PROPUESTA DE TRANSICIÓN DE SERVICIOS DE IPv4 A IPv6 PARA LA RED DE DATOS CABLEADA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL SAN MIGUEL DE IBARRA

Autor: Mera Gabriela

Director: MSc. Cuzme Fabián

***Resumen*— El protocolo de internet (IP, por sus siglas en inglés) versión cuatro, permite que los dispositivos tengan acceso a la Internet. Este recurso, con el evidente avance tecnológico que se experimenta en la actualidad, se está agotando significativamente. IPv4 dispone de alrededor de cuatro mil millones de direcciones y debido al gran surgimiento de Internet, se está terminando día a día. Por esta razón, el grupo de Trabajo de Ingeniería de Internet IETF crea el nuevo protocolo IPv6, como solución a la escasez de direcciones.**

El nuevo protocolo IPv6, permite direccionar alrededor de trescientos cuarenta sextillones de dispositivos, que frente a IPv4 es incomparable. El nuevo protocolo está siendo ya implementado en las redes y lo que se espera, es que coexista con IPv4 hasta que todo sea manejado con IPv6. Entonces, se necesita de un mecanismo de transición que permita manejar los dos protocolos, en tanto que IPv4 siga existiendo.

En Ecuador, el Ministerio de Telecomunicaciones y Sociedad de la información, mediante acuerdo ministerial No. 007-2012, ejecutó un plan de acciones para que se lleve a cabo una transición ordenada y coexistente de IPv4 a IPv6 con operadores, ISP (Proveedor de Internet), entidades y organismos del sector público y privado. Es por ello, que en sus plataformas electrónicas debe empezar a generarse tráfico IPv6. De acuerdo a lo establecido, surgió la propuesta para el Gobierno Autónomo Descentralizado Municipal de San Miguel de Ibarra, de empezar a utilizar este nuevo protocolo en los servicios WEB y Correo Electrónico.

El estudio de este proyecto, consiste en desarrollar un modelo de transición que permita utilizar un mecanismo para la coexistencia de los protocolos IPv4 e IPv6, basándose en las acciones que se encuentran en el acuerdo ministerial. Para ello, se va a realizar un análisis de la situación actual de la empresa, para verificar el soporte del protocolo IPv6 en cuanto a hardware, software, así como también de las aplicaciones y servicios.

Para finalizar, se realiza la configuración en equipos y servicios con un simulador de red, que permita evidenciar la coexistencia de los dos protocolos.

Palabras claves— IP, WEB, IPSec.

I. INTRODUCCION

La internet, conocido también como la red de redes, en la actualidad, es uno de los servicios más importantes que permiten conectar a varios usuarios ubicados en cualquier parte del mundo, para acceder a la información que necesite cualquier persona, realizar pagos electrónicos, consultar valores a pagar, chatear, observar imágenes, escuchar música, descargar o subir videos entre otros.

La internet, conocido también como la red de redes, en la actualidad, es uno de los servicios más importantes que permiten conectar a varios usuarios ubicados en cualquier parte del mundo, para acceder a la información que necesite cualquier persona, realizar pagos electrónicos, consultar valores a pagar, chatear, observar imágenes, escuchar música, descargar o subir videos entre otros.

El protocolo IP utilizado para establecer la comunicación es IPv4, que es una dirección de 32 bits de longitud y que permite contar con 4,294,967,296 de direcciones únicas, sin embargo, este direccionamiento está siendo reemplazado por el protocolo IPv6, debido a que en él se manejan direcciones de 128 bits dando lugar a 340.282.366.920.938.463.463.374.607.431.768.211.456 direcciones válidas. En consecuencia, las redes están ya migrando al nuevo protocolo IPv6 debido al crecimiento masivo de las redes como lo es IoT (Internet de las Cosas).

II. ANÁLISIS IPV4 E IPV6

A. LIMITACIONES DE IPV4

- **Agotamiento de direcciones IP:** Aunque se manejen 4.294.967.296 millones de direcciones, no es suficiente para la creciente demanda de redes que existen hoy en día. Por esta razón se ha utilizado NAT, para asignar una dirección pública a varias privadas, es un buen método para poder reutilizar las direcciones privadas, pero entonces va a conllevar a que en las comunicaciones se produzcan cuellos de botella.

- **Soporte para la entrega de datos en tiempo real:** Aplicaciones nuevas como video y audio, requieren QoS, por ello, se necesita una arquitectura flexible que permita afrontar el reto que supone la movilidad de sus usuarios.
- **Requerimientos de Seguridad a nivel IP:** Se utiliza para garantizar entrega de paquetes, y la norma es IPsec. En Ipv4 este campo es opcional, mientras que en IPv6 es obligatoria.
- **Expansión en la tabla de enrutamiento de Internet:** Con el aumento de nodos o servidores que están conectados a Internet, aumentan las rutas de red por lo que los routers deben manejar tablas de enrutamiento con mayor información y esto produce un aumento de recursos de la red en cuanto a memoria y procesamiento.

B. *CARACTERÍSTICAS DE IPV6*

- **Mayor espacio para direccionamiento de redes:** El protocolo IPv6 tiene una longitud de 128 bits para direcciones tanto de origen como de destino, en otras palabras 2128 posibles direcciones, a diferencia de Ipv4 que tiene 232 direcciones.
- **Direccionamiento más eficiente y jerárquico:** Permite que los routers principales dirijan el tráfico de manera más rápida e incluso que sus tablas de enrutamiento sean mucho más pequeñas.
- **Nuevo formato de cabecera:** Se desarrolló para que los routers realicen un consumo menor de procesamiento al manejar la información.
- **Configuración de direcciones:** Con IPv6 se puede simplificar la configuración en los hosts, permite el uso de un servidor DHCP para las direcciones con estado, y de igual manera se admite también las direcciones sin estado que son las que no utilizan un servidor DHCP.
- **QoS:** Esto permite darle cierto tipo de prioridad a un tráfico de datos, mediante un campo en la cabecera de IPv6 (Class Traffic), permitiendo que los routers proporcionen tratamiento especial a un flujo determinado de paquetes.
- **Seguridad:** en IPv6 es obligatorio el campo IPSEC, que permite seguridad de encriptación a la carga útil y autentificación de la fuente de comunicación.
- **Interacción con nodos vecino:** Utilizando el protocolo Neighbor Discovery que Ipv6 dispone es capaz de manejar una serie de mensajes que va a permitir la interacción con los nodos vecinos.

C. *DIRECCIONAMIENTO IPv6*

IPv6 extiende su dirección de 32 a 128 bits, que por el momento es suficiente para cubrir la gran demanda de usuarios en el futuro. Cuatro bits, representan un dígito hexadecimal, por lo tanto, una dirección IPv6 consta de 32 valores hexadecimales. A continuación, se va a presentar un ejemplo para ayudar a la comprensión del mismo en la Figura 1: (CISCO, 2013)

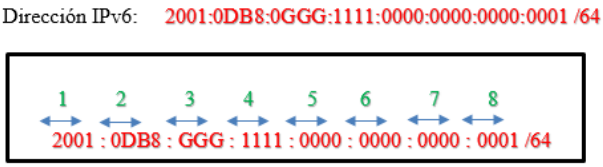

Figura 1: *Representación de una dirección IPv6 en octetos*
Fuente: Elaboración propia

D. *TIPO DE DIRECCIONES EN IPV6*.

Cada dirección se compone por 128 bits y existen tres tipos de direcciones en IPv6 y son:

- **Unicast:** identifican a una interfaz única, esto quiere decir, que un paquete destinado a una dirección unicast será entregado únicamente a la interfaz identificada con dicha dirección. (CISCO, 2013)
- **Anycast:** estas direcciones identifican a un conjunto de interfaces, de tal manera que un paquete enviado a una dirección anycast será entregado a un miembro que pertenezca a este grupo, que generalmente es el más cercano según la distancia asignada en el protocolo de encaminamiento.
- **Multicast:** al igual que las direcciones anycast, con la diferencia de que un paquete que sea enviado a una dirección multicast, es entregado a todas las interfaces del grupo. Las direcciones de broadcast no existen en IPv6, en reemplazo se han creado este tipo de direcciones. (LACNIC, 2012)

E. *PROTOCOLO IPSec*

Es un estándar que proporciona seguridad de la información, caracterizado por ser potente y flexible. Se ha creado debido a las falencias que tiene el protocolo IP que es la seguridad, esto permite que las redes actuales accedan a aplicaciones críticas como es la de manejar información que involucre transacciones empresariales. Del mismo modo, proporciona seguridad independientemente de alguna aplicación, de tal forma que lo convierte en una pieza imprescindible de las redes actuales.

Por lo tanto, IPsec se ha convertido en un componente básico de las redes IP, por ello se puede considerar una tecnología bastante madura para implantarla en redes cuya prioridad sea la seguridad. Si se habla de seguridad se refiere a la confidencialidad y la integridad de los datos que para muchas compañías es un requisito fundamental que sus redes deben proporcionar a los clientes.

IPSec se compone de:

- Dos protocolos de seguridad: IP Authentication Header (AH) e IP Encapsulating Security Payload (ESP) que proporcionan mecanismos de seguridad para proteger el tráfico IP.
- Un protocolo de gestión de claves: Internet Key Exchange (IKE) que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

TABLA I

IPv4	IPv6
Las direcciones tanto de origen como destino son de 32 bits de longitud (4 Bytes)	Las direcciones de origen y destino son de 128 bits de longitud (16 Bytes).
IPSec es un protocolo opcional.	IPSec es una obligatoriedad.
No existe identificación de paquetes QoS que manejen los routers en sus cabeceras.	Con la utilización del campo flow label, se tiene entendido que se está manejando QoS
La fragmentación de un paquete lo realiza el host como el router, que produce retardos.	La fragmentación en IPv6 lo realiza únicamente el host, porque el paquete es procesado en el nodo final de destino.
Su cabecera tiene un cheksum.	Es eliminado el campo cheksum.
Se emplean solicitudes ARP para resolver direcciones IPv4, en una dirección de capa física	Las tramas ARP, son reemplazadas con mensajes multicast neighbor Discovery
Usan registros A, para la resolución de direcciones IPv4 a dominios.	Usan registros AAAA, para la resolución de las direcciones IPv6.
Se utilizan las direcciones Broadcast, para enviar un paquete a todos los nodos de las subredes.	Se utiliza una dirección multicast para poder enviar la información a los nodos de un ámbito local del vínculo.
Se debe configurar las direcciones de manera manual o utilizando DHCP.	No requiere de configuraciones manuales o utilizar DHCP.

Fuente: (Nuñez, 2009)

F. COMPARACIÓN DE IPV4 CON IPV6.

En la Tabla I, se explican las principales diferencias de protocolos IPv4 e IPv6

G. MECANISMOS DE TRANSICIÓN

La transición de IPv4 a IPv6 no será posible de realizarla de un día para otro, por ello, es importante buscar alguna solución para que los dos protocolos puedan convivir un tiempo mientras todas las redes migren a IPv6 completamente. Por ejemplo, tratar de realizar actualizaciones de software en los nodos IPv4 actuales y definir que equipos son los que se debería cambiar para que manejen IPv6.

Dual Stack: Es el método más utilizado porque utiliza un nodo de doble pila IPv6/IPv4 y puede comunicar tanto un nodo IPv4 como un nodo IPv6. Para conseguirlo, se debe configurar los dos tipos de direccionamiento a cada uno de ellos. Este mecanismo permite activar o desactivar una de las pilas, por ello va a funcionar de tres maneras:

- Si está activada la pila IPv4, se comportará como un solo nodo IPv4.
- Si está activada la pila IPv6, se comportará como un solo nodo IPv6.
- Cuando estén activadas las dos pilas funcionará con los dos protocolos.

Recordar que IPv4 utiliza para configurar las direcciones utiliza DHCP o la forma estática, mientras que IPv6 utiliza configuración estática o DHCPv6. De la misma manera, el DNS, debe ser capaz de resolver los nombres de las direcciones en IPv4 como en IPv6, por lo tanto, debe manejar un nodo IPv6/IPv4, como se indica en la Figura 2.

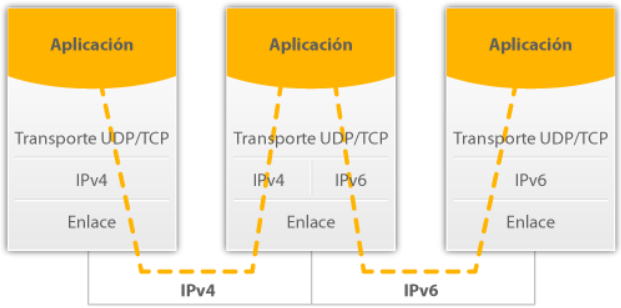

Figura 2: *Dual Stack*
Fuente: Recuperada de http://portalipv6.lacnic.net/dual-stack-o-pila-doble/

Túneles. El mecanismo túnel es utilizado para el transporte de paquetes IPv6 utilizando una infraestructura IPv4. Además, computadoras aisladas IPv6 pueden establecer sesiones IPv6 extremo a extremo utilizando IPv4 como la capa de transporte. Los túneles tienen como finalidad encapsular paquetes IPv6 dentro de paquetes IPv4, que luego serán encapsulados a un nodo destino IPv4 sobre una red que maneje IPv4.

Luego el nodo destino realizará la desencapsulación y extraerá los paquetes IPv6. Tomar en cuenta que, para poder aplicar este mecanismo, es necesario que los nodos extremos del túnel soporten Pila Dual. (Network Information Center México S.C., 2010)

Este mecanismo puede ser dividido en dos grupos:

Túneles manuales: Aquellos que para transportar un paquete IPv6 deben encapsularse en un paquete IPv4, por tanto, son túneles punto a punto que deben ser configurados manualmente. La configuración de túneles entre host y routers se puede realizar de las siguientes maneras:

- **Host a Host:** los host IPv6/IPv4 que están conectados con infraestructura IPv4, pueden encapsular paquetes IPv6 entre ellos mismos.
- **Router a Host:** los routers IPv6/IPv4 pueden encapsular paquetes IPv6 a su destino final.

***Túneles automáticos**:* Los nodos IPv6 pueden utilizar direcciones que sean compatibles con IPv4, con IPv6 o 6to4, es un túnel dinámico de paquetes IPv6 sobre una infraestructura de enrutamiento IPv4.

La configuración de túneles entre host y routers se puede realizar de las siguientes maneras:

- **Router a Router:** utiliza el túnel automático en donde los routers IPv6/IPv4, separados por una infraestructura IPv4 pueden encapsular paquetes IPv6 entre ellos mismos.
- **Host a Router:** Un host IPv6/IPv4 puede encapsular paquetes IPv6 a un router intermedio IPv6/IPv4 al cual se puede acceder mediante la infraestructura de enrutamiento IPv4.

Ahora se van a describir las tecnologías del túnel automático:

- **Túnel 6to4:** especifica un mecanismo para que los sitios IPv6 puedan comunicarse entre sí a través de la red IPv4 sin establecer configuraciones explícitas del túnel. La red IPv4 se comporta como una capa de enlace punto a punto de unidifusión en donde dominios de IPv6 se comunican a través de routers 6to4 llamados puertas de enlace 6to4.

Este método utiliza el prefijo de dirección global: 2002:WWXX:YYZZ::/48, WWXX:YYZZ: corresponde al ID de agregación del siguiente nivel de una dirección global. En la Figura 3 se indica la infraestructura de un túnel 6to4.

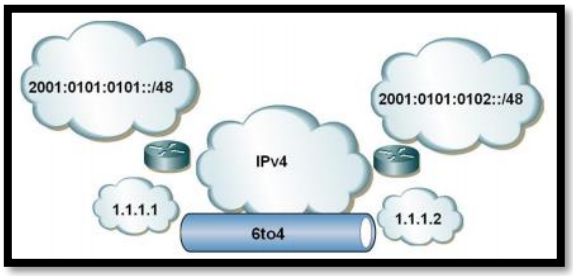

Figura 3: *Túnel 6to4*
Fuente: (Cedeño., 2013)

- **Túnel 6over4:** se lo llama también túnel de multidifusión de IPv4, donde 6over4 admite la comunicación entre nodos IPv6 e IPv4 a través de infraestructura IPv4, con capacidad de multidifusión. Para el buen desempeño de 6over4, la infraestructura IPv4 debe estar habilitada para multidifusión IPv4.

En este mecanismo, se debe crear un enlace virtual a través de un grupo IPv4 multicast con ámbito local – organizacional, recordando que el mecanismo multicast en IPv4 es opcional. Por tanto, las direcciones IPv6 multicast mapean direcciones IPv4 multicast para ejecutar. Para el encaminamiento entre IPv6 y el dominio 6over4 es suficiente configurar un router al menos en una de sus interfaces. (Cedeño., 2013)

En la Figura 4 se indica la infraestructura del túnel 6over4

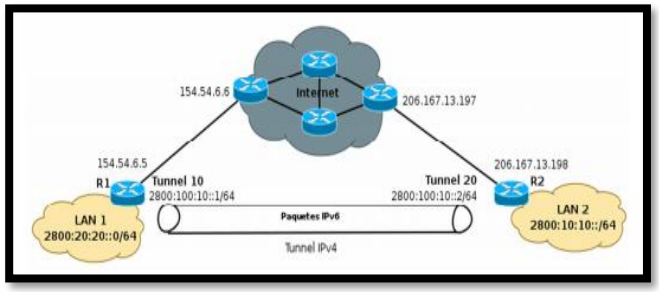

Figura 4: Túnel Teredo

Fuente: (Palet, 2007)

- **Túnel Teredo:** fue diseñado para garantizar las conectividades IPv6 de los nodos dual stack, localizados detrás de los dispositivos NAT sobre dominios IPv4, es decir, que define el encapsulamiento de paquetes IPv6 en datagramas UDP IPv4 para ser dirigidas a través de dispositivos NAT y en internet IPv4. En la Figura 5 se indica un cliente se comunica a través de un túnel Teredo con hosts IPv6 nativos. (Palet, 2007)

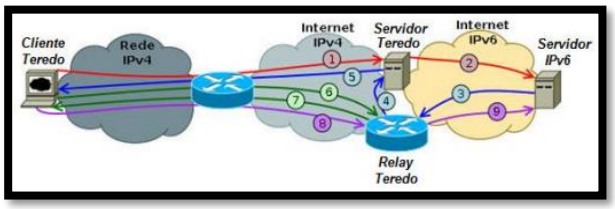

Figura 5: *Túnel Teredo*

Fuente: (Palet, 2007)

- **ISATAP:** Permite crear túneles IPv4/IPv6 de forma automática dentro de una infraestructura IPv4. Con respecto a 6over4 tiene algunas ventajas, por ejemplo, no necesita utilizar direcciones multicast IPv4 y soluciona problemas en redes remotas, como la baja escalabilidad en la agregación.

***Traducción*.** Este método permite un enrutamiento de forma transparente de la comunicación entre nodos que soporten ya sea la versión cuatro, la versión 6 o el mecanismo de doble pila. Operan de distintas maneras o capas, puede ser, traduciendo cabeceras IPv4 en cabeceras IPv6 y viceversa, conversiones en las direcciones o el intercambio del tráfico TCP a UDP (LACNIC, 2012)

H. SERVIDORES

Un servidor es un equipo que es parte de una red y provee de servicios a cualquier otro cliente. Debe cumplir

características en cuanto a hardware y software, además ser especializada con altas capacidades de proceso que permita almacenar varias aplicaciones y que éstas sean accesibles por parte de los usuarios de una red, si así lo requieren. (APR, 2016)

Tipos de Servidores. Un servidor puede ser dedicado o compartido. En el caso de ser dedicado, éste va a prestar todos sus recursos para atender peticiones que un cliente realice y si es compartido, va a ser utilizado para trabajar localmente en una red en el que se lo coloque. (APR, 2016)

Existen algunos tipos de servicios como:

- Base de Datos (BBD)
- DNS
- DHCP
- FTP
- Mail (Correo/mensajería)
- Proxy
- SSH
- Transmisión Multimedia
- Telnet
- Web

En este caso se estudiarán los servicios que se proponen para la transición de IPv4 a IPv6 que son: WEB y correo electrónico. La elección se ha realizado tomando en cuenta la disponibilidad de funcionamiento de los servicios que brinda a los usuarios internos como externos.

- **Servidor WEB**. La palabra WEB es asociada a Internet, debido a que existen navegadores disponibles en cualquier dispositivo con acceso a la red para acceder a estos sitios que ofrecen diferente tipo de información como: archivos, música, videos entre otros. (Corporación Digital Colombia, 2016)

  Por lo tanto, un servidor web es un lugar que alberga cualquier tipo de información que el usuario requiera por medio de un navegador que realiza el intercambio de información entre el usuario y el servidor mediante HTTP que generalmente en la navegación web usa el puerto 80 y se basa en el modelo cliente servidor y de igual manera HTTPS con el puerto 443. (Herramientas WEB, 2013)
- **Servidor de correo electrónico**. El mail o correo electrónico, es el sistema que permite enviar, recibir y gestionar mensajes de usuarios o clientes, unos a otros conectados en una misma red o usuarios de otras redes como el Internet. El intercambio de estos mensajes se realiza de forma asíncrona, para lograr la efectiva comunicación se necesita de algunos protocolos que son: POP, IMAP y SMTP. Estos protocolos proporcionan la interacción (transmisión y recepción) de correo electrónico entre ordenadores y servidores, con funciones características o específicas entre cada uno.

III. PLANTEAMIENTO DEL MODELO DE TRANSICIÓN Y ANÁLISIS DE SEGURIDAD EN IPV6

Se diseña un modelo de transición en el cual se puedan implementar las acciones estipuladas en el plan maestro que se encuentra en el acuerdo ministerial, que permita realizar una transición ordenada y coexistente de los dos protocolos. Así mismo, analizar los puntos críticos en los cuales se debería implementar el protocolo IPsec que permitan brindar seguridad a la red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra.

A. PLAN DE ACCIÓN PROPUESTO POR EL MINISTERIO DE TELECOMUNICACIONES (MINTEL)

Aquí se explican los lineamientos generales que el MINTEL ha propuesto para que se lleve a cabo la transición de IPv4 a IPv6. En la Figura 6 se explica un modelo generalizado de la metodología empleada.

Figura 6: *Transición y Coexistencia de IPv4 e IPv6 en Ecuador*
Fuente: Recuperado de http://www.telecomunicaciones.gob.ec/

B. MODELO DE TRANSICIÓN DE IPV4 A IPV6 PARA LA RED DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL SAN MIGUEL DE IBARRA

Para poder llevar a cabo la transición de IPv4 a IPv6 en esta empresa, es necesario que se ajusten las actividades de acuerdo al plan de transición propuesto por el MINTEL, es así como se ha diseñado el modelo de transición para el Gobierno Autónomo Descentralizado Municipal de San Miguel de Ibarra en el que se incluyen las actividades realizadas en fases.

1. FASE I: Planificación.

En esta fase es importante identificar y establecer los planes a futuro para la adopción del protocolo IPv6, determinando el recurso humano requerido para la delegación de funciones y responsabilidades en cada área y llevar a cabo el proceso de transición y coexistencia del protocolo IPv4 e IPv6.

1.1. ***Selección del personal***. Se debe elegir a los ingenieros que trabajan en el departamento TIC's de la entidad, para cumplir con todas las actividades que este proyecto demanda.

1.2. ***Capacitación y entrenamiento.*** Se debe realizar al personal de TIC's del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, con la finalidad de llevar a cabo el proyecto con responsabilidad que se requiere.

1.3. ***Cronograma de actividades.*** Esto va a permitir controlar que se realicen las actividades dispuestas en cada fase. Se debe tratar de establecer un periodo aproximado de tiempo en el que se culminará este proceso.

2. *FASE II: Diseño*

Esta etapa tiene como objetivo realizar el análisis actual de la empresa, identificando las áreas en donde se va a implementar IPv6, la topología de red, entre otros, para verificar el soporte del protocolo IPv6, de la misma manera seleccionar los servicios y aplicaciones que se van a manejar con el nuevo protocolo.

2.1. Análisis de la situación actual.

Se realiza un estudio completo a topología física, lógica de la red de datos de la entidad.

- ***Cableado Horizontal o de distribución***

  Se utiliza cable UTP Categoría 6, permite interconectar el backbone con las áreas de trabajo. Para los equipos terminales, se tienen cajetines sobrepuestos para tomas simples y dobles, con tapas de protección para las salidas RJ-45 para voz y datos.

  La interconexión del cableado horizontal entre el edificio principal y el edificio antiguo al correspondiente backbone, se encuentra sobre el cielo falso utilizando las bandejas metálicas y para los puntos de las áreas de trabajo está distribuido con canaletas.

- ***Cableado Vertical o Backbone***

  Este cableado cumple la función de interconectar el cableado de distribución de cada uno de los diferentes pisos del edificio principal con la utilización de fibra óptica y cable UTP con cada uno de los equipos de comunicación que se encuentran en el Data Center.

  El backbone del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra se interconecta con los equipos de comunicación que se sitúan en: el edificio antiguo, la dirección de Turismo y la dirección de Cultura mediante fibra óptica, éstos llegan al área de distribución principal MDF, ubicada en el departamento de Gestión de Tecnologías de la Información edificio principal. Las áreas de distribución secundarias SDF se encuentran en: el edificio antiguo primera planta, en la primera planta de dirección de turismo y en la dirección de cultura en la tercera planta.

  La fibra óptica es de tipo multimodo para la conexión entre las dependencias externas del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra y monomodo entre entidades independientes. Presenta una certificación ISO 9001 y cumple con las especificaciones ISO/IEC 11801 certificación Tier l en fibra óptica.

- Áreas de trabajo.

  Los dispositivos terminales como son computadoras, impresoras y teléfonos utilizan patch cord UTP categoría 6/Clase E, con conectores RJ-45 a los dos lados cumpliendo con las normas del cableado estructurado EIA y TIA.

- **Análisis de la infraestructura lógica de la red de datos:**

La LAN del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, dispone un direccionamiento IPv4 Clase B (172.X.X.X) con una máscara de red 255.255.248.0 que por el momento satisface la capacidad de usuarios que maneja la entidad y mediante el equipamiento existente garantiza la disponibilidad de sus servicios, además permite a la red un gran crecimiento y escalabilidad.

Para una mejor administración de la red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, se ha distribuido la red en VLAN's.

- **Topología Física de la Red de Datos del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra**

Para conocer y determinar los equipos que soportan el protocolo IPv6, es importante conocer la situación actual de la infraestructura física. En la actualidad, la red es capaz de transmitir y receptar señales de voz, datos y video, acceso a Internet y también permite la compartición de archivos.

De la misma manera internamente posee servicios como correo interno institucional, consultas de los correspondientes sistemas prediales, sistemas administrativos, financieros, entre otros servicios que favorecen al desempeño de las actividades de la entidad. Todo se maneja con el protocolo IPv4, más no se tiene ninguna relación de convivencia con el protocolo IPv6.

De la misma manera, se puede ver la conexión del switch core con fibra óptica con el enlace del proveedor Telconet, que proporciona un ancho de banda de 18 Mbps al Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra

También la conexión de los servidores físicos albergados en el Data Center. Aunque en este proyecto no se tomen en cuenta los enlaces inalámbricos, se los puede visualizar y son los enlaces conectados de color rojo. En la Figura 7, se describe la estructura física de la red local de datos, en la cual se pueden visualizar las conexiones de los enlaces LAN que van hacia los edificios de las dependencias tanto internas como externas.

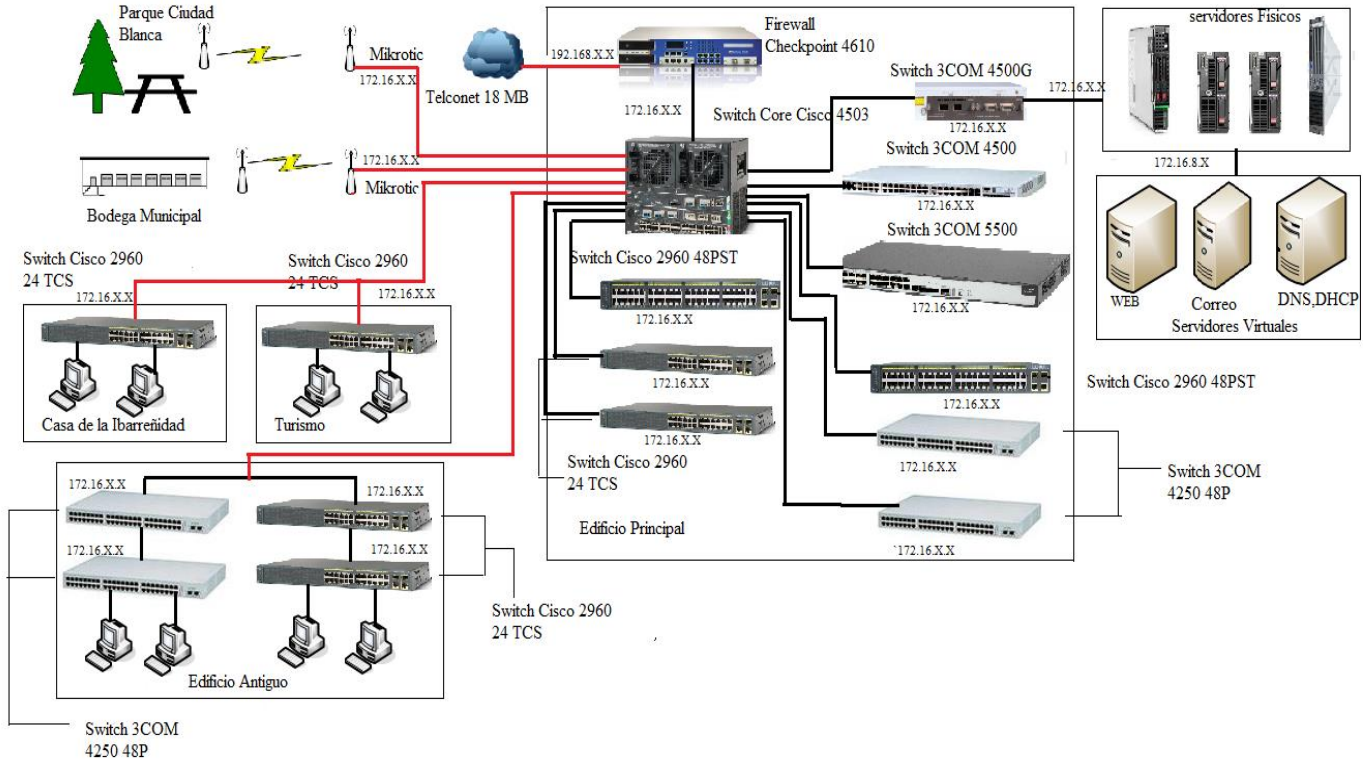

Figura 7: *Topología física de la red de datos cableada del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra*
Fuente: Departamento de Gestión de Información

2.2. Análisis de Hardware o Equipamiento de la Red

Se deben analizar los equipos para determinar si tienen el soporte IPv6, de los cuales se deben profundizar en los siguientes aspectos:

- ***Tiempo de uso/ años:*** Los equipos de red, tienen una vida útil de tres años, es decir su funcionamiento va a ser óptimo en este tiempo, pero no deben sobrepasar los diez años de uso. (Universidad Técnica Particular de Loja, 2010)
- ***Sistema operativo IOS:*** Las versiones desde 12.0()TS o T en adelante, tienen el soporte IPv6. (CISCO, 2016)

Por lo tanto, en el inventario realizado, los equipos switch marca 3COM, deben ser sustituidos, por no soportar las características para el buen desempeño de la red con IPv6. El equipamiento CISCO, funciona correctamente y sus IOS son compatibles con IPv6. En caso de tener un IOS, distinto se recomienda actualizarlo a versiones superiores a la 12.0()TS.

En cuanto a los servidores físicos, se puede decir que están actualizados los sistemas operativos que albergan a los servidores virtuales. Po lo tanto el análisis propio de cada sistema operativo se analiza en el siguiente punto.

El inventario en cuanto a hardware, permitirá a la presente administración de la red conocer los equipos aptos para la implementación del nuevo protocolo, o para actualizaciones en cualquier equipo que no disponga de las características que se ha analizado en este apartado.

2.3. Análisis de Software de los Equipos.

Se ha realizado un análisis en cuanto a los sistemas operativos que manejan los servidores virtuales y las computadoras de los usuarios que tiene el Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, en la que la mayoría de usuarios finales utilizan en

sus computadoras Windows 7 y Windows 8, y tienen el soporte para IPv6.

2.4. Selección de los servicios y aplicaciones seleccionadas para IPv6

Como se ha propuesto la transición de IPv4 a IPv6 para los servicios WEB y Correo Electrónico, se ha explicado ya la importancia que tienen para la entidad por lo tanto tener en consideración las siguientes recomendaciones:

- ✓ Se debe tener en cuenta de que dependen los otros servicios, por ejemplo, en el caso de servidor WEB, depende del servidor de base de datos, por lo tanto, este servicio también debe tener compatibilidad con IPv6.
- ✓ Debe existir la compatibilidad IPv4/IPv6, ya que algunos servicios no van a poder manejar los dos protocolos, por eso, hasta que adopten IPv6 elegir un mecanismo que permita mantener coexistencia entre estos dos protocolos.

2.5. Pool de direcciones IPv6.

Debe realizarse el pedido al proveedor de servicios Telconet. Este ISP, actualmente maneja y permite tener direccionamiento IPv6, el administrador de la red, debe realizar el trámite requerido para la asignación de un bloque IPv6. En caso de que no tuvieran este soporte, existe el trámite directo en la página de LACNIC: *http://www.lacnic.net/web/lacnic/ipv6-end-user*.

2.6. Análisis del protocolo de seguridad IPsec para IPv6.

IPsec (Internet Protocol Security), es un estándar creado por la IETF que permite proporcionar niveles de seguridad a la capa de red IP y a otros protocolos de capas superiores como TCP, UDP, entre otros. IPsec tiene soporte para IPv4 como para IPv6, pero en Ipv4 el uso no es obligatorio, mientras que para IPv6 está integrado y su uso es obligatorio.

Los principales servicios de seguridad que IPsec proporciona son:

- Integridad: Aquellos paquetes que no han sido cambiados o modificados en el trayecto de la comunicación.
- Confidencialidad: Se garantiza que el contenido de los paquetes solo sea conocido tanto por el emisor y por el receptor.
- Autenticidad: Se dice que el emisor del mensaje, es quien dice ser.

Para la implementación de este protocolo IPsec en la red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, se va a realizar utilizando ESP modo túnel. Es importante considerar que este protocolo se puede implementar en usuarios finales, en servidores o como en este caso que será implementado en los gateways de los switches. Para una mejor comprensión de la aplicación de este protocolo se va a detallar en las pruebas de funcionamiento que se han realizado para la red del municipio de Ibarra.

SSL, de la misma forma es el protocolo de seguridad que se implementa en las comunicaciones de la entidad, pero frente a IPsec, ¿cuál sería el más eficaz? Pues se van a determinar las características más importantes en la Tabla II.

Tabla II

Características	**SSL**	**IPsec**
Aplicaciones	Habilitadas en web, uso compartido de archivos, correo electrónico	Soportado para todas las aplicaciones IP.
Cifrado	En la escala de moderado a seguro debido a la longitud de clave de 40 a 256 bits.	En la escala de seguro, porque la longitud de claves es de 56 a 256bits.
Autenticidad	En la escala moderada, es unidireccional o bidireccional.	En la escala segura, debido a autenticación bilateral mediante secretos compartidos o con certificados digitales.
Complejidad de Conexión	En la escala baja porque se requiere de un navegador Web.	En la escala media debido a que puede resultar complicado sin los suficientes conocimientos técnicos.
Opciones de conexión	Cualquier dispositivo se puede conectar	Ciertos dispositivos con configuración específica

Fuente: Recuperado de: http://ecovi.uagro.mx/ccna4/course/module7/7.4.2.4/7.4.2.4.html

Cuando la seguridad representa un problema, IPsec es la mejor opción. Si el soporte y la facilidad de implementación son los principales problemas, considerar utilizar SSL. Pero en este proyecto se utilizará IPsec para verificar el funcionamiento con el protocolo IPv6.

2.7. ELECCIÓN DEL MECANISMO MÁS EFICIENTE PARA LA TRANSICIÓN DE IPV4 A IPV6 PARA LA RED DEL GOBIERNO AUTÓNOMO

DESCENTRALIZADO MUNICIPAL SAN MIGUEL DE IBARRA.

Es importante recalcar, que la transición de IPv4 a IPv6, para los ISP's y las empresas deben realizarla gradualmente y de la misma manera se debe mantener la interoperabilidad si esta llegara a efectuarse. Es por ello que se busca un mecanismo de transición que permita preservar las grandes inversiones que se han realizado en redes IPv4, y los mecanismos que se han revisado en el capítulo II permiten que las redes IPv4 con IPv6 mantengan interconexión entre ellas.

La migración de IPv4 a IPv6, puede ser complejo en grandes organizaciones, pero utilizando varias estrategias o mecanismos de convivencia van a ayudar en este proceso de transición. El objetivo de que este proceso se llegara a realizar, es con la finalidad de que los costos de transición y el impacto que produzca en una organización o empresa sean mínimos.

Para explicar las ventajas y desventajas de cada uno de los mecanismos estudiados, se va a presentar la Tabla III (comparativa) de cada uno de ellos para una correcta selección de transición:

TABLA III

MECANISMOS DE TRANSICIÓN

	Ventajas	Desventajas
Dual Stack	• Fácil de implementar. • Solución inmediata más accesible. • No hay necesidad de traducción ni encapsulamiento • Si falla la red IPv4, estará disponible la IPv6, y viceversa.	• Se debe mantener dos redes. • No hay reducción de demanda de direcciones IPv4.
Túneles	• Soportan varias plataformas como CISCO, Linux, entre otros.	• Se requieren conocer las dos direcciones IPv4 (origen y destino), las dos direcciones IPv6 (origen y destino), para la encapsulación. • Se necesita implementar dual Stack en cada uno de los puntos del túnel. • Requieren mayor configuración que la de los otros mecanismos. • Si se deja de manejar IPv4, esta infraestructura de red deberá migrar desde cero a IPv6.
Traducción	• Brinda escalabilidad a la red. • Permite el acceso a las dos redes en el caso de que un dispositivo IPv4 se quiera comunicar con un IPv6 y viceversa.	• Se tienen los mismos problemas que NAT en IPv4. • Produce cuellos de botella. • Se pierden los beneficios de IPv6. • Tiene cierta incompatibilidad con algunas aplicaciones.

Fuente: (Cedeño., 2013)

Después de haber identificado ventajas y desventajas entre de los mecanismos de transición, se va a elegir el que permita que se ajuste a las características de la red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra. Es por eso, que se va a elegir el mecanismo doble pila o Dual Stack, debido a que permite implementar el protocolo IPv6 sobre una red de infraestructura IPv4.

Otros mecanismos que se van a utilizar son el NAT64 y el DNS64. Cuando la red es IPv6 nativa y necesita llegar a sitios que son sólo IPv4 se realiza una traducción usando NAT, mediante un mapeo entre los paquetes IPv6 e IPv4. Se utiliza un prefijo especial para mapear direcciones IPv4 a IPv6: 64:ff9b::/96, el cual se encuentra definido en el RFC 6052.

Es necesario también realizar una modificación al DNS, llamada DNS64, que permite generar un registro AAAA aun cuando el destino no tenga dirección IPv6 (es decir, el DNS responda sólo con registros de tipo A).

Los usuarios nativos IPv6 acceden directamente a internet o a la nube de aplicaciones IPv6, pero cuando se necesita ir desde un usuario nativo IPv6 hacia la nube de aplicaciones IPv4, NAT64 realiza el mapeo que se necesita para comunicar a estos usuarios. Al usar un prefijo /96 se consigue que se

realice una asignación de los últimos 32 bits de una dirección IPv6 con los 32 bits de una dirección IPv4

Una dirección IPv6 se encuentra expresada en números hexadecimales, en cambio una dirección IPv4 está en números decimales, por tanto, NAT64 realizar el cálculo que permite la conversión. En la Figura 8 se evidencia el proceso de este mecanismo.

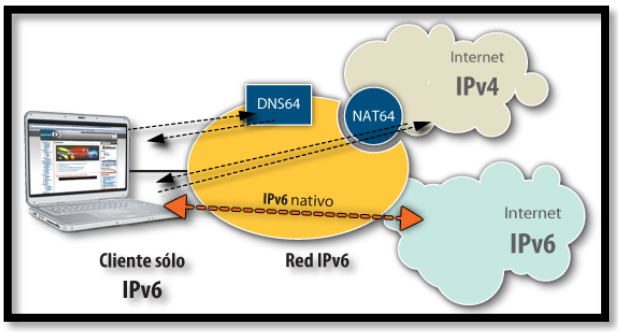

Figura 8: Mecanismo de Traducción

Fuente: Recuperado de http://portalipv6.lacnic.net/mecanismos-de-transicion/

3. *FASE III: Implementación y Análisis de pruebas*

La etapa final en la que se realizan las configuraciones en los equipos y se realizan las pruebas necesarias de funcionamiento para la coexistencia de IPv4 con IPv6.

3.1. Plan de direccionamiento IPv6

El Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra al tener como proveedor de servicios de Internet a Telconet, puede realizar un pedido para obtener un pool de direcciones IPv6 a esta empresa, debido a que es uno de los ISP's en el Ecuador, que ya manejan sus redes con el nuevo protocolo. Este requerimiento es inmediato, debido a que ya manejan un bloque de asignación IPv4, por lo tanto, el bloque de asignación IPv6 debería ser concebido sin ningún inconveniente.

3.2. Actualizaciones en Hardware y Software

Para los equipos CISCO, que no tienen una versión igual o superior a la 12.0()TS, se debe efectuar la actualización del IOS, de la siguiente manera:

1.- Ingresar a la terminal del equipo
2.- Verificar la versión con el comando *#show versión*
3.- Descargar la .ISO por ejemplo: 12-2.55.SE1
4. Borrar la versión anterior con el comando *#delete /f/r flash1:c2960-ipbase-mz.122.35-35.SE5*
5.- Copiar la nueva versión con el comando *#copy tpft flash1*
6.- Escribir en la memoria, y reiniciar con los comandos *#write mem y #reload.*

Finalmente se habilita IPv6:

*******Habilitación de ipv6********
Switch# configure terminal
Switch(confg)# sdm prefer dual-ipv4-and-ipv6 default
Switch(confg)# end
Switch# reload
****

En el caso de software se va a tener en cuenta los siguientes sistemas operativos:

- ✓ Windows
- ✓ Linux

3.3. Configuraciones de los equipos con IPv6.

En general, para los switches CISCO, que se encuentran en la topología de la red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, se debe habilitar IPv6 con los siguientes comandos:

*****Habilitación de protocolo IPv6**********

Switch# configure terminal

Switch(confg)# sdm prefer dual-ipv4-and-ipv6 default

Switch(confg)# end

Switch# reload

3.4. Pruebas de Funcionamiento

- En cuanto a la red Interna, se pudo verificar el acceso por parte de un usuario IPv4, IPv6 o con los dos direccionamientos al servidor WEB, que únicamente maneja IPv4. Es decir que para un usuario IPv6 acceda a este servicio, el servidor DNS64-NAT64, asigna una IPv6 para permitir el acceso a este usuario. Este proceso lo realiza de la siguiente manera:

Usuario ➔2001:db8:20:8::5678
Aplicación ➔ 172.16.8.6
Prefijo especial para mapear direcciones IPv4 a IPv6: 2001:db8:20:8:ffff::/96

IPv4 en binario ➔ 10101100.00010000.00001000.00000110
IPv4 en hexadecimal ➔ A C 1 0 0 8 0 6
Prefijo especial + IPv4 hexadecimal = IPv6 Asignada de aplicación
IPV6 Asignada de Aplicación ➔ 2800:68:19:2408:ffff::AC10:0806

- Para un usuario externo, este método va a funcionar de la misma manera, con todas las reglas de acceso que se hayan configurado en el Firewall.
- El mecanismo implementado doble pila, funciona correctamente ya que permite a usuarios con IPv4, IPv6 o clientes dual Stack, acceder a los servicios. Este mecanismo es más fácil, sin embargo, no es la única solución si solo se apoya en este criterio, debido a que no todas las aplicaciones o servicios van a tener compatibilidad con IPv6, es ahí donde se utiliza el servidor DNS64-NAT64.
- El tener funcionando dos mecanismos de transición, demanda la utilización de más recursos de la red, lo que no es óptimo, pero mientras las redes se adecuen a utilizar IPv6, es una solución bastante fiable.
- En servidor de correo, accede a las aplicaciones IPv4, a pesar de que maneje solo IPv6, esto es debido al DNS64, que permite crear registros AAAA, para mantener la conexión a estas aplicaciones que en muchos casos no son compatibles con IPv6. Existirán algunas aplicaciones nuevas que manejen el nuevo protocolo, y esta es una solución que se podría utilizar en tanto se maneje como protocolo nativo IPv6.
- Los equipos de red, funcionan de manera mucho más rápida con IPv6, debido a que se analizó que realizan menor procesamiento porque la cabecera es mucho más eficiente, analizan menos campos en la misma, lo que permite que las comunicaciones sean más veloces.

3.5. Monitorización de la red con la implementación de IPv6

El monitoreo de la red es un tema relevante en las redes de hoy en día, pues se pueden analizar varios factores que determinen resultados que al administrador le pueden alertar de varios beneficios o problemas. En este caso, analizar el tráfico IPv4 o IPv6 de los diferentes servicios de red, se vuelve importante porque esto permite determinar el uso del protocolo con el que se está conectado a la Internet. (Acosta, 2014)

De la misma manera, permite de acuerdo a los resultados que evidencie este monitoreo, se va a poder determinar acciones para solucionar el problema y conformar planes de contingencia para que los servicios de la red funcionen correctamente y los usuarios no tengan inconvenientes al momento de acceder a cualquiera de ellos. (Acosta, 2014)

Por esta razón, se ha analizado si la red del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, cuenta con alguna herramienta que permita analizar el tráfico de red y efectivamente existe implementada en la red la herramienta SNMP (Simple Network Management Protocol), que permite monitorear el tráfico que atraviesa por determinado dispositivo entre otras ventajas. Hay que tener en cuenta que el equipo que se monitorea es el que debe soportar SNMP para IPv6.

También, la herramienta Wireshark permite analizar con qué protocolos se está trabajando, que puede ser con IPv4 o IPv6, filtrado de paquetes entre otros. Existe la herramienta NetFlow que a diferencia de SNMP, permite obtener más información además de la carga de tráfico en la interfaz, por ejemplo, direcciones origen y destino o los protocolos de las capas superiores que atraviesan la interfaz. (Acosta, 2014)

Como se observa, existen muchas herramientas que pueden ser aprovechadas para el monitoreo de la red, cualquiera de ellas que se utilicen, permitirán analizar si la red, empieza ya a utilizar el protocolo IPv6 en sus servicios y si los usuarios hacen uso de la misma.

3.6. Riesgos y plan de contingencia con IPv6

Sin duda que un proyecto tecnológico de este tipo, puede tener varios riesgos, es por eso que se van a explicar en la Tabla IV los cuáles pueden ser:

TABLA IV

RIESGOS DE IMPLEMENTAR IPv6
Daño físico en el equipamiento de hardware
Pérdida de información
Incompatibilidad en hardware o software
Inestabilidad de las aplicaciones
Problemas con el funcionamiento del Sistema Operativo
Falta de compromiso por parte del personal del Departamento de Tecnologías Informáticas
Fallas de instalación y conexión de equipos
Falta de tiempo de adaptación al nuevo protocolo IPv6
Falta de capacitación al personal del Departamento de Tecnologías Informáticas

Fuente: Recuperado de http://www.magazcitum.com.mx/?p=568#.WB-xu_nhDIU

Ahora, de la misma manera los riesgos de no implementar IPv6 son los siguientes y se muestran en la Tabla V

TABLA V

RIESGOS DE NO IMPLEMENTAR IPv6
Dificultad para el surgimiento de nuevas redes
Alargar el tiempo de proceso de inclusión digital o reducir la cantidad de nuevos usuarios
Dificultar el surgimiento de nuevas aplicaciones
El costo de no implementar IPv6 podrá ser mayor que el de no implementarlo
Limitación de los ISP's para innovar y ofrecer nuevos servicios a los clientes

Fuente: Recuperado de http://www3.lacnic.net/eventos/lacnic23/miercoles/guillermo-cicileo-ipv6-para-tomadores-de-decisiones%20copia.pdf

Por último, se va a analizar el plan de contingencia, para va a permitir prevenir los riesgos con el objetivo de garantizar el buen desempeño del proyecto que asegure un servicio eficiente. En la Tabla VI, se indican las acciones que se deben llevar a cabo para prevenir los riesgos descritos anteriormente.

TABLA VI

Plan de contingencia
Respaldar toda la información en dispositivos de almacenamiento como discos duros, memorias USB, entre otros.
Revisar los manuales para la manipulación de los equipos de comunicación.
Realizar el mantenimiento y revisión del equipamiento de comunicación.
Supervisar las aplicaciones que se hayan implementado con IPv6.
Revisar las configuraciones y pruebas de funcionamiento.
Realizar las actualizaciones de los sistemas operativos continuamente.
Ejecutar planes de capacitación continua al personal de TIC's
Elaborar un cronograma de trabajo que permita supervisar cada una de las actividades a cada miembro de TIC's.
Evaluar al personal de TIC's con la finalidad de reforzar conocimientos para la adopción de IPv6.

Fuente: Recuperado de https://www.emaze.com/@AFRZQZOL/Plan-de-Transici%C3%B3n-IPv4-a-IPv6

IV. Análisis Costo-Beneficio

Se va a analizar el costo-beneficio del proyecto, que determine las ventajas de una posible implementación. Las entidades privadas se evalúan en términos de ganancia, en tanto que las públicas realizan la evaluación en términos de bienestar general. Es decir que el Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, al ser una entidad pública, los objetivos que persigue como institución gubernamental, se basa en el bienestar general social, en otras palabras, se debe buscar el beneficio social mejorando los aspectos: ambiental, cultural, tecnológico, entre otros. (Fabrycky, 2012)

4.1. Costo Social

En términos generales, el costo se refiere al precio que se debe pagar por un artículo. Sin embargo, el dinero proporcionado a las entidades públicas es por parte del Estado, entonces la obligación moral de las entidades públicas es invertir productivamente este dinero. Puesto el análisis que se pretende representar, se va a considerar como un costo social. El costo social, es el que debe pagar la sociedad cuando ocurre un acto de utilizar un recurso, y este costo puede estar ya incluido en los impuestos que los ciudadanos pagan al Estado. (Miller, 2010)

Para el análisis de los costos se van a considerar los siguientes aspectos:

A. Recurso Humano/Tecnológico

Son las personas que van a llevar a cabo la implementación de este proyecto. El personal del Departamento de Tecnologías de la Información, debe ser capacitado debido a que no se conoce mucho del tema y es necesario que se preparen en cuanto dure este proceso.

Costo de capacitación e implementación. Para realizar la estimación del costo que incluya la capacitación a todo el equipo que participará en el proyecto y la implementación para el protocolo IPv6, se ha tomado en cuenta una proforma que se pidió a la empresa Imbatec, debido a su pronta respuesta. Es una empresa que presta los servicios tecnológicos requeridos para este proceso ya que cuenta con ingenieros con certificación Cisco. De la misma manera tomando en cuenta los cursos que LACNIC ofertan para el conocimiento sugerido para este proceso que se encuentra en http://www.lacnic.net/web/anuncios/2015-cursos-ipv6, se ha realizado el siguiente análisis que se presenta en la Tabla VII.

TABLA VII

PRESUPUESTO DE CAPACITACIÓN E IMPLEMENTACIÓN			
Descripción	**Cantidad**	**Valor Unitario**	**Valor total**
Recurso Humano: 5 personas para capacitación	140 horas	$30	$4200
Implementación del Proyecto (Configuraciones en todo el equipamiento de red)	80 Horas	$30	$2400
		Total:	$6600

Fuente: Proforma Imbatec, Cursos LACNIC.

B. *Hardware.*

Una vez que se ha analizado el equipamiento de red, se pudo identificar que existen algunos equipos que deben ser sustituidos por otros que tengan las condiciones óptimas para poder funcionar adecuadamente, debido a que estos equipos tienen ya 10 años trabajando, y según el análisis realizado en el inventario de hardware se deben realizar estos cambios. Y con respecto al soporte IPv6, los demás equipos, están listos para ser configurados.

Costos de Hardware. Como se analizó en el inventario de hardware, existen equipos que deben ser sustituidos para la adopción del nuevo protocolo. En la Tabla VIII, se describen los equipos que deben ser sustituidos y el respectivo costo de cada uno de ellos.

TABLA VIII

PRESUPUESTO DE HARDWARE			
Unidad	**Descripción**	**Valor Unitario (USD)**	**Valor Total (USD)**
2	Switch de Acceso 4250T	1000	2000
2	Switch de Distribución 4250T	925	1850
1	Switch de Acceso 5500G/52	1046	1046
2	Switch de Distribución 4500	1139	2278
		TOTAL	7174

Fuente: http://www.mercadolibre.com.ec/

C. Software

El Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, utiliza en la mayoría de sus sistemas operativos software libre. Para realizar la simulación de este proyecto se hizo uso del mismo y se utilizaron los siguientes:

- Centos versión 6 (Sistema Operativo)
- GNS3 versión 1.3.11 (simulador de red)
- VMWare 11.1 (Plataforma para máquina virtual)
- Wireshark 2.0.3 (Analizador de red)

En el caso de GNS3, VMWare y Wireshark son versiones de software que ya se encuentran liberadas.

Costo de Software. El software libre no es sinónimo de software gratuito, libre quiere decir que son aquellos que su uso, modificación y distribución son permitidos a todos. Sin embargo, para la instalación en un equipo se requiere de unidades de almacenamiento en la que se encuentre el software. (Debian, 2016)

En la Tabla IX se indican los costos del software utilizado para la instalación en los respectivos equipos.

Tabla IX

PRESUPUESTO DE SOFTWARE	
Descripción	**Valor (USD)**
4 DVD's S.O Debian	12
4 DVD's Centos 6.5	12
TOTAL	24

Fuente: Recuperado de https://www.debian.org/intro/about.es.html

D. Costo total del proyecto

En la Tabla X se colocan los costos de capacitación e implementación, hardware y software que se necesitan para la puesta en marcha de este proyecto. También es importante que se considere un 10% adicional en caso de que se requiera contratar asesoramiento adicional en algunas configuraciones que pueden considerarse complejas. (Diaz, 2008)

TABLA X

PRESUPUESTO TOTAL	
Descripción	**Valor (USD)**
Presupuesto de Capacitación e Implementación	6600
Presupuesto de Hardware	7174
Presupuesto de Software	24
Imprevistos (10%)	1379.80
TOTAL	**15.177,80**

E. Razón Beneficio Costo

Para realizar este análisis, es importante considerar que, para esta entidad gubernamental, no se puede medir las ganancias en valores monetarios, más bien estas ganancias se transforman en beneficios que van a entregar a los usuarios internos como externos. También los beneficios que serán directamente para la red de datos del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra. Para ello, se van a describir estos beneficios en base a indicadores IPv4/IPv6 que se han realizado a lo largo de este estudio.

Autoconfiguración de dispositivos

- La característica plug and play, mecanismo que facilita a los usuarios en este caso a los internos la conexión automática a la red. Esto permite facilitar el proceso de administración de la red, ya que se asignará a cada usuario automáticamente una o varias direcciones IPv6.

Calidad de servicio a aplicaciones o servicios

- En el aspecto medioambiental, se pueden reducir costos, por ejemplo, si algún funcionario de la entidad tiene que viajar a una reunión importante en otro sitio, puede realizar desde la empresa una videoconferencia, aprovechando la mejora en cuanto a calidad de servicio.
- Lo que facilita la conexión extremo a extremo, que permite ampliar las ideas y dar mayor flexibilidad a desarrolladores, que de la misma manera reduce los costos de la técnica mencionada anteriormente.
- Con la mejora en la cabecera de IPv6 de etiqueta de flujo, permite que las características de calidad de servicio que existen en IPv4, sean mejoradas en IPv6, garantizando que las aplicaciones en tiempo real como videoconferencias o VoIP que pueden ser ofrecidas al usuario final mejoren de esta manera.

Implementación de máquinas inteligentes

- Cuando la implementación de IPv6 concluya, la mayor parte de tráfico en las redes de comunicación consistirá en transacciones entre máquinas sin la intervención por parte de los humanos. Esta evolución representará un cambio importante en el sector de las comunicaciones.
- La calidad de la experiencia para el usuario, puede mejorarse integrando la automatización de procesos en la entidad con la ayuda de objetos inteligentes conectados con direcciones IPv6 únicas.

Creación de Redes de Sensores

- Las redes de sensores que consisten en sensores autónomos que colaboran en la supervisión de condiciones físicas y medioambientales concretas. Permitirán que se controle varios parámetros como calor, temperatura, presión, sonido, vibración, entre otros. Pueden integrarse a sistemas inteligentes que permitan ser monitoreados cada uno, esto permitirá que la ciudad se vaya convirtiendo en una Smart City que beneficiará a los seres vivos de la ciudad de Ibarra.

Proyectos ambientalistas

- Pueden crearse algunos, por ejemplo, el control de velocidad de los vehículos públicos, que permitirá contribuir a mejorar la seguridad en el transporte para la ciudadanía.
- Beneficios de ahorro eléctrico, se pueden crear una red eléctrica inteligente que tenga por objetivo modernizar el sistema eléctrico con comunicaciones bilaterales para supervisar y gestionar la producción, trasmisión y distribución de energía eléctrica conjuntamente con la empresa Emelnorte, que contribuye al beneficio para los ciudadanos. Esto con el despliegue de IPv6 que se vea implementado en el Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra.

Seguridad

- La seguridad es un aspecto importante en cualquier red, es por ello que el protocolo IPv6 incluye este parámetro y puede proporcionar encriptación, autenticidad e integridad de la información.

Acceso a aplicaciones o servicios

- Los servicios o aplicaciones que manejen Dual Stack, permitirá que usuarios tanto IPv4 como IPv6 puedan acceder a ellos, debido a que todas las peticiones que se realizan a las aplicaciones desde un host IPv4 se responden desde los servidores IPv4, de igual manera las peticiones de un host IPv6 serán contestadas desde servidores IPv6.
- Al utilizar el mecanismo NAT64-DNS64, los usuarios nativos IPv6 acceden directamente a internet o a la nube de aplicaciones IPv6, pero cuando se necesita ir desde un usuario nativo IPv6 hacia la nube de aplicaciones IPv4, Nat64 realiza el mapeo que se necesita para comunicar a estos usuarios.
- IoT (Internet de las cosas), es uno de los aspectos más sobresalientes con IPv6, que será la red que interconecta objetos comunes equipados con módulos de inteligencia miniaturizados, que dará pie al desarrollo de grandes proyectos tecnológicos dedicados a mejorar la calidad de vida de los ciudadanos de la ciudad de Ibarra.

V. CONCLUSIONES

- El desarrollo de la propuesta de transición de servicios de IPv4 a IPv6 para el Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, permitió desarrollar un modelo que vaya de la mano con el plan de acción propuesto por el MINTEL, permitiendo una transición ordenada y eficaz para la coexistencia de los dos protocolos.

- El estudio del protocolo IPv6, permitió analizar las ventajas que tiene sobre IPv4, por ejemplo, la autoconfiguración de los hosts, mayor utilización de IP's, mejor procesamiento de la información, movilidad IP, incremento de seguridad aprovechando el protocolo IPsec.

- El equipamiento de red del GAD-I, en algunos equipos, se requiere la actualización de los IOS en específico en todas las versiones anteriores a la 12.0()T, en otros casos es necesario realizar el requerimiento de nuevos equipos debido a su tiempo de vida útil en el que se recomienda que los equipos no superen los diez años de uso.

- En cuanto a actualizaciones de software, en los sistemas operativos que manejan software libre, el kernel requerido para funcionar con IPv6 se tiene a partir de la versión 2.4 en adelante, se cumple con este objetivo y de la misma manera todos ellos tienen el soporte para IPv6.

- Es necesario que se analice el servidor de base de datos, debido a que las aplicaciones Web como correo necesitan de la información albergada en el mismo, por lo tanto, se debe analizar cuidadosamente cuales deben ser los servicios que necesiten mayor prioridad de transición.

- La elección del mecanismo de transición que se ha decidido utilizar es doble pila o dual Stack, que permite mantener la red funcionando tanto en IPv4 como en IPv6, teniendo como ventaja manejar los dos protocolos y tener coexistencia con los mismos. Si se llegara a dejar de utilizar la red IPv4, la red IPv6 estará disponible, permitiendo que la red siga estando disponible para todos los usuarios.

- Para mantener conectividad a usuarios que solo utilicen IPv6 y deban acceder a aplicaciones que se encuentren solamente utilizando IPv4, se hace necesaria la implementación de un traductor DNS64 y NAT64, el cual asignará una IPv6 a la aplicación IPv4 mediante una traducción que se consigue mapeando una dirección IPv4 a una IPv6.

- En cuanto a seguridad, se ha decidido aprovechar el protocolo IPsec, ya que su uso es imprescindible por ejemplo en el servidor WEB, debido a que se maneja

información delicada, por tanto, se ha implementado en dispositivos de gateway de seguridad o llamados también como intermedios utilizando el modo túnel con encapsulación ESP, el cual proporciona autenticación, integridad y confidencialidad en los paquetes transmitidos.

- Al realizar el análisis en cuanto a costos y beneficios, se determinó que el GAD-I, al ser una entidad gubernamental, cuando genera un proyecto, no se espera que se generen ganancias económicas y que se recupere el dinero invertido en un periodo de tiempo, más bien se traduce a beneficios sociales que permitan obtener satisfacción a los usuarios.

- Con el protocolo IPv6, se tiene capacidad para más usuarios, más redes, esta ventaja de IPv6 puede ser aprovechada para la implementación de proyectos tecnológicos que tengan relación con el tema IoT, que el GAD-I, puede aprovechar y trabajar en conjunto para lograr encaminar a la ciudad de Ibarra para ser una Smart City.

- Este proyecto, es realizado con la finalidad de que las empresas públicas o privadas de la ciudad de Ibarra, se motiven para empezar a desplegar IPv6 en las redes, de modo que se aprovechen todos los beneficios que se tiene al utilizar el protocolo de nueva generación.

- IPv6 presenta significativas oportunidades para crear modelos empresariales innovadores, esto debido a que se pueden asignar direcciones únicas a dispositivos cotidianos conectados lo que permitirá la generación de aplicaciones y servicios tecnológicos que permitirá la automatización, productividad y eficiencia de la empresa que maneje su red con el nuevo protocolo.

REFERENCES

6SOS. (5 de Enero de 2004). *IPv6 Servicio de Información y Soporte* . Obtenido de El protocolo IPv6: http://www.6sos.org/documentos/6SOS_El_Protocolo_IPv6_v4_0.pdf

Acosta, A. y. (2014). *IPv6 para operadores de Red*. (Ebook, Editor) Obtenido de http://portalipv6.lacnic.net/wp-content/uploads/2014/12/ipv6_operadores_red.pdf

Alonso, J. C. (2001). *Neighbor Discovery*. Obtenido de http://www.labs.lacnic.net/site/sites/default/files/ES-Neighbor_y_MTU-Discovery.pdf

Amelines, J. (2012). *IPv4toIPv6*.

APR. (2016). *Qué es un servidor y cuáles son los principales tipos de servidores (proxy,dns, web,ftp,pop3 y smtp, dhcp...)*. Obtenido de http://aprenderaprogramar.com/index.php?option=com_content&view=article&id=542:que-es-un-servidor-y-cuales-son-los-principales-tipos-de-servidores-proxydns-webftppop3-y-smtp-dhcp&catid=57:herramientas-informaticas&Itemid=179

Ariganello, E. (16 de Noviembre de 2012). *Aprende Redes*. Obtenido de INTRODUCCIÓN AL GNS3: http://aprenderedes.com/2012/11/introduccion-al-gns3/

Carlos, J. C. (s.f.). *Direccionamiento IPv6*. Obtenido de http://www.labs.lacnic.net/site/sites/default/files/001-Direccionamiento%20y%20Protocolo%20IPv6.pdf

Cedeño., J. C. (Febrero de 4 de 2013). *Propuesta de transición de IPv4 a IPv6.* Obtenido de Tunel 6to4: http://repositorio.ucsg.edu.ec/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf

CHECKPOINT. (5 de septiembre de 2015). *Check Point 4600 Appliance | Ficha de datos*. Obtenido de CHECK POINT 4600 APARATO: https://www.checkpoint.com/downloads/product-related/datasheets/4600-appliance-datasheet.pdf

Cicileo, G. R. (2009). *IPv6 para todos.* (E-Books, Ed.) Buenos Aires, Argentina.

CISCO. (2013). *Entendiento IPv6, Subredes y Direccionamiento.*

CISCO. (17 de Octubre de 2016). *Túnel IPv6 a través de una Red IPv4*. Obtenido de http://www.cisco.com/cisco/web/support/LA/102/1027/1027026_ipv6tunnel.pdf

CISCO Academy Network. (2009). *EIGRP*. Obtenido de http://giret.ufps.edu.co/cisco/descargas/tutoriales_docentes/ITN_PT_ILM-Docs%20Simulaciones.pdf

CISCO Systems. (s.f.). *OPSFv3 para IPv6*. Obtenido de http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/15-sy/iro-15-sy-book/ip6-route-ospfv3.html

Corporación Digital Colombia. (2016). *Colombia Digital*. Obtenido de https://colombiadigital.net/actualidad/articulos-informativos/conceptos-tic.html

De la Luz, S. (4 de Noviembre de 2010). *Criptografía : Algoritmos de cifrado de clave simétrica*. Obtenido de http://www.redeszone.net/2010/11/04/criptografia-algoritmos-de-cifrado-de-clave-simetrica/

Debian. (5 de Julio de 2016). Obtenido de https://www.debian.org/intro/about.es.html

Deering, S. (11 de Agosto de 2011). *ICMPv6 para IPv6*. Obtenido de www.ietf.org/rfc/rfc2463.txt

Diaz, J. (Mayo de 2008). *Formulación y evaluación de proyectos*. Obtenido de http://www.eumed.net/ce/2008a/

Fabrycky, W. (2012). *Decisiones Económicas, Análisis y Proyectos.* Ed. Prentice Hall.

Fundamentos de Redes. (2013). Obtenido de https://sites.google.com/site/fundamentosderedesutez tic1h/home

Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra. (12 de Abril de 2015). *Ibarra, ciudad a la que siempre se vuelve*. Obtenido de http://ibarra.gob.ec/web/index.php/informativo/ibarra1234/informacion-general

Herramientas WEB. (2013). *El protocolo Http*. Obtenido de http://neo.lcc.uma.es/evirtual/cdd/tutorial/Indice.html

Ibarra, G. A. (2015). *Servidores virtuales.* Ibarra.

Iglesias, S. (Noviembre de 2011). Análisis del protocolo IPsec. 51-63. Obtenido de Telefónica Investigación y Desarrollo.

INSAT. (s.f.). *La electrónica*. Obtenido de Sistema Hexadecimal: http://www.ite.educacion.es/formacion/materiales/47/cd/mod1b/1bb_4.htm

Internet Society. (2016). *Breve historia del Internet.* Recuperado el 25 de Abril de 2016, de http://www.internetsociety.org/es/breve-historia-de-internet

Kent, a. R. (1998). *Protocol Encapsulating Security Payload (ESP).* New York.

LACNIC. (2012). *No hay más direcciones IPv4 en América Latina y Caribe*. Obtenido de http://www.lacnic.net/web/anuncios/2014-no-hay-mas-direcciones-ipv4-en-lac

Lujan, P. (4 de Junio de 2015). *Error capa 8*. Obtenido de ¿Porqué se llama IPv4 e IPv6?: https://errorcapa8.wordpress.com/2015/06/04/por-que-se-llaman-ipv4-e-ipv6/

MacDonald, M. A. (2008). *Aspectos básicos de networking.* Madrid, España: Pearson.

Microsoft. (Enero de 2005). *Descubrimiento de escucha de multidifusión (MLD)*. Obtenido de https://msdn.microsoft.com/es-es/library/cc776494(v=ws.10).aspx

Miller, R. L. (2010). *Microeconomía Moderna.* Harla.

Ministerio de Industria, energía y turismo de España. (2013). *IP.v6 protocolo de internet versión 6*. Obtenido de Características de IPv6: http://www.ipv6.es/es-ES/Faqs/Paginas/tecnicas.aspx

Ministerio de Telecomunicaciones y Sociedad de la Información. (2012). Obtenido de http://www.telecomunicaciones.gob.ec/ecuador-lidera-el-cambio-a-la-ipv6-que-es-por-que-el-cambio-en-que-nos-beneficia/

Moya, F. A. (Septiembre de 2009). *Rediseño de la Red ISP READYNET CIA. LTDA., PROCEDIMIENTO PARA CONVERIR AL ISP EN UN SISTEMA AUTÓNOMO*. Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/1819/1/CD-2405.pdf

Network Information Center México S.C. (2010). *IPv6 Mx*.

Nuñez, D. (2009). *Estudio de migración de IPv4 a IPv6 para la empresa proveedora de Internet Milltec S.A.* Quito.

Palet, J. (Abril de 2007). *The Choice: IPv4 Exhaustion or Transition to IPv6.*

Pérez, S. (2001). *Análisis del protocolo IPSec: el estándar*. Obtenido de https://www.movistar.es/on/es/micro/seguridad/IPSec.pdf

Tanenbaum, A. S. (2011). *Redes de computadoras* (Vol. V). México: Pearson.

TRIPOD. (2016). *Protocolos de Enrutamiento*. Obtenido de RIPng: http://andersonramirez.tripod.com/protocolo.htm

Universidad de San Carlos de Guatemala. (Agosto de 2009). *MIGRACIÓN DEL PROTOCOLO IPv4 A IPv6 EN UNA RED, LOS BENEFICIOS Y SEGURIDAD QUE CONLLEVA ESTE CAMBIO.* Obtenido de Identificación de Direcciones IPv6: http://biblioteca.usac.edu.gt/tesis/08/08_0246_EO.pdf

Universidad Técnica Particular de Loja. (16 de Julio de 2010). *Propiedad planta y_equipo*. Obtenido de http://elizaherrera3/propiedad-planta-yequipo

Fabián G. Cuzme Ingeniero en Sistemas Informáticos, Universidad Técnica de Manabí – Ecuador en 2009. Actualmente es docente en la carrera de Ingeniería en Electrónica y Redes de Comunicación en la Universidad Técnica del Norte, Ibarra – Ecuador, obtuvo la Maestría en Redes de Comunicación en la Pontificia Universidad Católica del Ecuador, Quito – Ecuador en 2015.

Gabriela E. Mera Nació en Ibarra-Ecuador el 21 de septiembre de 1992, sus estudios primarios los realizó en el Instituto Rosales “La Salle”, sus estudios secundarios en el Colegio Nacional “Ibarra” donde finalizó en el año 2010, obteniendo el título de Bachiller en Ciencias Especialización Físico Matemático.

Actualmente, está realizando su proceso de titulación en Ingeniería en Electrónica y Redes de Comunicación, Universidad Técnica del Norte – Ecuador