Metodología de Transición del Protocolo de Internet Versión 4 a Versión 6 en el Gobierno Provincial de Imbabura

Carlos A. Vásquez, Stalin A. Hidrobo
Carrera de Ingeniería en Electrónica y Redes de Comunicación, Universidad Técnica del Norte
Ibarra, Ecuador
cavasquez@utn.edu.ec
sahidrobom@utn.edu.ec

***Resumen*— El crecimiento de la Internet ocasiona que la cantidad de direcciones IP del protocolo IPv4, llegue a su límite o a una situación de una posible escasez. Por esta razón se impulsa a las Instituciones Públicas de nuestro país para que adopten el protocolo IPv6, ya que existe el acuerdo ministerial 007-2012, titulado "Medidas Sobre IPv6", para implementar políticas públicas e incorporar el nuevo protocolo, además de la coexistencia con el anterior sistema.**

El proyecto que se presenta a continuación consiste en el desarrollo de una metodología que permita la transición del Protocolo de internet versión 4 a versión 6 para la Prefectura de Imbabura, para lo cual, inicialmente se realizó una investigación de los dos protocolos para compararlos, analizar sus ventajas y desventajas, con la finalidad de establecer una base para la futura implementación de una red integrada al protocolo IPv6.

***Terminos Indexados*—TCP, IPv6, Dual Stack, DNS64, NAT64.**

I. Introducción

Este proyecto está enfocado en el estudio del Protocolo de Internet versión 6 para el Gobierno Provincial de Imbabura, de tal manera que este pueda tener una metodología de transición con el protocolo de internet versión 4 utilizado actualmente en la Institución.

Para la transición del Protocolo de Internet Versión 4 hacia Versión 6 existen diferentes métodos, los cuales se dividen en 3 grupos: método de doble pila que permite un soporte para los dos protocolos tanto en los hosts como en los routers, método de túneles, están basados en la encapsulación de paquetes IPv6 dentro de paquetes IPv4 para proporcionar un mecanismo para usar la infraestructura de la red IPv4 durante el tiempo que se implemente la red IPv6 y por último los métodos de traducción cuya solución se basa en asignar de manera temporal direcciones IPv4 a nodos IPv6, para que de esta manera todos los nodos logren acceder tanto a la red de IPv6 como a la de IPv4. Se escogerá uno de estos mecanismos de transición mediante un análisis comparativo de sus ventajas y desventajas al momento de una futura implementación. Además se planteará la utilización de NAT64 el cual permite que los hosts que solo tienen conectividad IPv4 puedan comunicarse con los hosts que solamente tienen conectividad IPv6 y DNS64 que realiza el mapeo de los nombres de dominio de direcciones IPv6, de esta manera si el host necesita un DNS y recibe como respuesta una dirección de 32 bits utilizará IPv4, y si recibe una de 128 bits utilizará IPv6.

II. Fundamentos de IPv6

Cuando se utiliza Internet para cualquier actividad, como correo electrónico, navegación web, o cualquier aplicación o servicio, la comunicación entre los diferentes elementos de la red y nuestro computador o teléfono, utiliza un protocolo que denominamos Protocolo de Internet.

En los últimos años, desde que Internet tiene un uso comercial, la versión de este protocolo es IPv4.

Para que los dispositivos se conecten a la red, es necesaria una dirección IP. Cuando se diseñó IPv4, no se pensó que pudiera tener tanto éxito comercial, y dado que sólo dispone de 232 direcciones, junto con el imparable crecimiento de usuarios y dispositivos, implica que en poco tiempo estas direcciones se agotarán.

Por este motivo, el organismo que se encarga de la estandarización de los protocolos de Internet (IETF), ha trabajado en los últimos años en una nueva versión del Protocolo de Internet, concretamente la versión 6, que posee direcciones con una longitud de 128 bits, es decir 2128 posibles direcciones (340.282.366.920.938.463.463.374.607.431.768.211.456).

Con una coexistencia ordenada entre IPv4 e IPv6 el despliegue se irá realizando gradualmente, ya que irá desplazándolo a medida que los dispositivos de cliente, equipos de red, aplicaciones, contenidos y servicios se vayan adaptando a la nueva versión del protocolo de Internet.

Documento recibido en Abril del 2016. Esta investigación se realizó como proyecto previo para obtener el título profesional en la carrera de Ingeniería en Electrónica y Redes de Comunicación de la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica del Norte. C.A. Vásquez, Docente de la Universidad Técnica del Norte, en la Carrera de Ingeniería en Electrónica y Redes de Comunicación, Av. 17 de Julio sector El Olivo, Ibarra-Ecuador. S.A. Hidrobo, egresado de la Carrera de Ingeniería en Electrónica y Redes de Comunicación (teléfono 5939-6758-0385; e-mail: sahidrobom@utn.edu.ec).

A. *Características de IPv6*

1) Calidad de servicio (QoS): IPv6 agrega en su cabecera un nuevo campo denominado etiqueta de flujo, el cual permite que los enrutadores sean identificados y estos a su vez proporcionen un control especial de los paquetes que pertenecen a un mismo flujo. La creación de este nuevo campo permite el desarrollo de nuevos modelos de clasificación de flujos de tráfico. Un flujo es un grupo de paquetes entre un origen y un destino. Dado que el tráfico está identificado en el encabezado IPv6, la compatibilidad con QoS se puede obtener de una forma más sencilla.

2) Nodos vecinos: El protocolo Descubrimiento de neighbors (vecinos) en IPv6 es semejante al protocolo ARP en IPv4, es el mecanismo por el cual un nodo nuevo que se incorpore a la red, descubre la presencia de otros nodos en su mismo enlace, además es capaz de localizar a routers y mantiene la información de conectividad a los vecinos activos.

3) Capacidad de ampliación: El tamaño de direcciones cambia de 32 bits en IPv4 a 128 bits en IPv6, además se agregan encabezados de extensión a continuación del encabezado IPv6. El tamaño de los encabezados de extensión IPv6 sólo está limitado por el tamaño del paquete IPv6.

B. *Cabecera IPv6*

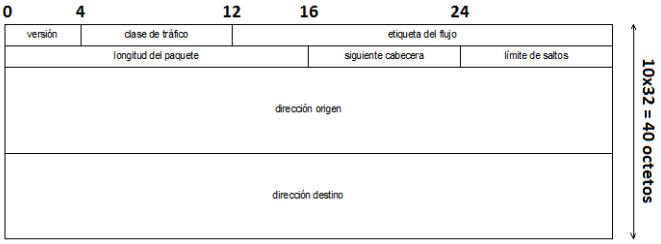

Fig.1. Formato de Cabecera IPv6

La cabecera básica de IPv6, mostrada en la Figura 1, tiene una longitud fija de 40 octetos, consistiendo en los siguientes campos:

- **Versión (4 bits):** Es el número de versión de IP, es decir, 6.
- **Clase de tráfico (8 bits):** El valor de este campo especifica la clase de tráfico. Los valores de 0-7 están definidos para tráfico de datos con control de la congestión, y de 8-15 para tráfico de vídeo y audio sin control de la congestión.
- **Etiqueta del flujo (20 bits):** Se crea para permitir tráficos con requisitos de tiempo real. Tiene una longitud de 20 bits. IPv6 define un flujo como una secuencia de paquetes enviados desde un origen a un destino específico. De este modo, la fuente asigna la misma etiqueta a todos los paquetes que forman parte del mismo flujo. Su uso viene descrito en la RFC 1809.
- **Longitud del paquete (16 bits):** Especifica el tamaño total del paquete, incluyendo la cabecera y los datos, en bytes. Es necesario porque también hay campos opcionales en la cabecera.
- **Siguiente cabecera (8 bits):** Indica el tipo de cabecera que sigue a la cabecera fija de IPv6, por ejemplo, una cabecera TCP/UDP, ICMPv6 o una cabecera IPv6 opcional.
- **Límite de saltos (8 bits**): Es el número de saltos máximo que le queda al paquete. El límite de saltos es establecido a un valor máximo por el origen y disminuye en 1 cada vez que un nodo encamina el paquete. Si el límite de saltos toma el valor 0, el paquete es descartado.
- **Dirección origen (128 bits):** Es la dirección del origen del paquete.
- **Dirección destino (128 bits):** Es la dirección del destino del paquete.

*1) Cabeceras de Extensión IPv6:*En IPv6 la cabecera es de tamaño fijo, pero existen ocasiones en los que la cabecera estándar de IPv6 no es suficiente, en esos casos es necesario ampliar la cabecera con las denominadas (cabeceras de extensión de IPv6), las cuales son cabeceras opcionales que se codifican aparte.

Estas cabeceras están situadas entre la cabecera de IPv6 y las cabeceras de nivel superior utilizando el campo (siguiente cabecera) de la cabecera de IPv6 para indicar su existencia a los nodos.

Las cabeceras de extensión no son examinadas tampoco procesadas a lo largo de la ruta, salvo en el nodo de destino, al no ser procesadas por los nodos intermedios, los libera de la necesidad de procesar información que no es necesaria para los mismos, de esta manera optimizando el funcionamiento de routers y nodos intermedios.

La arquitectura general es la siguiente:

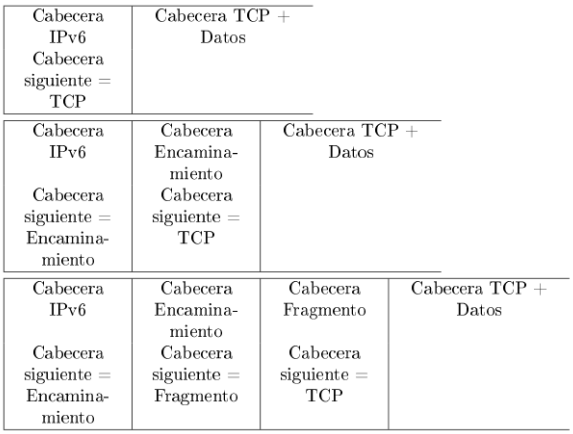

Fig.2. Arquitectura de Cabeceras de extensión IPv6

C. *Direccionamiento IPv6*

Los cambios dados por IPv6 no sólo se reflejan en la cantidad de direcciones, sino también incluyen nuevos tipos.

1) Tipos de Direcciones IPv6: Una dirección IPv6 puede ser clasificada en tres tipos:

- **Unicast:** Se utiliza únicamente para identificar una interfaz de un nodo IPv6. Un paquete enviado a una dirección unicast es entregado a la interfaz identificada por esa dirección.
- **Multicast:** Se utiliza para identificar a un grupo de interfaces IPv6. Un paquete enviado a una dirección multicast es procesado por todos los miembros del grupo multicast.
- **Anycast:** Se asigna a múltiples interfaces. Un paquete enviado a una dirección anycast es entregado a una de estas interfaces, usualmente la más cercana.

D. Resolución de nombres en IPv6

IPv6 fue diseñado para trabajar con direcciones de 128 bits de los hosts de origen y destino, lo cual resulta difícil para los usuarios utilizar y recordar direcciones de 32 dígitos hexadecimales para intentar acceder a los recursos de la red. Para esto, se puede utilizar nombres únicos, que son más sencillos de recordar.

Al utilizar un nombre para una dirección IPv6, es necesario asegurarse de que este sea único y que pueda resolverse en la dirección IPv6 correcta.

La resolución de nombres de host permite asignar correctamente un nombre de host a una dirección IPv6. Un nombre de host es un alias que se da a un nodo IPv6 para identificarlo como host IPv6. El nombre de un host puede tener un máximo de 255 caracteres e incluir caracteres alfabéticos y numéricos, guiones y puntos. Además, es posible asignar varios nombres al mismo host.

Los nombres de dominio se resuelven enviando consultas de nombres DNS a un servidor DNS configurado, este servidor resuelve el nombre de dominio consultado en una dirección IPv6 y devuelve el resultado.

E. IPv6 en el mundo y Latinoamérica

El despliegue de IPv6 en el mundo, tiene lugar, sin cambios rápidos, pero dependiendo del punto de vista de la red se puede observar su desarrollo.

En cuanto a las redes académicas, en Japón, Europa y Norteamérica se ha producido un despliegue muy importante, debido a las grandes inversiones públicas para fomentar el mismo. En el caso europeo, la Comisión Europea ha cofinanciado, junto con el sector privado, un gran número de proyectos de investigación y desarrollo, que a su vez han posibilitado a la industria, la adquisición de conocimientos y la culminación del desarrollo y la estandarización de IPv6.

Muchos países y regiones han adoptado políticas públicas, y recalcan que el despliegue de IPv6 no es caro si se planifica adecuadamente, es decir, con cierta anticipación, la cual depende del caso específico de cada red, y por tanto asegurándose que las adquisiciones de equipamiento, aplicaciones y servicios, tengan soporte de IPv6, de tal modo que no sea necesario realizar nuevas adquisiciones cuando se desee implementar IPv6.

Como consecuencia de este tipo de políticas públicas, en varios países y regiones de todo el mundo, hay fechas específicas para la activación obligatoria de IPv6 en las redes de la administración pública y otras redes relacionadas como educación, defensa, entre otras.

Desde el punto de vista de los grandes operadores de redes (carriers), que en su mayoría tienen redes intercontinentales, hace ya varios años han dado grandes pasos y tienen un soporte muy completo de IPv6.

La situación es muy diferente en la "última milla" ya que no han logrado explotar en su totalidad la implementación de IPv6, salvo excepciones notables sobre todo en Japón, algunos otros países asiáticos, y un reducido número de casos en Europa y Norteamérica.

Combinando datos de Google y APNIC, es posible notar que las áreas con mayor visibilidad en cuanto a penetración de IPv6 son Bélgica, Suiza, Luxemburgo, Alemania, Estonia, Estados Unidos, Noruega, Francia, Alemania, República Checa, Rumania, Perú (principal representante de la región latinoamericana en la lista) y Ecuador, como se indica en la Figura 26. Resulta interesante, que áreas con trabajo estable en cuanto a IPv6, como Brasil y países asiáticos (entre los que destacan China y la India) aun no aparezcan en posiciones destacadas en la estadística.

F. IPv6 en Ecuador

En la actualidad en Ecuador esta tecnología no se ha desarrollado en su totalidad, debido a la falta de información, conocimiento, o porque aún no es necesario que sea aplicada, pero esta tecnología avanza rápidamente y eventualmente se necesitará hacer uso de ella.

Las Instituciones de Educación Superior deben ser la base de información para que Ecuador adopte IPv6 como parte de su tecnología.

IPv6 no resuelve todos los problemas de su antecesor, pero es la alternativa técnica y económica más adecuada a la realidad de nuestro país para afrontar el crecimiento futuro de la Internet. La transición a IPv6 en Ecuador se está iniciando y se requiere mayor difusión y capacitación, para esto es muy importante impulsar las actividades que podría ofrecer el IPv6TF-EC.

G. Mecanismos de transición

Debido a que el protocolo más utilizado en la actualidad en Internet es el IPv4, no es posible su sustitución, es decir, no se puede apagar la red, ni siquiera por unos instantes y cambiar a IPv6.

Una de las principales razones para el diseño de IPv6, fue que pudiera realizarse una transición suave hacia la nueva versión del protocolo IP, sin que fuera necesario pasar de una versión a otra en forma abrupta.

Se están desarrollando mecanismos que facilitan la realización y entendimiento de la transición de IPv4 a IPv6. Entre dichos mecanismos que permitirán esta convivencia y la migración progresiva tanto de las redes como de los equipos de usuario se pueden destacar los siguientes:

- Dual Stack o Doble Pila
- Túneles
- Mecanismos de Traducción

1) Dual Stack: La doble pila hace referencia a una solución de nivel IP con doble pila de protocolos (RFC 4213: Mecanismos básicos de transición para hosts y ruteadores de IPv6), incluyendo de forma simultánea, tanto la pila de protocolos de IPv4 como la de IPv6 en cada dispositivo conectado a la red. Por tanto, cada dispositivo tendrá dos direcciones IP, una IPv4 y otra IPv6. Esto permite a los dispositivos establecer sesiones utilizando cualquiera de los dos protocolos según sus necesidades. Se trata de una solución fácil de implementar y ampliamente soportada, lo cual facilita el despliegue de IPv6.

De esta forma, cuando se establece una conexión hacia un destino sólo IPv4, se utilizará la conectividad IPv4 y si el destino es una dirección IPv6, se utilizará la red IPv6. En caso que el destino tenga los dos protocolos, normalmente se preferirá intentar conectar primero por IPv6 y en segunda instancia por IPv4, como se muestra en la Figura 3.

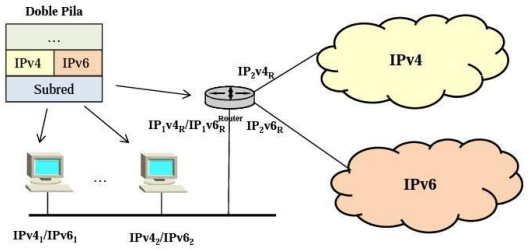

Fig.3. Doble Pila

2) Tuneles: Esta técnica permite interconectar las nubes IPv6 a través de un servicio IPv4 nativo por medio de un túnel. Los paquetes IPv6 son encapsulados por un router de extremo antes de ser transportado a través de la red IPv4, siendo desencapsulados en el extremo de la red IPv6 receptora, como se muestra en la Figura 4.

Se trata de una medida temporal, ya que, en el futuro, IPv4 irá desapareciendo paulatinamente y todos los dispositivos implementarán IPv6 de forma nativa.

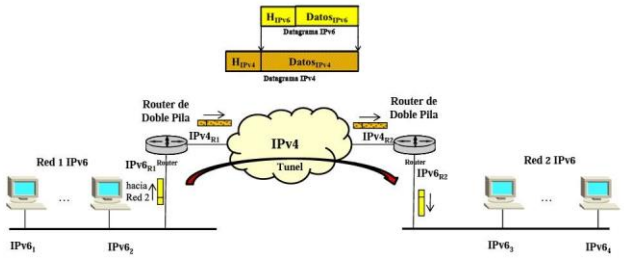

Fig.4. Túneles

3) Mecanismos de traducción: Consiste en utilizar un dispositivo en la red que convierta los paquetes de IPv4 a IPv6 y viceversa. Ese dispositivo tiene que ser capaz de realizar la traducción en los dos sentidos deco el fin de permitir la comunicación, como se muestra en la Figura 5.

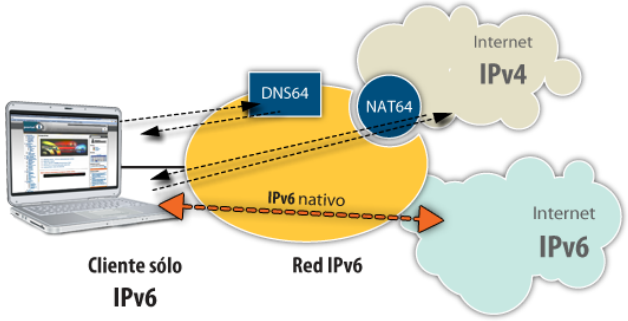

Fig.5. Mecanismos de traducción

F. NAT64

NAT64 es un mecanismo que permite a hosts con conectividad solo IPv6 comunicarse con hosts con conectividad solo IPv4.

La estructura para el NAT64 está definida en el RFC 6144, allí se define el marco para la traducción IPv4/IPv6. Dicha estructura debe tener los siguientes componentes:

- Traducción de direcciones
- Traducción de IP y ICMP
- Mantenimiento de estado de traducción
- DNS64
- ALG para protocolos de capa de aplicación

Un traductor de IP/ICMP tiene dos modos posibles de operación: stateles y stateful (RFC 6144). De esta forma NAT64 puede implementarse en modo stateless (RFC 6145) o modo stateful (RFC 6146).

Para lograr este objetivo se debe contar con un equipo de red que sea capaz de realizar una traslación de protocolos IPv4 a IPv6 y viceversa como se muestra en la Figura 6. Entre otras cosas, en este mapeo se debe incluir el mapeo de las direcciones de capa de red de los dos protocolos.

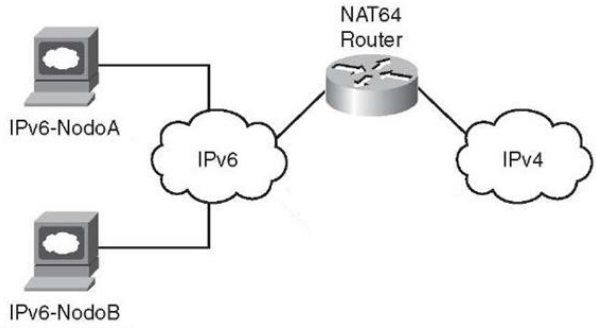

Fig.6. NAT64

G. DNS64

Para que los hosts solo IPv6, puedan comunicarse con los hosts solo IPv4 hace falta un componente adicional que hace la traducción a nivel de DNS. Este es el rol del DNS64, el cual se encarga de recibir las consultas DNS de los hosts solo IPv6 y modificar las respuestas de tal manera de incluir registros AAAA que mapean las direcciones IPv4 dentro del prefijo NAT64 (RFC 61471).

Ambos mecanismos permiten a un cliente IPv6 iniciar una comunicación con un servidor solo IPv4. También permiten la comunicación peer-to-peer entre un nodo IPv4 y uno IPv6, donde la comunicación puede haber sido inicializada por un extremo que usa NAT o técnicas de comunicaciones peer-to-peer, como se muestra en la Figura 7.

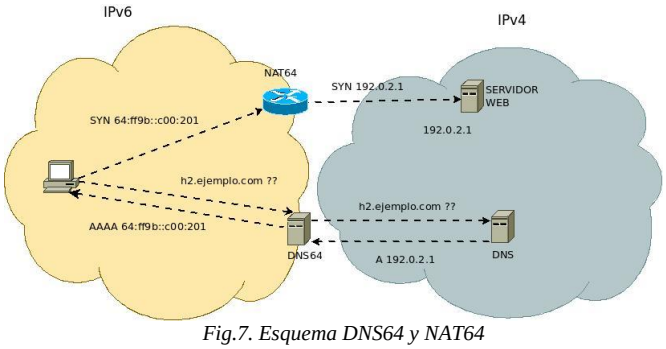

Fig.7. Esquema DNS64 y NAT64

Para permitir a un nodo IPv6 que inicia una comunicación con un

[1] RFC 6147: DNS64. Extensiones DNS para la traducción de direcciones de red de clientes IPv6 a servidores IPv4

nodo IPv4, hacer consultas al DNS acerca del nodo IPv4 con el cual se quiere comunicar, se usa el DNS64. El DNS64 se utiliza para resumir los registros AAAA a partir de los registros A. La dirección IPv6 contenida en el registro AAAA contiene un prefijo Pref64::/n. El NAT64 debe procesar solamente paquetes entrantes que contenga una dirección destino que pertenezcan al pool de direcciones IPv4 asignadas al NAT64.

III. Situación Actual de la Red de la Prefectura de Imbabura

La Prefectura de Imbabura es la institución encargada de coordinar, planificar, ejecutar y evaluar el Plan de Desarrollo Provincial Participativo; fortaleciendo la productividad, la vialidad, el manejo adecuado de sus recursos naturales y promoviendo la participación ciudadana; a fin de mejorar la calidad de vida de sus habitantes.

La Prefectura de Imbabura cuenta con un cuarto de equipos de comunicación ubicado en la planta alta 1 del edificio principal, al cual está conectado las diferentes dependencias y pisos del ya mencionado edificio principal. La Figura 8 indica la Topología Física de la Red.

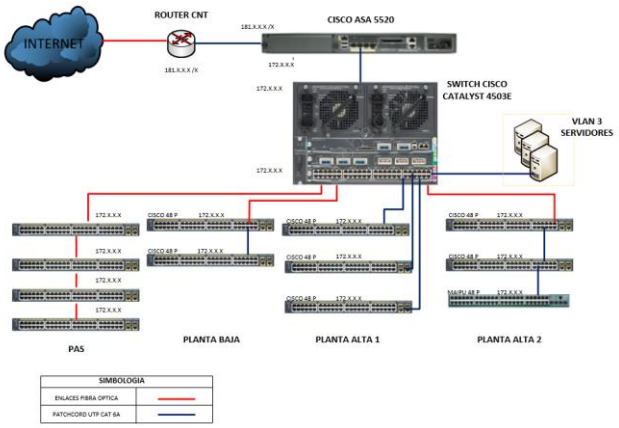

Fig. 8. Topología de la Red del Gobierno Provincial de Imbabura

El proveedor de servicios mediante un router CISCO 881 se conecta a la red pasando por el Switch CISCO ASA 5520 el cual cumple las funciones de Firewall, a continuación se conecta el Switch principal el mismo que cumple las funciones de CORE, este equipo tiene características y funciones de Capa 3, y es el encargado de recibir todas los enlaces de Conexión de Fibra Óptica entre edificios y entre pisos como se muestra en la Figura 2.

Los switch de acceso, tienen características y funciones de capa 2, son administrables y permiten la interconexión de todos los usuarios a la red de la Prefectura de Imbabura. La Figura 7 muestra la topología física de la red.

A. *Cuarto de Comunicaciones*

El Cuarto de Equipos de comunicación está ubicado en la Dirección de Tecnologías de la Información del edificio principal, éste cuenta con los siguientes elementos, como se muestra en la Figura 9.

- ✓ CISCO ASA 5520
- ✓ Switch CISCO 4503E (CORE
- ✓ 3 Switch CISCO Catalyst 2960S
- ✓ Switch CISCO Catalyst 2960X
- ✓ Armario de Servidores

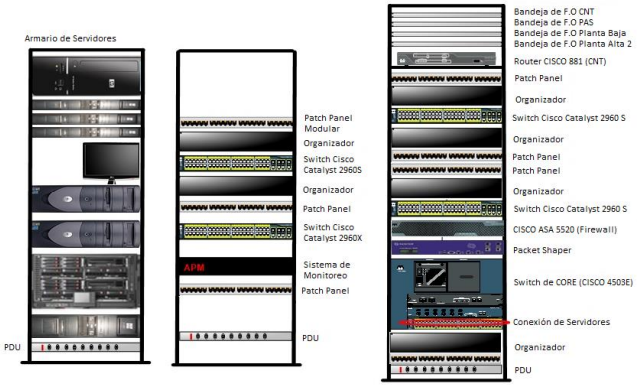

Fig. 9. Distribución de Equipos en el Cuarto de Comunicaciones

B. *Armario de Servidores*

El cuarto de comunicaciones alberga varios servidores, los cuales se listan a continuación:

- ✓ Servidor de Archivos (Alfresco)
- ✓ Servidor Web (Joomla)
- ✓ Servidor de Desarrollo de Software (Mantis)
- ✓ Servidor de Obtención de Licencias (Arcgis)
- ✓ Servidor de Gestión Documental (Quipux)
- ✓ Servidor Cloud (OwnCloud)
- ✓ Servidor de Camaras
- ✓ Servidor de Relojes Biometricos
- ✓ Servidor Proxy (Squid)
- ✓ Servidor DNS (OpenDNS)
- ✓ Servidor Ambiente de Desarrollo
- ✓ Servidor Geolocalización
- ✓ Servidor Sistema Financiero Contable
- ✓ Servidor de Streaming de Video
- ✓ Servidor de Telefonía IP
- ✓ Servidor DNS (OpenDNS)

Para este proyecto se realizará la coexistencia del Servidor Web y Servidor DNS. Estos se encuentran alojados en distintos equipos, los cuales se muestran en las Fichas Técnicas. El Servidor Blade Alberga la mayoría de Servidores, este cuenta con una distribución de 12 cuchillas divididas en 3 partes:

- ✓ 2 Servidores HP Proliant BL460c Generación 7
- ✓ 1 Servidor HP Proliant BL460c Generación 8

Dentro del Armario de servidores se ubica un dispositivo para almacenamiento y además varios equipos que se utilizan como servidores como se muestra en la Figura 10.

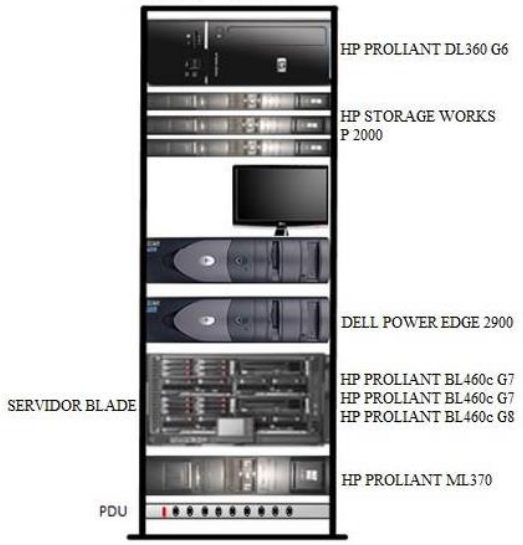

Fig. 10. Armario de Servidores

IV. METODOLOGÍA DE TRANSICIÓN DE IPV4 A IPV6 EN LA PREFECTURA DE IMBABURA

A. *Implementación de la metodología*

1) Etapa de información: Esta etapa se ha dividido en dos fases, la realización de encuestas acerca del protocolo IPv6, y la tabulación de los datos obtenidos. Con esto se aporta para que los encargados de la administración y soporte de la Dirección de Tecnologías de la Información de la Prefectura de Imbabura, estén informados acerca de la adopción a futuro de este protocolo.

Las encuestas irán dirigidas a todo el personal de TIC's, ya que tienen mayor conocimiento dentro del área de sistemas y redes de comunicación, el total de personal dentro de este departamento es de Nueve personas.

Encuestas: El objetivo de las encuestas, es saber qué conocimiento e interés posee el grupo sobre el protocolo IPv6.

La encuesta está dividida en cuatro partes y cada una de ellas se refiere a un tema en específico:

- **Parte I:** Conocimientos Generales de IPv6
- **Parte II:** Distribución de Información del Protocolo
- **Parte III:** Uso de Redes Nuevas
- **Parte IV:** Factor de Desventajas del Protocolo

2) Etapa de elaboración del plan de transición

- **Manual de Petición de Recursos IPv6 a LACNIC:** El proveedor de servicios de internet CNT al cual se encuentra conectada la red de datos la Prefectura de Imbabura, actualmente no brinda el servicio compartido de IPv4 a IPv6 por lo q se hizo necesario investigar cómo obtener un recurso de direcciones para una futura implementación del protocolo. Para esto existe la organización LACNIC que permite obtener un registro y asignación de direcciones IPv6 para organizaciones y usuarios finales ubicadas en América Latina y Caribe
  LACNIC contribuye al desarrollo de internet en la región mediante una política activa de cooperación. Para solicitar un bloque IPv6 como Usuario Final, LACNIC ofrece una asignación de direcciones IPv6, para poder encontrar sus políticas y formularios, es necesario entrar a su página oficial.
  A pesar de que hoy en día no se exige la aplicación de este protocolo, ni en el mercado corporativo, residencial y mucho menos en el estatal, es necesario mantenerse preparado para una futura migración. Para realizar esta petición de recursos se deben seguir los siguientes pasos:

  - ✓ Ingresar al portal IPv6 de LACNIC a la dirección http://portalipv6,lacnic.net
  - ✓ Click en la pestaña IPv6 y escoger la opción ¿Cómo obtener un bloque de direcciones IPv6?
  - ✓ Llenar el formulario correspondiente a usuarios finales
  - ✓ Finalmente luego de haber llenado la información se debe realizar el envío de la solicitud de recursos y esperar a que LACNIC envie su respuesta.

- **Plan de direccionamiento IPv6:** En la Tabla I se describe el direccionamiento IPv6 en base a las VLAN's reales de la Prefectura de Imbabura.

TABLA I
DIRECCIONAMIENTO IPV6 EN BASE A VLANS

NOMBRE	VLAN	GATEWAY IPv4DIR IPv4	DIR IPv6	GATEWAY VLAN IPv6
ADMIN_EQUIPOS	2	192.16.2.1	2001:DB8:3000:2::/64	2001:DB8:3000:2::1/64
SERVIDORES	3	192.16.3.1	2001:DB8:3000:3::/64	2001:DB8:3000:3::1/64
GESTION_TECNOLOGICA	4	192.16.4.1	2001:DB8:3000:4::/64	2001:DB8:3000:4::1/64
PREFECTURA	5	192.16.5.1/64	2001:DB8:3000:5::/64	2001:DB8:3000:5::/64
PROCURADURIA	6	192.16.6.1/64	2001:DB8:3000:6::/64	2001:DB8:3000:6::/64
PLANIFICACION	7	192.16.7.1/64	2001:DB8:3000:7::/64	2001:DB8:3000:7::/64
GESTION_TECNICA	8	192.16.8.1/64	2001:DB8:3000:8::/64	2001:DB8:3000:8::/64
RELACIONES_PUBLICAS	9	192.16.9.1/64	2001:DB8:3000:9::/64	2001:DB8:3000:9::/64
ADMIN_GENERAL	10	192.16.10.1/64	2001:DB8:3000:A::/64	2001:DB8:3000:A::/64
INFRAESTRUCT_FISICA	11	192.16.11.1/64	2001:DB8:3000:B::/64	2001:DB8:3000:B::/64
DESARROLLO_ECONOM	12	192.16.12.1/64	2001:DB8:3000:C::/64	2001:DB8:3000:C::/64
PAS	13	192.16.13.1/64	2001:DB8:3000:D::/64	2001:DB8:3000:D::/64
WIFI	20	192.16.14.1/64	2001:DB8:3000:E::/64	2001:DB8:3000:E::/64

WIFI_EXTERNA	15	192.16.15.1/64	2001:DB8:3000:F::/64	2001:DB8:3000:F::/64
BODEGA	16	192.16.16.1/64	2001:DB8:3000:10::/64	2001:DB8:3000:10::/64
FAUSTO-GIS	17	192.16.17.1/64	2001:DB8:3000:11::/64	2001:DB8:3000:11::/64
FISCALIZACION	18	192.16.18.1/64	2001:DB8:3000:12::/64	2001:DB8:3000:12::/64
CONTRATACIÓN PÚBLICA	19	192.16.19.1/64	2001:DB8:3000:13::/64	2001:DB8:3000:13::/64
INVITADOS	30	192.16.30.1/64	2001:DB8:3000:1E::/64	2001:DB8:3000:1E::/64
RELOJES_BIOM	31	192.16.31.1/64	2001:DB8:3000:1F::/64	2001:DB8:3000:1F::/64
CAMARAS	32	192.16.32.1/64	2001:DB8:3000:20::/64	2001:DB8:3000:20::/64
TELEFONIA	40	192.16.40.1/64	2001:DB8:3000:28::/64	2001:DB8:3000:28::/64
MUTUALISTA	50	192.16.50.1/64	2001:DB8:3000:32::/64	2001:DB8:3000:32::/64
ENLACE_EQUIPOS	101	192.16.101.1/64	2001:DB8:3000:65::/64	2001:DB8:3000:65::/64

La Tabla II muestra el direccionamiento para la WAN y LAN de la Prefectura de Imbabura.

TABLA II
DIRECCIONAMIENTO IPV4 E IPV6

NOMBRE	DIR IPv4	DIR IPv6
OUTSIDE (WAN) ASA	192.168.0.150/24	2001:DB8:3000::150/64
INSIDE (LAN) ASA	192.16.2.2	2001:DB8:3000:2::2/64
IP PUBLICA CNT	192.168.0.225/24	2001:DB8:3000::225/64
CORE	192.16.2.1/24	2001:DB8:3000:2::1/64
Red Local Sumarizada	192.16.0.0/16	

- **Plan de transición de acuerdo a los objetivos de la Prefectura de Imbabura:** Es conveniente que las instituciones públicas comiencen a prepararse, ya que, es posible empezar a adoptar esta tecnología, de tal manera, tomando en cuenta el objetivo institucional de "Tecnificar los procesos de administración y Gestión Institucional" se ha determinado seguir los siguientes pasos que pueden guiar a realizar la transición.

  - ✓ Hoy en día existen proveedores de servicios de internet que ofrecen conectividad IPv6. Se debe consultar al ISP sobre cómo va a brindar el servicio, sea compartiendo protocolos o solo acceso IPv6.
  - ✓ Controlar los equipos IPv4, específicamente los Switchs, servidores, PCs y dispositivos móviles de usuarios, para determinar los que admiten IPv6.
  - ✓ Realizar una auditoría de los Servicios y Aplicaciones para identificar los que están habilitados el protocolo IPv6.

  Para hacer uso de la información investigada, hay que identificar las partes de red de la institución que deberán cambiarse para adoptar IPv6, y para implementar esta tecnología es necesario tomar en consideración la probabilidad de necesitar recursos especializados en IPv6.

  - ✓ Utilizar Dual Stack (Doble Pila), para coexistir entre protocolos IPv4 e IPv6 en la red, ya que éstos pueden ser ejecutado en paralelo e independientemente, sin necesidad de túneles ni servicios de traducción, y así salir de forma gradual de IPv4.
  - ✓ Es necesario utilizar servicios de traducción para brindar la conectividad a los usuarios IPv6 que necesitan tener acceso a servicios y aplicaciones en IPv4. Este proceso se consigue llevar a cabo con el levantamiento de NAT64 y DNS64.
  - ✓ Supervisar el proceso y efectos de la transición de IPv6 mediante pruebas (en redes simuladas) que representen el funcionamiento de los dispositivos que conforman la red sobre el protocolo de internet versión 6 en la institución con la finalidad de observar ventajas y desventajas del proceso.

- **Selección del mecanismo de transición:** Tomando en cuenta las características de la red de la Prefectura de Imbabura, donde se plantea las metodologías de transición para su posterior implementación, y luego de haber analizado los dispositivos de red y servidores, se hace necesario utilizar una comparación técnica para escoger el método que mejor se adapte a la institución. En la Tabla III, se realiza una descripción de cada uno de los mecanismos de transición tomando en cuenta su forma de operación, configuración, ventajas y desventajas.

TABLA III
ANALISIS COMPARATIVO DE LOS MECANISMOS DE TRANSICIÓN

METODOS	Dual Stack	Túneles	Traducción
Forma de Operación	Utiliza de forma simultánea IPv4 e IPv6 en cada nodo de la red, lo que permite que los dos protocolos puedan interactuar entre sí de manera transparente.	Envía paquetes IPv6 dentro de paquetes IPv4 y viceversa, para transportarlos sobre el enrutamiento IPv4.	Traduce cabeceras IPv4 en cabeceras IPv6 y viceversa, realiza conversiones de direcciones o actúa en el intercambio de trafico TCP a UDP.
Configuración	Router, Switchs y host se configuran para admitir ambos protocolos. Cada uno de los nodos posee los dos stacks de protocolos.	Son configurados de forma automática, ya que los extremos del túnel están determinados por las direcciones IPv4 encapsuladas dentro de direcciones IPv6	Requiere tener habilitados los mecanismos de traducción IPv4 e IPv6 en los routers de las dos redes.

Ventajas	Administración conjunta de ambos Protocolos de internet.	Permite transmitir paquetes IPv6 mediante la infraestructura IPv4, sin necesidad de cambios a los mecanismos de enrutamiento.	Opera de distintas formas, traduciendo cabeceras IPv4 en cabeceras IPv6 y viceversa
Desventajas	Requiere que todo el equipamiento soporte los dos protocolos.	El uso de túneles genera retardo en una transmisión de datos.	No es una técnica deseable a largo plazo.

La transición de IPv4 a IPv6 no es una tarea sencilla, por lo que debe realizarse de una manera progresiva mientras sea posible la coexistencia entre los dos protocolos, teniendo en cuenta que los servicios que la institución presta no deben afectarse.

Luego de haber estudiado cada uno de los métodos y el análisis efectuado a la infraestructura de la red de la Prefectura de Imbabura, se pudo determinar que esta tiene compatibilidad con el protocolo IPv6, por lo que se escogió el método de coexistencia que se adapta de mejor manera a esta situación.

Por lo tanto, se utilizará el mecanismo de Dual Stack ya que este al ser una metodología de transición que trabaja sobre una red nativa IPv6, garantiza la conectividad de los dos protocolos desde el Firewall ASA hacia el Switch de CORE el cual realiza la distribución a cada uno de los Switchs de acceso para llegar a los host alojados en la red interna de la Prefectura de Imbabura, este método es adecuado debido a que todos los dispositivos de red son compatibles con el Protocolo IPv6.

Para el manejo de aplicaciones se vio la necesidad de utilizar métodos de traducción como son el NAT64 y DNS64, ya que estos no trabajan en una red basada en ipv4, sino en una red basada en ipv6, permitiendo la interconexión mediante el envío de paquetes IPv6 dentro de la red IPv4.

Debido a que no todas las aplicaciones de la red soportan el manejo de IPv6, se desarrolla la simulación de las aplicaciones DHCP, WEB y DNS, con la finalidad de probar el funcionamiento de los traductores de red, estos servicios fueron sugeridos por el administrador de la red.

Por tal razón se realizará el uso de estas metodologías para la simulación de la transición, tomando en cuenta que el proyecto al ser implementado no afecte a la estructura de red.

3) Etapa de implementación y configuración de la metodología: Tomando en cuenta que la topología de la red de la Prefectura de Imbabura tiene un modelo jerárquico, las configuraciones han sido realizadas de manera descendente, partiendo desde el Nivel de acceso, que en el caso de esta red está formado por el Switch de CORE y el Switch ASA (Firewall), atravesando por los Switchs de distribución los cuales están representados por los Switch 2960 de cada planta del edificio, llegando así a los servicios y aplicaciones que brinda la Institución.

- **Configuración de Router 881:**En este equipo de red no se puede realizar ninguna configuración, debido a que el proveedor de Internet no permite la manipulación del mismo, este router solamente cuenta con servicio sobre IPv4, ya que en la actualidad el proveedor de servicios CNT no ofrece la utilización compartida de IPv4 e IPv6.
- **Configuraciones en Firewall CISCO ASA5520:** La configuración del Firewall está basada en el control del tráfico de red y enrutamiento, es decir, se establecen las reglas que permiten o deniegan la comunicación entre las zonas INSIDE y OUTSIDE.
- **Configuraciones de Switch CISCO 4503 (CORE):** La configuración de las VLANS de la red local y la comunicación de ellas hacia el ASA 5520 se realizan en el Switch CORE. A continuación se activa VTP cliente para que se realice la propagación hacia los switch de distribución, además se activa el direccionamiento IPv4 e IPv6 para facilitar la coexistencia.
- **Configuración Switch CISCO 2960:** En una red conmutada, las VLAN separan a los dispositivos en diferentes dominios de colisión y subredes de Capa 3. Los dispositivos dentro de una VLAN pueden comunicarse entre sí sin necesidad de ruteo.
  El diseño de la topología segmenta la red que se muestra en la Figura 11, según el grupo o la función a la que corresponde el dispositivo. Por ejemplo, la VLAN del departamento de Tecnologías de la Información sólo tendrá dispositivos asociados con el departamento de Tecnología, mientras que en el departamento de Fiscalización la VLAN sólo tendrá dispositivos relacionados con Fiscalización. Si se habilita el ruteo, los dispositivos de cada VLAN pueden comunicarse entre sí, sin necesidad de que estén todos en el mismo dominio de transmisión.
  Dicho así, para que se propaguen las VLANs previamente configuradas en el Swiths de CORE se debe habilitar en cada Switch de la topología el cliente VTP y el puerto en modo troncal mediante los siguientes comandos para así recibir las actualizaciones de las VLANs.

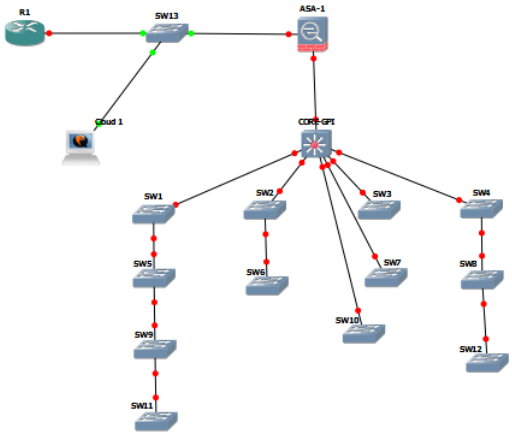

Fig. 11. Topología de la red

- **Configuración de aplicaciones seleccionadas:** Los servicios y aplicaciones se van a levantar sobre la plataforma

de software libre CentOS 6.4, con la finalidad de solventar la funcionalidad de la red en doble pila. El Sistema Operativo debe estar previamente instalado (la instalación CentOS se encuentra en el Anexo D). El desarrollo de las aplicaciones sirve como base demostrativa en el desarrollo del proceso de transición de los protocolos de internet IPv4 e IPv6.

- ✓ *Servidor Web:* En el levantamiento del Servidor WEB se establecerá que los servicios funcionen con los dos protocolos de internet (IPv4 / IPv6).
  El Servidor debe estar configurado en la interfaz tanto en IPv4 como en IPv6, con esto podrá recibir peticiones de los usuarios de ambos protocolos. En la Figura 12 se puede observar el funcionamiento de esta aplicación.

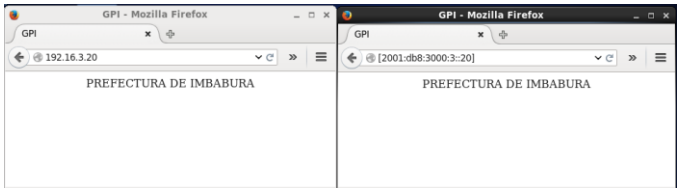

Fig. 12. Prueba de funcionamiento del servidor Web

- ✓ *Servidor DNS:* Para el funcionamiento del DNS64 es necesario instalar uno de los paquetes desarrollado para el servidor de nombre de dominios, en CentOS este paquete se llama bind.
  Para el funcionamiento del NAT64 es necesario instalar uno de los paquetes desarrollado para la traducción de direcciones de red, en CentOS este paquete se llama tayga.

V. CONCLUSIONES

Una de las principales razones de la creación del protocolo IPv6, fue la escasez de direcciones disponibles IPv4, es decir que la capacidad de asignación de direcciones se extiende a un rango mucho mayor, en comparación con el Protocolo de Internet versión 4, dando una solución a la necesidad de conectar una gran cantidad de dispositivos a la red.

Cada día es más importante que las instituciones tanto públicas como privadas conozcan sobre el protocolo IPv6, para que puedan planificar su uso en la infraestructura de red, de tal manera que en el momento que sea necesaria una transición completa, estas redes puedan adaptarse de manera efectiva al protocolo.

Luego de haber realizado el análisis de la red de datos de la Prefectura de Imbabura se pudo observar que todos los equipos que funcionan en la red son compatibles con el protocolo IPv6, con la realización de las encuestas se pudo determinar que a pesar del interés sobre la adopción de este protocolo la mayoría de personal principalmente de la Dirección de TIC's no conocen a profundidad sobre el tema y les gustaría recibir capacitaciones sobre el mismo.

Al realizar un análisis comparativo de los métodos de transición se pudo determinar que utilizar el método de doble pila era el más idóneo para los equipos de red de la Prefectura de Imbabura, ya que permite que cada uno de los protocolos trabajen de manera independiente, y a la vez todos los usuarios puedan acceder de manera continua a la red, sin causar interrupciones o caídas.

En cuanto a la implementación de aplicaciones se determinó el uso de mecanismos de traducción DNS64 y NAT64, siendo así, los usuarios que se encuentren solo en IPv6 deberán acceder a los diferentes servicios que aun trabajen específicamente en IPv4, lo cual garantiza una coexistencia de los protocolos.

Se realizó un plan de direccionamiento basado en la distribución existente en IPv4, se utilizó direcciones de acuerdo al RFC 4291, dejando así un modelo a seguir para al momento de realizar la implementación en la Prefectura de Imbabura.

Se utilizó el software GNS3 para la simulación, permitiendo la comprobación del funcionamiento del mecanismo de transición planteado, para esto se configuro de manera jerárquica cada uno de los dispositivos de red partiendo desde el Firewall Cisco ASA, pasando por el Switch de CORE y los Switch de acceso que permiten llegar al usuario final.

El análisis de factibilidad mostró que la implementación en un futuro de este proyecto es de suma importancia ya que permitirá que la Prefectura de Imbabura este a la vanguardia de la tecnología, pero para realizar este proceso se debe capacitar a cada miembro del personal para que conozcan más sobre la utilización de este protocolo.

REFERENCIAS

Defense Advanced Research Projects Agency. (Septiembre de 1981). Internet Protocol. Obtenido de IETF: http://tools.ietf.org/html/rfc791

Ahuatzin Sánchez, G. (Enero de 2005). Desarrollo de un esquema de traducción de direcciones IPv6-IPv4-IPv6. Obtenido de http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/ahuatzin_s_gl/capitulo2.pdf

Alonso, J. (2008). LACNIC. Obtenido de Coexistencia y Transición: http://www.labs.lacnic.net/site/sites/default/files/ES-Transicion.pdf

Alvarez, E. (2009). Introducción a IP version 4. Obtenido de Notas de clase IPv4: http://www-2.dc.uba.ar/materias/tc/downloads/apuntes/ipv4.pdf

Blank, A. G. (20 de Febrero de 2006). TCP/IP Foundations. San Francisco, Estados Unidos. Obtenido de http://www.eblib.com

Boronat Seguí, F., & Montagud Climent, M. (2013). Direccionamiento e Interconexión de Redes basada en TCP/IP (IPV4/IPV6, DHCP, NAT, Encaminamiento RIP y OSPF). Valencia: Editorial de la Universidad Politécnica de Valencia.

CCM. (Febrero de 2016). OpenDNS. Obtenido de http://es.ccm.net/faq/410-opendns-un-dns-rapido-y-util

Chamba, D. F. (2015). Universidad Regional Autónoma de los Andes Uniandes. Obtenido de http://www.dspace.uniandes.edu.ec/bitstream/123456789/333/1/TUAIS014-2015.pdf

Cicileo, G. (2012). Portal IPv6. Obtenido de Mecanismos de Transición: http://portalipv6.lacnic.net/mecanismos-de-transicion/

Cicileo, G., Gagliano, R., O'Flaherty, C., Olvera Morales, C., Palet Martínez, J., Rocha, M., & Vives Martínez, Á. (2009). IPv6 para Todos: Guía de uso y aplicación para diversos entornos. Buenos Aires: Internet Society. Capítulo Argentina.

CISCO. (2013). Catalyst 4500 Series Switches. Obtenido de http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-series-switches/data_sheet_c78-530856.pdf

CISCO. (Mayo de 2013). Catalyst 4503-E. Obtenido de

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1982.pdf

CISCO. (19 de Febrero de 2013). CISCO ASA 5520. Obtenido de http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1932.pdf

CISCO. (2014). Cisco 880 Series Integrated Services Routers. Obtenido de http://www.cisco.com/c/en/us/products/collateral/routers/887-integrated-services-router-isr/data_sheet_c78_459542.pdf

CISCO. (2015). Cisco Line Cards. Obtenido de http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/catalyst-4500-series-line-cards/product_data_sheet0900aecd802109ea.pdf

CISCO. (2016). Cisco Catalyst 2960-X Series Switches. Obtenido de http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/data_sheet_c78-728232.pdf

CISCO. (s.f.). Cisco Catalyst 2960 Series Switches. Obtenido de http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-series-switches/product_data_sheet0900aecd80322c0c.html

Coellar Solórzano, J., & Cedeño Mendoza, J. (2013). Propuesta para la Transición de IPv4 a IPv6 en el Ecuador a través de la Supertel. Guayaquil: Universidad Católica de Santiago de Guayaquil.

Collado, E. (25 de Mayo de 2009). IPv6. Obtenido de http://eduangi.com/blog/2009/05/25/cabeceras-de-extension-de-ipv6/

Definición de UNIX. (2010). Obtenido de ALEGSA: http://www.alegsa.com.ar/Dic/unix.php

DELL. (Mayo de 2006). Servidor DELL PowerEdge 2900. Obtenido de http://www.dell.com/downloads/emea/products/pedge/es/PE2900_Spec_Sheet_Quad.pdf

Edmond, K., & Whitney, T. (8 de Julio de 2012). La Historia de IPv6. Obtenido de The Prisma - The Multicultural Newspaper: http://www.theprisma.co.uk/es/2012/07/08/la-historia-de-ipv6/

Gerometta, O. (19 de Noviembre de 2011). IPv6 - Algo de Historia. Obtenido de Mis Libros de Networking: http://librosnetworking.blogspot.com/2011/11/ipv6-algo-de-historia.html

Gerometta, O. (4 de Enero de 2015). Mis Libros de Networking. Obtenido de es considerada una estrategia de corto plazo pero que permite la coexistencia de ambas redes para facilitar una transición hacia la red IPv6.

Gobierno de España . Ministerio de Industria, Energía y Turismo. (s.f.). IP.v6 Protocolo de Internet Versión 6. Obtenido de http://www.ipv6.es/es-ES/transicion/quees/Paginas/Transicion.aspx

Gobierno de España. (2010). IP.v6 Protocolo de Internet Versión 6. Obtenido de ¿Qué es IPv6?: http://www.ipv6.es/es-ES/introduccion/Paginas/QueesIPv6.aspx

Gobierno de España: MIET. (s.f.). Protocolo de Internet Versión 6. Obtenido de http://www.ipv6.es/es-ES/Faqs/Paginas/tecnicas.aspx#14

Guillermo, C. (s.f.). IPv6 Portal. Obtenido de http://portalipv6.lacnic.net/mecanismos-de-transicion/

Hewlett Packard Enterprise. (25 de Noviembre de 2015). HPE MSA P2000 G3 MSAS. Obtenido de http://www8.hp.com/h20195/v2/GetPDF.aspx/c04168365.pdf

Hewlett Packard Enterprise. (22 de Enero de 2016). HPE BladeSystem c3000 Enclosure. Obtenido de http://www8.hp.com/h20195/v2/GetPDF.aspx/c04128340.pdf

HP. (Marzo de 2003). Servidor Proliant ML370 G3. Obtenido de http://h10032.www1.hp.com/ctg/Manual/c00690216.pdf

HP. (14 de Octubre de 2011). HP Proliant DL360 G6. Obtenido de http://www.nts.nl/site/html/modules/pdf/Server/HP%20Proliant%20DL360G6.pdf

Prefectura de Imbabura. (2015). Prefectura de Imbabura. Obtenido de http://www.imbabura.gob.ec/

Sánchez Pinos, D. (2006). Herramientas de Transición a IPv6. Obtenido de http://dspace.ups.edu.ec/bitstream/123456789/205/3/Capitulo%202.pdf

Carlos A. Vásquez Nació en Quito - Ecuador el 19 de Septiembre de 1981. Ingeniero en Electrónica y Telecomunicaciones, Escuela Politécnica Nacional en 2008. Actualmente es docente de la Carrera de Ingeniería en Electrónica y Redes de Comunicación en la Universidad Técnica del Norte, Ibarra -Ecuador, y es egresado de la Maestría en Redes de Comunicación, Pontificia Universidad Católica del Ecuador, Quito - Ecuador

Stalin A. Hidrobo nació el 23 de Marzo de 2008, realizó sus estudios primarios en la Escuela “La Merced”. En el año 2004 obtuvo su título de Bachiller en ciencias especialización físico matemáticas en el colegio “Teodoro Gómez de la Torre”. Actualmente, egresada de la Carrera de Ingeniería en Electrónica y Redes de Comunicación de la Universidad Técnica del Norte de la ciudad de Ibarra.