METODOLOGÍA DE TRANSICIÓN DE IPv4 A IPv6 EN PyME

Andrés Alejandro Mora Franco
Universidad Pedagógica y Tecnológica de Colombia
+573187683800
andres.mora@uptc.edu.co

Jairo Alonso Mesa Lara
Universidad Pedagógica y Tecnológica de Colombia
+573103041375
jairo.mesa@uptc.edu.co

RESUMEN

En el presente artículo se expone una propuesta de metodología de transición del protocolo IPv4 a 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 en empresas del sector de las tecnologías de la información y comunicación del departamento de Boyacá.

PALABRAS CLAVE

Metodología, transición, IPv6, IPv4, Protocolo de Internet, traducción, túnel.

ABSTRACT

In this article a proposed methodology of transition from IPv4 to IPv6 protocol in small and medium-sized enterprises is exposed, which was the result of the research process followed in the work of master's degree entitled METODOLOGÍA PARA LA TRANSICIÓN DE IPv4 A IPv6 PARA PEQUEÑAS Y MEDIANAS EMPRESAS DEL SECTOR TIC, explaining the different stages that constitute it, focused on companies in the sector of technologies of information and communication of the Department of Boyacá.

KEYWORS

Methodology, transition, IPv6, IPv4, Internet Protocol, translation, tunnel.

1. 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).

De esta manera, el proceso no se puede realizar en una única etapa, puesto que la carga de trabajo requerida y los tiempos muertos a los que se pueden presentar en los dispositivos de la red, pueden obstaculizar las actividades de la empresa. Por este motivo, se recomienda que el proceso se divida en fases y éstas se ejecuten en el momento preciso, intentando programar los diferentes eventos para que no representen un obstáculo a la organización.

Particularmente en el caso de IPv6, es una tecnología que se proyecta como nuevo estándar de comunicación a nivel mundial, pero mientas 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 "retrocompatibilidad" de 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.

2. ANÁLISIS

En esta primera fase es necesario revisar qué se tiene, qué falta, cómo está configurado y qué características posee la empresa en preparación para fases posteriores. 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 éstos 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.

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).

Es conveniente realizar una lista de sistemas operativos (y software en general), detallando la versión instalada y la más reciente disponible. Esto permitirá determinar si presentarán problemas con el nuevo protocolo. Adicionalmente esta lista ayudará a llevar un control para determinar qué aplicativos necesitan actualizarse, lo cual es un proceso necesario a día de hoy. No tener los aplicativos actualizados es una puerta abierta para los atacantes.

Dentro de una PyME es común encontrarse con motores de bases de datos, software contable, administrador de clientes y proveedores, gestión de recursos humanos, aplicaciones de gestión de la calidad, así como software ofimático y antimalware (antivirus, entre otros). Todas esas aplicaciones (sistemas, plataformas, etc.) necesitarán su análisis individual, centrándose en los requisitos que requiere cada una para poder funcionar de forma correcta, como ancho de banda, dependencias de librerías, sistema operativo, uso de las API de otras aplicaciones (interoperabilidad), etc. No es obligatorio recuperar toda esa información, pero en cuanto más se tenga, mejor. Este último requisito es de vital importancia para verificar compatibilidad, puesto que, si interactúa con llamadas al sistema operativo, éste se encargará de tratar el tráfico para que más adelante éste se adapte al nuevo protocolo de forma transparente al usuario y sin carga de trabajo extra al desarrollador. Esta información servirá para determinar qué elemento puede causar problemas al momento de transmitir su información a través del nuevo protocolo.

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. Éstos 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.

De las diferentes políticas de seguridad que se puedan implementar, es una buena práctica identificar qué elementos son importantes para esa arquitectura en particular, y diseñar los mecanismos de aplicación y control para las mismas; éstas tienen que ser acordadas después de discutir las necesidades de la entidad, requisitos internacionales y guías de buenas prácticas para el fortalecimiento de la seguridad a nivel empresarial.

Toda esta información será valiosa al momento de replicarla en la nueva pila del protocolo, puesto que se tendrá que configurar de la misma forma. No es aconsejable que existan diferencias entre la política de seguridad para IPv4 e IPv6, esto generaría ambivalencia, y se vería evidenciado como huecos en la seguridad (vulnerabilidades). El protocolo IP cambió, pero el resto de protocolos del modelo TCP/IP sigue siendo los mismos. No hay que ignorar las diferentes configuraciones, incluida la de seguridad.

También hay que analizar no sólo elementos internos a la empresa, sino todos los que afecten de forma directa o indirecta al proceso, por ejemplo, las características del ISP; ¿cuánto es el ancho de banda?, consultar también sobre la tasa de reúso que maneja, su nivel de implementación de IPv6, etc.

Algo a lo cual no se le presta mucha atención, pero que es importante para que el sistema se comporte como es debido, corresponde a la experticia de los encargados del área de TI (o las personas que desempeñen ese papel en la empresa), ellos serán los encargados de configurar a la medida la infraestructura y su seguridad. Por este motivo será necesario tener en cuenta si se necesita capacitar al personal existente, o directamente hacer una contratación puntual para esa implementación; donde la mejor opción es que el personal tenga ese conocimiento, no siempre va a ser posible pedir asistencia a entes externos a la organización, ya sea por cuestiones de tiempo o privacidad.

Es necesario que se programen jornadas de capacitación, no tienen que ser tan constantes, sólo que cubran el avance de la tecnología que se ha implementado y lo relacionado con temas de seguridad afines. Esto creara personas que puedan reaccionar a problemas de una forma rápida y eficiente, minimizando daños, y a la larga, ahorrando los diferentes tipos de recursos de la organización.

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

3. 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. Dicha evaluación se desarrolla respecto a los requerimientos de actualizaciones y compras de elementos.

Se busca tener claro un plan de acción, poder contestar las preguntas:

- ¿Cómo?
- ¿Cuándo?
- ¿Quién?
- ¿Cuánto?

Siendo esta última, una 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.

Toda modificación que se requiera, ya sea a nivel lógica o física, hace parte de esta etapa. Por ejemplo, un mapa detallado de la red, de la nueva arquitectura (si es que la hay), y el modelo de direccionamiento que se piensa implementar con el nuevo protocolo IP. Teniendo en cuenta que por cada prefijo asignado, serán millones de direcciones posibles, el diseño de una técnica de asignación ayudará a gestionar la forma en la que se entregan a los clientes de la red. Algo para tener en cuenta, entregar direcciones consecutivas a los host, además de pertenecer a la ideología de IPv4, es altamente inseguro, puesto que con sólo recorrer las primeras direcciones se podrá pasar de un equipo al siguiente, a diferencia de incluir elementos aleatorios para ir saltando de dirección a dirección en todo el rango disponible.

Un elemento básico al momento de diseñar el proceso de transición, consiste en crear un plan de asignación de direcciones. Esto se hace mientras, o después de solicitar un bloque de direcciones a la empresa prestadora de servicios de Internet (ISP).

El plan de direccionamiento permitirá definir con certeza la forma en la que se van a gestionar las direcciones IPv6, cómo van a ser asignadas a los host y como éstas van a coexistir con el direccionamiento actual, IPv4. Para más información, puede consultar la guía de direccionamiento IPv6 para PyME de Cisco [1] o el manual de direccionamiento propuesto por RIPE NCC [2]. Para esto se hace necesario aplicar subnetting al prefijo IPv6 asignado por el ISP; en IPv4, esta técnica se utiliza para controlar la cantidad de direcciones que se asignan a una red (creando subredes es posible segmentar la red), en IPv6 se utiliza para optimizar el trazado de rutas y mejorar la definición de la seguridad de la red.

Para ayudar con el cálculo del direccionamiento, se pueden utilizar herramientas como calculadoras para tal fin. Algunos ejemplos son GestioIP[1] e IPPlan[2].

Como consideración, existen varias distinciones (categorías) de clientes, una de esas es según su movilidad, si son fijos o móviles. Partiendo de eso, se podría crear políticas para cada tipo de cliente, teniendo sus propias listas de control de acceso (ACL), direcciones fijas (gracias a la capacidad de movilidad que brinda el nuevo protocolo), incluso cuánto ancho de banda puede consumir.

Una de las partes más importantes de la presente fase corresponde a la selección de los métodos de transición a IPv6 que se ajustan a las características particulares de la empresa (analizados en la primera fase, análisis). Su selección se realizará según las necesidades de la adopción de nuevas tecnologías, del presupuesto asignado y del tiempo que se le vaya a dedicar al proceso. La gerencia juega un papel muy importante en este paso, por lo que explicarle las diferencias y características de cada método, y el beneficio que representaría para la organización, garantizarán su adopción, o por otra parte, su rechazo.

Para apoyar en el proceso de toma de decisiones, es necesario realizar simulaciones de la infraestructura de la red donde se

[1] GestioIP: http://www.gestioip.net/cgi-bin/subnet_calculator.cgi

[2] IPPlan: http://iptrack.sourceforge.net/

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[3], 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.

Si se desea utilizar máquinas virtuales (VirtualBox) en lugar de clientes simulados, primero hay que contar con algunas máquinas virtuales instaladas. Hay que recordar que es necesario agregar las máquinas de forma manual al simulador en la opción correspondiente en Preferencias, de no ser así, no aparecerán en la herramienta para añadirlas al proyecto.

Para efectos de la simulación es buena idea tener instalada una máquina virtual y proceder a clonarla, de forma enlazada. Con esto se ahorra tiempo sustancial al momento de plataformar la arquitectura en el simulador. Adicionalmente, la configuración de la interfaz de red de las máquinas virtuales de VirtualBox que se quieran compartir con GNS3 tienen que estar en modo "No conectado" para que éste las pueda gestionar y vincular a la simulación.

Para crear la arquitectura de red, sólo será cuestión de arrastrar los dispositivos desde la zona izquierda de la interfaz al área de trabajo, y para iniciar los equipos, hacer clic derecho sobre éstos, y seleccionar "Start". En la Figura 1 se puede observar la ejecución de varios clientes junto con un router, todos sistemas operativos reales, utilizando software en su versión completa.

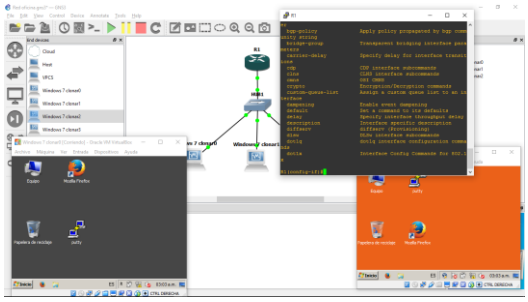

Figura 1. Routers y máquinas virtuales ejecutándose en GNS3

Si se necesita cambiar los diferentes adaptadores en un equipo, se puede hacer desde la configuración del mismo. La cantidad de "slots" variará según el tipo de IOS cargado en los routers y switches.

Si la simulación lo exige, es posible compartir la conexión de Internet a la simulación, de esa manera, los equipos podrán conectarse a direcciones globales para verificar conectividad, todo esto sin tocar ningún equipo físico en la infraestructura de la empresa.

La herramienta también instala Wireshark (analizador de tráfico de red), por lo que será posible hacer capturas como si de una red real se tratara.

Con la experiencia de la simulación, al momento de realizar el proceso real, no habrá dudas ni demoras en la configuración, puesto que, en teoría, se estaría repitiendo el proceso.

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.

4. IMPLEMENTACIÓN

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

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

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:

4.1 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).

[3] GNS3: http://www.gns3.com/

El beneficio 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.

No todo es bueno, actualmente hay demasiados servicios que utilizan la cuarta versión el protocolo, por lo que implementar una solución basada netamente en IPv6, podría generar conflicto e incompatibilidades, mientras se va llevando a cabo la transición en otras partes del mundo, algo insólito a día de hoy; como se mencionó, los tiempos muertos, caídas, y sitios inaccesibles son un elemento indeseable.

A día de hoy, no es una opción implementar el protocolo de forma única, eliminando del panorama IPv4, el cambio de tiene que dar de la forma menos traumática posible.

4.2 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

Analizando la carga de trabajo a nivel de tráfico de datos no se encuentra problema, ya que el tráfico que antes era IPv4, ahora será IPv6. La carga de trabajo será la misma, se mantiene el ancho de banda. Ahora, respecto al mantenimiento y control, se encuentra un problema; la complejidad al momento de mantener los dos protocolos de forma simultanea: dos espacios de almacenamiento, dos protocolos de routing (uno para IPv4, otro para IPv6), doble configuración de los dispositivos gestionables, doble configuración de seguridad (reglas de firewall) sin mencionar el tiempo dedicado a la gestión de todo el sistema, y capacitación del personal para que administren los dos protocolos.

Existe un problema con este mecanismo de transición. Si no se configura de forma correcta (en la parte del cliente), existe la posibilidad que los clientes al intentar acceder a un servidor remoto que esté configurado de la misma forma (doble pila), genere tiempos de respuesta muy altos, incluso no pueda llegar a conectar. Esto se da porque al tener prioridad la conexión mediante IPv6, es el método por defecto, y al carecer de la suficiente estabilidad (debido a una posible mala configuración), nunca conecta, generando error. La solución es implementar un algoritmo llamado Happy eyeballs [3], el cual consiste en generar una conexión simultánea al servidor por medio de IPv6 e IPv4, de tal forma que rápidamente verifica los tiempos de respuesta, si hay problemas con la conexión mediante IPv6, la realizará mediante IPv4, recordando este evento para futuros accesos. De esta forma el usuario no va a percibir ningún error, ni retrasos en la conexión.

4.3 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, 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.

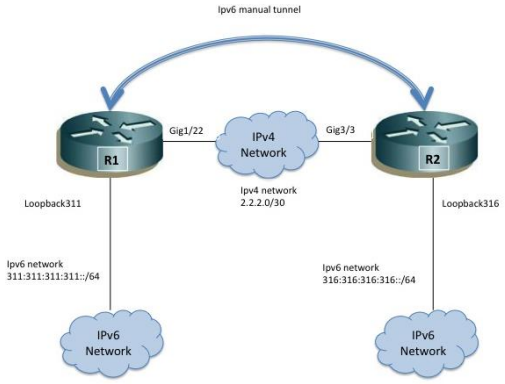

Figura 2. Túnel en una red IPv4 que conecta dos redes IPv6 [4]

Es posible tomar el tráfico que se genera en la red local (que es IPv6) y transmitirlo a un equipo remoto para que se puedan resolver las direcciones y acceder a los contenidos. Esto se realiza mediante un túnel que atraviesa la red IPv4, resultando un proceso transparente para los usuarios, puesto que no necesitan conocer que la red que lo conecta con el destino utiliza un protocolo incompatible.

El procedimiento se realiza encapsulando el tráfico IPv6 en paquetes IPv4, por lo que éstos viajaran 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.

Tenemos diferentes tipos de túneles:

- Túneles estáticos o automáticos. Donde la configuración del túnel (la configuración de cada extremo del túnel) se implementa de forma manual o automática, respectivamente. Esto afecta de forma

significativa el tiempo necesario para la creación de nuevo enlaces, donde la creación manual conlleva un tiempo considerable, tanto en el establecimiento como en el mantenimiento de la misma.
- Túneles punto a punto o multipunto. Donde el paquete al encapsularse para entrar en un extremo del túnel, sale por el otro extremo único de salida; o si es multipunto, un paquete entra por un extremo y puede salir por alguno de los múltiples extremos de salida.

También, con el mecanismo de transición de Túneles 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 [5] 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. Permiten encapsular paquetes IPv6 en paquetes IPv4 directamente, o utilizando una cabecera GRE. Corresponde a un túnel estático cuya configuración se realiza de forma manual. Su definición y características fueron propuestas en el RFC 4213. Si se utiliza tras una NAT, se hace necesario habilitar la función DMZ en el router.
- Tunnel bróker. Variación del túnel 6in4 descrito en el RFC 3053[6], donde existe un servidor que permite automatizar la creación de túneles 6in4. Los clientes se registran en el agente tunnel broker, donde este configurará el router del otro extremo, también proveerá instrucciones de configuración para que la red del cliente (o un equipo de la red) se pueda conectar mediante 6in4. Es posible encontrar un lista de tunnel broker actualizada en [7].
- Túneles 6to4**.** Túneles que permiten encapsular IPv6 en IPv4. A diferencia de los túneles 6in4, éstos se pueden crear de forma automática y la salida del otro extremo del túnel es multipunto. El prefijo utilizado para su direccionamiento ya está definido, corresponde a 2002::/16. Como requisito, necesita una dirección IPv4 pública en la parte de CPE del cliente. Esa dirección se utilizará para la creación del prefijo /48 de la red (concatenando el prefijo 2002::/16 con la dirección IPv4).
- Túneles 6RD. Evolución de 6to4, no requiere un prefijo reservado (como el 2002::/16 de 6to4), adicionalmente puede utilizar direcciones privadas, es una solución utilizada frecuentemente por ISP.
- Túneles DS-Lite. Diseñado para ayudar con el agotamiento de direcciones IPv4. Con este tipo de túnel es posible encapsular paquetes IPv4 en paquetes IPv6 para poder atravesar redes IPv6 y alcanzar servidores IPv4 o doble pila.
- ISATAP (Intra-Site Automatic Tunnel Addressing Protocol). Su objetivo consiste en transmitir información a través de una red IPv4 entre nodos doble pila. No se requiere que la red de transporte (IPv4) utilice multicast, ya que la configuración de los nodos (routers) se configura de forma manual en una lista. Es un protocolo creado por Microsoft para solventar el problema del agotamiento de direcciones y ayudar a la transición a IPv6. Compatible con sistemas operativos Windows XP en adelante. Sus especificaciones se pueden encontrar en el RFC 5214 [8].
- 6over4. Es otro sistema de tunelización donde se transmite información entre nodos doble pila a través de una red IPv4. No se suele utilizar porque requiere ciertas características que la gran mayoría de equipos en el lado del cliente o de la infraestructura de comunicación carece o no se configura adecuadamente. Sus especificaciones se pueden observar en le RFC 2529 [9].
- Túneles Teredo. Mecanismo de transición que permite comunicar dos redes IPv6 a través de una conexión IPv4. Funciona incluso estando detrás de una red NAT utilizando túneles donde se encapsulan los paquetes IPv6 en paquetes IPv4 UDP. Fue desarrollado por Christian Huitema (Microsoft) donde sus especificaciones se pueden encontrar en el RFC 4380 [10]. Los equipos de la red tienen que utilizar IPv6 nativo para poder funcionar. El cliente para sistemas GNU/Linux, BSD y MAC OS X se denomina Miredo.

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.

4.4 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 [11].

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. Ya no se utiliza, se volvió obsoleta en el año 2015 mediante el RFC 4966 [12]. 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. Permite el envío de paquetes de redes IPv6 a redes IPv4, con la condición en que estos paquetes sean unicast de tipo TCP, UDP e ICMP[13], [14]. Además, requiere direccionamiento público IPv4 y utiliza un prefijo y una dirección IPv4 válida para armar las direcciones. Se engaña a los nodos IPv6 (el que inicia la comunicación) haciéndole creer los que los nodos IPv4 son alcanzables mediante IPv6. Esto se logra enmascarando los paquetes IPv6 en paquetes IPv4 gracias a NAT64 para poder comunicar las dos redes.
- 464XLAT. Permite utilizar aplicaciones que no soportan IPv6. Se realiza doble traducción mediante NAT64. Para realizar esto, se proporciona una infraestructura básica IPv4 a los clientes que sólo tienen IPv6. Requiere una dirección IPv4 pública. Crea un entorno donde las aplicaciones que utilicen socket APIs no pierdan su funcionalidad y se puedan comunicar, así el resto de redes sea IPv6, la condición es que el otro extremo de la comunicación tiene que tener la pila del protocolo IPv4 o tener doble pila. El cliente CLAT puede ejecutarse incluso en dispositivos móviles, pero el dispositivo del otro extremo (el PLAT) debe contar con el hardware necesario para hacer la traducción.

5. PRUEBAS

Para analizar el estado de la implementación, se pueden realizar pruebas de conectividad, tiempos de respuesta y mediciones del ancho de banda máxima (disponible).

No se requieren herramientas especializadas, únicamente elementos presentes en la mayoría de equipos y el análisis correspondiente de los resultados, que permita detectar cualquier problema que se haya podido generar por una mala configuración (aunque si la simulación se realizó a conciencia, los problemas se habrían mitigado en gran medida).

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).

Para finalizar, es buena idea estar supervisando el estado de la red de forma constante, por lo menos las primeras semanas, para conocer de primera mano el estado de la transición y detectar posibles problemas a tiempo, antes de que sea un obstáculo en el trabajo diario de la empresa.

6. CONCLUSIONES

En todo proceso de transición se hace necesaria la inclusión de una metodología que guíe en dicho proceso, facilitando el trabajo y disminuyendo los posibles costos que de otra forma podrían poner en peligro el proyecto.

Al aplicar la metodología es posible detectar los posibles problemas que se puedan presentar en la infraestructura de red de la organización al momento de implementarse la transición, pudiendo analizar las causas y corregirlas antes de dicha etapa, reflejándose en un ahorro de tiempo y dinero.

Gracias a una metodología que guíe a las PyME, 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.

7. REFERENCIAS

[1] Cisco, “IPv6 Addressing Guide,” 2012. DOI= http://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/February2012/SBA_Ent_BN_IPv6AddressingGuide-February2012.pdf.

[2] SURFnet, “Preparing an IPv6 Addressing Plan,” 2011. DOI= http://www.rediris.es/conectividad/IPv6_addr_plan4.pdf.

[3] D. Wing and A. Yourtchenko, “RFC 6555: Happy Eyeballs: Success with Dual-Stack Hosts,” 2012.

[4] Cisco, “IPv6 manual tunnel Configuration Example,” 2011. DOI= http://docwiki.cisco.com/wiki/Ipv6_manual_tunnel_Configuration_Example.

[5] D. Farinacci, P. Traina, S. Hanks, and T. Li, “RFC 1702: Generic Routing Encapsulation over IPv4 networks,” 1994.

[6] I. Guardini, A. Durand, and D. Lento, “RFC 3053: IPv6 Tunnel Broker,” 2001.

[7] Wikipedia, “List of IPv6 tunnel brokers - Wikipedia, the free encyclopedia.” DOI= https://en.wikipedia.org/wiki/List_of_IPv6_tunnel_brokers.

[8] F. Templin, “RFC 5214: Intra-Site Automatic Tunnel Addressing Protocol (ISATAP),” 2008.

[9] B. Carpenter and C. Jung, “RFC 2529: Transmission of IPv6 over IPv4 domains without explicit tunnels,” pp. 1–10, 1999.

[10] C. Huitema, “RFC 4380: Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs),” 2006.

[11] J. Postel, “RFC 791: Internet Protocol,” 1981.

[12] D. . Aoun. C, “RFC 4966: Reasons to Move the Network Address Translator- Protocol Translator (NAT-PT) to Historic Status,” pp. 1–25, 2007.

[13] C. Bao, X. Li, and F. Baker, “RFC 6145: IP/ICMP Translation Algorithm,” 2011.

[14] M. Bagnulo, P. Matthews, and I. van Beijnum, “RFC 6146: Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers,” 2011.