UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGÍAS
MAESTRÍA EN CIENCIAS DE LA COMPUTACIÓN

DISEÑO DE LA INFRAESTRUCTURA TECNOLÓGICA DE RED PARA LA MIGRACIÓN DE IPV4 A IPV6 EN UN PROVEEDOR DE SERVICIOS DE INTERNET Y RED PRIVADA EN VENEZUELA. CASO TELCORP.

BARQUISIMETO, OCTUBRE 2011

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGÍA
MAESTRÍA EN CIENCIAS DE LA COMPUTACIÓN

DISEÑO DE LA INFRAESTRUCTURA TECNOLOGICA DE RED PARA LA MIGRACIÓN DE IPV4 A IPV6 EN UN PROVEEDOR DE SERVICIOS DE INTERNET Y RED PRIVADA EN VENEZUELA. CASO TELCORP.

Trabajo presentado como requisito parcial para optar al grado de
Magister Scientiarum en Ciencias de la Computación

Autor: Ing. Joselyne Infante

Tutor: Prof. Jesús Guédez

BARQUISIMETO, OCTUBRE 2011

DEDICATORIA

Dedico este éxito a los sueños, sí a los sueños, por ser la adrenalina más grande que pueda existir. Sin sueños, el día a día seria aburrido y no tendríamos por qué luchar. Dentro de los soñadores que más admiro en mi vida se encuentran Mis padres y mi esposo, a los cuales amo profundamente. Para ustedes, éste logro que es Un sueño más!!

AGRADECIMIENTO

En el transcurso de este nuevo sueño son muchas las cosas que tengo que agradecer:

A mi Dios bendito y adorado, GRACIAS, padre santo por todo lo que me das. No me canso de agradecerte por la vida, la salud, mi familia, mi alegría y mis amigos.

A mi esposo, que es mi nueva Familia. Te amo mi cielo y estoy infinitamente agradecida por TODO lo que has hecho por mí no solo en la culminación de esta meta, sino en todos los aspectos de mi vida. Te admiro mucho y le doy infinitas gracias a dios por darme la oportunidad de compartir con alguien como tú, mi cielo.

A mis padres y a mis hermanos, gracias por enseñarme el amor, el respeto, el sentido de la responsabilidad, las matemáticas, las letras, la amistad y todos los valores que hoy hacen un sueño más realidad, Los amo…

A mis compañeros de trabajo, hoy mis amigos, DIOS no puedo con ustedes, gracias por el apoyo José M (sin palabras, gracias amigo), Héctor, los pasantes, Cardone, Adriana, Reina y Alcadio.

A mi Jefe José Rondón, gracias por siempre creer en mí y en lo que hago, gracias por hacerme parte del maravilloso equipo Telcorp.

A mi tutor y amigo Jesús Guedez, éste es nuestro trabajo, Gracias por entender mis tiempos.

A mis amigos Emily, mi hermana desde ecuador no dejastes de ser parte de esto, gracias. Gisselot, amiga gracias por estar, por los cafecitos, por escucharme, sin palabras Hermana. Javier, gracias por la solidaridad. Yohana y Leidy, mis vecinas hermosas gracias. Libimar empezamos siendo compañeras de estudio y hoy somos amigas, GRACIAS por ayudarme tanto en este trabajo de investigación, fuiste mi bastón durante esta travesía.

Y a todas aquellas personas que se sientan parte de este éxito. Un besito para todos y ya.

“ cuando se tiene el amor de dios, un esposo, una familia y amigos como todos ustedes los sueños se convierten en Éxito y el éxito no es más que una felicidad compartida” Joselyne Infante

INDICE GENERAL

pp.

LISTA DE CUADROS

LISTA DE FIGURAS

UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGÍA
MAESTRÍA EN CIENCIAS DE LA COMPUTACIÓN

DISEÑO DE LA INFRAESTRUCTURA TECNOLÓGICA DE RED PARA LA MIGRACIÓN DE IPV4 A IPV6 EN UN PROVEEDOR DE SERVICIOS DE INTERNET Y RED PRIVADA EN VENEZUELA. CASO TELCORP.

Autor(a): Joselyne Infante
Tutor(a): Jesús Guédez

RESUMEN

La presente propuesta tiene como propósito Diseñar la Infraestructura Tecnológica de red para la migración de IPV4 a IPV6 en un proveedor de servicios de Internet (ISP) y red privada en Venezuela como lo es Telcorp, con el fin de solventar la limitante de la versión 4 del protocolo IPv4 en cuanto al agotamiento de direcciones IP públicas y permitir que el ISP siga operando en el rubro de las telecomunicaciones, ofreciendo los servicios para la cual fue concebida. Este proyecto se encuentra enmarcado dentro de la modalidad de proyecto especial y será desarrollado en cuatro fases: la primera fase de Diagnóstico de la situación actual de la infraestructura y operatividad en la empresa, la segunda fase de evaluación del mecanismo de transición a usar la tercera fase el diseño de la nueva Infraestructura a tecnológica que contemple la migración de IPV4 a IPV6. Y por ultimo el estudio de la viabilidad del proyecto desde el punto de vista técnico, económico y operativo. La investigación constituye desde el punto de vista académico y tecnológico un aporte documental en el área de redes, siendo base para otras investigaciones tanto en el sector empresarial como en el área académica, además promueve el desarrollo del país en inversiones privadas en la adquisición y uso de tecnologías de punta.

Palabras clave: Infraestructura tecnológica de red, ISP, IPV4, IPV6, migración.

INTRODUCCIÓN

En la actualidad se cuenta con grandes avances en el desarrollo tecnológico, uno de ellos es la Internet y su uso masivo, cada vez se incorporan a la red más dispositivos y usuarios. La globalización ha influido en esta masificación. Las empresas proveedoras de servicios de Internet usan las direcciones IP públicas para identificar a los equipos que salen a la red mundial. Estas direcciones usan el protocolo IP en la versión 4, IPv4.

Estas direcciones fueron concebidas para soportar 4.294.967.296 de direcciones en Internet. Sin embargo, éstas no fueron capaces de soportar el crecimiento de hoy día en Internet, es por ello que se han desarrollado varios mecanismos para el ahorro de direcciones IP públicas, estas contribuciones aún usadas no han sido suficientes y en tal sentido nace una versión del protocolo de última generación denominado IPv6.

Los proveedores de servicios de internet deben entonces migrar sus infraestructuras actuales para el soporte de IPV6 y de esta manera seguir prestando el servicio de Internet de forma idónea con direcciones públicas que identifiquen adecuadamente a los dispositivos que acceden a la red. Telcorp, formalmente Sistemas Telcorp CA, es un ISP de Venezuela desde el año 2002, dentro de su gama de servicios posee el proveer Internet al sector empresarial. Debido al agotamiento de direcciones IPV4 éste proveedor local se ha visto afectado en la prestación adecuada de este servicio. Es por ello que surge la necesidad de Diseñar una nueva Infraestructura tecnológica de red para este ISP que contemple los cambios que deban realizarse a nivel de las capas de la arquitectura TCP/IP en la infraestructura actual.

El propósito entonces del trabajo de Investigación es Diseñar la Infraestructura tecnológica de red para la migración de IPv4 a IPv6 en el ISP venezolano Telcorp, permitiendo de esta forma a la empresa seguir operando en el rubro de las telecomunicaciones usando IPV6 y sus bondades. La propuesta está estructurada de la siguiente manera:

El capítulo I contiene el Planteamiento del Problema, en donde se exponen los motivos que originaron el desarrollo de esta investigación, se formulan los Objetivos Generales y Específicos perseguidos e igualmente se presentan la Justificación e Importancia del estudio así como sus Alcances y Limitaciones.

El capítulo II contiene el Marco Teórico, donde se realiza la revisión detallada de parte documental relacionada con el tema objeto de estudio que sustenta teóricamente el proyecto, este capítulo está conformado por los Antecedentes de la Investigación, las Bases Teóricas, y la operacionalización de la variable de estudio.

El capítulo III muestra la metodología a seguir para la realización del trabajo, la Naturaleza de la Investigación, y las fases de la investigación en las que se encuentran la fase de diagnóstico, el estudio de la factibilidad y el diseño del proyecto.

El capítulo IV Contempla la propuesta de estudio como tal.

El capítulo V muestra las conclusiones y recomendaciones de la investigación.

Por último se presentan las referencias bibliográficas usadas y los anexos.

CAPÍTULO I

EL PROBLEMA

Planteamiento del problema

La tecnología hoy en día es considerada como un elemento importante en el proceso de globalización. Entre las tecnologías desarrolladas destaca Internet como medio masivo ya que es considerada como una verdadera revolución en la evolución de las comunicaciones del hombre. Visto de esa forma por, Bermúdez (2005):

> La revolución digital ha permitido que por un mismo canal podamos enviar texto, imagen y sonido a la velocidad de la luz. Pero la mayor revolución la ha supuesto Internet, sobre todo con su popularización en los últimos años, lo que ha terminado acabando con las últimas fronteras de la comunicación.

Ahora bien, el crecimiento de la internet en apenas siete décadas ha generado una cantidad de documentación y desarrollos tecnológicos, establecimiento de formalidades que mejoran las comunicaciones entre los ordenadores. Para que un usuario pueda acceder al contenido de la web es necesario el funcionamiento de varios protocolos o reglas definidas, entre ellas la pila de protocolo TCP/IP que es el modelo actual por el que se rige internet.

En este sentido, Atelin, y Dordoine. (2006) explican que la arquitectura TCP/IP usa las direcciones de red que permiten identificar a los dispositivos a través de Internet. El protocolo IP es el más comúnmente usado para la conexión a internet y las direcciones IP actualmente usan la versión cuatro (4) de este protocolo, de aquí en delante IPv4. Una dirección IPv4, consta de cuatro (4) octetos de bits y éstas son análogamente comparables con una dirección postal en el que el código postal identifica a la ciudad y se asemeja en este caso a la porción de red y la dirección

especifica del destinario del correo especifica la porción de host o los equipos finales dentro de un proceso de comunicación en una red de datos.

En efecto, LYM data comunications (2007) menciona que estas direcciones IPv4 fueron concebidas para conectar 4.294.967.296 dispositivos en la red pública. No obstante, esta versión del protocolo se quedó corta para el uso masivo de internet hoy en día, pues, cada vez existen más dispositivos como lo son: los teléfonos móviles, electrodomésticos, equipos industriales entre otros, que requieren estar conectados vía web.

Por ello, se crea la necesidad de usar algunas técnicas para ahorrar la utilización de las direcciones IPv4. Entre las alternativas para el ahorro de direcciones se establece la técnica de segmentar las direcciones en: IP públicas, las que salieran del enrutador (Router) local a la Internet, y las IP privadas, las direcciones que pueden usar los dispositivos de una red local. Según lo cita España (2003). Por su parte, Mañas (2004) menciona que, uno de los mecanismos, usados para ahorrar el espacio de direcciones IPv4 fue la división de Sub Redes o Enrutamiento entre dominios sin Clases (CIDR**),** que significó tomar prestados bits de la porción de host para usarlos como parte de red para así, usar solo las redes y los host que realmente se necesitaban. Sin embargo, CIDR no permitía escalabilidad en las redes y le quedaba la responsabilidad al administrador de la red de contemplar un crecimiento en el esquema de direccionamiento en su organización, sí estos cálculos eran superados, el esquema debía ser nuevamente replanteado. Así, estos mecanismos empleados aun hoy en día han alargado la vida del protocolo IPv4, pero el crecimiento inminente del internet y el uso de cada vez más dispositivos que requieren una dirección IP, terminó por que los organismos idearan y combinaran mecanismos y de esta manera surge traducción de direcciones IP privadas a públicas o NAT.

Precisamente, NAT permite que múltiples redes locales salgan a Internet con una sola dirección pública. Aunque NAT constituye muchas ventajas para el ahorro de las direcciones presenta otros inconvenientes, sobre todo cuando se requiere

acceder a un dispositivo específico dentro de la red, tal como lo establecen Baydal y otros (2005).

En consecuencia, al imparable crecimiento de Internet, la versión 4 del protocolo de Internet IPv4 tenía en sus inicios un límite de vida calculada para el año 2025, pero según el especialista G. Huston, la utilización total del direccionamiento de IPv4 no llegaría hasta el año 2011. Y efectivamente Huston tenía razón. El 3 de febrero del 2011 la Organización responsable de la asignación y administración de las Direcciones IP y recursos relacionados para la región de América Latina y el Caribe (LACNIC), comunica que el stock central de direcciones IPv4 ha quedado finalmente agotado.

Por esta razón, el grupo Especial sobre Ingeniería de Internet (Internet Engineering Task Force, IETF,), organización encargada de la evolución de la arquitectura en la Red, desde ya algunos años, desarrolló varias propuestas para la implementación de una IP de próxima generación. Como resultado, nace el protocolo de Internet versión 6 (IPv6). Este nuevo modelo se erigirá como sucesor de la versión 4 puesto que resuelve sus deficiencias y aporta nuevas funciones acordes a la evolución actual de la red.

En ese mismo sentido, Kaplan (2010) indica que: "Una dirección IPV6 posee 128 bits disponibles y soportará 340.282.366.920.938.463.463.374.607.431.768.211. 456 (2128 o 340 sextillones de direcciones) —cerca de 6,7 × 1017 (670 mil billones) de direcciones por cada milímetro cuadrado de la superficie de la tierra". Por lo que estima que cada dispositivo pueda tener su propia dirección IP.

Ahora bien, lo mencionado en párrafos anteriores en cuanto al agotamiento de direcciones IPv4 representa uno de los problemas que afectan a los Proveedores de servicios de Internet, de aquí en adelante ISP, debido a que disponen de menos direcciones IP públicas para ofrecer sus servicios. En tal sentido Telcorp, objeto de estudio de esta investigación, por ser ISP no escapa de esta situación. Esta empresa venezolana formalmente Sistemas Telcorp, C.A, RIF6. J-30917169- 0, de capital privado está autorizada por Conatel (órgano rector de las telecomunicaciones en

este país) según habilitación número: HGST 0289 para proveer servicios de Internet, transporte de datos y soluciones de tecnología de la información y comunicación para el mercado corporativo.

Igualmente, cuenta con cobertura en Caracas, Valencia, Maracay, Barquisimeto, Acarigua, Guarenas, Guatire, Valles del Tuy, Puerto la Cruz, Maturín, El Tigre y Puerto Ordaz. Posee una infraestructura propia de telecomunicaciones con equipos de última generación y enlaces de microondas que soportan velocidades de datos entre 10 y 100 Mbps, basado en protocolo nativo IP. Provee todo tipo de soluciones integrales de conectividad en Banda Ancha para Internet, Accesos Dedicados, Redes IP, Seguridad de Datos y Servicios Profesionales en Telecomunicaciones. (Más detalles de Telcorp, se muestran en el anexo N°1.)

Uno de los problemas específicos que enfrenta esta empresa relacionado con el uso de IPv4 tiene que ver con el servicio de Internet Dedicado, este servicio es simétrico y contempla velocidades desde 256 Kbps hasta 10 Mbps, comprendía inicialmente un conjunto de cuatro (4) direcciones IP Públicas, ideales para que los clientes alojaran sitios web, accedieran remotamente a servidores o equipos dentro de su red local. El año pasado la empresa solicito un conjunto de direcciones adicionales para seguir ofreciendo de manera idónea este servicio, no obstante el otorgamiento de estas direcciones no fue el esperado por la compañía, razón por la cual el servicio se ofrece ahora con una (1) sola dirección IP pública.

Del mismo modo, Telcorp posee una reserva pequeña de IP públicas para este año, lo que implica que el servicio de Internet dedicado, sea en estos momentos un servicio no escalable dentro de las ventas de la empresa. Esta pequeña reserva según las estimaciones de la gerencia comercial pueden ser soportadas hasta finales de año, bajando los índices de ventas por Internet dedicado. Para ello, el departamento de ventas debe esforzarse en comercializar otro servicio que posee un costo menor que es el Internet comercial, asimétrico, compartido y sin IP públicas, como consecuencia de esto la empresa puede tener repercusiones desde el punto de vista financiero. Tomado de Telcorp, (2009).

Hechas las consideraciones anteriores, como Proveedor de servicio de Internet y así seguir prestando la gama de servicios para los cuales fue concebida, es entonces cuando surge la necesidad de migrar su infraestructura actual para el soporte de IPV6 en su red de datos y de esta forma seguir sus operaciones en el rubro de las telecomunicaciones.

De igual manera, para migrar se requiere elaborar un plan que contemple el diseño de la nueva infraestructura de red, permitiéndole a Telcorp usar IPV6 y sus bondades en los servicios de Internet. Es por ello que la propuesta, pretende documentar todos los cambios que se originarán en el ISP sistemas Telcorp para la migración.

El propósito entonces, es evaluar la infraestructura de red actual para tener una visión general de los cambios que se deban realizar en ésta. Proporcionar un plan de migración basado en los estándares y las documentaciones para la adopción parcial y definitiva de este nuevo protocolo en la empresa objeto de estudio y los usuarios finales.

Así, se espera evaluar principalmente las capas 1, 2 de la arquitectura TCP/IP, ya que principalmente los proveedores de servicios de Internet operan en estas capas para proporcionar el acceso a la red pública, sin dejar de lado los cambios a nivel de capa superiores.

Finalmente, con base en la situación antes expuesta surgen las siguientes interrogantes: ¿Cuál es la situación actual del ISP Telcorp en su infraestructura de red para adoptar a IPV6? ¿Cuáles aspectos se deben considerar para determinar si es viable técnica, operativa y económicamente la migración de la Infraestructura de red de IPv4 a IPV6? ¿Cuáles son las alternativas de migración o metodologías existentes? ¿Cuáles cambios se deben hacer en la Infraestructura tecnológica de red este ISP para adoptar a IPV6 en su red de servicios?

Para concluir y dar respuesta a las interrogantes planteadas se propone el Diseño de la Infraestructura tecnológica de red para la migración de IPV4 a IPv6 en

el ISP Telcorp, que le permitan operar en el ámbito de las telecomunicaciones, tomando en cuenta el crecimiento del Internet como medio Global.

Objetivos de la Investigación

Objetivo General

Diseñar la Infraestructura tecnológica de red para la migración de IPV4 a IPv6 en el ISP venezolano Telcorp.

Objetivos Específicos

- Diagnosticar la situación actual de la empresa objeto de estudio en cuanto a su Infraestructura tecnológica de red actual y su operatividad.
- Evaluar las alternativas de migración o metodologías existentes.
- Elaborar un diseño de la nueva Infraestructura tecnológica de red que le permita al ISP venezolano Telcorp la migración de IPv4 a IPv6.
- Determinar la factibilidad técnica, operativa y económica del diseño de la nueva Infraestructura tecnológica que permita la migración de IPv4 a IPV6 en el ISP venezolano Telcorp.

Justificación e Importancia

Con el proyecto planteado se espera que la compañía pueda garantizar el uso del Internet de forma confiable a sus distintos clientes corporativos y que además pueda cumplir con las exigencias actuales de sus usuarios en cuanto a demandas de direcciones IP públicas y comunicaciones aptas para redes de nueva generación.

Así, el Diseño de la nueva Infraestructura tecnológica de red del Proveedor de servicios de Internet Telcorp para la migración del protocolo IPV4 a IPV6 permitirá a la empresa objeto de estudio continuar operando dentro del rubro de las

telecomunicaciones y garantizará sus procesos de negocio, aportando de esta forma un mayor nivel de competitividad.

Por su parte, considerando que Telcorp es una empresa local y que este trabajo trae beneficios en los servicios que esta ofrece a sus clientes. Igualmente, esta investigación significará mejoras en el sector empresarial promoviendo el uso de nuevas tecnologías en la industria nacional, ayudando indirectamente al desarrollo del país en inversiones privadas en la adquisición y uso de tecnologías de punta de la mano con las nuevas proyecciones globales.

Es importante resaltar que desde el punto de vista tecnológico, este proyecto, constituye un aporte documental en el área de las redes, siendo base para otras investigaciones tanto en el sector empresarial como en el área académica.

Alcance y Limitaciones

Esta investigación busca proporcionar al Proveedor de Servicio de Internet Telcorp, un plan de migración progresiva que le permita incorporar la nueva versión del protocolo de Internet IPV6 en su infraestructura tecnológica de red.

Cabe destacar, como ISP Telcorp debe abordar la implementación o interacción en los usuarios finales o clientes, por lo que se pretende además que la investigación arroje conclusiones en cuanto a las instalaciones en clientes y si existe o no la necesidad de cambios en los equipos terminales actuales. Se espera entonces, abordar un diseño basado en la arquitectura TCP/IP, destacándose en este proyecto los cambios primordiales en las capas: uno (1) dos (2) de TCP/IP, porque es donde principalmente opera la infraestructura de red del ISP objeto de estudio, sin dejar de lado los cambios a nivel de capa superiores. También, la investigación resolverá el problema de la empresa Telcorp en cuanto a la continuidad de la prestación del servicio de Internet dedicado.

Como limitante de este proyecto, es que abarca solo un ISP en este caso Telcorp, objeto de estudio de esta investigación.

CAPÍTULO II

MARCO TEÓRICO

Antecedentes de la Investigación

A continuación se hará referencia a trabajos de investigación realizados con anterioridad, que apoyan como antecedentes, al diseño de la infraestructura tecnológica de red para la migración de IPV4 a IPV6 en el ISP Telcorp**.**

Se tomó como referencia para esta investigación el trabajo presentado por Belmonte y otros (2007), titulado "*Transición a IPv6 de la Red de Datos del Campus de Moncloa"*. Con este proyecto se realizaron pruebas con el mecanismo de transición Dual Stack y también con configuraciones de aplicaciones para que soporten IPv6, entre otros. Los autores observaron que la tecnología IPv6 está madura y preparada para ser implantada en cualquier organización. En éste se examina la compatibilidad y coexistencia de las tecnologías IPV4 e IPV6 en el seno de la red de datos de la Universidad Computense de Madrid, presentado al efecto una simulación del escenario en el que se recrean los principales elementos de la infraestructura de la Red (routers, dispositivos de switching, principales servicios de aplicación, entre otros) así como un plan de direccionamiento a seguir ajustado a las características propias de la misma en coordinación con el ente RedIRIS, que es el actual proveedor de conectividad de la Universidad. Se considera antecedente para el desarrollo del diseño de la infraestructura tecnológica de red para la migración de IPV4 a IPV6 en Telcorp, debido a que los investigadores evalúan los cambios a realizarse en el campus a nivel de DNS, Routing, Configuración de Hosts Seguridad y Gestión de red, proporcionando una guía a través de ejemplos para configurar IPv6 sobre distintos sistemas operativos.

De igual forma, se tomó como aporte de esta investigación el trabajo de grado presentado por Bermejo y otros (2008) Titulado *Implementación de appliances para*

enrutado de IPv6 desde plataformas hardware económicas. La propuesta permitió valorar la introducción de conectividad IPv6 en la RR.DD de la Universidad Complutense utilizando técnicas de tunneling, sin acometer grandes cambios en la infraestructura actual, abriendo de ésta forma posibilidades para experimentar con IPv6 en los campos de: movilidad, seguridad a nivel de red, integración con otros dispositivos alternativos al computador, como teléfonos móviles, y aprovechamiento de la optimización de multicast, en escenarios como la videoconferencia, entre otros. Este trabajo es significativo para ésta investigación debido a que usa tecnologías económicas basadas en plataformas bajo estándares libres y permiten evaluar otra óptica en el momento de elegir la tecnología para migrar en el ISP Telcorp, tomando en cuenta el aspecto económico que es uno de los paradigmas difíciles de romper en las organizaciones para la transición a IPV6. Finalmente, éste trabajo muestra otra perspectiva para soluciones económicas de interoperatividad de IPV4 e IPV6.

De igual manera, el trabajo de grado titulado, *Propuesta para la implementación y la coexistencia de IPv4 e IPv6 en la red de datos de la Universidad Central de Venezuela,* presentado por Gamess, E (2008 se considera como antecedente para la propuesta ya que el autor explicó la importancia del uso de IPV6 para esa casa de estudio, considerando que poseen aproximadamente 60.000 estudiantes y 16.000 miembros del personal. El trabajo de investigación enmarcado dentro de la modalidad de proyecto factible, explica el crecimiento de la red universitaria, actualmente, cerca de 8.000 ordenadores conectado a ésta y como consecuencia de esta expansión, los usuarios sufrían bajo rendimiento y los administradores de red se enfrentaban a la escasez de direcciones IPv4 públicas. Para hacer frente a la este último problema, NAT (Network Address Translation) fue implementado desde hace varios años en la universidad. Sin embargo, tal y como lo indicó el autor NAT es una solución parcial ya que no ofrece verdaderas de conexiones de extremo a extremo y, en algunos servicios de Internet que necesitan para iniciar conexiones desde el exterior no funciona. En este trabajo, se presentó una solución a los problemas de congestión de tránsito el cual se alivió con una

actualización de la conexión entre la universidad y los principales ISP, y un más riguroso filtrado políticas. Para reducir el problema generado por la falta de direcciones IPv4, se implementó la nueva versión del Protocolo de Internet (IPv6) en la universidad. El autor usó las ventajas de túneles 6 to 4 para la migración. Esto permitió poseer un gran espacio de direcciones y muchas otras mejoras sobre IPv4 a la universidad dentro de su direccionamiento Local. El trabajo presentado está ligado a esta investigación por poseer alternativas de migración al nuevo protocolo IP en su versión 6 partiendo de una red IPV4.

Por su parte Hortega, H (2010) en su trabajo de grado titulado "*Análisis e implementación de un sistema video Streaming en redes dual stack IPv4/IPv6"*explicó las ventajas y desventajas de las arquitecturas IPv4 e IPv6 para el servicio de video en tiempo real. Para ello se realizaron las implementaciones en un servidor de video, operando en redes IPv4, IPv6 y Dual Stack (IPv4/IPv6), las pruebas permitieron observar las bondades de IPV4 e IPV6 respectivamente. Este trabajo es considerado como antecedente a ésta investigación debido a que el autor implementa uno de los mecanismos de transición como él es el dual stack realizando de esta manera recomendaciones basadas en las pruebas de su investigación. Entre ellas, destaca las consideraciones que hay que tomar en cuenta en una red IPV6 nativa diferenciándola con IPV4 y en entornos donde operan los dos protocolos. El trabajo hace énfasis en los problemas actuales de los retardos y uso de los recursos de los enrutadores que generan las redes IPV6 nativas.

También, el trabajo realizado por Rodríguez, M (2010) titulado "*Análisis y diseño de una reingeniería organizativa de la red del campus de la Universidad técnica de Manabí mediante la utilización de IPV6. Y su implementación en la facultad de ciencias informáticas en el laboratorio de redes*" es considerado una contribución para ésta investigación ya que la tesis presentó el diseño y análisis de una red IPv6 en la Universidad Técnica de Manabí y su implementación en el Laboratorio de Redes de la Facultad de Ciencias Informáticas conectada directamente a Internet. Se entregaron los criterios utilizados para la actualización de los equipos

de la red junto al plan de integración de IPv6. Se realizó una revisión del soporte IPv6 en sistemas operativos y servicios de red junto a un análisis sobre posibles ataques que afectan la seguridad de la red implementada. El desempeño de los equipos necesarios para la implementación de la red IPv6 en la Universidad Técnica de Manabí ha sido analizado en ambientes "dual-stack". Los resultados obtenidos concluyen un desempeño prácticamente idéntico al utilizar IPv4 y/o IPv6. Las mayores diferencias se observan en tráfico compuestos por paquetes pequeños (inferiores a 100 [byte]). Esta investigación está enmarcada en la modalidad de investigación diagnostica considerada como investigación científica y de campo. El autor uso la técnica de observación directa y la entrevista no estructurada para la recolección de datos.

El trabajo presentado por Rodríguez representa un antecedente a la propuesta ya que explica los criterios utilizados para la actualización de los equipos de la red junto al plan de integración de IPv6, sirviendo como base para el plan migración de IPV4 a IPV6 en Telcorp.

El reciente trabajo enmarcado dentro de la modalidad de proyecto factible; titulado "*Implementación del protocolo IPV6 en la infraestructura de red de dato de la UCLA",* realizado por González, J (2011), ha sido de gran ayuda para abordar la propuesta de esta investigación, debido a la similitud de la metodología utilizada y el esquema de planificación de las actividades con la finalidad de separar y ordenar las actividades ejecutadas por el autor. Dentro de las consideraciones plantadas por González destacan la importancia de la escogencia asertiva de equipos de red y telecomunicaciones en las etapas iniciales de una red de datos, basada el crecimiento futuro. También, la importancia del papel que juega el ISP principal como engranaje necesario entre la red Internet y la IT que se requiera migrar a IPv6. En la UCLA se logró implementar IPv6 lo que crea una perspectiva positiva en cuanto a la complejidad de la transición.

Bases Teóricas

En la actualidad el uso de Internet como la red de redes ha representado una herramienta en la vida diaria del hombre. La globalización va apoyada directamente de Internet. Tal y como se planteó en el capítulo I es necesario implementar, principalmente en los proveedores de servicios de Internet, otro protocolo para cubrir las necesidades actuales de los dispositivos y de los usuarios. Para poder comprender los cambios a nivel de Infraestructura tecnológica que deben hacerse para la migración a este nuevo protocolo de red es necesario explicar algunos conceptos primordiales como lo son: la definición de Infraestructura tecnológica, Protocolos de comunicación, el modelo de referencia OSI, la arquitectura TCP/IP, el detalle de las capas uno (1) dos (2) y tres (3) y cuatro (4), así como los conceptos y características del protocolo IP en su versión 4 y su versión 6, los mecanismos de transición de IPV4 a IPV6 y otros serán descritos a continuación:

Infraestructura Tecnológica

Zuluaga (2009), señala que se entiende por infraestructura tecnológica al conjunto de todos los elementos tecnológicos hardware y software: servidores, computadores, portátiles, impresoras, switches, routers, firewall, escaners, cableado estructurado, cpu`s, software informático, equipos de comunicación, internet, red lan.

La universidad autónoma de Cali (2010) describe que dentro de los componentes de infraestructuras tecnológicas se encuentran:

Infraestructura de Red o infraestructura de telecomunicaciones, Las máquinas virtuales o software, Los servidores de nombres, Las bases de datos, entre otros. Para efectos de esta investigación se detallara el contenido que respecta a hardware de red. El Observatorio de la Sociedad de la Información en Navarra (sf) detalla información respecto a las infraestructuras de telecomunicaciones o hardware de red.

"Todos los soportes físicos y lógicos (obra civil, equipos, programación) que permiten el transporte de servicios entre dos o más puntos de una red de telecomunicaciones". A través de las infraestructuras los usuarios acceden a los contenidos y servicios de telecomunicaciones.

En la publicación de Telefónica "La Sociedad de la Información en España: Perspectiva 2001-2005", citada por el Observatorio de la Sociedad de la Información en Navarra (ob.cit) se explica que las infraestructuras están formadas por tres componentes: terminales, redes, y servidores. Este es un concepto más amplio del que hasta ahora se venía aplicando a las infraestructuras y que en nuestra opinión es acertado aplicar, dado los importantes cambios que está experimentando la Sociedad de la Información con la aparición del Internet y la integración de las tecnologías de informática y de telecomunicaciones.

En la Parte II del Libro Verde de la Comisión Europea citado de igual forma por El Observatorio de la Sociedad de la Información en Navarra (ob. cit), se desglosan los componentes de las infraestructuras en los niveles que muestra la tabla número 1.

Cuadro 1.
Niveles de Infraestructura.

NIVELES	COMPONENTES	EJEMPLOS
1	Derechos de paso Obra civil	Terrenos, caminos, casetas, Conductos, galerías, torres de Antenas, baterías, alimentaciones eléctricas
2	Soportes para la Transmisión de Información	Cables: cobre, coaxial y fibra Óptica. Bandas de frecuencias. Líneas alquiladas
3	Equipos y terminales	Terminales de radio. Equipos de coaxial y F.O. Routers, Multiplexores Conmutadores

Fuente: Rodríguez, R. (2006)

Es importante señalar que para realizar cambios en infraestructuras es conveniente realizar planes para los Planes de Infraestructura Tecnológica a corto y largo plazo se refiere entre otras cuestiones a las estrategias empresariales respecto a:

La arquitectura de sistemas: Que se refiere al tipo de Sistemas que utilizará la empresa, la manera en que se interrelacionarán los sistemas, el grado de automatización al cual pretende llegar la empresa, el alcance de cada uno de los sistemas, y aspectos similares.

La dirección Tecnológica: Consiste en la elección de alguna línea de hardware y software de base. En general lo habitual es que se decida la ejecución de cierto tipo de aplicaciones utilizando una línea de hardware y software, u otra en otro tipo de aplicaciones. Los tipos de aplicaciones pueden ser por ejemplo: Sistemas Corporativos, Sistemas de Análisis de Datos, Sistemas de Toma de Decisiones, Ofimática, Edición Electrónica, Inteligencia Artificial, etc.

Las estrategias de migración: La constante evolución tecnológica exige cada vez más frecuentes procesos de migración desde las plataformas anteriores a las nuevas. Las estrategias de migración se refieren a la determinación de que sistemas serán migrados, hacia qué tipos de plataforma, en qué momento, y de qué manera.

Por último, en esta investigación en la que se diseñara la nueva infraestructura tecnológica de red que permita el Protocolo IPV6 y sus bondades para el ISP Telcorp aborda cambios en distintos protocolos de redes usados con IPV4. Es por ello que a continuación se detalla el concepto de protocolos.

Protocolos de Redes

Cisco Systems, (Ob.cit), explica que para que los dispositivos se puedan comunicar en forma exitosa, un nuevo conjunto de aplicaciones de protocolos debe describir los requerimientos e interacciones precisos. Las suites de protocolos de redes describen procesos como los siguientes:

1. El formato o la estructura del mensaje.

2. El método por el cual los dispositivos de networking comparten información sobre las rutas con otras redes.
3. Cómo y cuándo se transmiten mensajes de error y del sistema entre los dispositivos.
4. La configuración y la terminación de sesiones de transferencia de datos.

Con frecuencia, muchos de los protocolos que comprenden una suite hacen referencia a otros protocolos ampliamente utilizados o a estándares de la industria. Un estándar es un proceso o protocolo que ha sido avalado por la industria de redes y ratificado por una organización de estándares, como el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, Institute of Electrical and Electronics Engineers) o el Grupo de trabajo de ingeniería de Internet (IETF).

Beneficio de modelo de capas

Para visualizar la interacción entre varios protocolos, es común utilizar un modelo en capas. Este modelo describe el funcionamiento de los protocolos que se produce en cada capa y la interacción con las capas que se encuentran por encima y por debajo de ellas.

Hay beneficios por el uso de un modelo en capas para describir protocolos de red y operaciones. Uso de un modelo en capas:

1. Ayuda en el diseño de protocolos, ya que los protocolos que operan en una capa específica tienen información definida según la cual actúan, y una interfaz definida para las capas superiores e inferiores.
2. Fomenta la competencia, ya que los productos de distintos proveedores pueden trabajar en conjunto.
3. Evita que los cambios en la tecnología o en las capacidades de una capa afecten otras capas superiores e inferiores.
4. Proporciona un lenguaje común para describir las funciones y capacidades de networking.

Cisco Networking Academy (ob.cit.) explica que existen dos tipos básicos de modelos de networking: modelos de protocolo y modelos de referencia.

Un modelo de protocolo: proporciona un modelo que coincide fielmente con la estructura de una suite de protocolo en particular. El conjunto jerárquico de protocolos relacionados en una suite representa típicamente toda la funcionalidad requerida para interconectar la red humana con la red de datos. El modelo TCP/IP es un protocolo modelo porque describe las funciones que ocurren en cada capa de protocolos dentro de una suite de TCP/IP.

Un modelo de referencia: proporciona una referencia común para mantener la consistencia dentro de todos los tipos de protocolos y servicios de red. Un modelo de referencia no está pensado para ser una especificación de implementación ni para proporcionar un nivel de detalle suficiente para definir de forma precisa los servicios de la arquitectura de red. El objetivo principal de un modelo de referencia es ayudar a lograr un mayor conocimiento de las funciones y procesos involucrados.

Modelo TCP-IP

Para Cisco Systems, (Ob.cit), el modelo de protocolo en capas para comunicaciones de internetwork se creó a principios de la década de los setenta y se conoce con el nombre de modelo de Internet. Define cuatro categorías de funciones que deben existir para que las comunicaciones sean exitosas. La arquitectura de la suite de protocolos TCP/IP sigue la estructura de este modelo. Por esto, es común que al modelo de Internet se le conozca como modelo TCP/IP.

La mayoría de los modelos de protocolos describen un stack de protocolos específicos del proveedor. Sin embargo, puesto que el modelo TCP/IP es un estándar abierto, una compañía no controla la definición del modelo. Las definiciones del estándar y los protocolos TCP/IP se explican en un foro público y se definen en un conjunto de documentos disponibles al público. Estos documentos se denominan Solicitudes de comentarios (RFC). Contienen las especificaciones formales de los

protocolos de comunicación de datos y los recursos que describen el uso de los protocolos.

Las RFC (Solicitudes de comentarios) también contienen documentos técnicos y organizacionales sobre Internet, incluyendo las especificaciones técnicas y los documentos de las políticas producidos por el Grupo de trabajo de ingeniería de Internet (IETF). Ver figura N° 1

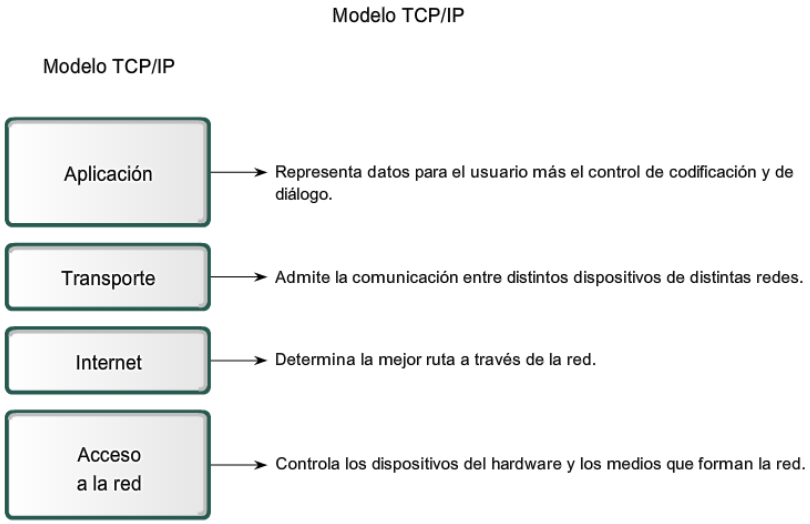


Figura N°1: Modelo TCP –IP

Fuente: Cisco Systems, (2008)

Capa de acceso a red

> El nivel de enlace de datos transforma el nivel físico, un simple medio de transmisión, en un enlace fiable y es responsable de la entrega nodo a nodo. Hace que el nivel físico aparezca ante el nivel superior (nivel de red) como un medio libre de errores.Forouzan (2002)

Entre las responsabilidades específicas del nivel de enlace de datos se incluyen las siguientes, planteadas de esta manera por el mismo autor:

Tramado. El nivel de enlace de datos fragmenta el flujo de bits recibidos del nivel de red en unidades de datos manejables denominadas tramas.

Direccionamiento físico. Si es necesario distribuir las tramas por distintos sistemas de la red, el nivel de enlace de dalos añade una cabecera a la trama para definir la dirección física del emisor (dirección fuente) y/o receptor (dirección destino) de la trama. Si hay que enviar la trama a un sistema fuera de la red del emisor, la dirección del receptor es la dirección del dispositivo que conecta su red a la siguiente.

Control de flujo. Si la velocidad a la que el receptor recibe los datos es menor que la velocidad de transmisión del emisor, el nivel de enlace de datos impone un mecanismo de control de flujo para prevenir el desbordamiento del receptor.

Control de errores. El nivel de enlace de datos añade Habilidad al nivel físico al incluir mecanismos para detectar y retransmitir las tramas defectuosas o perdidas. También usa un mecanismo para prevenir la duplicación de tramas. El control de errores se consigue normalmente a través de una cola que se añade al final de la trama.

Control de acceso. Cuando se conectan dos o más dispositivos al mismo enlace, los protocolos de nivel de enlace deben determinar en todo momento qué dispositivo tiene el control del enlace.

Por su parte, la arquitectura TCP /IP combina todo lo mencionado anteriormente relacionado con el acceso a la red con lo que en el modelo de referencia OSI se denomina capa física

- Características físicas de las interfaces y el medio. Contempla las características de la interfaz entre los dispositivos y el medio de transmisión. Además especifica el tipo de medio de transmisión.

- Representación de los bits. Los datos del nivel físico están formados por bits (cadenas de ceros y unos) sin interpretación. Para que logren transmitirse, deben codificarse en señales, eléctricas u ópticas. La capa física precisa el tipo de codificación (como los ceros y unos se convierten en señales).

- Tasa de datos. La capa 1, también específica la tasa de transmisión: el número de bits enviados cada segundo. Es decir, define la duración de un bit.

- Sincronización de los bits. El emisor y el receptor deben estar sincronizados a nivel de bit. En otras palabras, la sincronización de los relojes del emisor y receptor también respecta a esta capa.

- Configuración de la línea. El nivel físico está relacionado con la conexión de dispositivos al medio.

- Topología física. La topología física precisa cómo están conectados los dispositivos para formar una red. Los dispositivos deben estar conectados usando una topología en malla (cada dispositivo conectado a otro dispositivo), una topología en estrella (dispositivos conectados a través de un dispositivo central), una topología en anillo (un dispositivo conectado al siguiente, formando un anillo) o una topología ele bus (cada dispositivo está conectado a un enlace común).

- Modo de transmisión. El nivel físico también define la dirección de la transmisión entre dos dispositivos: simple, duplex o full-dúplex. En el modo simple es una comunicación en un solo sentido En el modo semidúplex, también llamada half dúplex dos dispositivos pueden enviar o recibir, pero no al mismo tiempo. En el modo full-dúplex (o simplemente dúplex), dos dispositivos pueden enviar o recibir al mismo tiempo.

La capa de red, o Capa 3 de OSI

Para Cisco Systems, (Ob.cit), la capa de red provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados. Para realizar este transporte de extremo a extremo la Capa 3 utiliza cuatro procesos básicos:

Direccionamiento: Primero, la capa de red debe proporcionar un mecanismo para direccionar estos dispositivos finales. Si las secciones individuales de datos deben dirigirse a un dispositivo final, este dispositivo debe tener una dirección única. En una red IPv4, cuando se agrega esta dirección a un dispositivo, al dispositivo se lo denomina host.

Encapsulación: Segundo, la capa de red debe proporcionar encapsulación. Los dispositivos no deben ser identificados sólo con una dirección; las secciones individuales, las PDU de la capa de red, deben, además, contener estas direcciones. Durante el proceso de encapsulación, la Capa 3 recibe la PDU de la Capa 4 y agrega un encabezado o etiqueta de Capa 3 para crear la PDU de la Capa 3. Cuando nos referimos a la capa de red, denominamos paquete a esta PDU. Cuando se crea un paquete, el encabezado debe contener, entre otra información, la dirección del host hacia el cual se lo está enviando. A esta dirección se la conoce como dirección de destino. El encabezado de la Capa 3 también contiene la dirección del host de origen. A esta dirección se la denomina dirección de origen.

Después de que la capa de red completa el proceso de encapsulación, el paquete se envía a la capa de enlace de datos a fin de prepararse para el transporte a través de los medios.

Enrutamiento: Luego, la capa de red debe proporcionar los servicios para dirigir estos paquetes a su host de destino. Los host de origen y destino no siempre están conectados a la misma red. En realidad, el paquete podría recorrer muchas redes diferentes. A lo largo de la ruta, cada paquete debe ser guiado a través de la red para que llegue a su destino final. Los dispositivos intermediarios que conectan las redes son los routers. La función del router es seleccionar las rutas y dirigir paquetes hacia su destino. Este proceso se conoce como enrutamiento. Durante el enrutamiento a través de una internetwork, el paquete puede recorrer muchos dispositivos intermediarios. A cada ruta que toma un paquete para llegar al próximo dispositivo se la llama salto. A medida que se reenvía el paquete, su contenido (la unidad de datos del protocolo [PDU] de la capa de transporte) permanece intacto hasta que llega al host de destino.

Desencapsulación: Finalmente, el paquete llega al host de destino y es procesado en la Capa 3. El host examina la dirección de destino para verificar que el paquete fue direccionado a este dispositivo. Si la dirección es correcta, el paquete es

desencapsulado por la capa de red y la PDU de la Capa 4 contenida en el paquete pasa hasta el servicio adecuado en la capa de Transporte.

Protocolos capa de red

Los protocolos implementados en la capa de red que llevan datos del usuario son:

- Protocolo de Internet versión 4 IPv4
- Protocolo de Internet versión 6 (IPv6)
- Intercambio Novell de paquetes de internetwork (IPX)
- AppleTalk
- Servicio de red sin conexión (CLNS/DECNet)

El Protocolo de Internet (IPv4 e IPv6) es el protocolo de la Capa 3 más ampliamente utilizado y son objetos de estudio en esta investigación Los demás protocolos no se analizarán en profundidad.

El Protocolo de Internet IPv4

Fue diseñado como un protocolo de bajo costo. Provee sólo las funciones necesarias para enviar un paquete desde un origen a un destino a través de un sistema interconectado de redes. El protocolo no fue diseñado para rastrear ni administrar el flujo de paquetes. Estas funciones son realizadas por otros protocolos en otras capas. Cisco Systems, (Ob.cit).

Características básicas de IPv4

- Sin conexión: no establece conexión antes de enviar los paquetes de datos. Los paquetes IP se envían sin notificar al host final que están llegando. Los protocolos orientados a la conexión, como TCP, requieren el intercambio de datos de control para establecer la conexión así como también los campos adicionales en el

encabezado de la PDU. Como IP trabaja sin conexión, no requiere un intercambio inicial de información de control para establecer una conexión de extremo a extremo antes de que los paquetes sean enviados, ni requiere campos adicionales en el encabezado de la PDU para mantener esta conexión. Este proceso reduce en gran medida la sobrecarga del IP.

Sin embargo, la entrega del paquete sin conexión puede hacer que los paquetes lleguen al destino fuera de secuencia. Si los paquetes que no funcionan o están perdidos crean problemas para la aplicación que usa los datos, luego los servicios de las capas superiores tendrán que resolver estas cuestiones. Máximo esfuerzo (no confiable): no se usan encabezados para garantizar la entrega de paquetes.

- Máximo esfuerzo (no confiable): no se usan encabezados para garantizar la entrega de paquetes: El protocolo IP no sobrecarga el servicio IP proporcionando confiabilidad. Comparado con un protocolo confiable, el encabezado del IP es más pequeño. Transportar estos encabezados más pequeños genera una menor sobrecarga. Menor sobrecarga significa menos demora en la entrega. Esta característica se prefiere para un protocolo de Capa 3.La función de la Capa 3 es transportar los paquetes entre los hosts tratando de colocar la menor carga posible en la red. La Capa 3 no se ocupa de ni advierte el tipo de comunicación contenida dentro de un paquete. Esta responsabilidad es la función de las capas superiores a medida que se requieren. Las capas superiores pueden decidir si la comunicación entre servicios necesita confiabilidad y si esta comunicación puede tolerar la sobrecarga que la confiabilidad requiere.

Se suele considerar que el IP es un protocolo no confiable. No confiable en este contexto no significa que el IP funciona adecuadamente algunas veces y no funciona bien en otras oportunidades. Tampoco significa que no es adecuado como protocolo de comunicaciones de datos. No confiable significa simplemente

que IP no tiene la capacidad de administrar ni recuperar paquetes no entregados o corruptos.

- Independiente de los medios: funciona sin importar los medios que transportan los datos. La capa de red tampoco está cargada con las características de los medios mediante los cuales se transportarán los paquetes. IPv4 y IPv6 operan independientemente de los medios que llevan los datos a capas inferiores del stack del protocolo, cualquier paquete IP individual puede ser comunicado eléctricamente por cable, como señales ópticas por fibra, o sin cables como señales de radio.

Es responsabilidad de la capa de enlace de datos de OSI tomar un paquete IP y prepararlo para transmitirlo por el medio de comunicación. Esto significa que el transporte de paquetes IP no está limitado a un medio en particular.

Existe, no obstante, una característica principal de los medios que la capa de red considera: el tamaño máximo de la PDU que cada medio puede transportar. A esta característica se la denomina Unidad máxima de transmisión (MTU). Parte de la comunicación de control entre la capa de Enlace de datos y la capa de red es establecer un tamaño máximo para el paquete. La capa de Enlace de datos pasa la MTU hacia arriba hasta la capa de red. La capa de red entonces determina de qué tamaño crear sus paquetes. En algunos casos, un dispositivo intermediario, generalmente un router, necesitará separar un paquete cuando se lo reenvía desde un medio a otro medio con una MTU más pequeña. A este proceso se lo llama fragmentación de paquetes o fragmentación.

Direcciones IP

Todas las maquinas conectadas a Internet tienen una dirección numérica única e irrepetible, llamada dirección IP y que sirve para identificar y poder comunicar a unas

máquinas o interfaces de red con otras, la dirección no se asigna arbitrariamente, se debe hacer una petición al centro de información de la red, conocido por sus siglas en inglés, NIC, el cual es el organismo responsable de la administración de las direcciones de toda la red.

Cada dispositivo de una red debe definirse en forma exclusiva. En la capa de red, es necesario identificar los paquetes de la transmisión con las direcciones de origen y de destino de los dos sistemas finales. Con IPv4, esto significa que cada paquete posee una dirección de origen de 32 bits y una dirección de destino de 32 bits en el encabezado de Capa 3. Cisco Systems, (Ob.cit).

Direcciones IPV4

Estas direcciones se usan en la red de datos como patrones binarios. Dentro de los dispositivos, se aplica la lógica digital para su interpretación. Para su mejor interpretación, éstas se representan las direcciones IPv4 utilizando el formato de decimal punteada. Cisco Systems, (Ob.cit).

Decimal punteada: Los patrones binarios que representan direcciones IPv4 se expresan mediante decimales punteados separando cada byte del patrón binario, llamado octeto, con un punto. Se le llama octeto debido a que cada número decimal representa un byte u 8 bits. Por ejemplo, la dirección: 10101100000100000000010000010100 se expresa como decimal punteada de la siguiente manera: 172.16.4.20. Los dispositivos utilizan la lógica binaria. El formato decimal punteado se usa para que a las personas les resulte más fácil utilizar y recordar direcciones.

Porciones de red y de host: En cada dirección IPv4, alguna porción de los bits de orden superior representan la dirección de red. En la Capa 3, se define una red como un grupo de hosts con patrones de bits idénticos en la porción de dirección de red de sus direcciones. A pesar de que los 32 bits definen la dirección host IPv4, existe una cantidad variable de bits que conforman la porción de host de la dirección.

La cantidad de bits usada en esta porción de host determina la cantidad de host que se puede tener dentro de la red. Con 8 bits se puede lograr un total de 256 patrones de bits diferentes. Esto significa que los bits para los tres octetos superiores representarían la porción de red.

Tipos de Direcciones IPV4

Dirección de red: La dirección de red es una manera estándar de hacer referencia a una red. Por ejemplo: se podría hacer referencia a la red de la figura como "red 10.0.0.0". Ésta es una manera mucho más conveniente y descriptiva de referirse a la red que utilizando un término como "la primera red".

Todos los hosts de la red 10.0.0.0 tendrán los mismos bits de red. Dentro del rango de dirección IPv4 de una red, la dirección más baja se reserva para la dirección de red. Esta dirección tiene un 0 para cada bit de host en la porción de host de la dirección. Cisco Systems, (Ob.cit), Ver figura N° 2

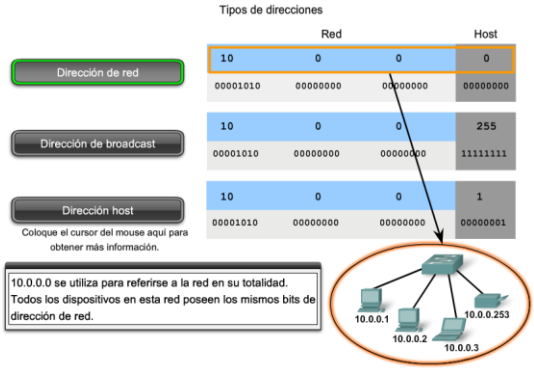


Figura N°2: Direcciones de Red

Fuente: Cisco Systems, (2008)

Dirección de broadcast: La dirección de broadcast IPv4 es una dirección especial para cada red que permite la comunicación a todos los host en esa red. Para enviar datos a todos los hosts de una red, un host puede enviar un solo paquete dirigido a la dirección de broadcast de la red. La dirección de broadcast utiliza la dirección más alta en el rango de la red. Ésta es la dirección en la cual los bits de la

porción de host son todos 1. Para la red 10.0.0.0 con 24 bits de red, la dirección de broadcast sería 10.0.0.255. A esta dirección se la conoce como broadcast dirigido. En la figura N° 3 se puede observar como la dirección de broadcast se usa para enviar paquetes a cada host que comparta la misma porción de red de la dirección. Cisco Systems, (Ob.cit),

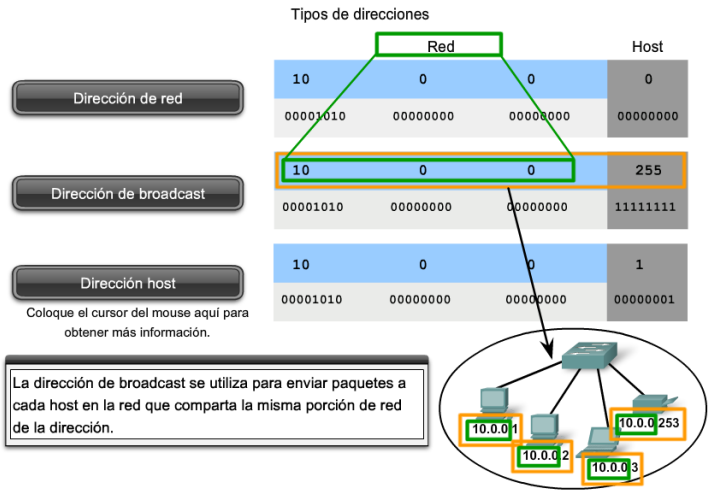


Figura N°3: Dirección de Broadcast

Fuente: Cisco Systems, (2008)

Direcciones host: Como se describe anteriormente, cada dispositivo final requiere una dirección única para enviar un paquete a dicho host. En las direcciones IPv4, se asignan los valores entre la dirección de red y la dirección de broadcast a los dispositivos en dicha red. En la figura N° 4 se puede notar que cada host de la red representada posee una dirección única. Cisco Systems, (Ob.cit),

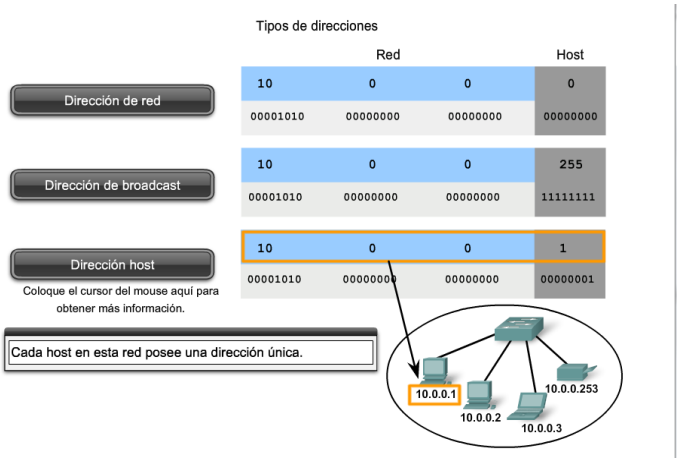


Figura N°4: Dirección de host

Fuente: Cisco Systems, (2008)

Tipos de comunicación en redes IPV4

Tráfico unicast: La comunicación unicast se usa para una comunicación normal de host a host, tanto en una red de cliente/servidor como en una red punto a punto. Cisco Systems, (Ob.cit),

Transmisión de broadcast: Dado que el tráfico de broadcast se usa para enviar paquetes a todos los hosts de la red, un paquete usa una dirección de broadcast especial. Cuando un host recibe un paquete con la dirección de broadcast como destino, éste procesa el paquete como lo haría con un paquete con dirección unicast. La transmisión de broadcast se usa para ubicar servicios o dispositivos especiales para los cuales no se conoce la dirección o cuando un host debe proporcionar información a todos los hosts de la red. Cisco Systems, (Ob.cit),

Existen dos tipos de broadcasts: broadcast dirigido y broadcast limitado. Broadcast dirigido: Un broadcast dirigido se envía a todos los hosts de una red específica. Broadcast limitado: El broadcast limitado se usa para la comunicación que está limitada a los hosts en la red local. Estos paquetes usan una dirección IPv4 de destino 255.255.255.255. Los routers no envían estos broadcasts. Los paquetes

dirigidos a la dirección de broadcast limitada sólo aparecerán en la red local. **Transmisión de multicast**: La transmisión de multicast está diseñada para conservar el ancho de banda de la red IPv4. Ésta reduce el tráfico al permitir que un host envíe un único paquete a un conjunto seleccionado de hosts. Para alcanzar hosts de destino múltiples mediante la comunicación unicast, sería necesario que el host de origen envíe un paquete individual dirigido a cada host. Con multicast, el host de origen puede enviar un único paquete que llegue a miles de hosts de destino. Algunos ejemplos de transmisión de multicast son: Distribución de audio y video, intercambio de información de enrutamiento por medio de protocolos de enrutamiento, distribución de software y suministro de noticias. Cisco Systems, (Ob.cit),

Direcciones IP Públicas y Privadas

El RFC [1918] hace referencia de la necesidad de establecer procedimientos en la asignación de direcciones IPV4, debido al constante crecimiento de Internet y el agotamiento de estas direcciones tal y como se cita textual a continuación:

> Internet ha crecido más allá de todas las previsiones. El continuo crecimiento exponencial continúa presentando nuevos retos. Uno de los retos es la constancia dentro de la comunidad de que el espacio de direcciones globalmente únicas se agotará. Un asunto distinto y bastante más acuciante es que la sobrecarga de encaminamiento crecerá más allá de las capacidades de los "Proveedores de Servicios de Internet", Internet Service Providers (ISP). Dentro de la comunidad existen iniciativas en curso para encontrar soluciones duraderas para ambos problemas. Mientras tanto es necesario reconsiderar los procedimientos de asignación de direcciones, y su impacto en el sistema de encaminamiento de Internet.

RFC [1918] divide en tres categorías las máquinas que usan IP dentro de las organizaciones o empresas:

Categoría 1: máquinas que no necesitan acceder a máquinas en otras empresas, o Internet en general; las máquinas dentro de esta categoría pueden usar direcciones IP que sean únicas dentro de la empresa, pero que pueden no ser.

Categoría 2: máquinas que necesitan acceso a un conjunto reducido de servicios externos (por ejemplo, e-mail, FTP, news, login remoto) que pueden ser gestionados por pasarelas intermedias (por ejemplo, pasarelas de nivel de aplicación). Para muchas máquinas en esta categoría, un acceso sin restricciones al exterior (el proporcionado por la conectividad IP) puede ser innecesario e incluso no deseable por razones de seguridad y/o privacidad. Como en el caso de las máquinas en la primera categoría, tales máquinas pueden usar direcciones IP que sean únicas dentro de la empresa, pero que puedan ser ambiguas entre empresas distintas.

Categoría 3: máquinas que necesitan acceso de nivel de red hacia el exterior de la empresa (proporcionado mediante la conectividad IP); las máquinas en esta última categoría necesitan direcciones IP que sean globalmente únicas. Cabe destacar que se refieren a las máquinas en la primera y segunda categorías como "privadas" y en la tercera categoría como "públicas".

Espacio de direcciones privado: RFC [1918] detalla que La "Autoridad de Números Asignados en Internet", Internet Assigned Numbers Authority (IANA), ha reservado los tres siguientes bloques de

Direcciones IP para el uso en Redes privadas:

Clase A: 10.0.0.0 - 10.255.255.255 (prefijo 10/8)

Clase B: 172.16.0.0 - 172.31.255.255 (prefijo 172.16/12)

Clase C: 192.168.0.0 - 192.168.255.255 (prefijo 192.168/16)

El primer bloque como "bloque de 24 bits", al segundo como "bloque de 20 bits" y al tercero como "bloque de 16 bits". El primer bloque no es más que un único número de red de clase A, mientras que el segundo bloque es un conjunto de 16 números de red de clase B contiguos, y el tercer bloque es un conjunto de 256 números de red de clase C contiguos.

De igual forma el [RFC1918] estipula algunas normativas con el uso de direcciones IP privadas y públicas entre ellas se encuentra que una organización que decida usar direcciones IP del espacio de direcciones definido como privada puede hacerlo sin tener que coordinarse con la IANA o con un registro de Internet. De esta manera el espacio de direcciones puede ser usado por muchas empresas. Las direcciones de este espacio de direcciones privado sólo serán únicas dentro de la empresa, o el conjunto de empresas que elijan colaborar sobre este espacio para que puedan comunicarse con las demás en su propia internet privada. Es importante señalar, que cualquier empresa que necesite espacio globalmente único necesita obtener tales direcciones de un registro de Internet. Una empresa que solicite direcciones IP para su conectividad externa nunca recibirá direcciones de los bloques definidos arriba.

El resto de máquinas serán públicas y usarán espacio de direcciones globalmente únicas asignadas por un registro de Internet. Las máquinas públicas pueden comunicarse con otras máquinas dentro de la empresa, tanto públicas como privadas, y pueden tener conectividad IP con máquinas públicas fuera de la empresa. Las máquinas públicas no tienen conectividad con las máquinas privadas de otras empresas. Cambiar una máquina de privada a pública o viceversa implica un cambio de dirección IP, cambios en las entradas DNS correspondientes, y cambios en los ficheros de configuración de otras máquinas que referencien a la máquina por su dirección IP.

Puesto que las direcciones privadas no tienen significado global, la información de encaminamiento acerca de las redes privadas no se propagará en los enlaces entre empresas, y los paquetes con direcciones origen o destino privadas no deberían ser reenviados por dichos enlaces. Se supone que los enrutadores en las redes que no usen espacio de direcciones privados, especialmente aquéllos situados en los proveedores de servicios de Internet, estarán configurado para rechazar (filtrar) la información de encaminamiento acerca de redes privadas. Si uno de estos enrutadores

recibe tal información, el rechazo no será tratado como un error en el protocolo de enrutamiento.

Mecanismos para el ahorro de direcciones

Tal y como fue mencionado en el planteamiento del problema el ahorro de direcciones públicas IPV4 trajo consigo el desarrollo una serie de técnicas o métodos que a continuación se presentan:

Sub- Redes: Como fue mencionado anteriormente en una dirección IP una porción de la red indica la dirección de la red (identificador de red) y la otra porción indica la estación (o host) en la red (identificador de estación). Esto significa que exista una jerarquía en el direccionamiento IP Para alcanzar una estación en Internet, se debe primero alcanzar la red que utiliza la primea porción de la dirección y posterior a ello se alcanza el dispositivo específico dentro de esa red. Es decir, las direcciones IP de las clases A, B y C están diseñadas con dos niveles de jerarquía. Sin embargo, en muchos casos, estos dos niveles de jerarquía no son suficientes. Tres niveles de jerarquía

Añadir subredes crea un nivel intermedio de jerarquía en el sistema de direccionamiento IP. Ahora se tienen tres niveles: el identificador de red, el de subred y el de estación. El identificador' de red es el primer nivel; define el sitio. El segundo nivel es el identificador de subred; define la subred física. El identificador de estación es el tercer nivel; define la conexión de la estación a la subred. Mencionado de esta manera por Forouzan (2002).

El encaminamiento de un datagrama (paquete) IP ahora involucra tres etapas: entrega al sitio, entrega a la subred y entrega a la estación.

Enmascaramiento: Es el proceso que extrae la dirección de la red física de una dirección IP. El enmascaramiento puede realizarse con o sin sub-redes. Si no se tienen subredes, el enmascaramiento extrae la dirección de red a partir de una

dirección IP Si se tienen subredes, el enmascaramiento extrae la dirección de la subred a partir de la dirección IP

Enmascaramiento sin subredes: Para ser compatibles, los encaminadores utilizan enmascaramiento incluso aunque no haya subredes.

Máscaras con subredes: Cuando hay subredes, la máscara puede variar.

La división de direcciones sin Clases se denomina, Enrutamiento entre dominio sin clases, por su parte, Tanenbaum, (2003) hace referencia al concepto del enrutamiento entre dominios sin clases (CIDR).

> El concepto básico del CIDR, que se describe en el RFC1519, es asignar las direcciones IP restantes en bloques de tamaño variable, independiente de las clases. Si un sitio necesita, digamos, 2000 direcciones, se le da un bloque de 2048 direcciones con un límite de 2048 bytes.

La división en pequeñas pociones de redes con clases y sin clases constituyeron un elemento importante en el ahorro de direcciones, sin embargo fue necesario usa otros mecanismos como NAT que a continuación se detalla.

NAT

El crecimiento exponencial de Internet hace que la insuficiencia de direcciones se convierta en un inconveniente. Una técnica para solucionar este problema es la traducción de direcciones de red, conocida como NAT (network adrres tranlation). NAT, especificada en el RFC1631, es el proceso de traducir o intercambiar una dirección por otra en la cabecera del paquete IP.

> NAT tiene como objetivo solucionar el problema de la falta de direcciones IP Publicas disponibles en Internet. Para hacerlo, utiliza encaminamiento privado en la red local y únicamente publica (traduce) al exterior las direcciones que sean realmente sean necesarias. Este proceso se aplica en el encaminador que separa la red Interna (privada) de la red externa (pública). Barcelo (ob.cit)

Así pues, NAT permite que las redes privadas utilicen direcciones IP no registradas y se pueda conectar a Internet. Cuando una dirección de la red local envía paquetes hacia la red pública, el Router la traducirá las direcciones. Es importante señalar que si no se traducen estas direcciones no se establecerá la comunicación con el exterior, se requiere de una dirección IP pública para poder llegar a la red externa.

Según, Barcelo (ob.cit) hay diferentes formas de traducción de direcciones, entre ellas:

NAT estático: Cada dirección privada tiene su dirección Pública equivalente.

NAT dinámico: El enrutador es el que posee la tabla de NAT de forma dinámica.

PAT: NAT con sobre carga TCP: permite traducir varias direcciones privadas de una red interna a una única dirección publican. De esta forma, para poder distinguir las diferentes comunicaciones utiliza, además, los identificadores de puerto TCP/UDP.

LSNAT (NAT con balanceo de carga): permite balancear la carga de dos direcciones públicas traducidas con NAT.

Palet (2011) en el portal de IPV6 url: http://portalIPv6.lacnic.net/ describe que IPv6 es:

> IPv6 es nueva versión del protocolo de redes de datos en los que Internet está basado. El IETF (Internet Engineering Task Force) desarrollo sus especificaciones básicas durante los años 90. La principal motivación para el diseño y despliegue de IPv6 fue la expansión del espacio de direcciones disponible en Internet, permitiendo así que se conecten billones de nuevos dispositivos (PDAs, teléfonos móviles, etc.), nuevos usuarios y tecnologías "siempre-conectadas" (xDSL, cable, Ethernet en el hogar, Fibra en el hogar, Comunicaciones a través de la red eléctrica, etc.).

En el RFC2460 describe las especificaciones del protocolo de Internet (IP) versión 6 (IPv6) éste ha sido diseñado como el sucesor para el IP versión 4 IPv4

[RFC-791]. Los cambios del IPv4 al IPv6 recaen principalmente en las siguientes categorías:

- Capacidades de Direccionamiento Extendida: El IPv6 incrementa el tamaño de dirección IP de 32 bits a 128 bits, para dar soporte a más niveles de direccionamiento jerárquico, un número mucho mayor de nodos direccionables y una autoconfiguración más simple de direcciones. La escalabilidad del enrutamiento multienvío se mejora agregando un campo "ámbito" a las direcciones multienvío. Y se define un nuevo tipo de dirección llamada "dirección envío a uno de", usado para enviar un paquete a cualquiera de un grupo de nodos.

- Simplificación del Formato de Cabecera: Algunos campos de la cabecera IPv4 se han sacado o se han hecho opcional, para reducir el costo del caso común de proceso de tratamiento de paquete y para limitar el costo del ancho de banda, de la cabecera IPv6 .

- Soporte Mejorado para las Extensiones y Opciones: Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten un reenvío más eficiente, límites menos rigurosos en la longitud de opciones, y mayor flexibilidad para introducir nuevas opciones en el futuro.

- Capacidad de Etiquetado de Flujo: Una nueva capacidad se agrega para permitir el etiquetado de paquetes que pertenecen a "flujos" de tráfico particulares para lo cual el remitente solicita tratamiento especial, como la calidad de servicio no estándar o el servicio en "tiempo real".

- Capacidades de Autenticación y Privacidad: Extensiones para utilizar autenticación, integridad de los datos, y (opcional) confidencialidad de los datos, se especifican para el IPv6.

A continuación se muestra un cuadro comparativo entre los protocolos IPV4 e IPV6. Ver Cuadro N°2:

Cuadro N° 2.
Comparativa IPV4 e IPV6.

IPv6	IPv4
Direcciones de 128 bits (16 bytes)	Direcciones de 32 bits (4 bytes)
Arquitectura jerárquica	Arquitectura plana
Configuración automática	Configuración manual
Multicast y anycast	También Broadcast
Seguridad obligatoria	Seguridad opcional
Identificación QoS	Sin Identificación QoS

Fuente: Fernández. (2010)

Direcciones IPv6

Direcciones especiales en IPv6

Dirección de auto-retorno o Loopback (::1) – No ha de ser asignada a una interfaz física; se trata de una interfaz "virtual", pues se trata de paquetes que no salen de la máquina que los emite; nos permite hacer un bucle para verificar la correcta inicialización del protocolo (dentro de una determinada máquina). Palet (2009)

Dirección no especificada (::) – Nunca debe ser asignada a ningún nodo, ya que se emplea para indicar la ausencia de dirección.

- Túneles dinámicos/automáticos de IPv6 sobre IPv4 (::<direcciónIPv4>) – Se denominan direcciones IPv6 compatibles con IPv4, y permiten la retransmisión de tráfico IPv6 sobre infraestructuras IPv4, de forma transparente. Ver figura N°5

80 bits	16 bits	32 bits
0000 ... 0000	0000	dirección IPv4

Figura N°5: Túneles dinámicos IPv4
Fuente: Palet, (2009)

- Representación automática de direcciones IPv4 sobre IPv6 (::FFFF:<dirección IPv4>) – permite que los nodos que sólo soportan IPv4, puedan seguir trabajando en redes IPv6. Se denominan "direcciones IPv6 mapeadas desde IPv4".Ver figura N°6

80 bits	16 bits	32 bits
0000 ... 0000	FFFF	Dirección IPv4

Figura N°6: Direcciones IPv6 mapeadas desde IPv4
Fuente: Palet, (2009)

Representación de las direcciones IPv6

La representación de las direcciones IPv6 sigue el siguiente esquema Palet (2009):

a) x:x:x:x:x:x:x:x, donde "x" es un valor hexadecimal de 16 bits, de la porción correspondiente a la dirección IPv6. No es preciso escribir los ceros a la izquierda de cada campo.

Ejemplos:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

1080:0:0:0:8:800:200C:417A

b) Dado que, por el direccionamiento que se ha definido, podrán existir largas cadenas de bits "cero", se permite la escritura de su abreviación, mediante el uso de "::", que representa múltiples grupos consecutivos de 16 bits "cero". Este símbolo sólo puede aparecer una vez en la dirección IPv6. Ejemplos:

Las direcciones:

0:0:0:0:0:0:0:1 (la dirección loopback) puede representarse como: ::1 (la dirección loopback)

c) Una forma alternativa y muy conveniente, cuando exista un entorno mixto IPv4 e IPv6 , es x:x:x:x:x:x:d:d:d:d, donde "x" representa valores hexadecimales de 16 bits (6 porciones de mayor peso), y "d" representa valores decimales de las 4 porciones de 8 bits de menor peso

(Representación estándar IPv4). Ejemplos:

0:0:0:0:0:0:**13.1.68.3** Puede representarse como: ::13.1.68.3

La representación de los prefijos IPv6 se realiza del siguiente modo:

dirección-IPv6/longitud-del-prefijo dónde:

- dirección-IPv6 = una dirección IPv6 en cualquiera de las notaciones válidas

- longitud-del-prefijo = valor decimal indicando cuantos bits contiguos de la parte izquierda de la dirección componen el prefijo

Por ejemplo, las representaciones válidas del prefijo de 60 bits

12AB00000000CD3, son:

12AB:0000:0000:CD30:0000:0000:0000:0000/60

12AB::CD30:0:0:0:0/60

12AB:0:0:CD30::/60

Por tanto, para escribir una dirección completa, indicando la subred, se puede hacer como: 12AB:0:0:CD30:123:4567:89AB:CDEF/60

Direcciones unicast locales

Las direcciones unicast, son agregables con máscaras de bits contiguos, similares al caso de IPv4, con CIDR (Class-less Interdomain Routing). Hay varias formas de asignación de direcciones unicast, y otras pueden ser definidas en el futuro.

Los nodos IPv6 pueden no tener ningún conocimiento o mínimo de la estructura interna de las direcciones IPv6, dependiendo de su misión en la red (por ejemplo, host

frente a router). Pero como mínimo, un nodo debe considerar que las direcciones unicast (incluyendo la propia), no tienen estructura, mencionado por Palet (2009).Ver figura N°7

128 bits
Dirección del nodo

Figura N°7: Dirección unicast local

Fuente: Palet, (2009)

El "identificador de interfaz" se emplea, por tanto, para identificar interfaces en un enlace, y deben de ser únicos en dicho enlace. En muchos casos también serán únicos en un ámbito más amplio. Por lo general, el identificador de interfaz coincidirá con la dirección de la capa de enlace de dicha interfaz. El mismo identificador de interfaz puede ser empleado en múltiples interfaces del mismo nodo, sin afectar a su exclusividad global en el ámbito IPv6.

Se han definido dos tipos de direcciones unicast de uso local: Local de Enlace (Link-Local) y Local de Sitio (Site-Local).

Las direcciones locales de enlace: Han sido diseñadas para direccionar un único enlace para propósitos de auto-configuración (mediante identificadores de interfaz), descubrimiento de vecinos, o situaciones en las que no hay routers. Palet (Ob.cit), ver figura N°8.

Tienen el siguiente formato:

10 bits	54 bits	64 bits
1111111010	0	Identificador de interfaz

Figura N°8: Dirección local de enlace

Fuente: Palet, (2009)

Se trata de direcciones FE80::<ID de interfaz>/10.

Por su parte las direcciones locales de sitio: permiten direccionar dentro de un "sitio" local u organización, sin la necesidad de un prefijo global. Se configuran mediante un identificador de subred, de 16 bits. Ver figura N°9

10 bits	38 bits	16 bits	64 bits
1111111011	0	ID de subred	Identificador de interfaz

Figura N°9: Dirección local de sitio

Fuente: Palet, (2009)

Se trata de direcciones FEC0::<ID de subred>:<ID de interfaz>/10

Por tanto, los routers no pueden retransmitir ningún paquete con direcciones fuente o destino que sean locales de enlace (su ámbito está limitado a la red local) ni "local de sitio" (su ámbito está limitado a la red local o de la organización).

Direcciones anycast (RFC2526)

Es importante señalar que las direcciones anycast tienen el mismo rango de direcciones que las unicast. Cuando una dirección unicast es asignada a más de una interfaz, convirtiéndose en una dirección anycast, los nodos a los que dicha dirección ha sido asignada, deben ser explícitamente configurados para que reconozcan que se trata de una dirección anycast.

Existe una dirección anycast, requerida para cada subred, que se denomina "dirección anycast del router de la subred" (subnet-router anycast address). Su sintaxis es equivalente al prefijo que especifica el enlace correspondiente de la dirección unicast, siendo el indicador de interfaz igual a cero: ver figura N°10.

n bits	128-n bits
Prefijo de subred	0000000000000000000

Figura N°10: Dirección anycast del router de la subred

Fuente: Palet, (2009)

Todos los routers han de soportar esta dirección para las subredes a las que están conectados. Los paquetes enviados a la "dirección anycast del Router de la subred", serán enviados a un router de la subred.

Dentro de cada subred, los 128 valores superiores de identificadores de interfaz están reservados para su asignación como direcciones anycast de la subred. La construcción de una dirección reservada de anycast de subred depende del tipo de direcciones IPv6 usadas dentro de la subred. Las direcciones cuyos tres primeros bits (prefijo de formato) tienen valores entre 001 y 111 (excepto las de multicast, 1111 1111), indican con el bit "universal/ local" igual a cero, que el identificador de interfaz tiene 64 bits, y por tanto no es globalmente único (es local). En este caso, las direcciones reservadas anycast de subred se construyen del siguiente modo, según Palet (Ob.cit): Ver figura N°11

64 bits	57 bits	7 bits
Prefijo de subred	1111110111 ... 111	ID anycast
	Identificador de interfaz	

Figura N°11: Direcciones reservadas anycast de subred
Fuente: Palet, (2009)

En el resto de los casos, el identificador de interfaz puede tener una longitud diferente de 64 bits, por lo que la construcción se realiza según el siguiente esquema (ver Figura N°12):

n bits	121-n bits	7 bits
Prefijo de subred	1111111 ... 1111111	ID anycast
	Identificador de interfaz	

Figura N°12: Forma dos para dirección reservada de anycast de subred
Fuente: Palet, (2009)

Direcciones multicast (RFC2375)

Una dirección multicast en IPv6, puede definirse como un identificador para un grupo de nodos. Un nodo puede pertenecer a uno o varios grupos multicast. Ver figura N°13

8	4	4	112 bits
11111111	000T	ámbito	Identificador de Grupo

Figura N°13: Dirección multicast IPv6
Fuente: Palet, (2009)

El bit "T" indica, si su valor es cero, una dirección multicast permanente, asignada únicamente por la autoridad de numeración global de Internet. En caso contrario, si su valor es uno, se trata de direcciones multicast temporales. Los 4 bits que le preceden, que por el momento están fijados a cero, están reservados para futuras actualizaciones. Las direcciones multicast no deben ser usadas como dirección fuente en un paquete IPv6, ni aparecer en ninguna cabecera de encaminado.

Las principales direcciones multicast reservadas son las incluidas en el rango FF0x:0:0:0:0:0:0:0.

Algunos ejemplos útiles de direcciones multicast, según su ámbito, serían:

- FF01:0:0:0:0:0:0:1 – todos los nodos (ámbito local)
- FF02:0:0:0:0:0:0:1 – todos los nodos (ámbito de enlace)

La dirección FF02:0:0:0:0:1:FFxx:xxxx, denominada "Solicited-Node Address", o dirección de nodo solicitada, permite calcular la dirección multicast a partir de la unicast o anycast de un determinado nodo. Para ello, se sustituyen los 24 bits de menor peso ("x") por los mismos bits de la dirección original.

Así, la dirección 4037::01:800:200E:8C6C se convertiría en FF02::1:FF0E:8C6C.

Cada nodo debe de calcular y unirse a todas las direcciones multicast que le corresponden para cada dirección unicast y anycast que tiene asignada.

Direcciones Requeridas para cualquier nodo

Todos los nodos, en el proceso de identificación, al unirse a la red, deben de reconocer como mínimo, las siguientes direcciones: Sus direcciones locales de enlace para cada interfaz, las direcciones unicast asignadas, La dirección de loopback, Las direcciones multicast de todos los nodos, Las direcciones multicast solicitadas para cada dirección unicast o anycast asignadas, Las direcciones multicast de todos los grupos a los que dicho host pertenece.

Además, en el caso de los routers, tienen que reconocer también: La dirección anycast del router de la subnet, para las interfaces en las que está configurado para actuar como Router; todas las direcciones anycast con las que el router ha sido configurado, las direcciones multicast de todos los routers Las direcciones multicast de todos los grupos a los que el router pertenece.

Además, todos los dispositivos con IPv6, deben de tener, predefinidos, los prefijos siguientes: Dirección no especificad, dirección de loopback, prefijo de multicast (FF), prefijos de uso local (local de enlace y local de sitio), direcciones multicast predefinidas y prefijos compatibles IPv4. Se debe de asumir que todas las demás direcciones son unicast a no ser que sean específicamente configuradas (por ejemplo las direcciones anycast).Palet (ob.cit).

Direcciones unicast globales agregables (RFC2374)

Dado que uno de los problemas que IPv6 resuelve es la mejor organización jerárquica del routing en las redes públicas (globales), es indispensable el concepto de direccionamiento “agregable”. En la actualidad ya se emplea este tipo de direcciones, basadas en la agregación por parte de los proveedores del troncal Internet, y los mecanismos adoptados para IPv6, permiten su continuidad. Pero además, se incorpora un mecanismo de agregación basado en “intercambios”. La combinación de

ambos es la que permite un encaminamiento mucho más eficiente, dando dos opciones de conectividad a unas u otras entidades de agregación.

Se trata de una organización basada en tres niveles:

- Topología Pública: conjunto de proveedores e "intercambiadores" que proporcionan servicios públicos de tránsito Internet.
- Topología de Sitio: redes de organizaciones que no proporcionan servicios públicos de tránsito a nodos fuera de su propio "sitio".
- Identificador de Interfaz: identifican interfaces de enlaces.

En la figura N°14, el formato de direcciones agregables ha sido diseñado para soportar proveedores de larga distancia (identificados como Proveedor 1-4), intercambiadores (Intercambiador 1 y 2), proveedores de niveles inferiores (podrían ser ISP's, identificados como Proveedor 5 y 6), y Clientes (Cliente A-F).

A diferencia de lo que ocurre actualmente, los intercambiadores también proporcionarán direcciones públicas IPv6. Las organizaciones conectadas a dichos intercambiadores también recibirán servicios de conectividad directos, indirectamente a través del intercambiador, de uno o varios proveedores de larga distancia. De esta forma, su direccionamiento es independiente de los proveedores de tráfico de larga distancia, y pueden, por tanto, cambiar de proveedor sin necesidad de renumerar su organización. Este es uno de los objetivos de IPv6.Ver figura N°14.

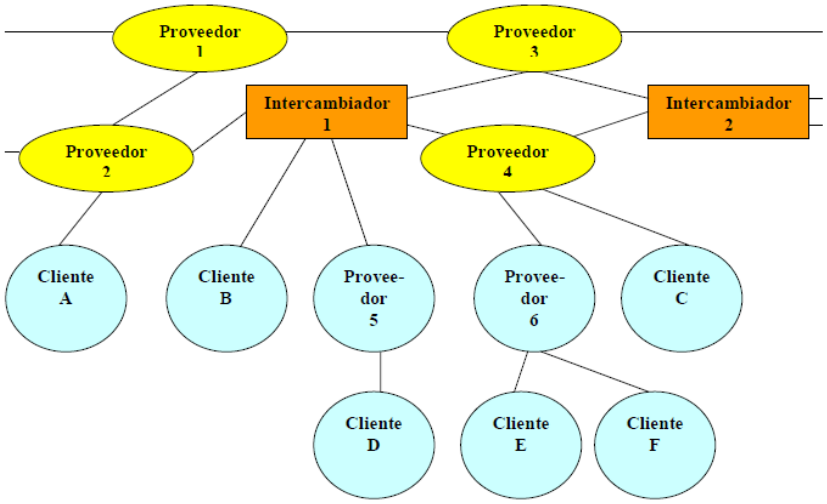


Figura N°14: Direcciones agregables – Conexión ISP
Fuente: Palet, (2009)

Además, una organización puede estar suscrita a múltiples proveedores (multi-homing o "multi-localización"), a través de un intercambiador, sin necesidad de tener prefijos de direcciones de cada uno de los proveedores.

El formato de las direcciones unicast globales agregables es el siguiente: ver figura N° 15:

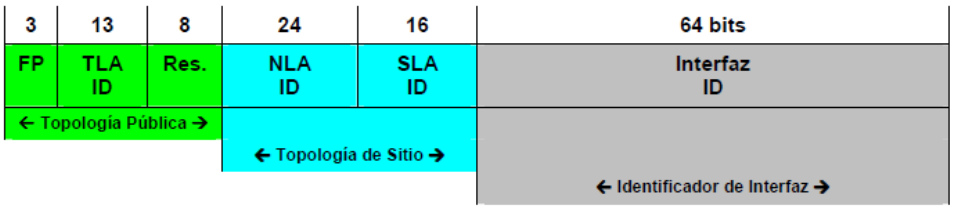


Figura N°15: Unicast globales agregables
Fuente: Palet, (2009)

Dónde, el campo reservado permitirá, en el futuro, ampliaciones "organizadas" del protocolo, por ejemplo ampliar el número de bits de los campos TLA y NLA. Por el momento contiene ceros.

Mecanismos de Transición IPV4 IPV6

Según Palet (2009), las Estrategias de Transición, definidas en el RFC1933:

La clave para la transición es la compatibilidad con la base instalada de dispositivos IPv4. Esta afirmación define un *conjunto de mecanismos que los hosts y routers IPv6 pueden implementar para ser* compatibles con host y routers IPv4. Estos mecanismos permitirán usar infraestructuras IPv4 para IPv6 y viceversa, dado que se prevé que su uso será prolongado, e incluso indefinido en muchas ocasiones.

Estos mecanismos de transición se dividen en tres clases principales:

• Dual Stack: Definido en el RFC2893 También llamados "nodos IPv6/IPv4". IPv6/IPv4 nodos tienen la capacidad de enviar y recibir IPv4 e IPv6 paquetes. Pueden directamente Interoperar con nodos IPv4 usando IPv4 paquetes, y también

directamente Interoperar con nodos IPv6 utilizando paquetes IPv6. Este mecanismo de transición permite a un enrutador, host o servidor utilizar un stack IPv4 y un stack IPv6 simultáneamente, lo que trae consigo dos grandes ventajas: por un lado un nodo con dual stack puede comunicarse con nodos que solo tienen un stack IPv4 de manera nativa y por el otro también puede comunicarse con nodos que solo tengan habilitado el stack IPv6 de manera nativa. Su principal desventaja es la necesidad de contar con una infraestructura de red que soporte el tráfico IPv6 de manera nativa.

Este mecanismo de transición permite a un nodo utilizar un stack (pila) IPv4 y un stack IPv6 simultáneamente teniendo dos grandes ventajas: por un lado un nodo con Dual Stack puede comunicarse con nodos que solo tienen Stack IPv4 de manera nativa y por el otro también puede comunicarse con nodos que solo tengan habilitado el Stack IPv6 de manera nativa. Esta técnica no es nueva, y fue usada en el pasado para el desarrollo de de IPv4 dentro de redes como: Internet Packet Exchange (IPX) y Digital Equipment Corporation Network (DECnet), entre otros.

Es importante mencionar, que las aplicaciones basadas en IPv4 deben ser modificadas para que éstas también soporten IPv6, ya que el API de las aplicaciones basadas en IPv4 está codificado para utilizar únicamente direcciones de 32 bits.

Ver figura N°16

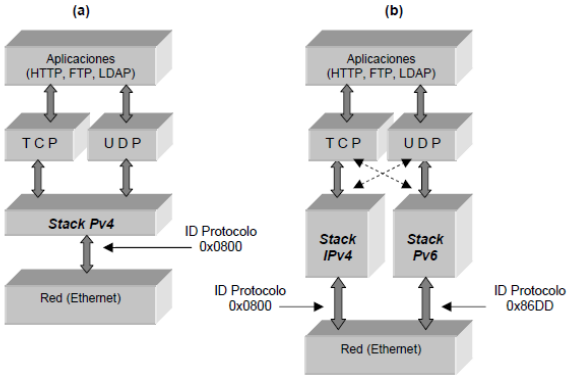


Figura N°16. Arquitectura de Dual Stack:
(Izquierda) Aplicaciones que solo utilizan el Stack IPv4 para enviar Paquetes
(Derecha) Aplicaciones que soportan ambos Stack's para enviar Paquetes
Fuente Palet (2009)

Las aplicaciones que soportan únicamente el Stack de IPv4 pueden utilizar TCP o UDP como capa de transporte para entregar los datos, después estos datos llegan al Stack IPv4, en donde son puestos dentro de paquetes IPv4. Estos paquetes IPv4 más tarde son llevados a la interfaz de red. El valor del identificador del protocolo de red usado por tramas Ethernet para paquetes IPv4 es 0x0800. Cuando las aplicaciones son modificadas para soportar IPv6 tal como se ve en la figura 7 (b), éstas pueden llamar la función del API correcta que pueda manejar direcciones de 128 bits. Así los datos que llegan al dual stack pueden seleccionar cuál de ellos utilizar para generar los paquetes.

Esta selección se puede realizar de dos maneras:

• Manual: Cuando el usuario conoce la dirección IPv6 del nodo destino. Para aplicaciones Web es necesario utilizar el formato para direcciones en un URL tal como está definido en elRFC 2732 [20].

El uso de direcciones manualmente establecidas solo es recomendable para propósitos de depuración, en lo posible debe utilizarse un servicio de nombrado.

• Utilizando un servicio de nombrado: Se puede configurar un Nombre de Dominio Completamente Calificado (FQDN) en un servidor de nombrado DNS con ambas direcciones IPv4 e IPv6 y eventualmente este puede ser consultado para proveer información acerca de la disponibilidad de un nodo sobre IPv4 o IPv6. Una aplicación que soporta ambos stack's IPv4 e IPv6 solicitará al servicio de nombrado le resuelva FQDN en ambos tipos de direcciones, pero generalmente dará preferencia a las direcciones IPv6. La figura N 17, explica gráficamente, en resumen lo que significa este mecanismo de transición

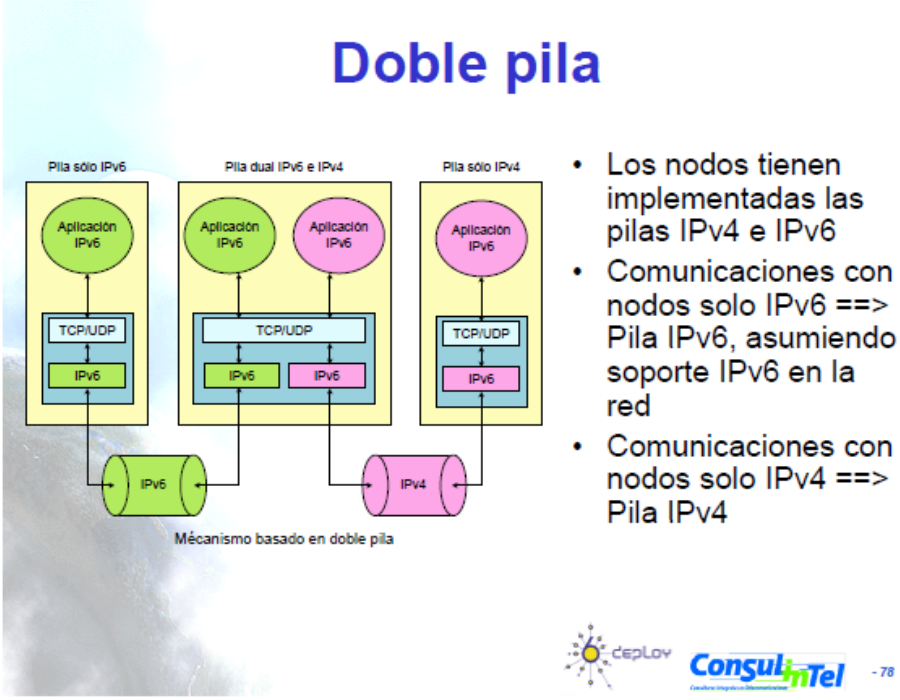


Figura N°: 17. Doble Pila
Fuente: Palet, (2009)

• Túneles: Este mecanismo de transición permite a un enrutador IPv6, host IPv6 o servidor IPv6 comunicarse con otras redes IPv6 a través de la infraestructura IPv4 actual. Esta técnica consiste en encapsular los paquetes IPv6 dentro de paquetes IPv4 y entonces enviarlos sobre una red IPv4 a un nodo IPv4 destino el cual se encargará de extraer los paquetes IPv6 y entregarlos a su destino final. La principal ventaja de éste mecanismo de transición es que solo es necesario tener un Dual Stack en los nodos que servirán como extremos del túnel. Su principal desventaja es el retardo adicional ocasionado por el encapsulado y desencapsulado de paquetes IPv6 en datagramas IPv4, así como el tráfico de un mayor número de paquetes ocasionado por la reducción de espacio para datos en los datagramas IPv4 que contienen dentro paquetes IPv6.

La principal función de los túneles es llevar protocolos incompatibles o datos específicos sobre una red, por ejemplo, los túneles del Protocolo de Enrutamiento

Multicast Vector Distancia (DVMRP) llevan datagramas multicast sobre redes unicast. IPSec en modo túnel lleva datos protegidos por un algoritmo de cifrado. Para el desarrollo de IPv6 sobre una infraestructura existente IPv4 los túneles proveen una manera básica de comunicación entre hosts o islas de hosts IPv6 utilizando IPv4 como medio de transporte. En la figura N°18, se muestra un túnel es creado para comunicar dos islas de hosts IPv6 sobre el Internet. Los enrutadores encargados de administrar el túnel deben tener configurado un dual stack para poder encapsular los paquetes IPv6 en datagramas IPv4 y viceversa.

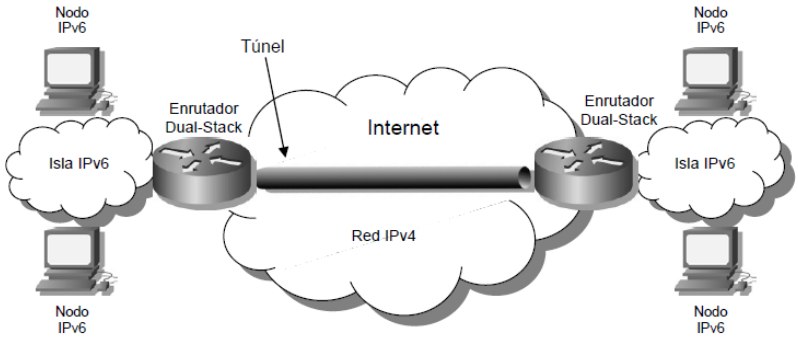


Figura N° 18. Túnel establecido entre dos islas IPv6 a través de la infraestructura IPv4
Fuente: Palet (2009)

Para poder configurar un túnel primero es necesario tomar en cuenta los siguientes aspectos:

• Habilitar el protocolo 41: Si se tiene configurado un cortafuegos sobre IPv4, es necesario establecer una regla que permita el acceso y salida al protocolo 41.

Como está descrito en el RFC 2893 "IPv6 Transition Mechanisms"[21] el número de protocolo asignado a la encapsulación de paquetes IPv6 en IPv4 es el 41. Este valor es utilizado en el campo "Número de Protocolo" en el encabezado de IPv4 para especificar la encapsulación de un paquete IPv6 en un paquete IPv4.

• Manejo de mensajes de error (ICMPv4): Algunos viejos enrutadores en caso de error solo regresan ocho octetos de datos, sin embargo, los nodos emisores de los paquetes IPv6 necesitan conocer los campos de direcciones IPv6 en el error y cada uno de ellos ocupa 16 octetos.

• Traducción de Direcciones de Red (NAT): No es posible establecer túneles IPv6 en IPv4 a través de NAT cuando éste está habilitado en modo traducción dinámica de puerto y redirección de puerto. Por otra parte, es posible establecer dichos túneles si NAT es configurado en modo estático como lo muestra el RFC 2766 [22].

Existen tres posibles escenarios para la creación de un túnel:

• Host a Host: Esta arquitectura requiere que ambos hosts tengan un Dual Stack configurado y solo permite el establecimiento de sesiones IPv6 extremo a extremo entre ellos.

• Host a Enrutador: Hosts con un Dual Stack pueden establecer un túnel con un enrutador que también cuente con un Dual Stack. El enrutador puede tener conectividad IPv6 nativa sobre otra interfaz por lo que esta arquitectura permite el establecimiento de sesiones IPv6 extremo a extremo entre cualquier host de la isla IPv6 y el host aislado a través del enrutador.

• Enrutador a Enrutador: Enrutadores con un Dual Stack sobre una red IPv4 pueden establecer un túnel hacia otro enrutador con Dual Stack. Estos enrutadores pueden ser utilizados para interconectar islas de hosts IPv6, por lo que cualquier host puede establecer sesiones IPv6 extremo a extremo con otro host de la otra isla IPv6.

En la figura N°19 se muestran los tres escenarios posibles para la creación de túneles, el caso (1) muestra la generación de un túnel host a host. El caso (2) presenta la generación de un túnel host a enrutador y por último, el caso (3) presenta la generación de un túnel enrutador a enrutador.

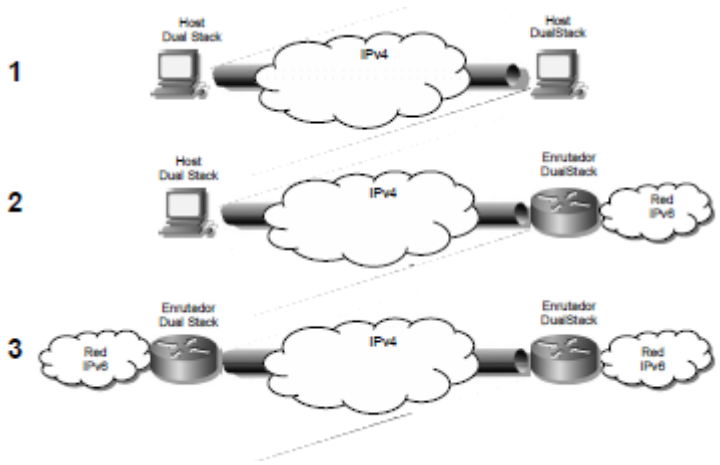


Figura N° 19. Escenarios para la creación de un túnel
Fuente: Palet (2009)

Técnicas para establecer Túneles

El IETF definió protocolos y técnicas para establecer túneles entre nodos con dual-stack, entre estas técnicas se encuentran las siguientes:

Túneles 6to4: En esta técnica los extremos del túnel están determinados por las direcciones globales IPv4 embebidas dentro de direcciones IPv6 6to4. Las direcciones IPv6

6to4 están formadas por la combinación de un prefijo de enrutamiento global 2002::/16 y una dirección IPv4 globalmente única. Los túneles 6to4 pueden ser configurados entre dos enrutadores en la orilla de sus respectivas redes, o entre un enrutador y un host. El único inconveniente de esta técnica para establecer túneles es que solo permiten enviar tráfico IPv6 entre hosts con prefijos de enrutamiento 2002. Para poder comunicarse con nodos con otros prefijos de enrutamiento tales como 2001::/16 y 3FFE::/16 es necesario utilizar un enrutador de reenvío (relay router) del 6bone el cual se encargará de proporcionar un servicio de enrutamiento global 6to4.ver figura N°20.

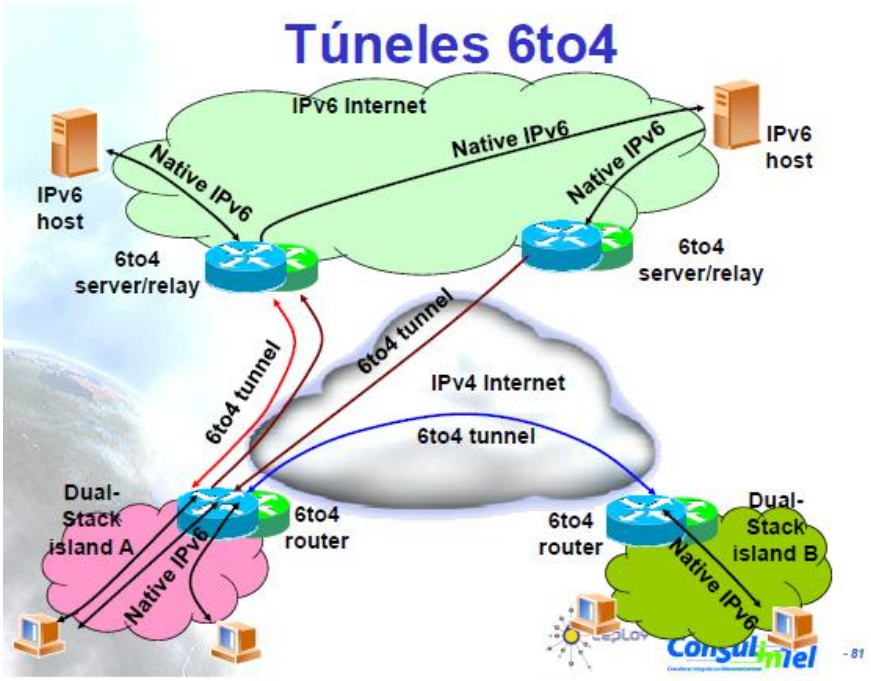


Figura N° 20. Tuneles 6to4
Fuente: Palet (2010)

• Intransite Automatic Tunnel Addressing Protocol (ISATAP): Esta técnica permite crear túneles IPv6-in-IPv4 automáticamente dentro de un sitio IPv4. Cada host solicita a un enrutador dentro del sitio IPv4 una dirección IPv6 e información de enrutamiento, de esta manera, los paquetes enviados al Internet IPv6 son enrutados a través del enrutador ISATAP y los paquetes destinados hacia otros hosts dentro del mismo sitio son entregados directamente mediante túneles ISATAP. Las direcciones IPv6 se configuran automáticamente mediante el protocolo "descubrimiento de enrutador" ISATAP, aunque también pueden ser configuradas de manera manual. Una dirección ISATAP al igual que una dirección 6to4 está formada por la concatenación de un prefijo global de agregación unicast IPv6 y el identificador de interfaz. El prefijo utilizado por ISATAP para habilitar una dirección ISATAP en un host es FE80::/10 (dirección local). El identificador de interfaz es formado agregando los 32 bits de la dirección IPv4, después se concatena el valor 0000:5EFE (reservado

por IANA para identificar direcciones ISATAP). Ejemplo: para una dirección IPv4 148.247.54.122 su dirección IPv6 ISATAP sería FE80::5EFE:94F7:367A. Las direcciones ISATAP también pueden utilizar prefijos unicast Globales de 64 bits, los cuales son asignados por los enrutadores. Cuando un nodo ISATAP desea comunicarse con otro nodo ISATAP sobre IPv6 el paquete IPv6 es encapsulado dentro de un datagrama IPv4 al igual que como sucede con el mecanismo 6to4.

• Tunnel Broker: El IETF definió este mecanismo para facilitar el desarrollo de túneles configurados sobre redes IPv4 ya que mediante esta técnica no se tiene que configurar manualmente cada extremo del túnel. Tal como está establecido en el RFC 3053 "IPv6 Tunnel Broker" [23] el tunnel broker es un sistema externo que actúa como un servidor sobre la red IPv4 y recibe peticiones de nodos con dual stack para configurar túneles automáticamente (modelo cliente-servidor). Estas peticiones son enviadas vía HTTP sobre IPv4 por el nodo que desea configurar dicho túnel. El tunnel broker entonces envía de vuelta al cliente información tal como la dirección IPv4 del servidor del túnel, la dirección IPv6 del servidor del túnel, la nueva dirección IPv6 que será asignada a este host con dual stack y las rutas IPv6 default para la configuración del túnel. Algunos tunnel broker's ya proporcionan scripts de configuración para los hosts clientes. Finamente el tunnel broker aplica comandos de manera remota sobre un enrutador con dual stack y que está conectado a un dominio IPv6 para habilitar el túnel configurado. Para poder hacer uso de esta técnica es necesario utilizar los servicios de alguna entidad que ofrezca el servicio de tunnel broker tales como:

- Freenet6
- Dolphins tunnel broker
- British Telecom tunnel broker
- Hurricane Electric
- SixXS

La gran mayoría de los tunnel brokers ofrecen el servicio de manera gratuita, el único requisito es registrarse mediante el llenado de un pequeño formulario.

• Generic Routing Encapsulation (GRE): Esta técnica fue desarrollada originalmente por Cisco para transportar tráfico Multicast sobre redes unicast y protocolos como IPX y Appletalk sobre IP, pero también puede transportar tráfico IPv6 sobre redes IPv4.

GRE no utiliza TCP o UDP, en su lugar trabaja directamente con la capa IP, utilizando el protocolo número 47. Este incluye sus propios mecanismos para verificar la entrega e integridad de los paquetes. La carga de un paquete GRE incluye un paquete de capa 3 completo con su encabezado y carga intactos. El enrutador en la entrada del túnel GRE toma los paquetes IP y los envuelve en un nuevo paquete con un encabezado GRE, después los envía por la red hasta que alcanzan el enrutador de la salida del túnel. Este extrae el paquete contenido dentro del paquete GRE y lo entrega al nodo destino

• TEREDO: La meta principal de esta técnica es entregar paquetes IPv6 a nodos con dual stack que se encuentran detrás de un dispositivo NAT sobre dominios IPv4. TEREDO fue diseñado por dos principales razones: la primera es que el buen funcionamiento de los túneles 6to4 recae en la configuración de una dirección pública IPv4 y la implementación de enrutamiento 6to4. Debido a que en muchas ocasiones se tienen configuraciones de NAT de varios niveles no sería posible asignar a cada uno de estos dispositivo NAT una dirección pública IPv4. La segunda razón por la que se creó TEREDO es debido a que los paquetes IPv6 encapsulados en paquetes IPv4 utilizan el valor 41 en el campo de protocolo en el encabezado del paquete IPv4 y la mayoría de los dispositivos NAT solamente son capaces de traducir TCP y UDP. Como el protocolo 41 no es común entre los dispositivos

NAT este tipo de paquetes no podrían fluir a través de ellos para alcanzar a los nodos destino. TEREDO utiliza como medio de transporte a UDP para la creación de túneles ya que los dispositivos NAT pueden manejar bien este protocolo a múltiples niveles de anidación. Utilizando una sola dirección IPv4 y mapeos UDP del dispositivo NAT es posible establecer túneles para diferentes hosts con dual stack

detrás de un mismo dispositivo NAT, para ello este mecanismo consta de tres componentes principales:

 Servidor TEREDO: Este servidor está conectado al Internet y cuenta con una dirección global IPv4. Se encarga de administrar la señalización y tráfico con los clientes TEREDO.

 Cliente TEREDO: este se encuentra detrás de un dispositivo NAT y solicita conectividad IPv6 al servidor TEREDO mediante paquetes UDP IPv4.

 TEREDO de reenvío: Está conectado a Internet IPv6 y actúa como enrutador IPv6 para brindar conectividad a los clientes TEREDO mediante el uso de paquetes UDP.

Cada una de estas técnicas está desarrollada para un escenario distinto de aplicación túneles 6to4 está diseñado para interconectar islas IPv6, ISATAP está diseñado para interconectar hosts a enrutadores don dual-stack, tunnel-broker está diseñado para conseguir conectividad IPv6 sobre nodos aislados en redes IPv4, GRE permite no solo encapsular tráfico IPv6 sino también IPX y Appletalk y TEREDO está diseñado para conseguir conectividad IPv6 en hosts que están detrás de dispositivos NAT. Ver figura N°21

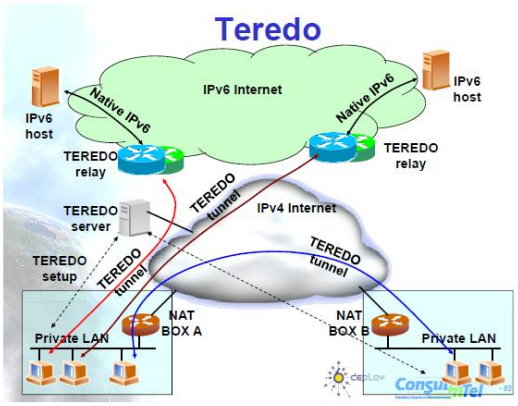


Figura N° 21: Teredo

Fuente: Palet, (2009)

• Traducción de protocolos: Este mecanismo de transición permite a un nodo que solo cuenta con el stack IPv6 habilitado dentro de una red IPv6 comunicarse con

otro nodo que solo tiene el stack IPv4 habilitado dentro de una red IPv4. Sin embargo, ésta técnica requiere tener habilitados mecanismos de traducción entre IPv4 e IPv6 en las orillas de ambas redes (enrutadores). La principal desventaja es que todo el peso de este mecanismo de transición recae en los dispositivos encargados de hacer dicha traducción, a los que no siempre se tiene acceso.

.Para que un nodo en una red IPv6 se puede comunicar con un nodo remoto en una red IPv4 debe usar los mecanismos de translación. Dentro de estos, se encuentra NAT-PT, Network Address Translation - Port Translation, que realiza un mapeo de direcciones IPv6 en direcciones IPv4 modificando la cabecera de los paquetes. Este proceso es similar al NAT tradicional realizado entre direcciones públicas y privadas del protocolo IPv4.La figura N° 22 muestra los distintos tipos de técnicas usadas para la traducción de direcciones IPv4 a IPv6

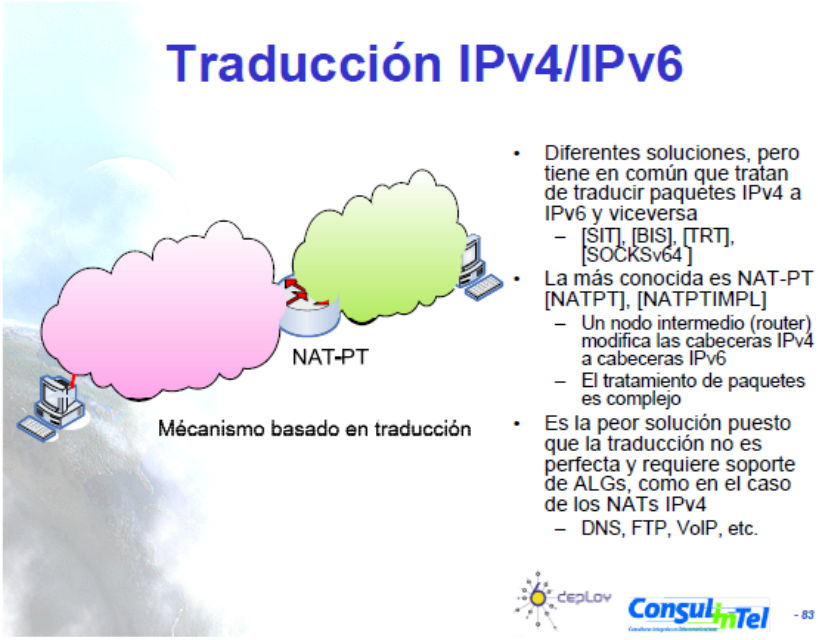


Figura N° 22: Traducción

Fuente: Palet, (2009)

Métodos de traducción:

Traductor IP/ICMP sin estado (SITT):

Ha sido marco de referencia para otros traductores. traduce el datagrama IP.

NAT - PT

En la figura N°23, se muestra el NAT básico usado en IPv4 en el que una dirección IPv4 es traducida a otra IPv4

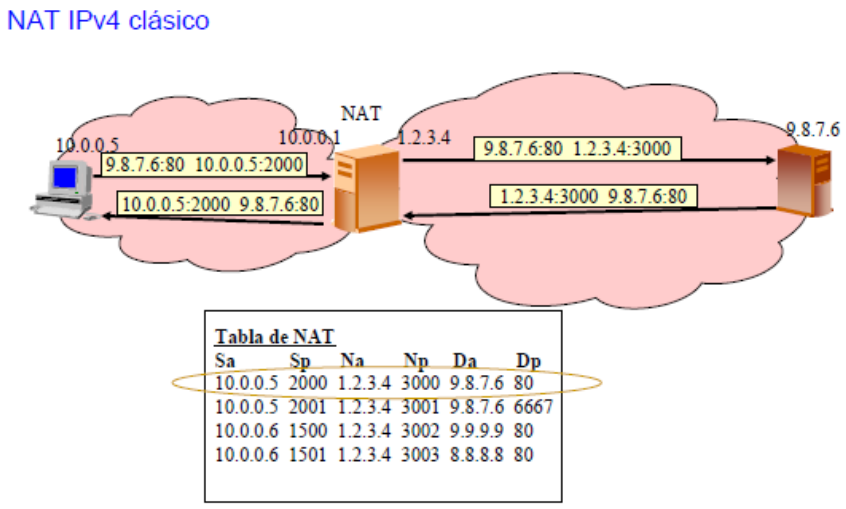


Figura N°23: NAT

Fuente: Palet, (2009)

En la siguiente Figura N° 24, se muestra un NAT- PT simple de IPv6 a IPv4 donde el origen es una dirección IPv6 con un puerto origen y el destino es una dirección Ipv4 con un puerto TCP/UDP destino

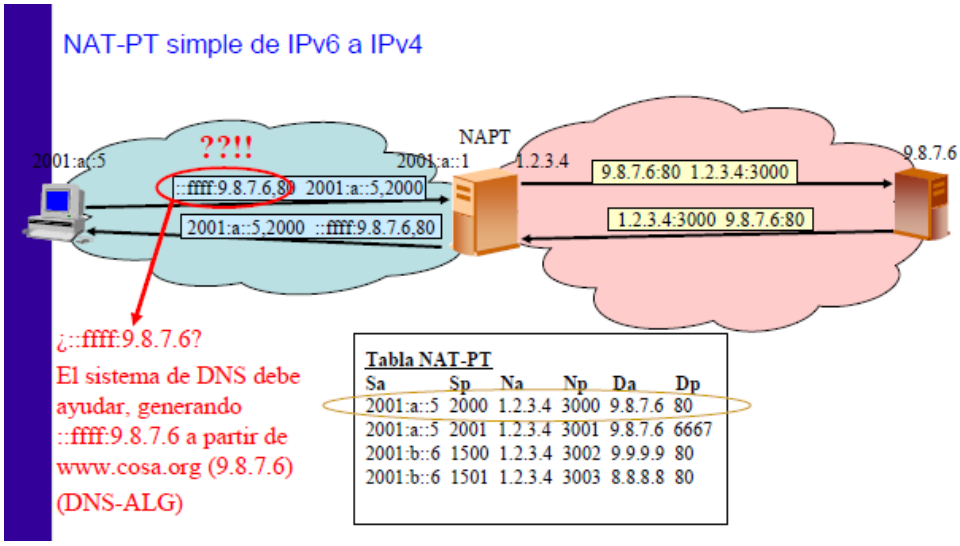


Figura N°24: NAT- PT

Fuente: Palet, (2009)

Existen cuatro situaciones que pueden darse a través de la NAP – PT, están son de un sitio IpV6 a una red IPv4 o viceversa de un sitio IPv4 a una red IPv6 configuradas de forma sencilla o un poca más compleja con traducciones basadas en los DNS tanto para sitios IPv4 e IPv6 respectivamente. Todas las situaciones, representadas gráficamente en la figura N °25.

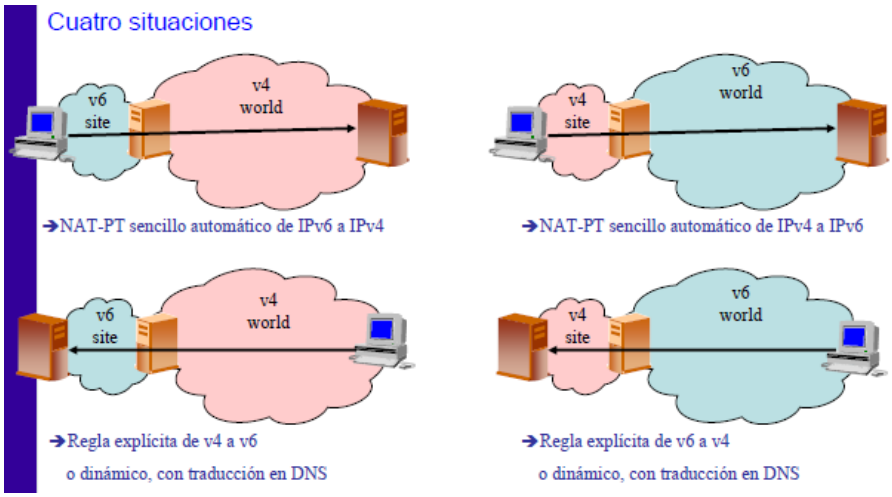


Figura N° 25 : Situaciones NAT

Fuente: Palet, (2010)

Para concluir y como cierre de las bases teóricas, las conceptualizaciones y caracterizaciones explicadas anteriormente guardan una concordancia directa con la investigación presentada en el diseño de la Infraestructura tecnológica de red en el ISP venezolano Telcorp.

Operacionalización de las Variables

Hernández y otros (2000), detalla dos definiciones de variables una la definición conceptual que señala como la definición "de diccionario" o de libros especializados, esta carece de las precisiones necesarias para medir los fenómenos a los que hace referencia el concepto. Y la otra la definición operacional de las variables, esta última constituye el conjunto de procedimientos que describe las actividades que un observador debe realizar para recibir las impresiones sensoriales que indican la existencia de un concepto teórico en mayor o menor grado.

Para Bavaresco (1996), las variables representan diferentes condiciones, cualidades, características o modalidades que asumen los objetos en estudio desde el inicio de la investigación.

Caridad y otros (2008) describen que operacionalizar es definir las variables para que sean medibles y manejables. Un investigador necesita traducir los conceptos (variables) a hechos observables para lograr su medición. Una definición operacional puede señalar el instrumento por medio del cual se hará la medición de las variables.

De igual manera, En la guía ejecutiva para la elaboración de protocolos de tesis y tesis (2004) se define a la Operacionalización de variables de la siguiente manera:

> Consiste en llevar una variable de un nivel abstracto a un nivel concreto, es decir, que permita medirla o calificarla. En esta sección, por cada variable incluida en el estudio, se deberá indicar: Definición teórica, Definición operacional; y en su caso, criterios, diagnósticos, Nivel de medición, Indicadores e Ítems de los instrumentos de investigación.

El objetivo general del presente proyecto es: Diseñar la infraestructura tecnológica de red para la migración de IPV4 a IPV6 en un proveedor de servicios de internet en Venezuela. Caso Telcorp, del cual se puede identificar como el objeto de estudio la infraestructura tecnológica de redes del ISP, las dimensiones de esta variable son las 4 capas de la arquitectura TCP/IP en la que se evaluará esta infraestructura, para ello se tienen indicadores por capas que se medirán usando distintas técnicas de recolección de datos que más adelante se detallan en el capítulo 3.

Cuadro 3.
Operacionalización de las Variables del Proyecto de Estudio.

Variable de estudio	Dimensiones	Indicadores	Instrumentos	Fuente
Diseño de la Infraestructura Tecnológica de Red para la migración de IPV4-IPV6 en el ISP Telcorp.	Arquitectura TCP/IP Aplicación	Datos	entrevistas	Direcciones de Operaciones
		Aplicaciones	Cuestionarios	Personal del NOC y operaciones
		Servicios	Observación Directa	
	Arquitectura TCP/IP Transporte	Direccionamiento de Puertos: TCP-UDP	Software de Monitoreo	
		Fragmentación	Diagramas de representación de la Red	
		Multiplexación y desmultiplexación		
	Arquitectura TCP/IP Internet	Direccionamiento lógico		
		Direccionamiento IP público y privado		
		Protocolos de red: IPV4 –IPV6		
		Dispositivos de Enrutamiento:		
		Tablas de enrutamiento		
	Arquitectura TCP/IP Acceso a Red	Características físicas de las interfaces y el medio		
		Representación de los bits		
Diseño de la Infraestructura Tecnológica de Red para la migración de IPV4-IPV6 en el ISP Telcorp		configuración de la línea		
		Topología física		
		Modo de transmisión		
		Tramado		

		Direccionamiento físico		
		Control de acceso al medio		
		Protocolos acceso al medio		

Fuente: El Autor

Finalmente, las variables presentadas en el cuadro anterior guardan una relación directa con todos los conceptos presentados en las bases teóricas donde se explican la definición de la variable de estudio Infraestructura tecnológica, la conceptualización de los dimensiones representadas por la arquitectura TCP/IP, el detalle de las capas uno (1) dos (2) , tres (3) y cuatro (4) y los fundamentación teórica relacionada con los elementos indicadores usados posteriormente en la realización de los instrumentos de medición.

CAPÍTULO III

MARCO METODOLÓGICO

Naturaleza de la Investigación

El presente trabajo de grado tiene como propósito diseñar la infraestructura tecnológica de red para la migración de IPV4 a IPV6 en un proveedor de servicio de Internet en Venezuela, específicamente Telcorp, permitiéndole a ésta seguir operando en el ámbito de las telecomunicaciones y proveer la gama de para la cual fue concebida.

Considerando los objetivos planteados, este trabajo se encuentra enmarcado en la modalidad de proyecto especial, cuyo desarrollo está orientado a proporcionar un diseño operativo viable, capaz de satisfacer las necesidades y los requerimientos del problema planteado. En el Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales de la UPEL (2002), un proyecto especial se define como:

> Trabajos que lleven a creaciones tangibles, susceptibles de ser utilizadas como soluciones a problemas demostrados. Se incluyen en esta categoría los trabajos de elaboración de libros de texto y de materiales de apoyo educativo, el desarrollo de software, prototipos y de productos tecnológicos en general, así como también los de creación literaria y artística. El estudiante podrá optar por esta categoría cuando el tipo de trabajo seleccionado tenga directa vinculación con el perfil de competencias profesionales del subprograma de postgrado que cursa, o así se establezca en el diseño curricular respectivo.

En referencia a la cita anterior, la investigación encaja en esta modalidad porque el diseño de la infraestructura tecnológica de red para la migración de IPv4 a IPv6 permitirá solucionar un problema demostrado para un proveedor local y que a su vez no es un problema global, como es el caso del agotamiento de las direcciones de

Internet IPv4, además tiene una relación directa con el programa de la maestría de ciencias de la computación en la mención redes de computadoras.

Para concluir, el enfoque metodológico del Diseño de la Infraestructura Tecnológica de Red para la Migración de IPv4 a IPv6 en el ISP Venezolano Telcorp será de tipo cualitativo y cuantitativo.

Diseño de la Investigación

El estudio propuesto de desarrollará en base a las siguientes fases: Fase I, Estudio Diagnóstico; Fase II, Evaluación del método de transición de IPv4 a IPv6. Fase III Diseño de la Propuesta, y Fase IV el estudio de Factibilidad avalado por la información contenida "Manual para la Elaboración de Trabajo Conducentes a Grado Académico de Especialización, Maestría y Doctorado", aprobado por el Consejo Universitario de la UCLA en su Sesión Nº 1353, (2002).

Fases del Estudio

Fase I. Diagnóstico

Se busca determinar la situación actual de la infraestructura tecnológica de red de la empresa Telcorp indagando los diferentes equipos, protocolos y otros presentes en las capas 1, 2, 3 y 4 de la arquitectura TCP/IP, así como la operatividad del ISP, para determinar la necesidad de migración al nuevo protocolo de Internet. Esta fase se realizará usando técnicas e instrumentos para recolectar los datos.

Población y Muestra

Vladimirovna (2002) define a la población "al conjunto de todos elementos de un tipo particular cuyo conocimiento es de interés."

En este trabajo de investigación las unidades de análisis objeto de observación y estudio serán las personas que conforman el área de operaciones de la empresa Sistemas Telcorp, CA. Cabe destacar que la organización posee actualmente siete (7) personas en el área operativa distribuidos de la siguiente manera: un (1) director de operaciones, un (1) gerente de operaciones, tres (3) ingenieros de Operaciones en la región central y uno (1) en la región centrooccidental y un (1) encargado del centro operaciones de la Red o NOC. La población o universo de estudio está conformada por un total de siete (7) profesionales del área de las telecomunicaciones que son los que le dan soporte y administran la infraestructura tecnológica de red de la empresa Telcorp.

Ya ubicado el universo de estudio, se procede a determinar la posibilidad de la recopilación de datos de forma particular sobre todas los elementos que conforman la población o si, por el contrario, se requiere introducir técnicas de muestreo para seleccionar un subconjunto representativo del total de la población de estudio.

Tomando en cuenta que Según Vladimirovna (ob.cit) "se llama muestra a cualquier subconjunto de la población" y que "...si la población posee pequeñas dimensiones, deben ser seleccionados en su totalidad, para así reducir el error en la muestra" según Ary (1996), para el caso de esta investigación los sujetos de estudio vienen representados por el total de la población, es decir las siete (7) personas que laboran en el área de Operaciones de la empresa sistemas Telcorp, CA.

Técnicas e Instrumentos de Recolección de Datos

La selección de técnicas e instrumentos de recolección de datos implica determinar por cuáles medios o procedimientos el investigador obtendrá la información necesaria para alcanzar los objetivos de la investigación." (Hurtado, 2000)

En el caso de esta investigación se utilizarán como técnicas para la recolección de los datos o instrumentos al cuestionario, la entrevista y la observación directa no participante y sistemática en la realidad objeto de estudio, a su vez, ésta se apoyará en herramientas de software de monitoreo y diagramas de documentación de la Red.

Cuestionario

Zapata (2005), expresa que "El diseño del cuestionario presupone estructurar un conjunto de cuestiones que están en el planteamiento del problema, pero que concreta las ideas, creencias o supuestos que tiene el investigador" En referencia a la consideración anterior, en ésta investigación se realizarán preguntas de opción múltiple a los sujetos de estudio referentes a la infraestructura de red actual, el modo de direccionamiento IP usado en la red Telcorp, entre otros aspectos relevantes.

En este propósito, se usará una escala tipo Likert de cinco alternativas para recopilar los datos necesarios en el diagnóstico de la situación actual. Esta escala, definida por Hernández y otros (1997), constituye "un conjunto de ítems presentados en forma de afirmaciones o juicios ante los cuales se pide la reacción de los sujetos a los que se les administra".

La entrevista

Una de las técnicas para recolectar datos en ésta propuesta es la entrevista de tipo Semi-estructurada con el fin de recabar datos pertinentes al levantamiento de información de la red. En este método las "...Preguntas están definidas previamente en un guión de entrevista pero la secuencia, así como su formulación pueden variar en función de cada sujeto entrevistado…"Blasco (2008), el tipo de preguntas a realizar se consideran abiertas conducidas. Así, en este tipo de preguntas se investigan hechos, opiniones o actitudes. Para el caso de ésta investigación como se requiere indagar sobre la situación actual la Infraestructura tecnológica de red (hechos) en la

empresa caso de estudio, desde la perspectiva de las personas que la operan (opiniones), éste tipo de preguntas se adapta perfectamente a lo que se quiere examinar.

Observación directa

En el caso de la propuesta se usará la Observación directa Sistemática y no Participativa donde "el investigador asumirá un papel de espectador de los hechos, del conjunto de actividades y relaciones laborales que se producen cotidianamente" visto de esta forma por Hernández y otros (ob.cit)

Ésta observación directa, tal y como se mencionó en párrafos anteriores será apoyada en herramientas de software, como los son:

- Programas de Monitoreo de Red (The Dude 3.4): para obtener información del funcionamiento de la red en tiempo real y elaborar estadísticas, estudios y diagramas.
- Diagramas de documentación de la red: Levantadas por el investigador en calidad de observación no participativa.

Validez y Confiabilidad del Instrumento

La validez es una condición necesaria de todo diseño e investigación y significa que dicho diseño, "permite detectar la relación real que pretendemos analizar", Arnal (1994) citado por Hurtado (2007), en otras palabras, la validez puede interpretarse que los resultados del instrumento contesten las preguntas enunciadas y no otro argumento. . Por la consideración anterior , los instrumentos usados para recolectar los datos en esta investigación, serán sometidos a la validez de su contenido ante el juicio de dos (2) expertos en el área, y un asesor metodológico, quienes evaluaran su contenido y aplicabilidad a objeto de obtener la información de una manera adecuada y acorde con los objetivos del presente trabajo.

Cabe destacar que como ésta investigación posee dos enfoques el cualitativo y el cuantitativo la validez de los instrumentos no deja de ser importante para el enfoque cuantitativo pero tiene un grado mayor de importancia para el enfoque cualitativo. En éste sentido, (Martínez, 2007) citado por (Rodríguez, 2010), explica que:

> La validez es la fuerza mayor de las investigaciones cualitativas. En efecto, el modo de recoger los datos, de captar los eventos desde diversas perspectivas, de vivir la realidad estudiada inmersa en su propia dinámica, ayuda a superar la subjetividad y da a estas investigaciones un rigor, una credibilidad en sus conclusiones que muy pocos métodos pueden ofrecer.

Con referencia a la confiabilidad, Hurtado (Ob.Cit) hace referencia textual de Ary (1989) señalando que:

> Confiabilidad Denota el grado de congruencia que se realiza en una medición. No le interesa saber si está midiendo lo que se desea, eso es una cuestión de validez. Un instrumento de medición puede ser confiable y no obstante carecer de validez. Sin embargo, no puede ser válido si antes no es confiable.

Para efectos de éste trabajo de investigación para el enfoque cuantitativo la confiabilidad, se determinará a través del Coeficiente Alpha de Cronbach, su valor puede variar entre cero y uno, si bien es posible la existencia de valores negativos, lo que indicaría que en la escala hay algunos ítems que miden lo opuesto a lo que miden los demás, señalados de esta forma por Medina (2006).

Ahora bien, cuanto más cercano esté el valor del Alpha de Cronbach a 1, mayor es la consistencia interna de los ítems que componen el instrumento de medida. Así, al ser como un coeficiente de correlación, no consta un convenio generalizado sobre el cuál es el criterio para determinar si es confiable o no. Para efectos de esta Investigación Los criterios que se usaran serán los definidos por Hernández y otros (1.996) quienes indican que si el Alpha es igual o mayor que 0,9, el instrumento de medición es alta confiabilidad; en el intervalo 0,89-0,76, el instrumento es de fuerte confiabilidad; entre 0,75- 0,50, el instrumento es de moderada confiabilidad; en el

intervalo 0,49- 0,01, el instrumento es de baja confiabilidad; entre 0,-1 no es confiable. La fórmula a usar es la siguiente: Ver figura N° 26.

$$\alpha = \left(\frac{N}{N-1} \right) * \left(\frac{1 - \sum SI^2}{St^2} \right)$$

Figura N°26: Alpha de Cronbach
Fuente: Hernández y otros, (2002)

En donde:

N = Es el número de ítems.

Σ SI^2 = Sumatoria de la varianza por ítems.

St^2 = Varianza Total.

El índice de confiabilidad debe ser menor o igual a uno (1) para que el valor indicativo del instrumento posea un alto grado de consistencia interna, lo que indica la precisión e integridad en los resultados.

Por su parte, en el enfoque cualitativo tal y como lo menciona Rodríguez (2010) "se considera una confiabilidad orientada hacia el nivel de concordancia interpretativa evaluadores o jueces de un mismo fenómeno. Una confiabilidad, sobre todo, interna o ínter-jueces". Por lo que en éste sentido la validez será tomada en cuenta para evaluar la confiabilidad del instrumento con este enfoque.

Técnicas de Análisis de los Datos

En cuanto a las técnicas de análisis de datos Rodriguez (ob.cit) señala que:

> Se presentan los datos numéricos con su respectivo análisis descriptivo (en caso de utilizarse técnicas cuantitativas) o se categoriza la información para luego presentar una síntesis descriptiva (en caso de utilizarse técnicas cualitativas). De acuerdo con Buendía y otros (1998), los datos categóricos o cualitativos pueden representarse o resumirse a través de tablas de frecuencias o descripciones gráficas.

En este sentido, Los resultados obtenidos del enfoque cuantitativo se analizaran mediante la estadística descriptiva, en el cual "los registros u observaciones efectuados proporcionan un serie de datos que necesariamente deben ser ordenados y presentados de una manera inteligible" Fernández (2002). Es decir, los resultados serán ordenados y presentados de una forma que puedan entenderse, "…. Este orden se puede hacer mediante tablas, gráficos y otros..."Landeau (2007). En el caso del enfoque cualitativo se representaran con tablas de frecuencias y se realizará un análisis de los resultados obtenidos en la tabla.

Fase II. Evaluación de las alternativas de migración o metodologías existentes

En esta fase se colocaran los métodos existentes para la migración del protocolo IPv4 a IPv6, en un cuadro comparativo de los mecanismos y se identificará el que se adoptará en la propuesta con su respectivo análisis.

Fase III. Estudio de Factibilidad

Después de abordar la manera en la que se obtendrá el diagnóstico de la situación actual es pertinente realizar un estudio de factibilidad para determinar la capacidad técnica, económica y operativa del proyecto.

Factibilidad Técnica

La factibilidad técnica viene determinada por la facilidad de mantener en funcionamiento el proyecto para ello se determinaran los requerimientos en cuanto a equipos tanto de hardware como de software y su disponibilidad, su facilidad de adquisición y la facilidad de poder reemplazarse en caso de daños u otros agentes externos que pongan en riesgo la integridad del diseño. En este sentido, se debe efectuar un estudio técnico de todos los elementos necesarios para la ejecución de la propuesta.

Factibilidad Económica

Para realizar la recopilación de la información necesaria para el diseño del proyecto, se tendrá en cuenta los requisitos necesarios (los cuales serán indicados en la factibilidad técnica) para efectuar el estudio económico, estableciéndose la vialidad del proyecto en cuanto a costo y beneficios. Así, de esta manera determinar su factibilidad desde el punto de vista económico.

Factibilidad Operativa

Luego de evaluar la factibilidad técnica y económica, es necesario determinar si la nueva infraestructura de red cuanta con personal capacitado para cualquier inconveniente técnico respecto de la misma o si es necesario una capacitación adicional para poder dar soporte y mantenimiento a la infraestructura propuesta. Es por ello, que debe determinarse la vialidad del proyecto desde el punto de vista operativo.

Fase IV. Diseño de la Propuesta

El proyecto consiste en el Diseño de la Infraestructura Tecnológica de red para la migración de IPV4 a IPV6 para el ISP venezolano Telcorp. Para tal fin se cumplirán los siguientes objetivos:

Objetivos del diseño

1. Realizar un banco de datos con el fin de recabar la información necesaria y la terminología a utilizar para el desarrollo de la investigación.
2. Evaluar las capas 1, 2, 3 y 4 de la arquitectura TCP/IP en la infraestructura actual para determinar los equipos y otros requerimientos en el cambio de la Infraestructura.
3. Determinar cuáles son los pasos a seguir para la tramitación de bloques IPV6 válidas.
4. Determinar cuál mecanismo de transición a de usarse para la adopción parcial y definitiva del protocolo IP versión 6.
5. Presentar un plan de migración para la empresa Telcorp.

CAPITULO IV

PROPUESTA DEL ESTUDIO

Fase I: Diagnóstico

El primer paso para presentar la propuesta de Diseño de la Infraestructura Tecnológica de Red para la Migración de IPv4 a IPv6 en el ISP Telcorp viene dado por los resultados del diagnóstico de la operatividad y estado de la infraestructura tecnológica actual de la empresa objeto de estudio con el fin de determinar qué cambios deben producirse en ella para adoptar al nuevo protocolo de Internet IPv6 . A continuación se presentan los pasos realizados para el diagnóstico:

Instrumentos de Recolección de Datos.

El proceso de recolección de los datos se realizó mediante la aplicación de los siguientes instrumentos:

Se aplicó una entrevista Semi estructurada, a las siete (7) personas que laboran el área de operaciones de Telcorp, el cual constó de veintiún (21) preguntas de tipo abiertas conducidas, explicadas en detalle en el capítulo III, específicamente, en el segmento que describe la entrevista. En este propósito el entrevistado podía elegir entre las opciones presentadas y si su respuesta no estaba dentro de las alternativas proporcionadas, podía también elegir otra opción y escribir su consideración. En el anexo N°2, Se muestra la entrevista aplicada.

De igual forma se empleó un cuestionario basado en una escala de tipo Likert, tal y como se detalla en el capítulo anterior. El cuestionario aplicado se observa en el anexo N°3.

Finalmente, se detalla la situación presentada a través de la observación directa, participante y sistemática.

Validez y confiabilidad de los instrumentos

Con el fin de validar el contenido de los instrumentos utilizados, se siguió el procedimiento sugerido, es decir, se sometió a la validez de criterios por juicio de expertos a través del formato para la validación del instrumento (Anexos N°4 y N°5). Con respecto a la confiabilidad instrumento del enfoque "Cuestionario 2", los resultados obtenidos se le aplicó el cálculo del coeficiente de confiabilidad Alpha de Cronbach. Una vez realizado los cálculos pertinentes a los valores correspondientes se obtuvo un Alpha = 0,7656 ó 76,56 % (Anexo N°6), esto se traduce en que el instrumento es de "Fuerte confiabilidad"; tal y como se indica en el capítulo III de ésta investigación.

Técnica de Análisis y Presentación de los Resultados

Las técnicas que se utilizaron para la obtención de información referente a la investigación fueron las siguientes:

Aplicación de la entrevista, realizada a las siete (7) personas que laboran en el área de Operaciones de la empresa objeto de estudio.

Aplicación de un cuestionario a las mismas siete personas, que son los encargados del mantenimiento y soporte de la infraestructura tecnológica de red en Telcorp.

Observación directa de la situación actual de la infraestructura tecnológica de red en la empresa Telcorp, realizada por el investigador.

Resultados de la Entrevista

Los resultados obtenidos de La entrevista (Anexo N°2) se muestran en todos los cuadros que a continuación se presentan, en cada uno de los tablas se muestran la

pregunta realizada y las 7 respuestas obtenidas, al igual que el análisis de cada una de ellas. Ver cuadro N°4.

Cuadro N° 4

Pregunta Número 1		
¿Qué interfaces físicas interconectan su red con su ISP principal?		
( )	Ethernet	
( )	E1	
( )	V.35	
( )	otra	Especifique:_____
Resultados		
Entrevistado:	Respuesta seleccionada	
1	Ethernet	
2	Ethernet	
3	Ethernet	
4	Ethernet	
5	Ethernet	
6	Ethernet	
7	Ethernet	
Pregunta Número 2		
¿Qué interfaces físicas interconectan sus clientes con su infraestructura tecnológica de red?		
( )	Ethernet	
( )	E1	
( )	V.35	
( )	otra	Especifique:_____
Resultados		
Entrevistado:	Respuesta seleccionada	
1	Ethernet	
2	Ethernet	
3	Ethernet	
4	Ethernet	
5	Ethernet	
6	Ethernet	
7	Ethernet	
Pregunta Número 3		
¿Qué interfaces físicas interconectan sus clientes con su infraestructura tecnológica de red?		
( )	Ethernet	
( )	E1	

( )	**V.35**	
( )	**otra**	**Especifique:_____**
Resultados		
Entrevistado:	**Respuesta seleccionada**	
1	**Ethernet**	
2	**Ethernet**	
3	**Ethernet**	
4	**Ethernet**	
5	**Ethernet**	
6	**Ethernet**	
7	**Ethernet**	

Fuente: El autor

Estas tres primeras preguntas evalúan la capa 1 de la arquitectura TCP/IP en la Infraestructura Tecnológica de red Telcorp, Según la información proporcionada por los entrevistados, Telcorp usa interfaces Ethernet para comunicarse con su ISP principal, entre sus nodos y la interfaz final que se le otorga al cliente para los servicios que ofrece es Ethernet o IEEE 802.3.

A continuación en el cuadro N°5, se presentan los resultados de las siguientes preguntas:

Cuadro N° 5.

Pregunta Número 4		
¿Cuál es su topología física usada entre los nodos y los clientes?		
( )	**Estrella**	
( )	**Malla**	
( )	**Anillo**	
( )	**Estrella extendida**	
( )	**Token ring**	
( )	**otra**	**especifique**
Resultados		
Entrevistado:	**Respuesta seleccionada**	
1	**Estrella**	
2	**Estrella**	
3	**Estrella**	

4	**Estrella**
5	**Estrella**
6	**Estrella**
7	**Estrella**
Pregunta Número 5	
¿Cuál es su topología física usada en los enlaces troncales?	
( )	**Estrella**
( )	**Malla**
( )	**Anillo**
( )	**Estrella extendida**
( )	**Token ring**
( )	**otra** **especifique**
Resultados	
Entrevistado:	**Respuesta seleccionada**
1	**Malla**
2	**Estrella extendida, Anillo y Malla**
3	**Estrella extendida, Anillo y Malla**
4	**Anillo**
5	**Estrella**
6	**Estrella**
7	**Estrella**

Fuente: El Autor

Las respuestas obtenidas muestran que la topología usada entre los nodos y los clientes es estrella en cual existe un nodo central y varios clientes conectados a ella. Por su parte para el área de troncales Telcorp posee topología hibrida en la que predomina la estrella, pero también poseen topología malla y anillo. Ambas preguntas permiten perfectamente identificar un aspecto de la capa Acceso a la red de la arquitectura TCP/IP.

A continuación en el cuadro N°6, se presentan los resultados de las siguientes preguntas:

Cuadro N°6.

Pregunta Número 6		
¿Cuál es el modo de transmisión usada por su infraestructura tecnológica de red?		
()	half duplex	
()	Dúplex	
()	Simplex	
()	full dúplex	
()	negociación automática	
()	otra	especifique

Resultados	
Entrevistado:	**Respuesta seleccionada**
1	Negociación Automática
2	Full duplex
3	Negociación Automática y full Duplex
4	Negociación Automática y full Duplex
5	Full Duplex
6	Negociación Automática
7	Negociación Automática

Fuente: El Autor

En las respuestas se observan que el modo de transmisión empleado en la IT de red de Telcorp es variada, entre dúplex,full, duplex y negociación automática. Se puede afirmar modo de transmisión Half Duplex puede estar presente en los equipos donde se negocia automáticamente, del resto no aparece dentro de las respuestas de los entrevistados. Lo que indica que la tecnología de Telcorp a nivel de modos de transmisión usa Ethernet superior a 10 base T.

A continuación en el cuadro N°7, se presentan los resultados de las siguientes preguntas:

Cuadro N°7

Pregunta Número 7
¿Cuál es el protocolo estándar de capa 2 del modelo de referencia OSI usado por su IT?

( )	Ethernet	
( )	Frame relay	
( )	X25	
( )	RDSI	
( )	Otro	especifique

Resultados	
Entrevistado:	**Respuesta seleccionada**
1	Ethernet
2	Ethernet
3	Ethernet
4	Ethernet
5	Ethernet
6	Ethernet
7	Ethernet

Fuente: El Autor

En la red Telcorp predomina el protocolo Ethernet tal y como se ha visto en el tipo de interfaces y otros aspectos preguntados con reactivos anteriores.

A continuación en el cuadro N°8, se presentan los resultados de los reactivos que evalúan el medio de transmisión.

Cuadro N°8.

Pregunta Número 8		
¿Cuál es el medio de transmisión usado entre un cliente y un nodo o punto de repetición?		
( )	Alámbrico – UTP	
( )	Alámbrico - Coaxial	
( )	Alámbrico - Fibra óptica	
( )	Inalámbrico	
( )	otro	especifique

Resultados	
Entrevistado:	**Respuesta seleccionada**
1	Inalámbrico
2	Inalámbrico y Alámbrico UTP

3	Inalámbrico y Alámbrico UTP
4	Inalámbrico
5	Inalámbrico
6	Inalámbrico
7	Inalámbrico

Pregunta Número 9		
¿Cuál es el medio de transmisión usado entre sus enlaces troncales (interconexión entre nodos)?		
( )	Alámbrico – UTP	
( )	Alámbrico - Coaxial	
( )	Alámbrico - Fibra óptica	
( )	Inalámbrico	
( )	otro	especifique

Resultados	
Entrevistado:	**Respuesta seleccionada**
1	Inalámbrico
2	Inalámbrico
3	Inalámbrico
4	Inalámbrico
5	Inalámbrico
6	Inalámbrico
7	Inalámbrico

Pregunta Número 10		
¿Cuál es el medio de transmisión usado entre su ISP y su nodo principal?		
( )	Alámbrico – UTP	
( )	Alámbrico - Coaxial	
( )	Alámbrico - Fibra óptica	
( )	Inalámbrico	
( )	otro	especifique

Resultados	
Entrevistado:	**Respuesta seleccionada**
1	Alámbrico - UTP
2	Alámbrico - Fibra óptica e Inalámbrico

3	Alámbrico – Fibra óptica e Inalámbrico
4	Alámbrico - UTP
5	Alámbrico - UTP
6	Alámbrico - UTP
7	Alámbrico - UTP

Fuente: El Autor

Los reactivos 8, 9 y 10 indican que Telcorp interconecta sus nodos a través de conexiones Inalámbricas y que el medio de transmisión entre su ISP y su nodo principal es de forma alámbrica a través de cable UTP o fibra óptica. Éste elemento es importante para la determinación del estado actual de la Infraestructura Tecnológica de red en Telcorp. Pues, define el medio de trasmisión.

A continuación en el cuadro N° 9, se presentan los resultados de las siguientes preguntas:

Cuadro N°9.

Pregunta Número 11	
¿Cuál es el método de acceso al medio usado entre sus nodos (puntos de repetición) y sus clientes?	
( )	CSMA/CD
( )	CSMA/CA
( )	Otro
Resultados	
Entrevistado:	**Respuesta seleccionada**
1	CSMA/CD
2	CSMA/CD
3	CSMA/CD
4	CSMA/CD Otro Wifi
5	CSMA/CA
6	CSMA/CA
7	CSMA/CA
Pregunta Número 12	

¿Cuál es el método de acceso al medio usado para interconectar sus enlaces troncales?	
( )	CSMA/CD
( )	CSMA/CA
( )	Otro
Resultados	
Entrevistado:	**Respuesta seleccionada**
1	CSMA/CA
2	CSMA/CA
3	CSMA/CA
4	Otro Wifi
5	CSMA/CA
6	CSMA/CA
7	CSMA/CA
Pregunta Número 13	
¿Cuál es el método de acceso al medio usado entre su nodo principal y su ISP?	
( )	CSMA/CD
( )	CSMA/CA
( )	Otro
Resultados	
Entrevistado:	**Respuesta seleccionada**
1	CSMA/CD
2	CSMA/CD
3	CSMA/CD
4	CSMA/CD
5	CSMA/CD
6	CSMA/CD
7	CSMA/CD

Fuente: El Autor

Las repuestas de los entrevistados en los anteriores reactivos demuestran que el método de acceso al medio usado en la IT Telcorp, coincide precisamente con el medio seleccionado por en las preguntas anteriores. Donde destaca Ethernet que

posee como método de acceso al medio a CSMA/CD y CSMA/CA que define el método de acceso en redes inalámbricas, medio de transmisión usado en la red Telcorp.

A continuación en el cuadro N° 10, se presentan los resultados de las los reactivos que evalúan la capa de Internet:

Cuadro N° 10.

Pregunta Número 14	
¿Cuál es el protocolo de capa 3 del modelo de referencia OSI usado en su IT?	
( )	IPV4
( )	IPV6
( )	IPX
( )	Netware
( )	Otro
Resultados	
Entrevistado:	**Respuesta seleccionada**
1	IPv4
2	IPv4
3	IPv4
4	IPv4
5	IPv4
6	IPv4
7	IPv4
Pregunta Número 15	
¿Su direccionamiento IP privado (local) se corresponde con la clase de direcciones?	
( )	A
( )	B
( )	C
( )	D
( )	Otra
Resultados	
Entrevistado:	**Respuesta seleccionada**

1	B
2	B
3	C
4	B
5	B
6	B
7	B
Pregunta Número 16	
¿Su direccionamiento IP público se corresponde con la clase de direcciones?	
( )	A
( )	B
( )	C
( )	D
( )	Otra
Resultados	
Entrevistado:	**Respuesta seleccionada**
1	C
2	C
3	B
4	C
5	C
6	C
7	C

Fuente: El Autor

En las respuestas obtenidas se puede notar que la empresa no usa direccionamiento IPv6 y que actualmente posee direcciones clase B y C IPv4, tanto para su red Interna como la externa.

A continuación en el cuadro N° 11, se presentan los resultados de las pregunta 17:

Cuadro N°11.

Pregunta Número 17	
¿Cuál es el mecanismo usado para la traducción de direcciones IP privadas a públicas?	
( )	NAT
( )	PAT
( )	DINAMIC DNS
( )	No aplica
( )	Otros
Resultados	
Entrevistado:	**Respuesta seleccionada**
1	Nat
2	Nat
3	Nat
4	Nat y dinamic DNS
5	Nat y dinamic DNS
6	Nat
7	Nat

Fuente: El Autor

Como se muestra en los resultados anteriores, actualmente el ISP objeto de estudio emplea diversos mecanismos para resolver el problema del agotamiento de direcciones Ip públicas IPv4, tales como NAT.

A continuación en el cuadro N° 12, se presentan los resultados de las pregunta 18 y 19:

Cuadro N°12.

Pregunta Número 18	
¿En el esquema planteado por los órganos reguladores de direcciones IP públicas, Telcorp es considerado como un ISP?	
( )	Global
( )	Regional
( )	Local

( )	Otros
Resultados	
Entrevistado:	**Respuesta seleccionada**
1	local
2	local
3	local
4	local
5	local
6	local
7	local
Pregunta Número 19	
¿A Quién le corresponde realizar la resolución de nombres de dominio en los servicios que Telcorp ofrece a sus clientes?	
( )	Telcorp
( )	ISP Global
( )	ISP Regional
( )	Otros
1	ISP global
2	Isp regionales
3	Otros:Bt latam
4	Telcorp y Otros: BT latam
5	Otros:Bt latam
6	Otros:Bt latam
7	Otros:Bt latam

Fuente: El Autor

En las respuestas obtenidas se denota que el ISP primario, también llamado regional y global es el que realiza en IPv4 la resolución de nombres.

A continuación en el cuadro N° 13, se presentan los resultados de las pregunta 20 y 21, reactivos que evalúan el tipo de enrutamiento actual que usa la IT de Telcorp:

Cuadro N°13.

Pregunta Número 20	
¿Qué tipo de enrutamiento usa su Infraestructura Tecnológica de Red?	
( )	Estático
( )	dinámico
( )	Otros
Resultados	
Entrevistado:	**Respuesta seleccionada**
1	dinámico
2	dinámico y estático
3	dinámico y estático
4	dinámico y estático
5	otros: ambos
6	otros: ambos
7	otros: los dos
Pregunta Número 21	
¿Qué protocolo de enrutamiento es usado por Telcorp en su IT?	
( )	RIP
( )	RIP V2
( )	IGRP
( )	EIGRP
( )	OSPF
( )	IS-IS
( )	otros
Resultados	
Entrevistado:	**Respuesta seleccionada**
1	Ospf
2	Ospf
3	Ospf

4	Ospf
5	Ospf
6	Ospf
7	Ospf

Fuente: El Autor

En los resultados anteriores, se puede notar que Telcorp combina protocolos de enrutamiento dinámico con enrutamiento estático permitiendo afirmar que el protocolo de enrutamiento dinámico, empleado por Telcorp es el OSPF. Con estos resultados, se conoce los elementos presentes en la IT del ISP.

Resultados del Cuestionario

A continuación se presentan los resultados de la aplicación del cuestionario dirigido a los miembros del equipo técnico de la empresa Telcorp. Las abreviaturas de las categorías de respuestas son las siguientes:

TD: Totalmente en Desacuerdo

ED: En Desacuerdo

NEU: Neutro

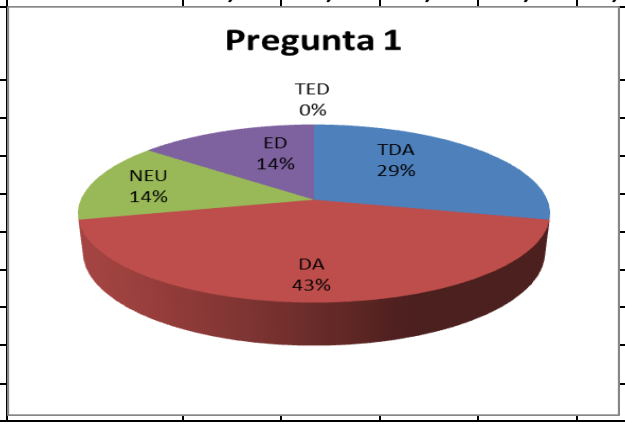
DA: De Acuerdo

TA: Totalmente de Acuerdo

Según lo establecido por escalamiento líkert, el máximo valor de cinco (5) a TA (Totalmente de Acuerdo) y el valor uno (1) es asignado a TD (Totalmente en Desacuerdo). El resumen de casos del cuestionario se muestran en el (Anexo N°7). A continuación se realiza el respectivo cuadro de frecuencia, gráfico representativo y el detalle de lo observado estadísticamente tabulado. Ver cuadros N° 14, 15, 16, 17, 18, 19,20 y 21

Cuadro N°14.
Pregunta N°1 del cuestionario

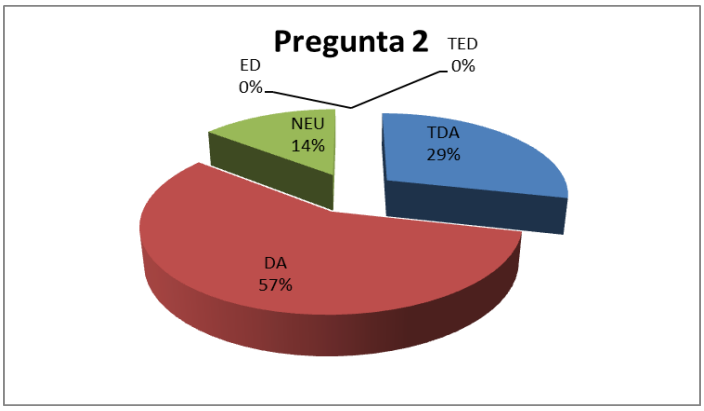
Pregunta 1.	¿Las interfaces de la infraestructura tecnológica de red Telcorp son Ethernet?					
	Pregunta 1	TDA	DA	NEU	ED	TED
		2	3	1	1	0
		28,57	42,86	14,29	14,29	0,00



Fuente: El Autor

Cuadro N°14.
Pregunta N°2 del cuestionario

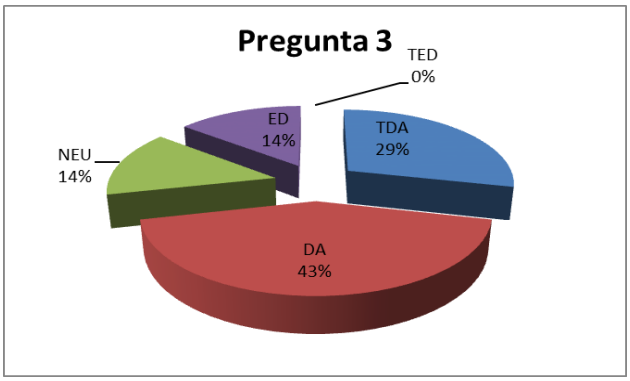
Pregunta 2. ¿Cree usted que el esquema de direccionamiento actual usado por Telcorp, NO garantiza la sustentabilidad de los servicios de Internet dedicado?						
	Pregunta 2	TDA	DA	NEU	ED	TED
		2	4	1	0	0
		28,57	57,14	14,29	0,00	0,00



Fuente: El Autor

Cuadro N°15
Pregunta N°3 del cuestionario

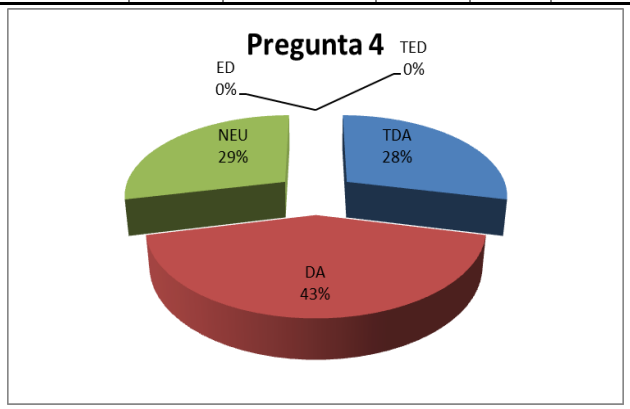
¿Cree usted que los equipos de RF permiten trafico IPv6?					
Pregunta 3	**TDA**	**DA**	**NEU**	**ED**	**TED**
	2	**3**	**1**	**1**	**0**
	28,57	**42,86**	**14,29**	**14,29**	**0,00**



Fuente: El Autor

Cuadro N°16
Pregunta N°4 del cuestionario

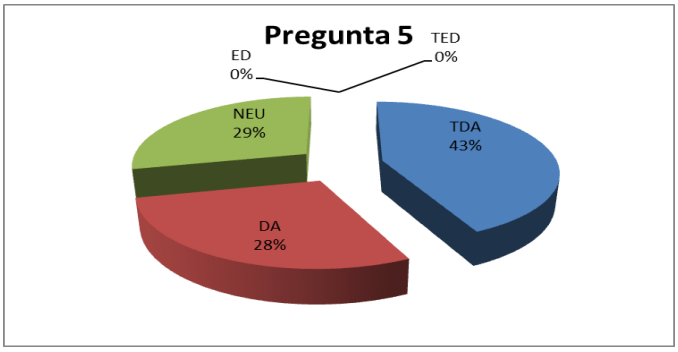
¿Cree usted que los enrutadores usados en la Infraestructura tecnológica de red que usa Telcorp poseen soporte para IPv6?					
Pregunta 4	**TDA**	**DA**	**NEU**	**ED**	**TED**
	2	**3**	**2**	**0**	**0**
	28,57	**42,86**	**28,57**	**0,00**	**0,00**



Fuente: El Autor

Cuadro N°17
Pregunta N°5 del cuestionario

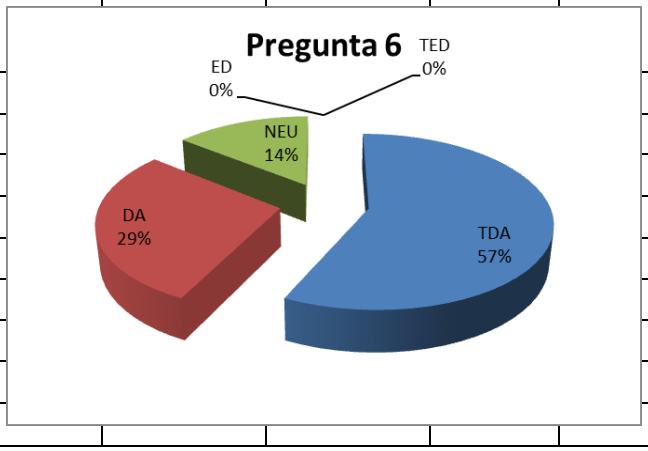
Pregunta 5. ¿Telcorp usa NAT como mecanismo de traducción de direcciones IP privadas a públicas?					
Pregunta 5	TDA	DA	NEU	ED	TED
	3	2	2	0	0
	42,86	28,57	28,57	0,00	0,00



Fuente: El Autor

Cuadro N°18
Pregunta N°6 del cuestionario

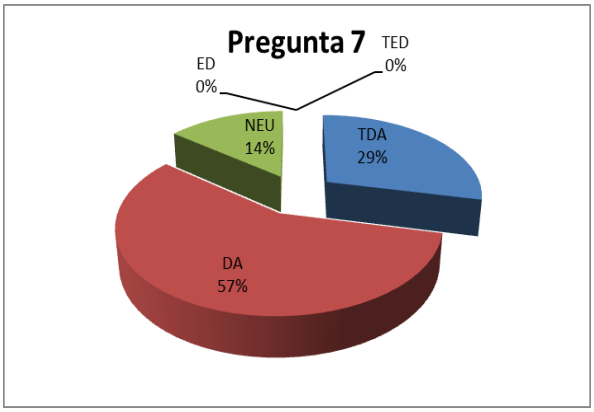
Pregunta 6 ¿Telcorp, combina en su Infraestructura enrutamiento dinámico con enrutamiento estático?					
Pregunta 6	TDA	DA	NEU	ED	TED
	4	2	1	0	0
	57,14	28,57	14,29	0,00	0,00



Fuente: El Autor

Cuadro N°19
Pregunta N°7 del cuestionario

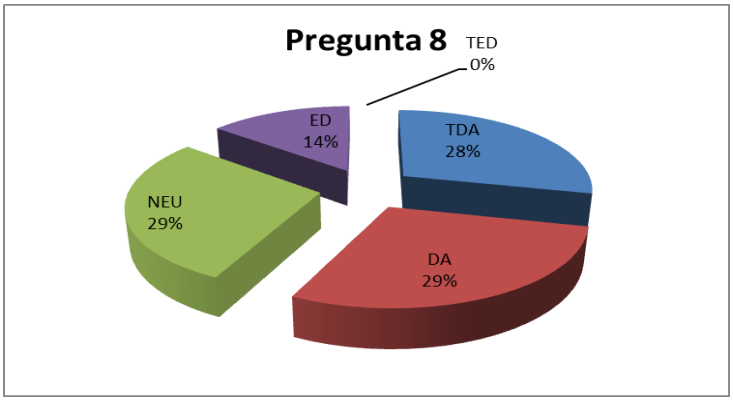
Pregunta 7 ¿Los enrutadores de Telcorp, permiten re direccionar puertos TCP/ UDP?					
Pregunta 7	TDA	DA	NEU	ED	TED
	2	4	1	0	0
	28,57	57,14	14,29	0,00	0,00



Fuente: El Autor

Cuadro N°20
Pregunta N°8 del cuestionario

Pregunta 8. ¿Telcorp como ISP, posee configuraciones en su firewall para que algunas aplicaciones de clientes sean rechazadas y aceptadas?					
Pregunta 8	TDA	DA	NEU	ED	TED
	2	2	2	1	0
	28,57	28,57	28,57	14,29	0,00



Fuente: El Autor

El cuestionario reafirmo la información obtenida en la entrevista sobre el uso de técnicas de traducción de direcciones IP, sobre el reenvío de puertos capa de transporte y otros aspectos de la IT de red en el ISP Telcorp. Como se determino en los resultados del cuestionario desde la perspectiva del 86 % de los empleados del área de operaciones de la empresa Telcorp consideran que el esquema de direccionamiento actual NO garantiza la sustentabilidad de los servicios de Internet dedicado, además la información obtenida reafirma el uso d**e** NAT y otros para resolver el problema.

Observación directa

La observación directa permitió no solo corroborar algunos elementos presentes en la IT de Telcorp sino que además con esta fase se levantó información un poco más detallada del funcionamiento de la red y de la empresa objeto estudio. Esta etapa permitió registrar mapas, diagramas y otros elementos no percibidos en los anteriores instrumentos. A continuación se muestra la información recabada en esta etapa.

Telcorp, formalmente Sistemas Telcorp, C.A5., RIF6. J-30917169-0, es una empresa legalmente constituida en 2002 para proveer servicios de Internet, transporte de datos y soluciones de tecnología de la información y comunicación para el mercado corporativo. A continuación se muestra el organigrama de la empresa. Ver Figura N° 27

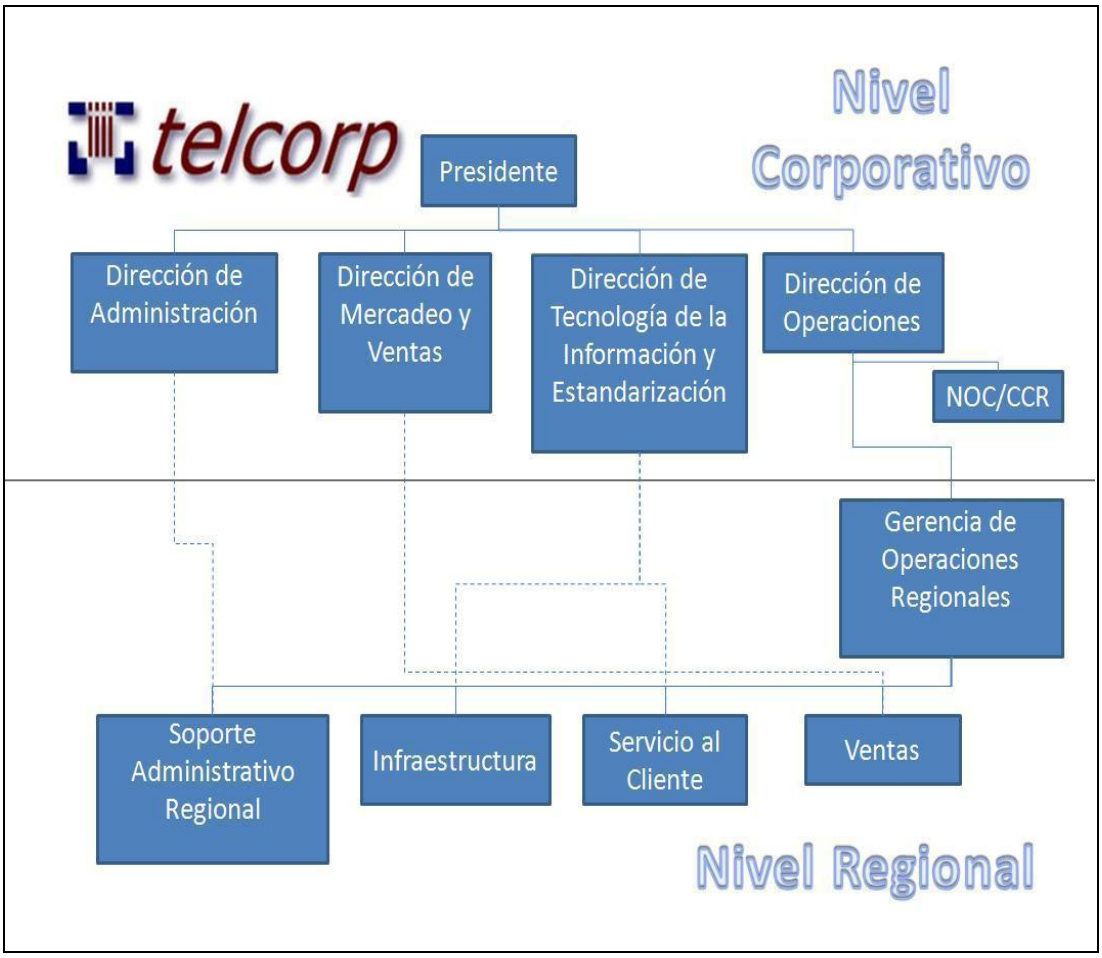


Figura N°27: Organigrama de Telcorp
Fuente: Telcorp (2008)

Las líneas continuas representan las dependencias en cuanto a dirección, mientras que las líneas punteadas representan las dependencias en cuanto a control. Típicamente el trabajo en la empresa se desarrolla en equipos pequeños integrados por personas líderes, preparadas profesionalmente, con capacidad de toma de decisión, resolución de problemas y de armonizar con el resto del equipo en un trabajo eficiente.

Ahora bien, con respecto a la infraestructura tecnológica de Telcorp lo primero que se hizo fue un inventario de todos los equipos que usa la IT (ver anexo N°8). La IT tiene un esquema jerárquico en el que el nodo principal funciona en el

distrito capital, actualmente posee nodos de coberturas en Valencia, Barquisimeto y el oriente del país. Cada nodo a su vez posee puntos de repetición que interconectan a nodos o a clientes directamente.

El nodo Valencia conjunto con el principal cubren toda la región central de Venezuela: Carabobo, Aragua, Distrito capital, Vargas y Miranda.

El nodo Barquisimeto: Cubre toda la región centroccidental: Lara, Yaracuy, Portuguesa y con recientes proyectos para Zulia, Falcón y Barinas.

El nodo Oriente, cubre toda la región Oriental: Anzoategui, Monagas, Nueva Esparta, Sucre y Bolivar. Todo este nodo se cubre con el apoyo en cuanto a soporte y monitoreo de otra empresa de telecomunicaciones de la región.

El esquema es jerárquico porque cada nodo posee a su vez sub- nodos que pueden poseer otros Sub-nodos o clientes directos. Esta particularidad de la red hace un poco más fácil la implementación de IPv6, ya que este protocolo está concebido para trabajar de forma jerárquica, por lo menos para el tema de los prefijos de sub-redes y asignación del plan de numeración. En la figura N°28 se muestra el Diagrama general de la red Telcorp a nivel nacional.

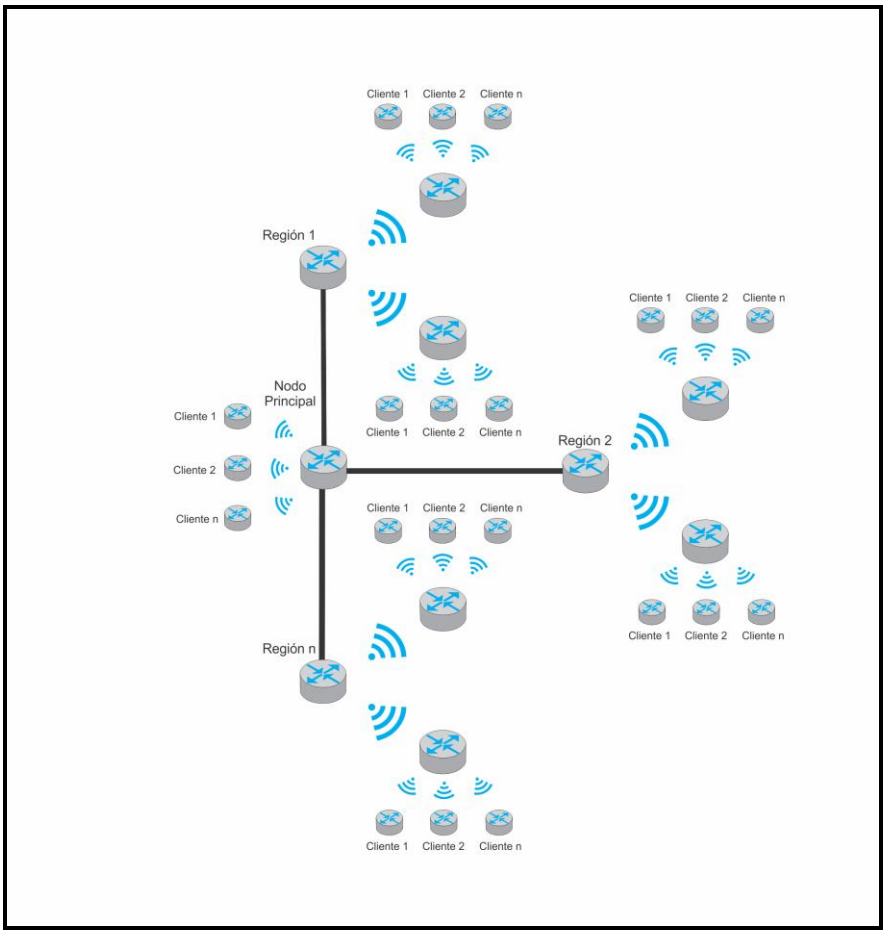


Figura N°28: Diagrama actual de la Red Telcorp
Fuente: Telcorp (2010)

El protocolo estándar en capa 2 (OSI) es Ethernet, los estándares Wimax y Wifi para la interconexión entre nodos y última milla (desde el último nodo hasta el cliente). La red Telcorp posee múltiples tecnologías en las que destacan las marcas Mikrotik, Motorola y Ubiquiti (marca de bajo costo con la funcionalidad de marcas prestigiosas).

El Protocolo de enrutamiento empleado en Telcorp, es el OSPF combinado con enrutamiento estático.

Usa NAT para el ofrecer el Internet comercial el cual es un servicio asimétrico y sin IP públicas. A diferencias de otros proveedores que atacan el mercado residencial, ésta empresa de telecomunicaciones es una empresa que ofrece

solo servicios a clientes corporativos (Pymes, Industrias, Comercio, Universidades, entre otros).

De esta forma, en la actualidad, posee una cartera de clientes significativa, los cuales se encuentran distribuidos entre los distintos servicios que ésta posee.

La empresa cuenta con un centro de operaciones de la Red en donde son atendidos todos los requerimientos de los clientes en cuanto a soporte, Ver figura N°29.

Figura N°29: NOC Telcorp
Fuente: El Autor

Por su parte, para el monitoreo se emplea una herramienta de software llamada DUDE que permite determinar el estado de los dispositivos en la Red. Ver figura N°30.

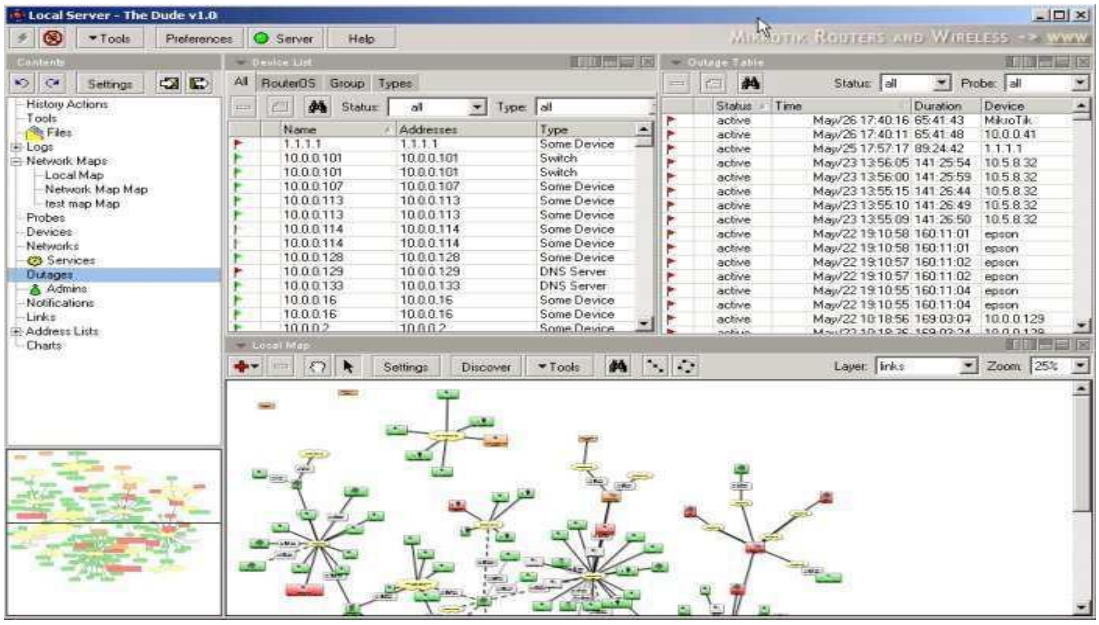


Figura N°30: Herramienta de monitoreo The Dude
Fuente: El Autor

Fase II. Evaluación de las alternativas de migración o metodologías existentes.

Luego de haber realizado el diagnostico, se hace necesario para este trabajo de investigación abarcar un punto de partida y es la selección de una alternativa de transición.

Así, el mayor problema para la introducción de IPv6 en Internet está en cómo realizar la transición de IPv4 a IPv6 de forma que no se interrumpa el servicio. Durante los últimos años IETF ha desarrollado múltiples métodos de transición y coexistencia entre IPv4 e IPv6.

Método de transición

El método de transición es un conjunto de mecanismos y de protocolos implementados en hosts y routers que en conjunto con esta guía se podrá llegar a una transición transparente.

Cuadro N°21.
Matriz de evaluación.

Parámetros	Túneles	Dual Stack (doble pila)	Traducción
Enlaces Inalámbricos de última milla funcionaran con IPv4	Permite la Interoperatividad pero la desencapsulación en origen y destino agrega un retardo a la transmisión.	Viable para que la Red inalámbrica opere en IPv4 y pueda monitorearse y los clientes IPv4 continúen Operando	No es recomendado.
Servicio de Red privada de datos	Se requiere disponibilidad de una red IPV4, mientras dure la transición; tal requerimiento se debe a que el servicio de Red privada de datos, no será migrado de forma automática sino posteriormente y los túneles no aplican para este tipo de soluciones.	Es viable, debido a que el servicio inicialmente se continuara prestando en IPv4, ya que el mismo no requiere de una Dirección IP pública para su funcionamiento.	No es necesario.
Monitoreo	Se debe realizar un Túnel con la PC de monitoreo para que puedan también monitorearse la red IPv6.	Permite monitoreo para dispositivos IPv4 e IPv6 respectivamente.	No se puede monitorear, debido a que la traducción enmascara a los dispositivos involucrados.

Capacidad de los enrutadores	Soportada	Soportada	Soportada.
Tiempo de ejecución Facilidad de implementación	Relativamente rápida, pero requiere de alguna configuraciones complejas, dependiendo los casos.	Relativamente rápida, menos compleja y más silenciosa en el caso de los clientes de Telcorp.	Relativamente rápida pero requiere de configuraciones complejas y una de las condiciones es que no existan NAT IPv4 creados en los enrutadores y en la IT de red del ISP Telcorp como se notó el diagnóstico se usa NAT

Fuente: El Autor

El mecanismo llamado Doble Pila o Dual Stack es la forma más directa para los nodos IPv6 permitan la compatibilidad con nodos IPv4. Se pueden configurar hoy en día estos nodos con ambas direcciones IP, tanto de la versión 6 como de la versión 4 estos son llamados nodos "IPv6/IPv4". Estos nodos tienen la habilidad de enviar y recibir paquetes IPv6 e IPv4, pudiendo así interoperar directamente con nodos IPv4 usando paquetes IPv4, y también operar con nodos IPv6 usando paquetes IPv6.

Además, en el caso particular de Telcorp, por poseer clientes operativos (información mostrada en la observación directa), DUAL STACK le permite la migración de la forma más silenciosa para los clientes IPv4 activos. Se requiere que exista una red IPv4 para el servicio de red privada de datos o interconexión de sucursales, el cual no requiere de direcciones IP públicas y para el monitoreo de los radio enlaces inalámbricos que interconectan los puntos de repetición de Telcorp. Adicional a esto la red actual tiene configurado NAT y en el caso de mecanismos de

traducción uno de los elementos necesarios es que no existan NAT IPv4 configurados.

Por las consideraciones anteriores, el mecanismo elegido para el caso Telcorp, es el DUALSTACK

Fase IV. Diseño de la Infraestructura tecnológica de red

Descripción de la propuesta

La propuesta consiste en el diseño de la Infraestructura tecnológica de red para la empresa Telcorp, formalmente Sistemas Telcorp, C.A. con el fin de resolver el problema existente en la prestación del servicio dedicado específicamente, la entrega de direcciones IP públicas en sus clientes corporativos.

Para el diseño de la propuesta se desarrollaron varias etapas las cuales consisten en lo siguiente:

- Creación de un cuadro de comprobación de compatibilidades tanto de hardware como de software para determinar los cambios que deben realizarse.
- Consideraciones para la capa 1 y 2 (OSI) también aplica para la capa de (acceso a Red) de la arquitectura TCP/IP.
- Consideraciones en la Capa de Internet (TCP/IP) o Capa de Red (OSI).
    - Obtención de bloques de direcciones IPv6.
    - Determinar si existe disponibilidad de IPv6 en los ISP primarios
    - Preparar un plan de Numeración
    - Simular un esquema mínimo por región con IPv6 y el protocolo de enrutamiento usado por Telcorp
- Consideraciones para Capas Superiores
- Creación del plan de migración por etapas (Diagrama de Gantt)

Todo esto con el fin de proporcionar el esquema por el cual se regirá la posterior implementación de este protocolo de red en el ISP venezolano, Telcorp.

Desarrollo de la propuesta

Creación de un cuadro de comprobación de compatibilidades tanto de Hardware como de software para determinar los cambios que deben realizarse.

El punto de partida de esta propuesta fue la realización de una tabla de compatibilidades de los distintos equipos usados en la Infraestructura tecnológica de red de Telcorp, información obtenida del inventario de equipos realizado en el levantamiento de información. Ver Cuadros N°24 y 25.

Cuadro N°24
Compatibilidad del hardware.

Descripción	Versión	Modelo	Compatibilidad
Equipo	Marca	Modelos	Compatibilidad
Enrutador	Mikrotik	RB750 y RB750 G	El sistema operativo de Mikrotik se llama Router OS el cual soporta protocolo de Internet versión 4 (IPv4), así como del protocolo de Internet versión 6 (IPv6)" Ver anexo N°10
Switch	Cisco	2900	Todos estos productos tanto en 5.7 Ghz como en 2.4 ghz operan en el modo de puente y WDS estos dispositivos soportan la transmisión transparente de IPv6. Mas detalles Ver anexos N°: 11.1,11.2, 11.3, 11.4,11.5 y 11.6 y 11.7
Equipo de RF	Ubiquiti	Nanostation5, Nanobridge M5, Nanostation loco 5, Nanostation M5, Bullet M5 Nanostation loco M5 Rocket M5	

Equipo de RF	Motorola	Canopy BH 5G y Canopy AP 5G Canopy SM 5G	Los equipos canopy soportan transporte de capa 2 de interrupción, con soporte para todos los protocolos comunes de Ethernet incluyendo IPV6, NetBIOS, DHCP, IPX, por lo que si es compatible. Ver anexo N°12
Antena	Ubiquiti	Nanostation2, Nanobridge M2, Nanostation loco 2, Nanostation M2, Bullet M2 y Nanostation loco M2	Todos estos productos tanto en 5.7 Ghz como en 2.4 ghz operan en el modo de puente y WDS estos dispositivos soportan la transmisión transparente de IPv6. Mas detalles en los anexos: - anexo N°12.1 - anexo N°13.1 - anexo N°13.2 - anexo N°13.3 - anexo N°13.4 - anexo N°13.5 - anexo N°13.6
Antena	Ubiquiti	Rocket M2	Sí. Ver anexo N°13.7
Antena Antena	Motorola Motorola	Canopy BH 2G Canopy AP 2G	Ver anexo N°14 Ver anexo N°14
Computadora Personal	VIT		Compatible, depende del sistema operativo Poseen interfaces físicas Ethernet
Portátiles	ACER	Aspire	Compatible, depende del sistema operativo Poseen interfaces físicas Ethernet
Portátiles VIT			Compatible, depende del sistema operativo Poseen interfaces físicas Ethernet

Fuente: El Autor

Cuadro N°25
Compatibilidad del software

Descripción	Compatibilidad
RouterOs , v5+	Sí. Ver anexo N°15
RouterOs , v4	Sí. Ver anexo N°15
Router OS 3.2.9	No hay que actualizarla a versión superior 3beta10. Ver anexo N°15
Sistema Operativo Windows XP	Sí. Ver anexo N°16
Windows Vista	Sí. Ver anexo N°17
Windows 7	Sí. Ver anexo N°18
Software de Monitoreo Dude	Aún No
Ubuntu	Sí. Ver anexo N°19
AirOs3 AirOs5	Solo modo transparente
Team Viewer	Sí. Ver anexo N°20
Cisco IOS	Sí. Ver anexo N°21

Fuente: El Autor

Consideraciones de Hardware y Software

La mayoría de los componentes tanto de software y hardware poseen disponibilidad para implementar IPv6, teniendo esto una gran ventaja para la empresa objeto de estudio. Sin embargo, hay algunas consideraciones a tomar en cuenta principalmente con el software de Monitoreo Dude, que actualmente no posee soporte para IPv6.

Inicialmente se usará el software Dude para continuar monitoreando los radio enlaces, los enrutadores funcionarán en modo Dual.

Sin embargo, se evaluó la adquisición de la herramienta de monitoreo WhatsUP Gold, que tiene prestancia tanto para IPv4 como para IPv6 y ya fue utilizada anteriormente en la empresa Telcorp, y se prevé adquirirla a mediano plazo

En la factibilidad técnica se encuentra las especificaciones técnicas de éste software y en la económica los costos asociados a esta.

Otro punto importante, es que la licencia de tres (3) enrutadores Mikrotik deben ser actualizadas, debido a que el año de actualización en estos equipos ya caduco. Los veintidós (22) enrutadores de troncales poseen ya la última actualización de la licencia y los otros veinte (20) aunque no poseen la última versión aun no superan en año y pueden actualizarse de forma rápida. A continuación se presenta gráficamente lo explicado en el párrafo. Ver figura N°31.

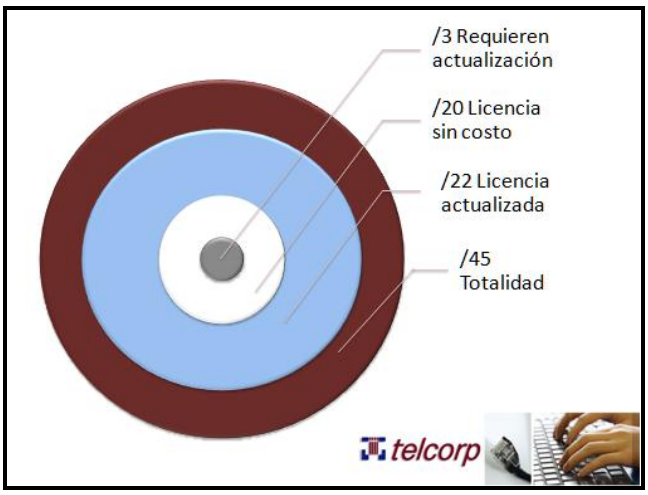


Figura N°31: Actualizaciones de RouterOS requeridas.
Fuente: El Autor

Luego de analizar de una forma general el Hardware y el software usado en la Infraestructura Tecnológica de red en el ISP Telcorp, se procedió a realizar las diversas recomendaciones por capas de la arquitectura TCP/IP.

Consideraciones para la capa 1 y 2 (OSI) también aplica para la capa de acceso a Red de la arquitectura TCP/IP.

La Infraestructura Tecnológica de red actual de Telcorp no debe hacer cambios significativos en la capa 1 y 2 OSI. Telcorp usa en su infraestructura los

estándares más comunes en el que prevalece Ethernet y el estándar para redes inalámbricas IEEE 802.11.

Los enlaces inalámbricos con tecnología Wi-Max, funcionan en modo Transparente para IPv6. En IPv4 a estos dispositivos se les asigna direcciones IP para monitorearlas y configurarlas tal y como se muestra en la figura N °32.

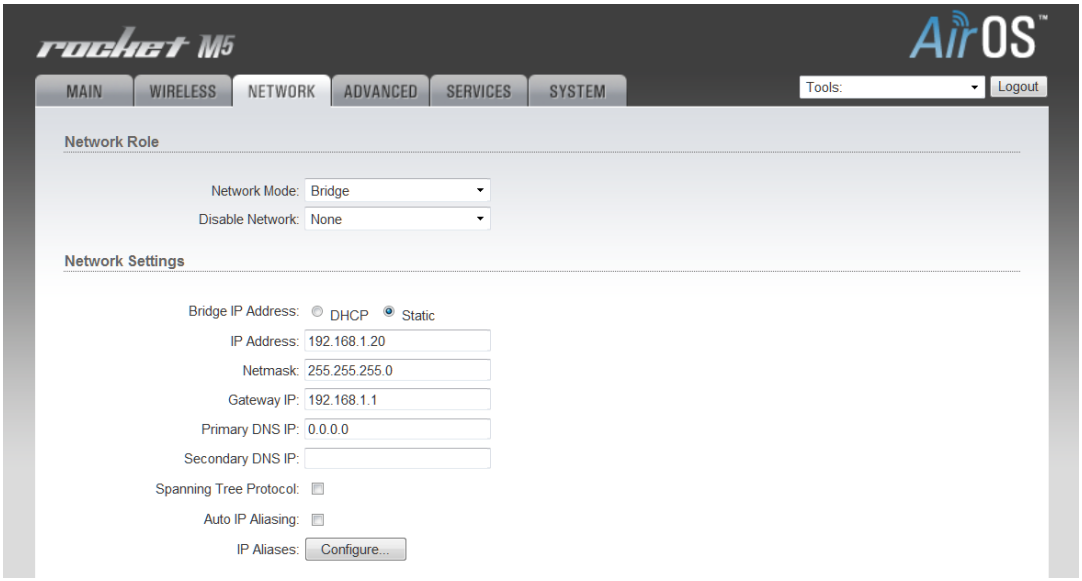


Figura N°32: Configuración de direcciones IPv4 en equipos RF
Fuente: El Autor

Estos equipos no se usan para enrutar paquetes sino que funcionan en la capa 2 OSI similar a un Switch en una LAN, es decir, cuando la interfaz LAN del equipo RF se conecta a una interfaz de un router es este el que se encarga de direccionar los paquetes de origen a destino. Estos equipos de RF usan un firmware (programa almacenado en un chip de memoria flash de un dispositivo de hardware cuya función es asegurar su correcto funcionamiento.) para que el administrador de la red pueda configurar los parámetros de calidad de la señal, alinear la antena, el ancho de banda que tendrá el radio enlace entre otros pero aún no posee prestancia para IPv6. Sin embargo, tiene la ventaja de funcionar en modo transparente, es decir enviar las tramas de origen a destino sin procesar la cabecera IP. Por lo que se esperara que el

fabricante actualice el firmware para soporte IPv6 durante la transición mundial a este estándar.

Cabe destacar que el único cambio que deben realizarse en las configuraciones de los radios enlaces es que deben estar configurados como modo inalámbrico Access-Point WDS (Sistema de distribución inalámbrico) o estación –WDS. Tal y como se muestra en las figuras N°33 y N°34

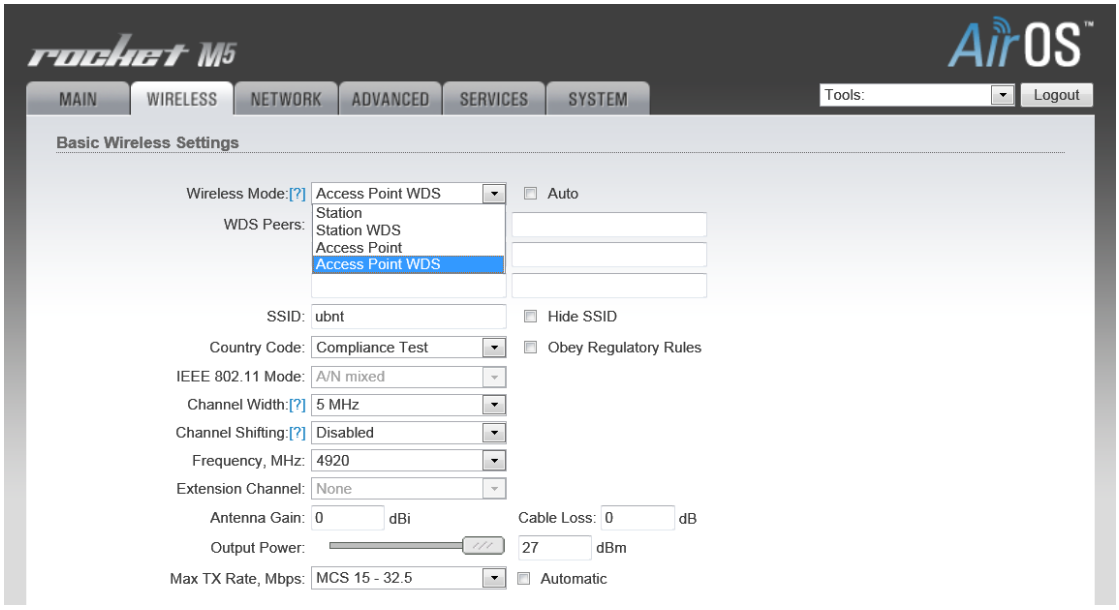


Figura N°33: Access Point WDS
Fuente: El Autor

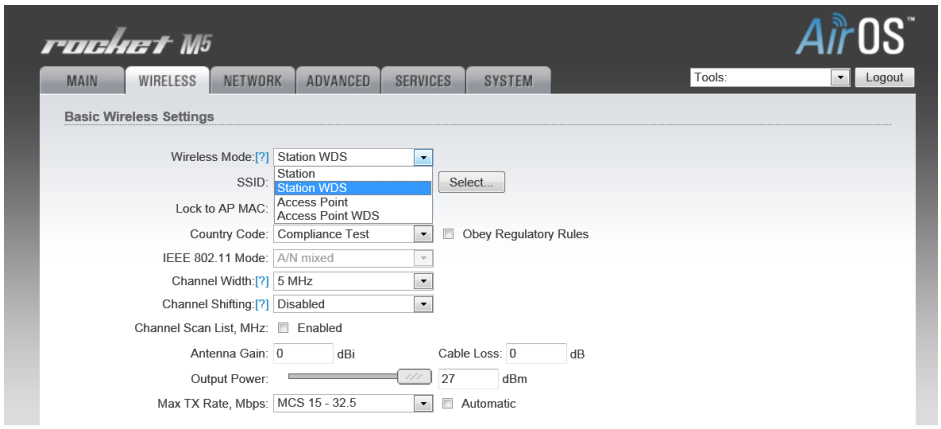


Figura N°34: Estación WDS
Fuente: El Autor

Consideraciones en la Capa de Internet (TCP/IP) o Capa de Red (OSI).

Los cambios más significativos a realizarse en la infraestructura tecnológica de red del ISP objeto de estudio son precisamente en esta capa, pues el esquema de identificación actual, las tablas de enrutamiento, las configuraciones de los enrutadores son aspectos a considerar para la transición.

Obtención de bloques de direcciones IPv6.

Uno de los objetivos de la propuesta es proporcionar la información necesaria a la empresa objeto de estudio para que pueda obtener un espacio de direcciones IPv6 públicas, es por ello que se creó en el anexo N°22 un manual para la obtención de direcciones IPv6. Si bien esta información es de conocimiento público, la propuesta presenta una alternativa para que Telcorp disponga de todas las herramientas a la mano cuando decida realizar la migración.

Determinar si existe disponibilidad de IPv6 en los ISP primarios

Partiendo del punto anterior y ya sabiendo las políticas de asignaciones de los organismos competentes, se procedió a determinar si los ISP principales de Telcorp disponían de una red IPv6.

El proveedor principal de Internet de Telcorp es una Importante empresa de telecomunicaciones que por políticas de confidencialidad no puede ser revelado para efectos de este trabajo de investigación.

Éste proveedor en el año 2008 migró al protocolo de Internet versión 6 y posee disponibilidad inmediata para entregar una Sub-Red inicialmente /48 a Telcorp y posteriormente puede ser el intermediario en LACNIC, para la obtención del /32 que le corresponde a Telcorp como ISP. Ver anexo N°22.

El ISP secundario, no posee implementado IPv6 y está en pleno proceso de transición. En este sentido, para ésta investigación el mecanismo elegido DUAL STACK es idóneo para operar con los dos ISP.

Por su parte, el proveedor principal, entrega una gran cantidad de ancho de banda en un punto único en la capital del país y Telcorp usa su Infraestructura para trasladar este Internet para sus nodos regionales y sus nodos locales en el distrito capital. Éste ancho de banda es entregado por una Interface Ethernet. Cabe destacar que el ISP principal posee personal altamente capacitado y ha apoyado al personal de Telcorp con conocimientos técnicos en este periodo de transición.

Preparar un plan de Numeración

El esquema planteado en la red Telcorp, es el siguiente:

Tal y como se ha mencionado en párrafos anteriores, a Telcorp por ser un ISP le corresponde directamente de LACNIC un prefijo /32. Con éste, la empresa cuenta con 65536 sub-redes /48 para distribuir en sus regiones o sucursales y clientes directamente.

Como aún no se cuenta con un prefijo asignado, se trabajó para efectos de éste plan de numeración con un prefijo /32 dado como ejemplo para el cálculo de direcciones IP. Es muy importante mencionar que este prefijo / 32 se divide a su vez en prefijos /48 (tal y como se nota en el cuadro N° 26 representan a las regiones o sucursales que posee Telcorp), en este sentido si no se obtiene este prefijo / 32 de igual forma el ISP primario puede otorgar /48 a cada región, al agotarse este esquema en una región solicita otro prefijo /48. Ver Cuadro N°26

Cuadro N°26.
Subredes /32.

	2001:1350:: /32	REGION
	Direcciones de Sub Redes	Region 1
1	2001:1350:0:0:0:0:0:0/48	Region 2
2	2001:1350:1:0:0:0:0:0/48	Region 3
3	2001:1350:2:0:0:0:0:0/48	Region 4
4	2001:1350:3:0:0:0:0:0/48	Region 5
5	2001:1350:4:0:0:0:0:0/48	Region 6
6	2001:1350:5:0:0:0:0:0/48	Region 7

7	2001:1350:6:0:0:0:0:0/48	Region 8
8	2001:1350:7:0:0:0:0:0/48	Region 9
9	2001:1350:8:0:0:0:0:0/48	Region 10
10	2001:1350:9:0:0:0:0:0/48	Region 11
11	2001:1350:a:0:0:0:0:0/48	Region 12
12	2001:1350:b:0:0:0:0:0/48	Region 13
13	**2001:1350:c:0:0:0:0:0/48**	Region 14
	.	Region …
	.	Region …
	.	Region…
65536	2001:1350:ffff:0:0:0:0:0/48	Region 65536

Fuente: El Autor

Partiendo de este punto y coherente con la asignación directa por parte del ISP primario para la región capital, lo cual es un /48 se trabajo una región en este caso la Numero 13 y se creo el estándar de numeración de la red Telcorp. Ver figura N°35:

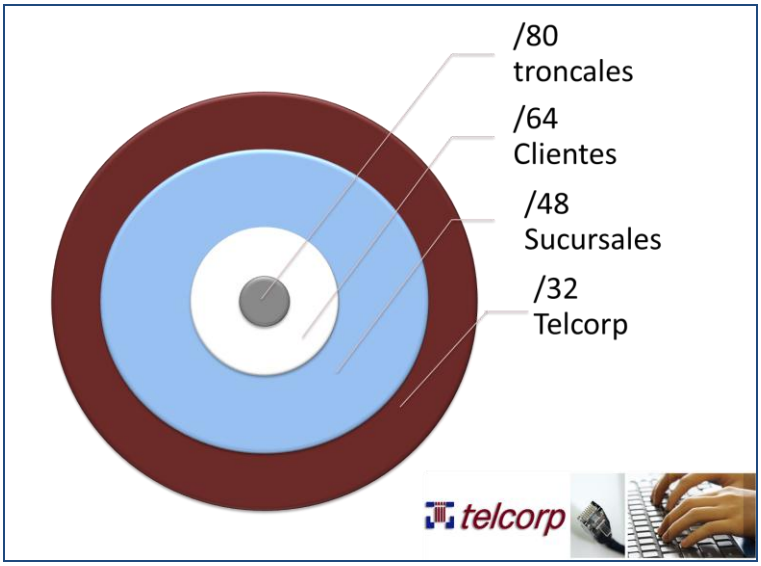


Figura N°35: Plan de numeración Telcorp.
Fuente: El Autor

En este esquema para Telcorp, el prefijo /48 se convierte a su vez en 65536 Sub-redes /64 de 256 hosts por sub-red, para que cada región posea oportunidad de crecimiento y expansión. De acabarse ésta asignación la sucursal obtendrá otro /48

para que pueda repartirlo de la misma manera. En este esquema, los clientes que actualmente perciben una (1) dirección IPv4 pública obtendrán 256 direcciones IPv6 al contratar el Internet dedicado de Telcorp. A continuación se presenta la organización de estas direcciones en cada región:

Del /48 obtenido del nodo principal de Telcorp, las regiones se asignarán de la siguiente manera:

El /48 fue convertido en 65536 sub-redes /64

Las primeras 80 Sub- redes /64 para dividirlas en /80 para uso de troncales y loopback para infraestructura Telcorp.

Cada punto de repetición de Telcorp obtendrá un bloque de 200 sub –redes /64, se consideró este número debido a que por la tecnología de última milla de Telcorp (inalámbrica) los nodos tienen una capacidad máxima y esta viene dada por este numero 200. Cada punto de repetición puede tener un máximo de 200 Clientes conectados a él y si la capacidad se supera debe ó encontrarse otro punto o colocar otros enlaces en el mismo punto considerándolo como otro nodo.

A continuación se presenta la tabla que muestra las sub redes para troncales y las sub redes de 20 nodos que es actual número de puntos que posee la red Telcorp. Partiendo de la región N° 14 seleccionada en la tabla anterior, Ver Cuadro N°27

Cuadro N°27.
Rangos de direcciones.

Reservado Telcorp	2001:1350:c:0:0:0:0:0/64	
Direcciones para troncales	2001:1350:c:1:0:0:0:0/64	2001:1350:c:13:0:0:0:0/64
Reservado Telcorp	2001:1350:c:14:0:0:0:0/64	2001:1350:c:1d:0:0:0:0/64
Direcciones para antenas	2001:1350:c:1e:0:0:0:0/64	2001:1350:c:31:0:0:0:0/64
Reservado Telcorp	2001:1350:c:32:0:0:0:0/64	2001:1350:c:3b:0:0:0:0/64
Direcciones de loopback	2001:1350:c:3c:0:0:0:0/64	2001:1350:c:45:0:0:0:0/64
Reservado	2001:1350:c:46:0:0:0:0/64	2001:1350:c:4f:0:0:0:0/64

Telcorp				
Nodo 1	2001:1350:c:50:0:0:0:0/64	2001:1350:c:117:0:0:0:0/64		
Nodo 2	2001:1350:c:118:0:0:0:0/64	2001:1350:c:1df:0:0:0:0/64		
Nodo 3	2001:1350:c:1e0:0:0:0:0/64	2001:1350:c:2a7:0:0:0:0/64		
.	.	.		
.	.	.		
.	.	.		
Nodo…..	2001:1350:c:fed3:0:0:0:0/64	2001:1350:c:ffff:0:0:0:0/64		
Direcciones de loopback		Router ID	Process	Área
Loopback nodo 1	2001:1350:c:3c:0:0:0:9/64	10.10.10.10	400	1
Loopback nodo 2	2001:1350:c:3c:0:0:0:6/64	10.10.5.5	400	1
Loopback nodo 3	2001:1350:c:3c:0:0:0:3/64	10.10.2.2	400	1

Fuente: El Autor

Luego la asignación para troncales quedo de la siguiente manera. Ver Cuadro N°28.

Cuadro N°28.
Asignación de direcciones para troncales.

2001:1350:c:1:0:0:0:0 /64	DIRECCION IP INTERFAZ 1 ROUTER X	DIRECCION IP INTERFAZ 1 ROUTER Y	ASIGNADO A:
2001:1350:c:1:0:0:0:0/80	2001:1350:c:1:0:0:0:1/80	2001:1350:c:1:0:0:0:2/80	Enlace A
2001:1350:c:1:1:0:0:0/80	2001:1350:c:1:1:0:0:1/80	2001:1350:c:1:1:0:0:2/80	Enlace B
2001:1350:c:1:2:0:0:0/80	2001:1350:c:1:2:0:0:1/80	2001:1350:c:1:2:0:0:2/80	Enlace C
2001:1350:c:1:3:0:0:0/80	2001:1350:c:1:3:0:0:1/80	2001:1350:c:1:3:0:0:2/80	Enlace D
2001:1350:c:1:4:0:0:0/80	2001:1350:c:1:4:0:0:1/80	2001:1350:c:1:4:0:0:2/80	Enlace E
2001:1350:c:1:5:0:0:0/80	2001:1350:c:1:5:0:0:1/80	2001:1350:c:1:5:0:0:2/80	Enlace F

2001:1350:c:1:6:0:0:0/80	2001:1350:c:1:6:0:0:1/80	2001:1350:c:1:6:0:0:2/80	Enlace G
2001:1350:c:1:7:0:0:0/80	2001:1350:c:1:7:0:0:0/80	2001:1350:c:1:7:0:0:0/80	Enlace H
2001:1350:c:1:8:0:0:0/80	2001:1350:c:1:8:0:0:0/80	2001:1350:c:1:8:0:0:0/80	Enlace I
2001:1350:c:1:9:0:0:0/80	2001:1350:c:1:9:0:0:0/80	2001:1350:c:1:9:0:0:0/80	Enlace J
2001:1350:c:1:a:0:0:0/80	2001:1350:c:1:a:0:0:0/80	2001:1350:c:1:a:0:0:0/80	Enlace K
2001:1350:c:1:b:0:0:0/80	2001:1350:c:1:b:0:0:0/80	2001:1350:c:1:b:0:0:0/80	Enlace L
2001:1350:c:1:c:0:0:0/80			.
2001:1350:c:1:d:0:0:0/80			.
2001:1350:c:1:e:0:0:0/80			.
2001:1350:c:1:f:0:0:0/80			.
2001:1350:c:1:10:0:0:0/80			.
2001:1350:c:1:11:0:0:0/80			.
2001:1350:c:1:12:0:0:0/80			.
2001:1350:c:1:13:0:0:0/80			.
2001:1350:c:1:14:0:0:0/80			.
2001:1350:c:1:15:0:0:0/80			.
2001:1350:c:1:16:0:0:0/80			.
2001:1350:c:1:17:0:0:0/80			.
2001:1350:c:1:18:0:0:0/80			.
2001:1350:c:1:19:0:0:0/80			.
2001:1350:c:1:1a:0:0:0/80			.
2001:1350:c:1:1b:0:0:0/80			.
2001:1350:c:1:1c:0:0:0/80			.

2001:1350:c:1:1d:0:0:0/80			.

Fuente: El Autor

Simulación de un esquema mínimo por región.

Con el fin de probar el esquema propuesto se simuló una configuración parcial en el software Packet Tracer de Cisco. Éste esquema mínimo, consiste en tres nodos mallados funcionando con el protocolo de enrutamiento dinámico OSPF para disponer de rutas redundantes o de respaldos.

Esta simulación se realiza con equipos marca Cisco y los enrutadores de Telcorp son marca Mikrotik, sin embargo el esquema y la esencia de las configuraciones es la misma. Ver anexo N°23. Manual de configuraciones IPv6 en router Mikrotik.

La figura N°36, muestra el esquema simulado.

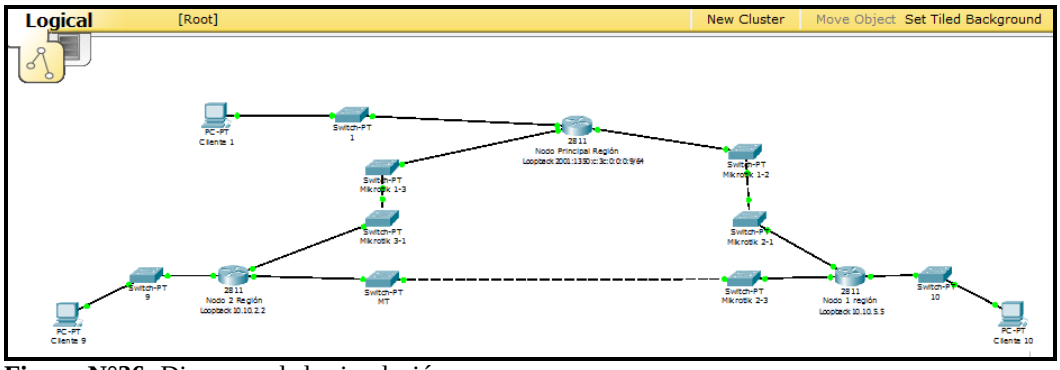


Figura N°36: Diagrama de la simulación
Fuente: El Autor

Se configuró en Packet Tracer el router llamado “Nodo Principal” con la dirección IPv6 correspondiente. El cuadro N°29 muestra las configuraciones que están establecidas en los equipos.

Cuadro N°29
Configuración de los equipos.

Sub- Red	Dir. IP router Nodo Principal	Dir. IP router Nodo 1	Dir. IP router Nodo 2			
2001:1350:c:1:0:0:0:0/80	2001:1350:c:1:0:0:0:1/80	2001:1350:c:1:0:0:0:2/80	Enlace A Nodo Principal - Nodo2			
2001:1350:c:1:2:0:0:0/80	2001:1350:c:1:2:0:0:1/80	2001:1350:c:1:2:0:0:2/80	Enlace C Nodo 2 - Nodo 1			
2001:1350:c:1:4:0:0:0/80	2001:1350:c:1:4:0:0:1/80	2001:1350:c:1:4:0:0:2/80	Enlace E Nodo Principal -Nodo 1			
		Router ID	Process	Área		
Loopback Nodo principal	2001:1350:c:3c:0:0:0:9/64	10.10.10.10	400	1		
Loopback Nodo 1	2001:1350:c:3c:0:0:0:6/64	10.10.5.5	400	1		
Loopback Nodo 2	2001:1350:c:3c:0:0:0:3/64	10.10.2.2	400	1		
		Interfaz Router Telcorp	Equipos Cliente	Interfaz Router Cliente	Cantidades de direcciones Clientes	Cliente N°
81	2001:1350:c:50:0:0:0:0/64	2001:1350:c:50:0:0:0:1/64	2001:1350:c:50:0:0:0:2/64 - 2001:1350:c:50:f:f:f:ffe /64	2001:1350:c:50:f:f:f:ffff/64	251	Cliente 1
282	2001:1350:c:119:0:0:0:0/64	2001:1350:c:119:0:0:0:1/64	2001:1350:c:119:0:0:0:2/64 - 2001:1350:c:119:f:f:f:fffe/64	2001:1350:c:119:f:f:f:ffff/64	251	Cliente 9
482	2001:1350:c:1e1:0:0:0:0/64	2001:1350:c:1e1:0:0:0:1/64	2001:1350:c:1e1:0:0:0:2/64 - 2001:1350:c:1e1:f:f:f:fffe/64	2001:1350:c:1e1:f:f:f:ffff/64	251	Cliente 10

Fuente: El Autor

Luego, se configuró el protocolo de enrutamiento dinámico OSPF en los tres routers (en IPv6 este protocolo se configura directamente en las interfaces haciendo del conocimiento de los vecinos las redes que comprende la topología).

Para determinar que el protocolo de enrutamiento dinámico funciona de forma correcta se realizó una prueba de conectividad y traza de la ruta. Ver figura N°37.

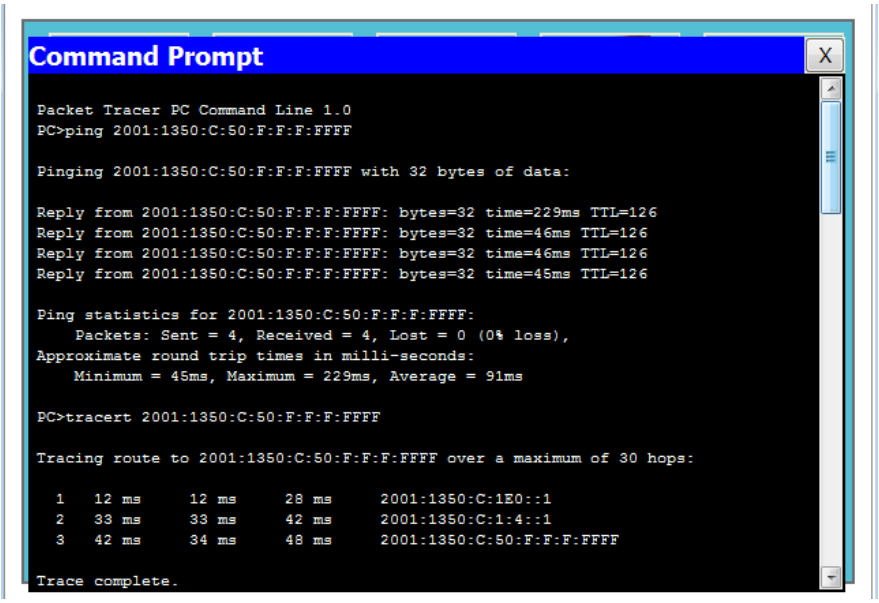


Figura N°37: Prueba de conectividad y traza de ruta
Fuente: El Autor

Otro elemento importante de probar era que OSPF al igual que en IPv4 permitiera la redundancia de las redes. En este sentido, se simuló una caída de un enlace entre el nodo 1 y el nodo principal. Ver figura N°38.

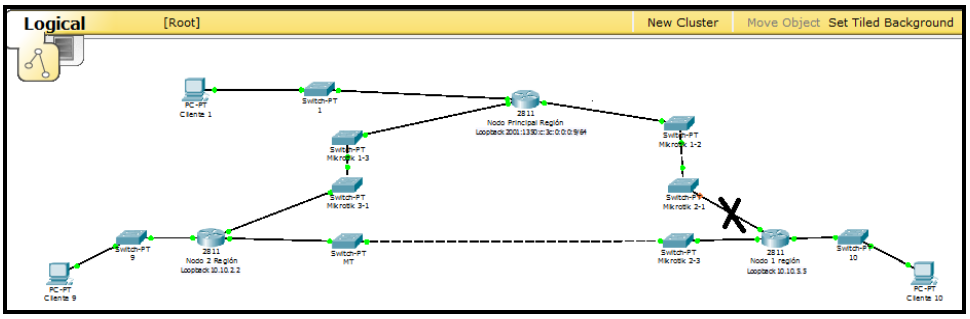


Figura N°38: Simulación de caída de enlace entre nodos.
Fuente: El Autor

Para probar la redundancia se realizó el mismo tracert desde el host 10 al host 1. En la figura se muestran las dos trazas. Ver figura N°39.

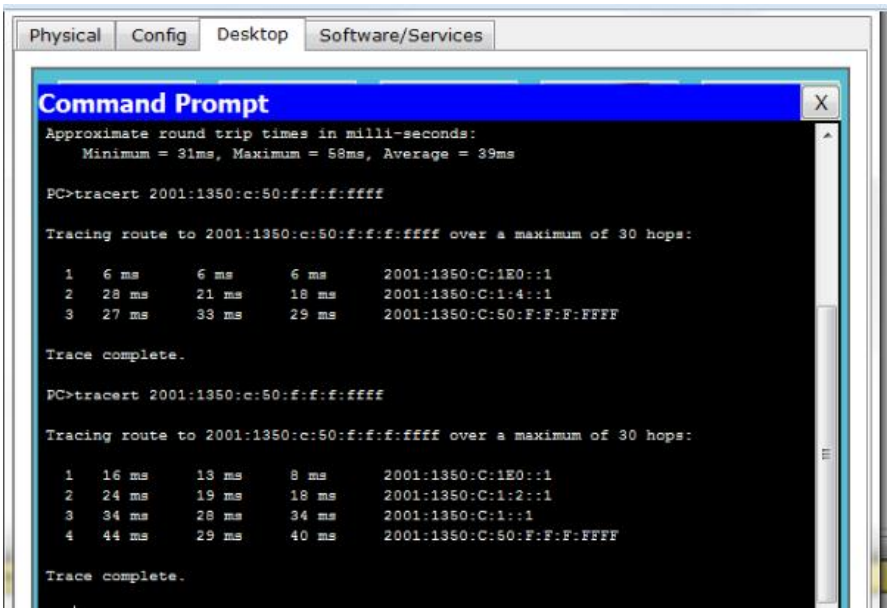


Figura N°39: Traza de ruta para simulación de redundancia con IPv6.
Fuente: El Autor

De esta forma, existe la viabilidad de configurar los principales protocolos usados en la red Telcorp.

Consideraciones para Capas Superiores

Este estudio contempla las consideraciones tanto del nivel transporte (comunicación entre procesos) como del nivel aplicación, abordando casos concretos de algunos protocolos más comunes establecidos en la arquitectura TCP/IP.

En el caso específico de DNS el mecanismo de transición elegido para este diseño resuelve las peticiones DNS en las aplicaciones como tal. Ver figura N°40

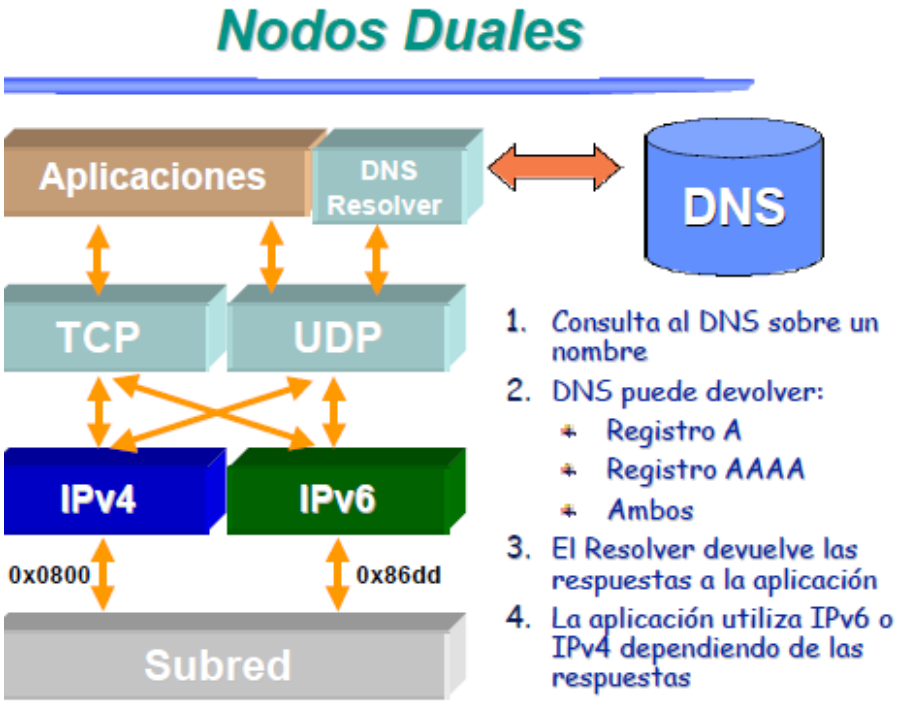


Figura N°40: Funcionamiento de la doble pila y su implicación en las capas superiores.
Fuente: palet (2009)

DNS es un punto que los administradores deben de considerar antes de configurar hosts IPv6 o con dual-stack.

Los DNS Servers de 32 bits no pueden manejar la resolución de nombres para las direcciones de 128 bits que maneja IPv6. Para resolver este problema los diseñadores de IETF han definido un estándar de DNS para IPv6 (RFC 1886, DNS Extensions to support IP version 6). Esta especificación crea nuevos registros tipo "AAAA", los cuales harán el mapeo de los nombres de dominio a las direcciones IPv6.

Una vez que un DNS capaz de resolver direcciones IPv6 sea configurado, los hosts dual-stack podrán interactuar intercambiando información con nodos IPv6. Si un host dual-stack hace un requerimiento a un DNS y recibe como respuesta una

dirección de 32 bits, se utilizará IPv4. Si se recibe una dirección de 128 bits, se utilizará IPv6.

Algunas acciones a tomar:

- En sitios donde el DNS no se ha migrado a IPv6, los hosts deberán resolver el mapeo de direcciones a nombre manualmente a través de tablas locales configuradas manualmente.
- Las aplicaciones que no accesen directamente al stack de la red, no tendrán que ser modificados para correr en el ambiente de dual-stack.
- Las aplicaciones de red que interactúan directamente con IP y sus componentes relacionados requerirán de migración si van a utilizar el protocolo IPv6, por ejemplo, las aplicaciones que accesan el DNS, deberán de ser mejoradas con la capacidad de requerir los nuevos registros de 128 bits.

Es importante mencionar que, la Infraestructura de Telcorp opera comúnmente en las capas 1, 2 y 3 de la arquitectura TCP/IP. A pesar de que como ISP no le corresponde directamente las Aplicaciones de usuarios, ni los servidores de Clientes. En esta investigación se considero realizar un manual para clientes con los detalles de las configuraciones finales de los servicios más comunes. En el anexo N°24 se muestra el manual explicativos de servicios (capas superiores para los clientes prospectos IPv6)

Plan de Migración

Todas estas consideraciones permitieron Crear el plan de migración por etapas (Diagrama de Gantt) para el ISP Telcorp. El plan se ejecutará desde tres (3) perspectivas: las consideraciones iniciales, la parte de implementación como tal y el área de ventas. Es de hacer notar que el plan considera todos los aspectos que se evaluaron en este trabajo de investigación. Sin embargo, este plan puede ser mejorado y cambiado por Telcorp durante su desarrollo.

El plan es a cinco (5 años) y por temas de representación el plan se encuentra en las siguientes páginas de forma consecutiva comenzando desde el año 2010 hasta el año 2015. Ver figuras N°41, N°42, N°43, N°44, N°45 y N°46.

A continuación se presenta el Plan de Migración Propuesto para Telcorp:

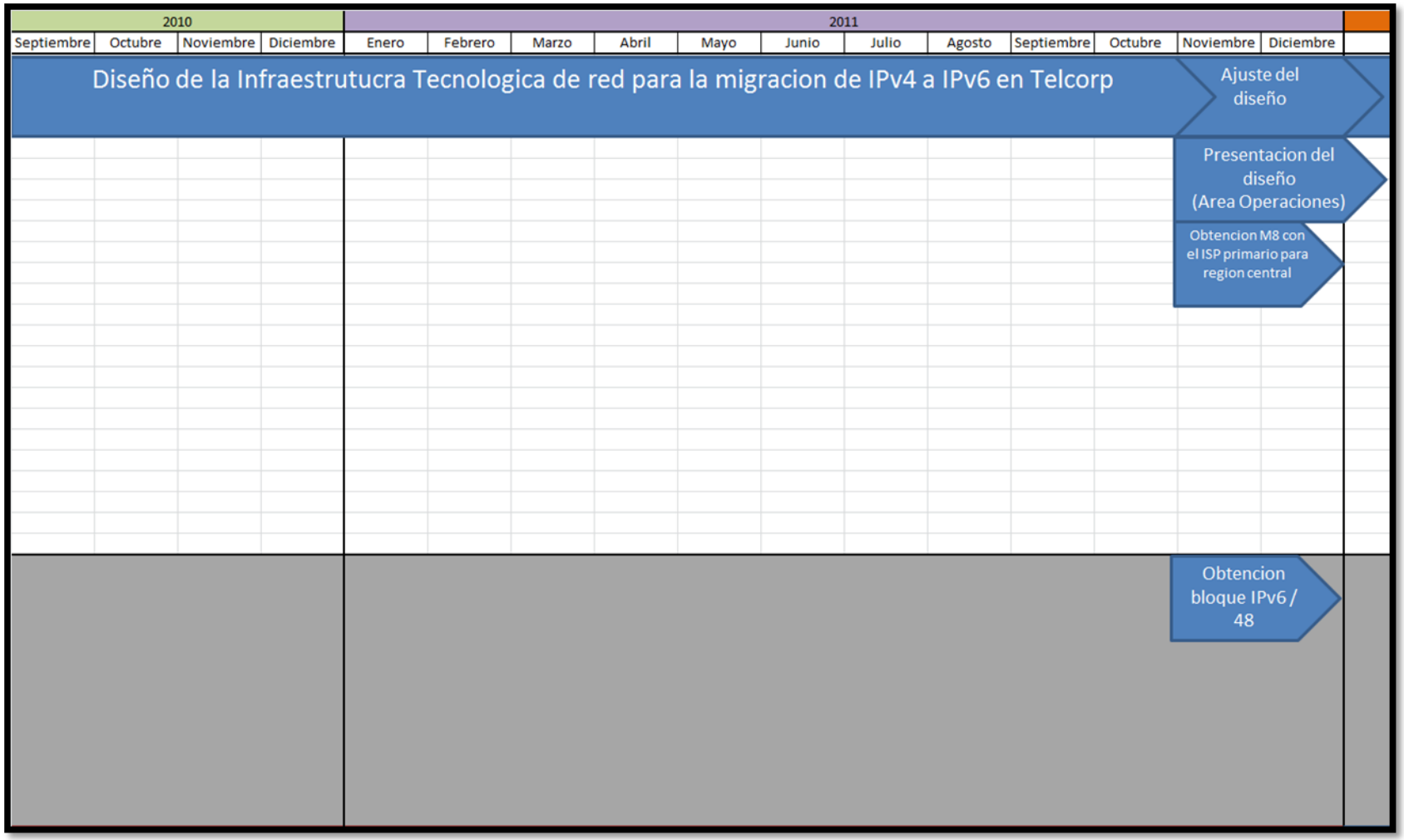


Figura N°41: Plan de migración, parte 1
Fuente: El Autor

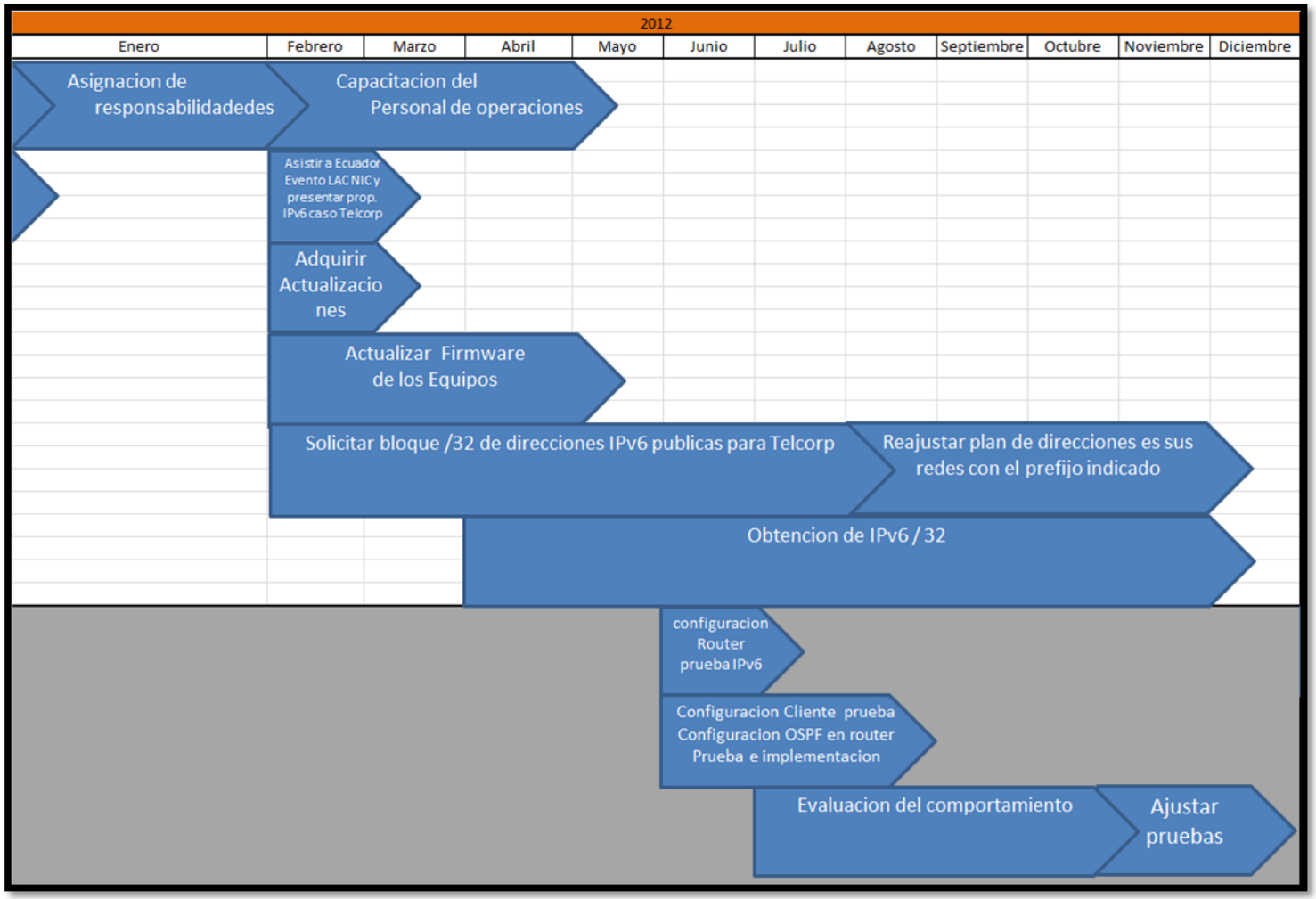


Figura N°42: Plan de migración, parte 2
Fuente: El Autor

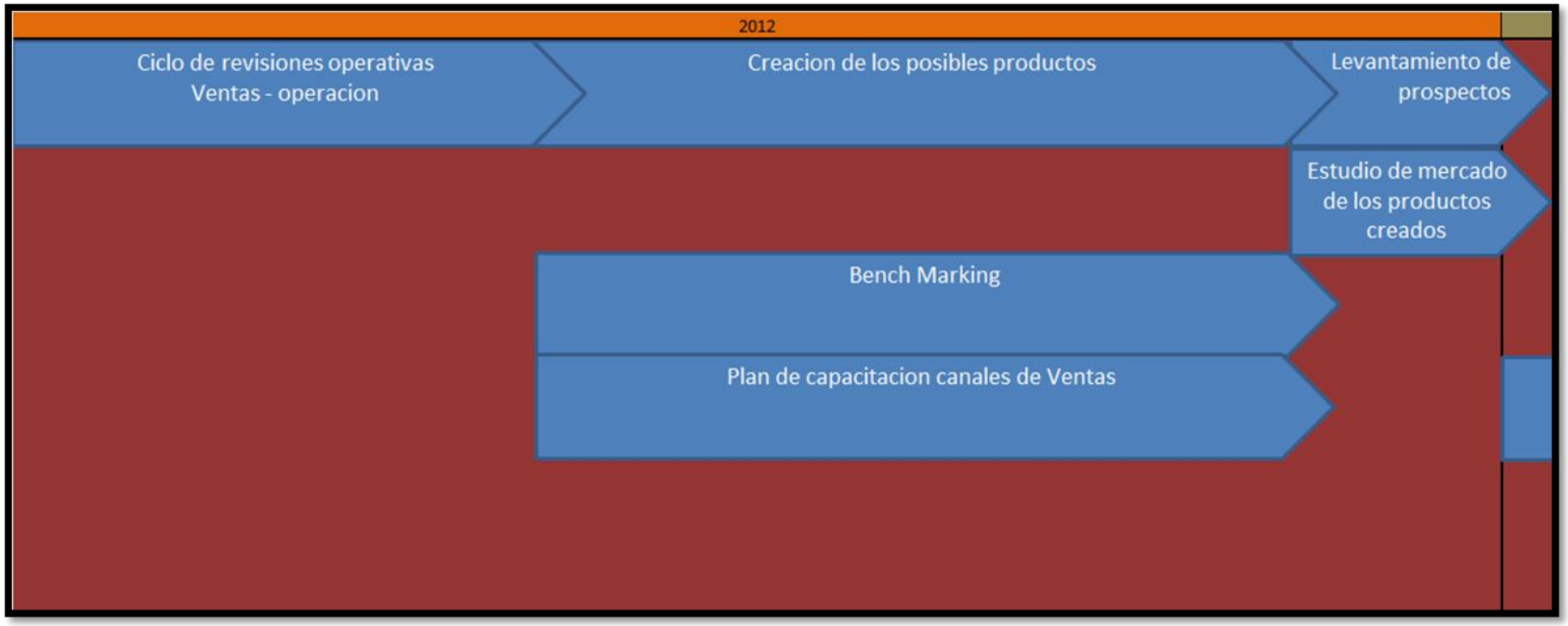


Figura N°43: Plan de migración, parte 3
Fuente: El Autor

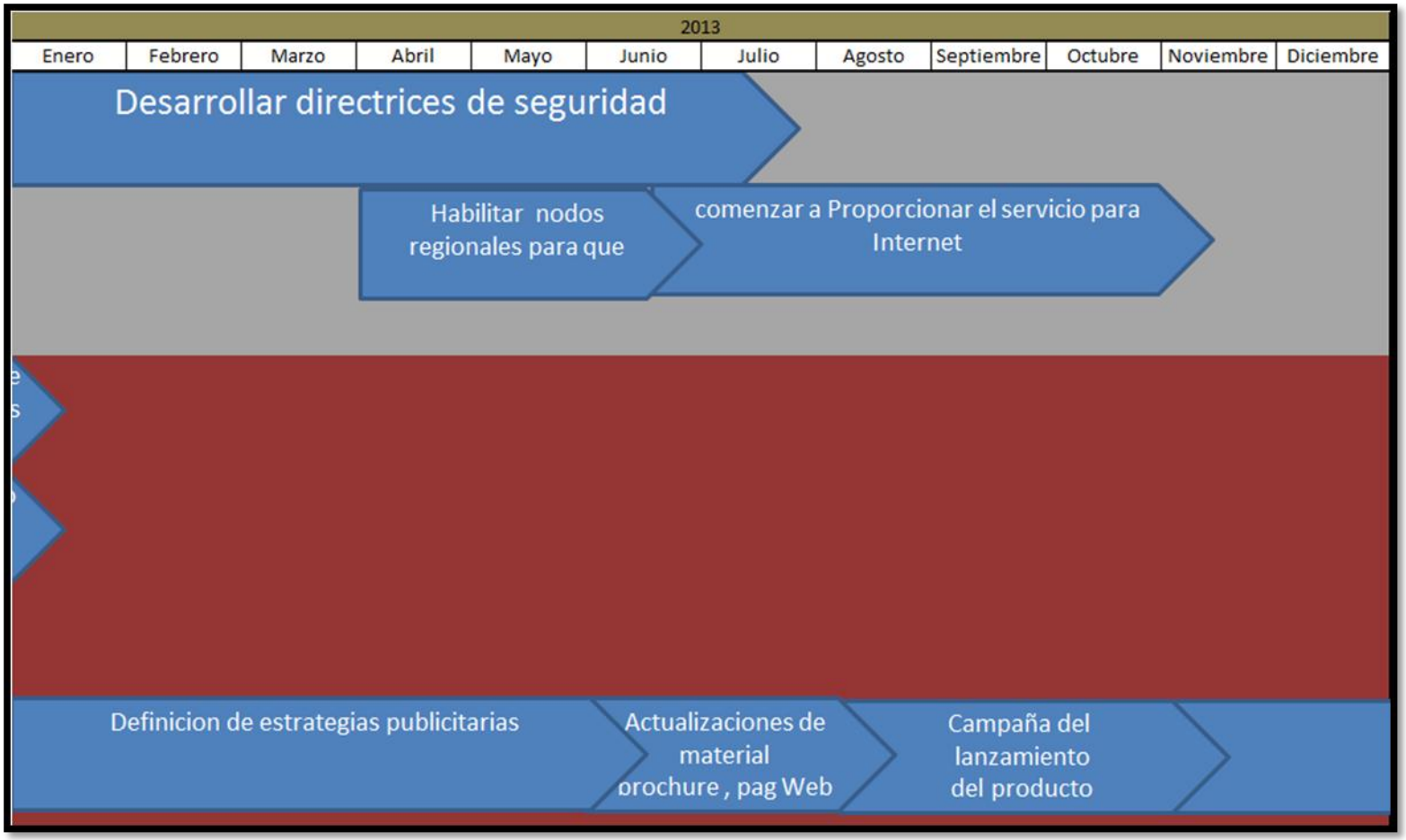


Figura N°44: Plan de migración, parte 4
Fuente: El Autor

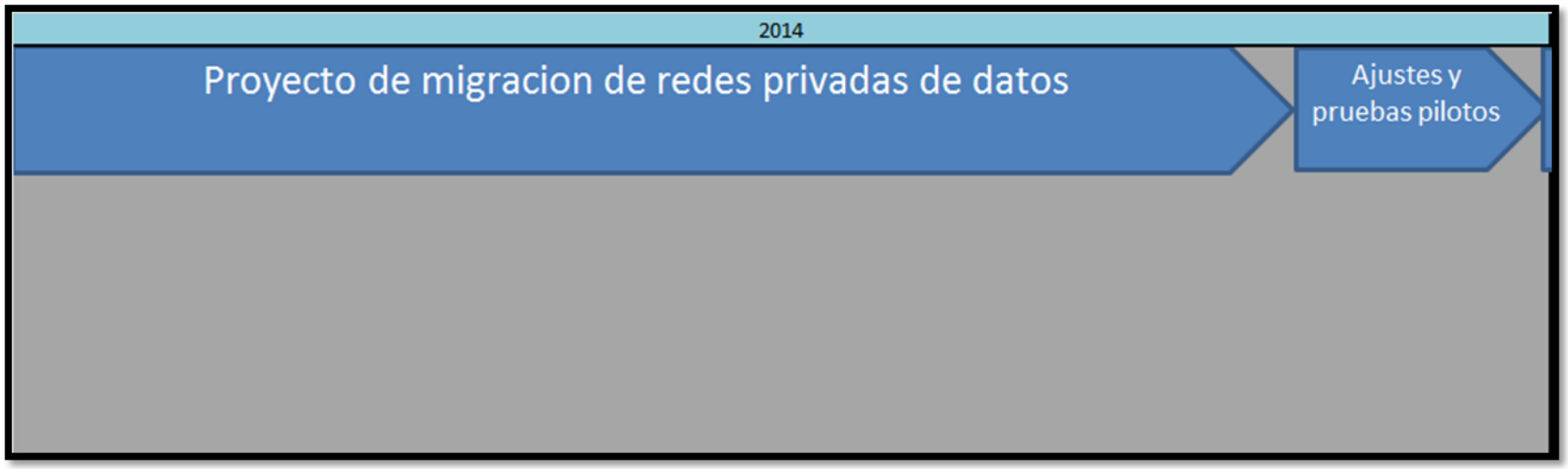


Figura N°45: Plan de migración, parte 5
Fuente: El Autor

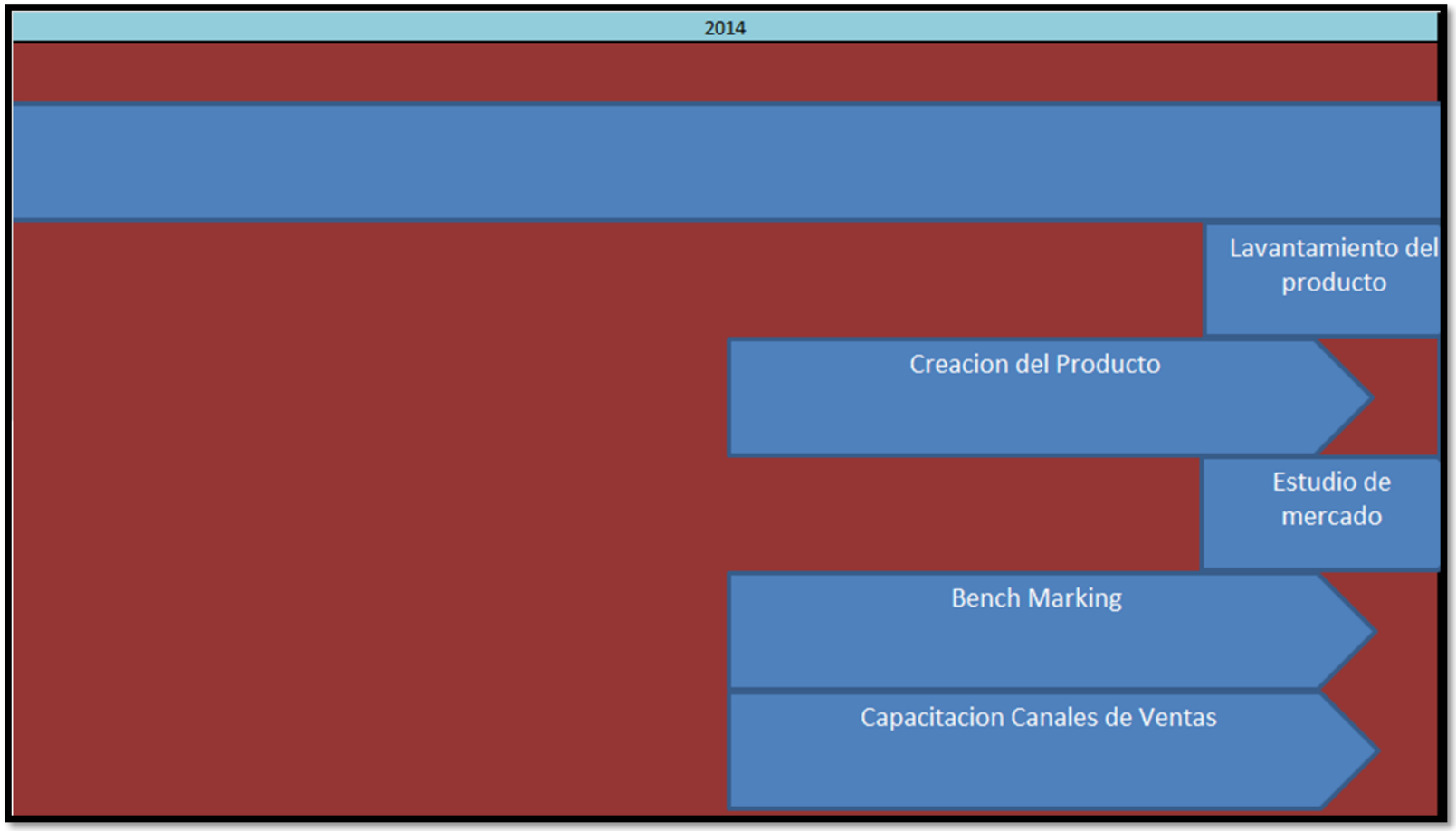


Figura N°46: Plan de migración, parte 6
Fuente: El Autor

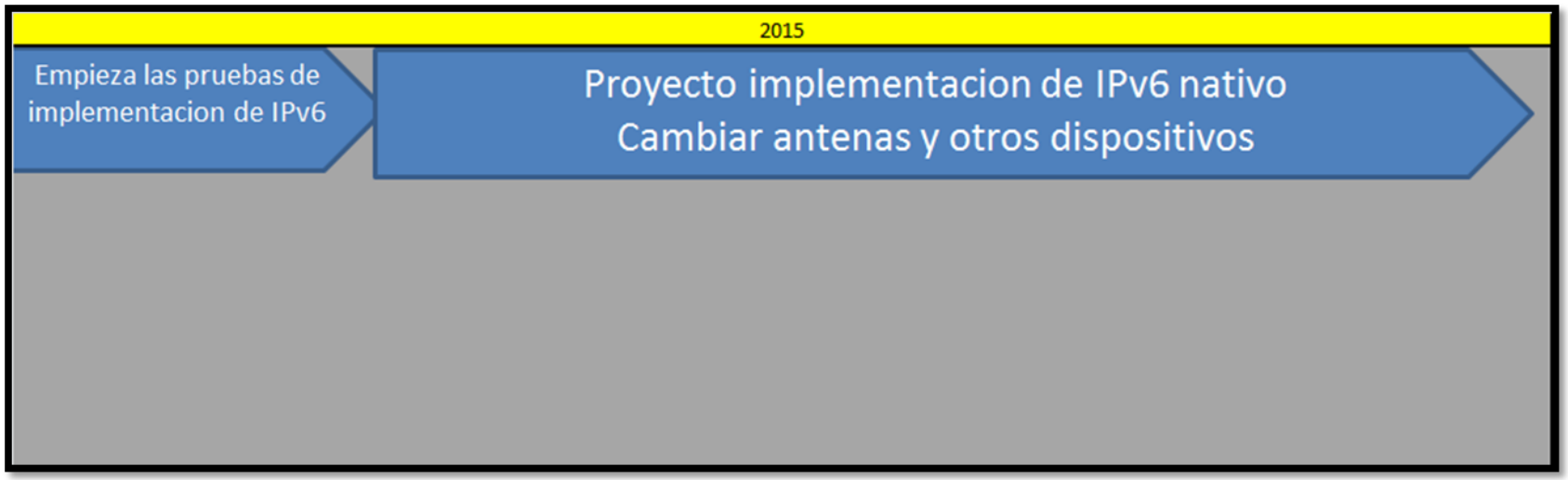


Figura N°47: Plan de migración, parte 7
Fuente: El Autor

Figura N°48: Plan de migración, parte 8
Fuente: El Autor

Fase III. Estudio de Factibilidad

Uno de los objetivos de esta investigación es determinar la factibilidad técnica, operativa y económica del diseño de la nueva Infraestructura tecnológica de red del ISP Telcorp con el fin de migrar de IPv4 a IPv6 en el ISP venezolano Telcorp.

Según Luna (1.999) "la factibilidad es el grado en que lograr algo es posible o las posibilidades que tiene de lograrse".

En esta fase acota Hernández, (ob.cit) "… es donde se establecen los criterios que permiten asegurar el uso óptimo de los recursos empleados así como los efectos del proyecto en el área o sector al que se destina".

Factibilidad Técnica

La viabilidad técnica de esta propuesta está garantizada, ya que:

Los requerimientos técnicos planteados en la propuesta son de fácil adquisición y existe disponibilidad de los equipos para la solución planteada. Este proyecto se adapta a realizar modificaciones para así ajustar el sistema a cualquier necesidad que surja en el tiempo.

Las especificaciones técnicas de los equipos disponibles, se corresponden en su totalidad con las necesarias para el óptimo funcionamiento de la solución planteada.

A continuación se presenta el cuadro de factibilidad técnica:

Cuadro N°22.
Factibilidad Técnica. Actualización de Software.

Ítem	Nombre	Descripción	Cantidad
1	Actualización de Licencia de Router OS	RouterOS soporta muchas aplicaciones utilizadas por los proveedores de servicios de Internet, por ejemplo, OSPF ,	**3**

		BGP , Multiprotocol Label Switching (VPLS / MPLS). El producto es compatible con Mikrotik RouterOS soporta protocolo de Internet versión 4 (IPv4), así como del protocolo de Internet versión 6 (IPv6).	
2	Software de Monitoreo Watsup Gold	Ver anexo N° 9	**1**

Fuente: El Autor

Finalmente, por lo mencionado en párrafos anteriores la propuesta es técnicamente factible.

Factibilidad Económica

Los costos asociados a la implementación de las políticas fueron entregados a la gerencia de administración y a la Dirección de operaciones para que evaluaran la disponibilidad presupuestaria de la misma quedando como resultado se obtuvo, que por ser la propuesta una herramienta que garantiza la sustentabilidad del negocio y algo estrictamente necesario a corto, mediano o a largo plazo es considerado vital para la continuidad del negocio se implementará la migración del protocolo IPv4 a IPv6 en Telcorp, y que los costos asociados a este cambio serán asumidos por la empresa y es viable desde el punto de vista económico considerando la relación costo beneficio que se obtendrá al realizarse. Razón por la cual el proyecto es factible desde el punto de vista económico.

La tabla muestra los aspectos económicos asociados a la propuesta.

Cuadro N°23.
Factibilidad Económica.

Ítem	Nombre	Descripción	Cantidad	Precio (Bs)
1	Actualización de Licencia de Router OS	Descrita en la factibilidad técnica	**3**	3600
2	Software de Monitoreo Watsup Gold		**1**	114637,5
3	Capacitación del personal de Operaciones	Capacitación por parte de Alejandro Acosta BT latam Venezuela. Modulo: 1. Direccionamiento IPV6. 2. Mecanismos de Transmisión. 3. Enrutamiento.	**7**	45000
Total				163237,5

Fuente: El Autor

Factibilidad Operativa

Para la propuesta de diseño de infraestructura tecnológica de red para la migración de IPv4 a IPv6 en el ISP venezolano Telcorp, la factibilidad operativa está garantizada, ya que:

Existe muy buena disposición, por parte de la empresa Telcorp, desde los niveles más altos hasta los más bajos, conscientes de la necesidad del cambio de protocolo IP.

La empresa Telcorp, cuenta con personal altamente capacitado en su departamento de operaciones, de igual manera cuenta con el apoyo del personal de la empresa proveedora de servicios ISP primario. Sin embargo, es necesaria la capacitación del personal para el cambio de esquema y adopción de IPv6.

También, la propuesta no considera un cambio radical y el mecanismo de transición elegido DUAL STACK, permite que el IPv4 no se descarte del todo y la red siga operando bajo los esquemas planteados, por ende facilita su operatividad.

De igual manera existe suficiente tiempo en el plan de migración para que todo el personal operativo trabaje, investigue y opere la red IPv6.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Esta investigación proporcionó al Proveedor de Servicio de Internet Telcorp, un plan de migración progresiva permitiéndole incorporar la nueva versión del protocolo de Internet IPV6 en su infraestructura tecnológica de red.

También, la investigación arrojó conclusiones en cuanto a las implementaciones en clientes, desarrollándose un manual para facilitarles a los usuarios la implementación y uso de direcciones IPv6 públicas.

Se abordó el diseño basado en la arquitectura TCP/IP, destacándose en este proyecto los cambios primordiales en las capas: uno (1) dos (2) de TCP/IP, porque es donde principalmente opera la infraestructura de red del ISP objeto de estudio, sin dejar de lado los cambios a nivel de capa superiores.

También, la investigación resolvió el problema de la empresa Telcorp en cuanto a la continuidad de la prestación del servicio de Internet dedicado, presentando una alternativa viable para seguir ofreciendo este servicio y alineado con las tecnologías actuales.

REFERENCIAS BIBLIOGRÁFICAS

Atelin, P y Dordoine, J. 2006. *Redes informáticas: conceptos fundamentales*. Ediciones ENI. Barcelona, España

Bagnulo, M (2005). "*Herramientas para la conectividad IPv6 con múltiples proveedores*." Trabajo de grado Doctoral. Universidad Carlos III de Madrid. Madrid, España.

Bavaresco, A. (1996). *Proceso Metodológico de la Investigación. 3era. Edición*. Servicios Bibliotecarios de la Universidad del Zulia. Maracaibo, Venezuela.

Baydal, E y otros (2005). *Curso de redes de computadores para ingenieros*. Editorial de la Universidad politécnica de Valencia (UPV). Valencia, España.

Blasco, T y Otero, L (2008). *La entrevista (I)*, Centro Nacional de Medicina Tropical. Instituto de Salud Carlos III. Nure Investigación, nº 33.

Bermúdez, 2005. *Internet y la globalización de la información.* URL: http://www.noticias.com/internet-y-la-globalizacion-de-la-informacion.32799. (Consulta: Febrero 04 ,2011)

Caridad, L y otros (2008). *Marco metodológico*. Universidad nacional experimental politécnica de la fuerza armada nacional. (UNEFA). Disponible: http://www.slideshare.net/emilmichinel/marco-metodolgico1-presentation (Presentación)

Castel. 1999. *La edad de la información tomo I edición en español*. Siglo XXI editores. Buenos aires, Argentina

Cisco Systems, Networking Academy (2008). *Aspectos Básicos de Networking*. URL:http://cisco.netacad.net. (Consulta: Febrero 16, 2011).

Díaz, H. 2006. *Técnica de Estudios II. Ilustrados.com*. Perú. URL: http://site.ebrary.com/lib/biblioelectronuclasp/Doc?id=10113728. (Consulta: julio 15, 2010).

España, M (2003).*Servicios avanzados de telecomunicación*. Ediciones Díaz de santos. Madrid, España.

Fernández, A (2010). *Tutorial de IPV6 .Universidad nacional autónoma de México*. Disponible: http://www.IPv6 .unam.mx/documentos/Tutorial-IPv6 -UNAM.pdf

Fernández, S y otros. (2002). *Estadística descriptiva*. Esic editorial. Madrid, España.

Forouzan,B (2002).Transmisión de Datos y Redes de Comunicaciones Segunda edición. McGarw-Hill Interamericana de España. Madrid, España.

Forouzan, B (2003). *Introducción a las ciencias de la computación*. Internacional Thomson editores. México DF, México.

Gamess, E (2008). *Propuesta para la implementación y la coexistencia de IPv4 e IPv6 en la red de datos de la Universidad Central de Venezuela***.** Trabajo de grado. Universidad central de Venezuela. Caracas, Venezuela.

González, J (2011). *Implementación del protocolo IPv6 en la Infraestructura de red de dato de la UCLA.* Trabajo de grado. Universidad Centroccidental Lisandro Alvarado. Barquisimeto, Venezuela.

Hernández, R. y otros (1.996) *Metodología de la investigación*. ED.: McGrawHill Interamericana, S.A. México DFMéxico.

Hernández, R. y otros (1.997) *Metodología de la investigación*. ED.: McGrawHill Interamericana, S.A. México DFMéxico.

Hernández, R. y otros (2000*) Metodología de la investigación*. ED.: McGrawHill Interamericana, S.A. México DFMéxico

Hurtado, I y Toro, J (2007). *Los libros del nacional. Paradigmas y métodos de investigación en tiempos de cambio*. Caracas Venezuela. Editorial CEC, SA

Hurtado, M. (2.000). *Metodología de la investigación holística*. ED.: SYPAL, Caracas Venezuela

IETF, 2011. URL: http://www.ietf.org/, (Consulta: Febrero 3, 2011)

Kaplan, A. (2010). *Proyecto de Documentación de FreeBSD .Manual de FreeBSD. Capítulo 29. Networking avanzado*. URL: **http://www.freebsd.org/doc/es/books/handbook/index.html.** (Consulta: febrero 23,2011)

LACNIC, 2011. *Nueva era en Internet: Se terminó el stock central de direcciones IPv4 de Internet*. URL: http://lacnic.net/sp/anuncios/2011-agotamiento-IPv4.html, (Consulta: febrero 3, 2011)

Landeau, R (2007). *Elaboración de Trabajo de Investigación*. Editorial Alfa. Caracas, Venezuela

Llorentes, O.2004. *Transición a IPv6 en un departamento universitario*. Trabajo de grado. Universidad Politécnica de Madrid. Madrid. España.

LYM Data comunications (2007). *La Red Inteligente: Ahorro energético y Telecomunicaciones.* LYM Data comunications. España.

Mañas, J. 2004. *Mundo IP*. Ediciones Nowtilus. Madrid, España.

Medina, M.P. (2006). *Los equipos multiculturales en la empresa multinacional: un modelo explicativo de sus resultados*". Tesis doctoral accesible a texto completo en http://www.eumed.net/tesis/2006/mpmb/. (Consulta Marzo 30, 2011)

Moreno, M. 2004. *IPv6 Interoperabilidad y robustez.* Trabajo de grado. Instituto politécnico Nacional. México DF, México.

Godoy, N. 2011. *Efecto del uso de las VPN en el rendimiento de la tecnología MPLS bajo el protocolo IPV6* . Trabajo de grado universidad del Zulia. Maracaibo, Venezuela.

Mujica, M. 2007. *Diseño de un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" Sede Rectoral.* Trabajo de grado. Universidad Centroccidental "Lisandro Alvarado". Barquisimeto. Venezuela.

Observatorio de la Sociedad de la Información en Navarra. *Clases de Infraestructuras y Redes*. URL http://www.cfnavarra.es/webgn/sou/instituc/dw/pdf/2clases%20de%20infraestructuras%20y%20redes.pdf (Consulta: Enero 15, 2011)

Ordoñez, S (2010). *Planeación de Infraestructura Tecnológica*. URL: http://tyraelmx.blogspot.com/2010/02/planeacion-de-infraestructura-fisica.html. (Consulta Marzo 03,2011)

Palet, J. 2009. *Tutorial de IPv6* . Consulintel. Madrid España.

Palet, J y otros (2009). *IPV Para todos: guía de uso y aplicación para diversos entornos.* ISOC ar. Asociación civil de argentinos en Internet. Buenos aires, Argentina

Palet, J (2011). URL: http://portalIPv6 .lacnic.net. (Consulta: febrero 4, 2011).

Puigdemunt T. y Alvarado G. (1999). *Introducción a las redes.* URL: http://www.pchardware.org/redes/redes_intro.php (Consulta: febrero 2, 2011).

Quemada, 2004. *Cátedra Telefónica en la UPM Internet de Nueva Generación. Hacia una Internet de Nueva Generación*. (Versión 6, 2 de Enero de 2004).

[RFC791] Internet Protocol (IP) URL: http://www.ietf.org/rfc/rfc791.txt (consulta Febrero 23,2011)

[RFC1519] Classless Inter-Domain Routing (CIDR) URL: http://www.ietf.org/rfc/rfc1519.txt (consulta Febrero 23, 2011)

RFC1631 The IP Network Address Translator (NAT) URL: http://www.ietf.org/rfc/rfc1631.txt (consulta Febrero 21,2011)

[RFC1918] Address Allocation for Private Internets URL: http://www.ietf.org/rfc/rfc1918.txt (consulta Enero 17,2011)

[RFC1933] Transition Mechanisms for IPv6 Hosts and Routers URL: http://www.ietf.org/rfc/rfc1933.txt (consulta Enero 17,2011)

[RFC2526] Reserved IPv6 Subnet Anycast Addresses URL: http://www.ietf.org/rfc/rfc2526.txt (consulta marzo 24,2011)

[RFC2529] Transmission of IPv6 over IPv4 Domains without Explicit Tunnels. URL: http://www.ietf.org/rfc/rfc2529.txt (consulta marzo 24,2011)

[RFC2375] IPv6 Multicast Address Assignments URL: http://www.ietf.org/rfc/rfc2375.txt (consulta Enero 17,2011)

[RFC2374] An IPv6 Aggregatable Global Unicast Address Format URL: http://www.ietf.org/rfc/rfc2374.txt (consulta Febrero 23,2011)

[RFC2460] Internet Protocol, Version 6 (IPv6) Specification URL: http://www.ietf.org/rfc/rfc2460.txt (consulta marzo, 15 2011)

Rodríguez, M y Zambrano A (2010) titulado "*Análisis y diseño de una reingeniería organizativa de la red del campus de la universidad técnica de Manabí mediante la utilización de IPV6 . Y su implementación en la facultad de ciencias informáticas en el laboratorio de redes*" Trabajo de grado. Universidad Técnica de Manabí. Manabí, Ecuador.

Ruiz, A (2008) . *Diseño de sistemas de respaldo de rutas para troncales tcp/ip en una empresa proveedora de servicios de internet e interconexión de redes*. Trabajo de grado. Universidad Simón Bolívar. Caracas, Venezuela.

Tanenbaum, A (2003). *Redes de computadora. Cuarta edición.* Pearson educación de México. SA. México.

Telcorp. *Manual de organización Sistemas Telcorp,* Ca. Home Page. URL: http://www.telcorp.com.ve (Consulta: enero, 29, 2011).

Universidad autónoma de Cali (2010). *Infraestructura tecnológica*. URL: http://www.slideshare.net/capa007/infraestructura-s5?from=share_email_logout3, (Consulta Marzo 12,2011).

Universidad Autónoma del Estado de México (2004) .*Guía ejecutiva para la elaboración de protocolos de tesis y tesis Segunda edición.* México DF, México

Universidad Centroccidental "Lisandro Alvarado". 2002. Manual para la Elaboración del Trabajo Conducente a Grado Académico de Especialización, Maestría y Doctorado. Sesión Ordinaria Nº 1353.

Universidad Nacional Experimental Sur del Lago "Jesus Maria Semprum" UNESUR. *Normas para la Elaboración y Presentación de los Trabajos de Grado*. (2008)

Universidad Experimental pedagógica Libertador. 2002. *Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales de la UPEL*.

Vladimirovna, O. (2002). *Fundamentos de Probabilidad y Estadística*. Universidad autónoma del estado de México. México.

Zuluaga, C (2009).*Administración de la Infraestructura Tecnológica*. URL: http://www.quindio.gov.co/home/docs/items/item_100/P-DAP-71AdministraciondelainfraestructuratecnologicaNV01.pdf (Consulta Marzo 12,2011).

Zapata, O (2005) *Herramientas para elaborar tesis e investigaciones socioeducativas*. Editorial Pax México DF, México.

ANEXOS

ANEXO 1.PRESENTACIÓN CORPORATIVA DE TELCORP