se alojan las aplicaciones, bases de Datos de la entidad.

La infraestructura actual de las sedes territoriales se compone de ROUTER marca BDCOM BSR2800-24E, este equipo cuenta con un SWITCH embebido fast-ethernet de 24 puertos para suplir las necesidades de conectividad en la sede, un equipo ruckus R300 que brinda conectividad inalámbrica en cada sede y no tienen respaldo en cuanto a UM, en el punto central y las sedes con mayor relevancia se dispone de enrutadores CISCO ISR 4451-X y routers CISCO ISR 4431 que tienen mayores capacidades y prestaciones los cuales por su naturaleza y características tiene una fiabilidad alta, la entidad no ha realizado actividades dirigidas a la implementación del protocolo por varias razones como:

- El rápido crecimiento de la entidad y la falta de continuidad en los proyectos de modernización , han hecho que se llegue rápidamente al escenario en el que no se tiene preparado un plan de contingencia para la implementación de nuevos protocolos de direccionamiento en dicha entidad.

- No contar con un diseño de red para IPV6 que le permita a la entidad mantener una alta disponibilidad al ofrecer sus servicios al público, además de no disponer de como monitorear y controlar el tráfico se resume en el continuo aplazamiento de su migración a IPV6 y la aplicación de nuevas herramientas en la red.

- La poca capacitación acerca del protocolo IPV6 para su despliegue en la red, así como la asignación de recursos económicos para su implementación contribuyen a retrasar el proceso de transición a este protocolo.

Al no tomar ningún plan de acción para mejorar la disponibilidad de la red, la entidad se estaría exponiendo a una alta posibilidad de fallo en su red y al no implementar el protocolo IPV6 se estarían sub utilizando los equipos que permiten este protocolo y seguirá retrasando la convergencia con las redes Ipv6 de otras entidades.

Por otra parte la entidad no estaría cumpliendo con la circular 2710 emitida por el MinTIC exponiéndose a sanciones, las cuales están consignadas en la ley 1341 del 30 de julio del 2009 artículo 65 [23], de entre las cuales pueden alcanzar los 2000 salarios mínimos legales mensuales, caducidad del contrato o cancelación de la licencia y la suspensión de operación al público hasta por dos meses ya que retrasaría el plan que tiene el estado de avanzar con la adopción de este protocolo.

3.2 ASPECTOS A SOLUCIONAR

Contar con un diseño de red junto con el plan de transición que permita migrar la red de la entidad al protocolo IPv6 no solo hará que cumpla con lo estipulado en la circular 2710 de 2017 emitida por el MinTIC si no que permite colocarla la entidad a la vanguardia tecnológica permitiéndole desarrollar aplicaciones más modernas.

Con la implementación de Ipv6 la entidad no enfrentará el problema de falta de direccionamiento para publicar sus servidores o para la asignación de ips a sus nuevos equipos cuando en el futuro crezca la red , la calidad del servicio tendrá una gran mejoría ya que el protocolo IPv6 utiliza los campos Etiqueta de flujo y Clase de servicio que pueden ser utilizados para la implementación de QoS mejorando el desempeño de las aplicaciones críticas como voz sobre IP y video, a diferencia del actual protocolo IPv4 en donde por defecto proporciona un envío de tráfico de mejor esfuerzo.

La seguridad también se verá reforzada con la implementación de IPv6 ya que este protocolo permite la encripción de la información así como la autenticación del remitente del paquete ,se verá una mejora en tiempo de consulta para las aplicaciones sensibles a la fragmentación de paquetes común en IPv4 como las de base de datos utilizadas por la entidad, ya que IPv6 permite el uso de jumboframes transportando cargas útiles grandes sin necesidad de fragmentar.

3.3 SOLUCION PROPUESTA

Generar un plan de transición y un diseño de segmentación de la red donde se incluyan conexiones redundantes en las sedes principales además del plan de direccionamiento que permita adoptar el protocolo IPV6 sin que se vean afectados los servicios actuales de IPV4 y buscando la convergencia entre todos los dispositivos involucrados en la red, esto partiendo de un diseño que permita la coexistencia de los protocolos sin problemas en las máquinas actuales, para ello simular una porción del diseño planteado que contenga las características más relevantes de conectividad en IPV6 en el punto central y algunas sedes principales como Bogotá, Cali, Barranquilla y Medellín.

4. ESTADO DEL ARTE

4.1 EL PROTOCOLO IPV6

Cuando se realiza una conexión entre dos dispositivos ya sea en una red local o a través de internet se utiliza el protocolo de direccionamiento ip (Internet protocol). Según la norma RFC 791 señala básicamente que el protocolo está diseñado para transmitir bloques de datos o paquetes de bits llamados datagramas desde una fuente hacia un destino. Esto quiere decir que cualquier información se encapsula en paquetes de datos que son transportadas en direcciones ip que no se pueden repetir.

El protocolo de internet fue creado para dar un identificador único a los hosts de una red, actualmente el protocolo de direccionamiento IPv4 es el más utilizado, este está diseñado para usar una dirección ip conformada por 32 bits, lo que indica que puede direccionar poco más de 4 mil millones de dispositivos en la red. Algunos de estos rangos de direccionamiento se han reservado para redes privadas y en consecuencia para su utilización no es necesario solicitarlo a alguna autoridad especializada, lo contrario ocurre con el direccionamiento público que es asignado y controlado por algunas entidades especializadas globalmente como la IANA (Agencia Internacional de Asignación de Números de Internet) [16] y en américa latina por LACNIC (Registro de Direcciones de Internet de América Latina y Caribe). LACNIC asigna bloques de direccionamiento público a los ISP y otras redes de cada país para que sean utilizados y distribuidos de forma ordenada a los usuarios finales [24].

Desde 1983 se ha venido empleando la versión IPv4 del protocolo, y debido que ha sido un recurso muy utilizado, limitado y con el crecimiento de la internet ya se está llegando al punto de agotamiento del direccionamiento público. Actualmente en América latina sólo a las entidades que nunca se les ha asignado un bloque de direccionamiento IPv4 lo pueden adquirir, pero como máximo de máscara /22, las demás entidades o proveedores de servicios no lo pueden hacer. Dentro de poco tiempo no se podrá asignar ipv4 ni siquiera a las entidades nuevas.

El protocolo IPv6 es una nueva versión de IP (Internet Protocol), diseñada para reemplazar la versión IPv4, actualmente en uso. Ipv6 es un protocolo que fue desarrollado en la década de los 90s en el IETF (Internet Engineering Task Force)[11], para dar mayor capacidad en la asignación de direccionamiento de red, debido a que incrementa el tamaño de las direcciones ip a 128 bit, a diferencia de Ipv4 que cuenta con una capacidad limitada de direcciones de 32 bits. Esto quiere decir que con la implementación de este protocolo se tiene una mayor capacidad para conectar una mayor cantidad de dispositivos a internet, así mismo el diseño del protocolo aumenta mayores beneficios en seguridad, calidad de servicio,

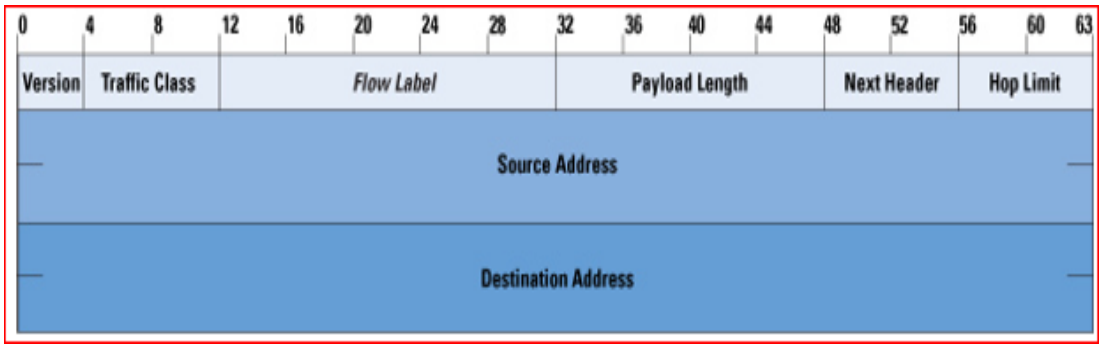
capacidad de transmisión y facilita la administración de la red, entre otras cosas[31].

Según lo indicado por el protocolo cada elemento de la red debe poseer un direccionamiento ip único que lo identifique en internet, garantizando de esta forma que haya conexión entre dos dispositivos únicos sin posibilidad que se repita su direccionamiento ip. Los beneficios y cambios que trae el protocolo IPv6 con respecto del IPv4 están señalados en la norma rfc 2460, como son Capacidades de Direccionamiento Extendida, Simplificación del Formato de Cabecera, Soporte Mejorado para las Extensiones y Opciones, Capacidad de Etiquetado de Flujo y Capacidades de Autenticación y Privacidad.

IPv6 modificó el formato de la cabecera para mejorar las limitaciones que tenía IPv4, aumentando su tamaño en 40 bytes esto representa el doble con respecto a la anterior que tan solo es de 20 bytes [14]. Además, la cabecera es de longitud fija y los campos están alineados en campos de 64 bits lo que permite que sea más fácil el procesamiento para los equipos de red. También se han incluido campos para implementar calidad de servicio dependiendo el tipo de tráfico.

Otras funciones de IPv6 no están disponibles en la cabecera estándar, pero se pueden insertar en las cabeceras de extensión que están ubicadas en la cabecera IPv6 y las cabeceras de nivel superior utilizando el campo de siguiente cabecera (Next Header), estas son solamente procesadas por los nodos de destino de esta manera optimizando el procesamiento de los equipos intermedios.

Figura 1. Encabezado Ipv6



Fuente: http://www.ijser.org

Mucha veces en IPv4 es necesario la configuración de DHCP (Dynamic Host Configuration Protocol) para destinar una ip, un Gateway y los DNS (Domain Name system) a un usuario o un host en la red para poder tener salida hacia internet, en IPv6 esta configuración está incluida dentro del mismo protocolo, de esta manera los routers asignan una dirección pública y un gateway predeterminado, así mismo proporciona una dirección de anycast para conocer el mejor destino para los servidores de DNS, simplificando la búsqueda del servidor de destino.

El direccionamiento de red en IPv4 está diferenciado entre privado y público debido a esto para que un usuario en una red privada pueda tener conectividad hacia un host en otra red o internet es necesaria la configuración del protocolo NAT(Network Address Translation), que hace que aumente el procesamiento de los paquetes en el router y de esta manera se ve afectado su rendimiento, en IPv6 esto ya no será necesario ahorrando procesamiento en los equipos.

En el datagrama de IPv6 en la cabecera principal se inserta la información principal de enrutamiento, para enviar información secundaria se han creado las cabeceras de extensión que pueden o no enviarse, de esta forma se optimizan los recursos de los elementos intermediarios en la red ya que no tienen que procesar información que solo es útil para el host de destino.

Se incorpora la posibilidad de aumentar considerablemente el tamaño de los paquetes de datos hasta una longitud jumboframe, también está incorporado Ipsec permitiendo la encriptación y autenticación de los datos proporcionando mayor seguridad en el intercambio de información.

Como en IPv6 asigna una dirección ip única que identifica a un solo dispositivo existe la posibilidad que los usuarios puedan moverse entre redes sin necesidad de actualizar su direccionamiento, por defecto proporciona calidad de servicio permitiendo que los routers tomen decisiones sobre los paquetes dependiendo de la prioridad [1]. Es de resaltar que el despliegue de IPv6 se irá realizando gradualmente, en una coexistencia ordenada con IPv4, al que se irá desplazando a medida que dispositivos electrónicos con conexión a Internet, equipos de red, aplicaciones, contenidos y servicios se vayan adaptando a la nueva versión del protocolo de Internet[6].

4.2 IMPLEMENTACIÓN DE IPV6 EN COLOMBIA

El protocolo Ipv6 es fundamental para continuar con el desarrollo de Internet , por lo que desde los operadores de redes, las empresas, los desarrolladores de contenido y toda entidad que interactúe con Internet deben implementar Ipv6 para garantizar la conectividad a nivel global [30].

Al día de hoy conviven los 2 protocolos a nivel mundial el Ipv4 e IPv6 , el cambio a un protocolo nativo de Ipv6 no se puede dar de un día para otro pero los operadores de redes están avanzando rápido en la modernización desde sus interconexiones principales hasta los puntos de acceso de sus clientes para ofrecer conectividad en Ipv6 pero también el cliente debe realizar la migración de su red interna a Ipv6 ,se ve que los operadores de red en Colombia han realizado una gran inversión en el sector de las telecomunicaciones para poder ofrecer conectividad Ipv6 a sus clientes y por lo tanto están interesados en impulsar su implementación ofreciendo nuevos

servicios para conseguir el retorno de esta inversión[25].

El gobierno también tienen un papel crucial como promotor en el proceso de migración a Ipv6 por lo que es su responsabilidad mediante las entidades que regulan las Telecomunicaciones intensificar los intercambios de experiencias e información relevante a tener en cuenta en un proceso de migración de protocolo de direccionamiento así como también de desarrollar políticas que promuevan esa actualización tecnológica, es por eso que en Colombia el ministerio de la TICs elaboró la resolución 2710 de Octubre de 2017 [26] donde se informa que las entidades territoriales tienen como plazo máximo el 31 de Diciembre de 2020 para efectuar la transición del protocolo IPV4 al protocolo IPV6 so penas económicas[8].

En Colombia hay redes como RENATA que ya están en Ipv6 [29] al igual que muchas entidades que ya cumplen con la implementación del protocolo Ipv6 y que actualmente están en periodos de prueba y expansión, en la siguiente tabla se pueden ver algunas de ellas.

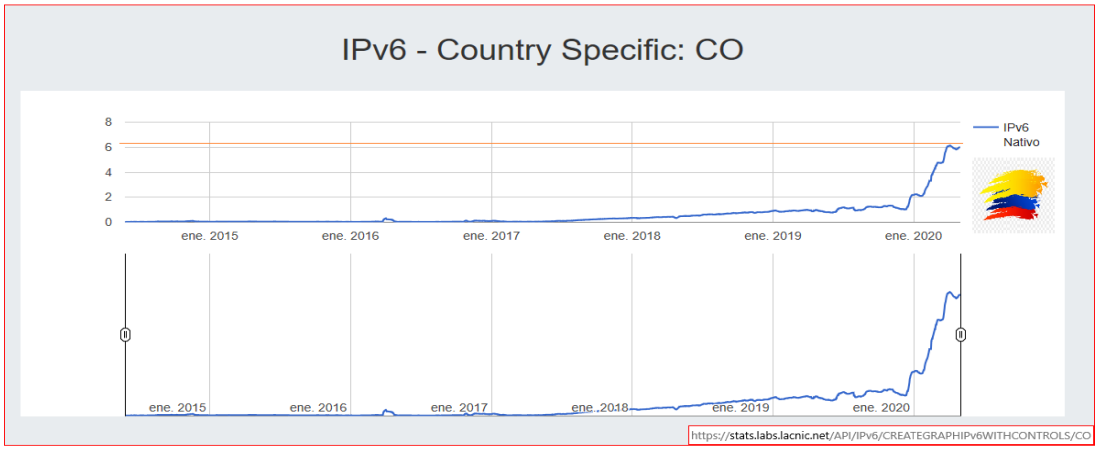
Tabla 1. Progreso en la implementación de Ipv6 en Colombia

Organización	Url	Pool ipv6	% IPv6	Implementado
Contraloría de Bogotá	http://www.contraloriabogota.gov.co/	2801:10:7000::/48	98%	Marzo de 2018
Empresa de Recursos Tecnológicos	http://www.ert.com.co/	2800:9F0::/32	95%	Junio de 2019
Instituto de Desarrollo Urbano	http://www.idu.gov.co	2800:490:4002::/48	93%	Diciembre de 2019
Unidad administradora Solidaria	https://www.orgsolidarias.gov.co/	2001:13f8:1100::/48	90%	Octubre de 2018

Fuente: https://www.renata.edu.co/protocolo-ipv6-en-colombia

Es importante destacar que en cumplimiento de las medidas tomadas por el gobierno Colombiano y el ministerio de las TICS, las organizaciones privadas y públicas han mostrado más compromiso con la adopción del protocolo aumentando un 4.5% su implementación en el último año [13].

Figura 2. Implementación de Ipv6 en Colombia a hoy



Fuente: https://stats.labs.lacnic.net

Según estadísticas en la página de control de LACNIC, en Colombia se tiene al 2020 un porcentaje de implementación del protocolo Ipv6 a nivel nacional que ronda el 6% , como se ve en la figura anterior.

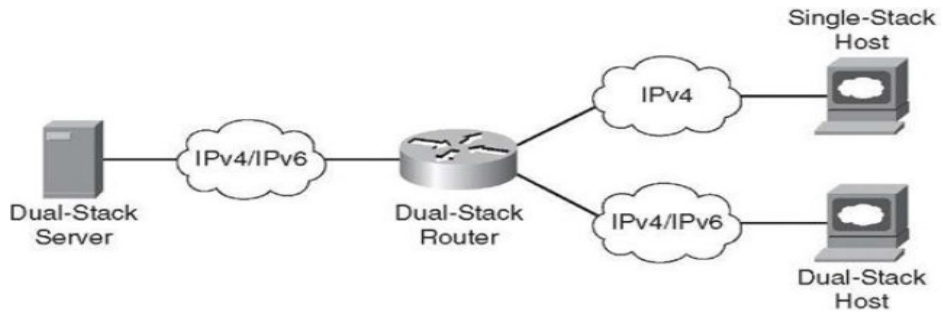
4.3 METODOS DE TRANSICION A IPv6

Coordinar una migración inmediata y masiva del protocolo Ipv4 a Ipv6 es imposible ya que Internet es una red multiprotocolo que es compartida por muchos sistemas que transportan gran variedad de paquetes por medio de una gran variedad de redes con características diferentes, esto hace que para poder incorporar el protocolo Ipv6 en ellas se tenga que hacer uso de diferentes técnicas propuestas inicialmente en grupos de trabajo de la IETF (Internet Engineering Task Force) y RFC (Request for Comments) [10].

Para realizar gradualmente la migración hacia el protocolo Ipv6 de las plataformas existentes en Ipv4, se debe por ahora garantizar la interoperabilidad entre estos 2 protocolos cuando no se dispone de una red nativa Ipv6 y se debe usar la infraestructura actual, ya sea porque no se dispone de equipos que soporten el protocolo Ipv6 o porque es elevado el costo de implementar el protocolo en los equipos del proveedor del canal [21]. Algunos de los métodos de transición más utilizados que permiten la interoperabilidad entre los protocolos Ipv4 e Ipv6 son:

4.3.1 Doble pila (Dual Stack): El método de transición más utilizado propone mantener en el mismo nodo dos pilas una para el protocolo Ipv4 y otro para el protocolo Ipv6, trabajando en forma simultánea el contenido de IPv4 e IPv6, por lo que ofrece una estrategia de coexistencia muy flexible [2]. el hardware donde se implemente este método debe tener un buen desempeño a nivel de procesamiento, ya que debe realizar doble trabajo al trasladar los paquetes a la pila correspondiente dependiendo del protocolo indicado en la cabecera del paquete. Tiene la ventaja de no necesitar más encapsulaciones permitiendo un enrutamiento rápido .

Figura 3. Topologia Dual-Stack



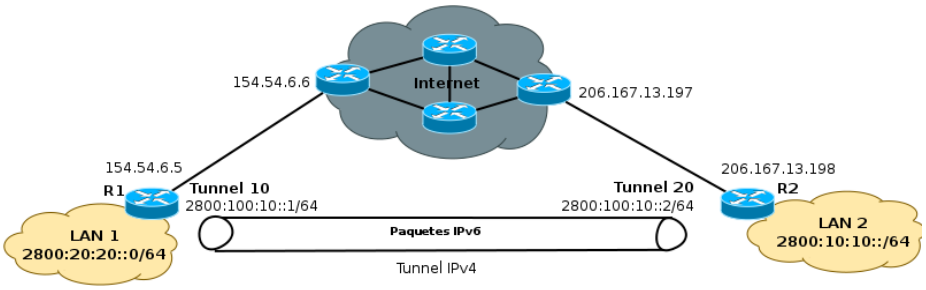
Fuente: http://www.ijser.org

4.3.2 Tunelización: El uso de túneles permite reutilizar la infraestructura Ipv4, para comunicar dos equipos que tienen el protocolo Ipv6 y que atraviesan un tramo de red en Ipv4, valiéndose de la encapsulación del paquete en Ipv4.

Este procedimiento de tunelizar permite realizar la migración gradual hacia el protocolo Ipv6, ya que desde que se tenga conectividad Ipv4 en las puntas del tunnel, se podrá pasar por ellos tráfico Ipv6, muy útil en operadores que no soportan aún el protocolo Ipv6 y que por costos no es factible un cambio de UM inmediata.

En un sentido la punta de entrada del túnel crea una cabecera de Ipv4 y dentro del payload envía la cabecera Ipv6 y sus datos, al llegar a la otra punta es desencapsulado el paquete Ipv4, quedando solo la cabecera de Ipv6 junto con su carga útil [10]. Este método está sujeto a mantener el tamaño del paquete encapsulado , por lo que no se puede pasar del tamaño máximo del paquete permitido MTU.

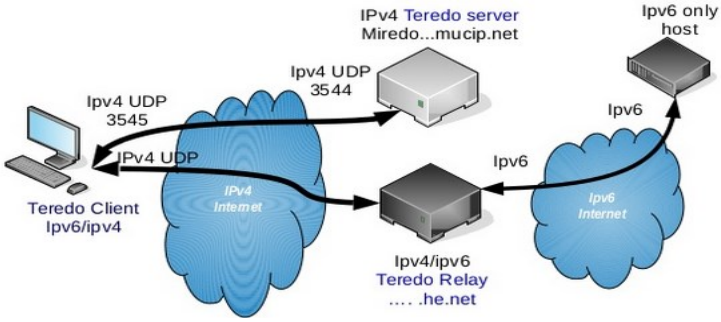
Figura 4. Tunnel Ipv4 to Ipv6



Fuente: http://www.redesymas.net

4.3.3 Teredo: Es una tecnología de transición a Ipv6, que a diferencia de los otros métodos es capaz de realizar las traslaciones detrás de un router con NAT, para ello se vale de un servidor que escucha por el puerto UDP 3545, allí llegan todas las solicitudes que van hacia el protocolo contrario, tan pronto llegan al servidor este realiza un cambio en la cabecera del paquete encapsulándolo y lo reenvía por el túnel que tiene a cada protocolo IPv6 o IPv4 en los host mapeados.

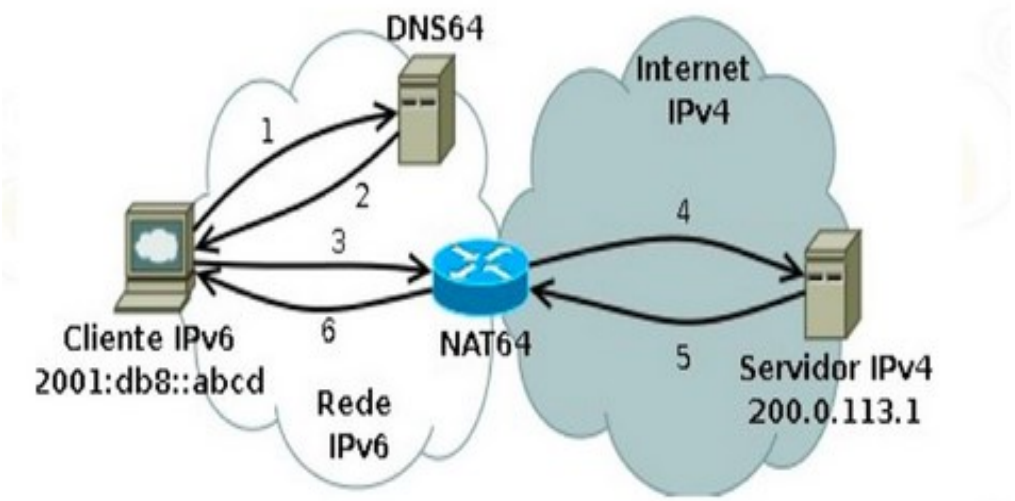
Figura 5. Técnica Teredo



Fuente:https://www.slideshare.net/rinnocente/ipv6-course

4.3.4 Nat64: Este método de transición a Ipv6, es muy parecido a como se realiza el NAT en los routers, ya que se mantiene una tabla que relaciona un direccionamiento origen con un direccionamiento destino. El algoritmo de Nat64 permite a máquinas Ipv6 comunicarse con servidores Ipv4, este servidor que puede ser un router tiene una interface en direccionamiento Ipv4 y otra en direccionamiento Ipv6 pero solo con una máscara de 96 bits, entonces se debe reconstruir la dirección destino complementando el direccionamiento Ipv6 con los 32 bits de la ip en Ipv4 [3]. El servidor mantiene un mapeo de estas conversiones para distribuir el tráfico según la dirección de destino, permitiendo la comunicación entre equipos corriendo diferente protocolo IP.

Figura 6. Método NAT64



Fuente:*https://slideplayer.es/slide/10270212/*

El funcionamiento de los diferentes métodos de transición a IPv6 definidos anteriormente así como el comportamiento general de la red diseñada se puede evaluar con anterioridad a la implementación por medio de un software computacional, dedicado a descartar errores y optimizar configuraciones ofreciendo un grado alto de certeza de la funcionalidad del diseño.

Con el uso de estos simuladores se puede evitar el influir negativamente en partes de la red que funcionaba correctamente así como también permiten dimensionar correctamente los equipos a utilizar evitando incurrir en pérdidas económicas, algunos de los simuladores más populares en el campo de las Telecomunicaciones son : Packet Tracert, OPNET, GNS3 y EVE-NG a continuación se verá una descripción de cada uno de ellos.

5. HERRAMIENTAS DE SIMULACIÓN DE REDES

En el mundo moderno los sistemas de redes de comunicaciones son esenciales para el funcionamiento de muchas empresas y es por eso que son una de las principales preocupaciones de los diseñadores de redes. Es importante abordar a través de la simulación el estudio de muchos parámetros del diseño de una red de comunicaciones y para ello es apropiado el uso de herramientas de modelado de redes de software abierto o privado.

Debemos tener en cuenta que la simulación en nuestro caso es un método que intenta reproducir un comportamiento real de dispositivos y elementos de red, que son difíciles o costosos de probar en la vida real.

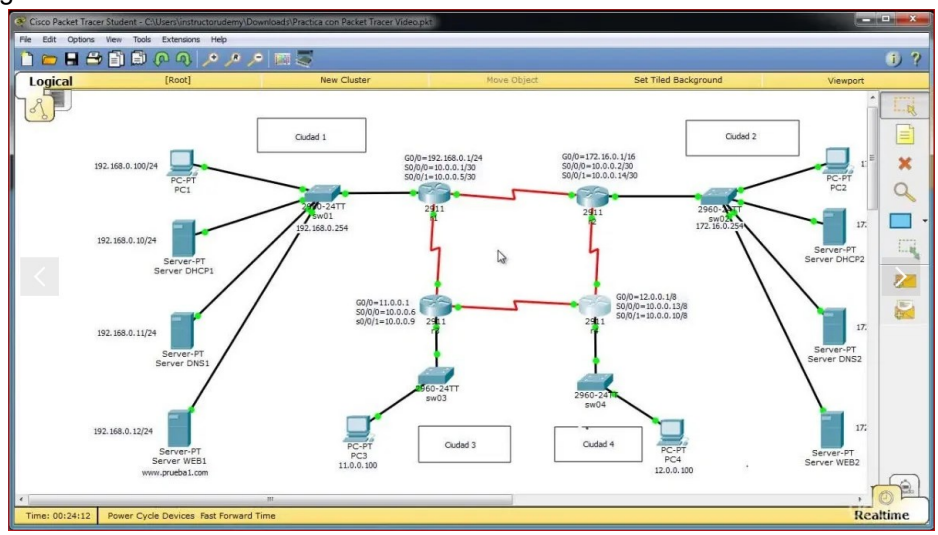
El uso de estos simuladores permite evaluar el desempeño de una red diseñada y así evitar tomar decisiones equivocadas como terminar implementando una red que no cumpla con lo propuesto o que provoque pérdidas económicas.

Existe gran cantidad de simuladores de redes de comunicaciones con una variedad de equipos virtuales y protocolos que pueden simular unos son básicos, especiales para comenzar la enseñanza en redes como JIMSIM y TOGGIT pero hay otros más destacables, por el tipo de licencia, por la cantidad de equipos que puede simular o lo aproximado a la realidad que pueden ser sus resultados, entre ellos encontramos Packet Tracer, GNS3, EVE-NG y OPNET [12].

5.1 SIMULADOR PACKET TRACER

Este simulador fue creado por CISCO para ayudar a que los alumnos de las academias de Networking tuvieran una buena experiencia de aprendizaje y adquirieran habilidades prácticas en redes, es ampliamente utilizado en instituciones educativas del área de comunicaciones y Telemática. Este simulador de entornos de redes de comunicaciones tiene una fiabilidad moderada; mediante la selección de dispositivos propios de la marca Cisco y la ubicación de estos en una área de trabajo se logra montar una topología para ser analizada.

Figura 7. Simulador Packet Tracert



Fuente:*https://codelatin.com*

Este programa permite emular entornos utilizando solo equipos que corren imágenes propias de IOS Cisco con dos modos de operación, una de ellas es operación de simulación que haciendo uso de un menú de controles admite el despliegue de ventanas durante la simulación en las que aparece alguna descripción del proceso de transmisión de los paquetes. Otro modo es la operación en tiempo real, este modo está diseñado para ver en tiempo real el estado activo o inactivo de los equipos cuando se envía tráfico como ping o snmp a través de la red [2].

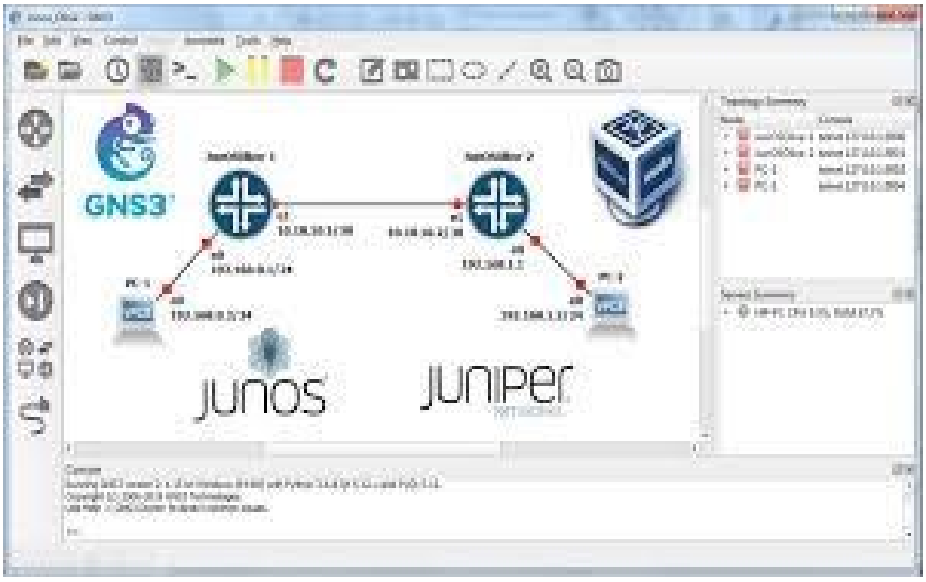
Packet Tracert tiene como ventajas, el enfoque pedagógico que lo convierte en una herramienta muy útil y fácil de manejar, permite ver por capas el proceso de transmisión y recepción de paquetes y permite la simulación de protocolos de enrutamiento RIPv2 y la ejecución de STP. Algunas de las desventajas de este programa es que es propietario por lo que no permite simular máquinas multimarca, tampoco tiene implementados los equipos de red para simular telefonía celular y satélites, además por considerarse de fiabilidad moderada no es muy utilizado fuera de ambientes académicos.

5.2 SIMULADOR GNS3

Un simulador destacable es GNS3, ya que tiene un tipo de licencia (GNU GPL v2) de código abierto y una gran cercanía con una buena cantidad de equipos reales, también se resalta su capacidad de interactuar con otros tipos de software como vware, Dynamips y Wireshark. Este simulador de interfaz gráfica permite simular topologías de redes complejas en el computador, no se tiene que pagar para usar GNS3 en un entorno personal o comercial. Esto es diferente a otras herramientas

en el mercado actual que son de propiedad del proveedor o de software pagado. Debido a que GNS3 es un software de código abierto, puede verificar todo el código fuente en GitHub incluso se puede contribuir al desarrollo de GNS3 [12].

Figura 8. Simulador GNS3



Fuente: https://telectronika.com/tutoriales/gns3-tutorial-juniper-junos-olive-sobre-virtualbox

GNS3 no limita la cantidad de dispositivos que puede ejecutar en una topología. Solo está limitado por los recursos de hardware que tiene disponibles. Otras soluciones como Cisco limitan el número de dispositivos en una topología a 20 dispositivos Cisco (dependiendo de la licencia) GNS3 no hace eso y puede ejecutar cientos de dispositivos en una topología GNS3 suponiendo que tengamos el hardware para hacerlo.

El programa consta de un área de trabajo donde se implementa la topología, arrastrando equipos de diferentes marcas que previamente se han creado instalando la imagen virtual, se realizan las conexiones entre ellos y se pueden abrir ventanas CLI por equipo para realizar su configuración.

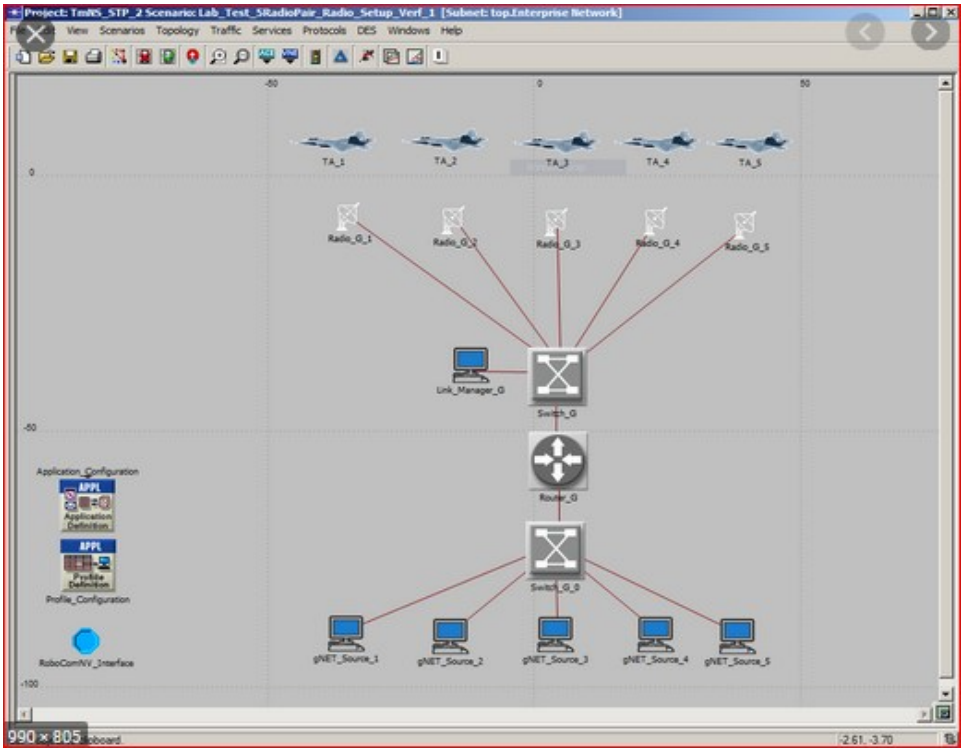
5.3 SIMULADOR OPNET

Riverbed es una compañía de tecnología especializada en la mejora del desempeño de redes y aplicaciones en la red en Mayo de 2012 esta empresa compró los derechos que OPNET Technologies tenía sobre su desarrollo en simulación de redes OPNET (Optimized Network Engieneering Tools).

OPNET Modeler es uno de los simuladores con más avanzada en el campo de las redes de Telecomunicaciones, una de sus cualidades más importantes es que este software está orientado a objetos con una gran cantidad de atributos a configurar permitiéndole al usuario interactuar fácilmente interpretar y crear escenarios que emulen una situación real en una red [32].

El programa tiene gran cantidad de librerías, y es ampliamente utilizado en la educación donde se tiene como núcleo la enseñanza básica y de temas avanzados de comunicaciones por ser altamente intuitivo y funcional. Se puede definir como un simulador dinámico y discreto que realiza cálculos determinísticos basándose en teoría de redes de colas.

Figura 9. Simulador Opnet



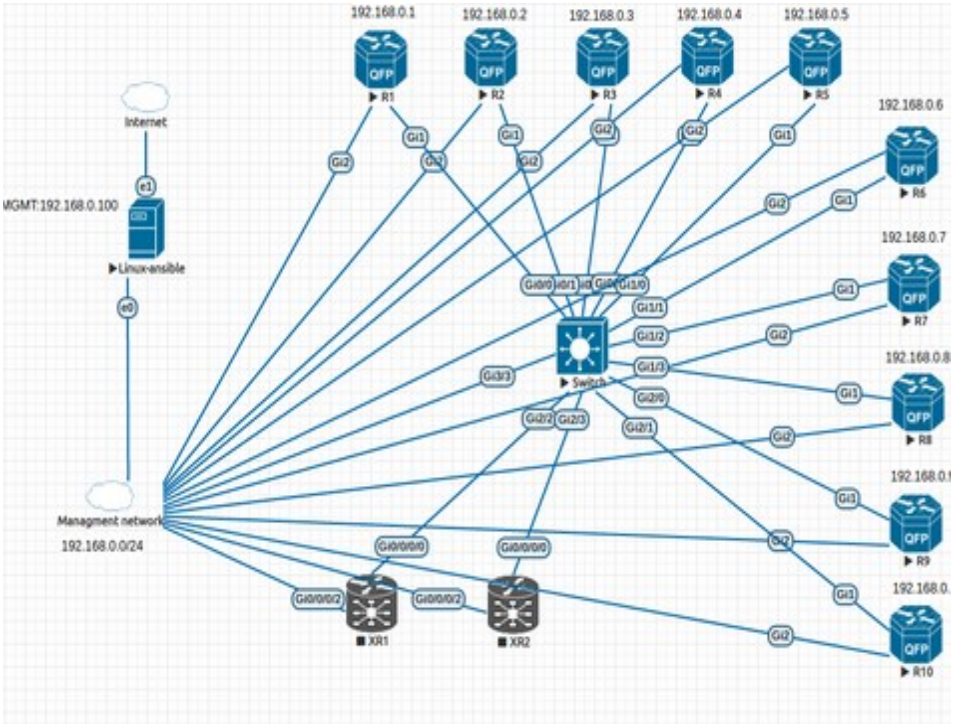
Fuente: https://www.robocomtech.com/projects/op/

El simulador OPNET está integrado por varios editores que proporcionan las herramientas necesarias para crear las topologías de red, en él se cuentan los editores de proyecto, de nodos, de enlaces, de rutas y de estadística. Es una herramienta ideal para evaluar las prestaciones de una red que esté sometida a diferentes condiciones de simulación como: caídas de enlace, pérdidas de paquetes y flujos variables de tráfico.

5.4 SIMULADOR EVE -NG

Este simulador relativamente nuevo es un software de emulación de red que soporta múltiples marcas, proporcionando múltiples oportunidades a los ingenieros de redes que quieren simular sin la influencia de las políticas de seguridad corporativas, pues permite ejecutarse en un entorno totalmente aislado .

Figura 10. Simulador EVE-NG



Fuente: https://www.robocomtech.com/projects/op

En su esquema de funcionamiento es muy similar al GNS3, ya que es necesario cargar las imágenes del sistema operativo del dispositivo a simular, por ejemplo en los equipos CISCO se debe cargar los IOS específicos para cada modelo [12].

Permite tener un control de las interfaces configuradas sobre la interfaz gráfica, al mostrar bastante información de las configuraciones relacionadas con cada puerto, este es un simulador no orientado a objetos por lo que es más específico en su configuración en otras palabras se debe configurar cada equipo por líneas de comando, con la desventaja de tener que conocer el set de comandos y la jerarquía que utiliza cada uno para sus configuraciones. A continuación se muestra una tabla con las características principales de cada simulador.

Tabla 2. Comparación de características de los simuladores

SIMULADOR	CARACTERISTICAS PRINCIPALES
PACKET TRACERT	* Interfaz grafica. * software Libre. * Alcance Academico. * Simulacion Mono marca Cisco. * Corre sobre Linux, Windows,Mac * Soporta enrutamiento basico segun imagen. * Soporta colaboración. * Se requieren imagenes de equipos reales. * Bajo consumo de recursos de CPU y Memoria.
OPNET	* Interfaz grafica. * Software Comercial y Academico. * Orientado a Objetos. * Simulacion discreta de eventos. * Alcance Profesional . * Corre sobre Windows,Mac y algunos Linux. * Moderado consumo de recursos de CPU y Memoria.
GNS3	* Interfaz grafica. * software Libre. * Alcance Profesional con imagen real. * Simulacion Multimarca. * Corre sobre Linux, Windows,Mac * Soporta enrutamiento avanzado segun imagen. * Soporta conectividad entre Maquinas virtuales. * Se debe tener las imagenes de los diferentes equipos. * Alto consumo de recursos de CPU y Memoria.
EVE-GN	* Interfaz grafica. * Software propietario * Alcance Profesional con imagen real. * Simulacion Multimarca. * Corre sobre Linux, Windows,Mac * Soporta enrutamiento avanzado segun imagen. * Se debe contar con las imagenes de los diferentes equipos. * Alto consumo de recursos de CPU y Memoria.

Fuente: Los autores.

6. JUSTIFICACIÓN

La actual digitalización de los negocios, el constante desarrollo de internet y especialmente del internet de las cosas (IOT) hacen que sea necesario la migración por parte de las empresas a IPv6, ya que no será posible la conexión con otras organizaciones con solo IPv4 debido a la gran cantidad de terminales. Así mismo de no realizarse la migración, la futura solicitud a un ISP de un nuevo pool de direccionamiento IPv4 será más costosa, y será más complicado el crecimiento y mantener la conectividad hacia Internet [15].

La adopción del nuevo protocolo trae grandes ventajas en el funcionamiento de la red de la entidad ya que por su diseño incorpora mecanismos de seguridad, calidad de servicio e incrementa el rendimiento, optimizando el funcionamiento y reduciendo el procesamiento de los equipos. Su implementación reduce el inconveniente de que las empresas adquieran en un futuro equipos obsoletos que solo soporten IPv4 disminuyendo la posibilidad de aplicar las buenas prácticas en cuanto a desarrollo de nuevas aplicaciones y servicios.

Según el organismo internacional encargado del Registro de Direcciones de Internet de América Latina y Caribe (Lacnic), Colombia ocupa el puesto 12 en la implementación de IPv6 en la región. De hecho, el país es superado por Uruguay, Brasil, México y Ecuador, los cuales tienen un tráfico de más del 20% sobre este protocolo, mientras que Colombia tiene un despliegue de solo el 6% [23].

Al realizar el plan y diseño de la red para migrar a IPv6 la entidad, se logra poner en práctica los conocimientos adquiridos en la especialización de Diseño de redes Telemáticas permitiendo adquirir experiencia y acercarse a las necesidades reales en el campo de las Telecomunicaciones en Colombia; el diseño y los resultados obtenidos pueden ser de gran ayuda y consulta para futuros proyectos en la universidad "El Bosque" que tengan relación en la adopción del protocolo IPv6, ya que puede convertirse este proyecto en una guía general aplicable a cualquier tipo de compañía que requiera implementar el protocolo Ipv6 en su red.

7. OBJETIVOS

7.1. GENERAL.

Diseñar una red de datos con buena disponibilidad y un plan de direccionamiento que permita la transición a IPV6 de todos los dispositivos que componen actualmente la red de datos en una entidad del estado para dar cumplimiento a la circular 2710 del Mintic.

7.2. ESPECÍFICOS.

1. Caracterizar la información del esquema de red en la entidad a migrar a IPv6.

2. Diseñar un plan de implementación del protocolo IPV6 sobre la red existente sin afectar a los servicios en funcionamiento, ni su desempeño.

3. Verificar el funcionamiento del diseño propuesto mediante un sistema computacional.

8. REQUERIMIENTOS

- Se debe levantar la topología actual con la relación de equipos que la conforman.
- La coexistencia de IPv4 e IPv6 no debe afectar a los servicios y aplicaciones actuales del cliente.
- El diseño de la red Ipv6 no debe afectar la seguridad de la red actual.
- Se debe reutilizar la infraestructura existente con sus capacidades actuales, siempre que sea posible.
- Se debe realizar la verificación del funcionamiento de la red IPv6 mediante la simulación de una parte de la red que contenga al menos las sedes principales (Bogotá, Medellín, Cali y Barranquilla) y algunas sedes remotas.
- La red IPv6 diseñada debe soportar un crecimiento del 10% de los hosts.
- Desde el segmento IPv6 de las sedes se debe dar salida a Internet por medio de la sede principal de la entidad.
- Se debe entregar la topología final actualizada con los segmentos IPv6 con sus respectivas aclaraciones.
- La implementación de la transición de IPv4 a IPv6 es decisión de la entidad objeto del análisis, por lo que el alcance del proyecto es una propuesta de solución de red en IPv6.

9. METODOLOGÍA DE DESARROLLO

Con la necesidad de prevenir retrasos en la ejecución de las actividades que permiten acercarse a un efectivo cumplimiento de los objetivos específicos planteados en este proyecto, se hace imperativo adoptar la metodología denominada SCRUM ya que el eje de esta metodología se centra en el trabajo en equipo; para cumplir con los objetivos se procede a dividirlos en actividades que sean más fáciles de controlar, entonces:

Al Caracterizar la información del esquema de red actual se debe:

- Dimensionar la red existente indagando sobre la cantidad de sedes remotas y la cantidad de máquinas en la red LAN.
- Recolectar información sobre tipo de tráfico que transporta la red actualmente .
- Identificar la prioridad del tipo de tráfico para el cliente.
- Identificar los equipos de red que conforman la topología actualmente y sus características relacionadas con el Ancho de banda soportado y compatibilidad con el protocolo de Internet IPv6.
- Identificar los proveedores de Última Milla de las sedes y confirmar con ellos la capacidad de propagación del protocolo IPV6 a través de su red.

Al Diseñar un plan de implementación del protocolo IPV6 sobre la red existente sin afectación de los servicios en funcionamiento ni su desempeño, se debe:

- Solicitar y obtener ante las entidades encargadas los recursos de direccionamiento IPv6 que serían asignados para uso del cliente .
- Crear un plan de direccionamiento IPv6 y correlacionar con los segmentos IPv4 utilizados actualmente por el cliente.
- Realizar una comparación de ventajas y desventajas de los métodos de transición de IPv4 a IPv6 como son Dual Stack, Túneles y Traducción EUI64.
- Determinar cuál método de transición de IPv4 a IPv6 se utilizará en cada sede teniendo en cuenta las anteriores comparaciones.
- Completar la topología de red del cliente incluyendo equipos o canales que permitan mejorar la disponibilidad del servicio en sus sedes más sensibles a fallos (Bogotá, Cali, Barranquilla y Medellín).
- Presentar el diseño final de red con la topología en Ipv4 e Ipv6 .

Al Verificar el funcionamiento del diseño propuesto mediante un sistema computacional se debe:

- Realizar una comparación entre los diferentes sistemas computacionales, que permiten emular redes.
- Determinar qué sistema de cómputo permite simular apropiadamente una

parte de la red.

- ➢ Utilizar el sistema elegido anteriormente para comprobar el correcto funcionamiento de la red.
- ➢ Documentar los resultados obtenidos y observaciones para la implementación del plan de transición de Ipv4 a Ipv6 en la entidad.

Al documentar los resultados y presentar las conclusiones se debe:

- ➢ Realizar reunión de seguimiento para aprobación del documento final.
- ➢ Realizar correcciones sugeridas por parte de los directores y asesores del proyecto.
- ➢ Sustentar el proyecto ante los jurados.
- ➢ Entregar el documento a la biblioteca para que lo pueda consultar la comunidad universitaria.

10. DESARROLLO

10.1 PLAN PARA LA TRANSICIÓN A IPV6 EN LA ENTIDAD

Antes de comenzar el proceso de transición al protocolo IPv6 en una red de datos es necesario trazar un plan donde se especifiquen los pasos que se deben tener en cuenta para conseguir una transición controlada sin afectar los servicios que actualmente soporta la red, y cuando se enfrenta el reto de hacer una migración de protocolo de direccionamiento a Ipv6 en una red surge la primeras preguntas: ¿A cuales equipos le vamos a implementar IPv6?, ¿A Cuántos equipos le vamos a implementar IPv6? y ¿Cuáles de estos soportan IPv6? , es por esto que se precisa levantar mediante un análisis de la infraestructura de la entidad un inventario de los equipos que la conforman y poder definir cuáles de estos necesitan ser reemplazados o actualizados para poder adoptar el protocolo IPv6.

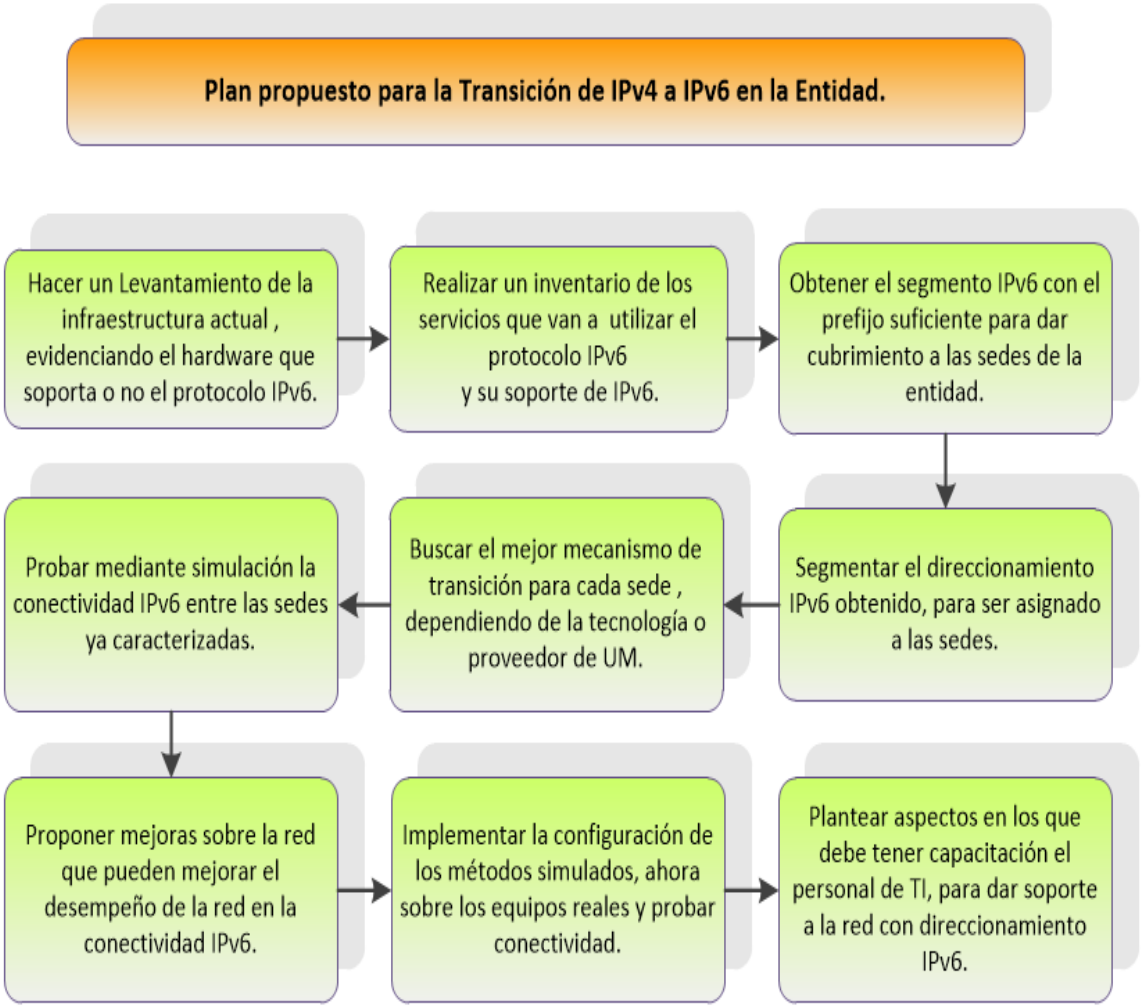
Los servicios que actualmente maneja la entidad así como el Software deben ser objeto de análisis para determinar si soportan el protocolo IPv6 así entonces servicios como directorio Activo, Servicios Web, Correo Electrónico, DHCP, voz IP o Software de Inventarios y herramientas colaborativas deben ser relacionadas.

El pool IPv6 debe ser solicitado al proveedor de servicios de Internet, pero esto tendría problemas si en un futuro se termina el contrato con este proveedor ya que al ser el pool del operador se debería realizar nueva segmentación y configuración del direccionamiento con el pool asignado por el nuevo operador; para librar esta situación es recomendable hacer la solicitud de un pool como usuario final a LACNIC que es la entidad encargada de asignar el direccionamiento a las entidades y organizaciones de América Latina y el Caribe donde se le reservará un pool con una asignación mínima de prefijo /48.

El direccionamiento IPv6 obtenido debe ser segmentado de forma tal que cubra las necesidades de las sedes de la entidad en forma ordenada y escalable, ya que el principal objetivo de la migración es disponer de direccionamiento suficiente para asignar a los nuevos dispositivos que se conecten a la red. Es importante también solicitar el enrutamiento de este direccionamiento al proveedor de servicios de Internet, con el propósito de anunciarlo a la nube y de confirmar con él que método de transición es apropiado utilizar en cada sede dependiendo de la tecnología utilizada en la UM o del soporte del protocolo de Ipv6 por parte del proveedor de UM, luego de esto es necesario realizar un laboratorio de conectividad si en la entidad no se dispone de la forma de hacer un laboratorio, es necesario realizar una simulación en un software computacional que nos permita comprobar la conectividad entre los equipos de la red.

Siempre hay oportunidades de mejorar el desempeño de una red, por lo que de los resultados del análisis de la infraestructura actual se debe sugerir cambios que permitan optimizar la red y sacarle provecho a los beneficios de IPv6, si se toma la decisión de implementar el protocolo se debe configurar lo simulado anteriormente en los equipos reales en un escenario controlado, si no presenta problemas de conectividad se extenderá está a todas las sedes. Es recomendable plantear los aspectos primordiales en la administración de redes con coexistencia de protocolos IPv4 e IPv6 mediante una capacitación del personal para minimizar los riesgos de fallas al completar la migración a IPv6 nativo esto cuando se apague IPv4. En el siguiente esquema se plantea de forma resumida los pasos necesarios para la transición sugerida del protocolo IPV4 a Ipv6 en la entidad.

Figura 11. Plan propuesto para la transición de IPv4 a IPv6 de la Entidad



Fuente: Los autores.

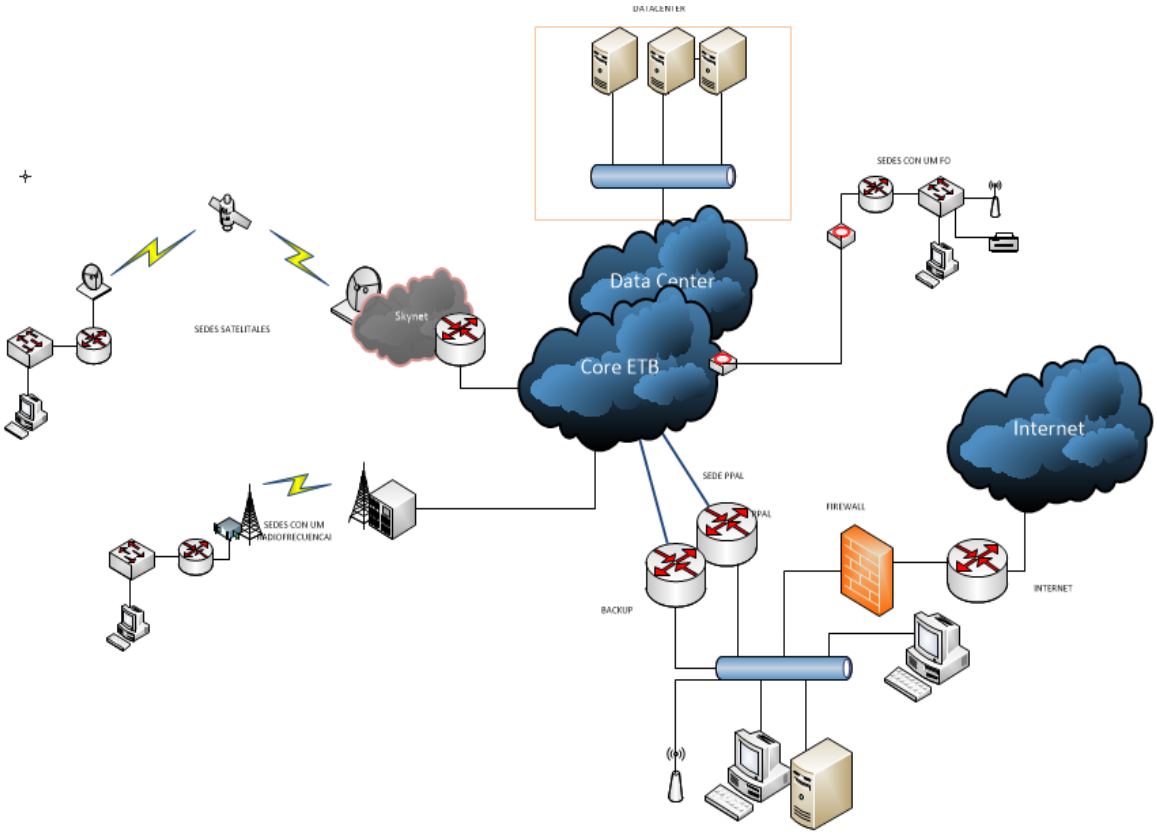
10.1.1 Análisis de la topología actual de la red. Se encontró durante el análisis que el principal proveedor es ETB el cual entrega la conectividad a las sedes en una red MPLS full mesh implicando que todos los puntos tienen conexión directa entre sedes con un máximo de un salto en direccionamiento capa 3 para las que se encuentran en red propia de ETB y de una adición de dos o máximo 3 saltos capa 3 con proveedores terceros de ETB en zonas de difícil acceso, los equipos de enrutamiento son todos propiedad del proveedor y son ajustados según el ancho de banda contratado por el mismo en modalidad arriendo, los equipos que proveen wifi también son parte de un producto que ofrece el proveedor, los únicos equipos propiedad del cliente son los equipos de seguridad ubicados en el datacenter del proveedor, los switch utilizados en las sedes de gran tamaño, las impresoras locales en las sedes de de inspección y algunas territoriales no cuentan con tarjeta de red y son propiedad del cliente, se gestiona a través de algún equipo en la sede, las impresoras que si están integradas a la red se encuentran bajo la modalidad de arriendo implicando que el proveedor debe ajustarlas o cambiarlas si se realiza la migración.

Los enrutadores utilizados varían entre 3 modelos diferentes según el BW contratado al proveedor, se observa que las sede pequeñas fueron entregadas con el equipo BDCOM BSR2800-24E, este esquipo es ampliamente usado en la solución completa del cliente ya que el equipo cuenta con un SW fast ethernet embebido de 24 puertos, ofreciendo una alta densidad de conexiones en las sedes remotas cubriendo sin problemas las necesidades en este tipo de sedes los anchos de banda contratados por la entidad varían entre los 3Mb/s, para el segundo rango de sedes las cuales la entidad considera territoriales los equipos utilizados son también los BDCOM BSR2800-24E los cuales manejaran un ancho de banda de 10MB para el resto de parámetros mencionados antes se manejaran las mismas condiciones con el agregado que se tendrán conexiones a nivel LAN con switches HP 1910-48G para los sitios donde se cuente con más de una planta y poder responder a las necesidades de conectividad.

Para las sedes con mayor ancho de banda se optó por equipos cisco 4431 con una capacidad de ancho de banda de fábrica de 500MB ampliable vía licenciamiento a 1GB, para estos casos se encontraron switch HP 1910-48G, estos equipos son gestionables y no cuentan con capacidades capa 3, facilitando el paso del tráfico ipv6 ya que no tienen ninguna interacción con el protocolo, todas las sedes donde fue solicitado conexión wifi el proveedor entrego equipo Ruckus R300, estos equipos se encuentran gestionados de manera remota y utilizan de manera independiente un enrutamiento para su gestión, en cuanto a la conectividad de las sedes se observa que en los diagramas no cuentan con direccionamiento en la solución implicando que su configuración en la solución es en modo bridge con las vlans necesarias para separar el tráfico hasta el router. El router será el encargado de habilitar la interoperabilidad entre los segmentos físicos y el segmento wifi o en algunos casos donde solo se cuente con un único segmento y todas las maquinas se encuentre sobre el mismo. Esto será tomado en cuenta el diseño propuesto.

Finalmente, para el punto central de la topología encontraremos un equipo cisco 4451-x para recibir la conectividad avanzada de un canal de 500MB, este equipo de fábrica soporta 1GB y de ser necesario es posible ampliarlo a 2GB con licenciamiento, adicional encontraremos un cisco 4431 el cual es el encargado de realizar la conexión de toda la red de datos a internet con un canal de 300MB.

Figura 12. Ejemplo de Modelo de Infraestructura actual en la entidad



Fuente:Los autores.

10.1.1.1 Inventario de TI para la red actual. Se observa que las sedes territoriales se comunican con una sede principal por medio de una red MPLS propiedad del ISP (ETB) y que tienen conectividad en Ipv4 a Internet por medio de un direccionamiento público que con la ayudad del Firewall en la sede principal realiza NAT, esta es una configuración típica en muchas entidades.

En este caso particular, las sedes están categorizadas en sedes Inspecciones, sedes Territoriales ,sedes Capitales, Data Center y sede Ppal ;también se encontró que actualmente en todas las ultimas millas de las sedes entre los routers y los PE del ISP se utiliza enrutamiento estático a diferencia de la sede Ppal que cuenta actualmente con protocolo BGP .

Tabla 3. Inventario de recursos tecnológicos en la red actual

Tipo Sede	# Sedes	BW	Equipos Actuales en estas sedes
Inspecciones	124	3 Mb	5 Puestos (Cableados). 3 Teléfonos ips yealink (sip-t22p) 1 impresora local (epson l395) 1 Router BDCOM BSR2800-24E
Territoriales	32	10 Mb	20 Puestos de trabajo (Entre cableados y wifi) 2 Ap Ruckus r300 2 Maquinas de impresion 1 switch HP 1910-48G 10 Telefonos ip yealink. 1 Router BDCOM BSR2800-24E
Capitales	1	500 Mb BOGOTA PPAL	80 Puestos de trabajo cableados y WIFI. 12 Aps ruckus r300 3 Sw HP 1910-48G 1 router ISR 4451-X 3 servidores Dell power edge (correo,aplicativo Intranet ,aplicativo Datos) 6 maquinas de impresion Xerox Multifuncionales. 60 telefonos ip yealink.
	1	25 Mb MEDELLÍN	50 Puestos de trabajo cableados y WIFI. 4 aps ruckus r300 1 Router ISR 4431 2 Sw HP 1910-48Ga 2 máquina de impresión Xerox Multifuncionales. 30 teléfonos ip yealink.
	1	25 Mb CALI	50 Puestos de trabajo cableados y WIFI. 4 aps ruckus r300 1 Router ISR 4431 2 Sw HP 1910-48Ga 2 maquina de impresion Xerox Multifuncionales. 30 teléfonos ip yealink

Fuente: Los autores.

Tabla 3. Inventario de recursos tecnológicos en la red actual(Continuación)

Tipo Sede	# Sedes	BW	Equipos Actuales en estas sedes
Capital	1	25 Mb BARRANQUILLA	50 Puestos de trabajo cableados y WIFI. 4 aps ruckus r300 1 Router ISR 4431 2 Sw HP 1910-48Ga 2 maquina de impresión Xerox Multifuncionales. 30 teléfonos ip yealink
Internet	1	300 Mb INTERNET PPAL	1 Firewall FORTIGATE 200B 1 router cisco 4451X

Fuente: Los autores.

Al obtener el inventario se realizó una investigación para determinar si los equipos encontrados soportan el protocolo Ipv6. Para el caso de la familia de equipos Cisco 4000 se encontró que todos soportan el protocolo, también lo hacen los equipos Bdcom según la información entregada por el proveedor Energitel al ISP. Para el equipo de seguridad Fortigate 200B en la página del proveedor se observó que aunque no tiene las ultimas prestaciones si tiene soporte del protocolo ipv6.

El resto de equipos como los acces-point de la marca Ruckus se encuentran configurados en modo bridge y no se ven afectados por la implementación del protocolo, las máquinas impresoras de gran tamaño Xerox que se encuentran conectadas a la red del cliente se encuentran bajo contrato y con soporte para configuración de Ipv6, los switches marca HP 1910 con los que cuenta el cliente en todas sus sedes también soportan el protocolo Ipv6 según su data-sheet, aunque en la mayoría de sedes son utilizados en capa 2.

10.1.1.2 Servicios. Los sistemas de información de la entidad están a cargo del grupo TI de soporte informático, ellos tienen la responsabilidad de administrar la infraestructura y dar soporte relacionado con el almacenamiento, procesamiento, transmisión, control y seguridad informática granizando la continuidad de los servicios

La información que fue suministrada por parte del grupo de TI acerca de los servicios con los que actualmente cuenta la entidad se describen a continuación:

- Servicios Web: Los servidores en donde se alojan sus páginas web son Apache e IIS (Internet Information Services), que por las versiones que están

actualmente en uso escuchan tanto en IPv4 e IPv6 por el puerto 80. Además, cuentan con servidores de aplicaciones Java y .NET.

- Servicio DNS: La labor de realizar la traducción de nombres de dominio esta a cargo de un servidor con una versión de BIND que trabaja con ipv6. Se puede configurar el servidor DNS para que atienda peticiones de igual manera en IPv4 e IPv6, siendo capaz de recibir y enviar información en ambos protocolos.

- Telefonía IP: La telefonía IP de la entidad está conformada por teléfonos ip yealink SIP-T22P que soportan los estándares de ipv6.

- Bases de datos: Oracle y SQL Server configurados en un servidor Dell power edge el cual permite la configuración de direccionamiento IPv6.

- Correo electrónico: Para su correo corporativo, la entidad cuenta con el software Microsoft Exchange Server configurado en un servidor Dell power edge el cual permite la configuración de direccionamiento IPv6.

- Internet: El servicio de internet esta dimensionado para soportar el tráfico tanto de la sede principal como de sus sedes territoriales e inspecciones.

- DHCP: En la red operativa se encuentran configurados los servidores de DHCP *(Dynamic Host Configuration Protocol*) localmente en cada router de la sede, entregando direccionamiento privado dinámico Ipv4 con mascara /24 a los equipos que están en su mismo dominio.

10.1.1.3 Análisis de capacidad de soporte de Ipv6 del ISP y Terceros. No todos los proveedores de servicios de Telecomunicaciones en Colombia están preparados para implementar y ofrecer a sus clientes servicios sobre Ipv6, en varios de estos operadores al día de hoy no han trabajado en adelantar actividades para hacer la transición de sus redes a unas que soporten Ipv6, para muchos proveedores de servicios de Internet es complejo desplegar Ipv6 en su red en gran medida por la incompatibilidad que se ha creado al utilizar diferentes tecnologías a lo largo de los años.

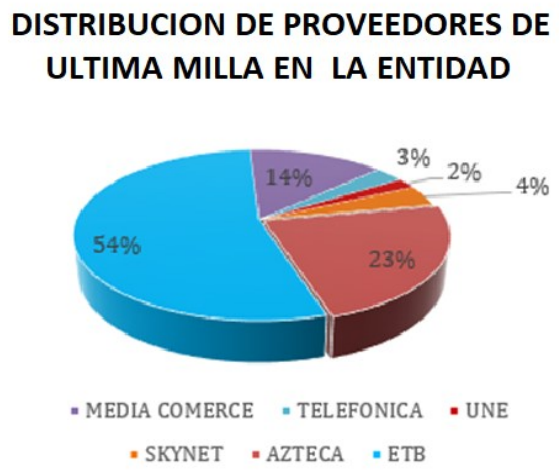
El medio físico utilizado en la última milla en las diferentes sedes de la entidad obedece a múltiples factores como, condiciones climáticas, permisos para utilización de alguna infraestructura existente, distancia o disponibilidad de red en la zona, por ejemplo en algunas de las sedes ETB no tiene cobertura de fibra óptica por eso hace uso de Radio frecuencia para ofrecer el servicio de conectividad IP como en las sedes Territoriales: Magdalena, Urabá y Quibdó.

Las tecnologías que utilizan los operadores en zonas urbanas donde se encuentran las principales sedes de la entidad se basan de fibra óptica como por ejemplo la sede Ppal de la entidad en Bogotá y las sedes Capitales como: Barranquilla, Cali y Medellín que se encuentran aprovisionadas directamente por el ISP ETB (Empresa de Telecomunicaciones de Bogotá), este ISP tiene soporte de Ipv6 en su red Core y tiene contratado la responsabilidad por la conectividad del resto de las sedes de la entidad.

En las zonas rurales alejadas ETB no implementa infraestructura para un solo cliente por motivos de rentabilidad, por lo que subcontrata el servicio de última milla con otros proveedores, en algunos casos estos proveedores entregan el trafico taggeado con una vlan por cada sede en la interconexión que tienen con el ISP principal(ETB) como por ejemplo TV Azteca y Media Comerce en tecnologías de última milla como Fibra óptica y radio, estos operadores al no intervenir con la capa de red no presentan ninguna limitación para la implementación del protocolo Ipv6.

Hay otros operadores como Skynet (que utiliza microondas como última milla) y Telefónica(Con radiofrecuencia) que si intervienen en la capa de red ya que deben realizar el enrutamiento del direccionamiento de cada sede en su red, y entregan todo el tráfico en una sola vlan de interconexión, estos operadores enrutan direccionamiento Ipv4 y por ahora no ofrecen soporte de Ipv6 en su red por lo que se tendrá que implementar un método de transición a Ipv6 que permita incorporar estas sedes a la solución. En la siguiente gráfica y tabla se puede ver el porcentaje de sedes que tienen en la última milla operadores que soportan el protocolo Ipv6 nativo.

Figura 13. Distribución de proveedores de servicios en la entidad



Fuente: Los autores.

Tabla 4. Relación de soporte de Ipv6 nativo por los operadores de UM

SOPORTE NATIVO DE IPV6 EN PROVEEDOR UM			
PROVEEDOR	SOPORTA	%	TOTAL
AZTECA	SI	23%	91%
ETB		54%	
MEDIA COMERCE		14%	
TELEFONICA	NO	3%	9%
UNE		2%	
SKYNET		4%	

Fuente: Los autores

La conexión a Internet en la sede principal se hace mediante el Firewall Fortigate 200B que administra la empresa SIGMA , quienes indican que el firewall cumple con los requisitos para la transición al protocolo Ipv6 y que ellos están en la capacidad de configurar los parámetros en el momento que se requiera. En el anexo B se encuentra la discriminación de las sedes de la entidad con su correspondiente proveedor de última milla y se indica si soporta Ipv6 nativo.

10.2 DISEÑO Y MEJORAS EN LA RED PARA MIGRAR A IPV6.

Con el fin de obtener el máximo beneficio de la transición del protocolo Ipv4 a Ipv6 en la entidad es necesario realizar actividades propias de un diseño de red como es el estudio y segmentación del direccionamiento Ipv6 que se ajuste a las condiciones actuales de la red y que permita adaptarse a los cambios futuros evitando afectar la continuidad del servicio y facilitando una transición controlada.

Es necesario proponer mejoras sobre la red actual que le den a esta más valor como disponibilidad y estabilidad así como herramientas de gestión y capacitación a sus administradores para que puedan optimizar los tiempos de resolución de fallas y cuenten con información útil para cuando se enfrenten a situaciones de toma de decisiones. Como se vio en el plan de transición anterior, es necesario hacer la segmentación de direccionamiento Ipv6 y la definición de los métodos de transición propias para cada sede según su topología de UM, a continuación se explica detalladamente este tema y adicionalmente se entregan varias recomendaciones de mejora en la red para que sean tenidas en cuenta por la entidad a la hora de decidir la implementación del protocolo Ipv6.

10.2.1 Adquisición y Segmentación de pool IPv6 propuesto para las sedes.

Como se mencionó anteriormente es recomendable como usuario final solicitar el pool de direccionamiento Ipv6 directamente a LACNIC para no tener que realizar el proceso de asignación de direccionamiento cada vez que se cambie de ISP, LACNIC pide al solicitante cumplir con los siguientes compromisos para realizar y mantener la asignación de direccionamiento Ipv6 :

- Anunciar en los equipos de borde hacia Internet el bloque asignado con la mínima desagregación posible.
- Entregar una descripción detallada de la topología de la red.
- Realizar un informe detallado de los planes de enrutamiento.
- Realizar el registro en WHOIS antes de 7 días después de la asignación.

Suponiendo que después de la solicitud presentada a LACNIC por parte de la entidad del estado, le sea asignado el pool y prefijo 2800:26c:14a::/48 ya que para usuarios finales LACNIC entrega como regla general un prefijo /48. Si tenemos en cuenta la cantidad de sedes a las que se les debe asignar direccionamiento entre sedes tenemos la siguiente relación:

Figura 14. Cantidad de equipos por sede

Tipo de Sede	# Sedes	# Dispositivos que requieren IPv6
DataCenter	1	3
Sede Principal	1	210
Sedes Capitales	3	120
Sedes Territoriales	32	50
Sedes Inspecciones	124	20

Fuente: Área TI de la Entidad.

Se observa que la sede Principal tiene 210 equipos y es la que más requiere de direcciones Ipv6 mientras que el tipo de sedes caracterizadas como Inspecciones son las que menos direcciones Ipv6 necesita pero que más subredes necesita ya que tiene 124 sedes en esta categorización. Como se mencionó anteriormente el protocolo Ipv6 dispone de un espacio de direccionamiento muy grande por lo que con el prefijo /48 asignado a la entidad se tiene bastante recurso disponible para realizar la segmentación de direcciones Ipv6.

El tamaño de las sedes y su distribución geográfica fueron los parámetros que se tuvieron en cuenta para caracterizar las sedes , es importante realizar esta diferenciación de sedes para poder llevar un control del direccionamiento y facilitar la identificación de fallas a futuro así como poder simplificar el enrutamiento para la aplicación de reglas de seguridad por parte de los administradores del Firewall, ahora si se toma el prefijo /48 y reservamos el siguiente nibble para identificar el tipo

de sede hasta el prefijo /52, se puede asignar la siguiente relación donde se clasifican hasta 16 tipos de sedes:

Figura 15. Segmentación Ipv6 por categoría

Segmento IPv6 Asignado según tipo de sede						
2800:26c:14a	**::/52**					**Caracterización**
2800:26c:14a:	0	0	0	0	::/64	Inspecciones
2800:26c:14a:	a	0	0	0	::/64	Territoriales
2800:26c:14a:	b	0	0	0	::/64	Capitales
2800:26c:14a:	c	0	0	0	::/64	Datacenter
2800:26c:14a:	f	f	0	0	::/126	Reservado para Ips Wan

Con este nibble podemos manejar hasta 16 categorias de sedes,

Fuente: Los autores.

Si ahora tomamos los siguientes 2 nibbles hasta el prefijo /60 para la identificación de la sede dentro de la categoría, podremos identificar hasta 256 sedes por categoría por ejemplo veamos cómo quedaría dentro de la categorización de Inspecciones (nibble categorización = 0).

Figura 16. Segmentación Ipv6 para sedes Inspecciones

Segmento IPv6 Asignado para LAN Inspecciones						
2800:26c:14a	**::/60**					**Inspecciones**
2800:26c:14a:	0	0	0	0	::/64	inspección 1
2800:26c:14a:	0	0	1	0	::/64	inspección 2
2800:26c:14a:	0	0	2	0	::/64	inspección 3
2800:26c:14a:	0	0	3	0	::/64	inspección 4
2800:26c:14a:	0	0	4	0	::/64	inspección 5
2800:26c:14a:	0	0	5	0	::/64	inspección 6
2800:26c:14a:	0	0	6	0	::/64	inspección 7
2800:26c:14a:	...	...	...	0	...	...
2800:26c:14a:	0	7	a	0	::/64	inspección 123
2800:26c:14a:	0	7	b	0	::/64	inspección 124

Nibble = 0 , indica Categoria Inpecciones

Con el incremento de este octeto se puede direccionar hasta 256 inspecciones .

Fuente: Los autores.

Dentro de la sedes se puede hacer segmentación del direccionamiento por vlans utilizando el siguiente nibble hasta alcanzar el prefijo /64 con el que podemos hacer una diferenciación por sede de hasta 16 vlans, como ejemplo en la primera sede de inspecciones quedaría así:

Figura 17. Segmentación Ipv6 para vlan en las sedes de Inspecciones

Segmento IPv6 LAN Inspecciones con campo de Vlan						
2800:26c:14a:	**::/64**					**Inspección 1**
2800:26c:14a:	0	0	0	0	::/64	Vlan Datos
2800:26c:14a:	0	0	0	1	::/64	Vlan Voz
…	..	..	..	..	…	…
2800:26c:14a:	0	0	0	f	::/64	Vlan n=16

Con el incremento de este nibble se podra segmentar el direccionamiento por vlans , hasta 16 vlans.

Fuente: Los autores.

En la siguiente grafica se puede ver el formato para la segmentación Ipv6 para las sedes Territoriales con el nibble de categoría = a.

Figura 18. Segmentación Ipv6 para sedes Territoriales.

Segmento IPv6 Asignado para LAN Territoriales						
2800:26c:14a:	**a000::/64**					**Territoriales**
2800:26c:14a:	a	0	0	0	::/64	Pool Datos Territorial 1
2800:26c:14a:	a	0	0	1	::/64	Pool Voz Territorial 1
2800:26c:14a:	a	0	1	0	::/64	Pool Datos Territorial 2
2800:26c:14a:	a	0	1	0	::/64	Pool Voz Territorial 2
..	..	..	..	..	..	..
2800:26c:14a:	a	f	f	0	::/64	Pool Datos Territorial 256
2800:26c:14a:	a	f	f	1	::/64	Pool Voz Territorial 256

Fuente: Los autores.

La segmentación Ipv6 para las sedes Capitales con el nibble de categoría = b, quedaría así:

Figura 19. Segmentación Ipv6 para sedes Capitales

Segmento IPv6 Asignado para LAN Capitales						
2800:26c:14a:	**b000::/64**					**Capitales**
2800:26c:14a:	b	0	0	0	::/64	Pool Datos Capital 1
2800:26c:14a:	b	0	0	1	::/64	Pool Voz Capital 1
2800:26c:14a:	b	0	1	0	::/64	Pool Datos Capital 2
2800:26c:14a:	b	0	1	0	::/64	Pool Voz Capital 2
..		..	..	..	..	..
2800:26c:14a:	b	f	f	0	::/64	Pool Datos Capital 256
2800:26c:14a:	b	f	f	1	::/64	Pool Voz Capital 256

Fuente: Los autores.

Los equipos ubicados en el Datacenter tendrán direccionamiento Ipv6 con el siguiente formato, ya que se utiliza el nibble de categoría = c.

Figura 20. Segmentación Ipv6 para los equipos de DataCenter.

Segmento IPv6 Asignado para equipos Datacenter						
2800:26c:14a:	**c000::/64**					**Datacenter**
2800:26c:14a:	c	0	0	0	::0/64	Equipo 1 DC
2800:26c:14a:	c	0	0	0	::1/64	Equipo 2 DC
2800:26c:14a:	c	0	0	0	::2/64	Equipo 3 DC
2800:26c:14a:	c	0	0	0	::3/64	Equipo 4 DC
..		..	..	..	..	..

Fuente: Los autores.

También se ha reservado direccionamiento Ipv6 con prefijos /126 para cuando sea necesario configurar interfaces Wan con direccionamiento propio , o para realizar Interwan entre equipos con el siguiente formato:

Figura 21. Segmentación Ipv6 Wan en las sedes

Segmento IPv6 Reservado para Wan								
2800:26c:14ª	**::/126**							**Wan par Categorias**
2800:26c:14a:	f	f	0	0	0	0	::/126	Reservado para Wan Inspecciones
2800:26c:14a:	f	f	0	a	0	0	::/126	Reservado para Wan Territoriales
2800:26c:14a:	f	f	0	b	0	0	::/126	Reservado para Wan CApitales
2800:26c:14a:	f	f	0	c	0	0	::/126	Reservado para Interwan DC
2800:26c:14a:	f	f	0	..	0	0	::/126	…

Este nibble especifica la Categoria de la sede.

Con el incremento de estos 2 nibbles se segmenta direccionamiento Wan /126 dentro de cada categoria.

Fuente: Los autores.

La asignación de direccionamiento Ipv6 a los equipos de comunicaciones como Routers, Aps, Swiches y Servidores se realiza de forma manual ya que es necesario tener control de que direccionamiento tiene en sus interfaces por ser los equipos más susceptibles a ataques o que requieren una trazabilidad para detectar fallos, por esta razón del pool Ipv6 asignado a cada sede se reservarán las primeras 128 ips para direccionamiento fijo de los equipos críticos. El resto de direccionamiento Ipv6 de las sedes será asignado por medio de un servidor DHCP, y se llevará registro del direccionamiento por medio de un administrador de espacio de direccionamiento. En el anexo B se relaciona el detalladamente el direccionamiento asignado a cada sede de la entidad.

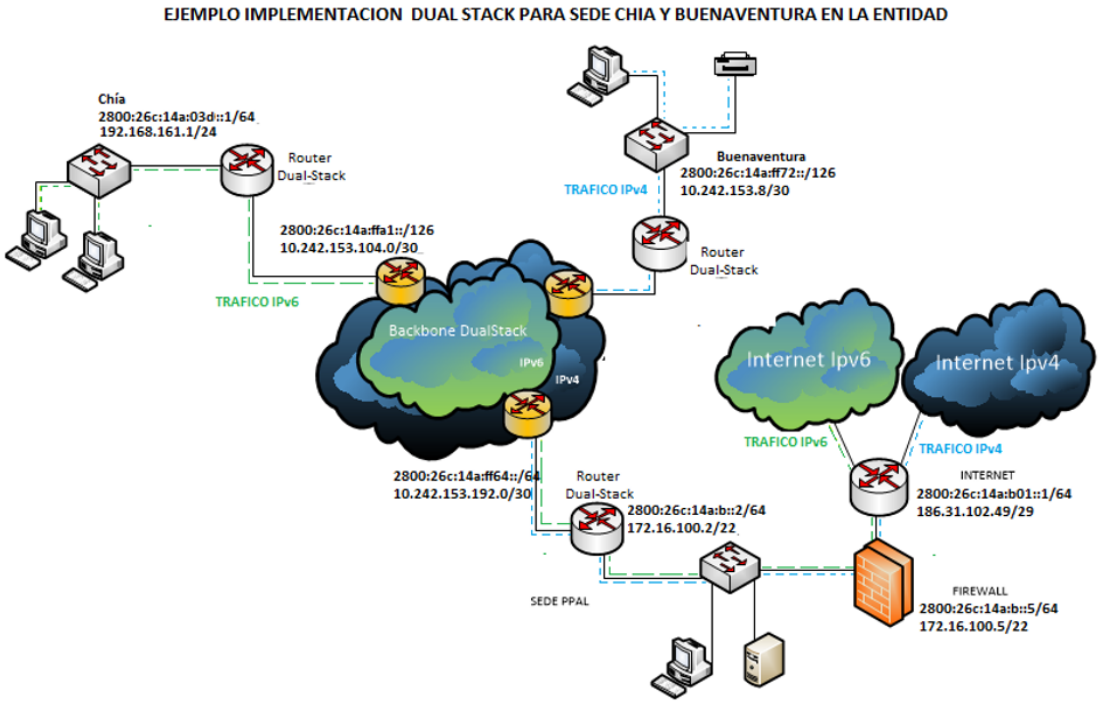
10.2.2 Aplicación de métodos de transición a IPv6 en la entidad. El 91 % de los proveedores de UM en la entidad soportan la configuración del protocolo Ipv6 así como todos los equipos de cómputo, por lo que no se tiene problema a la hora de configurar las máquinas en las sedes en doble pila para garantizar la conectividad a la nube de Internet Ipv6 y a los sitios que aún están sobre Ipv4 y con los que se debe tener conectividad desde la entidad hasta que en un futuro esos sitios sean Ipv6 nativos.

La necesidad de mantener la conectividad con sitios sobre Ipv4 hace que la transición a Ipv6 nativo no sea de un día para otro, y por eso es necesario hacer uso de un método de transición como el DUAL STACK que permita los flujos de comunicación entre los protocolos de Ipv4 e Ipv6 sin que se tengan que hacer más cambios en las maquinas del cliente hasta que el protocolo Ipv4 sea apagado y ya no se requiera tampoco está pila.

Los hosts de toda la entidad corren actualmente sistemas operativos Windows 7 y 10 que ya traen el soporte de los 2 protocolos así como también están preparados los servidores Power Edge, los routers BDCOM y los routers CISCO que también soportan ambos protocolos en sus interfaces, se preguntó al ISP ETB sobre si tiene forma de soportar Ipv6 y este confirmó que tiene la posibilidad de configurar Dual-Stack en las interfaces de sus equipos PE .

En la siguiente gráfica se muestra el ejemplo de las sedes Chía y Buenaventura en las que entonces se puede implementar la configuración dual-stack, por ser el mejor método para garantizar una transición controlada aunque consuma más recursos de máquina, es el método de transición elegido a implementar en la entidad para todas las sedes donde los proveedores de UM tienen soporte de ipv6 con el fin de garantizar la conectividad hacia sitios en los protocolos Ipv4 e Ipv6.

Figura 22. Topología para implementación de Dual-Stack en la entidad



Fuente: Los autores.

Como se mencionó anteriormente, al realizar el levantamiento de información sobre la infraestructura de la entidad también se encontró que en algunas sedes que se encuentran muy alejadas geográficamente, el proveedor de servicios de conectividad enlaza estas sedes por medio de microondas y no tiene soporte de ipv6 en varios de sus equipos intermedios, por lo que es necesario hacer uso de Túneles 6to4 como método de transición a Ipv6, estos túneles permiten el trafico Ipv6 de la sede hacia destinos Ipv6 nativos mediante la encapsulación de los paquetes Ipv6 en paquetes Ipv4 para su entrega a través de la infraestructura Ipv4 del operador, es de hacer notar que este proceso no afecta el trafico Ipv4 que actualmente cursa por el canal, aunque si requiere de cuidado en la configuración del MTU de los tuneles.

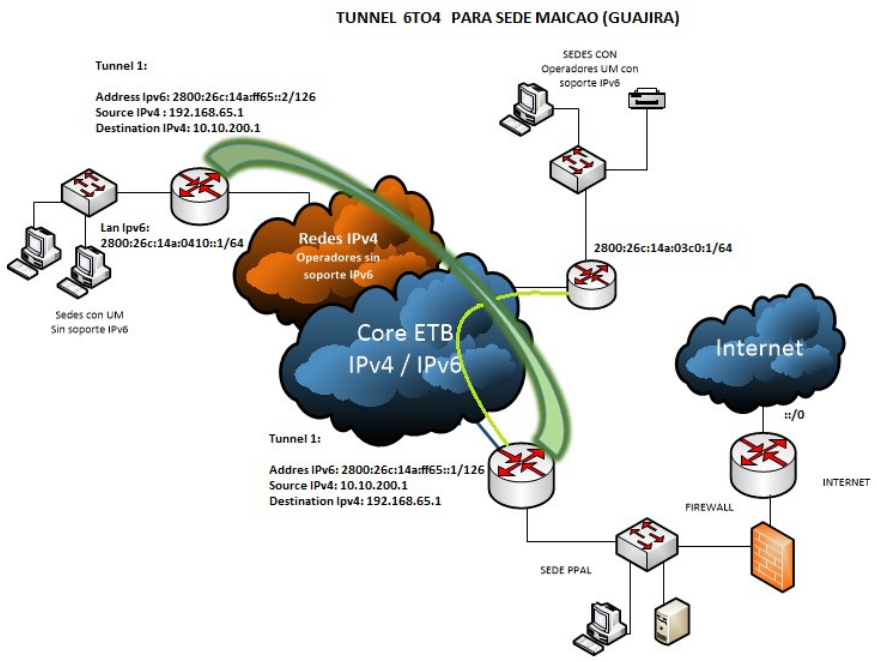
Para su implementación es necesario conocer el direccionamiento Ipv4 que se encuentra asignado de forma fija en la sede (no por DHCP) a una interface que permanezca físicamente activa y una ip Ipv4 fija generalmente asignada a una interface Loopback en el router Central de la entidad que actuará como server relay (Punto de intercambio de enrutamiento), se debe garantizar que exista conectividad entre estos dos extremos con la menor latencia posible y una MTU mínima de 1500 bytes, así se facilita el establecimiento del túnel y el tráfico de paquetes grandes en

Ipv6 ya que al enviar paquetes grandes el protocolo Ipv6 realiza una segmentación automática del paquete grande en varios paquetes de tamaño 1500 bytes.

En el caso particular de la entidad todas las sedes remotas tienen routers marca BDCOM BSR2800-24E que tienen una jerarquía y configuración similar a los equipos CISCO que son routers más reconocidos comercialmente, mientras que la sede central de la entidad cuenta con un router CISCO ISR 4451-X podemos entonces decir que el formato de la configuración para todos los túneles en las sedes donde el operador de UM no soporta el protocolo Ipv6 es la misma, solo cambia los direccionamientos Ipv6 utilizados por los asignados a cada sede en la etapa anterior, el prefijo Ipv6 /126 utilizado como ip address en la configuración del túnel se toma también de las direcciones reservadas anteriormente con el formato Interwan que estan relacionadas en el Anexo B.

En la siguiente grafica se puede ver un ejemplo de cómo se implementará el método de transición de Ipv4 a Ipv6 en la sede de Maicao en la Guajira mediante túnel 6to4 ya que allí actualmente el proveedor de UM no soporta Ipv6. Aquí se puede apreciar que el trafico Ipv6 de la sede remota para poder salir a Internet o poder conectarse a otra sede con Ipv6 como Fusagasugá debe encapsular el trafico dentro del túnel para que llegue por Ipv4 a la sede central y desde allí ser redireccionado hacia Internet por medio del Firewall , o al Core del ISP ETB si el trafico va a otra sede que si tiene UM con soporte Ipv6 o por otro túnel si es necesario alcanzar otra sede sin soporte de Ipv6 en la UM.

Figura 23. Topología para implementación de Túnel 6to4 en la entidad.

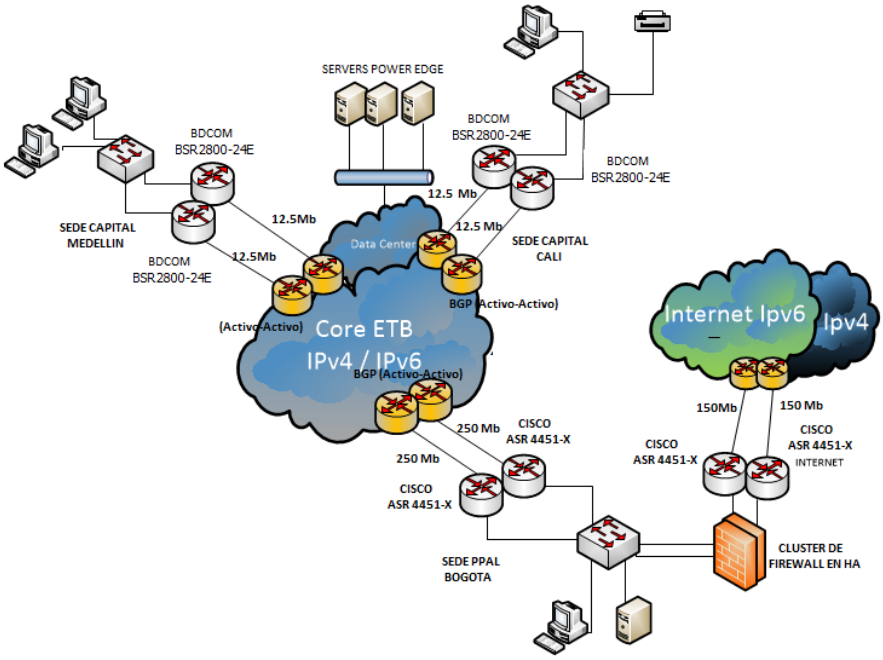


Fuente: Los autores.

10.2.3 Redundancia en sedes capitales para mejorar la disponibilidad. En la red actual solo la sede principal cuenta con equipos de respaldo como router Backup en configuración Activo-Pasivo y la configuración de alta disponibilidad HA en el firewall realizada por el administrador del mismo, según la información proporcionada por el personal de TI de la entidad estos equipos han protegido ya en varias oportunidades el punto principal, pero también indica que en los últimos años se ha dado autonomía a las sedes capitales para administrar a un conjunto de inspecciones, por lo que es muy frecuente que varias sedes inspecciones se comuniquen con una sede capital para consultar o compartir información y estos servicios si se han visto interrumpidos por la pérdida de conectividad en las ultimas millas de las sedes capitales frecuentemente por obras en el casco urbano que han tenido un tiempo de reparación considerable afectando el desarrollo de las actividades de esta región.

Se sugiere a la entidad para mejorar la disponibilidad de estos enlaces contratar con un proveedor de servicios diferentes una última milla para implementar un canal backup en cada sede capital que se configure en estado Activo-Activo y que con el fin de aprovechar los 2 canales de cada sede capital sin incrementar exageradamente el costo de implementación se reparta el BW de banda actual entre estos 2 enlaces, evitando así el pago de un canal ocioso logrando que en el momento que se presente una falla el canal sobreviviente asuma la carga total del tráfico aunque con la mitad del ancho de banda normal mientras se repara la falla, la configuración sugerida puede verse en la siguiente gráfica :

Figura 24. Topología propuesta para mejorar disponibilidad en enlaces de sede capitales



Fuente: Los autores.

Los operadores de servicios en Colombia tienen SLAs (Acuerdos de Nivel de servicio) establecidos en los que garantizan un nivel de disponibilidad de la última milla ya definida por la tecnología utilizada o por la cantidad de equipos y fuentes de poder utilizadas en el canal de datos, por ejemplo el ISP ETB para una configuración con 2 ultimas millas y con 2 equipos routers ofrece una disponibilidad de 99.9 que sería mayor a la que actualmente tiene la red en las ultimas millas de las sedes capitales, para disponibilidades mucho mayores la entidad debería incurrir en costos muy altos.

10.2.4 Servidor DHCP centralizado con gestión. La implementación del protocolo Ipv6 en la entidad permitirá la conexión de una gran cantidad de máquinas a diferencia de su predecesor Ipv4, esta característica da paso a la adopción de muchas tecnologías de IoT y a futuras modificaciones en las normas de las entidades que ya hoy se vienen dando que permitan la conexión a la red corporativa de diferentes tipos de dispositivos como celulares o tablets que ahora hacen parte de las herramientas de trabajo. Actualmente se tiene servicios de DHCP en algunas sedes de la entidad con los servidores configurados sobre los routers, por lo que se vuelve tedioso la modificación o visualización de estos registros ya que se debe ingresar uno por uno para poder llevar un control manual del direccionamiento, en la siguiente grafica se ve la configuración típica del servidor DHCP en una sede.

Figura 25. Ejemplo de servidor DHCP configurado actualmente sobre el router

```
Router_Entidad_Iba#
!
ip dhcp excluded-address 172.16.29.1 172.16.29.10
!
ip dhcp pool LAN_1
 network 172.16.29.0 255.255.255.0
 default-router 172.16.29.1
 dns-server 200.75.51.132 200.75.51.133
 lease 0 4
!
interface GigabitEthernet0/5
 description CONEXION LAN
 ip address 172.16.29.1 255.255.255.0
 ip virtual-reassembly in
 duplex auto
 speed auto
```

Fuente: Los autores.

La administración de este direccionamiento es complicado en una entidad con una proyección de crecimiento importante, por lo que se recomienda implementar una plataforma de gestión de direccionamiento aprovechando el hecho de que los servidores que se tienen actualmente corren un sistema operativo de Microsoft con una versión superior a Windows Server 2008 se sugiere adquirir la característica de IPAM (Internet Protocol Address Management) o adquirir una solución de otra compañía como Solarwinds que permita instalar sobre los servidores ya existentes y que además de las características de gestión de direccionamiento ofrece herramientas de gestión y monitoreo de la red con múltiples servicios de alarmas y

control, la funcionalidad IPAM unificaría la gestión de hosts, servidores de DNS y DHCP mediante la recolección de información de DNS y DHCP con políticas de grupo permitiendo Visualizar, Gestionar y Configurar el espacio de direccionamiento IP de una forma centralizada.

10.2.5 Gestión y Monitoreo de la red. Debido al tamaño y complejidad de la infraestructura de red que opera en la entidad, se hace necesario la implementación de un sistema de gestión y monitoreo que permita la administración y control de los elementos que la conforman, de esta manera poder supervisar y mantener una red eficiente y con alta disponibilidad, ayudando a los ingenieros encargados de administrar la infraestructura de TI de la entidad a ejecutar un conjunto de funciones necesarias para planificar, asignar, implementar, controlar, coordinar y monitorear sus recursos de red.

Con la implementación de un sistema de gestión y monitoreo se garantiza un aumento en el rendimiento de la red, ya que facilita la identificación con claridad de todos sus parámetros permitiendo un diagnóstico preciso, y de esta manera permitir la detección temprana de posibles fallas y corregir las que puedan afectar su normal funcionamiento, garantizando una alta disponibilidad y el continuo acceso por parte de los usuarios. Así mismo se debe solicitar al ISP ETB que incluya en las configuraciones de los routers el envío de copias de seguridad periódicas mediante la sincronización con servidores actualizados NTP (Network Time Protocol) para tener la garantía de un respaldo de los datos sensibles de la organización, evitando posibles pérdidas de información por fallos en los servidores de red o por eventuales amenazas internas o externas a las que esta esté expuesta.

La centralización de la gestión de red en la entidad permitirá tener un mayor control y vigilancia de todos los dispositivos que la integran brindando un mejor panorama de la infraestructura que la conforma y de esta forma poder dar una respuesta más efectiva ante cualquier evento, al implementar el sistema de gestión en la red de la entidad es necesario considerar los de mayor aceptación y uso como lo es el modelo FACPS (Fault,Configuraion,Accounting,Performance,Security) que ofrece una solución automatizada y altamente escalable con funcionalidad para detectar fallas, realizar estadísticas y configuraciones llegando hasta permitir la detección automática de conexión de dispositivos en la red.

10.3 SIMULACIÓN COMO HERRAMIENTA EN EL DISEÑO

Para realizar la simulación se optó por utilizar el simulador Riverbed Modeler Academic Edition 17.5 la cual es la versión actual del programa de simulación opnet modeler ya que este fue adquirido por la compañía Riverbed, la cual tiene las siguientes limitantes generales para su versión educativa: limitado a 50 millones de eventos, 80 host y un máximo de 20 nodos “los nodos son puntos de enrutamiento” a pesar de estas limitaciones fue considerado idóneo para el desarrollo del proyecto por su diseño donde no se tuvo en cuenta la configuración en los equipos, pues el enfoque de esta herramienta de simulación está enfocado más al diseño de redes eliminando la necesidad de tener conocimiento específico en cada una de las maquinas a simular y la falta de un entorno real donde se pueda observar tráfico.

Inicialmente se presentarán los elementos comunes en todas las topologías a simular, se partirá de la parametrización extraída del cliente y definiendo tres tipos de escenarios a simular donde se aplicaron configuraciones en ipv4 representando las conexiones existentes, configuraciones en ipv6 nativo y finalmente una prueba con túnel 6 to 4, luego se compararon los resultados de las simulaciones para obtener resultados. El programa ofrece un espacio de simulación grafico donde se deben ubicar los equipos a simular, como primer parámetro se debe generar una topología en la cual trabajar, observando la librería de objetos tendremos acuerdos comerciales para simular equipos de grandes marcas, pero para efectos prácticos se optó por utilizar elementos genéricos para no atar la simulación a algún tipo de fabricante ofreciendo mayor flexibilidad al diseño y centrándonos en el objetivo de las pruebas y es la migración a ipv6.

Figura 26. Elementos seleccionados a utilizar en las topologías de simulación.

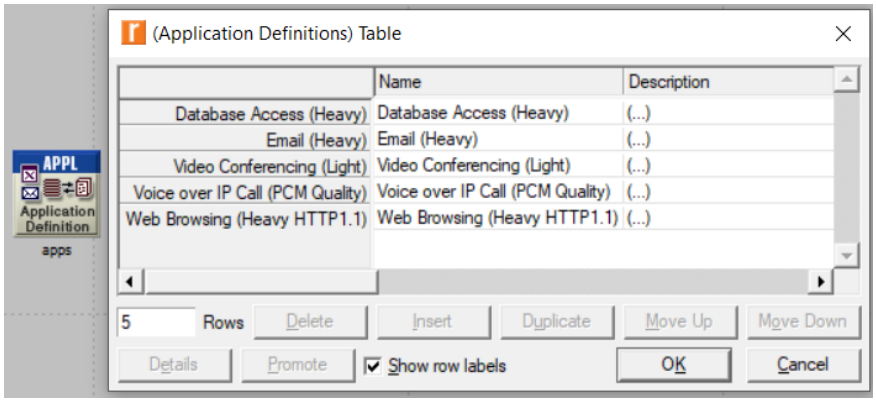
Fuente: Software Riverbed

Durante la creación de los escenarios de prueba se utilizaron los elementos de la figura anterior, no se observa la necesidad de simular otros dispositivos ya que el objetivo es observar el comportamiento de las maquinas al ser migradas a ipv6 y luego partir de estos resultados para obtener unas conclusiones que validen lo

expresado en el documento, paso a seguir se generó un conjunto de aplicaciones, estas aplicaciones no pueden se asignadas directamente en las maquinas es por esta razón que son agrupadas en perfiles los cuales son lo que realmente serán asignados a los terminales, esta aplicaciones son las encargadas de generarnos el tráfico desde y hacia las maquinas, teniendo esto claro en las topologías propuestas se diseñaron para que las aplicaciones tengan consumo en los servidores de cada una de estas siempre teniendo la flexibilidad de manipular los perfiles y poder reasignar la forma en la que están distribuidas las aplicaciones en la maquinas.

Buscando que los resultados obtenidos sean homogéneos se definieron perfiles estándar para todos los escenarios los cuales serán presentados a continuación.

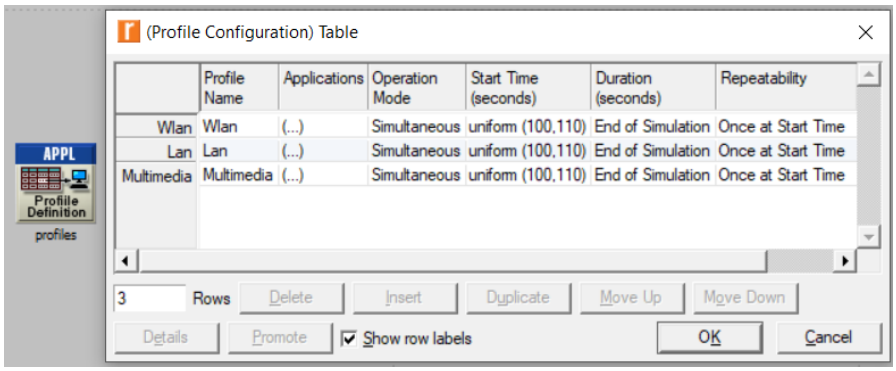
Figura 27. presentación de aplicaciones



Fuente: Software Riverbed

Al tener las aplicaciones ya generadas se procedió a agruparlas en perfiles los cuales fueron utilizados en cada una de las maquinas simuladas.

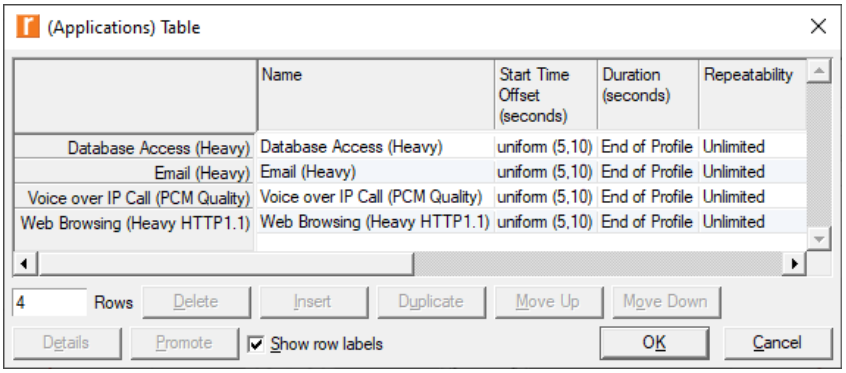
Figura 28. Perfiles estándar para todos los escenarios



Fuente: Software Riverbed

Un dato para destacar es que los perfiles corrieron todas las aplicaciones de forma simultánea, con la finalidad de que las simulaciones nos entregaran resultados constantes.

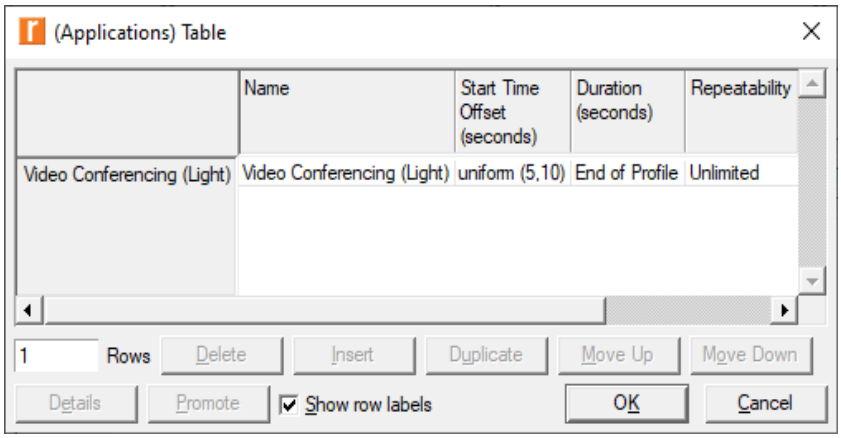
Figura 29. Perfil generado Lan y Wlan



Fuente: Software Riverbed

Las maquinas Wlan y lan comparten el grupo de aplicaciones descritas en la imagen, con esto se garantizó que tanto los equipos cableados como los inalámbricos gozaran de acceso a las mismas aplicaciones sin discriminar su tipo de conexión, que es lo que se podría encontrar en cualquier entorno de oficina.

Figura 30. Perfil multimedia

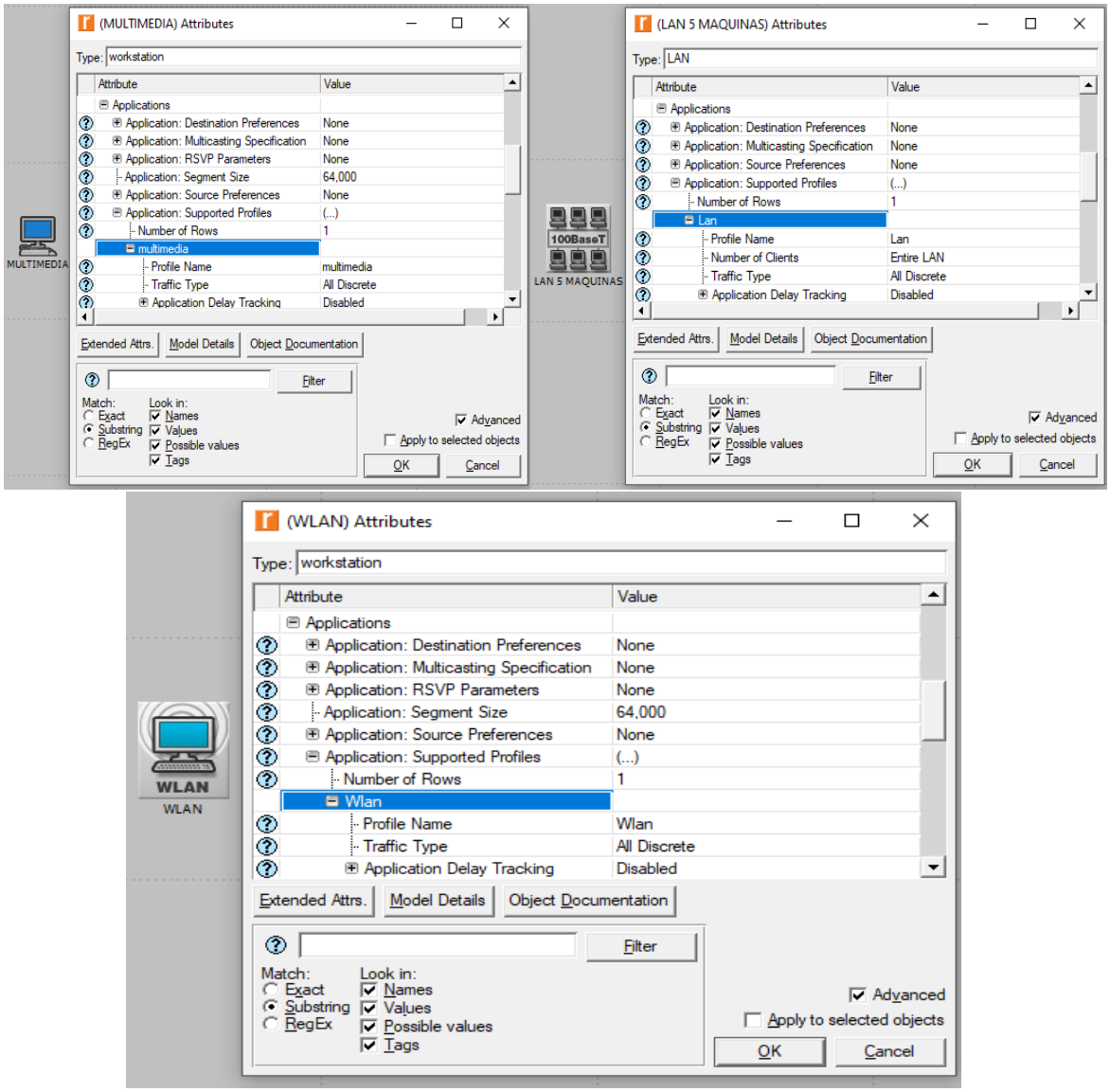


Fuente: Software Riverbed

Para el equipo multimedia se creó un perfil independiente donde se manejará video conferencia, la finalidad de este tipo de equipo fue simular la disposición de una maquina de video conferencias que día a día es más recurrente en la oficinas.

En las siguientes imágenes se presentaran los apartados donde de configuraron los perfiles a las maquinas de las simulaciones.

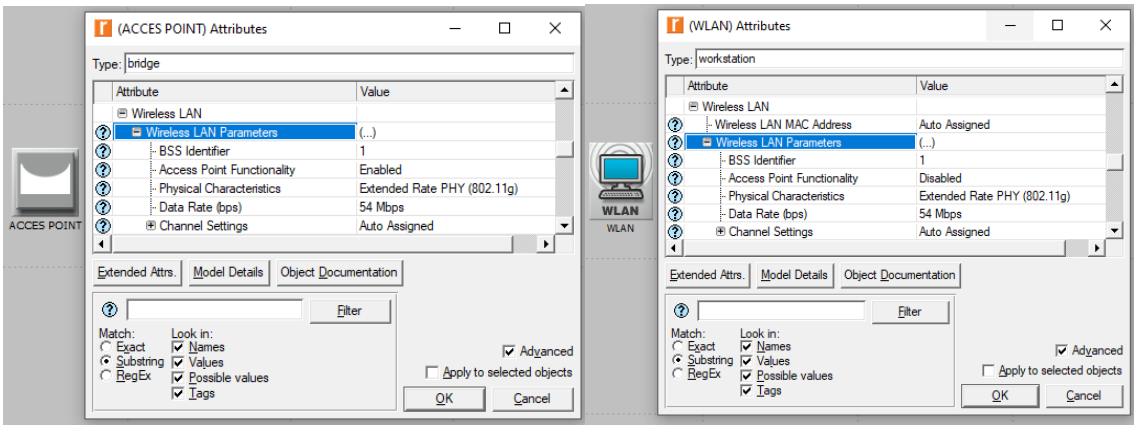
Figura 31. Configuración de perfil para maquina multimedia y terminales “consumidor”



Fuente: Software Riverbed

Para las maquinas inalámbricas se realizó un paso adicional y fue realizar el enlace inalámbrico con estándar 802.11G a 54MB entre el acces point tipo bridge y las maquinas inalámbricas, se menciona el tipo de ap ya que el simulador también cuenta con ap con enrutamiento, se utilizó esta velocidad para evitar cuellos de botella con las maquinas conectadas y no se utilizó ap con enrutamiento ya que no es necesario, el cliente promedio no utiliza enrutamiento en sus aps.

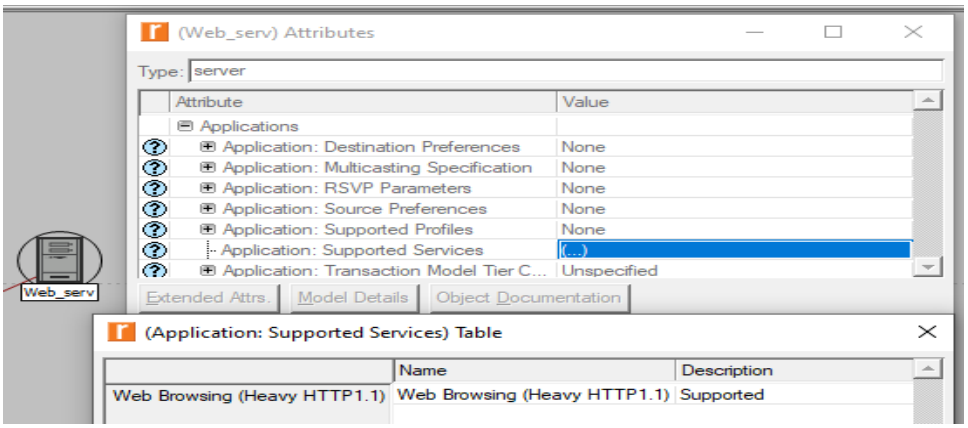
Figura 32. Configuración Bss Id y velocidad sobre ap y cliente



Fuente: Software Riverbed

Luego de la asignación de los perfiles se procedió a la asignación de los servicios sobre los servidores, como ejemplo se realizó una captura de asignación de recurso web en el webserver.

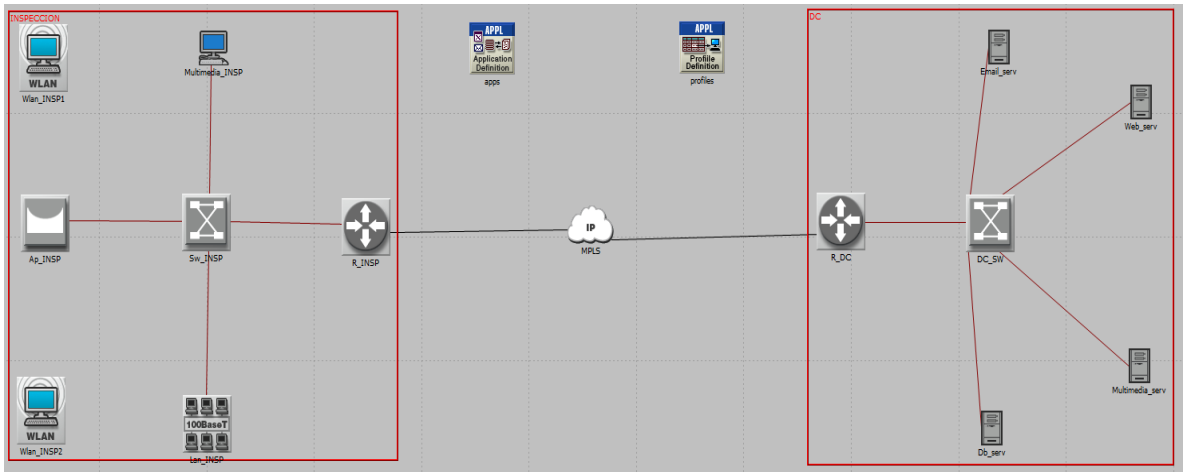
Figura 33. Configuración de perfil para servidor web “fuente”



Fuente: Software Riverbed

Estos pasos fueron ejecutados en todas las máquinas y en todos los escenarios como preparación para la simulación, en las topologías todas las conexiones wan se realizaron con enlaces PPP_DS3 “45MB” debido al tipo de modelos de router presentes en el programa, entre routers y switches las conexiones fueron de 100MB, enlaces ethernet 10MB hacia las máquinas y conexiones con estándar wifi 802.11G a 54Mbps, este tipo de enlaces nos garantizaron que no tendríamos problemas de cuello de botella a nivel lan. A continuación, se ilustrarán las 3 topologías simuladas que fueron usadas para la realización del trabajo.

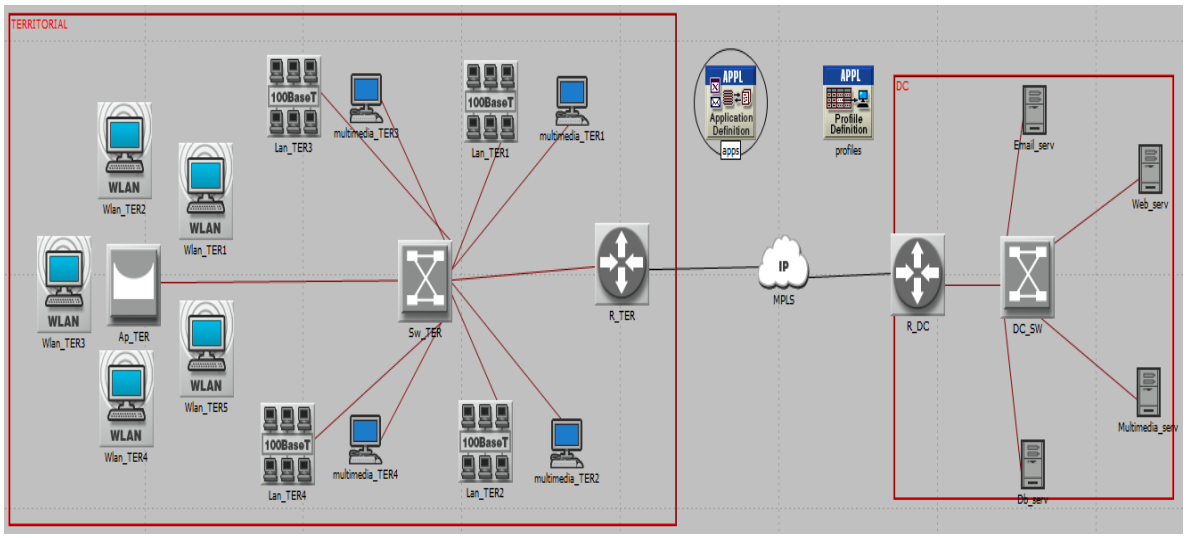
Figura 34. Topología simulada de una sede tipo inspección.



Fuente: Software Riverbed

Para este tipo de sedes se dimensiono solo un grupo de trabajo lan de 5 máquinas con su respectiva maquina multimedia y dos máquinas conectadas de manera inalámbrica a través de un ap. Para un total de 8 máquinas, estas sedes se caracterizan por tener un tamaño reducido ya que estarían en sitios remotos.

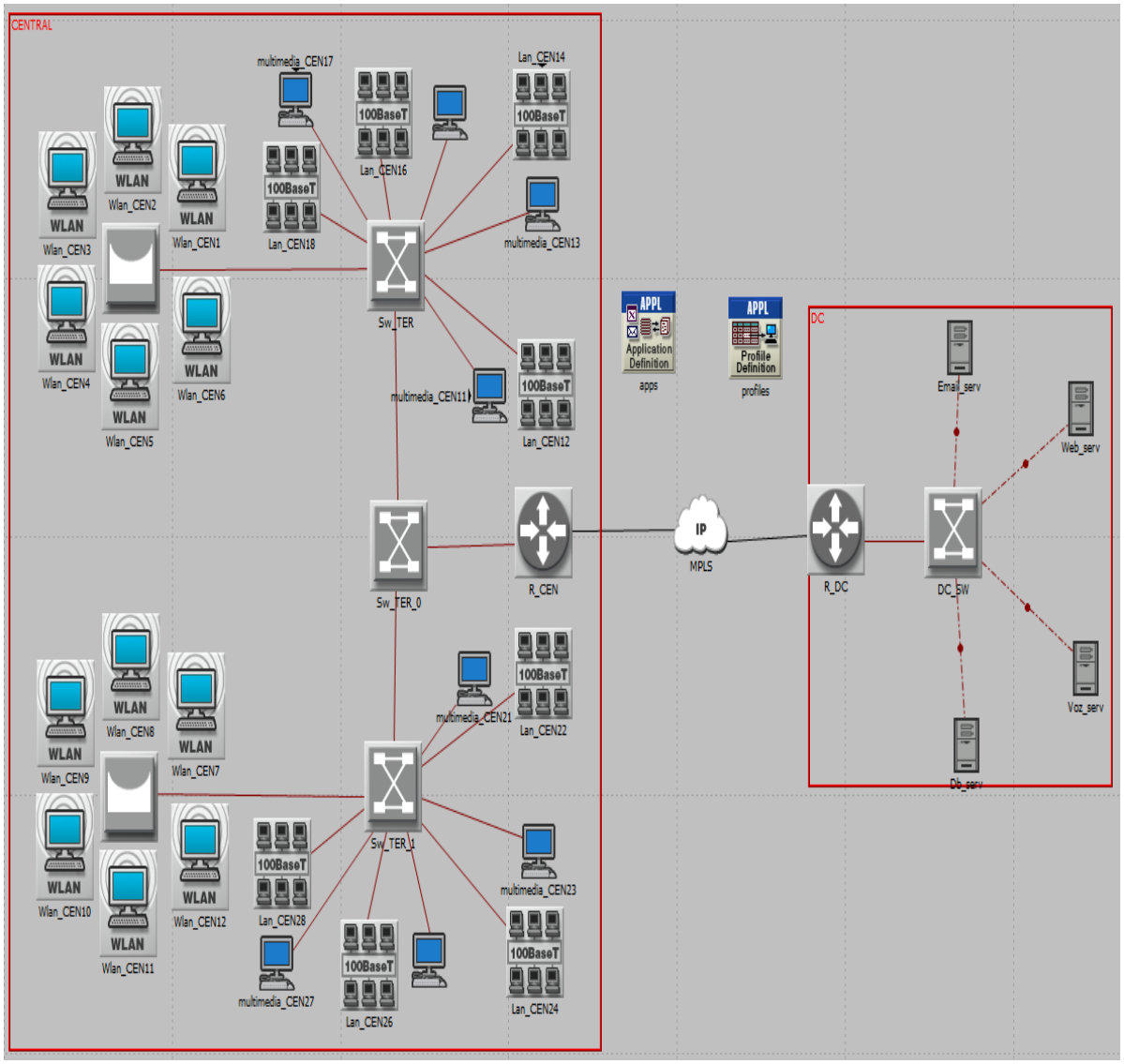
Figura 35. Topología simulada de una sede tipo territorial.



Fuente: Software Riverbed

Para este tipo de sedes se dimensiono 5 grupos de trabajo donde están compuestos por 4 grupos lan de 5 máquinas cada uno con una maquina multimedia y un punto de acceso con 5 clientes inalámbricos. Para un total de 29 máquinas. Esta topología representa sedes donde la entidad tiene un tamaño considerable.

Figura 36. Topología simulada de una sede tipo central

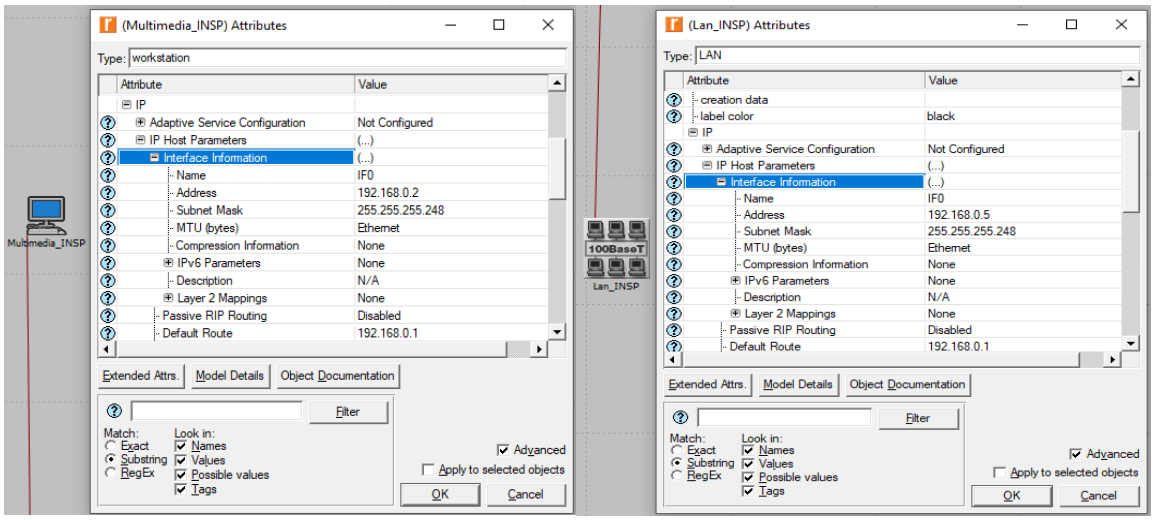


Fuente: Software Riverbed

Para este tipo de sedes se dimensiono 10 grupos de trabajo donde están compuestos por 8 grupos lan de 5 máquinas cada uno con una maquina multimedia y dos puntos de acceso con 6 clientes inalámbricos cada uno, se agrega un SW central y los grupos se dividen a la mitad para representar el equivalente a una oficina de dos plantas contando con un total de 60 máquinas. .
Esta es en nuestras simulaciones la que cuenta con un mayor número de máquinas, debido a su tamaño se sobre entiende que no es necesariamente el punto central sino representa la conectividad de una sede de considerable tamaño por donde pasan los tramites de una regio en particular.

10.3.1 Simulación de conectividad Ipv4. En las próximas graficas se muestra el procedimiento de configuración por elemento en el software Riverbed, para realizar la simulación del escenario con el protocolo Ipv4.

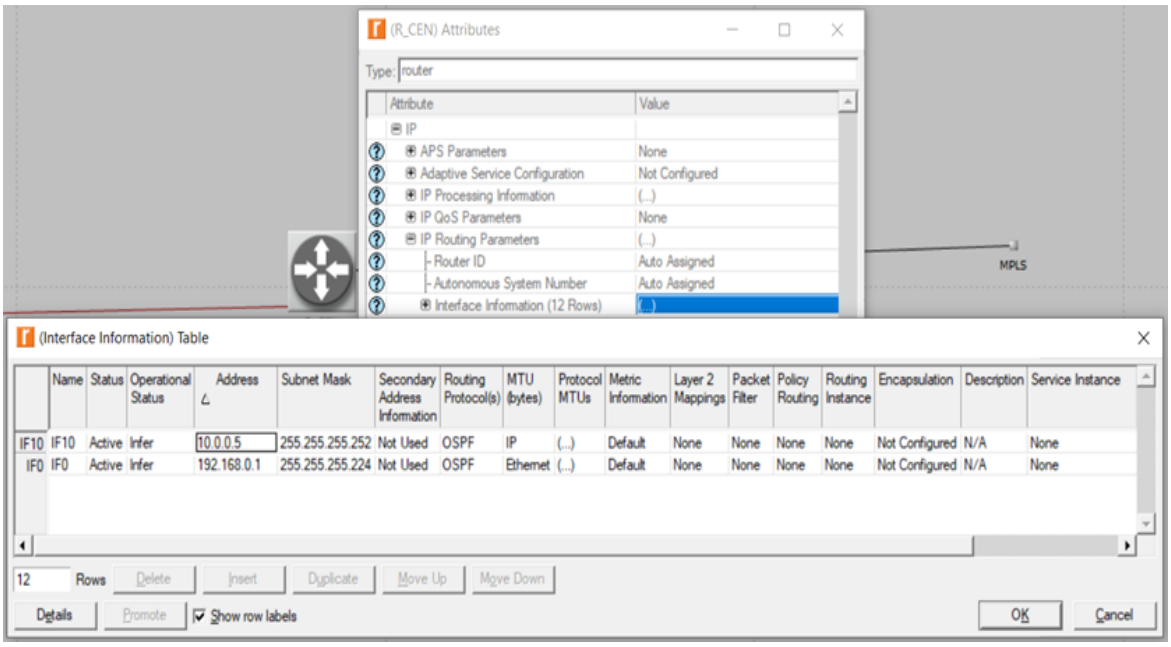
Figura 37. Configuración de direccionamiento ipv4 en máquinas terminales



Fuente: Software Riverbed

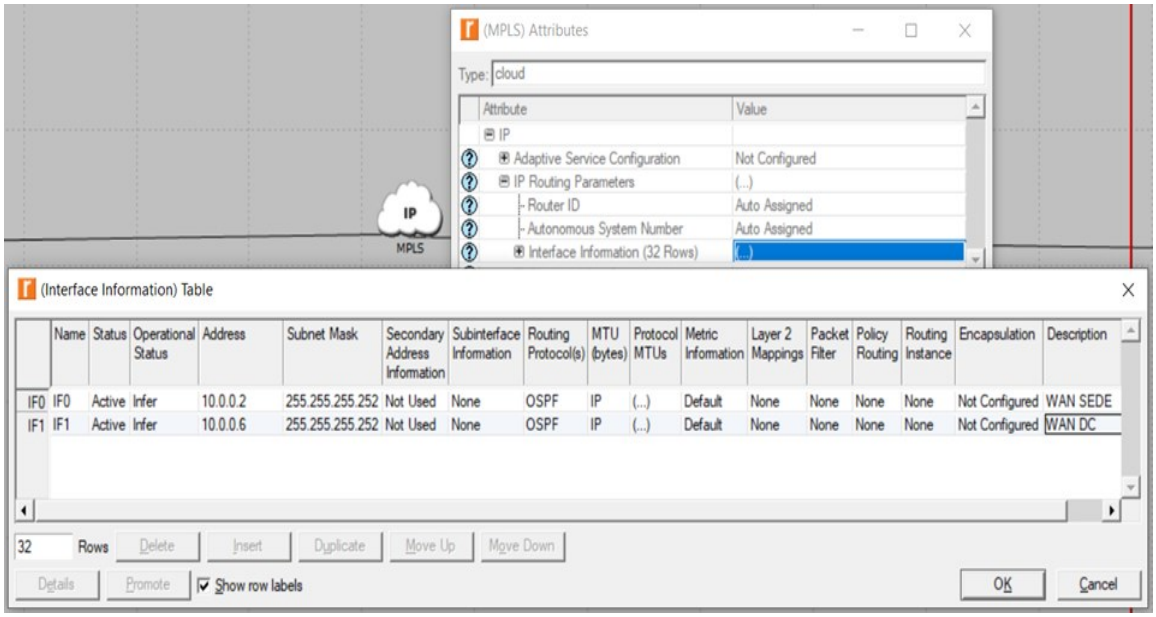
En los siguientes gráficos se realizó el mismo proceso, pero como se observa se adicionan las tablas de enrutamiento.

Figura 38. Configuración de direccionamiento ipv4 router sede



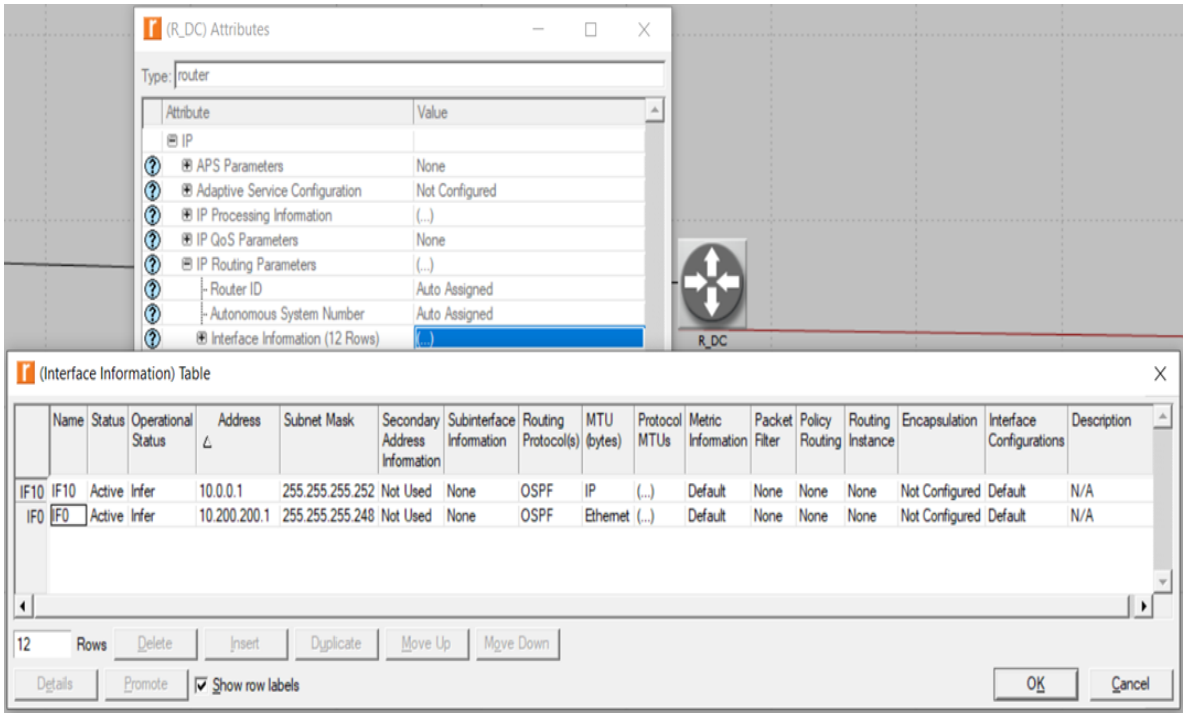
Fuente: Software Riverbed

Figura 39. Muestra de configuración en mpls



Fuente: Software Riverbed

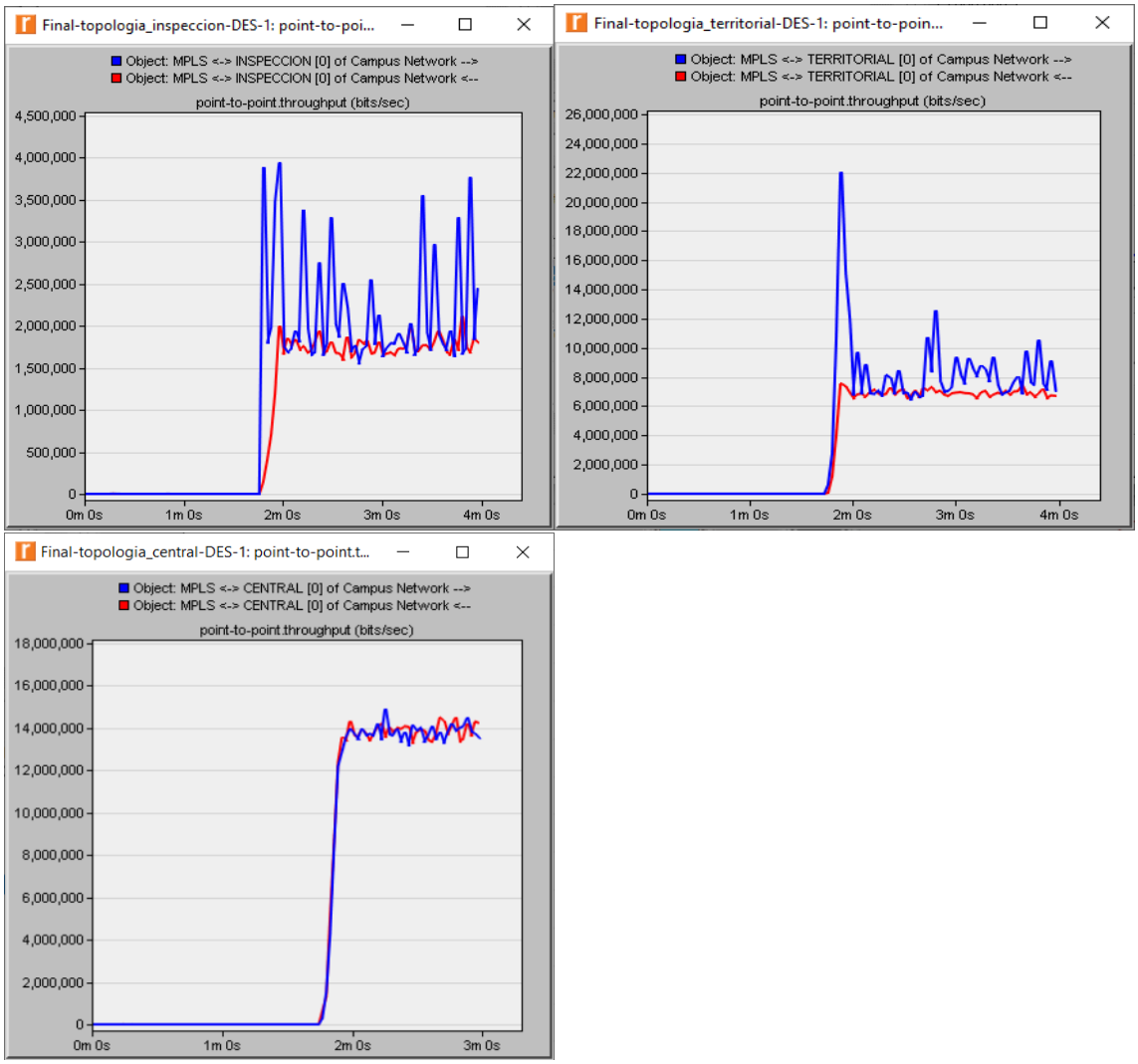
Figura 40. Configuración de direccionamiento ipv4 router datacenter



Fuente: Software Riverbed

En los siguientes gráficos se observan los resultados del Throughput generados en la simulación de Ipv4 por cada una de las topologías expuestas anteriormente.

Figura 41. Resultado de consumo Ipv4 para Territoriales, Inspecciones y punto Central

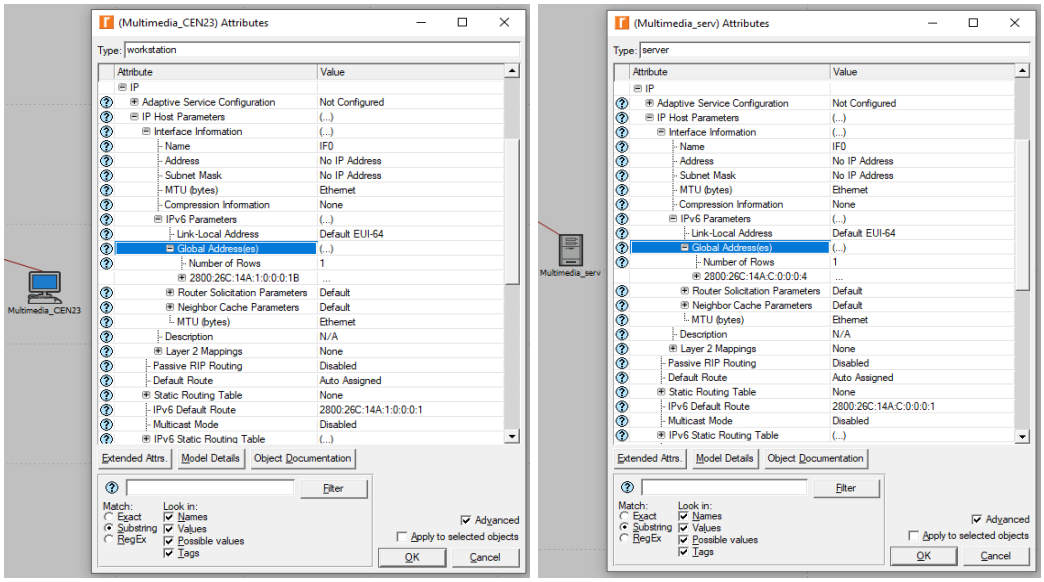


Fuente: Los autores.

Como se observa en las gráficas el trafico Ipv4 para una sede tipo Inspección es en promedio de 2.1Mb/s, en una sede Territorial hay un promedio de 7.5 Mb/s de trafico Ipv4, mientras que la sede central muestra un tráfico generado de 14 Mb/s independientemente del tráfico que le llegaría de otras sedes. Esta simulación de los escenarios bajo el protocolo Ipv4 es necesaria para tener una base de comparación y contrastar más adelante los resultados generados en los escenarios de Ipv6 nativo y de Ipv6 a través de un tunnel 6 to 4.

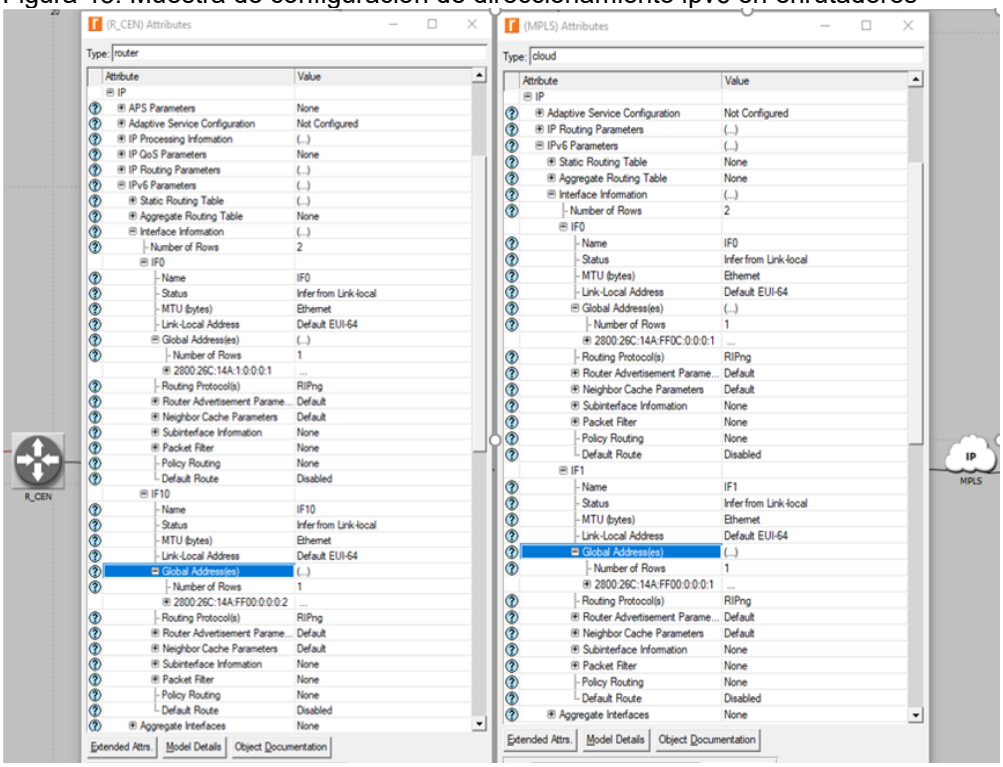
10.3.2 Simulación de conectividad Ipv6. En las próximas graficas se muestra el procedimiento de configuración por elemento en simulador de red, para realizar la simulación del escenario con el protocolo Ipv6 nativo.

Figura 42. Muestra de configuración de direccionamiento ipv6 en equipos terminales



Fuente: Software Riverbed.

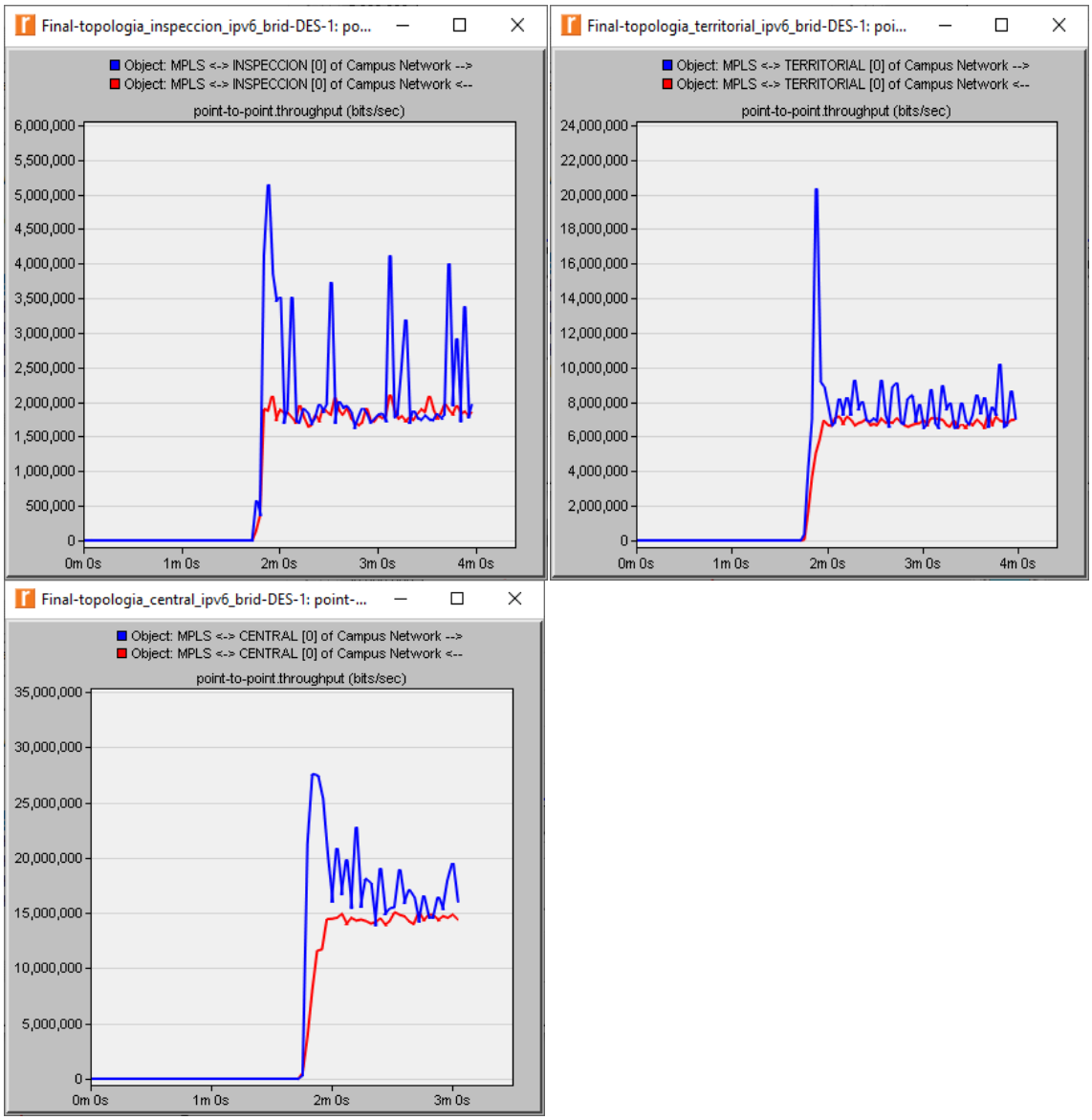
Figura 43. Muestra de configuración de direccionamiento ipv6 en enrutadores



Fuente: Software Riverbed.

En las siguientes figuras se observan los resultados del Throughput generados en la simulación de Ipv6 por cada una de las topologías expuestas anteriormente.

Figura 44. Consumo inspección en ipv6 en las sedes Inspecciones, Territoriales y central



Fuente: Los autores.

Al simular la misma topología anterior pero ahora con el direccionamiento Ipv6 nativo se observó que la conectividad funcionó sin ningún problema y que el Throughput tuvo un comportamiento muy similar, esta prueba se realizó con Ipv6 nativo ya que el protocolo Ipv6 tiene una pila independiente al del protocolo Ipv4 y es la base del modelo dual-stack, retransmitir el paquete por el next hop que tenga el mismo protocolo del paquete de entrada, prefiriendo siempre la tabla de enrutamiento de Ipv6 si está disponible.

10.3.3 Simulación de conectividad Ipv6 por medio de Túnel sobre IPv4. A continuación, se realiza la prueba de configuración para el entorno con túnel 6 to 4, para hacerlo más sencillo se mostrará solo la configuración de los enrutadores y la nube MPLS, en el caso de los enrutadores cambia la configuración inicialmente mostraremos las interfaces wan en ipv4 y al final la configuración del túnel 6 to 4 con sus respectivas rutas.

Figura 45. Configuración Ipv4 Wan

(Interface Information) Table

	Name	Status	Operational Status	Address	Subnet Mask	Secondary Address Information	Subinterface Information	Routing Protocol(s)	MTU (bytes)	Protocol MTUs	Metric Information	Packet Filter	Policy Routing	Routing Instance	Encapsulation	Interface Configurations	Description
IF10	IF10	Active	Infer	10.0.0.6	255.255.255.252	Not Used	None	OSPF	IP	(...)	Default	None	None	None	Not Configured	Default	WAN

12 Rows Delete Insert Duplicate Move Up Move Down

Details Promote Show row labels OK Cancel

(Interface Information) Table

	Name	Status	Operational Status	Address	Subnet Mask	Secondary Address Information	Subinterface Information	Routing Protocol(s)	MTU (bytes)	Protocol MTUs	Metric Information	Packet Filter	Policy Routing	Routing Instance	Encapsulation	VRF Sitemap	Interface Configurations	Description
IF10	IF10	Active	Infer	10.0.0.2	255.255.255.252	Not Used	None	OSPF	IP	(...)	Default	None	None	None	Not Configured	None	Default	WAN

12 Rows Delete Insert Duplicate Move Up Move Down

Details Promote Show row labels OK Cancel

(Interface Information) Table

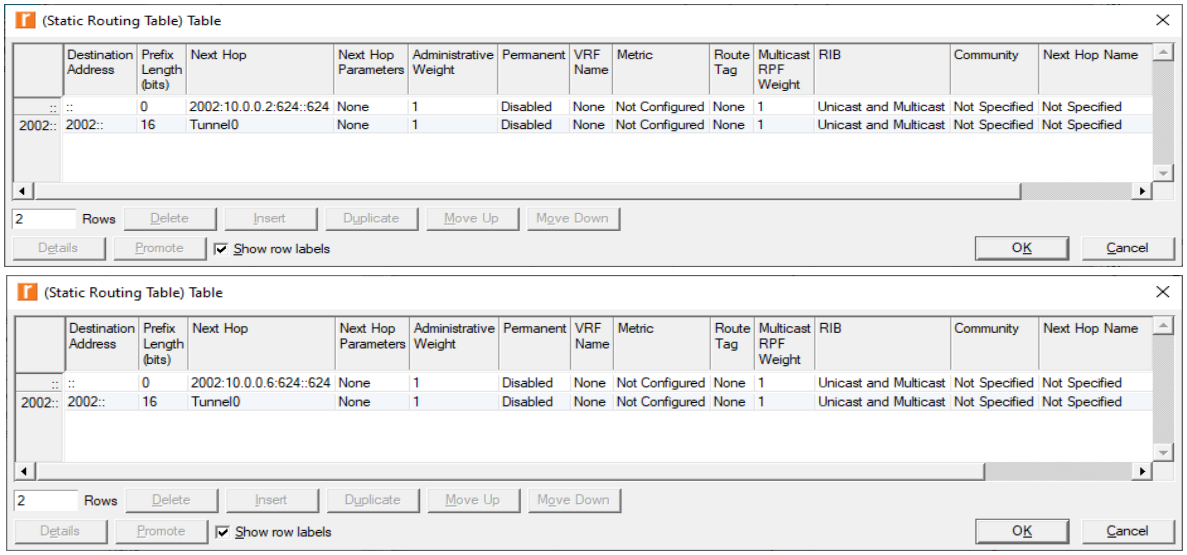
	Name	Status	Operational Status	Address	Subnet Mask	Secondary Address Information	Subinterface Information	Routing Protocol(s)	MTU (bytes)	Protocol MTUs	Metric Information	Packet Filter	Policy Routing	Routing Instance	Encapsulation	VRF Sitemap	Interface Configurations	Description
IF0	IF0	Active	Infer	10.0.0.1	255.255.255.252	Not Used	None	OSPF	IP	(...)	Default	None	None	None	Not Configured	None	Default	WAN_DC
IF1	IF1	Active	Infer	10.0.0.5	255.255.255.252	Not Used	None	OSPF	IP	(...)	Default	None	None	None	Not Configured	None	Default	WAN_SEDE

32 Rows Delete Insert Duplicate Move Up Move Down

Details Promote Show row labels OK Cancel

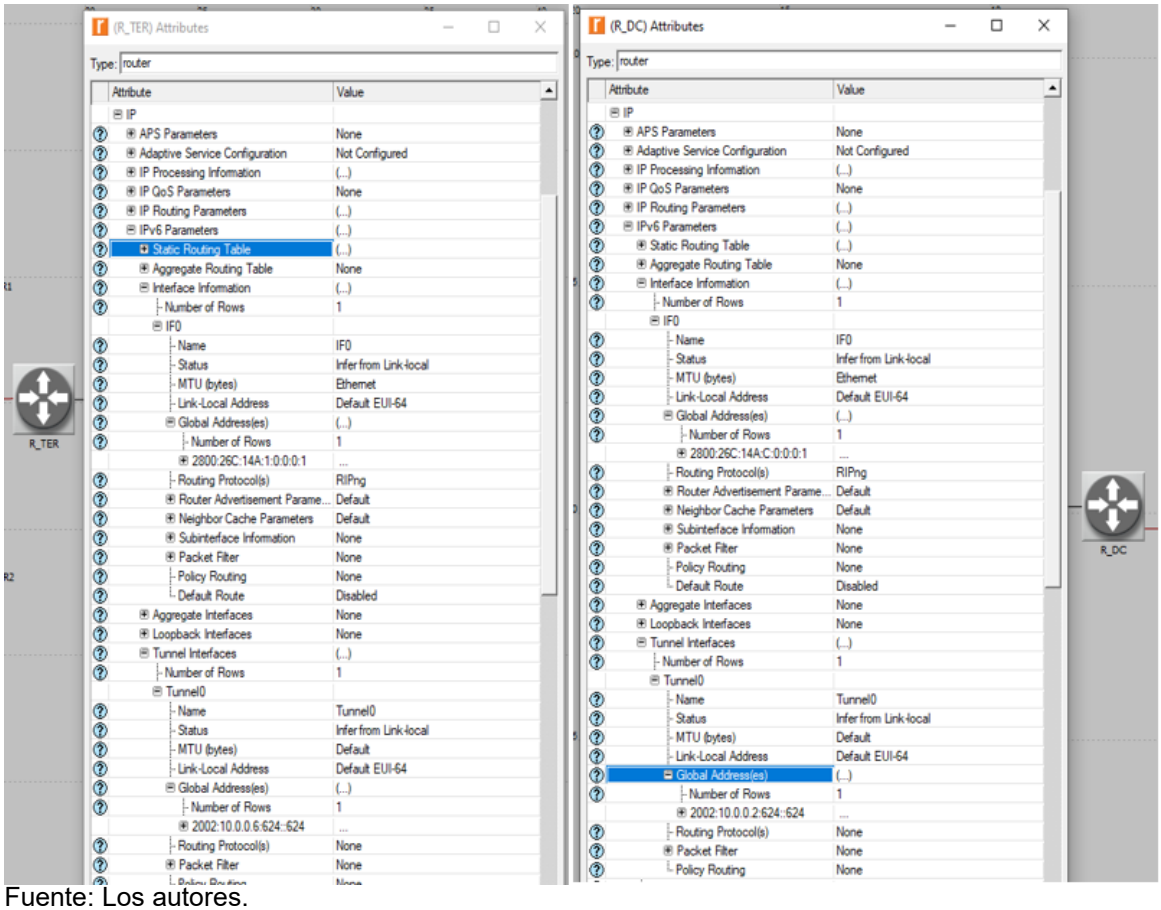
Fuente: Los autores.

Figura 46. Configuración de extremos Ipv4 del Tunnel



Fuente: Los autores.

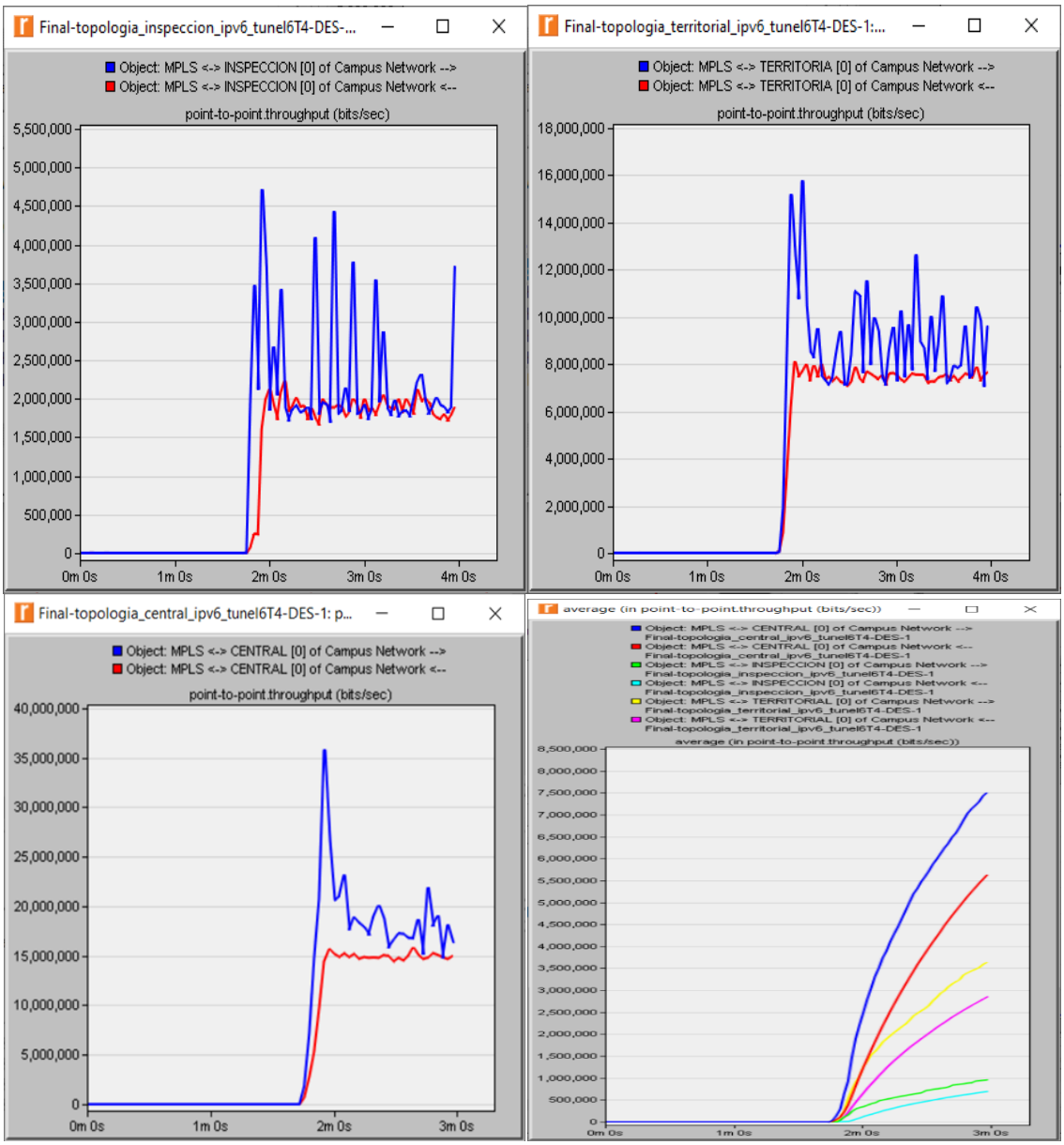
Figura 47. Configuración de Interfaces en los enrutadores en Ipv6



Fuente: Los autores.

En las siguientes figuras se observan los resultados del Throughput generados en la simulación de Ipv6 por cada una de las topologías expuestas anteriormente.

Figura 48. Gráfico de consumo túnel 6 to 4 en Inspecciones y Territoriales

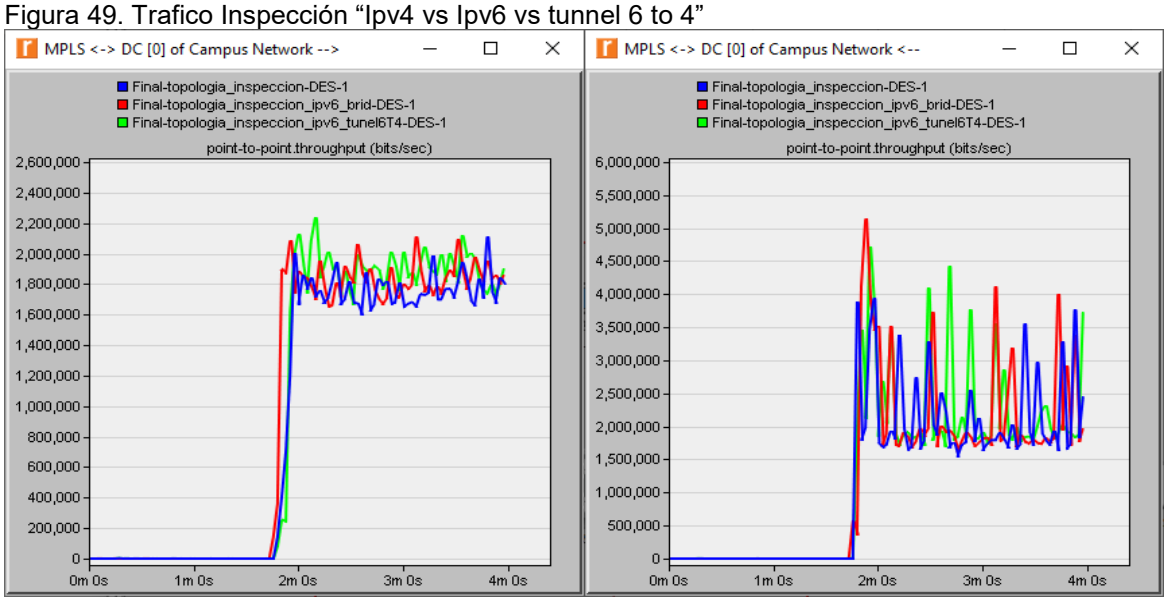


Fuente: Los autores

En las gráficas que resultan de la simulación utilizando un tunnel 6 to 4 para permitir la conectividad Ipv6 sobre un enlace Ipv4, se observó que hay un leve incremento en el trafico esto debido a que todo el tráfico IPv6 va empaquetado en la carga útil de los paquetes IPv4, para ello los paquetes grandes de Ipv6 son fraccionados en el MTU disponible del tunnel que es generalmente de 1460 bytes.

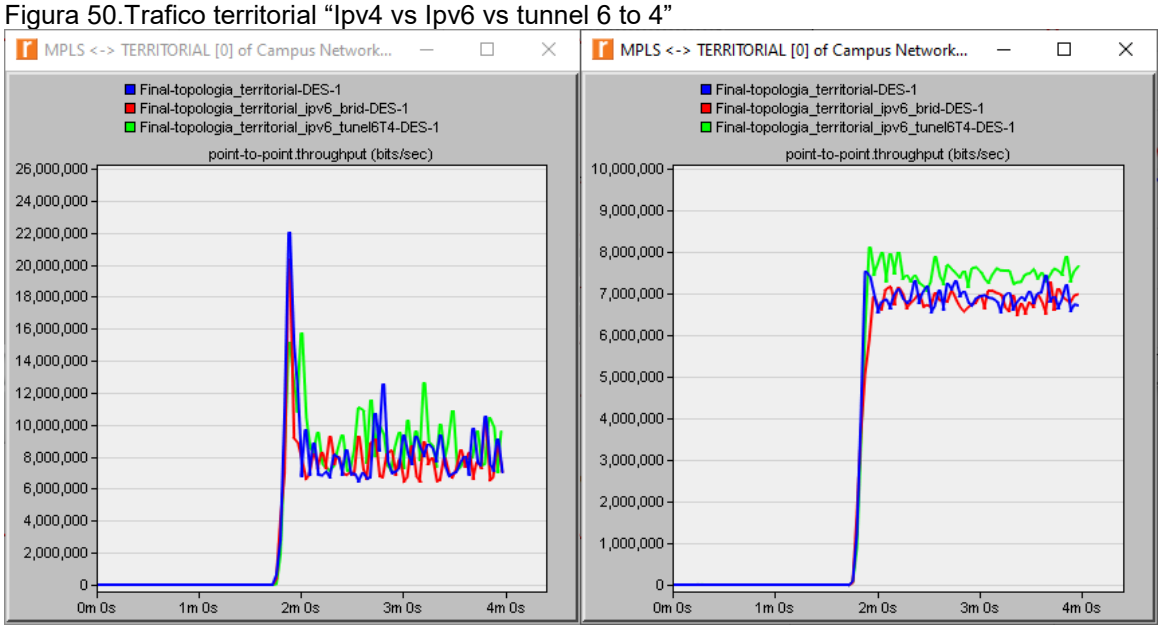
10.3.4 Comparación de desempeño de los 3 escenarios simulados. Luego de realizar estas simulaciones con lo indicado se prosiguió a evaluar a través de los gráficos generados la eficiencia, obteniendo los pros y contras de cada escenario. Se considera que las sedes centrales deben llevar obligatoriamente enlaces con el proveedor principal quien debe soportar el protocolo de manera nativa, se simulo solo para realizar comparaciones. Para poder ver de manera más óptima las diferencias en el siguiente apartado se realizó una comparación visual de los grafico generados.

Figura 49. Trafico Inspección “Ipv4 vs Ipv6 vs tunnel 6 to 4”



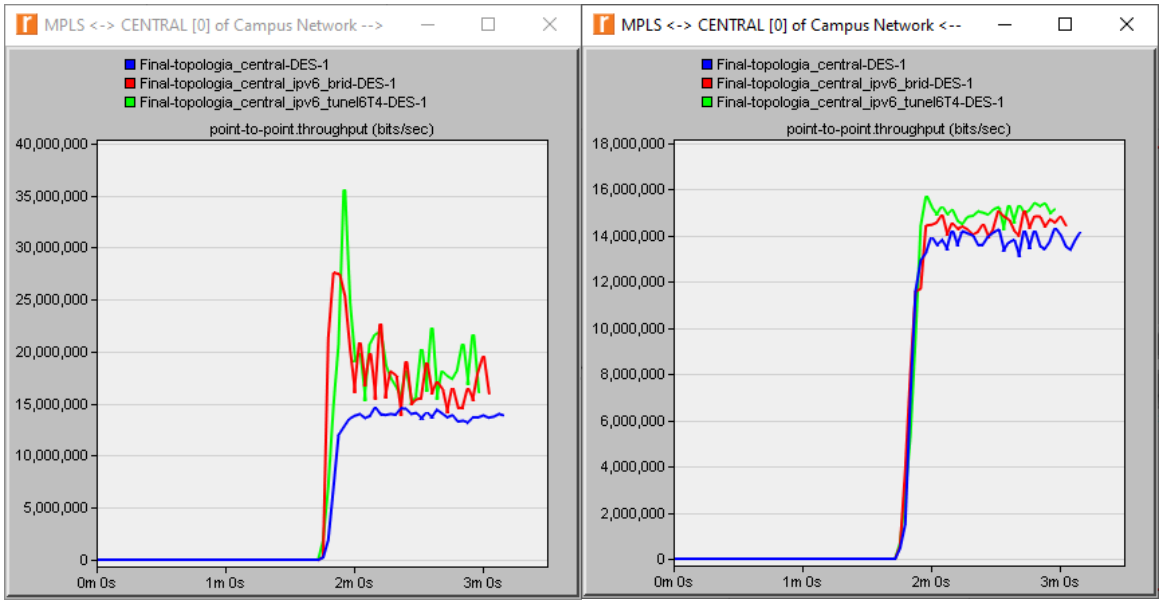
Fuente: Los autores.

Figura 50.Trafico territorial “Ipv4 vs Ipv6 vs tunnel 6 to 4”



Fuente: Los autores.

Figura 51. Trafico *central "Ipv4 vs Ipv6 vs túnnel 6 to 4"*



A través de la simulación podemos concluir los siguientes puntos clave

- La diferencia de tráfico no es significativa a pesar del cambio de tamaño de encabezado, no implica ampliación en la capacidad de los enlaces.
- Al realizar la migración los pools de direcciones disponibles son muy grandes eliminando la necesidad de reasignar direcciones por el aumento de máquinas en la Lan.
- Al desaparecer la necesidad de realizar NAT los routers podrán aprovechar sus capacidades para otro tipo de tareas como QoS.

11. RESULTADOS

- Se realizó un plan de migración que permite la transición del protocolo Ipv4 a Ipv6 de forma controlada, y que puede ser utilizado por cualquier entidad que esté pensando adoptar el protocolo Ipv6.

- Se encontró que mediante un software computacional es posible prever el comportamiento del tráfico en una red antes de comenzar su implementación y así evitar cometer errores cuando se ejecute.

- Se observó mediante la simulación que hay un leve aumento de traficó en el escenario donde se utilizó el tunnel 6to4, que se debe al encapsulamiento del paquete Ipv6 dentro de la carga útil del protocolo Ipv4.

- Se realizó una caracterización de las sedes de la entidad y con base en esta se generó un plan de direccionamiento que permita identificar más fácil y rápidamente las futuras fallas al incluir dentro de la dirección Ipv6 campos que identifican la categoría, la sede y hasta la vlan del servicio afectado.

- Se observó que con el espacio de direccionamiento que se asigna por parte de LACNIC a los clientes finales, se favorece inmensamente la escalabilidad de la red ya que el número de dispositivos que se pueden conectar a esta es bastante grande.

12. DISCUSIÓN

Todos los beneficios que tiene implícito el protocolo hacen considerar que su implementación es inevitable y necesaria, ya que el constante desarrollo en las telecomunicaciones y la interconectividad de los dispositivos de red hacen que por temas de seguridad, gran capacidad de ip's y calidad de servicio entre otros, se tenga que migrar hacia él, permitiendo aprovechar sus capacidades. A medida que crece la red, paralelamente crece el número de direcciones ip necesarias, por esto con la implementación de ipv6 habrá la posibilidad tener una cantidad de direcciones muy grande permitiendo la escalabilidad de la red, la adaptabilidad a los nuevos servicios de telecomunicaciones y la movilidad de los usuarios.

Con la implementación del protocolo cada elemento en la red tendrá la posibilidad de conectarse a internet directamente mediante una ip global, eliminando la necesidad de realizar alguna configuración adicional en los dispositivos de red, como por ejemplo el NAT en los routers, de esta manera se reducen procesos que afectan el rendimiento de la red, así mismo su diseño le facilitará al operador poder implementar mecanismos de cifrado dificultando la interceptación de las comunicaciones, de igual manera se protegerá la privacidad del usuario. La posibilidad de un ataque a la red por medio de fuerza bruta será casi imposible ya que el atacante tendrá que escanear millones de direcciones ip.

Según políticas internacionales el tráfico sobre el protocolo IPv6 tiene prioridad sobre el de IPv4, de esta manera las aplicaciones que se encuentren sobre el nuevo protocolo tendrán una mejoría en los tiempos de respuesta, también se puede evidenciar que con su implementación no se deben realizar modificaciones en el ancho de banda de sus enlaces ya que el throughput con respecto a IPv4 es prácticamente el mismo como se evidencio en la simulación. También se podrá tener acceso a nuevas herramientas tecnológicas, como, por ejemplo, el blockchain que según el MinTic es una tecnología clave para la gestión y administración de la información.

Además de traer beneficios a nivel técnico la transición debe cumplir con lo establecido por la ley colombiana, que a través del ministerio de las tecnologías de la información y las comunicaciones (Min Tic) emitió la circular 2710 del 3 de octubre del 2017 que establece como plazo máximo el 31 de Diciembre de 2020 para la implementación de Ipv6 en las entidades territoriales del país, ya que de no cumplir esta resolución acarreara sanciones.

13. CONCLUSIONES

Al tratarse de una entidad pública su infraestructura tecnológica permanece actualizada debido a las periódicas licitaciones que realiza el gobierno, lo que significa que cada dispositivo de red cuenta con los requerimientos necesarios de software y hardware que permiten la transición al nuevo protocolo, esto se debe a que el protocolo IPv6 se encuentra disponible desde 1998 y los dispositivos con tecnología reciente cuentan con los componentes necesarios para la compatibilidad con ambos protocolos.

Se demostró que con un solo pool de direcciones IPv6 asignado por LACNIC es posible suplir las necesidades de conectividad de cualquier entidad sin importar su tamaño, ya que el prefijo mínimo asignado para entidades y organizaciones es de /48 lo que implica una gran cantidad de direcciones disponibles, este prefijo es más grande que todo el direccionamiento actual de internet en IPv4. De esta manera permite su crecimiento en el futuro sin ninguna restricción de direccionamiento.

Mediante la simulación se pudo constatar que la red cumple con los requisitos y está preparada para realizar la transición de todos sus servicios de forma ordenada y transparente, sin afectar la conectividad ni modificar el ancho de banda de los canales, de esta manera pueden mantener sus dispositivos de red, lo que implica que se hagan solamente actualizaciones de software por parte del proveedor si se llegaran a necesitar. Además de esto si la entidad necesitara adaptar un protocolo nuevo o algún tipo de tecnología adicional se debe considerar un estudio nuevo evaluando específicamente los requisitos de dicha tecnología

Con la adopción del nuevo protocolo la entidad queda preparada para cumplir con los requisitos exigidos por el ministerio de las tecnologías de la información (MinTic), que busca que todas las entidades del gobierno estén a la vanguardia de la innovación tecnológica y de esta manera promover el uso de este protocolo en el país.

Luego de analizar la topología de la entidad y la infraestructura utilizada por los ISP, se puede recomendar bajo el criterio de funcionalidad y escalabilidad la utilización del mecanismo de transición Dual-Stack en el 91% de las sedes en la entidad, ya que este le permite a la entidad la comunicación en IPv6 sin afectar la actual conectividad por el protocolo IPv4 así como la posibilidad de expandir la cantidad de nodos sin incurrir en un aumento de las cargas de procesamiento ni en reconfiguraciones de los demás equipos reduciendo así la probabilidad de fallas o degradación en el servicio. Para el otro 9% de las sedes que no soportan IPv6 en el operador de última milla se recomienda la implementación del mecanismo de

transición túnel 6to4 ya que también bajo el criterio de funcionalidad y procesamiento le permite a la entidad mantener la conectividad con el resto de sedes IPv6 por medio de la encapsulación en el protocolo IPv4 solo con un leve incremento del procesamiento en los equipos routers y sin necesidad de implementar servidores de traslación como en el caso de Teredo o Nat-64.

14. REFERENCIAS

[1] ARCHIER, Jean-Paul IPv6. Principios e implementación. Editorial Eni, 2017 456p

[2] CISCO. Cisco, Dual Stack Network. 2018. {En Linea}. {Consultado el 17 de Enero de 2020}. Disponible en https://www.cisco.com/c/dam/docs/ gov/IPV6at_a _glance_c45-625859.pdf

[3] CISCO. IPv6 Implementation Guide. {En Linea}. {Consultado el 20 de Enero de 2020}. Disponible en: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/c onfigu ration/15-2mt/ipv6-15-2mt-book.html

[4] DEL REY, Marina. Internet Protocol Darpa Internet Program Protocol Specification. RFC:791. University of Southern California. {En Linea}. {Consultado el 30 de Abril de 2020}. Disponible https://tools.ietf.org/html/rfc791

[5] DEERING,S. Especificación Protocolo Internet, Versión 6 (IPv6).RFC 2460. {En Linea}. {Consultado el 30 de Abril de 2020}. Disponible en https://www.rfc-es.org /rfc /rfc2460-es.txt

[6] DANS, Alex. Nuevas formas de promover IPv6 en Latinoamérica y el Caribe2. {En Linea}. {Consultado el 20 de Enero de 2020}. Disponible en: https://www.icann. org/news/blog/doctor-ipv6-nuevas-formas-de-promover-ipv6-en-latinoamerica-y-el-caribe

[7] EGEVANG,K. The IP Network Address Translator (NAT).RFC 1631. {En Linea}. {Consultado el 30 de Abril de 2020}. Disponible en https://tools.ietf.org/html/rfc1631

[8] FERNANDEZ ALCANTARA, Azael. Requerimientos de IPv6 para equipos de TIC. {En Linea}. {Consultado el 18 de Enero de 2020}. Disponible en: http://www.ipv6.unam.mx/documentos/BCOP-Requerimientos-IPv6_Equipos-Red-LACNOG_2016.pdf

[9] FULLER,V. Classless Inter-domain Routing (CIDR) The Internet Address Assignment and Aggregation.RFC 4632. {En Linea}.{Consultado el 10 de Enero de 2020}. Disponible en https://tools.ietf.org/html/rfc4632

[10] GILLIGAN,R. Basic Transition Mechanisms for IPv6 Hosts and Routers, RFC 4213. {En Linea}. {Consultado el 17 de Enero de 2020}. Disponible en https://tools.ietf.org/html/rfc4213

[11] GUTIÉRREZ , Liliana. IPv6 una realidad. 1ra edicion; editorial Ediciones de la U. 2019. 206 p

[12] GNS3. Modelos de Red y simuladores. {En Linea}. {Consultado el 1 de Mayo de 2020}. Disponible en https://gns3.com/5-mejores-simuladores

[13] GOOGLE. Adopcion de Ipv6 por pais. {En Linea}. {Consultado el 05 de Febrero de 2020}. Disponible en: https://www.google.com/intl/es/ipv6/statistics.html

[14] GUILLERMO,Cicileo. Ipv6 para Todos. 2da edicion. Editorial ISOC-AR Capitulo Argentina de Internet Society, 2016. 155 p

[15] HAGEN,Silvia. IPv6 Essentials. 2nd edition. Editorial O'Reilly Media, 2012. 438 p.

[16] IANA. Espacio de direcciones IPv6 asignadas por IANA. {En Linea}. {Consultado el 25 de Enero de 2020}. Disponible en: https://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml

[17] IEEE. 802.3u-1995 - IEEE Standards for Local and Metropolitan Area Networks. {En Linea}.{Consultado el 30 de Abril de 2020}. Disponible en https://standards.ieee.org/standard/802_3u-1995.html

[18] ITU. Committed to connecting the world ITU-T Y.2060". {En Linea}. {Consultado el 30 de Abril de 2020}. Disponible https://www.itu.int/en/ITU-T/gsi/iot/Pages /default.aspx

[19] KAUFMANN ,Morgan. Network Routing, Algorithms, Protocols and Architectures. Karthikeyan Ramasamy,2017. 848 p

[20] KASCH,W. Network Time Protocol versión 4. {Consultado el 10 de Mayo de 2020} . Disponible en https://tools.ietf.org/html/rfc5905

[21] LACNIC. El crecimiento de IPv6 y las perspectivas para 2020. {En Linea}. {Consultado el 08 de Enero de 2020}. Disponible en: https://prensa.lacnic.net/news/ipv6/el-crecimiento-de-ipv6-y-las-perspectivas-para-2020

[22] LACNIC. Estadísticas de LACNIC en Colombia. {En Linea}.{Consultado el 23 de Enero de 2020}. Disponible en:https://stats.labs.lacnic.net/api/ipv6/createhipv6withcontrols/co

[23] LACNIC. Políticas sobre el agotamiento del espacio de direcciones IPv4. { En Linea}.{Consultado el 27 de Diciembre de 2019}. Disponible en http://www.lacnic.net/web/lacnic/manual-11

[24] LACNIC. Registro de organizaciones que implementan IPv6. {En Linea}. {Consultado el 11 de Enero de 2020}. Disponible en http://portalipv6 .lacnic .net/quienes-implementan

[25] LYNCH , Tomas. IPv6 para operadores de Red. Editorial ISOC-AR Capitulo Argentina de Internet Society. 1ª Edición. 2015, 164 p

[26] MINISTERIO DE TECNOLOGIA DE LA INFORMACION. Agotadas direcciones de Internet. Grupo de Investigación de Teleinformática { En Linea}.{Consultado el 27 de Diciembre de 2019}. Disponible en https://www.mintic.gov.co/portal /604/articles-6115 _archivo_pdf.pdf.

[27] MINISTERIO DE TECNOLOGIA DE LA INFORMACION. Circular 2710 de 3 de octubre de 2017. {En Linea}.{Consultado el 08 de Enero de 2020}. Disponible en: https://www.mintic.gov.co/portal/604/articles-61192_recurso_1.pdf

[28] MINISTERIO DE TECNOLOGIA DE LA INFORMACION. Ipv6 en Colombia. { En Linea}.{Consultado el 11 de Enero de 2020}. Disponible en http://www.mintic.gov .co/portal/604/w3-article-7195.html

[29] PETER,Loshin. IPv6 : Theory, Protocol, and Practice, 2014. 320 p

[30] RENATA. El protocolo IPv6 en Colombia. {En Linea}. {Consultado el 09 de Enero de 2020}. Disponible en: https://www.renata.edu.co/protocolo-ipv6-en-colo mbia

[31] SETHIVASIL,S. The Practical OPNET® User Guide forComputer Network Simulation. Editorial CRC Press, 2015. 507 p

[32] SOCIEDAD PROMOTORA DE IPV6. Internet hoy. {En Linea}.{Consultado el 11 de Enero de 2020}.Disponible en:http://www.internet society.org/deploy360/ip v6/

[33] WOZABAL, Karl . Ip network Design Guide. Editorial International Technical Support Organization, 1999. 309 p

ANEXO A. LISTADO DE SEDES EN EL TERRITORIO NACIONAL

TERRITORIAL	INSPECCION	JURISDICCION
GUAJIRA	Barrancas	Barrancas- Hatonuevo
CUNDINAMARCA	Funza	Cota- Funza- Mosquera
ANTIOQUIA	Bagre	El Bagre- Zaragoza
MAGDALENA	Santa Marta	Santa Marta
NORTE DE SANTANDER	Salazar de las Palmas	Arboledas- Cucutilla- Gramalote- Lourdes- Salazar de las Palmas- Villacaro
ATLANTICO	Barranquilla	Barranquilla- Malambo- Puerto Colombia- Soledad- Remolino (Mag)- Sitio Nuevo (Mag)
CESAR	Jagua de Ibirico	La Jagua de Ibirico- Becerril
CASANARE	Monterrey	Monterrey- Sabanalarga- Tauramena- Villanueva
CALDAS	Manzanares	Manzanares- Marquetalia- Pensilvania
MAGDALENA	Pivijay	Pivijay
CESAR	Bosconia	Astrea- Bosconia- El Copey- Chimichagua
ANTIOQUIA	Concordia	Betulia- Concordia- Salgar- Urrao
GUAJIRA	Maicao	Albania- Maicao- Manaure- Uribia
CESAR	Valledupar	Manaure- Pueblo Bello- Robles (La Paz)- San Diego- Valledupar
CORDOBA	Planeta rico	Buenavista- Planeta Rica- Pueblo Nuevo
NORTE DE SANTANDER	Los Patios	Los Patios- Villa del Rosario
ARAUCA	Arauca	Arauca- Arauquita- Cravo Norte
CORDOBA	Tierralta	Tierralta- Valencia
MAGDALENA	Fundación	Algarrobo- Aracataca- Fundación- El Retén
MAGDALENA	Plato	Ariguaní- Concordia- Chivolo- Nueva Granada- Plato- Sabana de San Angel- Santa Barbara de Pinto- Tenerife- Zapayán
ANTIOQUIA	Puerto Berrio	Caracolí- Maceo- Puerto Berrio- Puerto Nare- Puerto Triunfo
HUILA	Neiva	Aipe- Algeciras- Baraya- Campoalegre- Colombia- Hobo- Iquira- Neiva- Palermo- Rivera- Santa María- Tello- Teruel- Villavieja- Yaguará
VALLE DEL CAUCA	Cali	Cali- Dagua- Jamundí- La Cumbre- Vijes- Yumbo
CUNDINAMARCA	Ubate	Carmen de Carupa- Cucunubá- Fúquene- Guachetá- Lenguazaque- Simijaca- Susa- Sutatausa- Tausa- Ubaté
URABA - APARTADO	Apartadó	Apartadó- Carepa- Chigorodó- Mutatá

TERRITORIAL	INSPECCION	JURISDICCION
CORDOBA	Cereté	Cereté- San Carlos- Cienaga de Oro- San Pelayo- Cotorra
META	Granada	Cubarral- El Castillo- El Dorado- Fuente de Oro- Granada- La Uribe- Lejanías- Medellín de Ariari- Mesetas- Puerto Concordia- Puerto Lleras- Puerto Rico- San Juan de Arama- San Martín- Vista Hermosa
BOLIVAR	Cartagena	Arjona- Arroyo Hondo- Cartagena- Clemencia- Mahates- San Estanislao- Santa Catalina- Santa Rosa de Lima- Soplaviento- San Cristóbal- Turbaco- Turbaná- Villanueva
ATLANTICO	Sabanalarga	Candelaria- Luruaco- Manatí- Ponedera- Repelón- Sabanalarga
SUCRE	Tolu	Coveñas- Los Palmitos- San Onofre- Santiago de Tolú- Tolú Viejo
VALLE DEL CAUCA	Cartago	Alcalá- Ansermanuevo- Argelia- Cartago- El Águila- El Cairo- La Victoria- Obando- Ulloa- San José del Palmar (Chocó)
META	Villavicencio	Acacías- Castilla Nueva- El Calvario- Guamal- La Macarena- Mapiripán- San Carlos de Guaroa- San Juanito- Villavicencio- Guayabetal (Cund)- Quetame (Cund)
ANTIOQUIA	Sonson	Abejorral- Argelia- Nariño- Sonsón
SANTANDER	Velez	Aguada- Bolívar- Chipatá- El Peñón- Guavatá- La Paz- Landázuri- Santa Helena del Opón- Sucre- Vélez
CORDOBA	Monteria	Canalete- Los Córdobas- Montería- Puerto Escondido- Arboletes (Ant)
QUINDIO	Quimbaya	Filandia- Montenegro- Quimbaya
CESAR	Codazzi	Agustín Codazzi
URABA - APARTADO	Turbo	Necoclí- San Juan de Urabá- San Pedro de Urabá- Turbo
NARIÑO	Tumaco	Barbacoas- El Charco- Francisco Pizarro- La Tola- Maguí- Mosquera- Roberto Payán- Santa Bárbara- Tumaco
VALLE DEL CAUCA	Buenaventura	Buenaventura
META	Puerto Lopez	Cabuyaro- Puerto López
ANTIOQUIA	Cisneros	Carolina- Cisneros- Gómez–Plata- Guadalupe- San Roque- Santo Domingo- Yolombó
CALDAS	Manizales	Chinchiná- Filadelfia- Manizales- Neira- Palestina- Villamaría

TERRITORIAL	INSPECCION	JURISDICCION
ANTIOQUIA	Amaga	Amagá- Angelópolis- Fredonia- Titiribí- Venecia
CAUCA	Guapi	Guapi- López de Micay- Timbiquí
SANTANDER	Bucaramanga	Bucaramanga- California- Charta- El Playón- Floridablanca- Girón- Lebrija- Los Santos- Matanza- Piedecuesta- Rionegro- Santa Bárbara- Suratá- Tona- Vetas- Cáchira (Nte Sder)
CHOCO	Bahia Solano	Bahía Solano- Juradó- Nuquí
META	Puerto Gaitan	Puerto Gaitán
RISARALDA	Dosquebradas	Dosquebradas
SANTANDER	Malaga	Capitanejo- Carcasí- Cerrito- Concepción- Enciso- Guaca- Macaravita- Málaga- Molagavita- San Andrés- San José de Miranda- San Miguel
BOYACA	Soata	Boavita- Chiscas- Chita- Covarachía- El Cocuy- El Espino- Guacamayas- Güicán- Jericó- La Uvita- Panqueba- San Mateo- Sativanorte- Sativasur- Soatá- Susacón- Tipacoque
TOLIMA	Libano	Casabianca- Herveo- Líbano- Murillo- Villahermosa
TOLIMA	Mariquita	Ambalema- Armero-Guayabal- Falán- Fresno- Honda- Lérida- Mariquita- Palocabildo- Santa Isabel
ANTIOQUIA	Santa fe de Antioquia	Anzá- Buriticá- Caicedo- Ebéjico- Giraldo- Liborina- Olaya- Sabanalarga- San Jerónimo- Santafé de Antioquia- Sopetrán
GUAJIRA	Riohacha	Riohacha- Dibulla
ATLANTICO	Campo de la cruz	Campo de la Cruz- Santa Lucía- Suán- Cerro San Antonio (Mag)- El Piñón (Mag)- Pedraza (Mag)- Salamina (Mag)- Calamar (Bol)
MAGDALENA	El Banco	El Banco- Guamal- Altos del Rosario (Bol)- Barranco de Loba (Bol)- El Peñón (Bol)- San Martín de Loba (Bol)
CUNDINAMARCA	Soacha	El Colegio- Granada- San Antonio del Tequendama- San Antonio de Tena- Sibaté- Soacha- Tena
ANTIOQUIA	Santa Rosa de Osos	Belmira- Don Matías- Entrerríos- Ituango- San José de la Montaña- San Andrés de Cuerquia- Santa Rosa de Osos- Toledo

TERRITORIAL	INSPECCION	JURISDICCION
TOLIMA	Chaparral	Ataco- Chaparral- Planadas- Rioblanco- Roncesvalles- San Antonio
NARIÑO	Pasto	Ancuyá- Buesaco- Consacá- Chachaguí- El Tablón- El Tambo- La Florida- Linares- Nariño- Olaya Herrera- Pasto- Sandoná- Tangua- Yacuanquer
RISARALDA	Pereira	Marsella- Pereira
BARRANCABERMEJA	Barrancabermeja	Barrancabermeja- Cimitarra- Puerto Parra- Yondó (Ant)
BOGOTA	Bogotá. D.C	Bogotá D.C.
CUNDINAMARCA	Facatativá	Albán- Anolaima- Bituima- Bojacá- Cachipay- El Rosal- Facatativá- Guayabal de Síquima- La Florida- Madrid- San Juan de Río Seco- Subachoque- Vianí- Zipacón
SUCRE	Sincelejo	Sincelejo- Buenavista- Chalán- Colosó- Corozal- El Roble- Galeras- Morroa- Ovejas- Sampués- San Antonio de Palmito- San Juan de Betulia- San Pedro- San Luis de Sincé
NORTE DE SANTANDER	Chinácota	Chinácota- Durania- Bochalema- Herrán- Ragonvalia
ANTIOQUIA	Medellin	Armenia- Barbosa- Bello- Caldas- Copacabana- Envigado- Girardota- Heliconia- Itagüí- La Estrella- Medellín- Sabaneta- San Pedro
ANTIOQUIA	Rionegro	Carmen de Viboral- La Ceja- La Unión- Marinilla- Retiro- Rionegro- Santuario
SANTANDER	Puerto Wilches	Puerto Wilches- San Pablo (Bol)- Canta Gallo (Bol)
NORTE DE SANTANDER	Tibú	El Tarra- Tibú
SANTANDER	Barbosa	Barbosa- Florián- Gámbita- Güepsa- Jesús María- La belleza- Puente Nacional- San Benito- Chitaraque (Boy)- Moniquirá (Boy)- San José de Pare (Boy)- Santa Ana (Boy)- Togüi (Boy)
BOLIVAR	Carmen de bolívar	El Carmen de Bolívar- El Guamo- María La Baja- San Jacinto- San Juan Nepomuceno- Córdoba- Zambrano
BOYACA	Chiquinquirá	Briceño- Buenavista- Caldas- Coper- Chiquinquirá- La Victoria- Maripí- Muzo- Otanche- Pauna- Quipama- Ráquira- Saboyá- San Miguel de Sema- San Pablo de Borbur- Santa Sofía- Sutamarchán- Tinjacá-

TERRITORIAL	INSPECCION	JURISDICCION
NORTE DE SANTANDER	Ocaña	Abrego- Convención- El Carmen- Hacarí- La Playa- Ocaña- San Calixto- Teorama- González (Cesar)- Río de Oro (Cesar)
SAN ANDRES	San Andres	San Andrés- Providencia
CESAR	Aguachica	Aguachica- Gamarra- La Gloria- San Alberto- San Martín- Arenal (Bol)- Morales (Bol)- Simití (Bol)- Santa Rosa del Sur (Bol)- La Esperanza (Nte Sant)
BOYACA	Duitama	Belén- Cerinza- Duitama- Paipa- Santa Rosa de Viterbo- Tutasá
CAUCA	Santander de Quilichao	Buenos Aires- Caldono- Caloto- Corinto- Miranda- Padilla- Puerto Tejada- Santander de Quilichao- Suárez- Toribio- Villarrica
PUTUMAYO	Puerto Asís	Puerto Asís- Puerto Caicedo- Puerto Leguizamo
CASANARE	Yopal	Aguazul- Chámela- Hato Corozal- Maní- Nunchía- Orocué- Paz de Ariporo- Pore- Recetor- San Luis de Palenque- Támara- Trinidad- Yopal- Pajarito (Boyacá)
CAUCA	Popayán	Cajibío- El Tambo- Jámbalo- La Sierra- Morales- Piendamó- Popayán- Puracé (Coconucos)- Rosas- Silvia- Sotará (Paíspamba)- Timbío- Totoró
TOLIMA	Ibague	Ibagué- Alvarado- Anzoátegui- Cajamarca- Piedras- Rovira- Valle de San Juan- Venadillo
GUAVIARE	San José	Calamar- El Retorno- Miraflores- San José del Guaviare
NORTE DE SANTANDER	Pamplona	Cácota- Chitagá- Labateca- Mutiscua- Pamplona- Pamplonita- Silos- Toledo
CUNDINAMARCA	Zipaquirá	Cogua- El Peñón- Gachancipá- Guatavita- La Palma- Nemocón- Pacho- Paime- Sopó- San Cayetano- Sesquilé- Supatá- Tocancipá- Villa Gómez- Yacopí- Zipaquirá
QUINDIO	Armenia	Armenia- Buenavista- Calarcá- Circasia- Córdoba- Génova- La Tebaida- Pijao- Salento
VALLE DEL CAUCA	Tuluá	Andalucía- Bugalagrande- Riofrío- Trujillo- Tuluá
RISARALDA	La Virginia	Apía- Balboa- Belén de Umbría- La Celia- La Virginia- Pueblo Rico- Santuario- Viterbo (Caldas)- Belalcázar (Caldas)
VALLE DEL CAUCA	Buga	Buga- Calima- Guacarí- Restrepo- San Pedro- Yotoco

TERRITORIAL	INSPECCION	JURISDICCION
SANTANDER	San Vicente de chucuri	Betulia- El Carmen- San Vicente de Chucurí- Zapatoca
ANTIOQUIA	Andes	Andes- Betania- Ciudad Bolívar- Hispania- Jardín- Jericó- Pueblorrico- Tarso.
ARAUCA	Tame	Fortul- Puerto Rondón- Saravena- Tame- Cubará (Boy)
CALDAS	Salamina	Aguadas- Aránzazu- La Merced- Marulanda- Pácora- Salamina
TOLIMA	Melgar	Carmen de Apicalá- Cunday- Icononzo- Melgar- Villarrica
BOYACA	Sogamoso	Aquitania- Beteitivá- Busbanzá- Corrales- Cuitiva- Firavitoba- Gámeza- Iza- Floresta- Labranzagrande- Mongua- Monguí- Nobsa- Paya- Paz del Río- Pesca- Pisba- Socha- Socotá- Sogamoso- Tasco- Tibasosa- Tópaga- Tota- Sacaba (Casanare)- La Salina (Casanare)
PUTUMAYO	Orito	Orito- Valle del Guamués (La Hormiga)- San Miguel
ANTIOQUIA	Cañas Gordas	Abriaquí- Cañasgordas- Dabeiba- Frontino- Peque- Uramita
SANTANDER	Sabana de Torres	Sabana de Torres
BOLIVAR	Magangue	Magangué- Montecristo- Pinillos- San Jacinto del Cauca- Tiquisio
MAGDALENA	Cienaga	Ciénaga- Pueblo Viejo- Zona Bananera
CORDOBA	Sahagun	Chimá- Chinú- San Andrés de Sotavento- Sahagún
CORDOBA	Montelibano	Ayapel - La Apartada- Montelíbano- Puerto Libertador
AMAZONAS	Leticia	El Encanto- La Chorrera- La Pedrera- La Victoria- Puerto Alegría- Leticia- Miritíi-Paraná- Puerto Arica- Puerto Nariño- Puerto Santander- Tarapacá.
CUNDINAMARCA	Girardot	Agua de Dios- Anapoima- Beltrán- Girardot- Guataquí- Jerusalén- La Mesa- Nariño- Nilo- Pulí- Apulo (Rafael Reyes)- Ricaurte- Tocaima- Viotá- Flandes (Tol)
BOYACA	Guateque	Almeida- Chinavita- Chivor- Garagoa- Guateque- Guayatá- La Capilla- Macanal- Pachavita- San Luis de Gaceno- Santa María- Somondoco- Sutatenza- Tenza- Umbita. Chocontá (Cund)- Gachalá (Cund)- Gachetá (

TERRITORIAL	INSPECCION	JURISDICCION
CALDAS	Anserma	Anserma- Risaralda- San José- Guática (Risar)- Mistrato (Risar)
ANTIOQUIA	Guarne	Alejandría- Cocorná- Concepción- Granada- Guarne- Guatapé- Peñol- San Vicente- San Rafael- San Carlos- San francisco- San Luis
CHOCO	Quibdo	Alto Baudó- Atrato- Bagadó- Bojayá- El Carmen de Atrato- Lloró- Medio Atrato- Quibdó- Río Quito- Murindó (Ant)- Vigía del Fuerte (Ant)
CAQUETA	El Doncello	Cartagena del Chaira- El Doncello- El Paujil- Puerto Rico- San Vicente del Caguán.
TERRITORIAL	INSPECCION	JURISDICCION
NARIÑO	Tuquerres	El Peñol- Funes- Guaitarilla- Iles- Imués- La Llanada- Linares- Los Andes (Sotomayor)- Mallama- Ospina- Providencia- Ricaurte- Samaniego- Santa Cruz- Sapuyes- Túquerres
BOYACA	Tunja	Arcabuco- Berbeo- Boyacá- Campohermoso- Chiquiza- Chivatá- Ciénaga- Cómbita- Cucaita- Gachantivá- Jenesano- Miraflores- Motavita- Nuevo Colón- Oicatá- Páez- Ramiriquí- Rondón- Sáchica- Samacá- San Eduardo- Siachoque- Sora- Soracá- Sotaquirá- Tunja- Tuta- Turmequé- Tibaná- Toca- Ventaquemada- Villa de Leiva- Viracachá- Zetaquira
CUNDINAMARCA	Fusagasuga	Arbeláez- Cabrera- Fusagasuga- Ospina Pérez- Pandi- Pasca- San Bernardo- Silvania- Tibacuy- Venecia
CUNDINAMARCA		
ANTIOQUIA	Santa Barbara	Caramanta- La Pintada- Montebello- Santa Bárbara- Támesis- Valparaíso
HUILA	Plata	La Argentina- La Plata- Nátaga- Paicol- Tesalia- Inza (Cauca)- Paez Belalcazar (Cauca)
SANTANDER	Socorro	Chima- Confines- Contratación- El Guacamayo- Galán- Guadalupe- Guápota- Hato- Oiba- Palmar- Palmas del Socorro- Simacota- Socorro- Suaita
SUCRE	San Marcos	Caimito- La Unión- San Benito Abad- San Marcos
HUILA	Pitalito	Acevedo- Elías- Isnos- Oporapa- Palestina- Pitalito- Salado Blanco- San Agustín- Timaná
CESAR	Chiriguaná	Chiriguaná- El Paso (La Loma)

TERRITORIAL	INSPECCION	JURISDICCION
NARIÑO	Ipiales	Aldana- Contadero- Córdoba- Cuaspud-Cumbal- Guachucal- Gualmatán- Ipiales-Potosí- Puérres- Pupiales
CHOCO	Itsmina	Andagoya- Alto San Juan- Bajo Baudó (Pizarro)- Cantón de San Pablo- Certeguí-Condoto- Istmina- Litoral de San Juan- Medio Baudó- Medio San Juan- Novita- Río Iró- Sipi-Tadó- Unión Panamericana
CUNDINAMARCA	Chía	Cajicá- Chía- Guasca- La Calera- Suesca-Tabio- Tenjo- Villa Pinzón
ATLANTICO	Baranoa	Baranoa- Galapa- Juan de Acosta- Palmar de Varela- Piojó- Polo Nuevo- Sabanagrande-Santo Tomás- Tubará- Usiacurí
NORTE DE SANTANDER	San José de Cúcuta	Bucarasica- Cúcuta- El Zulia- Puerto Santander- San Cayetano- Santiago-Sardinata
GUAINIA	Puerto Inirida	Inírida- Barranco Minas- Cacahual- La Guadalupe- Morichal Nuevo- Pana Pana-Puerto Colombia- San Felipe
PUTUMAYO	Mocoa	Mocoa- Colón- Puerto Guzmán- San Francisco- Santiago- Sibundoy- Villagarzón
VALLE DEL CAUCA	Roldanillo	Bolívar- El Dovio- La Unión- Roldanillo- Toro-Versalles- Zarzal
VICHADA	Puerto Carreño	Cumaribo- La Primavera- Puerto Carreño-Santa Rosalía
CALDAS	Puerto Boyacá	Puerto Boyacá (Bycá)
VALLE DEL CAUCA	Sevilla	Caicedonia- Sevilla
CAUCA	Patia-Bordo	Sucre- Argelia- Balboa- Mercaderes- Patía (El Bordo)
SUCRE	Majagual	Guaranda- Majagual- Sucre- Achí (Bol)
ANTIOQUIA	Segovia	Amalfi- Remedios- Segovia- Vegachí- Yalí.
CUNDINAMARCA	Caqueza	Cáqueza- Chipaque- Choachí- Fómeque-Fosca- Gutiérrez- Ubaque- Une
CUNDINAMARCA	Villeta	Caparrapí- Chaguaní- Guaduas- La Peña- La Vega- Nimaima- Nocaima- Quebradanegra-Quipile- San Francisco- Sasaima- Topaipí-Utica- Vergara- Villeta
TOLIMA	Espinal	Alpujarra- Coello- Coyaima- Dolores- Espinal-Guamo- Natagaima- Ortega- Prado-Purificación- Saldaña- San Luis- Suárez
CORDOBA	Lorica	Lorica- Momil- Moñitos- Purísima- San Antero-San Bernardo del Viento

TERRITORIAL	INSPECCION	JURISDICCION
CHOCO	Rio Sucio	Acandí- Belén de Bajirá- Carmen del Darién- Ungía- Río Sucio
HUILA	Garzón	Agrado- Altamira- Garzón- Gigante- Guadalupe- Pital- Suaza - Tarqui
ANTIOQUIA	Yarumal	Angostura- Anorí- Briceño- Campamento- Valdivia- Yarumal
VALLE DEL CAUCA	Palmira	Candelaria- El Cerrito- Florida- Ginebra- Palmira- Pradera
CAUCA	Bolivar	Almaguer- Bolívar- Florencia- La Vega- Piamonte- San Sebastián- Santa Rosa
CESAR	Curumani	Curumaní- Pailitas- Pelaya- Rio Viejo (Bol)- Regidor (Bol)- Tamalameque
CAQUETA	Florencia	Albania- Belén de los Andaquíes- Curillo- Florencia- La Montañita- Milan- Morelia- San José de Fragua- Solano- Solita- Valparaiso
BOLIVAR	Mompos	Cicuco- Hatillo de Loba- Margarita- Mompos- San Fernando- Talaigua Nueva- Vijiño del Carmen (Mag)- San Sebastián de Buenavista (Mag)- San Zenón (Mag)- Santa Ana (Mag)
ANTIOQUIA	Caucacia	Cáceres- Caucasia- Nechí- Tarazá
SANTANDER	San Gil	Aratoca- Barichara- Cabrera- Cepitá- Charalá- Coromoro- Curití- Encino- Jordán- Mogotes- Ocamonte- Onzaga- Páramo- Pinchote- San Gil- San Joaquín- Valle de San José- Villanueva
CALDAS	Rio Sucio	Marmato- Riosucio- Supía- Quinchía (Risaralda)
META	Cumaral	Barranca de Upía- Cumaral- Restrepo- Medina (Cund)- Paratebueno (Cund)
VAUPES	Mitu	Carurú- Mitú- Pacoa- Papunaua- Taraira- Yavaraté
GUAJIRA	Fonseca	Distracción- El Molino- Fonseca- La Jagua del Pilar- Nazareth- San Juan del Cesar- Urumita- Villa Nueva

ANEXO B. RELACION DE DIRECCIONAMIENTO IPV6 ASIGNADO

CIUDADES PRINCIPALES Y DATACENTER

TERRITORIAL	INSPECCION	SEGMENTO IPV4	SEGMENTO IPV6	OPERADOR
BOGOTA	Bogotá. D.C	172.16.100.0/22	2800:26c:14a:b000::/64	ETB
ANTIOQUIA	Medellín	172.16.104.0/22	2800:26c:14a:b010::/64	ETB
ATLANTICO	Barranquilla	172.16.108.0/22	2800:26c:14a:b020::/64	ETB
META	Villavicencio	172.16.112.0/22	2800:26c:14a:b030::/64	ETB
VALLE DEL CAUCA	Cali	172.16.116.0/22	2800:26c:14a:b040::/64	ETB

DATACENTER	DC	172.16.200.0/22	2800:26c:14a:c000::/64	ETB

TERRITORIAL	INSPECCION	SEGMENTO IPV4	SEGMENTO IPV6	OPERADOR
AMAZONAS	Leticia	172.16.0.0/23	2800:26c:14a:a000::/64	SKYNET
ARAUCA	Arauca	172.16.2.0/23	2800:26c:14a:a010::/64	ETB
BARRANCABERMEJA	Barrancabermeja	172.16.4.0/23	2800:26c:14a:a020::/64	TELEFONICA
BOLIVAR	Cartagena	172.16.6.0/23	2800:26c:14a:a030::/64	ETB
BOYACA	Tunja	172.16.8.0/23	2800:26c:14a:a040::/64	ETB
CALDAS	Manizales	172.16.10.0/23	2800:26c:14a:a050::/64	ETB
CAQUETA	Florencia	172.16.12.0/23	2800:26c:14a:a060::/64	ETB
CASANARE	Yopal	172.16.14.0/23	2800:26c:14a:a070::/64	ETB
CAUCA	Popayán	172.16.16.0/23	2800:26c:14a:a080::/64	ETB
CESAR	Valledupar	172.16.18.0/23	2800:26c:14a:a090::/64	ETB
CHOCO	Quibdó	172.16.20.0/23	2800:26c:14a:a0a0::/64	SKYNET
CORDOBA	Montería	172.16.22.0/23	2800:26c:14a:a0b0::/64	MEDIA COMERCE
CUNDINAMARCA	Facatativá	172.16.24.0/23	2800:26c:14a:a0c0::/64	ETB
GUAINIA	Puerto Inírida	172.16.26.0/23	2800:26c:14a:a0d0::/64	SKYNET
GUAJIRA	Riohacha	172.16.28.0/23	2800:26c:14a:a0e0::/64	MEDIA COMERCE
GUAVIARE	San José	172.16.30.0/23	2800:26c:14a:a0f0::/64	SKYNET
HUILA	Neiva	172.16.32.0/23	2800:26c:14a:a100::/64	ETB
MAGDALENA	Santa Marta	172.16.34.0/23	2800:26c:14a:a110::/64	ETB
NARIÑO	Pasto	172.16.36.0/23	2800:26c:14a:a120::/64	ETB
NORTE DE SANTANDER	Pamplona	172.16.38.0/23	2800:26c:14a:a130::/64	ETB
PUTUMAYO	Mocoa	172.16.40.0/23	2800:26c:14a:a140::/64	SKYNET
QUINDIO	Armenia	172.16.42.0/23	2800:26c:14a:a150::/64	ETB
RISARALDA	Pereira	172.16.44.0/23	2800:26c:14a:a160::/64	ETB
SAN ANDRES	San Andres	172.16.46.0/23	2800:26c:14a:a170::/64	SOL CABLEVISION

TERRITORIAL	INSPECCION	SEGMENTO IPV4	SEGMENTO IPV6	OPERADOR
SANTANDER	Bucaramanga	172.16.48.0/23	2800:26c:14a:a180::/64	ETB
SUCRE	Sincelejo	172.16.50.0/23	2800:26c:14a:a190::/64	ETB
TOLIMA	Ibagué	172.16.52.0/23	2800:26c:14a:a1a0::/64	ETB
URABA - APARTADO	Apartadó	172.16.54.0/23	2800:26c:14a:a1b0::/64	SKYNET
VAUPES	Mitú	172.16.56.0/23	2800:26c:14a:a1c0::/64	SKYNET
VICHADA	Puerto Carreño	172.16.58.0/23	2800:26c:14a:a1d0::/64	SKYNET

INPECCIONES

TERRITORIAL	INSPECCION	SEGMENTO IPV4	SEGMENTO IPV6	OPERADOR
ANTIOQUIA	Bagre	192.168.0.0/24	2800:26c:14a:0000::/64	AZTECA
ANTIOQUIA	Concordia	192.168.1.0/24	2800:26c:14a:0010::/64	UNE
ANTIOQUIA	Puerto Berrio	192.168.2.0/24	2800:26c:14a:0020::/64	AZTECA
ANTIOQUIA	Sonson	192.168.3.0/24	2800:26c:14a:0030::/64	AZTECA
ANTIOQUIA	Cisneros	192.168.4.0/24	2800:26c:14a:0040::/64	UNE
ANTIOQUIA	Amaga	192.168.5.0/24	2800:26c:14a:0050::/64	AZTECA
ANTIOQUIA	Santa fe de Antioquia	192.168.6.0/24	2800:26c:14a:0060::/64	UNE
ANTIOQUIA	Santa Rosa de Osos	192.168.7.0/24	2800:26c:14a:0070::/64	UNE
ANTIOQUIA	Rionegro	192.168.8.0/24	2800:26c:14a:0080::/64	ETB
ANTIOQUIA	Andes	192.168.9.0/24	2800:26c:14a:0090::/64	AZTECA
ANTIOQUIA	Cañas Gordas	192.168.10.0/24	2800:26c:14a:00a0::/64	UNE
ANTIOQUIA	Guarne	192.168.11.0/24	2800:26c:14a:00b0::/64	ETB
ANTIOQUIA	Santa Barbara	192.168.12.0/24	2800:26c:14a:00c0::/64	UNE
ANTIOQUIA	Segovia	192.168.13.0/24	2800:26c:14a:00d0::/64	UNE
ANTIOQUIA	Yarumal	192.168.14.0/24	2800:26c:14a:00e0::/64	UNE
ANTIOQUIA	Caucacia	192.168.15.0/24	2800:26c:14a:00f0::/64	ETB
ARAUCA	Tame	192.168.16.0/24	2800:26c:14a:0100::/64	UNE
ATLANTICO	Sabanalarga	192.168.17.0/24	2800:26c:14a:0110::/64	MEDIA COMERCE
ATLANTICO	Campo de la cruz	192.168.18.0/24	2800:26c:14a:0120::/64	MEDIA COMERCE
ATLANTICO	Baranoa	192.168.19.0/24	2800:26c:14a:0130::/64	MEDIA COMERCE
BOLIVAR	Carmen de bolívar	192.168.20.0/24	2800:26c:14a:0140::/64	MEDIA COMERCE
BOLIVAR	Magangue	192.168.21.0/24	2800:26c:14a:0150::/64	MEDIA COMERCE
BOLIVAR	Mompos	192.168.22.0/24	2800:26c:14a:0160::/64	UNE
BOYACA	Soata	192.168.23.0/24	2800:26c:14a:0170::/64	ETB
BOYACA	Chiquinquirá	192.168.24.0/24	2800:26c:14a:0180::/64	ETB
BOYACA	Duitama	192.168.25.0/24	2800:26c:14a:0190::/64	ETB
BOYACA	Sogamoso	192.168.26.0/24	2800:26c:14a:01a0::/64	ETB

TERRITORIAL	INSPECCION	SEGMENTO IPV4	SEGMENTO IPV6	OPERADOR
BOYACA	Guateque	192.168.27.0/24	2800:26c:14a:01b0::/64	ETB
CALDAS	Manzanares	192.168.28.0/24	2800:26c:14a:01c0::/64	UNE
CALDAS	La Dorada	192.168.29.0/24	2800:26c:14a:01d0::/64	ETB
CALDAS	Salamina	192.168.30.0/24	2800:26c:14a:01e0::/64	UNE
CALDAS	Anserma	192.168.31.0/24	2800:26c:14a:01f0::/64	ETB
CALDAS	Puerto Boyacá	192.168.32.0/24	2800:26c:14a:0200::/64	ETB
CALDAS	Rio Sucio	192.168.33.0/24	2800:26c:14a:0210::/64	UNE
CAQUETA	El Doncello	192.168.34.0/24	2800:26c:14a:0220::/64	UNE
CASANARE	Monterrey	192.168.35.0/24	2800:26c:14a:0230::/64	ETB
CAUCA	Guapi	192.168.36.0/24	2800:26c:14a:0240::/64	ETB
CAUCA	Santander de Quilichao	192.168.37.0/24	2800:26c:14a:0250::/64	ETB
CAUCA	Patia-Bordo	192.168.38.0/24	2800:26c:14a:0260::/64	ETB
CAUCA	Bolivar	192.168.39.0/24	2800:26c:14a:0270::/64	ETB
CESAR	Jagua de Ibirico	192.168.40.0/24	2800:26c:14a:0280::/64	TELEFONICA
CESAR	Bosconia	192.168.41.0/24	2800:26c:14a:0290::/64	MEDIA COMERCE
CESAR	Codazzi	192.168.42.0/24	2800:26c:14a:02a0::/64	TELEFONICA
CESAR	Aguachica	192.168.43.0/24	2800:26c:14a:02b0::/64	TELEFONICA
CESAR	Chiriguaná	192.168.44.0/24	2800:26c:14a:02c0::/64	TELEFOICA
CESAR	Curumani	192.168.45.0/24	2800:26c:14a:02d0::/64	SKYNET
CHOCO	Bahia Solano	192.168.46.0/24	2800:26c:14a:02e0::/64	SKYNET
CHOCO	Itsmina	192.168.47.0/24	2800:26c:14a:02f0::/64	SKYNET
CHOCO	Rio Sucio	192.168.48.0/24	2800:26c:14a:0300::/64	SKYNET
CORDOBA	Planeta rico	192.168.49.0/24	2800:26c:14a:0310::/64	MEDIA COMERCE
CORDOBA	Tierralta	192.168.50.0/24	2800:26c:14a:0320::/64	MEDIA COMERCE
CORDOBA	Cereté	192.168.51.0/24	2800:26c:14a:0330::/64	MEDIA COMERCE
CORDOBA	Sahagun	192.168.52.0/24	2800:26c:14a:0340::/64	MEDIA COMERCE
CORDOBA	Montelibano	192.168.53.0/24	2800:26c:14a:0350::/64	MEDIA COMERCE
CORDOBA	Lorica	192.168.54.0/24	2800:26c:14a:0360::/64	MEDIA COMERCE
CUNDINAMARCA	Funza	192.168.55.0/24	2800:26c:14a:0370::/64	ETB
CUNDINAMARCA	Ubate	192.168.56.0/24	2800:26c:14a:0380::/64	ETB
CUNDINAMARCA	Soacha	192.168.57.0/24	2800:26c:14a:0390::/64	ETB
CUNDINAMARCA	Zipaquirá	192.168.58.0/24	2800:26c:14a:03a0::/64	ETB
CUNDINAMARCA	Girardot	192.168.59.0/24	2800:26c:14a:03b0::/64	ETB
CUNDINAMARCA	Fusagasuga	192.168.60.0/24	2800:26c:14a:03c0::/64	ETB
CUNDINAMARCA	Chía	192.168.61.0/24	2800:26c:14a:03d0::/64	ETB
CUNDINAMARCA	Caqueza	192.168.62.0/24	2800:26c:14a:03e0::/64	ETB
CUNDINAMARCA	Villeta	192.168.63.0/24	2800:26c:14a:03f0::/64	ETB

TERRITORIAL	INSPECCION	SEGMENTO IPV4	SEGMENTO IPV6	OPERADOR
GUAJIRA	Maicao	192.168.65.0/24	2800:26c:14a:0410::/64	SKYNET
GUAJIRA	Barrancas	192.168.64.0/24	2800:26c:14a:0400::/64	SKYNET
GUAJIRA	Fonseca	192.168.66.0/24	2800:26c:14a:0420::/64	SKYNET
HUILA	Plata	192.168.67.0/24	2800:26c:14a:0430::/64	ETB
HUILA	Pitalito	192.168.68.0/24	2800:26c:14a:0440::/64	ETB
HUILA	Garzón	192.168.69.0/24	2800:26c:14a:0450::/64	ETB
MAGDALENA	Pivijay	192.168.70.0/24	2800:26c:14a:0460::/64	MEDIA COMERCE
MAGDALENA	Fundación	192.168.71.0/24	2800:26c:14a:0470::/64	MEDIA COMERCE
MAGDALENA	Plato	192.168.72.0/24	2800:26c:14a:0480::/64	MEDIA COMERCE
MAGDALENA	El Banco	192.168.73.0/24	2800:26c:14a:0490::/64	MEDIA COMERCE
MAGDALENA	Cienaga	192.168.74.0/24	2800:26c:14a:04a0::/64	MEDIA COMERCE
META	Granada	192.168.75.0/24	2800:26c:14a:04b0::/64	ETB
META	Puerto Lopez	192.168.76.0/24	2800:26c:14a:04c0::/64	ETB
META	Puerto Gaitan	192.168.77.0/24	2800:26c:14a:04d0::/64	ETB
META	Cumaral	192.168.78.0/24	2800:26c:14a:04e0::/64	ETB
NARIÑO	Tumaco	192.168.79.0/24	2800:26c:14a:04f0::/64	UNE
NARIÑO	La Union	192.168.80.0/24	2800:26c:14a:0500::/64	UNE
NARIÑO	Tuquerres	192.168.81.0/24	2800:26c:14a:0510::/64	UNE
NARIÑO	Ipiales	192.168.82.0/24	2800:26c:14a:0520::/64	ETB
NORTE DE SANTANDER	Salazar de las Palmas	192.168.83.0/24	2800:26c:14a:0530::/64	TELEFONICA
NORTE DE SANTANDER	Los Patios	192.168.84.0/24	2800:26c:14a:0540::/64	TELEFONICA
NORTE DE SANTANDER	Chinácota	192.168.85.0/24	2800:26c:14a:0550::/64	TELEFONICA
NORTE DE SANTANDER	Tibú	192.168.86.0/24	2800:26c:14a:0560::/64	ETB
NORTE DE SANTANDER	Ocaña	192.168.87.0/24	2800:26c:14a:0570::/64	ETB
NORTE DE SANTANDER	San José de Cúcuta	192.168.88.0/24	2800:26c:14a:0580::/64	ETB
PUTUMAYO	Puerto Asís	192.168.89.0/24	2800:26c:14a:0590::/64	SKYNET
PUTUMAYO	Orito	192.168.90.0/24	2800:26c:14a:05a0::/64	SKYNET
QUINDIO	Quimbaya	192.168.91.0/24	2800:26c:14a:05b0::/64	UNE
RISARALDA	Dosquebradas	192.168.92.0/24	2800:26c:14a:05c0::/64	UNE
RISARALDA	La Virginia	192.168.93.0/24	2800:26c:14a:05d0::/64	UNE
RISARALDA	Santa Rosa de Cabal	192.168.94.0/24	2800:26c:14a:05e0::/64	ETB
RISARALDA	Santa Rosa de Cabal	192.168.95.0/24	2800:26c:14a:05f0::/64	ETB
SANTANDER	Velez	192.168.96.0/24	2800:26c:14a:0600::/64	ETB

TERRITORIAL	INSPECCION	SEGMENTO IPV4	SEGMENTO IPV6	OPERADOR
SANTANDER	Puerto Wilches	192.168.97.0/24	2800:26c:14a:0610::/64	UNE
SANTANDER	Barbosa	192.168.98.0/24	2800:26c:14a:0620::/64	ETB
SANTANDER	Malaga	192.168.99.0/24	2800:26c:14a:0630::/64	ETB
SANTANDER	San Vicente de chucuri	192.168.100.0/24	2800:26c:14a:0640::/64	TELEFONICA
SANTANDER	Sabana de Torres	192.168.101.0/24	2800:26c:14a:0650::/64	MEDIA COMERCE
SANTANDER	Socorro	192.168.102.0/24	2800:26c:14a:0660::/64	TELEFONICA
SANTANDER	San Gil	192.168.103.0/24	2800:26c:14a:0670::/64	ETB
SUCRE	Tolu	192.168.104.0/24	2800:26c:14a:0680::/64	MEDIA COMERCE
SUCRE	San Marcos	192.168.105.0/24	2800:26c:14a:0690::/64	MEDIA COMERCE
SUCRE	Majagual	192.168.106.0/24	2800:26c:14a:06a0::/64	MEDIA COMERCE
TOLIMA	Libano	192.168.107.0/24	2800:26c:14a:06b0::/64	ETB
TOLIMA	Mariquita	192.168.108.0/24	2800:26c:14a:06c0::/64	ETB
TOLIMA	Chaparral	192.168.109.0/24	2800:26c:14a:06d0::/64	UNE
TOLIMA	Melgar	192.168.110.0/24	2800:26c:14a:06e0::/64	ETB
TOLIMA	Espinal	192.168.111.0/24	2800:26c:14a:06f0::/64	ETB
URABA - APARTADO	Turbo	192.168.112.0/24	2800:26c:14a:0700::/64	SKYNET
VALLE DEL CAUCA	Cartago	192.168.113.0/24	2800:26c:14a:0710::/64	UNE
VALLE DEL CAUCA	Buenaventura	192.168.114.0/24	2800:26c:14a:0720::/64	UNE
VALLE DEL CAUCA	Tuluá	192.168.115.0/24	2800:26c:14a:0730::/64	ETB
VALLE DEL CAUCA	Buga	192.168.116.0/24	2800:26c:14a:0740::/64	ETB
VALLE DEL CAUCA	Roldanillo	192.168.117.0/24	2800:26c:14a:0750::/64	UNE
VALLE DEL CAUCA	Sevilla	192.168.118.0/24	2800:26c:14a:0760::/64	ETB
VALLE DEL CAUCA	Palmira	192.168.119.0/24	2800:26c:14a:0770::/64	ETB

SEDES SIN SOPORTE DE IPV6 EN RED DEL OPERADOR DE ULTIMA MILLA

AMAZONAS	Leticia	172.16.0.0/23	2800:26c:14a:a000::/64	SKYNET
CESAR	Curumani	192.168.45.0/24	2800:26c:14a:02d0::/64	SKYNET
CESAR	Codazzi	192.168.42.0/24	2800:26c:14a:02a0::/64	TELEFONICA
CESAR	Aguachica	192.168.43.0/24	2800:26c:14a:02b0::/64	TELEFONICA
GUAJIRA	Maicao	192.168.65.0/24	2800:26c:14a:0410::/64	SKYNET
GUAJIRA	Barrancas	192.168.64.0/24	2800:26c:14a:0400::/64	SKYNET
GUAJIRA	Fonseca	192.168.66.0/24	2800:26c:14a:0420::/64	SKYNET
PUTUMAYO	Puerto Asís	192.168.89.0/24	2800:26c:14a:0590::/64	SKYNET
PUTUMAYO	Orito	192.168.90.0/24	2800:26c:14a:05a0::/64	SKYNET
SANTANDER	San Vicente de chucuri	192.168.100.0/24	2800:26c:14a:0640::/64	TELEFONICA