ISSN 1909-2407

METODOLOGÍA DE TRANSICIÓN DE IPV4 A IPV6 EN PYMES.

Methodology of transition from IPV4 to IPV6 in SMES.

Andrés Alejandro Mora Franco[1]; Jairo Alonso Mesa Lara[2;]

1. Ingeniero de Sistemas y Computación. Docente Escuela de Ingeniería de Sistemas y Computación. Universidad Pedagógica y Tecnológica de Colombia. Grupo de Investigación TELEMATICs Uptc. Email: Andres.mora@uptc.edu.co
2. Magister en Ciencias de la Información y las Comunicaciones. Ingeniero Electrónico. Docente Escuela de Ingeniería de Sistemas y Computación. Universidad Pedagógica y Tecnológica de Colombia. Grupo de Investigación INFELCOM Uptc. Email: Jairo.mesa@uptc.edu.co

Recibido: 18/06/2017 Revisado: 22/06/2017 Aceptado: 10/08/2017

COMO CITAR ESTE ARTÍCULO: Mora AA, Mesa JA. Metodología de transición de IPV4 a IPV6 en PYMES. Rev.salud.hist.sanid.on-line 2017;12(2): 75-86 (Mayo-Agosto). Disponible en http://www.shs.agenf.org/ Fecha de consulta ( ).

RESUMEN

En el presente artículo se expone una propuesta de metodología de transición del protocolo de Internet en su cuarta versión (IPv4) a su sexta versión (IPv6) en pequeñas y medianas empresas, la cual fue el resultado del proceso de investigación seguido en el trabajo de grado de maestría titulado METODOLOGÍA PARA LA TRANSICIÓN DE IPv4 A IPv6 PARA PEQUEÑAS Y MEDIANAS EMPRESAS DEL SECTOR TIC, donde se explican las diferentes etapas que la conforman, enfocado a algunas empresas del sector de las tecnologías de la información y comunicación del departamento de Boyacá. Dicha metodología servirá como guía para la transición hacia este nuevo protocolo, debido a la escasez de direcciones IPv4 asignables y a las recomiendas dadas por el gobierno nacional que promuevan dicha migración en cara a la competitividad y la actualización tecnológica. Para la creación de la metodología se revisaron los mecanizamos de transición entre estos dos protocolos, así como cuáles de éstos eran propicios para su implementación en una pequeña y mediana empresa. Como conclusión, se generó un documento guía que servirá de apoyo al personal TI de la empresa para poder llevar a cabo esta tarea; en el presente artículo se explica de forma breve dicha metodología.

Palabras clave: - IPv4; IPv6; doble pila; metodología; protocolo de Internet.

ABSTRACT

In this article a proposed methodology of transition from Internet Protocol in its fourth version (IPv4) to its sixth version (IPv6) in small and medium enterprises, which was the result of the research process followed in the work exposed master's degree titled METODOLOGÍA PARA LA TRANSICIÓN DE IPv4 A IPv6 PARA PEQUEÑAS Y MEDIANAS EMPRESAS DEL SECTOR TIC, where the different stages that make up the methodology, focused on some companies in the information technology and communications department of Boyacá industry are explained. This methodology will guide the transition to this new protocol, due to the shortage of assignable IPv4 addresses and to recommend given by the national government to promote such migration to the competitiveness and technological upgrading. For creating the mechanize the methodology of transition between these two protocols were reviewed and which of these were favorable for implementation in small and medium enterprises. In conclusion, a guidance document that will support the IT staff of the company to carry out this task is generated; in this article briefly explains the methodology.

Keywords: Internet Protocol; double stack; methodology; IPv4; IPv6.

INTRODUCCIÓN

Con el agotamiento de las direcciones IP (IPv4) a nivel mundial, la implementación de su nueva versión (IPv6) y la necesidad de que las pequeñas y medianas empresa (PYMES) puedan acceder a los servicios que sólo estarán disponibles bajo este nuevo protocolo, se presenta una metodología de transición que les permitirá implementarlo.

Una metodología que guíe en el proceso de transición busca disminuir costos y posibles problemas en la implementación, facilitando el proceso para posibles interesados, y permitiéndoles acceder a mecanismos que antes les eran prohibitivos o de difícil instalación, como lo es el establecimiento de esquemas de seguridad para la red.

MIGRACIÓN vs. TRANSICIÓN

Adoptar IPv6 como nuevo protocolo de Internet en una organización puede llegar a ser un evento traumático para los miembros de la misma, esto es debido a los cambios que se tienen que realizar tanto en la infraestructura, como en la forma en la que se manejan los procesos, siendo esta última consideración muy importante, si la empresa tiene relación directa con el campo de las Tecnologías de la Información y las Comunicaciones (TIC).

Particularmente en el caso de IPv6, es una tecnología que se proyecta como nuevo estándar de comunicación a nivel mundial, pero mientras eso sucede, se hace necesario mantener compatibilidad con el viejo protocolo (IPv4), por lo tanto, la migración no es posible, puesto que se perdería la compatibilidad con IPv4 en la red (los dos protocolos son incompatibles entre sí); un proceso de transición es la vía recomendada, se sigue manteniendo activa la cuarta versión del protocolo, mientras toma fuerza la implementación de la sexta a nivel mundial. Llegado el momento, será posible eliminar esa compatibilidad quedando únicamente IPv6 como mecanismo por defecto para la transmisión de información entre equipos en una red de datos. Si se llega a dar esta última etapa, sería posible conseguir un rendimiento adicional en la red donde se trabajará únicamente con IPv6, esto es debido a que los dispositivos no tendrán que dedicar parte de sus recursos a mantener una pila de la cuarta versión del protocolo, pudiendo utilizar toda su capacidad en el nuevo.

ANÁLISIS

En la primera fase del proceso es necesario revisar qué se tiene, qué falta, cómo está configurado y qué características posee la empresa en preparación para fases posteriores como se resume en Figura 1**¡Error! No se encuentra el origen de la referencia.**. En esta fase hay que conocer la empresa, puesto que el proceso de migración no es algo genérico que se pueda aplicar a cualquier organización indistintamente, hay que personalizarlo a

cada una si se quiere obtener buenos resultados. Para esto se hace necesario hacer un inventario de todos los elementos telemáticos que se pueden ver afectados por la implementación de IPv6, iniciando por identificar los equipos físicos (hardware), determinando si estos equipos actualmente soportan IPv6, sus características, ubicación, uso y cualquier información que permita identificarlos dentro del espacio físico y de los procesos de la empresa.

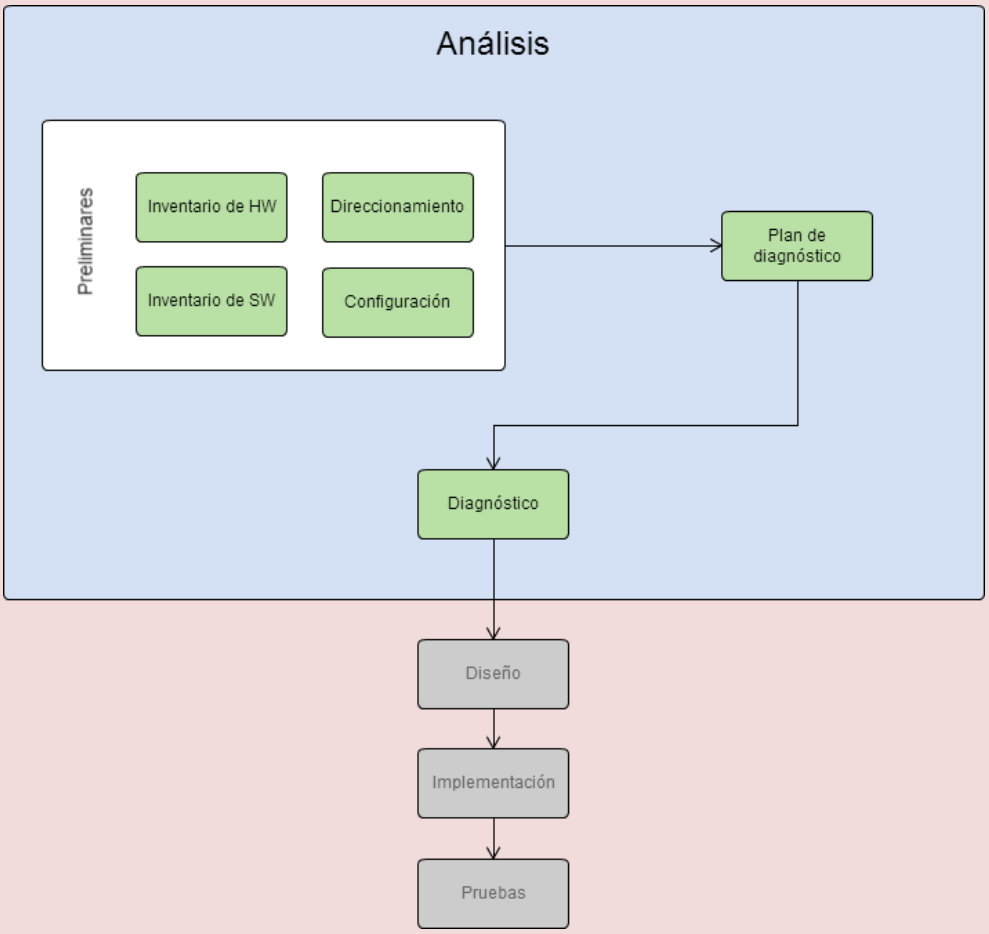

Figura 1. Primera fase. Análisis

Para realizar lo anterior, se sugiere la utilización de hojas de inventario para conocer los tipos y cantidad de dispositivos. No se requiere un diseño específico para este material, lo importante es que se diligencien con la mayor especificidad posible, dependiendo de la cantidad de información existente.

Así mismo, con una lista de chequeo se podrá conocer el nivel de compatibilidad con el proceso de transición; generando estadísticas para preparar un plan de mejoramiento para la futura transición. Aquí es necesario, revisar las características de cada tipo de dispositivo

en su datasheet (hoja de especificaciones), es posible encontrarlo en la página del fabricante; si no es así, en foros especializados o grupos de discusión.

Si es necesario, se puede generar una lista con los elementos que se tendrán que adquirir. Esta lista debe estar sustentada de acuerdo a la necesidad e impacto que generará ese dispositivo (o elemento) en la nueva infraestructura de red. Este paso es importante puesto que ayudará en el proceso de convencer a la gerencia, demostrando la importancia que tienen esos equipos, posibilitando el visto bueno para la aprobación del presupuesto, y su posterior adquisición.

Otro elemento a considerar dentro del inventario, corresponde al software. Acá se contemplan elementos como firmware y aplicativos de la organización, así como los sistemas operativos de uso diario, ya sean de escritorio, servidor y móviles, revisando si son compatibles con la implementación del nuevo protocolo o si alguno requiere iniciar un proceso de actualización o configuración específica para que así lo sea, o si definitivamente son sistemas obsoletos (requiriendo la adquisición de nuevos equipos).

En este paso se genera un análisis del funcionamiento de IPv4, qué tipo de datos se transmiten en la red, para generar una lista de requisitos a tener en cuenta en el proceso de transición, cuánto es el ancho de banda consumido por aplicaciones, usuarios particulares, capacidad máxima del medio (ethernet, o WiFi), entre otros. Esto con el fin de medir el impacto que tenga el proceso de transición en la red finalizado el proceso.

Se tiene que generar un plan que permita llevar de forma controlada el proceso de actualización de aplicaciones. Éste se tiene que acoplar a los mecanismos de gestión de la calidad de la empresa, para que los elementos intangibles estén siempre actualizados. Estos procesos son útiles porque corrigen problemas (posibles vulnerabilidades) y añaden nuevas características a los dispositivos.

Un elemento que es muy importante y que se tiene que considerar, son los relacionados con la seguridad; éstos son imprescindibles en toda infraestructura de red, ya sea la configuración de cada equipo que integre múltiples funciones, o de los dispositivos dedicados a una única tarea. Éstos deben estar claros (bien definidos), son generados a partir de un análisis de necesidades, así como de las características del software instalado, que influya de forma directa en la seguridad de la organización.

Algo que hay que recordar: cuanto más preparados se esté, menos traumática será la implementación.

DISEÑO

Tras conocer el estado de la red, tanto físico, lógico y en su configuración; se podrá iniciar el proceso para definir cómo y cuándo se va a llevar a cabo el proceso de transición. Este diseño tendrá que evaluar los análisis realizados en la fase anterior, para definir qué elementos son los que cumplen con los requisitos exigidos para esta transición, es decir, conocer las necesidades para que el proceso se pueda iniciar, como se resume en Figura 2. Dicha evaluación se desarrolla respecto a los requerimientos de actualizaciones y compras de elementos.

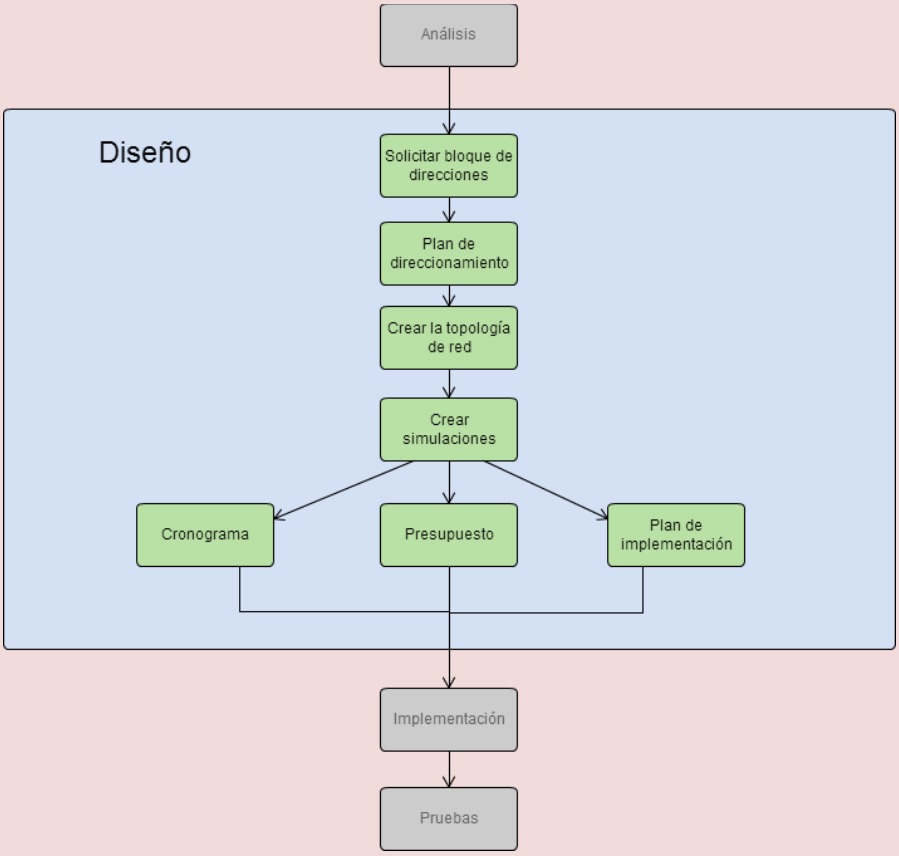

Figura 2. Segunda fase. Diseño

Se busca tener claro un plan de acción para poder contestar las preguntas: ¿Cómo?, ¿Cuándo?, ¿Quién? Y ¿Cuánto? Siendo esta última, uno de los elementos decisivos para que el proceso pase a su siguiente fase. Ayuda a este fin conocer qué se va a hacer (diseño) y cuánto va a costar (presupuesto).

Realizar un diseño de calidad, garantiza una implementación sin mayores inconvenientes, ahorrando recursos, y malestares a los miembros de la empresa. Algunos puntos a considerar en este diseño son: ¿Se cuenta con conexión a internet de calidad?, ¿El ISP ya actualizó su infraestructura "core" (y de transporte) para soportar IPv6, permitiendo la asignación de prefijos a los usuarios?, ¿Se desea invertir (dinero o infraestructura) en

mecanismos adicionales para conectar la red local a redes externas para poder alcanzar nodos IPv6 en Internet?, o por el contrario, ¿Se desea que el tráfico de red no tenga un punto de salida geolocalizado fuera de la empresa?

Al responder las preguntas anteriores será posible definir qué técnica de transición utilizar. Permite trazar un plan de acción que ayudará a conocer cómo proceder, cómo realizar la adopción del protocolo, si se va a efectuar en un día, una semana o más (dependiendo del conocimiento que se recabó de los elementos de la organización), realizándose de forma coordinada en una única configuración general, o si se va a desarrollar de forma paulatina, abarcando un área diferente de la empresa cada vez, hasta alcanzar el 100% de áreas con IPv6 implementado.

Para apoyar en el proceso de toma de decisiones, es necesario realizar simulaciones de la infraestructura de la red donde se piensa implementar, preferiblemente que utilice el firmware real que se implementa en los equipos de cómputo o de red. Una herramienta que permite lo anterior es GNS3 (http://www.gns3.com), donde el personal de TI de la pyme podrá crear el mapa de la red y su topología. Adicionalmente, para cada host en la simulación, se podrá representar como máquinas virtuales (VirtualBox) y para los switches y routers, se utilizarán copias originales de los firmwares utilizados en los dispositivos físicos. Este esquema permitirá:

- Preparar de antemano el procedimiento de transición (configuración de los equipos), puesto que la configuración se puede extrapolar al mundo real.
- Conocer el comportamiento de la red frente a diversos estímulos, por ejemplo, si la configuración en curso pone en peligro la integridad del software de la organización, posibles problemas de seguridad, entre otros.

Al terminar esta fase, se tendrá la red lista para iniciar su proceso de transición (no se ha tocado la configuración de los equipos físicos aún). Se conocen los posibles problemas que pueden surgir, y lo más importante, cómo solucionarlos. Algunos de los documentos que se generan son: el cronograma del proyecto detallando toda actividad, el presupuesto aprobado, según los elementos o servicios que sean necesarios adquirir y el plan de implementación, que corresponde a la serie de pasos y consideraciones a tener en cuenta para realizar la transición. En este último paso sirven en gran medida las simulaciones.

IMPLEMENTACIÓN

Teniendo el plan de implementación, el presupuesto aprobado y el cronograma de actividades, se procede a realizar la implementación del proceso de transición (se resume en Figura 3), para lo cual se puede optar por:

- Implementación de IPv6 de forma nativa o mediante doble pila.
- Utilizando túneles.
- Utilizando traducción.

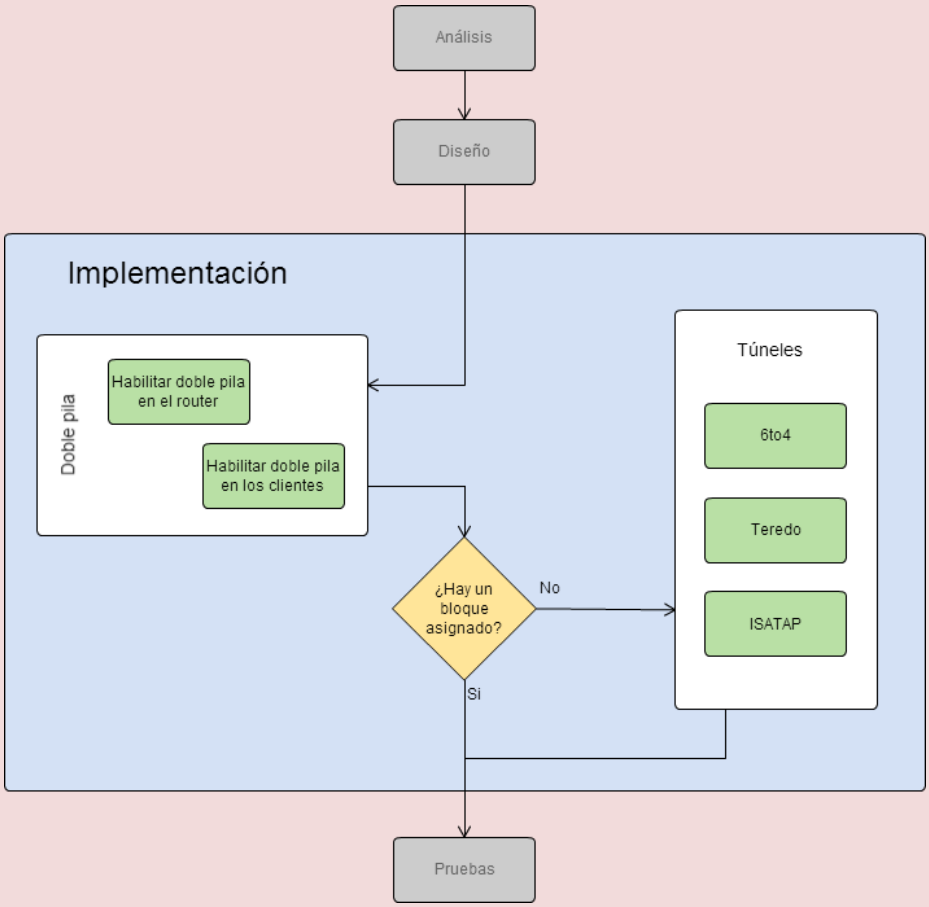

Figura 3. Tercera fase. Implementación

El mecanismo a utilizar dependerá de las características de la empresa y de los riesgos que quieran asumir para la implementación de IPv6 en la infraestructura de red. Algunos de éstos son:

A. IPv6 de forma nativa

Es la opción recomendada cuando no se cuenta con una distribución de red o si se desea hacer una renovación completa de la misma.

La red local funcionaría íntegramente con este nuevo protocolo, sería incompatible con IPv4 (si no se aplican medidas adicionales). Es importante destacar que no siempre se puede llevar a cabo, ya que los tiempos muertos generarían pérdida considerable de trabajo. Así que esta es la opción ideal si hasta ahora se está configurando la infraestructura de datos (o se está planeando una reestructuración tecnológica).

El beneficio de esta técnica es palpable. En un futuro, cuando IPv6 esté establecido a nivel mundial y ya no se implementen tecnologías basadas en IPv4, su uso será natural; no será necesario realizar cambios en su configuración, su transición será nula, ya que ésta se implementó desde un inicio.

B. Doble pila

Consiste en configurar la red bajo el protocolo IPv6, pero sin eliminar IPv4; es decir, los dos protocolos van a coexistir en la red, en el mismo medio, en las tarjetas de red y equipos activos van a estar circulando a la vez los dos tipos de paquetes.

No se realiza cambios en la configuración en la red basada en IPv4, los tiempos muertos y cortes del servicio son mínimos, mientras se configura la nueva pila en los elementos activos de red.

Como ambos protocolos existen al mismo tiempo, será posible alcanzar servidores que trabajen en IPv6 e IPv4 indistintamente. Es transparente para los usuarios.

Los tiempos de instalación y configuración son mínimos, pero los de mantenimiento serían los mismos que se tienen actualmente para la red bajo IPv4, puesto que los elementos como la configuración de reglas de seguridad y listas de acceso se tienen que implementar y mantener en la nueva pila, como se viene haciendo con la antigua. Lo cual significa: doble trabajo.

Actualmente existe preferencia de un protocolo sobre el otro, así:

IPv6 nativo > IPv4 nativo > Túneles y traducción

C. Túneles

Si antes se dijo que no era deseable implementar IPv6 de forma nativa en la red porque se podía perder el acceso a equipos remotos, puesto que la infraestructura que conecta los dos equipos está bajo IPv4, sí es posible contar con dicho acceso mediante la utilización de túneles que unen ambos extremos de la red, atravesando redes intermediarias que son incompatibles con IPv6.

Esta técnica encapsula el tráfico IPv6 en paquetes IPv4, por lo que éstos viajarán por la red antigua sin resistencia alguna. Al llegar a su destino los paquetes sufren un proceso de desencapsulación, volviendo a ser paquetes IPv6 que llegarán al destino. El camino de regreso, es igual al de ida.

Su uso es recomendable cuando se desea enviar paquetes de un protocolo por un canal que no lo soporta.

Es posible encapsular paquetes de la siguiente forma:

- Paquetes IPv6 dentro de paquetes IPv4. Corresponde al método tradicional.
- IPv6 dentro de IPv4, pero cambiando su cabecera, ya sea añadiendo una cabecera GRE (Farinacci, Traina, Hanks, & Li, 1994) o una cabecera UDP (se puede utilizar para atravesar NAT).
- Paquetes IPv4 dentro de paquetes IPv6. No se recomienda.

Según lo anterior, existen varios mecanismos basados en túneles, como lo son: túneles 6in4, tunnel bróker, túneles 6to4, túneles 6RD, túneles DS-Lite, ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), 6over4 y túneles Teredo.

De las anteriores alternativas, 6to4 e ISATAP posibilitan la utilización de túneles en infraestructuras de red limitadas, brindando elementos de seguridad y facilidad de configuración.

D. Traducción

Si la red está configurada para trabajar en IPv6 y se necesita acceder a otra que sólo habla IPv4, existen dos opciones para que se puedan comunicar.

- Aplicar doble pila de protocolos en algún extremo (o en ambos).
- Traducir el tráfico de un protocolo a otro.

Este método corresponde a la última opción, no es aconsejable su implantación puesto que el rendimiento de la red decae drásticamente, sin mencionar que se seguiría dando soporte a un protocolo que prácticamente nació con Internet (Postel, 1981).

Con lo anterior en mente las posibles traducciones serían:

- Traducir redes IPv6 nativas hacia redes IPv4 nativas. Se puede utilizar NAT64 y DNS64.
- La traducción de redes IPv4 nativas hacia redes IPv6 nativas. Se volvió obsoleta en el año 2015 (Aoun. C, 2007). La recomendación en este caso, es aplicar doble pila en la red que es IPv4 nativa, o utilizar otro mecanismo de transición.

Algunos de los mecanismos de transición que aplican traducción son NAT64/DNS64 y 464XLAT.

PRUEBAS

Para analizar el estado de la implementación, se recomienda realizar pruebas de conectividad, tiempos de respuesta y mediciones del ancho de banda máxima (disponible) como se muestra en Figura. 4.

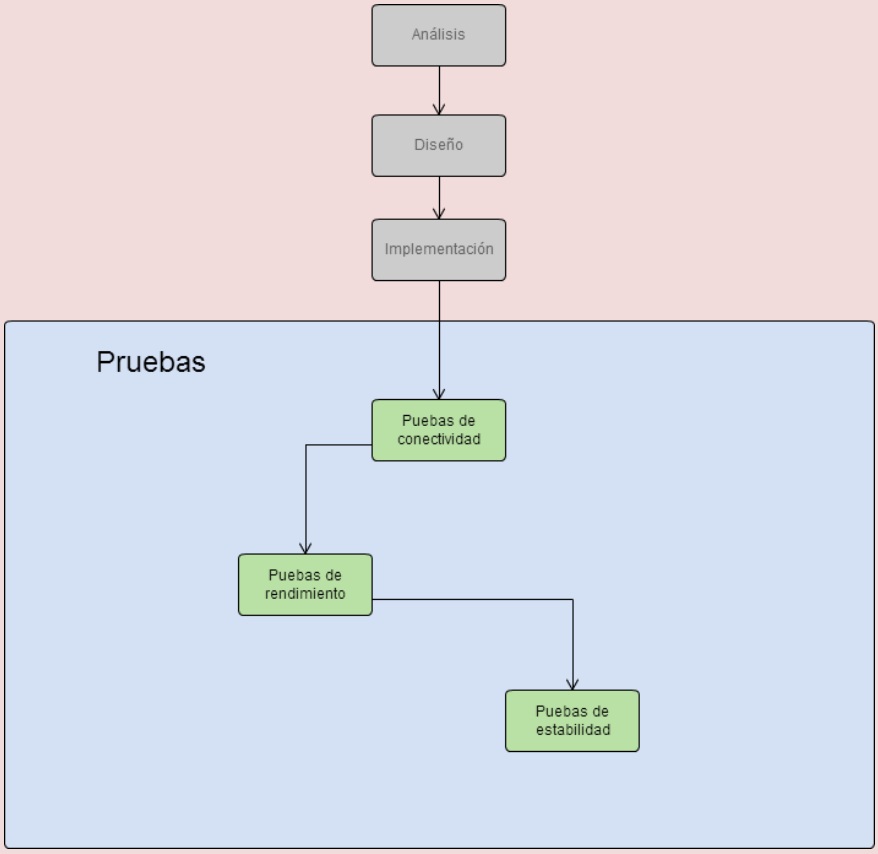

Figura. 4. Cuarta fase. Pruebas

Para medir el estado de conectividad y tiempos de respuesta de la red, se puede hacer uso del protocolo ICMPv6, específicamente *ping*. Si hay algún problema al momento de alcanzar alguna máquina, revisar el estado de su autoconfiguración (SLAAC), o algoritmos de rutas.

Por último, para verificar la capacidad del canal, se puede hacer uso de iPerf, el cual, mediante la generación de tráfico aleatorio, permite medir la capacidad del canal y la velocidad máxima de transmisión. Con esto será posible calcular si la migración supuso alguna pérdida en el rendimiento de la red (comparando los resultados de IPv6 con los de IPv4 antes de implementar el protocolo).

CONCLUSIONES

Al utilizar una metodología de transición que guíe en este proceso, permitirá facilitar el trabajo y disminuirá los posibles costos que de otra forma pondrían en peligro el proyecto, permitiendo conocer de antemano el presupuesto, necesidades particulares de la empresa y otros elementos importantes para su ejecución.

Cada fase alimenta la siguiente, por lo tanto, un buen trabajo de recolección de información y análisis, permitirá una rápida culminación del proyecto, disminuyendo tiempos muertos y repeticiones de tareas de fases anteriores. Así mismo, será posible detectar los posibles problemas que se puedan presentar en la infraestructura de red de la organización tras la implementación, pudiendo conocer las causas y corregirlas, reflejándose en un ahorro de tiempo y dinero.

Gracias a una metodología que guíe a las pymes, éstas podrán adoptar nuevos estándares mundiales y regulaciones nacionales, que les permitirá la adopción de nuevas tecnologías, aumentar su rendimiento y mejorar sus procesos internos, sentando las bases para la expansión del nuevo protocolo a nivel regional.

AGRADECIMIENTOS

Agradezco a los grupos de investigación TelemaTICs e INFELCOM por el apoyo brindado en el proceso de investigación.

REFERENCIAS

Aoun. C, D. . (2007). RFC 4966: Reasons to Move the Network Address Translator- Protocol Translator (NAT-PT) to Historic Status, 1–25. Retrieved from https://www.ietf.org/rfc/rfc4966.txt

Cisco. (2011). IPv6 manual tunnel Configuration Example. Retrieved November 19, 2015, from http://docwiki.cisco.com/wiki/Ipv6_manual_tunnel_Configuration_Example

Cisco. (2012). IPv6 Addressing Guide. Retrieved November 19, 2015, from http://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/February2012/SBA_Ent_BN_IPv6AddressingGuide-February2012.pdf

Farinacci, D., Traina, P., Hanks, S., & Li, T. (1994). RFC 1702: Generic Routing Encapsulation over IPv4 networks. Retrieved from https://tools.ietf.org/html/rfc1702

Postel, J. (1981). RFC 791: Internet Protocol. Retrieved from https://tools.ietf.org/html/rfc791

SURFnet. (2011). Preparing an IPv6 Addressing Plan. Retrieved November 19, 2015, from http://www.rediris.es/conectividad/IPv6_addr_plan4.pdf